Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par
Jean Berstel, Alain Lascoux et Dominique Perrin

*

Tome 4 : 1956–1960

Institut Gaspard-Monge, Université Paris-Est
2009

Introduction
Tome IV : 1956–1960

L'article *Une théorie algébrique du codage* [1956-3] est un texte fondateur. Cet exposé au séminaire d'algèbre de Paul Dubreil (suivi d'une publication comme note aux Comptes rendus [1956-5]) contient en effet la présentation de la problématique du codage en termes algébriques et, notamment le fait que la propriété de décodage unique équivaut à celle d'une base d'un sous-monoïde libre. L'article contient notamment la caractérisation des sous-monoïdes libres comme des sous-monoïdes *libérables* (on dit maintenant *stables* et Paul Cohn parle d'*anti-idéaux* [3]).

Une version en anglais est présentée à un colloque IRE au MIT *On the application of semigroup methods to some problems in coding* [1956-6]. Elle contient cette jolie illustration de la définition d'un ensemble complet à droite (on disait alors *net à droite*) : « If M is the free semigroup of all phonetic sentences in English and M' the subset of all *semantically correct sentences*, M' is neat in M. For instance : "pri wat law chur coco feet" (obtained from King Lear, Act III, with Tippet's help) is fitted into a complete message in M' by adding : "...and this gentlemen, was, may-be, my best example of a semantically void utterance" ».

La note *Jeux de Nim et solutions* [1956-8], avec Claude Berge, fait suite à une première note [1], signée de Claude Berge seul, et qui porte elle aussi sur les fonctions de Grundy sur les graphes infinis.

La note aux Comptes-Rendus $\mathcal{D}$ *représentation des demi-groupes* [1957-1] contient la définition de ce que Clifford et Preston nommeront dans leur livre [2] le *groupe de Schützenberger* d'une $\mathcal{H}$-classe et les *représentations de Schützenberger* relatives à une $\mathcal{D}$-classe. Elle fait suite à une note préliminaire *Sur une représentation des demi-groupes* [1956-9] publiée l'année précédente dans laquelle la représentation est relative à l'idéal minimal et pour laquelle le groupe est le groupe de Suschkevitch. Elle sera suivie d'une nouvelle note *Sur la représentation monomiale des demi-groupes* [1958-4] donnant une construction plus générale.

La note *Sur une propriété combinatoire des demi-groupes libres* [1957-3] est une preuve erronée de la conjecture sur l'équivalence commutative des codes maximaux aux codes préfixes dont il sera question plus loin (tome 9).

L'article *Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées* [1958-3] est la première présentation des liens entre bases des algèbres de Lie libres, factorisations des monoïdes libres et codes comma-free (qui sont le « problème de mathéma-

tiques appliquées » dont il est question).

L'article *A characteristic property of certain polynomials of E. F. Moore and C. Shannon* [1959-1] est publié dans une revue à diffusion limitée et contient l'énoncé de ce qui est maintenant connu comme le théorème de Kruskal-Katona (voir [4]).

La note *Sur l'équation* $a^{2+n} = b^{2+m}c^{2+p}$ *dans un groupe libre* [1959-2] est une préfiguration de l'article publié avec Roger Lyndon [1962-5].

---

[1] Claude Berge. La fonction de Grundy d'un graphe infini. *C. R. Acad. Sci. Paris*, 242 :1404–1407, 1956.

[2] Alfred H. Clifford and Gordon B. Preston. *The Algebraic Theory of Semigroups. Vol. I.* Mathematical Surveys, No. 7. American Mathematical Society, Providence, R.I., 1961.

[3] Paul M. Cohn. *Free Rings and Their Relations*, volume 19 of *London Mathematical Society Monographs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, second edition, 1985.

[4] Donald E. Knuth. *The Art of Computer Programming. Vol. 4, Fasc. 3.* Addison-Wesley, Upper Saddle River, NJ, 2005. Generating all combinations and partitions.

Année 1956

Bibliographie

[1] M. H. Hecaen, J. de Ajuriaguerra, and Marcel-Paul Schützenberger. De l'influence relative de l'hypertension intracranienne et de la localisation sur les troubles psychiques au cours de tumeurs cérébrales. *Revue neurologique*, 94(3) :259–263, 1956. Séance du 2 février 1956.

[2] M. E. Martin, Ph. Paumelle, and Marcel-Paul Schützenberger. Observation statistique sur le rang dans la fratrie des alcooliques. *Revue de l'alcoolisme*, 4(4) :109–112, 1956.

[3] Marcel-Paul Schützenberger. Une théorie algébrique du codage. In *Séminaire Dubreil-Pisot, année 1955-56*, Exposé No. 15, 27 février 1956, 24 pages. Inst. H. Poincaré, Paris, 1956.

[4] Marcel-Paul Schützenberger. Théorie du codage et des événements récurrents. In *Séminaire de calcul des probabilités*, 16 mars 1956, 11 pages. Publ. Inst. Statist. Univ. Paris, Inst. H. Poincaré, Paris, 1956.

[5] Marcel-Paul Schützenberger. Une théorie algébrique du codage. *C. R. Acad. Sci. Paris*, 242 :862–864, 1956.

[6] Marcel-Paul Schützenberger. On the application of semigroup methods to some problems in coding. *IRE Trans. Inf. Theory*, IT-2 :47–60, 1956.

[7] Marcel-Paul Schützenberger. On some measures of information used in statistics. In *Third London Symposium on Information Theory, Sept. 12th to 16th, 1955*, pages 18–25. Butterwords Scientific Publications, London, 1956.

[8] Claude Berge and Marcel-Paul Schützenberger. Jeux de Nim et solutions. *C. R. Acad. Sci. Paris*, 242 :1672–1674, 1956.

[9] Marcel-Paul Schützenberger. Sur une représentation des demi-groupes. *C. R. Acad. Sci. Paris*, 242 :2907–2908, 1956.

[10] Marcel-Paul Schützenberger. Sur deux représentations des demi-groupes finis. *C. R. Acad. Sci. Paris*, 243 :1385–1387, 1956.

Imprimé avec le périodique
REVUE NEUROLOGIQUE

Tome 94 — N° 3 — 1956
(pp. 259-263).

DE L'INFLUENCE RELATIVE DE L'HYPERTENSION INTRACRANIENNE ET DE LA LOCALISATION SUR LES TROUBLES PSYCHIQUES AU COURS DES TUMEURS CÉRÉBRALES,

PAR MM.

P. SCHUTZENBERGER, H. HECAEN et J. de AJURIAGUERRA

Notre matériel se compose de 439 tumeurs cérébrales observées dans le service du Pr Agrégé M. David. Les troubles mentaux ont été constatés dans 229 de ces observations. Une étude détaillée de ces observations fait l'objet d'une monographie, actuellement sous presse ; aussi cette communication n'aura-t-elle pour but que d'en discuter un aspect important au point de vue méthodologique.

L'examen psychiatrique a été conduit chez tous ces malades par deux d'entre nous. Pour permettre l'étude statistique, les divers troubles psychiques ont été classés sous 3 grandes rubriques : états confuso-démentiels, troubles de l'humeur et du caractère, troubles paroxystiques.

Nous avons réuni sous la rubrique des états confuso-démentiels toute une gamme d'états déficitaires s'étendant depuis l'état d'obtusion à la détérioration intellectuelle.

Par troubles de l'humeur et du caractère, nous entendons les modifications de la sphère thymique et de la personnalité.

A côté de ces états permanents, nous avons isolé les désordres paroxystiques principalement centrés sur les manifestations hallucinatoires.

La localisation a été affirmée d'après les constatations autopsiques ou opératoires, exceptionnellement par des données neuroradiologiques. En vue de l'étude statistique, nous avons dû procéder à un certain regroupement, sur la classification régionale utilisée dans notre travail d'ensemble ; nous laissons inchangés les groupes des tumeurs, frontales, mésodiencéphaliques et sous-tentorielles. Par contre, nous avons réuni les tumeurs temporales et fronto-temporales, préférant adjoindre ce dernier groupe aux tumeurs temporales qu'aux frontales. En effet, si nous modifions ainsi très certainement la proportion des troubles paroxystiques nous devons d'emblée signaler que la recherche statistique n'a pour ces manifestations qu'un intérêt limité, étant donné le caractère d'évidence clinique. D'autre part, une tumeur fronto-temporale n'atteint pas, en général, du moins de manière importante, la région fronto-polaire.

Un dernier groupe, étiqueté « Reste », a été constitué par les tumeurs rolandiques, pariétales et occipitales, auxquelles nous avons joint les rares cas de tumeurs calleuses (la plupart des atteintes calleuses de notre série ont été classées parmi les tumeurs bifrontales).

Nous avons admis comme critère de l'hypertension intracranienne la stase papillaire, en classant comme tels les aspects ophtalmoscopiques allant du simple œdème papillaire à la stase avec exsudats et hémorragies. Il nous a paru, en effet, que les autres signes de l'hypertension intracranienne dépendaient trop de l'interprétation personnelle. En outre, pour ne pas subdiviser à l'extrême nos groupes, il ne nous a pas été possible de tenir compte des degrés de l'œdème papillaire ; d'ailleurs, il nous paraît difficile d'apprécier par ce seul symptôme les degrés d'intensité de l'œdème cérébral et de l'hypertension réelle.

Nous insisterons ultérieurement sur le fait qu'aucune discontinuité nette ne peut répondre à la notation en « stase » ou « absence de stase » et qu'il s'agit là essentiellement d'une variable continue.

La fréquence relative des divers troubles et de leur association ne sera pas envisagée ici.

On doit étudier d'abord les rapports entre les deux critères de base retenus : la localisation d'une part, l'hypertension intracranienne d'autre part, cette dernière appréciée par la présence de stase papillaire identifiée opérationnellement à l'hypertension.

Effectivement, le pourcentage des stases n'est pas le même dans les différentes localisations, comme en permettent de juger les chiffres (1re colonne du tableau). Un test d'homogénéité par χ^2 établit la réalité des différences observées. $\chi^2 = 15{,}2$ pour 4 degrés de liberté.

Notons d'emblée que le pourcentage le plus élevé se rencontre dans le groupe frontal, suivi par le groupe sous-tentoriel, puis par le groupe temporal, puis par le reste et enfin par le groupe mésodiencéphalique.

L'étude statistique sera réalisée groupement psychiatrique par groupement psychiatrique, tels qu'ils ont été définis plus haut. La stase et la localisation étant liées, ne peuvent donc être traitées ensemble. Il nous faut ainsi considérer 10 groupes, c'est-à-dire chacun de nos groupements régionaux sous l'angle stase et absence de stase et les envisager de façon distincte.

Cette manière de faire est seule possible et on doit attirer l'attention des chercheurs sur ce point puisque des travaux statistiques comme ceux de Busch repris par Maxwell ne peuvent aboutir à des conclusions nettes en raison du fait que sont seules accessibles d'une part la fréquence de la stase par localisation, et d'autre part la fréquence des troubles psychiatriques par localisation sans qu'existe la possibilité d'établir la corrélation entre eux.

I. — Les états confuso-démentiels.

Les chiffres (cf. tableau) permettent les constatations suivantes :

1° dans un groupe comme dans l'autre, l'extrême diversité des fréquences des états confuso-démentiels selon la localisation. Par exemple, on note 63 p. 100 de troubles confusionnels pour le groupe frontal et 28,1 p. 100 pour le groupe sous-tentoriel ;

2° le parallélisme de ces fréquences par localisation dans le groupe présentant de la stase et dans le groupe n'en présentant pas ; dans les deux cas, le groupe frontal vient en tête tandis que le groupe sous-tentoriel est en fin de liste ;

3° pour chaque localisation, la moindre fréquence des états confusionnels pour le groupe sans stase papillaire que pour le groupe avec stase papillaire.

Ceci indique, et un calcul plus raffiné pourrait le prouver formellement, que la stase papillaire — en soi, si l'on peut dire, parce qu'elle dépend déjà de la localisation — a un rôle au moins adjuvant sur la manifestation des troubles, mais, d'autre part, montre que, même avec un facteur stase constant (sous réserve d'une discussion ultérieure), ces localisations par elles-mêmes ont une importance différente.

	Stase	Etats confuso-démentiels			Troubles Humeur et caractère			Troubles paroxystiques		
	(S +)	S +	S —	Total	S +	S —	Total	S +	S —	Total
Frontal.....	60/80 = % 75,0	38/60 = % 63,3	10/20 = % 50,0	60,0	20/60 = % 33,3	10/20 = % 50,0	37,5	4/60 = % 6,7	4/20 = % 20,0	10,0
Fronto-temporal et Temporal.....	58/99 = 58,0	24/58 = 50,0	13/41 = 31,7	42,4	12/58 = 20,6	10/41 = 24,3	22,2	17/58 = 29,3	1/41 = 17,0	24,0
Mésodiencéphalique.....	26/61 = 42,6	8/26 = 30,7	8/35 = 22,8	26,2	10/26 = 38,4	3/35 = 8,5	21,3	5/26 = 11,5	5/35 = 14,2	13,1
Reste.....	61/114 = 53,5	22/61 = 36.1	14/53 = 26,4	31,6	13/61 = 21,3	6/53 = 11,3	16,7	8/61 = 13,1	6/53 = 11,3	12,3
Sous-tentoriel..	57/85 = 67,0	16/57 = 28,1	3/28 = 10,7	22,4	8/57 = 14,0	2/28 = 7,1	11,8	1/51 = 12,3	2/28 = 7,1	10,7
Total,.....	262/439 = 59,68	119/262 = 43,1	48/177 = 27,1		63/262 = 24,0	31/177 = 17,5		39/262 = 14,9	24/177 = 13,5	

II. — Troubles de l'humeur et du caractère et troubles paroxystiques.

Il faut faire remarquer d'emblée que le phénomène est beaucoup moins net pour les troubles paroxystiques. En effet, la classification utilisée pour ces troubles a été globale, réunissant aux désordres hallucinatoires d'autres manifestations d'ailleurs rares. En outre, la plus grande majorité des manifestations hallucinatoires relève de l'atteinte temporo-occipitale.

Les troubles paroxystiques ont surtout été introduits dans ce tableau par souci de complétude. En ce qui concerne les troubles de l'humeur et du caractère, le phénomène est en gros le même que pour les états confuso-démentiels, c'est-à-dire qu'on note une fréquence inégale des troubles selon le siège et quelle que soit la stase — et ceci de façon relativement parallèle dans les deux groupes.

Cependant, on doit souligner quelques discordances assez nettes :

1° Dans le groupe frontal, tant pour les troubles de l'humeur et du caractère que pour les troubles paroxystiques, il existe une différence entre leurs fréquences selon la stase, différence qui est inverse de celle à laquelle on aurait pu s'attendre.

Quoique cette différence ne soit pas significative, elle prend toute sa valeur par contraste avec l'influence générale de la stase sur les troubles mentaux.

Tout au moins pour les troubles de l'humeur et du caractère, on peut suggérer à titre d'hypothèse que cette discordance provient de ce que lorsque la stase est présente, la confusion très fréquente dans le groupe frontal avec stase masque les troubles de la personnalité ;

2° Dans le groupe mésodiencéphalique, à l'inverse, la présence de la stase semble avoir un effet favorisant très important sur l'apparition des troubles de l'humeur, à un point tel qu'il faut faire passer du premier au dernier rang leur fréquence du groupe avec stase au groupe sans stase. Là aussi une hypothèse peut être suggérée, avant d'admettre qu'il s'agit d'un phénomène aléatoire ; la stase est habituellement le fait des tumeurs infiltrantes susceptibles d'atteindre plus intensément les mécanismes hypothalamiques.

Il faut noter d'ailleurs que sur l'ensemble des 15 groupes de pourcentage examinés, il est presque nécessaire logiquement que certains présentent des irrégularités par rapport aux tendances générales et ainsi que notre discussion *a posteriori* de ces irrégularités ne saurait être que difficilement concluante.

3° On notera enfin que, dans l'ensemble et pour autant que l'on puisse l'apprécier, l'influence différentielle de la stase est très nettement moins importante pour les troubles de la personnalité que pour les troubles confusionnels considérés isolément (les chiffres n'auraient qu'une valeur indicative $\chi^2 = 2.68$) et qu'elle est presque nulle pour les troubles paroxystiques.

4° Il est intéressant de remarquer la décroissance régulière de la fréquence des troubles de l'humeur et du caractère depuis la localisation frontale jusqu'à la localisation sous-tentorielle. Le groupe mésodiencéphalique se classant correctement avant le reste (principalement composé de tumeurs pariétales et occipitales).

Discussion générale.

Indépendamment du groupement psychiatrique étudié, deux faits se dégagent des chiffres présentés :

1° l'effet de la stase à l'intérieur d'un même groupe régional ;

2° l'effet de la localisation à l'intérieur des individus présentant de l'hypertension intracranienne telle qu'elle est jugée par le critère de stase.

Néanmoins, un examen plus attentif des chiffres montre, pour les deux premiers groupes cliniques, un parallélisme de fréquence des troubles avec les fréquences de la stase en fonction des localisations. Ceci avec l'exception notable du groupe sous-

tentoriel qui présente à la fois le moins de troubles psychiatriques dans l'ensemble et le plus de stase (à l'exception du groupe frontal).

Ce parallélisme existe dans les chiffres de Bushtable 1 de Maxwell (une estimation très grossière de ce parallélisme est fournie par un coefficient de corrélation par un rang ρ de Spearman $= 0{,}75$) : le seul cas nettement discordant étant celui des méningiomes qui donnent d'ailleurs dans les chiffres de Bush un chiffre anormalement élevé de « torpeur ».

En raison des données admises sur le rôle de la région sous-tentorielle, il semble normal que sa gravité psychiatrique soit moindre que celle des autres groupes. Aussi, nous l'écarterons désormais de la discussion.

Ceci fait, le parallélisme entre gravité psychiatrique et stase devient rigoureux pour les états confuso-démentiels et encore très satisfaisant pour les troubles de l'humeur et du caractère, et on doit se demander s'il n'y aurait pas là une simple conséquence de la méthode d'observation employée. En effet, l'hypertension intracranienne dont la stase n'est qu'une manifestation, varie continuellement d'un malade à l'autre sans présenter vraisemblablement la discontinuité nette que suggère la notation « stase » ou « non-stase ». Il est donc normal que si un groupe défini par un autre critère présente une fréquence élevée de stase, ceci signifie en réalité que le degré moyen d'hypertension intracranienne de ses membres soit plus élevé aussi bien pour les sujets classés dans le groupe avec stase que parmi les sujets classés dans le groupe sans stase. Ainsi donc, il nous est impossible d'éliminer parfaitement l'influence de l'hypertension intracranienne de nos statistiques, et il ne nous est donc pas possible, sur la base des chiffres rassemblés, d'exclure entièrement l'hypothèse que les différences entre localisations (à l'exception du groupe sous-tentoriel proviennent, tout au moins en partie, de celles-ci.

Conclusions.

Les questions et réponses suivantes résument le plus nettement nos conclusions :

1° la localisation est-elle toujours sans influence ? Non, car les localisations sous-tentorielles donnent un pourcentage de troubles psychiques très inférieur à celni des autres localisations, bien que le facteur stase y soit particulièrement marqué.

2° la localisation à l'intérieur des groupes définis a-t-elle toujours de l'influence ? Tel est notre sentiment d'après les chiffres présentés, mais on ne peut exclure l'hypothèse selon laquelle ce serait l'hypertension intracranienne qui aurait le rôle prédominant dans le déclenchement des troubles psychiatriques au cours des tumeurs supratentorielles.

(*Travail du Centre Neuro-Chirurgical des Hôpitaux psychiatriques de la Seine, Pr agrégé Marcel David.*)

LA REVUE DE L'ALCOOLISME

Trimestrielle

Editée par
Le Groupement Médical d'Etudes sur l'Alcoolisme
et
Le Comité National de Défense contre l'Alcoolisme

TOME IV N° 4

Octobre - Décembre 1956

RÉDACTION ET ADMINISTRATION : 14 *bis*, Rue d'Alger - NANTES
Abonnement : 500 frs C. P. Groupement Médical Nantes 719-83
Etranger : 650 frs
Le Numéro : 150 frs

E. MARTIN, M. P. SCHUTZENBERGER et Ph. PAUMELLE.

OBSERVATION STATISTIQUE SUR LE RANG DANS LA FRATRIE DES ALCOOLIQUES

Le 14 juin 1952 dans la « Semaine des hôpitaux de Paris », DUCHENE, SCHUTZENBERGER, BIRO et SCHMITZ publiaient leur observation statistique sur l'écart d'âge des couples dont le mari est alcoolique. Une réflexion clinique les avait amenés à remarquer la fréquence des hommes alcooliques chroniques ayant épousé des femmes d'un âge très supérieur au leur. La statistique effectuée sur un échantillon de 145 hommes mariés avait confirmé cette impression.

Une démarche analogue nous a amenés à tenter de préciser les particularités du rang dans la fratrie de nos malades. De telles études ont, pour nous, le grand mérite d'éclairer les contours de la personnalité de l'alcoolique. Nous sommes, en effet, de plus en plus persuadés que l'alcoolisme chronique est le fait de personnalités présentant une structure très particulière. La génèse des troubles fait sans doute intervenir de très nombreux facteurs tant organiques que psychologiques ; le fait de préciser certains aspects de leur histoire et leur situation familiale contribuera, nous semble-t-il, à fonder d'une manière objective le mode d'abord thérapeutique sous un angle psychothérapique au sens large du mot.

Pour étudier le rang dans la fratrie, nous avons choisi deux échantillons :

— 206 malades dont 171 hommes et 35 femmes } consultation du Dr PAUMELLE dans le 13e arrondissement.

— 264 malades dont 221 hommes et 43 femmes } consultation du Dr MARTIN au Pré-St-Gervais.

Ces deux groupes représentant tous les malades venus consulter en 1954 et 1955 pour lesquels les renseignements sur la fratrie avaient pu être relevés. Nous avons éliminé dans les deux échantillons toutes les structures familiales complexes (enfants de plusieurs lits).

Voici leur distribution en isolant les derniers de famille (Tableau p. 110).

HOMMES

XIII^e arrondissement

Nombre d'enfants dans la famille	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
derniers de famille	28	22	15	4	4	5	2	1	1								0	1	
TOTAL des malades	28	40	34	16	18	14	5	5	3	1	2	1	2	0	1	0		1	

soit **55 derniers de famille** (fils uniques éliminés) sur **171 malades**

Pré-St-Gervais

Nombre d'enfants dans la famille	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
derniers de famille	26	16	10	8	3	4	3	2	2	1	1	2							
TOTAL des malades																			

soit **52 derniers de famille** (fils uniques éliminés) sur **221 malades**

FEMMES

XIII^e arrondissement

Nombre d'enfants dans la famille	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
dernières de famille	9	6	3	1	3	2	1					1							
TOTAL des malades	9	6	3	3	4	5	1	1	1	0	0	1	1						

soit **17 dernières de famille** (filles uniques éliminées) sur **35 malades**

Pré-St-Gervais

Nombre d'enfants dans la famille	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
dernières de famille	8	4	3	0	1	0	1	1	0	1	0	0	1						
TOTAL des malades	8	7	8	1	5	4	2	2	1	2	0	1	1	0	1				

soit **12 dernières de famille** (filles uniques éliminées) sur **43 malades**

L'analyse de ces documents permet les remarques suivantes :

— Les deux échantillons sont grossièrement comparables du point de vue proportion des sexes ; les femmes représentent 16, 3 % du total du Pré-St-Gervais et 16 % du total des malades dans le 13e arrondissement ;

Les familles nombreuses sont plus largement représentées à la consultation du Pré-St-Gervais dans les deux sexes ;

— Si l'on calcule le nombre théorique des derniers de famille que l'on aurait dû rencontrer, en supposant que la prédisposition à l'alcoolisme soit la même quelque soit le rang de naissance, on trouve :

	XIIIe		Pré-St-Gervais	
	H	**F**	**H**	**F**
Valeur théorique : (1)	43,54	6,92	49,04	9,25
Valeur observée :	55	17	52	12

On constate que dans les deux échantillons, un nombre très supérieur de derniers de famille (que le calcul révèle être significatif dans les deux sexes) est indiscutable. On observera :

1° que le phénomène est toujours plus net chez les femmes ;

2° que dans l'échantillon de la consultation du Pré-St-Gervais, le phénomène n'apparaît nettement que pour les familles nombreuses (6 enfants et plus).

En se limitant à celles-ci, on trouve :
Pré-St-Gervais - Hommes : (familles de plus de 6 enfants)
valeur théorique : (1) 10,44
valeur observée : 15

3° que les enfants uniques dont il n'a pas été tenu compte dans les calculs précédents, ont une fréquence différente dans les deux sexes.

Pourcentage des enfants uniques sur le total des 2 échantillons :
Hommes : 13,8 %
Femmes : 21,8 %

4° un calcul analogue, une fois éliminés les derniers-nés, ne révèle aucune différence significative selon le rang de naissance.

On peut, cependant, être frappé d'une relative fréquence des avant-derniers.

Nous devons souligner le contraste entre les recrutements des deux consultations envisagées :

I. — CONSULTATION DU PRE-ST-GERVAIS :

Milieu culturel et social relativement pauvre avec fratries nombreuses particulièrement fréquentes. La quasi-totalité des malades est adressée par les services sociaux et le volontariat l'exception.

Les derniers-nés sont en règle l'objet de frustrations relativement importantes : rejet favorisé par des conditions économiques difficiles. Famille souvent elle-même perturbée sur le plan affectif.

---

(1) Total des quotients du nombre des malades appartenant à chaque fratrie sur le nombre d'enfants de ladite fratrie.

II. — CONSULTATION DU XIIIe ARRONDISSEMENT :

Milieu culturel et social très varié et prédominance des fratries de deux ou trois enfants — 49 % des volontaires — les derniers-nés sont assez souvent de familles unies et ont rarement été l'objet de frustrations matérielles, les formes diverses d'hyperprotection dont ils ont fait l'objet de la part des parents ne leur ayant pas permis d'acquérir une personnalité d'adulte.

Les données statistiques que nous venons d'évoquer, selon nous, doivent être interprêtées dans le cadre des facteurs d'immaturation de la personnalité. Leur étude détaillée montre que des évènements identiques mais profondément différents quant au vécu du sujet, peuvent intervenir dans la génèse de l'alcoolisme chronique.

Dr PAUMELLE :

Permettez-moi, avant de terminer, une réponse rapide aux interventions sur mon rapport.

Je suis extrêmement heureux de constater l'accord de M. Lereboullet sur la majorité des points de mon rapport.

Qu'il me permette seulement de revenir sur une question particulièrement importante, celle du temps consacré à chaque malade. Il pense que les normes que je propose sont trop larges. Pour ma part, je persiste à les considérer comme nécessaires si l'on vise une psychothérapie du malade, en plus de l'examen somatique et du contrôle de la sobriété.

Un petit point très particulier sur la question importante qu'a abordée M. Lecomte : celle des rapports entre les services de police et les dispensaires. Il a tout à fait raison de dire qu'il ne s'agit pas d'avoir, pour le médecin, une attitude démagogique. J'espère que ce n'est pas ce qu'on a tiré de mon propos.

Professeur HEUYER (Paris).

— Il est tard. Je n'ai pas l'intention de faire de très longs commentaires.

Je remercie d'abord les rapporteurs : M. PAUMELLE et M. DUCHENE de leurs très remarquables rapports. Le rapport de M. PAUMELLE est un rapport très administratif. Le rapport de M. DUCHENE est un rapport plus médical, dans l'étude de chaque cas.

Il y a d'abord un point indiscutable : les consultations pour alcooliques sont utiles : elles sont même nécessaires dans l'état actuel des choses. Les résultats qui ont été obtenus sont, dans l'ensemble, satisfaisants. On considère qu'il y a un quart de bons résultats. 25 % de bons résultats, c'est déjà quelque chose ! Comme le disait M. DUCHENE, un quart de bons résultats permet de diminuer singulièrement la charge des finances, quand on sait ce que coûte un internement ou la prison, pour des sujets qui, s'ils n'étaient pas passés par la consultation, seraient certainement devenus une charge sociale au lieu de recommencer de travailler et d'être utiles à leurs familles. Par conséquent, il ne peut être question de discuter l'utilité de ces consultations.

Dans les communications qui ont été faites, on a insisté beaucoup sur le point de vue psychologique des causes de l'alcoolisme. Monsieur MARTIN a trouvé la raison de ces alcoolismes individuels dans des conflits personnels, qui remontent à l'enfance. M. PAUMELLE vient de faire une étude très intéressante, au point de vue de la statistique, sur le rang familial dans la fratrie

Séminaire Dubreil.
Algèbre et théorie
des nombres

M. P. Schützenberger

Une théorie algébrique du codage

Séminaire Dubreil. Algèbre et théorie des nombres, tome 9 (1955-1956), exp. n° 15, p. 1-24.

<http://www.numdam.org/item?id=SD_1955-1956__9__A10_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire P. DUBREIL et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1955/1956
-:-:-:-

27 février 1956

Exposé n° 15

UNE THÉORIE ALGÉBRIQUE DU CODAGE,

par M.P. SCHÜTZENBERGER.

Introduction.

Soient donnés deux ensembles discrets (en général finis dans la pratique) :

Λ_0 : l'ensemble des messages élémentaires

A_0 : l'ensemble des lettres ou "alphabet".

En théorie des communications, le problème du codage consiste à représenter les messages, c'est-à-dire les suites de messages élémentaires par des suites de lettres selon une règle fixée à l'avance (un "code" ou "dictionnaire") de telle sorte que la retraduction soit possible et ceci en fonction d'exigences techniques de nature diverse.

Par exemple, Λ_0 étant l'ensemble des signes typographiques habituels et A_0 un "alphabet" consistant en les trois "lettres" "point" "trait" et "intervalle".

Le code télégraphique morse est le système de convention dans lequel "a" est représenté par "point trait intervalle" , "b" par "trait point point point intervalle" ... etc. On appellera respectivement "codage" et "décodage" les deux opérations inverses qui font passer des suites de messages aux suites de lettres et réciproquement.

Plus généralement on pourrait voir dans tout langage, naturel ou artificiel, un code (plus souvent d'ailleurs : une série de codes superposés : phonémiques, grammaticaux, sémantiques, etc.) traduisant en sons, signes ou gestes des idées, des sentiments, etc. Une définition encore plus générale a été étudiée par J. Riguet [1] , et nous désignerons ici, pour abréger, sous le nom de "codes", certaines structures qui idéalisent les restrictions plus ou moins explicitement ou rigoureusement admises par la quasi-totalité des systèmes utilisés dans la théorie des communications stricto sensu :

1°) Universalité : Toute suite de messages élémentaires correspond à une suite de lettres au moins.

2°) Catégoricité : Cette suite de lettre est unique pour une suite de messages élémentaires donnée.

3°) Univocité du décodage : Réciproquement, si une suite de lettres correspond à une suite de messages élémentaires, cette dernière est unique.

4°) Isomorphie : Si les messages " λ " et " μ " sont codés respectivement par " ℓ " et "m" , le message " $\lambda\mu$ " est codé par " ℓ m".

Le code morse satisfait rigoureusement à ces quatre conditions et aussi, dans une certaine mesure, ce code compliqué qu'est la transcription orthographique française du langage parlé(1).

Formellement il est clair que les conditions énoncées conduisent à la :

Définition :

Λ et A étant respectivement les demi-groupes libres engendrés par Λ_0 et A_0 , une application $\mathcal{C}$ de Λ_0 sur une partie P_0 de A sera un code, si et seulement si l'extension de $\mathcal{C}$ à Λ détermine un isomorphisme de Λ sur le sous-demi-groupe P de A engendré par les suites de lettres constituant P_0 .

On appellera "mot" les suites de lettres constituant P_0 et, pour abréger, "message" aussi bien les éléments de P que ceux de Λ . Un code sera défini par la donnée de Λ_0 , A_0 et $\mathcal{C}$, ou plus fréquemment par celle de A et de P , puisque, A et P étant des demi-groupes, leur donnée implique celle de leurs générateurs.

---

(1) Les contre-exemples suivants illustrent la signification des conditions précédentes :

ad 1°) : le phonème "t*" (le click dental du Bantou, utilisé en France pour stimuler les chevaux) est intranscriptible dans l'orthographe française.

ad 2°) : le phonème "K" est codé K (Képi) ou ch (choléra) ou c (carotte) ou qu (quai).

ad 3°) : la graphie "ent" code plusieurs phonèmes distincts (vent, vient viennent).

ad 4°) : la graphie "oi" qui se lit "ua" et devrait s'écrire "oua".

15-03

La définition précédente fait apparaitre la théorie de codage comme une application de la théorie des demi-groupes. Il est particulièrement remarquable que les concepts fondamentaux de cette dernière, introduits par P. Dubreil [3], [4], [5] en 1941, et étudiés depuis par lui-même et son école du point de vue abstrait, aient des interprétations immédiates et importantes sur le plan de la réalisation concrète des machines codeuses ou transcodeuses.

Sous un autre angle, la théorie des événements récurrents de W. Feller [6], dans laquelle on étudie des processus stochastiques sur les suites de lettres à partir d'autres processus définis sur les suites de messages élémentaires, et réciproquement se rattache étroitement à la théorie du codage, comme l'a montré Mandelbrot qui a utilisé cette analogie dès 1951 [7], [8] : les processus récurrents sont des codes unitaires au sens que nous donnerons plus loin à ce terme. En retour, l'extension par Feller lui-même de sa théorie à des alphabets topologiques spéciaux, ouvre la voie à des généralisations intéressantes qui feront l'objet d'un exposé ultérieur.

Enfin, la théorie développée ici est une théorie "sans bruit" dans laquelle on ne se préoccupe pas des problèmes que pose au décodeur une altération d'origine aléatoire des messages à décoder. Le contraste avec les travaux actuels sur cette question (Cf : [10] ou [11] par exemple) est moins grand qu'il ne paraît. En particulier, la notion de "code absorbant" y joue un rôle considérable, et ne sera ici l'objet que de remarques incidentes.

Exemple.

L'exposé sera simplifié si un exemple est traité qui montre la nature du problème :

Soit le code[2] suivant dans l'alphabet $A_0 = \{ a, b, c \}$:

$\mathcal{C}\alpha \to a$; $\mathcal{C}\beta = bb$; $\mathcal{C}\gamma = c$; $\mathcal{C}\delta = ab$; $\mathcal{C}\varepsilon = bcb$.

Il n'y a aucune difficulté à réaliser le codage d'une suite de messages élémentaires. Par exemple : $\mathcal{C}(\alpha\,\varepsilon\,\delta\,\varepsilon) = abcbabbcb = m$.

Le décodage par contre n'est pas aussi direct : en procédant de gauche à droite, en effet, le "a" initial est, a priori, aussi bien "α" que la première lettre du mot δ . Cependant cette dernière hypothèse est prouvée fausse, car "c" (troisième lettre du message) devrait être lu "γ" et la séquence restante (babbcb) ne pourrait pas être décodée puisqu'aucun mot ne commence par "ba". Donc selon des notations évidentes :

(2) On prouvera plus loin qu'il s'agit bien d'un code.

15-04

$$m = \alpha.\ bcb.abbcb = \alpha\xi abbcb = \alpha\xi m'$$

La même ambiguité se présente à nouveau : si la lettre initiale "a" du message restant m' était α on aurait nécessairement : $m' = \alpha bbcb = \alpha\beta cb = \alpha\beta\gamma b$ et b resterait sans pouvoir être décodé. Donc : $m' = \delta bcb = \delta\varepsilon$ et l'on retrouve bien $\mathcal{C}_m^{-1} = \alpha\xi\delta\varepsilon$. Observons au passage qu'il se peut que l'ambiguité ne soit susceptible d'être levée qu'avant un délai très long :

Le message $q = a(bbc)^n$ (a suivi de n-fois bbc) correspond à $\alpha(\beta\gamma)^n$, et le message $qb = a(bbc)^n b$ correspond à $\delta\varepsilon^n$.

Il est donc nécessaire :

1°) De systématiser les méthodes de décodage (2e section).

2°) De rendre possible leur mécanisation en les simplifiant au maximum par l'emploi de structures moins lourdes que les demi-groupes libres A et P : (3e section).

3°) D'étudier des codes particulièrement maniables (les codes unitaires nets) et de montrer qu'ils forment une "classe admissible" en ce sens qu'ils sont aussi efficaces que n'importe quel autre code du point de vue de la longueur moyenne des mots. (3e et 4e section).

1.- Méthodes de décodage.

Soient A un demi-groupe libre, P un sous-demi-groupe de celui-ci. Le premier problème sera de caractériser algébriquement les P susceptibles de correspondre à un code.

On posera : $P_0 = P - ((P - \emptyset)^2 \cup \emptyset)$ = l'ensemble des $p \in P - \emptyset$ tels que $p'p'' \in P$ et $p', p'' \in P$ impliquent $p' = \emptyset$ ou $p'' = \emptyset$ (3). Comme A est un demi-groupe libre chaque élément possède une "longueur" (le nombre de générateurs figurant dans son expression) et par récurrence, il est clair que tout $p \in P$ est d'au moins une manière décomposable en un produit $p = p_1 p_2 \cdots p_m$ où tous les p_i appartiennent à P_0.

Proposition 1.1.- Une condition nécessaire et suffisante pour que $P \subset A$ corresponde à un code est que la décomposition en produits d'éléments $p_i \in P_0$ soit unique pour tout $p \in P$.

(3) Ici, et par la suite, on désignera par $\emptyset$ la suite vide comme distincte de $\emptyset$: l'ensemble vide. On conviendra en outre que la "suite vide" est un élément de tout demi-groupe considéré dont elle est évidemment un élément neutre.

15-05

Attachons en effet à tout p_i un $\lambda_i = \mathcal{C}^{-1} p_i$ par une correspondance biunivoque. L'extension de $\mathcal{C}$ au demi-groupe libre Λ engendré par les λ_i est un homomorphisme de Λ sur P puisque si $\lambda = \lambda_1 \lambda_2 \dots \lambda_m$, $\mathcal{C}\lambda = \mathcal{C}\lambda_1 \mathcal{C}\lambda_2 \dots \mathcal{C}\lambda_m = p_1 p_2 \dots p_m$. Cet homomorphisme est un isomorphisme sur si et seulement si $\lambda \neq \lambda'$ entraine $\mathcal{C}\lambda \neq \mathcal{C}\lambda'$ c'est-à-dire si et seulement si $p_1 p_2 \dots p_m \neq p'_1 p'_2 \dots p'_m$ quels que soient p_i, $p'_i \in P_0$.

Considérons, pour P quelconque, un élément $a = a_1 a_2 \dots a_n$ de $\mathfrak{A}$ où les a_i sont des lettres $(a_i \in A_0)$.

Définition. On appellera indice critique de a tout indice i tel que $a_1 a_2 \dots a_i = {}^{*}a_i \in P$ et $a_{i+1} a_{i+2} \dots a_n = a_i^{*} \in P$. Evidemment l'ensemble J_a des indices critiques de a n'est non vide que si $a = {}^{*}a_i \, a_i^{*} \in P$.

Proposition 1.2.- Si J est un indice critique de la sous-séquence de a $b = b_{i,i'} = a_{i+1} a_{i+2} \dots a_{i'}$ où $i, i' \in J_a$ il est aussi un indice critique de a.

En effet si ${}^{*}b_J = a_{i+1} a_{i+2} \dots a_J \in P$ et $b_J^{*} = a_{J+i} \dots a_{i'} \in P$ on a aussi ${}^{*}a_i \, {}^{*}b_J = {}^{*}a_J \in P$ et $b_J^{*} a_{i'}^{*} = a_J^{*} \in P$.

Proposition 1.3.- Une condition nécessaire et suffisante pour que $P \subset A$ corresponde à un code est que, pour tout $a \in P$ et toute sous-séquence de a, $b = b_{ii'}$ $i, i' \in J_a$ entraine $b \in P$.

La condition est suffisante car si $J_a = \{1 = i_1 < i_2 < \dots i_m = n\}$ d'une part les sous-séquences $b_{i_k i_{k+1}}$ sont indécomposables d'après 1.2 et sont donc des mots,

d'autre part il ne peut exister aucune autre décomposition de a puisque celle-ci impliquerait l'existence d'un indice critique $i' \notin J_a$.

La condition est nécessaire : supposons que $b_{ii'} \notin P$. Il existe dans J_a J et J' (éventuellement : $J = 1$ et $J' = n$) tels que :

1°) $J < i < i' < J'$

2°) b_{Ji}, $b_{Ji'}$, $b_{iJ'}$, $b_{JJ'} \in P$

3°) $|J' - J|$

soit minimum parmi les couples J et J' satisfaisant à 1°) et 2°).

$c = b_{JJ'}$ possède deux décompositions en mots au moins : l'une avec :

$$p_1 p_2 \dots p_{m'_1} = b_{Ji'} \quad \text{et} \quad p_{m_1+1} \dots p_m = b_{i'J'}$$

l'autre avec

$$p'_1 p'_2 \dots p_{m'_1} = b_{Ji} \quad \text{et} \quad p_{m'_1+1} \dots p_{m'} = b_{iJ'} \quad (p_i \in P_0)$$

Ces deux décompositions sont distinctes, car si par exemple on avait $p_1 = p'_1 = a_1 a_2 \dots a_{J''}$ le couple (J'', J') satisferait à 1°) et 2°) et on aurait $|J' - J''| < |J' - J|$ en contradiction avec 3°). Une conséquence de la proposition précédente est le

Théorème 1.4.- Une condition nécessaire et suffisante pour que le sous-demi-groupe P du demi-groupe libre A corresponde à un groupe est que :

$$P^{(-1)}P \cap PP^{(-1)} \subset P \qquad (4) \tag{1.4}$$

En effet la condition indiquée signifie simplement que : p , p' , pq , $qp' \in P$ implique $q \in P$ et il suffit d'appliquer la proposition en prenant $a = pqp' \in P$.

Si $P \subset A$, où A n'est pas nécessairement un demi-groupe libre, satisfait 1.4, on dira que P est "libérable" dans A . Un autre corollaire intéressant est obtenu en remarquant que $P \subset A$ correspond à un code si et seulement si P est isomorphe à un demi-groupe libre. Soit $\mathcal{L}_A$ l'ensemble des sous-demi-groupe de A qui satisfont à cette propriété et soit δ le "demi-groupe libre vide" ($P_0 = \emptyset$) que l'on supposera appartenir à $\mathcal{L}_A$:

Proposition 1.5.- $\mathcal{L}_A$ est un treillis.

Comme $A \in \mathcal{L}_A$, il suffit de montrer que $P \in \mathcal{L}_A$ et $P' \in \mathcal{L}_A$ entraine $P \cap P' = \delta$ où $P \cap P' = P'' \in \mathcal{L}_A$. Or si $p_1 p_2$, $p_1 q$, $q p_2 \in P''$, $q \in P$ et $q \in P'$ puisque P et P' satisfont à la relation 1.4 , donc $q \in P''$ et P'' satisfait aussi 1.4.

Définition. Un code sera dit unitaire à gauche si $P^{(-1)}P \subset P$ (unitaire à droite si $PP^{(-1)} \subset P$)

---

(4) Les conventions d'écritures suivantes seront systématiquement employées : (à droite ou à gauche).

$$X^{[-1]}Y = Y .^{\cdot} X = \{\hat{z} : \forall_X x \quad xz \in Y\}$$

$$X^{(-1)}Y = A - (A - Y) .^{\cdot} X = \{\hat{z} : \exists_X x \quad xz \in Y\}$$

si X est un élément, les symboles $x^{[-1]}$ et $x^{(-1)}$ ont le même sens. On observera que les "parenthèses" satisfont à une série d'identité parallèle à celle qui est bien connue pour les "crochets" . Notamment :

$$X^{(-1)}(Y^{(-1)}Z) = (YX)^{(-1)}Z \; ; \; X^{(-1)}(ZY^{(-1)}) = (X^{(-1)}Z)Y^{(-1)} ;$$

$X^{(-1)}(XY) \supset Y$ etc. Toutefois :

$$(X \cup Y)^{(-1)}Z = X^{(-1)}Z \cup Y^{(-1)}Z \quad \text{et} \quad (X \cup Y)^{[-1]}Z = X^{[-1]}Z \cap X^{[-1]}Z \text{ , etc.}$$

On écrira $X^{(-n)}Z$ pour $X^{(-1)}(X^{(-1)}(X^{(-1)} \dots Z))) = (X^n)^{(-1)}Z$.

15-07

On a évidemment :

Proposition 1.6.- Tout sous-demi-groupe unitaire P d'un demi-groupe libre correspond à un code.

La définition précédente est exactement celle de P. Dubreil [3]. Elle conduit à un décodage très simple : soit en effet $a = a_1 \dots a_n \in P$ une suite de lettres. Procédant de gauche à droite, soit $i \neq 1$ le plus petit indice tel que $a_i^* \in P$. Par hypothèse, puisque P est unitaire, $a_i^* \in P$ et $i \in J_a$. Donc $b_{1i} \in P_0$ et il suffit de recommencer sur la suite $a' = a_{i+1} \dots a_n \in P$ pour aboutir au décodage de a .

Exemple : Soit le code "opposé" de celui donné en exemple dans l'introduction :

$\mathcal{G}\alpha = a$; $\mathcal{G}\beta = bb$; $\mathcal{G}\gamma = c$; $\mathcal{G}\delta = ba$; $\mathcal{G}\varepsilon = bcb$

On vérifie (Cf. plus bas) que P est unitaire et que le décodage de $m = bcbbabcba$ s'effectue directement sans essais et erreurs :

$$m = \varepsilon babcba = \varepsilon\delta bcba = \varepsilon\delta\varepsilon a = \varepsilon\delta\varepsilon\alpha .$$

Le problème consistant à déterminer pratiquement si un ensemble P_0 de mots correspond ou non à un code avait été résolu par Sardinas et Patterson [12] par des considérations purement combinatoires sans faire appel à la notion de demi-groupe. Leurs résultats peuvent être améliorés de la façon suivante :

supposons que $\emptyset \notin P_0$ et que $P_0 \cap P_0^2 = \emptyset$

Proposition 1.7.- Si l'on pose $P_1 = P_0^{(-1)} P_0$ et par récurrence :

$$P_{n+1} = P_n^{(-1)} P_0 \cup P_0^{(-1)} P_n \text{ alors : } P_n = \bigcup_{n'+n''=n} P_0^{-(n')} P_0^{n''} .$$

Par définition P_1 = l'ensemble des $q \in A$ tels qu'il existe $p, p' \in P_0$ avec $pq = p'$. Supposons établi que pour $n \leq n_0$ on ait montré que :

P_n = l'ensemble des q tels qu'il existe $p_1 , p_2 \dots p_{n'} , p'_1 p'_2 \dots p'_{n''} \in P_0$ $(n' + n'' = n)$ avec

$$p_1 p_2 \dots p_{n'} q = p'_1 p'_2 \dots p'_{n''} \qquad (1)$$

Tout élément q' P_{n+1} est défini par :

soit $pq' = q$ (2)

soit $qq' = p$ (3)

avec $p \in P_0$, $q \in P_n$

15-08

Dans le premier cas, multiplions (2) à gauche par $p_1 p_2 \cdots p_{n'}$, il vient:

$$p_1 p_2 \cdots p_{n'} pq' = p_1 p_2 \cdots p_{n'} q \quad \text{soit :} \quad q' \; P^{-(n+1)} P^{n''} .$$

Dans le second cas, multiplions (1) à droite par q' , il vient :

$$p_1 p_2 \cdots p_{n'} q q' = p'_1 p'_2 \cdots p'_{n''} q' \quad \text{soit d'après (3) :} \quad q' \; P^{(-n'')} P^{n'+1} .$$

Proposition 1.8.- Une condition nécessaire et suffisante pour que P_0 soit l'ensemble des mots d'un code est que, pour tout $n \geqslant 1$, $P_n \cap P_0 = \emptyset$.

En effet, on aura ou non affaire à un code selon que pour tout $a \in A$

$$a = p_1 p_2 \cdots p_m = p'_1 p'_2 \cdots p'_{m'} q \qquad (p_i , p'_i \in P_0 \; ; \; p_1 \neq p'_1)$$

entrainera ou non $q \notin P$.

L'intérêt de cette proposition est que, si le code est borné c'est-à-dire si la longueur de tous ses mots est bornée, les $q \in P_n$ sont des diviseurs à gauche ou à droite des séquences composant P_0 , donc sont bornés eux-mêmes et en nombre fini s'il en est de même de la puissance de l'alphabet. Dans ces conditions il existe un $n < \infty$ tel que

soit $P_n = \emptyset$ et par conséquent $P_{n'} = \emptyset$ pour tout $n' \geqslant n$
soit $P_n = P_{n+r}$ et par conséquent $P_{n+J+kr} = P_{n+J}$ pour tout $J \leqslant r$ et tout k .

On a donc · Dans un code borné

Proposition 1.9.- Une condition nécessaire et suffisante pour qu'il existe une valeur fixe $L < \infty$ telle que la connaissance des $m + L$ premières lettres (à gauche) du message permette quel que soit m de décoder les m premières lettres sans ambiguité est qu'il existe un $n < \infty$ tel que $P_n = \emptyset$.

En particulier une condition nécessaire et suffisante pour que le code soit unitaire à gauche est que $P_1 = \emptyset$.

En effet si un tel n n'existe pas, on peut construire des $a \in A$ de la forme 1.9 pour des valeurs aussi grandes que l'on veut de $m + m'$. Inversement si $P_n = \emptyset$ et si $a = p_1 \cdots p_m = p'_1 p'_2 \cdots p_{m'} q$ on a $p_i = p'_i$ pour tout $i \leqslant m_0$ avec $m - m_0 + m' - m_0 \quad n$.

Les notions suivantes sont utiles pour caractériser certains types de codes :

Définition. Un code sera dit
net (à droite) si $PA^{(-1)} = A$
absorbant (à droite) si $PP^{(-1)} = A$

15-09

La notion de code net est encore exactement celle de P. Dubreil [3]: un code est net à droite si quel que soit la séquence de lettres $a = a_1\, a_2 \cdots a_n \notin P$ il existe au moins une séquence $b = a_{n+1}\, a_{n+2} \cdots a_m$ tel que $ab \in P$.

Le code orthographique du français n'est pas net, car il est impossible d'ajouter des lettres à droite de la séquence "Khtg" par exemple qui la complète en un mot. Par contre le code formé par l'ensemble P des phrases sémantiquement correctes est net, car à toute suite de mots ou de signes on peut au besoin rajouter la clause. "Les x-dernières syllabes que j'ai énoncées étaient un exemple de sentence sémantiquement absurde."

La notion de code absorbant est encore plus forte que la notion de code net : elle signifie que quel que soit $a \notin P$ il existe $q \in P$ (et non pas seulement dans A) tel que $aq \in P$. On démontre :

Proposition 1.10.- Si A est fini, quel que soit $P \subset A$, $A^{[-1]}P \neq \emptyset$ est équivalent à $PP^{(-1)} = A$.

En effet $A^{[-1]}P \ni r$ signifie que $ar \in P$ pour tout $a \in A$.

Réciproquement soit $p_1 \in P$ tel $a_1\, p_1 \in P$ pour au moins un $a_1 \in A - P = A_1$ et par récurrence :

$p_i \in P$ tel que $a_i\, p_i \in P$ pour au moins un $a_i \in A_i = A_{i-1}\, p_{i-1} - P$.

Les ensembles $A'_1 = P\, p_1^{-1}$; $A'_2 = P(p_1\, p_2)^{-1}$ soient strictement croissants ; donc pour un certain $i = J$: $A_J = \emptyset$ et $p_1\, p_2 \cdots p_J \in A^{[-1]}P$.
Il est clair que si un code est unitaire net ou absorbant à droite, il ne s'en suit pas qu'il le soit aussi à gauche. En particulier :

Proposition 1.11.- Une condition nécessaire (mais non suffisante) pour qu'un code soit absorbant à droite est qu'il soit unitaire à gauche et net à droite et qu'il ne soit pas unitaire à droite.

En effet si $PP^{(-1)} = A$, P n'est libérable ($P^{(-1)}P \cap PP^{(-1)} \subset P$) que s'il est unitaire à gauche. D'autre part s'il n'était pas net, il existerait w tel que $wx \notin P$ pour tout x .

Remarque. Les énoncés précédents semblent avoir une partie pratique assez faible puisque, par exemple la recherche des indices critiques d'une séquence s'effectue pratiquement en vérifiant que ${}^*a_i$ et a_i^* sont décodables. Pour aller plus loin il nous faudrait trouver des demi-groupes $\bar{A}$ et $\bar{P}$ de préférence finis et une application φ tels que pour tout $a \in A$, $\varphi a \in \bar{P}$

entraine $a \in P$. C'est ce que nous ferons dans la section suivante. Il se trouve cependant que ces notions dépassent largement le cadre des problèmes de codage et il a paru aussi simple de les traiter en toute généralité pour un A quelconque et un complexe $K \subset A$ qui n'en est pas nécessairement un sous-demi-groupe.

2.- Equivalence syntaxiques.

Soient A un demi-groupe contenant un élément neutre, K une partie quelconque de A .

Définition. On dira que a est syntaxiquement plus fort que b dans A , par rapport à K ($a \gtrdot b$ (A , K)) si pour tout $x, y \in A$:

(II) $\quad xby \in K$ entraine $xay \in K$

Si $a \gtrdot b(A, K)$ et $b \gtrdot (A, K)$, a et b seront "syntaxiquement équivalents" ($a \equiv b(A, K)$).

Proposition 2.1.- $\gtrdot(A, K)$ est une relation régulière, réflexive, transitive (une relation de préordre (2) compatible avec la structure de demi-groupe). Manifestement $a \gtrdot a$ (A , K) et $a \gtrdot b$ (A , K) et $b \gtrdot c$ (A , K) entrainent $a \gtrdot c$ (A , K).

D'autre part, si (II) est vraie pour tout x , $y \in A$, (II) est encore vraie pour $x \in Av$ et $y \in vA$. Donc $a \gtrdot b$ (A , K) entraine $uav \gtrdot ubv$ (A , K) et en particulier si $a \gtrdot a'$ (A , K) et $b \gtrdot b'$ (A , K) on a successivement:

$ab \gtrdot a'b$ (A , K) et $a'b \gtrdot a'b'$ (A , K) d'où $aa' \gtrdot bb'$ (A , K) .

Proposition 2.2.- $\gtrdot(A, K)$ est la plus forte des relations régulières de préordre pour laquelle K soit supérieurement saturé (5). K est supérieurement saturé pour $\gtrdot(A, K)$ car $b \in K$ et $a \gtrdot b$ (A , K) entraine en particulier $a \in K$ en faisant $x = y = \emptyset$ dans (II). Réciproquement, si ρ est régulière et K supérieurement saturé pour ρ $a \rho b$ implique $(xay) \rho (xby)$ et en particulier $xby \in K$ entraine $xay \in K$ donc $a \rho b$ implique $a \gtrdot b$ (A,K).

Proposition 2.3.- Si A est un groupe fini $\gtrdot(A, K)$ se réduit à une relation d'équivalence qui est précisément l'équivalence normale associée au plus grand sous-groupe normal G de A qui soit contenu dans l'un des complexes de K .

(5) ρ étant une relation de préordre ($\gtrdot$ réflexive et transitive) on dire que K est supérieurement saturé pour ρ si $a \rho b$ et $b \in K$ entrainent $a \in K$. ρ est régulière si $a \rho b$ entraine $(xay) \rho (xby)$ pour tout x , y . (Cf [3]) .

En effet : si A est un groupe $a \geqslant b\ (A\ ,\ K)$ peut s'écrire : $K\, y^{-1}\, a^{-1}\, b\, y \subset K$ c'est-à-dire encore $a^{-1}\, b \in G$ où G est l'ensemble des c tels que $K\, y^{-1} c\, y \subset K$ pour tout y. Mais, d'une part $Kd \subset K$ est équivalent à $Kd = K$, d'autre part $c, c' \in G$ entraine $cc' \in G$. Donc G est le plus grand sous-groupe normal de A tel que $KG = K$ et l'on a : $K = \bigcup_{x \in K} xG$ c'est-à-dire $G \subset k^{-1} K$ pour tout $k \in K$.

Remarque 1.- Si l'on voulait interpréter l'équivalence syntaxique dans le code des "phrases françaises grammaticalement correctes" on trouverait par exemple que "postulat" $\not\equiv$ "axiome" $\equiv$ "hippopotame" car on peut aussi bien dire "l'axiome d'Euclide est à la base de la géométrie élémentaire" que "l'hippopotame d'Euclide ...etc" alors que la phrase "l'postulat d'Euclide ...etc" est incorrecte.

Remarque 2.- Dans ce même cadre linguistique il serait possible et utile de généraliser la définition précédente

Définition.- Le n-tuple $a = (a_1\ ,\ \ldots\ ,\ a_n)$ d'éléments de A est "syntaxiquement plus fort que le n-tuple $b = (b_1\ ,\ b_2 \ \ldots\ b_n)$ dans A par rapport à K et au n+1-tuple $(g_0\ ,\ g_1 \ \ldots\ g_n) = g$" si pour tout 2n-tuple $(x_1\ ,\ y_1\ ,\ x_2\ ,\ y_2 \ \ldots\ x_n\ ,\ y_n) = (x\ ,\ y)$ $g_0\, x_1 b_1 y_1\, g_1\, x_2\, b_2 \ \ldots\ g_{n-1} x_n\, b_n\, y_n\, g_n = g_{(x,y)}(b) \in K$ entraine $g_{(x,y)}(a) \in K$. $(a \geqslant b (A\ ,\ K\ ;\ g))$

Les propriétés 2.1 et 2.2 subsistent et naturellement $a_i \equiv b_i\ (A\ ,\ K)$ pour tout i entraine $a \geqslant b\ (A\ ,\ K\ ;\ g)$ la réciproque n'étant pas forcément vraie.

Nous ne ferons pas usage ici de cette notion générale.

Définition. Soit φ_K l'homomorphisme attaché à $\equiv (A\ ,\ K)$. On posera $\bar{A} = \varphi_K A$; $\bar{K} = \varphi_K K$; si $K = P \supset P^2$ on dira que A et P sont les demi-groupes syntaxiques fondamentaux (GSF) de $(A \supset P)$.

Si $\varphi_K = 1$ (φ_K réduit à l'application identique) on dira que $K\ (= \bar{K})$ est syntaxiquement simple dans $A\ (= \bar{A})$.

Proposition 2.4.- $a \geqslant b\ (A\ ,\ K)$ est équivalent à $\varphi_K a \geqslant \varphi_K b\ (\bar{A}\ ,\ \bar{K})$. Donc $\bar{K}$ est syntaxiquement simple dans $\bar{A}$.

D'une part $xby \in K$ entraine $\varphi_K x\, \varphi_K b\, \varphi_K y \in \varphi_K K$.

D'autre part : $\varphi_K x\, \varphi_K b\, \varphi_K y = \varphi_K(xby) \in \varphi_K K$ entraine $xby \in K$ puisque K est saturé. Donc $\varphi_K a \equiv \varphi_K b\ (\varphi_K A\ ;\ \varphi_K K)$ est équivalent à $a \equiv b\ (A\ ,\ K)$ donc encore à $\varphi_K a = \varphi_K b$ dans $\varphi_K A$.

15-12

Proposition 2.5.- Si $K \supset K^2 = Q$ est un sous-demi-groupe, chacune des propriétés suivantes est simultanément vraie ou non pour $Q \subset A$ et pour $\varphi_Q\, Q \subset \varphi_Q\, A$: Q est libérable, unitaire, net, absorbant.

Soient $B \supset R$ deux demi-groupes quelconques et Ψ un homomorphisme. Une condition nécessaire et suffisante pour que quel que soit $x \in B$, $\Psi(Qx^{-1}) = \Psi Q(\Psi x)^{-1}$, est que Q soit saturé pour l'équivalence d'homomorphisme attachée à Ψ. Car :

$a \in Qx^{-1} \rightleftarrows ax \in Q$ qui entraine : $\Psi a\, \Psi x \in \Psi Q$ soit $\Psi a \in \Psi Q(\Psi x)^{-1}$; et réciproquement : $\Psi a\, \Psi x = \Psi q \in \Psi Q$ entraine $ax \in q$ est la définition même de la saturation.

Or les propriétés indiquées ne font appel qu'à l'opération $Q X^{(-1)} = \bigcup_{x \in X} Q x^{-1}$.

Proposition 2.6.- Soient $A \supset K$ et Ψ un homomorphisme. Une condition nécessaire et suffisante pour que $\varphi_K = \varphi_{\Psi_K} \circ \Psi$ au sens de la composition $(\circ)$ des homomorphismes est que K soit saturé pour l'équivalence σ attachée à Ψ (ce que l'on peut noter $\Psi^{-1}\Psi K = K$).

La condition est nécessaire : si $a \in A - K$, $k \in K$ et $\Psi k = \Psi a = k' \in \Psi K$ alors $(\varphi_{\Psi_K} \circ \Psi)\, k = (\varphi_{\Psi_K} \circ \Psi) a$ et $\varphi_K a \neq \varphi_K k$.

La condition est suffisante : si σ est moins forte que $\equiv (A, K)$ $a \equiv b\ (A, K)$ entraine $\Psi a \equiv \Psi b\ (\Psi A, \Psi K)$.

Définition. Si A est un demi-groupe libre et K un complexe de A nous dirons que $A \supset K$ est une extension libre de $A' \supset K'$ s'il existe un homomorphisme Ψ tel que (1) $A' = \Psi A$, (2) $K' = \Psi K$, (3) $\Psi^{-1}\Psi K = K$.

Proposition 2.7.- L'ensemble des couples $(A' \supset P')$ tels que leurs GSF soient isomorphes au couple syntaxiquement simple $(\bar{A} \supset \bar{P})$ est identique à l'ensemble des couples $(\Psi A \supset \Psi P)$ où $(A \supset P)$ est une extension libre de $\bar{A} \supset \bar{P}$ et où $\Psi^{-1}\Psi P = P$.

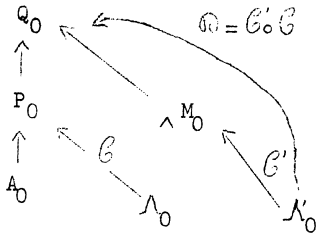
En effet d'après 2.6 on a : d'une part $\varphi_P A = \bar{A}$ et $\varphi_P P = \bar{P}$ d'autre part $\varphi_P = \varphi_{\Psi_P} \circ \Psi$.

Remarque 1. 2.7 montre que l'on peut construire pour toute puissance α de l'alphabet assez grande au moins un code admettant comme GSF un couple syntaxiquement simple $\bar{A} \supset \bar{P}$ où $\bar{P}$ est libérable dans $\bar{A}$ donné :

15-13

Si $\bar{g}_1 \dots \bar{g}_m$ sont des générateurs de $\bar{A}$ et $\bar{h}_J$ d'autres éléments de $\bar{A}$, il suffit de faire correspondre les lettres $a_{1_1} a_{1_2} \dots a_{1_i}$ à $\bar{g}_1$ les lettres $a_{2_1} a_{2_2} \dots a_{2_{i'}}$ à $\bar{g}_2 \dots$, $a_{m_1} a_{m_2} \dots a_{m_{i''}}$ à $\bar{g}_m$ et $a_{J_1} \dots a_{J_{i''}}$ à $\bar{h}_J$ en posant $\Psi a_{\ell,k} = \bar{a}_\ell \in \bar{A}$ et de définir P par $\Psi^{-1}\bar{P}$ ce qui assure que $\Psi^{-1}\Psi P = P$. On observera qu'en général pour un tel choix quelconque de générateurs l'ensemble des mots $P_0 = P - ((P - \phi)^2 \cup \phi)$ n'est pas borné même si $\bar{A}$ est fini.

Remarque 2. Un problème important est celui du surcodage : c'est-à-dire celui de l'utilisation des mots d'un code primaire comme "lettres" d'un alphabet secondaire ainsi qu'il est indiqué dans le schéma ci-contre, qui est illustré par les identifications suivantes :



A_0 : l'"alphabet"morse formé des trois "lettres primaires" : point, trait intervalle

Λ_0 : l'ensemble des signes typographiques mis en correspondance par $\mathcal{C}$ avec :

P_0 : l'ensemble des séquences de points traits et intervalles qui représentent des signes typographiques dans le code Morse. P_0 est à la fois un ensemble de mots primaires et un alphabet secondaire.

Λ'_0 : l'ensemble des mots du français écrit mis en correspondance

1°) par $\mathcal{C}'$ avec M_0 : l'ensemble des séquences de signes typographiques qui représentent des mots du français écrit (M_0 est un ensemble de mots primaires pour $\mathcal{C}'$).

2°) par $\mathfrak{A} = \mathcal{C}' \circ \mathcal{C}$ avec Q_0 : l'ensemble des suites de points, traits intervalles, qui représentent des mots du français écrit (Q_0 est un ensemble de mots secondaires par rapport à P_0 et primaires par rapport à $\mathfrak{A}$).

Il serait utile de caractériser au moins partiellement les GSF de $(A \supset Q)$ au moyen de ceux des "facteurs" $(A \supset P)$ et $(\Lambda \supset M)$. Le problème sera étudié dans un autre travail et les énoncés suivants très simples sont avec 2.6 et 2.7 à la base des démonstrations.

Proposition 2.8.- Si K et K' sont deux complexes de A $a \geqslant b$ (A, K) et $a \geqslant b$ (A, K') entrainent $a \geqslant b$ $(A, K \cap K')$

Immédiat : car $xby \in K \cap K'$ entraine $xby \in K$ et $xby \in K'$ qui entrainent $xay \in K$ et $xay \in K'$ donc $xay \in K \cap K'$.

On observera que même si K et K' étaient des demi-groupes P et P' il serait possible que $P \supset P'$ sans que pour autant $\equiv (A , P)$ soit plus forte que $\equiv (A , P')$ au contraire de ce qui se produit si A est un groupe. En effet, l'intersection de $\equiv (A , P)$ et de $\equiv (A , P')$ si $(P' \subset P)$ est identique à l'intersection de $\equiv (A , P')$ et $\equiv (A , P - P')$ qui ne sont pas en général identiques.

Proposition 2.9.- Si $A' \subset A$ et $K' = A' \cap K$ la restriction de $\geqslant (A , K)$ à A' est plus forte que $\geqslant (A' , K')$. En effet, $xby \in K'$ implique $xay \in K$ par hypothèse et, si $a , b , x , y \in A'$, on a donc $xay \in A \cap K = K'$.

3.- Préfixes.

Définition. On appellera "préfixe à droite" ($\Pi_i^* \in \Pi^*$) (respectivement préfixe à gauche : ${}^*\Pi_J \in {}^*\Pi$) les classes d'équivalence de A pour la relation $\sim^* (A , P)$ (respectivement ${}^*\sim (A , P)$) définie par : $a \sim^* b \ (A , P)$ si et seulement si $a^{-1}P = b^{-1}P$ (respectivement : $a \, {}^*\!\sim b \ (A , P)$ si et seulement si $Pa^{-1} = Pb^{-1}$) .

Il est classique [3] que :

Proposition 3.1.- La relation $\sim^* (AP)$ est régulière à droite (respectivement : ${}^*\sim (AP)$ est régulière à gauche) et $\equiv (A , P)$ est plus forte que l'intersection de $\sim^* (AP)$ et ${}^*\sim (A , P)$.

En effet $a \equiv b \ (A , P)$ s'écrit aussi bien :

$(ax)^{-1}P = (bx)^{-1}P$ pour tout x que $P(xa)^{-1} = P(xb)^{-1}$ pour tout x .

Il en résulte :

Proposition 3.2.- La représentation A^* des éléments $x \in A$ comme application de l'ensemble Π^* des préfixes à droite (à gauche) dans lui-même est une représentation isomorphe de $\bar{A}$.

En effet puisque $\sim^*$ est régulière à droite $a , b \in \Pi_i^*$ entraine $ax , bx \in \Pi_J^* = \Pi_i^* x$ pour un certain J quels que soient a , b et x , d'autre part $\Pi_i^* x = \Pi_i^* y$ pour tout $\Pi_i^* \in \Pi$ entraine $x \equiv y \ (A , P)$ et réciproquement.

15-15

On déduit de cette remarque la :

Proposition 3.3.- $A \supset P$ étant deux demi-groupes quelconques si $\varphi_P P = \bar{P}$ est un groupe $A = \varphi_P A$ s'il est fini, est la réunion d'un groupe et éventuellement d'un zéro.[6]

En effet la représentation 3.2 étant isomorphe $\bar{P}$ est un groupe si et seulement si toutes les applications correspondantes de Π^* dans lui-même sont des permutations. Donc si $a \in A$ est tel que $xay \in P$ pour au moins un couple $x, y \in A$, a est aussi une permutation. Sinon $ab \equiv ba \equiv a\ (A, P)$ pour tout b et $\varphi_P a = 0$.

Remarque 1. Il est possible et souvent commode de développer la théorie de l'équivalence syntaxique de la façon suivante : soit $a \in A$. L'ensemble $a^{-1}P$ est celui des séquences $b \in A$ telles que $ab \in P$ et l'ensemble $\Pi_a^* = P\,(a^{-1}P)^{[-1]}$ celui des séquences c telles que $cb \in P$ pour tout $b \in a\,P$.

Evidemment $a \in \Pi_a^*$ et $\Pi_a^{[-1]} P = a^{-1}P$. On peut vérifier que Π_a^* ainsi défini est précisément le préfixe à droite qui contient a. De la même manière on trouverait ${}^*\Pi_a = (Pa^{-1})^{[-1]} P$, et la relation ρ entre préfixes à droite et à gauche définie par : $\Pi_i^* \rho {}^*\Pi_J$ si et seulement si $a \in \Pi_i^*$ et $b \in {}^*\Pi_J$ entraine $ab \in P$, permet d'établir une correspondance de Galois [2] entre Π^* et ${}^*\Pi$. Le treillis complet associé pourrait être appelé le "treillis fondamental" du code $(A \supset P)$ et ses propriétés, une fois encore, ne dépendent que des GSF $(\bar{A} \supset \bar{P})$.

Remarque 2. Il est utile de distinguer certains préfixes remarquables :

Π_0^* : le résidu de P dans A au sens de P. Dubreil [3] : l'ensemble des a tels que ax n'appartienne à P pour aucun x.

Π_∞^* : le préfixe "absorbant" : l'ensemble des a tels que $ax \in P$ pour tout x.

Π_1^* : le préfixe unité tel que $a \in \Pi_1$ entraine $a \in P$ et $ax \in P$ seulement si $x \in P$.

$\Pi_{p_i}^{*1}$: les préfixes qui sont des sous-classes de P ($a \in \Pi_{p_i}$ entraine $a \in P$).

L'existence ou la non-existence de tels préfixes non vides est trivialement liée au fait que le code est net, absorbant, unitaire etc.

[6] un zéro est un élément 0 tel que $x0 = 0x = 0$ pour tout x.

15-16

Exemple. Soit le code suivant (unitaire à droite) :

$$G\alpha = a \quad ; \quad G\beta = ab \quad ; \quad G\gamma = bb$$
$$\Pi_0^* \ni b \quad ; \quad \Pi_\infty^* \ni a \quad ; \quad \Pi_1^* \ni bb \quad ; \quad \Pi_{p\rho} \ni ab \ .$$

Proposition 3.4.- Si l'alphabet d'un code est fini, et si la longueur de ses mots est bornée par $L < \infty$ alors son GSF $\bar{A}$ est fini.

Puisque $\bar{A}$ possède une représentation comme groupe d'application de Π (7) dans lui-même, il suffit de montrer que Π est fini. Or si $ax \in P$, ou bien la longueur de x est $\leq L$, ou bien il existe x' diviseurs à gauche de x de longueur inférieure à L tels que $ax' \in P$. Donc $a^{-1}P = b^{-}P$ si et seulement si $a^{-1}P \cap X_L = b^{-}P \cap X_L$ où X_L est l'ensemble fini des séquences de lettres de longueur $\leq L$.

Proposition 3.5.- Dans tout code unitaire l'ensemble des préfixes différents du résidu est une image homomorphe de l'ensemble des diviseurs (à gauche) des mots.

Montrons d'abord que $p \in P$ entraine $(pa)^{-1}P = a^{-1}P$ pour tout a. Or $pax \in P$ entraine $ax \in P$ par hypothèse puisque P est unitaire.

Soit donc $a \in \Pi_i \neq \Pi_0$; il existe y tel que $ay \in P$ donc a est diviseur à gauche d'une suite de mots donc, ou bien a est lui-même diviseur à gauche d'un mot, ou bien il existe $p \in P$, tel que $a = pa'$ et $a' \in \Pi_i$, d'où le résultat par récurrence. On en déduit la remarque utile suivante :

Proposition 3.6.- Il existe une correspondance biunivoque entre les codes unitaires et les structures d'arbres enracinés (8), les codes nets, correspondant

(7) Pour simplifier et puisque dans la pratique un ordre temporel est toujours prescrit pour la suite des lettres, nous conviendrons dorénavant sauf mention expresse du contraire, que préfixe signifie, préfixe à droite ; unitaire : unitaire à gauche ; net : net à droite. Cette convention est la plus simple quand l'ordre temporel est identifié avec l'ordre gauche $\longrightarrow$ droite.

(8) Soit U un ensemble ordonné par ρ. Pour tout u soit $\rho[u]$ = l'ensemble des $u' \in U$ tels que $u' \rho u$. U est un arbre enraciné si 1°) $\bigcap_{u \in U} \rho[u] = u_1 \neq \emptyset$ (u_1 est la racine) 2°) pour tout $\rho[u]$ est un ensemble totalement ordonné. Si $u \in \rho[v]$ entraine $v = u$ u est une extrémité, sinon u est un noeud. Si pour tout u qui n'est pas une extrémité il existe un nombre fixe $K < \infty$ de v tels que 1°) $u \rho v$ et 2°) $u \rho w \rho v$ entraine $w = u$ ou $w = v$, l'arbre est dit complet.

aux arbres complets.

Il suffit d'identifier la racine à la séquence vide, les noeuds aux diviseurs à gauche des mots, et les extrémités aux mots eux-mêmes. On observera que deux diviseurs appartiennent au même préfixe si et seulement si les sous-arbres correspondant dont ils sont les racines sont identiques.

Exemple : soit le code suivant :

$\mathcal{C}\alpha$ = aaa ; $\mathcal{C}\beta$ = aab ; $\mathcal{C}\gamma$ = ab ; $\mathcal{C}\delta$ = baa ; $\mathcal{C}\varepsilon$ = bab ; $\mathcal{C}\xi$ = bb

il lui correspond l'arbre ci-contre (figure 1). Les diviseurs "a" et "b" appartiennent au même préfixe.

figure 1

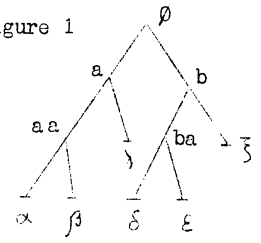
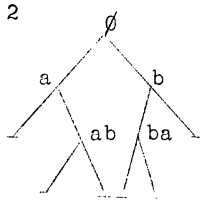


figure 2



On prendra garde que des arbres équivalents à des permutations près de noeuds correspondent en général à des codes dont les GSF sont différents. (l'arbre de la figure 2 par exemple est équivalent par permutation à celui de la figure 1 mais son code à un autre GSF) .

Une conséquence immédiate de la représentation des codes unitaires par des arbres enracinés est :

Proposition 3.7.- Dans un code unitaire une condition nécessaire et suffisante pour que tous les mots aient une longueur bornée est que, si a et ax appartiennent au même préfixe, il existe au moins un diviseur à gauche x' de x tel que $ax' \in P$.

En effet les sous-arbres a et ax ne sont jamais identiques, si $ax' \notin P$, pour tous les diviseurs à gauches de x'.

Proposition 3.8.- Une condition nécessaire et suffisante pour qu'un code unitaire dont la longueur des mots est bornée par $L < \infty$ possède une suite non vide de lettres ℓ telle que $\varphi_P \ell$ soit un élément neutre bilatère de $\varphi_P A$ est qu'il existe une lettre $a \in A_0$ telle que les séquences a , a^2 = aa . a^3 = aaa , ... , $C = a^m \in P$ forment un système de représentants de ses préfixes, à l'exception éventuelle du résidu π_0 .

15-18

Par hypothèse ℓ est une application de Π sur lui-même, si donc ℓ contient la lettre a dans son expression, a est une permutation des préfixes (Cf. 3.3) et puisque la longueur des mots est bornée il existe un m minimum fini tel que $a^m \in P$ et $a^m \equiv \ell$ (A, P). On vient de voir que $a^{m'} \sim a^{m''}$ m', m" $\leq$ m entraine m' = m". Soit $b \in \Pi'$. Pour au moins un $n' < \infty$, $ba^{n'} \in P$ mais aussi pour un $m' = m - n'$ (à un multiple de m près) $a^{m'} a^{n'} \in P$ donc Π' est identique au préfixe contenant $a^{m'}$ puisque la multiplication à droite par $a^{n'}$ est une permutation. On en déduit :

Proposition 3.9.- Si la longueur des mots d'un code est bornée et si la puissance de son alphabet est finie, une condition nécessaire et suffisante pour que son GSF $\bar{A}$ soit un groupe est que $P_0 = X_\ell$ (= l'ensemble de toutes les séquences de longueur ℓ : code uniforme de longueur ℓ). Dans ce cas $\bar{A}$ est le groupe cyclique d'ordre ℓ et P se réduit à son élément neutre.

De 3.7, il résulte que toutes les lettres de l'alphabet doivent correspondre à des permutations circulaires de même ordre ℓ sur les préfixes. Montrons que $a^n b \sim a^{n+1}$ quels que soient les lettres a et b, (il sera convenu que les indices seront des entiers positifs réduits modulo ℓ.

Supposons que, pour un n' et un m', $m' \leq n'$, on ait $a^{n'} b \sim a^{m'}$ et considérons les séquences non bornées $c_x = a^{n'}(ba^{m'-n'})^x$ (n' fois suivis de x fois la sous-séquence b suivi de m' - n' a).

On vérifie facilement qu'aucun de leurs diviseurs à gauche n'appartient à P (ils sont tous $\sim$ à un $a^{n''}$ où $n'' \leq n'$). Donc $c_x a^{\ell - n'} \in P$ est un mot contrairement à l'hypothèse selon laquelle la longueur des mots est bornée. Donc pour tout n' $a^{n'} b \sim a^{m'}$ où 1°) m' parcourt avec n' l'ensemble de tous les nombres $\leq \ell$ (car b est une permutation !) 2°) $m' > n'$ si $n' \neq \ell$. Ceci n'est possible que si $m' = n' + 1$ (modulo ℓ) ou encore que si $a \equiv b$ (A, P) puisque $\Pi_i a \sim \Pi_i b$ pour tout préfixe. Donc $\bar{A}$ est un groupe fini à un seul générateur, etc.

Remarque.

Le résultat précédent pose le problème de savoir s'il existe des couples syntaxiquement simples $\bar{A} \supset \bar{P}$ où $\bar{P}$ serait unitaire et not à droite et à gauche sans que $\bar{A}$ soit un groupe et tels que pour au moins un choix de générateurs la longueur des mots soit bornée. La proposition 3.10 est une réponse

15-19

très partielle à cette question. Nous montrons d'abord

Proposition 3.9.- La condition nécessaire et suffisante pour que l'élément u du demi-groupe libre A satisfasse pour au moins un couple $v, w \neq \emptyset$ à : $a = uv = wu$ où la longueur ℓ de a est inférieure ou égale au double de la longueur ℓ' de u est que u soit de la forme $x(yx)^n$.

Raisonnons par récurrence : les longueurs de v et w étant strictement inférieures à $\ell/2$ on a :

$a = wrv$ pour un certain r et $u = wr = rv$.

Si la longueur de r est plus petite ou égale $\ell'/2$ on a encore : $u = rsr$ avec $w = rs$ et $v = sr$. Sinon on est ramené au problème initial avec u au lieu de a et r au lieu de u. Comme les longueurs des séquences ne peuvent que décroitre strictement on a bien le résultat.

Proposition 3.10.- Pour un alphabet de $K < \infty$ lettres il existe au moins un code du type qui vient d'être décrit et dont le nombre de mots est égal à $1 + K^{\ell} - 2K^{\ell''} + K^{2\ell''}$ pour tout $\ell \geqslant 3$ et $\ell'' < \ell/2$.

Nous considérons d'abord le code uniforme $\mathcal{A}$ dont P_0 est identique à l'ensemble X_ℓ de toutes les séquences de ℓ lettres. Il satisfait aux conditions voulues sauf que son GSF est un groupe.

Soit u une séquence fixe de longueur $\ell' < \ell$ et soient les ensembles suivants :

P'_0 : les mots (de $X_\ell = P_0$) dont u est un diviseur à gauche ($P'_0 = u(u^{-1}P_0)$)

P''_0 : les mots dont u est un diviseur à droite mais non à gauche ($P''_0 = (P_0 u^{-1})u - P'_0 \cap (P_0 u^{-1})u$)

X : l'ensemble des séquences de longueur $\ell'' = \ell - \ell'$

Q'_0 : l'ensemble $P''_0 X_{\ell''}$ des séquences de la forme $q = pv$ avec $p \in P''_0$ et $v \in X_{\ell''}$.

Considérons le code $\mathcal{B}$ dont l'ensemble Q_0 des mots est la réunion de u, Q'_0 et de l'ensemble $Q''_0 = P_0 - (P'_0 \cup P''_0)$. Par construction $\mathcal{B}$ est unitaire à gauche et net à droite. D'autre part si $q, q' \in Q_0$ q ne peut évidemment pas être un diviseur à droite de q' dans les cas suivants :

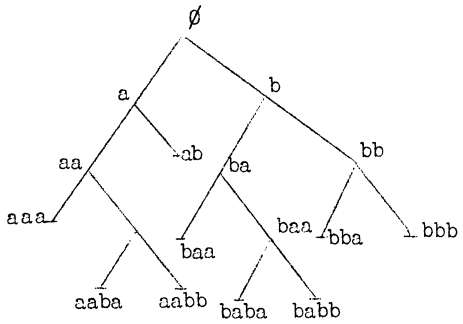
1°) $q' = u$; 2°) $q \in Q'_0$; 3°) $q \in Q''_0$ et $q' \in Q''_0$; 4°) $q = u$ et $q' \in Q''_0$

15-20

Il reste à discuter 5°) le cas de $q \in Q_0''$ et $q' \in Q_0'$ mais les mots de Q_0'' sont de la forme $xuv = xp$ avec $v \in X_{\ell''}$ et $p \in P_0'$ et $p \in \mathbb{P}_0'$ ne peut admettre aucun diviseur propre à droite de longueur ℓ . 6°) $\mathcal{B}$ sera donc unitaire à droite si et seulement si $Q_0' u^{-1} = \emptyset$ ou encore si $uvu^{-1} = \emptyset$ pour tout $v \in X_{\ell''}$. Ceci n'est possible comme on l'a vu en 3.9 que si $\ell' > \ell/2$ et si u n'est pas de la forme exceptionnelle $x(yx)^n$. Le calcul du nombre des mots n'offre aucune difficulté.

Exemple.

Le cas le plus simple ($K = 2$; $\ell = 3$) est décrit par l'arbre suivant. Il contient 9 mots et son GSF (privé de l'élément neutre bilatère) a 24 éléments et ne possède pas d'idéaux propres. Cette dernière particularité n'est pas une nécessité pour les GSF des codes de ce type.



(u = ab)

4.- Méthodes de dénombrement.

On supposera désormais toujours que l'alphabet a une puissance $K < \infty$. On dira, pour abréger, qu'un code est borné si la longueur de ses mots est plus petite que $L < \infty$.

Nous commencerons par compléter et systématiser divers résultats plus ou moins explicitement connus et utilisés par les auteurs qui ont étudié ces questions et notamment B. Mandelbrot [9] .

Notations $g(t) = 1 - \sum_{i=1}^{\infty} n_i t^i$: (avec n_i = nombre des mots de longueur i)

La fonction de structure du code $G(t) = 1 + \sum_{i=1}^{\infty} N_i t^i$ (avec N_i = nombre des éléments de P de longueur i) : la fonction génératrice du code.

15-21

$H(t) = |Dt - 1|$ la fonction caractéristique du code avec D : la somme des matrices correspondant aux lettres de A_0 dans la représentation régulière de $\bar{A}$.

$h_d(t)$ et $h_g(t)$: les déterminants correspondants dans les représentations de $\bar{A}$ comme demi-groupe d'application dans eux-mêmes de Π^* et de $^*\Pi$.

Proposition 4.1.- $g(t)$ est un diviseur commun et $H(t)$ un multiple commun de $h_g(t)$ et $h_d(t)$. On a $G(t) = \frac{1}{g(t)}$. Introduisons encore $N_i(\bar{a})$: nombre de séquences a de longueur i telles que $\varphi_P a = \bar{a} \in P$. Les $N_i(\bar{a})$ sont liés entre eux par un système d'équations aux différences finies :

$$N_{i+1}(\bar{a}) = \sum_{\bar{b} \in \bar{A}} \delta_{\bar{a},\bar{b}} N_i(\bar{a})$$

où $\delta_{\bar{a},\bar{b}} = 0$ ou $1, 2, \ldots, K$ selon qu'il existe $0, 1, 2, \ldots, K$ lettres a_i dans A_0 telles que $\varphi(a\, a_i) = \bar{b} \in \bar{A}$. La matrice des $\delta_{\bar{a},\bar{b}}$ est précisément D et si les ρ_J sont les racines du déterminant $|Dt - 1|$ on sait que $N_i(\bar{a}) = \sum_J \beta_{\bar{a},J} \rho_J^{-i}$ pour un certain système de constantes $\beta_{\bar{a},J}$. D'autre part, les $N_i(\Pi^*)$ ou les N_i qui sont obtenus comme sommes (par rapport à $\bar{a}$) de certains $N_i(\bar{a})$ peuvent être calculés directement à partir de représentation de $\bar{A}$ sur Π^* ou sur $^*\Pi$ ce qui établit les relations de divisibilité indiquées. Enfin on a directement $N = \sum_i N_{\ell-i}\, n_i$ ce qui donne $G(t) = 1/g(t)$ par un raisonnement classique. (Cf. 6)

Proposition 4.2.- La fonction de structure d'un code borné unitaire (à gauche) et net (à droite) (code UND) est de la forme :

$$g(t) = (1 - Kt)\, \bar{g}(t) \quad \text{où} : \bar{g}(t) = 1 + \sum \bar{n}_i\, t^i \quad \text{avec} \quad 0 \leq \bar{n}_{i+1} \leq K n_i .$$

K^{-1} en est donc la plus petite racine positive. Réciproquement tout polynome $g(t)$ de la forme précédente peut être considéré comme la fonction de structure d'au moins un code UND.

Soit $\bar{n}_\ell$ le nombre des séquences de longueur ℓ qui sont diviseur propre à gauche des mots d'un code unitaire (= qui correspondent aux "noeuds" de l'arbre de codage). On a : $\bar{n}_0 = 1$ et $\bar{n}_{\ell+1} + n_{\ell+1} \leq K\bar{n}_\ell$ le signe $\leq$ n'étant partout remplacé par le signe = que si l'arbre est complet, c'est-à-dire si le code est net. Multipliant ces égalités par t^{+1} et sommant, on obtient bien : $g(t) = (1 - Kt)\, \bar{g}(t)$.

15-22

Réciproquement, un polynome de la forme $g(t) = 1 - \sum^{\ell} n_i t^i$ $(n_i \geqslant 0)$ admet au moins un diviseur de la forme $(1 - K't)$ et l'on a : $g(t) = (1 - K't)(1 + \bar{n}_1 t + \bar{n}_2 t^2 \ldots)$ avec $\bar{n}_{\ell+1} \leq K'\bar{n}_i$ pour tout i. Donc si $g(t)$ est un polynome $0 \leqslant \bar{n}_{i+1} \leqslant K'\bar{n}_i$.

D'autre part K' ne saurait être $> K$ car sinon pour ℓ assez grand $N_\ell = \sum \beta_J \gamma_J^{-\ell} \geqslant \beta_1 K'^{\ell}$ serait plus grand que K^ℓ, ce qui est impossible puisqu'il s'agit d'un code et que ceci signifierait que à au moins l'une des K^ℓ suites de ℓ lettres correspondent plusieurs séquences de mots. Enfin si $\bar{n}_i$ satisfait à $0 \leqslant n_{i+1} \leqslant K'\bar{n}_i$ pour tout i il est facile de construire un arbre dont $\bar{n}_i$ et n_i sont respectivement les nombres de noeuds et d'extrémités à distance i de la racine [9]. On observera :

Proposition 4.3.- Dans un code UND le coefficient β_1 de K^i dans l'expression $N_i = \sum \beta_J \gamma_J^{-i}$ est précisément l'inverse de la longueur moyenne $\bar{L}$ des mots quand la fréquence des mots de longueur ℓ est proportionnelle à $K^{-\ell}$.

En effet : $G(t) = \dfrac{1}{g(t)} = \dfrac{(\bar{g}(K^{-1}))^{-1}}{1 - Kt} + \dfrac{B}{\bar{g}(t)}$ où B est une certaine constante.

D'autre part, on a, par hypothèse :

$L = \sum n_i \, i \, K^{-i}$ c'est-à-dire que $-L$ est la valeur de $\dfrac{\partial g(t)}{\partial t} K^{-1}$ pour $t = K^{-1}$ soit encore précisément $\bar{g}(K^{-1})$.

Remarque.

Attachons à tout $a_i \in A_0$ une probabilité $\omega_i \geqslant 0$ $(\sum \omega_i = 1)$ et considérons au lieu de D la matrice $\sum \omega_i D_i$ en appelant D_i la matrice associée à a_i dans la représentation régulière de $\bar{A}$. Les mêmes considérations sont encore valables et les fonctions $N_i(\bar{a})$ deviennent des probabilités dans un processus stochastique (sur A) ou les lettres successives sont tirées au sort indépendamment et avec les probabilités constantes ω_i. Le cas traité ici correspond à un changement d'échelle sur t (qui devrait être remplacé par $t_1 = tK^{-1}$) à celui où tous les ω_i sont égaux et on vérifiera que les propriétés 4.1, 4.2, 4.3 sont des théorèmes bien connus pour les chaines de Markoff. Une théorie peut aussi être développée dans laquelle les matrices D_i n'ont pas nécessairement leurs éléments égaux à zéro ou à un, mais il peut alors

[9] Ceci complète une démonstration de B. Mandelbrot [8] qui laissait ouverte la possibilité que β_1 (le coefficient du terme correspondant à la plus petite racine) soit plus grand pour certains codes non unitaires que pour tout code unitaire.

15-23

se produire que la relation d'équivalence $\equiv (A, P)$ doive être remplacée par une relation plus faible pour tenir compte de la dépendance en chaine des lettres.

Nous n'avons besoin ici que des méthodes énumératives pour établir les deux résultats suivants qui relèvent strictement de la théorie algébrique des demi-groupes et qu'il semblerait difficile d'obtenir autrement.

Proposition 4.4.- Tout code borné d'alphabet fini net à droite est unitaire à gauche.

Soit $L < \infty$ la longueur maximum des mots du code. Puisque le code est net, il correspond, à chacune des K^{ℓ} séquences de longueurs ℓ, au moins une séquence de longueur $\leq \ell + L$ qui appartient à P est dont elle est un diviseur à gauche. Donc : $N_{\ell} + N_{\ell+1} + \ldots N_{\ell+L} \geq K^{\ell}$ pour tout ℓ assez grand. Donc 4.1, au moins une des racines de $g(t)$ est $\leq K^{-1}$ et comme il s'agit d'un code cette racine de module minimum est précisément K^{-1}. Donc (4.2), $g(t)$ est identique à la fonction de structure d'un certain code UND.

Considérons maintenant P'_0, le sous-ensemble des mots du code qui n'admettent aucun autre mot comme diviseur à gauche. Puisque le code est net toute séquence

soit admet un $p \in P'_0$ comme diviseur à gauche

soit est un diviseur à gauche d'un $p \in P'_0$.

Donc l'arbre de codage correspondant au code UND est complet et sa fonction de structure $g'(t)$ admet la racine K^{-1}. Il est impossible que $P'_0 \neq P_0$ car ceci impliquerait que $g(t) = g'(t) - \sum n''_i t^i$ (où les n''_i correspondent aux mots de $P_0 - P'_0$) ce qui ne se peut puisque $g(K^{-1}) = g'(K^{-1}) = 0$. Donc $P'_0 = P_0$ et le code est bien UND.

Proposition 4.5.- Si un code est UND

ou bien il est aussi net à gauche (et par conséquent unitaire à droite)

ou bien le code opposé est tel qu'il existe des séquences non bornées dont le premier mot ne peut pas être décodé sans que soit connue la totalité du message.

On a vu (proposition 1.9) que s'il existait une borne L à de telles séquences on aurait $P_n = \emptyset$ pour un $n < \infty$ ou encore (en posant P_0^m = l'ensemble des séquences formées de m mots non vides) que pour un certain n' $P_0^{n'}$ ne contiendrait aucune paire d'éléments dont l'un soit diviseur à gauche de l'autre.

Or il est clair que si P_0 est l'ensemble des mots d'un code net il en est de même de P_0^n et réciproquement car la fonction de structure $g_n(t)$ de P_0^n est donnée par : $1 - g_n(t) = (1 - g(t))^n$ quel que soit P_0 et n'admet la racine K^{-1} que si $g(t)$ l'admet elle-même. Si donc $\{P_0^m\}$ était unitaire, il serait net puisque la fonction génératrice d'un code est la même que celle du code opposé. Donc $\{P_0\}$ lui-même serait à la fois unitaire et net des deux côtés.

BIBLIOGRAPHIE

[1] - J. RIGUET : Sur la représentation des syntaxes. (à paraitre dans : Zeitschrift für math. Log., 1955).

[2] - J. RIGUET : Relations binaires (Bull. Soc. math. France, t. 76, 1948, p. 114-155).

P. DUBREIL : Trois mémoires intitulés "Contribution à la théorie des demi-groupes. (I, II, III).

[3] - I : Mem. Acad. Sci. Paris, t. 63, 1941, p. 1-52.

[4] - II : Rendiconti di Matematica e delle sue applicazioni, Università di Roma, serie V, vol. X , 1951, p. 183-200.

[5] - III : Bull. Soc. math. France, t. 81 , 1953 , p. 289-306.

[6] - W. FELLER : Introduction to Probability theory. (Wiley, New York 1950) chapitre 12.

[7] - B. MANDELBROT : Thèse, Paris 1952.

[8] - B. MANDELBROT : On recurrent noise limiting codes (Proc. Symp. Inf. Networks, Brooklin, 1954, p. 206-221).

[9] - B. MANDELBROT : Mémoire dans : Proc. Symp. Inf. Theory, 1955 (à paraitre chez Butterworth,London).

[10] - P. ELIAS : Idem

[11] - D. SLEPIAN : Idem

[12] - A.A. SARDINAS et G.W. PATTERSON : A necessary and sufficient condition for unique decomposition ... of coded messages. (Univ. Pennsylvania, Res. Div. reports 50.27 , march 1950).

INSTITUT HENRI POINCARE

SEMINAIRE DE CALCUL DES PROBABILITES

THEORIE DU CODAGE
ET DES EVENEMENTS RECURRENTS

Exposé de M.P. SCHUTZENBERGER

du 16 mars 1956

I. Rappel de la théorie de Feller :(1)

Soit $\xi(t)$ un processus stochastique. Un évènement $\mathcal{E}$ défini sur $\xi(t)$ est un "évènement récurrent" si et seulement si :

1) Il existe une règle permettant de décider si $\mathcal{E}$ s'est ou non produit au temps t_1 en connaissant seulement les valeurs de $\xi(t)$ pour $0 < t \leqslant t_1$.

2) Si $\mathcal{E}$ s'est produit en t_1 sur la suite de valeurs $\xi_1(t)$ $(0 < t \leqslant t_1)$ et si $\xi_2(t)$ est une autre suite $(0 < t \leqslant t_2)$, soit :

$$\xi_3(t) = \xi_1(t) \quad \text{pour} \quad 0 < t \leqslant t_1$$

$$= \xi_2(t - t_1) \quad \text{pour} \quad t_1 < t \leqslant t_2$$

$\mathcal{E}$ se produit au temps $t_1 + t_2$ pour ξ_3 si et seulement s'il se produit au temps t_2 pour ξ_2.

3) Dans ces conditions :

$$\Pr(\xi_3) = \Pr(\xi_1) \quad \Pr(\xi_2)$$

On dit aussi que $\xi(t)$ est un processus "régénératif"(2)

Exemples : 1) $\xi(t)$ est un processus continu à accroissements indépendants ξ défini par :

$$\int_0^t \xi(t)\, dt = 0.$$

---

(1) W. Feller. An Introduction to Probability Theory. Wiley N.Y. 1950), chap. 12.

(2) M.S. Bartlett. Stochastic Processes. Cambridge U. Press, 1955, chap. 3.

2) Le temps est discret. $\xi(t)$ est une suite de variables binomiales indépendantes ξ étant l'apparition de "0", suivi de ℓ "1", suivi d'un "0" ("run" de longueur ℓ). Nous supposerons toujours que le temps et l'ensemble des valeurs possibles de ξ sont discrets.

II. Rappel de la notion de code : (3) (4)

Un demi-groupe libre A engendré par les lettres $\{a_1 \; a_2 \cdots a_n\}$ formant l'alphabet A_0

Une partie P_0 de A : le dictionnaire constitué par les "mots". P le sous demi-groupe de A engendré par P_0. Les séquences appartenant à P étant appelées messages.

P_0 est un code si et seulement si toute suite de lettres $s \in P$ est d'une façon unique un produit de mots. Le code unitaire (5) (sous-entendu "à gauche") si et seulement si $s \; s' \in P$ et $s \in P$ entrainent $s' \in P$. Le code est net (5) (sous-entendu: "à droite") si pour tout $s \in A$, il existe $s' \in A$ tel que $s \; s' \in P$.

Il est bien connu :

Une condition nécessaire et suffisante pour qu'un code soit unitaire est qu'aucun de ses mots ne soit le début d'un autre mot (en langage algébrique : ne soit diviseur à gauche d'un autre mot)..

Réciproquement, s'il en est bien ainsi : pour toutes les séquences de P_0, P_0 est un code.

Exemple :

$A_0 = \{a, b\}$ (alphabet "binaire")

$P_0 = \{a \; a; ab ; baa ; bab ; bb\}$ est l'ensemble des mots d'un code unitaire.

---

(3) Cf. l'exposé fait le 28/11 au Séminaire d'algèbre de M. P. Dubreil (on le référera par l'abréviation "M.P.S.")

(4) Ceci est un cas particulier d'une définition plus générale de J. Riguet.

(5) C'est la définition de P. Dubreil d'un sous groupe unitaire ou net. Mem. Acad. Sc. (1941) pp 1-52

Le dictionnaire opposé ({aa, ba, aab ; bab, bb} correspond bien à un code, mais celui-ci n'est pas unitaire.

Etant donnésun code et une suite "s" de lettres qui est un message, on appellera "décodage" l'opération qui consiste à décomposer s en un produit de p P_0.

Exemple :

m = a a a b b a a se décode : /a a/a b/b a a

On remarque que si le code n'est pas unitaire, l'opération peut nécessiter la connaissance de tout le message avant que soient levées les ambiguités :

Dans le code opposé au précédent :

a a b b a a a =

soit/a a/ b b / a a / a ;

soit/a a b / b a / a a /

La deuxième possibilité est seule à retenir, puisque /a n'est pas un mot.

Si l'on attribue des probabilités fixes aux mots d'un code et que l'on effectue des tirages indépendants, on obtient un processus stochastique sur les suites de lettres :

A tout code unitaire peut être associé un évènement récurrent (l'évènement "fin de mot") et réciproquement (6). En effet, si un processus régénératif est donné, il suffit de considérer comme mots les suites $\xi_i(t)$ telles que ξ se produise en t et ne se soit produit pour aucun $t' < t$.(2) implique que le sous demi groupe est unitaire, donc correspond à un code ; (3) spécifie que les mots sont fournis par un processus indépendant à probabilités fixes.

III. Notion de Préfixe (7, cf. p. 4)

Soit $\approx$ la relation d'équivalence entre séquences de A définie par : $s_1 \approx s_2$ si et seulement si quelle que soit la séquence x :

$$\Pr(s_1 x / s_1) = \Pr(s_2 x / s_2)$$

---

(6) Ce résultat a été utilisé sous une forme un peu différente dès 1952 par B. Mandelbrot qui a le premier souligné les rapports entre codage et évènements récurrents.

Manifestement quel que soit $s' \in A$:

$$s_1 \approx s_2 \quad \text{entraîne} \quad s_1 s' \approx s_2 s'$$

car $\Pr(s_1 s' x / s_1 s') = \Pr(s_1 s' x / s_1) : \Pr(s_1 s'/s_1)$

$= \Pr(s_2 s' x / s_2) : \Pr(s_2 s'/ s_2) = \Pr(s_2 s' x/ s_2 s')$

On appellera "préfixe" $\tilde{s}$ l'ensemble des séquences équivalentes à s selon $\approx$.

La notion de préfixe est une sorte de généralisation de celle de résumé exhaustif de G. Darmois : Si un message commence par s_1, la distribution de son "futur" à partir de sa dernière lettre ne dépend que de $\tilde{s}_1$.

Proposition III.1

Dans un code UN (unitaire à gauche et net à droite) l'ensemble des messages constitue un préfixe unique que l'on désignera toujours par α_1.

(immédiat d'après (I.(3)). La proposition admet une réciproque, mais nous n'aurons pas besoin de celle-ci). Dans les applications les plus fréquentes l'ensemble $\mathcal{A}$ des préfixes est fini - ou a une structure topologique très simple (Cf. M.P.S.).

Si $\xi(t)$ $(0 \leq t < t_1)$ représente les lettres successives d'une séquence aléatoire, on peut lui associer $\tilde{\xi}(t)$ qui est une variable aléatoire prenant ses valeurs dans $\mathcal{A}$: par construction, la suite des $\tilde{\xi}(t)$ est une chaîne de Markoff d'ordre 1 caractérisée par les probabilités de transition $p_{ij}(k)$ (que $\tilde{\xi}(t)$ passe du préfixe α_i au préfixe α_j par adjonction de la lettre $a_k \in A_0$).

Exemple :

(Code donné plus haut en exemple), les préfixes sont :

$$\alpha_1 \; ; \alpha_2 = \tilde{a} \; ; \alpha_3 = \tilde{b} \; ; \alpha_4 = \tilde{b a} :$$

Les probabilités des mots étant :

---

(7) Les préfixes utilisés ici sont plus généraux que ceux introduits dans M.P.S. : en toute rigueur, on devrait les appeler préfixes stochastiques. On a d'ailleurs "$\approx$ plus fine que $\sim$" pour équivalence purement algébrique $\sim$ définie plus bas (IV).

$Pr(a\ a) = p_1$; $Pr(a\ b)$ pr ; $Pr(b\ a\ a) = p_3$; $Pr(b\ a\ b) = p_4$

$Pr(b\ b) = p_5$ $(p_1 + p_2 + p_3 + p_4 + p_5 = 1)$, on botient la matrice :

	α_1	α_2	α_3	α_4
α_1	0	p_1+p_2	$p_3+p_4+\beta$	0
α_2	1	0	0	0
α_3	0	0	0	p_3+p_4 / $p_3+p_4+\beta$
α_4	1	0	0	0

On appellera Π cette matrice dans le cas général et on désignera par $h(\lambda)$ le déterminant $|\lambda\Pi - I|$.

Supposons en particulier que le code soit unitaire : s'il n'était pas net, il existerait un préfixe α_0 contenant toutes les séquences telles que $Pr(s\ s' \in P) = 0$ quel que soit s'. En outre deux cas peuvent se présenter :

ou bien il existe un préfixe au moins $\alpha_i \neq \alpha$ tel que l'on puisse trouver s et s' avec $\tilde{s} = \tilde{s}\tilde{s'} = \alpha_i$ sans que $\tilde{s}\,\tilde{s''} = \alpha_1$ pour aucun s'' diviseur à gauche de s' : dans ce cas il existe des mots de longueurs non bornées (toutes les séquences de la forme $s(s')^n s''$ où s'' est tel que $s\ s'' \in P$) même si α est fini ;

ou bien il n'en existe pas et alors l'ensemble α est fini si tous les mots ont une longueur bornée, car il existe en "ordre local" sur α (la matrice Π privée des lignes et des colonnes d'α et α_1 est nulle en dessous de la diagonale principale).

Dans ce dernier cas qui est le plus important dans la Théorie des communications, on a :

Proposition III.2

$$h(\lambda) = 1 - \sum \Pi_i \lambda^2$$

où Π_i désigne la somme des probabilités des mots de longueur i.

et $H(\lambda) = 1 + \sum_{i=1}^{\infty} \Pi_i \lambda^i = 1/h(\lambda)$

où $\overline{\Pi}_i$ est la probabilité qu'une séquence de longueur i soit un message. En outre une condition nécessaire et suffisante pour que le code soit net est que $h(1) = 0$.

Dans ces conditions $\overline{\Pi}_i = \beta_1 + \sum_j \beta_j \rho_j^{-i} \ldots$

où les ρ_j sont les autres racines de $h(\lambda) = 0$ (dont les modules sont > 1, sauf si la longueur des mots admet un P.G.C.D. $\neq 1$) et où les β_j sont des constantes avec :

$$\beta_1^{-1} = \left[\frac{\partial}{\partial \lambda} h(\lambda) \right]_{\lambda=1} = \text{longueur moyenne des mots.}$$

Tous ces résultats sont des interprétations immédiates de résultats bien connus pour les chaînes de Markoff et nous n'en entreprendrons pas la démonstration : - l'identité $H(\lambda) = (h(\lambda))^{-1}$ est précisément le théorème fondamental de Feller. La preuve de sa validité et son extension au cas où les mots n'ont pas une longueur bornée ne demande que quelques précautions supplémentaires.

IV. Le décodage des messages altérés par le bruit

Supposons un code UN dont la longueur des mots est bornée, mais non constante.

Puisque le décodage s'effectue de proche en proche, il semblerait que la plus légère altération dût détruire , sauf chance exceptionnelle, la totalité de la signification. Par exemple (nous supposerons toujours pour simplifier qu'il s'agit d'un code binaire et que c'est la première lettre seule qui est altérée), dans le code que nous avons déjà utilisé

a a a b b a a se décode aa/ ab / aa /, mais b a a b b a a se décode
b a a/b b/a a/

Observons cependant que s'il se trouvait (comme dans le cas présent) que le décodage du message et du message altéré conduisent à placer la "fin de mot" à la même n-ième lettre, le reste de la séquence serait correctement déchiffrable - en supposant que de nouvelles altérations ne se produisent pas.

Donc, si ce phénomène est assez fréquent et si les altérations sont rares, une large partie du message sera encore utilisable.

Considérons algébriquement le problème : si s est le début du message, s' le début du message altéré, nous , nous voulons que les lettres suivantes s'' soient telles que :

$$s\, s'' \in P \quad \text{et} \quad s'\, s'' \in P$$

En particulier si $s \in P$, il faut que $s'' \in P$ (puisque le code est unitaire) et le problème qui se pose est de savoir s'il existe un $s' \notin P$ tel que $s'\, s'' \in P$.

Ceci est indépendant - dans une certaine mesure - de toute question de probabilités et nous redéfinissons des "préfixes-algébriques" par : $s_1 \sim s_2$ si et seulement si $s_1 x \in P$ entraine $s_2 x \in P$ pour tout $x \in A$.

Dans les cas étudiés $s_1 \approx s_2$ entraine $s_1 \sim s_2$ et il n'y aura pas d'inconvénient à parler désormais du préfixe $\tilde{s}$ pour signifier le préfixe algébrique formé par la classe d'équivalence de s par $\sim$.

Nous avons encore une représentation matricielle : et cette fois chacune des lettres $a_1 \in A_0$ correspond à une application dans lui-même de $\mathcal{C}$ c'est à dire à une matrice dont chaque ligne contient Un seul élément (égal à 1) différent de zéro.

α_1 et α_0 ont la même signification que précédemment (α_0 est vide puisque le code est supposé net). Ceci fournit une représentation du demi-groupe A engendré par A_0 qui est finie dans le cas étudié et par conséquent isomorphe à une image homomophe $\bar{A}$ de A que l'on a appelée "le demi groupe fondamental du code" (M.P.S. Section 3).

Naturellement, le code opposé aurait un autre système de préfixes, ce qui donnerait une autre représentation (toujours isomorphe, mais en général non équivalente à la précédente, d'ailleurs).

Définition

Un code sera dit absorbant s'il existe au moins une suite q finie, de probabilité non nulle telle que quel que soit $s \in A$ sq appartienne à P. Pour en terminer avec les considérations intuitives, indiquons que si un code est absorbant, quelle soit l'aléération unique produite au début du message, le décodage de celle-ci sera presque certainement correct à partir d'une certaine longueur : en effet, d'une part la dernière lettre de sq est toujours une fin de mot quel que soit s et par conséquent les décodages de $s\, q\, s''$ et $s'\, q\, s''$ concordent au moins à partir de cette lettre, d'autre part q appartient lui-même à P, donc les messages de m mots ne le contenant pas, ont une probabilité inférieure à :

$$(1 - Pr(q))^m \quad \text{qui tend vers zéro avec } 1/m.$$

On a donc comme une sorte de propriété ergodique en ce sens que le décodage d'un message dans un code absorbant tend à être indépendant du décodage correct ou non de ses premiers mots.

Proposition IV.1

Une condition nécessaire et suffisante pour qu'un code unitaire,

net, borné (UMB) soit absorbant est que quel soit $s \in A$, il existe $s' \in P$ tel que $ss' \in P$.

Considérons la représentation de A comme demi-groupe d'application de $\mathcal{O}_0$ dans lui-même : la condition signifie que quel que soit $\tilde{s}$ il existe $s' \in P$ avec $ss' \in P$: les matrices correspondant aux mots transforment le préfixe α_1 dans lui-même par hypothèse.

Soit donc $s_1' \in P$ tel que $ss_1' \in P$ pour au moins un $s_1 \notin P$; $\alpha s_1'$ est strictement plus petit que α, soit de nouveau $s_2 \notin P$, $s_2 \notin P$, $s_2 s_1' \notin P$, il existe $s_2' \in P$ tel que $s_2 \tilde{s}_2' \in P$ et $\alpha s_1' s_2'$ est encore de puissance strictement inférieure $\alpha s_1'$ etc. On finit ainsi par construire au moins une séquence $s_1', s_2' \ldots s_m' \in P$ qui est précisément la séquence q cherchée.

Observons d'ailleurs que "q" a une représentation très remarquable : "q" s'il existe correspond à la matrice dont les éléments de la colonne α_1 (et ceux-là seulement) sont égaux à 1.

Comme pour tous les problèmes ergodiques des conditions d'indécomposabilité jouent un rôle fondamental.

Proposition IV.2

Une condition nécessaire et suffisante pour que le code soit absorbant est que quelles que soient les suites s et s', on puisse trouver une suite s'' telle que $ss'' \sim s's''$ (c'est-à-dire $\tilde{s}\tilde{s}'' = \tilde{s}'\tilde{s}''$).

La condition est nécessaire, car si q existe $\tilde{s}q = \alpha_1$ quel que soit q.

Elle est suffisante, car elle implique pour tout $s \notin P$ qu'il existe s' tel que $ss'' \sim s's''$ pour $s'' \in P$. On en déduit :

Proposition IV.3

Les codes suivants ne sont pas absorbants :

a) les codes unitaires à droite

b) les codes dont le P.G.C.D. des longueurs des mots est différente de 1.

c) les codes "composés uniformes" dont l'ensemble des "mots" P_0 est l'ensemble P_0^{ν} de tous les messages formés de ν mots d'un autre code unitaire noté P_0'.

a) est immédiat : unitaire à droite signifie que $ss' \in P$ et $s' \in P$ impliquent $s \in P$ (l'existence de tels codes n'est pas évidente. Une famille infinie d'exemples est donnée dans M.P.S.)

b) : immédiat aussi : si la longueur $|s|$ de s différe de la longueur s' de s' par une quantité non équivalente à zéro (module ℓ) il en est de même de sx et de $s'x$ quel que soit $x \in A$.

c) Considérons s' formé de m' mots successifs de P'_o. Quel que soit $s \in P$, la séquence $s's$ est décodable dans P' et $_oy$ est formée de $m' + k_\nu$ mots (de P') donc elle ne peut jamais appartenir à P.

Malgré de longs efforts, je n'ai réussi ni à trouver d'autres codes (UNB) qui ne soient pas absorbants, ni à prouver que ce sont là les seuls codes qui ne jouissent pas de cette propriété ergodique.

En dehors de résultats encore fragmentaires, on ne connaît qu'un seul énoncé assez général que nous allons établir.

Préalablement, posons pour simplifier $|s|$ = la longueur de s quel que soit $s \in A$ et considérons le cas où, k étant le nombre des lettres de A_o, la probabilité d'un mot s quelconque est égale à $K^{-|s|}$. On vérifie que dans ce cas, si le code est UNB, les lettres successives du processus de codage apparaissent avec les mêmes fréquences que si elles étaient tirées indépendamment et avec des probabilités égales.

On a alors :

$\overline{\pi}_i = k^{-i}\,\overline{n}_i$ (respectivement $\pi_i = k_i^{-1}\,n_i$) où $\overline{n}_i$ (resp. n_i) est le nombre de messages (resp. mots) de longueur i. Soit alors h. la longueur moyenne des mots.

D'autre part v étant une séquence fixe, considérons l'ensemble $V \subset P_o^m$ (pour m assez grand fixe aussi) des séquences formées de m mots et admettant v comme diviseur à droite. Posons :

$$\gamma_v = \sum_{w \in V} k^{-|w|+|v|}$$

Proposition IV.4.

Une condition nécessaire et suffisante pour qu'un code UNB ne rentrant dans aucune des classes décrites en IV.3 soit absorbant est qu'il existe une séquence v telle que :

$$2k^{|v|}\,\gamma_v > h$$

Démonstration.

Appelons $D_\ell(u,v)$ l'ensemble des séquences de longueur $\ell > |u| + |v|$ admettant u et v respectivement comme diviseurs à gauche et à droite, où u est une séquence fixe.

1°) Le nombre des séquences distinctes de D (u, v) est

$$k^{-(\ell - |u| - |v|)} = d_\ell$$

Soit $D'_\ell(u,v)$ le sous-ensemble de $D_\ell(u, v)$ formé par les séquences de longueur ℓ de la forme ux avec $x \in P$.

2°) Le nombre des séquences distinctes de D' (u,v) est de la forme :

$$d'_\ell = k^{-(\ell-|u|)} \gamma_v h^{-1} + \varepsilon(\ell) \quad \text{où} \quad k^{-\ell}\, \varepsilon(\ell) \longrightarrow 0 \quad \text{avec} \quad \ell .$$

En effet d'_ℓ est égal au nombre $V_{\ell-|u|}$ des messages de longueur $\ell - |u|$ admettant v comme diviseur à droite : c'est-à-dire si v_i est le nombre des w de longueur i dans V :

$$V_{\ell-|u|} \sum \bar{n}_{\ell-|u|-i}\, V_i \quad \text{Or (III.2)} \quad n_i = k^{-i} h^{-1} + \varepsilon_1(i)$$

(car $h(\lambda)$ n'a qu'une seule racine de module égal à 1 après l'exclusion du cas b) de IV.2).

Donc :

$$V_{\ell|u|} = k^{-\ell+|u|} \cdot h^{-1} \left\{ \sum_{w \in V} k^{-|w|+v} \right\} + \varepsilon_2(\ell)$$

3°) Le nombre d'' des messages appartenant à $D_\ell(u,v)$ est de la forme :

$$d''_\ell = k^{-\ell+|u|} \gamma_v h^{-1} + \varepsilon_3(\ell)$$

Soient u' le diviseur à gauche maximum de u qui appartienne à P et u''_1, u''_2 ... $u''_i \in U$ les messages minimum qui admettent u comme diviseur à droite

$$d''_\ell = \sum_{u''_i \in U} v_{\ell - |u''_i|} = \sum_{u'' \in U} k^{-\ell + |u''|} \gamma_v h^{-1} + \varepsilon_s(\ell)$$

$$= k^{\ell + |u'|} \gamma_v h^{-1} \left\{ \sum_{u'' \in U} k^{-|u'| + |u''|} \right\} + \varepsilon_s(\ell)$$

Or l'expression dans l'accolade est égale à $k^{|u| - |u'|}$ puisque le code est net.

4°) $d''_\ell + d'_\ell > d_\ell$ pour $\ell \to \infty$ est équivalent à =

$2 \gamma_v k^v > h$

(le calcul est immédiat).

Donc, si l'inégalité est vérifiée, quel que soit u fini, il existe, pour ℓ assez grand, au moins un élément de $D_\ell(u,v)$ qui est un message, c'est-à-dire qu'il existe un $s \in P$ avec $u\,s \in P$, ce qui établit le résultat d'après IV. 1, et IV. 2.

Exemple : Nous reprenons le code déjà traité en exemple :

$k = 2$; $h = 2\ 1/4 + 2\ 1/4 + 2\ 1/4 + 3\ 1/8 = 18/8$

Soit $v = a\ a$; $\gamma_v\ (1/4 + 1/8 = 3/8$. $|v| = 2$.

On a : $2 \times 3/8 \times 4 > 18/8$. Donc ce code est absorbant. ($q = a\ a$ précisément).

-:-:-:-:-:-:-:-:-

ALGÈBRE. — *Une théorie algébrique du codage.*

Note de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

Étant donné un ensemble A_0 de « messages élémentaires » et un ensemble A_0 de « lettres » on peut définir un code comme une correspondance $\mathcal{C}$ entre les éléments de A_0 et certaines séquences de lettres (les « mots ») telle qu'inversement à toute semblable séquence corresponde au plus une suite unique de messages. Ceci revient à dire que le décodage doit être sans ambiguïté quand il est possible ou encore que $\mathcal{C}^{-1}$ est quasi fonctionnelle (1). Ces structures jouent un certain rôle dans la théorie des algorithmes et, en calcul des probabilités, dans celles des événements récurrents (2) puisque cette dernière étudie les processus stochastiques sur les suites de lettres associés par $\mathcal{C}$ à d'autres définis sur A_0.

Le but de la présente Note est d'indiquer comment cette théorie peut être replacée dans ce qui semble être son domaine naturel : la théorie des demi-groupes et l'on observera que les notions utilisées ici, qui sont classiques (3) dans ce domaine ont une interprétation très immédiate et souvent importante sur le plan de la réalisation physique des machines codeuses et transcodeuses.

Définition. — 1° Soient A et A respectivement les demi-groupes libres engendrés par A_0 et A_0. On dira que la structure $(A_0, A_0, \mathcal{C})$ est un code (4) si l'extension de $\mathcal{C}$ à A est un isomorphisme entre A et un sous-demi-groupe P de A.

2° Un code sera dit fini si la longueur de tous ses mots (c'est-à-dire des éléments de $P_0 = \mathcal{C}A_0$) est finie; *unitaire* (3) à gauche ou à droite, *net* (3) à gauche ou à droite s'il en est de même du sous-demi-groupe $P \subset A$.

3° K étant une partie quelconque d'un demi-groupe quelconque aussi D, on appellera « *équivalence syntactique* » $[\equiv (D; K)]$ la relation entre éléments de D : $a \equiv a' (D; K)$ si et seulement si pour tout $x, y \in D$ $xay \in K \Leftrightarrow xa'y \in K$.

(1) J. Riguet, *Bull. Soc. Math. France*, 76, 1948, p. 129.

(2) *Cf.* B. Mandelbrot, *Contr. théorie math. des jeux de communications*, Paris, 1953, p. 124, pour une étude des relations entre codage et événements récurrents.

(3) *Cf.* P. Dubreil, *Mém. Acad. Sc.*, 63, 1941, p. 16, auquel sont empruntés les éléments de la théorie des demi-groupes utilisés ici.

On démontre :

$\equiv\!:(D;K)$ est une relation d'équivalence régulière (3). (En effet la définition s'écrit aussi $K\cdot.ay=:K\cdot.a'y$ pour tout y. Donc $\equiv\!:$ qui est manifestement une équivalence, est régulière à droite et à gauche.)

Si K est un sous-demi-groupe Q de D, $\equiv\!:(D;Q)$ est la moins fine des relations d'équivalence régulières pour lesquelles Q soit saturé (3). (En effet si ρ est une telle relation $a\rho a'$ entraîne $xay\rho xa'y$ et, par conséquent, $xay\in Q$ entraîne $xa'y\in Q$.)

Evidemment si D était un groupe $\equiv\!:(D;K)$ serait l'équivalence normale associée au plus grand sous-groupe invariant contenu dans K. On appellera φ_K l'homomorphisme attaché à $\equiv\!:(D;K)$. La relation $\equiv\!:(\varphi_K D;\varphi_K K)$ est réduite à l'égalité et l'on dira que $\varphi_K K$ est *syntactiquement simple* dans $\varphi_K D$. Si $A\supset P$ est un code $\varphi_P A$ et $\varphi_P P$ en seront les *demi-groupes fondamentaux*. On démontre : Si le code est fini, $\varphi_P A$ est fini (la réciproque n'est pas vraie : en particulier si $\varphi_P A$ est un groupe, le code n'est fini que s'il est cyclique et $\varphi_P P$ réduit à l'élément unité). P est unitaire ou net en même temps que $\varphi_P P$. Réciproquement il est important de savoir si un couple de demi-groupes $A'\supset P'$ syntactiquement simples peuvent être les demi-groupes fondamentaux d'un code pour un certain choix de générateurs :

Une condition nécessaire et suffisante est que pour tout $p,q\in P'$ $ps\in P'$ et $sq\subset P'$ *entraîne* $s\in P'$.

La propriété est donc indépendante du choix des générateurs. La démonstration que nous ne pouvons donner ici repose sur le fait que si $s\notin P'$ la suite psq correspondrait à deux suites de messages irréductiblement distinctes. Il en résulte la possibilité de construire explicitement tous les codes (qui sont en nombre infini) correspondant à des demi-groupes fondamentaux donnés.

Enfin des méthodes d'énumération permettent d'énoncer :

Si $(\Lambda_0, A_0, \mathcal{C})$ est un code fini et si P est un demi-groupe net, P est unitaire. (La réciproque n'est pas vraie.)

En effet le fait que P soit unitaire correspond à la possibilité d'ordonner ses mots de façon lexicographique sans qu'aucun ne soit le commencement d'un autre (ou encore qu'il existe un « arbre de codage ») et le fait qu'il soit net à la possibilité qu'une séquence quelconque de lettre puisse être complétée en une suite de mots.

---

(4) J. Riguet emploie le mot code dans une acception plus générale. La définition adoptée ici est celle implicitement utilisée dans la théorie des communications.

Ceci permet de répondre à un problème pratique d'optimalité (5) en montrant que la classe des codes unitaires est admissible. En outre ceci indique l'existence de codes finis nets et unitaires à gauche et à droite à la fois qui ne correspondent à aucun groupe. L'inventaire de ces demi-groupes particuliers reste encore à faire.

(5) Posé par : A. A. Sardinas et G. W. Patterson, *Res. Div. Reports*, 1950, p. 50-27. University of Pennsylvania.

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*, t. 242, p. 862-864, séance du 13 février 1956.)

GAUTHIER-VILLARS,
ÉDITEUR-IMPRIMEUR-LIBRAIRE DES COMPTES RENDUS DES SÉANCES DE L'ACADÉMIE DES SCIENCES
149553-56 Paris. — Quai des Grands-Augustins, 55.

IRE
Transactions
on INFORMATION THEORY

Vol. IT-2, No. 3 September, 1956

1956 SYMPOSIUM ON INFORMATION THEORY

held at

Massachusetts Institute of Technology
Cambridge, Massachusetts

September 10-12, 1956

PUBLISHED BY THE
Professional Group on Information Theory

ON an APPLICATION of SEMI GROUPS METHODS TO SOME PROBLEMS in CODING

By M.P. Schützenberger
(C.N.R.S. Paris)

0. Introduction.

The current paper deals with a chapter in what could be called communication theory in extensive form : it starts with extremely restricted structures and it stops where begins the canonical problem of optimalisation. It even ends sooner for no full use of the definitions is made and the main ergodic theorem is stated without proof.

Actually the nature itself of the question under study has commanded these restrictions together with the architecture of the paper : we give a abstract model of some sort of language and we try to show how semi group concepts apply fruitfully to it with the hope that some of them may be at least of stimulating interest to specialists working on natural languages.

As frequent in the field of cybernetic, the mathematics involved even if quite simple are far away from classical analysis and, indeed, many of the necessary tools had to be sharpened especially for the purpose.

Thus the paper is twofold : in a first part the model and its main properties are discussed at a concrete level on the simplest cases : the coding and decoding with length bounded codes. In a second part a selection of theorems are proved whenever the necessary semi group theoretic preliminaries are not exacting. The link along this tail of appendices is the theory developped verbally in the first part. Finally a special chapter provides a bridge toward probalistic applications.

It is proper at this place to acknowledge the contributions of three authors who influenced deeply the building of the theory :

Sardinas and Patterson[1] who discussed first on a logical basis the general coding process.

B. Mandelbrot[2] who recognised and studied extensively the role of "word units" in communication theory and related the problem to Feller's recurrent events.

P. Dubreuil[3] and his school whose pionnering work on discrete semi groups has provided many basic concepts and arguments as it will be seen below.

Part I

1. Preliminary definition of a discrete semi group language :

We shall be concerned with the two basic sets of communication theory :

The set of all messages which may possibly be sent.

The set of all signals available for transmission along the line.

The main feature of the theory is the postulationnal requirement that the signals as well as the messages pertain both to some common class of structures so that coding and decoding not only be inverse operations but far more generally, be special instances of a quite broad new process, that of translation.

This identity of structure itself between two sets is a result from the basic restriction that they develop homogeneously in time - or more accurately that both admit a common partial order and composition operation.

That such requirements are rather stringent is clearly seen by the exemple of photography (two exposures give rarely a result which is, in any sense, equivalent to a third one) or even by harmonic modulation where Fourier transform exchanges so well time and frequency that finite signals cannot be fully adequate.

On the other hand, languages either spoken, written or gesticulated are somewhat akin with our consideration, and we shall use the name of "discrete semi group languages" (d.s.g.l.) for naming the elemental concepts of our study.

The definitions below are quite general and as said before, no full use of them will be made here - very little gain in simplicity would be achieved by using more restrictive ones.

DEFINITIONS :

I. A discrete semi group language will be a set Λ of object called "messages" satisfying the following conditions :

I.1. If λ_i and λ_j pertain to Λ so does their "product" $\lambda_k = \lambda_i \lambda_j$ made up of "λ_i" followed by "λ_j" (λ_i will be said a left divisor and λ_j a right divisor of λ_k).

I.2. If λ_i , λ_j and λ_k pertain to Λ and if $\lambda_\ell = \lambda_i \lambda_j$ and $\lambda_m = \lambda_j \lambda_k$ then $\lambda_i \lambda_m$ is identical with $\lambda_\ell \lambda_k$.

I.3. The "vacuous message" ρ pertains to Λ and satisfies $\rho \lambda_i = \lambda_i \rho = \lambda_i$ for all $\lambda_i \in \Lambda$

I.4. There is a sub set Λ_c from Λ called "dictionary" or "basis" whose elements are called "words". Λ_c is such as :

I.4.1. ρ does not pertain to Λ_c

I.4.2 for all $\lambda_i \in \Lambda - \rho$

either $\lambda_i \in \Lambda_c$

either these exist a unique finite set of words $\lambda_{i_1}, \lambda_{i_2}, \ldots \lambda_{i_m} \in \Lambda_0$ with

$\lambda_i = \lambda_{i_1} \lambda_{i_2} \ldots \lambda_{i_m}$.

II. Given two d.s.g.l. Λ and M a correspondence θ between the elements of two subsets $\Lambda' \subset \Lambda$ and $M' \subset M$ will be said a translation if it satisfies :

II.1. The correspondence is one to one where ever it is defined.

II.2. If $\lambda_i, \lambda_j \in \Lambda', \theta\lambda_i = \mu_i, \theta\lambda_j = \mu_j$, then $\lambda_i \lambda_j \in \Lambda'$ and $\theta(\lambda_i \lambda_j) = \mu_i \mu_j$

II.3. The translation will be said :

Total from Λ to M, if $\Lambda' = \Lambda$.
Subtotal from Λ to M, if for all $\lambda_i \in \Lambda$ there is at least a $\lambda_j \in \Lambda$ such as $\lambda_i \lambda_j \in \Lambda'$.

III. A neat coding of Λ into M will be a translation total from Λ to M and subtotal from M to Λ.

In algebraic form we could reduce our axiomatic to :

I' : Λ is the free discrete semi group generated by Λ_0

II' : A translation is an isomorphism between the sub semi groups $\Lambda' \subset \Lambda$ and $M' \subset M$

III' : A translation is a neat coding if $\Lambda' = \Lambda$ and M' is a subsemigroup of M neat on the right. (Note that "subsemigroup" entails I.1, I.2 and I.3 ; "free" corresponds to unique in I.4.2 , "discrete" to finite at the same place).

2. Practical significance of the axiomatic :

Let us take a simple example in coding :
$\Lambda_0 = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$; $M_0 = \{+, -\}$
(M_0 is the usual binary alphabet; Λ is the set of all strings of a finite number of the "elementary messages" λ_i $(i = 1, 2, 3, 4)$ and M is built in the same way with the "letters" + and - .

When coding, we want to establish a correspondence between Λ and some subset M' of M satisfying two conditions :

1) to every $\lambda \in \Lambda$ corresponds at least one $\mu \in M$ ("total" character of the coding)

2) to any distinct $\lambda, \lambda' \in \Lambda$ must correspond distinct $\mu, \mu' \in M'$ in order that the deciphering be free from ambiguity.

A priori any one to one correspondance between Λ and a subset M' from M would do - but usually this could imply that we cannot proceed to the sending of the message before we know it in its totality. So a further practical condition - which is not too easy to formulate rigourously - could be :

3) For a reasonably large number of messages λ the coding is such that for any right multiple λ' of λ (i.e. any $\lambda' = \lambda\lambda''$) the signals μ and μ' have a reasonably long common left divisor μ_1, (i.e. are of the form : $\mu = \mu_1 \mu_2$ and $\mu' = \mu_1 \mu_2'$).

The simplest way of fulfilling these desiderata is to assign to each $\lambda_i \in \Lambda_0$ a string of binary letters μ_i (which very conveniently we may too call a word) and for any sequence $\lambda_{i_1}, \lambda_{i_2}, \ldots \lambda_{i_m}$ to send the corresponding sequence: $\mu_{i_1}, \mu_{i_2} \ldots \mu_{i_m}$.

For example, with the correspondance : θ_1 :
$\lambda_1 \to + = \mu_1$; $\lambda_2 \to +- = \mu_2$; $\lambda_3 \to -+- = \mu_3$;
$\lambda_4 \to -- = \mu_4$
we would have :
$\lambda_2\lambda_3\lambda_1\lambda_1\lambda_2 \to +\,+\,-\,-\,+\,-\,+\,+\,+\,+\,-\,-$.

It is not obvious however how the set M_0' of the words μ_i has to be selected so that decoding be free from ambiguity :

At my knowledge, the question has been raised first and practically solved by Sardinas and Patterson in a pioneering paper(1).

With the help of semi group concepts we may however obtain a deeper insight into their whole procedure which was purely logical :

We are looking for a total translation from Λ to M and it is quite axiomatic that the decoding is unambiguous if and only if the sub semi group M' generated by M_0' is isomorphoric to the free semigroup Λ - or - for short - that M' is a free subsemigroup of M .

Algebraic consequences of this simple remark are to be found in appendix 1.

Now would come a fourth requirement : (admissibility)

4) The length of the words μ_i must be as small as possible in respect of some a priori probability distribution on Λ .

As a matter of fact (4) will be met incidentally, so to say, in wiew of another condition we put in definition III :

That the translation from M back to A be sub total :

What this means exactly is that any sequence μ of binary digit be a left divisor of at least one message $\mu' \in M'$ which can be completely and exactly retranslated into A .

This condition together with the possibility of one-to-one deciphering implies automatically that the code be unitary (as defined below)(see appendix 0), and admissible in that sense that it meets the optimality requirement (4) in respect of at least one a priori probability distribution of the words. (*)

3. Discussion of the decoding methods : scansion

This being settled we have to look more closely at the decoding.

For avoiding repetition let us observe that A does not play any role by itself since the $\lambda_i \in A_0$ are in a one-to-one correspondance with the words $\mu_i \in M'_0$. So we may perfectly well dispense from mentioning it altogether.

But in order to stress when a given string μ of binary symbols is really a set made up of a sequence of words and not any odd sequence of + and - we shall say that μ is a complete message (for instance : " + + - - + - " $= \mu_2 \mu_3$ is a complete message, but " + + - - " is not) and indicate it by enclosing it into two / signs, which shall denote too, end and beginning of the words.

Let us try to decode the following complete message in code $\mathcal{C}_1$:

/ + + - - + - - + - - + /

The only way open is trial and error : the first + may be:

- either μ_1 itself
- either the first letter from $\mu_2 = /+ + - /$

so that we have the choice between :

/ + / + - - + - - + - - + / and / + + - / - + - - + - - + /

In the first case no further doubt comes in and we are lead to :

/ + / + / - - / + / - / + / - / + / = $\mu_1 \mu_1 \mu_4 \mu_1 \mu_4 \mu_1 \mu_4 \mu_1$

In the second we obtain :

/ + + - / - + - / + - - / + = $\mu_2 \mu_3 \mu_3 - +$

Since here - + is left at loose end (strictly speaking) the first translation was the good one, being known that the transmission is over. Observe that if, on the contrary, the signal was the same as before except for an added terminal - digit, the conclusion would be exactly opposite :

/ + + - / - + - / - + - / + - /

is the only fitting "scansion" as we could say by borrowing from prosody this term for its classical flavour.

So the inverse translation from M back to A does not look like satisfying very reasonably the above condition 3.

An obvious remedy to it would be to limit still more the set M'_0 . B. Mandelbrot, who has first discussed these problems has distinguished several possibilities :

1) Uniform codes : in which every word has the same length (i.e. number of letters), this criterium giving a direct scansion (examples: all the noise reducing codes introduced so far except for a proposal of "sequential coding" by Peter Elias(4) and some examples by Lemnael(5).)
2) More generally : what we shall call :

   Unitary codes : i.e. codes in which no word is a left divisor of another word (examples : Fano's, Huffman's, Shannon's codes)
3) Natural codes : (introduced by B. Mandelbrot) in which a special letter points out the end of the word (example : most of the spoken or written languages).

   Further, Mandelbrot has shown that any unitary code is, at least asymptotically, as good from the point of view of economy of length as any other one. It could seem futile then to care for more extensive classes were we not prompted by other circumstances - and especially by the threat of a noise.

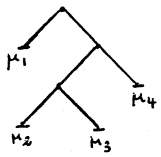
4. Noise absorption and eryodism.

Consider indeed the following code : $\mathcal{C}_2$

$\mu_1 = +$; $\mu_2 = - + +$; $\mu_3 = - + -$; $\mu_4 = - -$

(which is, parenthetically, just the previous one with the time arrow inverted)

It is unitary all right so that we may represent it by a "tree" in the familiar fashion :



(south west arrow : +

south east arrow : -)

The "neat" condition (subtotality of the translation from M back to A) is reflecting itself in the fact that any branch of the tree

(*) If M is the free semi group of all phonemic sequences in English and M' the sub set of all "semantically correct sentences", M' is neat in M .

For instance :

" /pri wat law cut chur coco feet .."(obtained from King Lear, Act III, scene I, with Tippet's help) is fitted into a complete message in M' by adding : "... and this, Gentlemen, was, may-be, my best example of a semantically void utterance /")

ends with a word (for example the code $\mu_1 = +$; $\mu_2 = -++$; $\mu_3 = --$ would not be neat since no word nor sequence of words may begin with $/- + - \ldots$).

Suppose that we have to decode the sequence :

$$/- + - - + - + - - + - -$$

we obtain directly :

$$/- + - / - + - / + / - - / + / - - /$$

and we could have written it down extemporaneously without waiting for the end of the transmission.

But if the first digit had been blurred by noise, this straight forward attitude could not be kept : indeed we decipher the uncertain message

$$/?- - + - + - - + - - \ldots$$

either as :

$$/+/+/-/+/-+-/-+-/- \ldots$$

either as above :

$$/-+-/-+-/+/--/+/--/ \ldots$$

and as long as the message is going on we have no evidence for deciding between this two interpretations. Things nonetheless are not so bad as they look at first glance :

Suppose that the next letters which appear be $+ + - + - + - \ldots$

so that up to this time the two alternative versions are :

$$/+/+/-/+/-+-/-+-/-+-/+//-+-/+/- \ldots$$
$$/-+-/-+-/+/--/+/--/+/+//-+-/+/- \ldots$$

By the seemingly fortuitous fact that in both case the end of a word falls exactly as the same spot (marked // above), the two translations coincidate from this point on and since one of them must be right so is the end of the deciphering - assuming of course that no new error of transmission takes place.

Practically, if such a fact was frequent enough, this would mean that for very low levels of noise, considerable parts of the "meaning" could be preserved. We shall see that this ergodic property (i.e. this relative independence for long sequences of the scansion of the end from that of the beginning) is the rule rather than the exception.

More specifically, for neat codes whose words have all a bounded lenght an apart from three exceptional families there is at least one finite sequence of words - say μ_∞ such that whatever be the initial sequence α, $\alpha\mu_\infty/$ is a complete message. This implies that, when decoding, any blurring or error in α is "absorbed" by μ_∞ and that from the end of μ_∞ on, the scansion starts all right afresh.

Now if the words are given randomly and independently with fixed probabilities, it is clear that the probability for a given sequence not to contain μ_∞ tends with its length exponentially to zero so that any initial error is most likely to have only limited effects.

5. Syntactic equivalence and the fondamental semi groups.

Suppose we be given in code $\mathcal{C}_2$ the following fragment μ from a message :

$$\mu = \ldots + - - + - - + - + - - \ldots$$

By trial and error we see that only three scansions can possibly be fitted to it :

1) $\ldots/+/--/+/--/+/-+-/- \ldots$

2) $\ldots +/-/+/--/+/-+-/- \ldots$

3) $\ldots +-/-+-/-+-/+/--/ \ldots$

In the same manner the fragment

$$\mu' = \ldots + - + - + - \ldots$$

would give alternatives :

1) $\ldots/+/-+-/+/- \ldots$

2) $\ldots +/-+-/+/- \ldots$

3) $\ldots +-/+/-+-/ \ldots$

Disregarding the "meaning" of μ and μ' (i.e. their eventual decoding into the $\mathcal{A}$ language) we may observe that "functionally", so to say, μ and μ' are quite similar :

If the complete message is $/\mu_1 \mu \mu_2/$, the only possibilities are for each of the three scansions :

1) μ_1 is a complete message and μ_2 starts with $-/\ldots$ or $++/\ldots$ or $+-/\ldots$ (so as to make use of the $/- \ldots$ left at the end of μ).

2) μ_1 is ending by $\ldots/-+$ (so as to use $\ldots+/$) and μ_2 starts as above.

3) μ_1 ends with $\ldots/-$ (for the sake of $\ldots+-/$) and μ_2 is a complete message.

Easy check shows that the same applies exactly to μ' and we shall say that μ and μ' are syntactically equivalent (*) ($\mu \equiv \mu'$). Actually both are equivalent to an even simpler fragment :

$$\mu'' = \ldots + - \ldots$$

since this last one admits the same scansions :

1) $\ldots/+/-\ldots$; 2) $\ldots +/- \ldots$; 3) $\ldots +-/\ldots$

(*) It is interesting to observe that syntactic equivalence has a direct application to normal linguistics:

If $\mathcal{M}'$ is the set of all sentences grammatically correct :

$\mu_1 \equiv \mu_2$ (approximatively !) if and only if μ_1 and μ_2 pertain to the same grammatical category (for instance in English : both adjectives, or both "verbs at the third person of the present" etc.)

Now the key point is that for any four finite fragments, μ_1 , μ_2 , μ_3 and μ_4

$\mu_1 \equiv \mu_2$ and $\mu_3 \equiv \mu_4$ implies $\mu_1\mu_3 \equiv \mu_2\mu_4$.

The syntactic equivalence is thus fully compatible with the semi group structure of M and if we consider classes for $\equiv$ (i.e. the subsets of elements from M which are syntactically equivalent between themselves), these classes make a new semi group $\overline{M}$ which is an homomorphic image of M .

$\overline{M} \supset \overline{M}_o$, the fondamental semi group of the coding (f.s.g.) is most usually finite and is easily represented by matrices, but before we explain how, we need still a new concept : that of prefix :

Consider again two fragments μ and μ' but assume, now, that both are beginning at a / mark:

Even if μ and μ' are not syntactically equivalent, it could happen that under this supplementary restriction any further fragment which completes μ into a full message would do the same to μ' :

One could say that " μ and μ' as beginning of messages are syntactically equivalent on the right" (in symbols : $\mu \sim \mu'$)

For example :

$\mu = /---\cdots$ and $\mu' = /+-\cdots$ are not in the relation $\equiv$ (since $/-+\mu'' =$ is a complete message although $/-+\mu' = /++/-\cdots$ is not complete), but $\mu \sim \mu'$ all the same for $\mu\mu''$ is a complete message if and only if

$\mu'' = -/\cdots$ or $++/\cdots$ or $+-/\cdots$

just as well as for μ' .

We call prefixes the classes π_i of fragments for this new relation $\sim$.

For the code $\mathcal{C}_2$, there are three prefixes :

$\pi_1 \ni |\emptyset|$ (words and words only are bringing a $\mu \in \pi_1$ into a complete message.

π_1 contains all the words and its existence is typical of unitary coding).

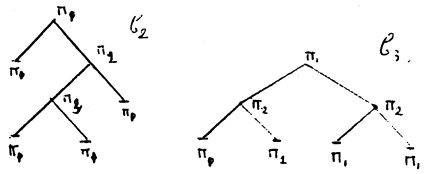
$\pi_2 \ni /-\cdots$ (the corresponding right divisors are $-/\cdots$, $++/\cdots$ and $+-/\cdots$)

$\pi_3 \ni /-+\cdots$ (the corresponding right divisor are $+/\cdots$ or $-/\cdots$).

Now if $\mu_1 \sim \mu_2$, one proves that

$\mu_1\mu_3 \sim \mu_2\mu_3$, too, whatever be μ_3

With unitary codes prefixes correspond to nodes of the tree in a one to many fashion : Two nodes being in relation $\sim$ ("pertain to the same prefix") if the subtrees below them are identical. Such things does not occur in our $\mathcal{C}_2$ code (see below), but are quite typical of uniform codes.



In the code $\mathcal{C}_3$ of length 2 ($\mu_1 = ++$; $\mu_2 = +-$; $\mu_3 = -+$; $\mu_4 = --$) there is only two prefixes : one, π_1 , corresponding to complete messages - i.e. to sequences with an even number of letters - and another one, π_2 , corresponding to odd length sequences.

6. Matrix representation of the fundamental semi group.

If we have started reading just at the beginning of the transmission, we may consider at any time t the prefix $\pi(t)$ to which pertain the initial fragment till the t-th letter as a "state" which changes at any new letter received.

For instance - apart from any meaning again - the sequence $|+--+--\cdots$ corresponds to the following sequence of prefixes :

$\pi_1, \pi_1, \pi_2, \pi_1, \pi_2, \pi_3, \pi_1, \pi_1, \pi_2 \cdots$

It is easy to visualise " + " and " - " respectively as the transition matrices :

	π_1	π_2	π_3
π_1	1	0	0
π_2	0	0	1
π_3	1	0	0

(+)

	π_1	π_2	π_3
π_1	0	1	0
π_2	1	0	0
π_3	1	0	0

(-)

(+ lets π_1 invariant since it is a word. It sends π_2 into π_3 and makes a word from π_3 etc..)

These matrices correspond in a one to one fashion to the elements of the fondament semi group, for instance:

1	0	0
1	0	0
1	0	0

(+ +)

0	0	1
1	0	0
1	0	0

(- +)

(with the usual line by column multiplication) is the matrice given below. What are the matrices corresponding to complete messages ? In the general case they are the matrices of the subsemigroups $\overline{M}'_d$ image of M' by the syntactic homomorphism .

But if the code is unitary, $\overline{M}'$ is characterised very nicely, since $\mu \in M'$ implies that μ sends π_d into itself : $\overline{M}'$ is just the set of the matrices of with 1 in the top left corner.

Further, noise absorption - or ergodic - properties reflect themselves quite directly on this matrix representation.

Suppose that the correct message $/\mu \ldots$ and the perturbated message $/\mu' \ldots$ fall back both at this very time on a common scansion mark $/$. If the prefix corresponding to μ was π and that corresponding to μ' was π', this would mean that the next signals sends both π and π' into $\cdot\pi_1$.

On the matrices this is expressed by the fact that in column π_1 there is two 1's : one in the line π and another one in line π'. In particular μ_∞ is a matrix with 1 everywhere in column π_1 . But this in turn is linked closely with the fact that $\overline{M}$ is a semi group and not a group (whose matrices should all have a single 1 by column).

Consider as a counter example the uniform code with four words :

Its f.s.g. is just the cyclic group of order two, made up of the two elements :

	π_1	π_2
π_1	0	1
π_2	1	0

	π_1	π_2
π_1	1	0
π_2	0	1

(+ or − or any odd length sequence)

(ϕ or ++ or +− or − + or ... etc. or any even length sequence).

No real absorption takes place for indeed if we had missed the first letter of the transmission and started wrongly scanding from the second letter, the error will obvious go on as long as does the message.

As a matter of fact uniform codes are the only neat codes with a bounded length for words whose f.s.g. is a group. They are the first exceptional non ergodic family.

7. Super coding.

We have given a very general definition of "translation" which suggests the possibility of more complex processes involving not only two but several languages. In the general case, things are a bit confused and we shall restrict ourself to Unitary Neat Coding from K into Λ and from Λ into M .

Suppose for instance that we have the following set up :

K is a d.s.g.l. with words k_i $(1 \leq i \leq 7)$

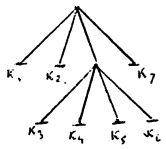
Λ is a d.s.g.l. with words λ_i $(1 \leq i \leq 4)$

M is our familiar binary d.s.g.l.

Each word of Λ is coded in M as in example 2:
$\lambda_1 \to +\,;\ \lambda_2 \to -++\,;\ \lambda_3 = -+-\,;\ \lambda_4 = ---$.

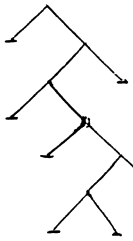
Each word of K is coded by the following sequences $\lambda^{(j)}$ of Λ (for clarity we use upper and lower indices) : $k_1 \to \lambda^1 = \lambda_1\,;\ k_2 \to \lambda^2 = \lambda_2\,;\ k_3 \to \lambda^3 = \lambda_3\lambda_1$
$k_4 \to \lambda^4 = \lambda_3\lambda_2\,;\ k_5 \to \lambda^5 = \lambda_3\lambda_3\,;\ k_6 \to \lambda^6 = \lambda_3\lambda_4\,;\ k_7 \to \lambda^7 = \lambda_4$.

This coding is unitary and neat all right and corresponds to the tree :



Now there is again a coding of K into M when every λ^j is written in binary alphabet :
$k_1 \to +\,;\ k_2 \to -+-\,.\ k_3 \to -+-+\,;\ k_4 \to -+--++\,;$
$k_5 \to -+--+-\,;\ k_6 \to -+---\,,\ k_7 \to -+---$.

It is not difficult to see that this $K \to M$ coding is unitary and neat. Its tree is given below.



Since we know the importance of fundamental semi groups we would be interested to get at once that ($\overline{M}$) of the $K \to M$ process from the other two ($\overline{\Lambda}$ for $K \to \Lambda$ and M for $\Lambda \to M$) or, alternatively, to know the relation between the syntactic equivalences on the bottom structure M . $\equiv(\Lambda$ in respect of $\Lambda \to M$, without K appearing in the picture and $\equiv(K)$ in respect of $K \to M$ with Λ put off from the circuit.

The main result is that :

$\mu_1 \not\equiv \mu_2\ (\Lambda)$ entails $\mu_1 \not\equiv \mu_2\ (M)$

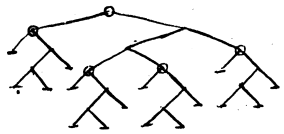
or, if one prefers, that $\overline{M}$ is a homomorphic image of $\overline{\overline{M}}$.

This is rather convenient from a technical point of view for it allows what is called a

filtering. If starting from the assumption that the λ_i are provided independently with fixed probabilities by the source, we discover later on that, actually, they were just building blocks in some higher degree semantic units (sent again independently of each other as a second approximation) we can preserve at least some of the features of our initial approximation.

But the main point for us here lies in another aspect.

Suppose that the $K \to \Lambda$ coding be uniform. in general the $K \to M$ one will not be so, but it will fail to be ergodic just the same, giving us the second of the three exceptional families mentionned above. We shall call such codes "uniformly composed codes". An example is given below :



$\mathcal{C}_2 \otimes \mathcal{C}_2$

$K \to M$

$K \to \Lambda$: uniform of length two

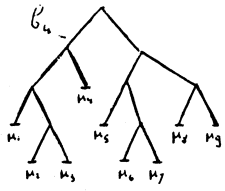
$\Lambda \to M$: our usual $\mathcal{C}_2$

The nodes indicated with a o are the ones corresponding to nodes in the $K \to \Lambda$ coding.

8. Anagrammatic codes.

Let us come now into the last family. For this we produce the following horrible example : $\mathcal{C}_4$

$\mu_1 = +++;\ \mu_2 = ++-;\ \mu_3 = +--;\ \mu_4 = +-.$
$\mu_5 = -++,\ \mu_6 = -+-+;\ \mu_7 = -+--,\ \mu_8 = --+,\ \mu_9 = ---.$



$\mathcal{C}_4$ is not uniform - nor composed uniformily of a smaller code. But it has the property that by inverting its words we found again a unitary code and, indeed, its symmetric image (symmetric in respect of the N.S. line !)

Since ergodicity is somewhat synonimous of irreversibility of time, we are put on the alert by this oddity.

Indeed, absorption is linked very closely with the problem of reading "backward" messages with an inverted code, but, without entering this amusing theory, we can see at once that $\mathcal{C}_4$ and all its family are not ergodic.

If a code is unitary the only sequence which let π_1 invariant are the complere messages, whose set is M'. In symbols, this means :

$\mu_1 \mu_2 \in M'$ and $\mu_1 \in M'$ implies $\mu_2 \in M'$

Suppose now that the same property be true on the other direction, i.e. that we had :

$\mu_1 \mu_2 \in M'$ and $\mu_2 \in M'$ implies $\mu_1 \in M'$

Let μ_1 be a complete message which is the unperturbated beginning of the transmission; μ'_1 , its noise corrupted form and μ_2 any other complete message. By the above condition $\mu'_1 \mu_2$ may have a final scansion like that of $\mu_1 \mu_2$ if and only if μ'_1 is a complete message, too.

As this is usually not the case the error will go on till the end.

Codes which are unitary for both directions of time (anagrammatic codes) are not yet fully explored but a construction for various infinite families of them is known. With binary alphabet, there is just the one given above and its symmetric for less than 16 words. It is conjectured that there is still no more than 38 other one below 32 words (on about 10^{16} distinct usual unitary neat codes of this size or less!).

So the family is really exceptionally interesting and deserves further studies since with the uniform and the uniformily composed codes, anagrammatic codes are the only length-bounded codes escaping ergodicity.

References.

1. A.Sardinas and Patterson (1953) Convention records of the I.R.E.
2. B.Mandelbrot .
   1953. Proc.Symp.Comm.Theory. London.
   1954. Proc. Symp. Inf. Network.
   1955. Proc. Symp. Comm. Theory . London.
3. P. Dubreil.
   1941. Mem. Acad. Sci. p. 1-52.
   1951. Rendiconti di Math. 81 p. 289 - 306.
   1953. Bull. Soc. Math. (10) p. 183 - 200.
4. P.Elias.
   1955. Proc. Symp. Comm. Theory. London.
5. A.E.Laemmel.
   1953. ibid.

A Reprint from

INFORMATION THEORY

THIRD LONDON SYMPOSIUM

Papers read at a Symposium on 'Information Theory'
held at the Royal Institution, London,
September 12th to 16th 1955

Edited by
COLIN CHERRY

Published by
BUTTERWORTHS SCIENTIFIC PUBLICATIONS
88 KINGSWAY, LONDON, W.C.2

3

ON SOME MEASURES OF INFORMATION USED IN STATISTICS

M. P. Schützenberger
Paris

As is well known, the concepts of information with which statistics and communication theory deal are different, both in their formal expression and in their content. In statistics, when the problem is to estimate the value of an unknown parameter θ through the observation of the state ξ of a physical system, the *a priori* probability $P(\xi \mid \theta)$ depending upon θ, one is led to introduce the expression

$$F = \sum \left(\frac{\partial}{\partial \theta} P(x \mid \theta) \right)^2 \frac{1}{P(x \mid \theta)}$$

with the summation running over all the possible states x of ξ. A whole family of theorems[2, 4, 6] relates F, under appropriate regularity conditions, to a lower bound of the variance of the difference $\theta - \hat{\theta}$ between the true value of θ and its estimated value $\hat{\theta}$.

On the other hand, in communication theory, one is accustomed to evaluate the amount of information on ξ itself by:

$$H = -\sum P(\xi) \log P(\xi)$$

It is remarkable that so much interest has been devoted to this last quantity rather than to the older expression F, which was defined by Sir Ronald Fisher[3] as early as in 1921 and which has been very cursorily dealt with by communication specialists.

Moreover, F and H are not the only measures of the information relative to 'something' contained in an experiment involving *a priori* probability. In the second main problem of statistics—that of deciding on the basis of observation of ξ which of the hypotheses $\theta = \theta_0$ or $\theta = \theta_1$ is true—the following expression

$$W_i = \sum P(x \mid \theta_i) \log \frac{P(x \mid \theta_i)}{P(x \mid \theta_j)} \qquad (i = 0, 1, j = 0, 1, j \neq i)$$

enters in a natural way. Wald[9] has shown that whatever be the procedure used (sequential or not) for the test, the expectation of the number of independent trials needed to reach a given level of security could not be smaller than K/W, where K depends on the probability of error which defines the level of security. In consequence, W could be termed the measure of the information relative to the dilemma $\theta = \theta_0$ or θ_1 afforded by ξ. Indeed, quite close connexions do exist between F, H and W.

M. P. SCHÜTZENBERGER

After BARTLETT[1], let us consider the modified form

$$H^{\star} = -\Sigma\, P(x \mid \theta) \log P(x \mid \theta + \varepsilon)$$

and suppose that $\log P(x \mid \theta + \varepsilon)$ may be developed into a series in ascending powers of ε. Then, after some simplification

$$H^{\star} = H + \varepsilon^2 F + \text{terms of higher order in } \varepsilon$$

On the same line of reasoning, if $\theta_0 = \theta_2 + \varepsilon$ and $\theta_1 = \theta_2 - \varepsilon$, where ε is infinitely small, it may be shown that the random variate

$$z(x) = \log \frac{P(x \mid \theta_0)}{P(x \mid \theta_1)}$$

(the expectation of which is W_0, when $\theta = \theta_0$) is distributed with mean $2\varepsilon^2 F$ and variance $4\varepsilon^2 F$, to terms of higher order in ε. More general relations between F and W have been recently studied by KULLBACK[5].

The aim of this present communication (also of reference 8) is to show that these analogies are deeply rooted in the very nature of what we are ready to call a 'measure of information'. As a matter of fact, the leading principle of the axiomatization we shall attempt is more or less a sophistication of WOODWARD's[10] approach to the same problem: that when performing the complete determination of ξ, one may stop at an intermediate level and obtain the total information by adding together: (a) a term corresponding to the information up to this point; (b) a term corresponding to the information from this point on, weighted with the adequate conditional probabilities.

We shall however restrict the postulation of this 'Huygens principle' to those intermediate observations only, which exclude definitely some contingencies, instead of requiring it for all of them, as is the case with Woodward's axiomatic approach which turns out to be unnecessarily exacting. With this weaker form, a purely algebraic treatment is possible giving, besides the 'conventional' H, the expressions F and W, as special cases of the complete solution, which can be explicitly given under some regularity conditions.

For the sake of simplicity, the argument will be split into two parts: the first (Condition I and Theorem I) could be extended to cases other than information, and entails the abstract equivalent of a principle of separation of variates. The second (Condition II and Theorem II) determines the specific character of the information *i.e.* introduces the 'log P' function.

The regularity Conditions III and IV could be presumably weakened by introducing another postulate which is satisfied by H, F and W: the condition that the information be non-negative. Further research would be needed along this line, which we shall only mention here together with the not too difficult possibility of extending Theorem I to non-finite cases, under proper restrictions. A more general theory (using *modular* instead of *distributive* lattices and *idempotent linear operator* instead of *equivalence relations*) may be developed and gives an axiomatic definition of the variance (as corresponding to H and *not* to F) and of the so-called 'chi-square' measure of discrepancy (as corresponding to W) [see reference 11].

First of all, let us make it clear that we are not looking for a measure of the information provided by one given result of the observations, but for a

measure of what amount may be obtained on the average with the help of a given observational set-up. For representing the general situation, we shall consider a physical system whose state ξ is still unknown. For the sake of simplicity it will be supposed, throughout the paper, that ξ can take on only one of a finite set E of values $x, y, z \ldots$. In practice, even if ξ were a continuous variate, this quantification could always be assumed, since any real measurement may be done with a finite precision only.

The *a priori* probabilities with which ξ may be any of the states $x, y \ldots$ will be written $P(x), P(y) \ldots$ and we shall suppose that they are functions of some unknown parameter(s) symbolized by θ. With respect to the physical system, an observer Ω_i is characterized by the degree of accuracy with which he is able to recognize ξ. For instance, if ξ is a numerical variate with possible values 0, 1, 2 or 3, an observer Ω_0 may be unable to know more about ξ than to ascertain whether it is zero or not; another one, Ω_2, whether it is odd or even *etc.* Accordingly, to each observed Ω_i corresponds an equivalence relation ρ_i between the possible states of ξ; that is to say, a partition of E into disjoint subsets $(X), (Y) \ldots (Z)$, Ω_i being unable to 'separate' two states when they pertain to the same 'class of equivalence' of ρ_i.

Between equivalence relations on E exists the usual partial ordering relation $\rho' < \rho$ (ρ' is finer than ρ: every class of ρ' is contained in a class of ρ), which means that the observer Ω' is able to perform every distinction between states which Ω can do. Further, if $\rho' < \rho$, and if X is a class of ρ, we shall denote by $\rho'[X]$ (the '*restriction* of ρ' to X') the equivalence relation induced by ρ' on the subset X of E. If, for some subset X, $\rho'[X] = \rho''[X]$ we shall write: $\rho' \equiv \rho[X]$ ('ρ and ρ' are identical on X').

With these notions at hand we may now compare observers, or rather pairs of observers.

Definition: The two pairs of equivalence relations (ρ_i, ρ_j) and (ρ_k, ρ_e), where $\rho_i < \rho_j$ and $\rho_k < \rho_e$, will be said to be in the relation $\sim$ if, and only if, there exists a partition of E into disjoint subsets E' and E'' such that

$$\rho_i \equiv \rho_k[E']; \quad \rho_j \equiv \rho_e[E']; \quad \rho_i \equiv \rho_j[E'']; \quad \rho_k \equiv \rho_e[E'']$$

For instance, let $E = \{a, b, c, d, e, f, g\}$ and:

$$\rho_i = (abc)(d)(e)(fg); \quad \rho_j = (abc)(d)(efg); \quad \rho_k = (ab)(cd)(e)(fg);$$
$$\rho_e = (ab)(cd)(efg)$$

One sees that $(\rho_i, \rho_j) \sim (\rho_k, \rho_e)$, by taking $E' = (efg)$ and $E'' = (abcd)$, for then:

$$\rho_i[E'] = \rho_k[E'] = (e)(fg); \qquad \rho_j[E'] = \rho_e[E'] = (efg)$$
$$\rho_i = [E''] = \rho_j[E''] = (abc)(d); \quad \rho_k[E''] = \rho_e[E''] = (ab)(cd)$$

It is readily demonstrated that $\sim$ is again an equivalence relation on the set of all ordered pairs of equivalence relations. For that it is enough to remark that from ρ_i and ρ_j (with $\rho_i < \rho_j$) E'' is unequivocally determined as the union of those classes which are in the same time classes of ρ_i and of ρ_j. [Parenthetically, let us observe that if, in addition, $\rho_j < \rho_e$ one has too, $\rho_i < \rho_k$ and $(\rho_i, \rho_k) \sim (\rho_j, \rho_e)$ so that the $\sim$ relation looks quite like an abstract version of the equality relation between two fractions.]

M. P. SCHÜTZENBERGER

Consider now, for a given finite E, the set R of all the equivalence relations on E, and a function $f(\ )$ of R in to some additive group **a**.

Definition: The function $f(\ )$ will be called a valuation on R if for every quadruple of relations $(\rho_i, \rho_j) \sim (\rho_k, \rho_e)$ entails $f(\rho_i) - f(\rho_j) = f(\rho_k) - f(\rho_e)$.

Theorem I: Any valuation $f(\ )$ of the set of all equivalence relations on the finite E may be written in the form $f(\rho) = \Sigma g(X)$ where the summation extends to all classes X of ρ.

Proof: Consider for any equivalence relation into k classes $\rho = (X)(Y) \ldots (T)$ the three other relations: ρ_X, the finest among the equivalence relations admitting the class (X), $\rho_{\bar{X}}$ the finest among all equivalence relations admitting the class $(Y), (Z) \ldots (T)$, and ρ_0 the finest among all the equivalence relations; one has

$$(\rho_0, \rho_X) \sim (\rho_{\bar{X}}, \rho) \textit{ i.e. if } f(\ ) \text{ is a valuation: } f(\rho) = f(\rho_X) + f(\rho_{\bar{X}}) - f(\rho_0)$$

Thus if the theorem is proved for all the equivalence relations with no more than $k-1$ classes, it is proved for the relations with k classes, since

$$f(\rho) = \{\sum_{x \epsilon X} g(x)\} + \{g(x) + \sum_{y \epsilon E - X} g(g)\} - \{\sum_{x \epsilon E} g(x)\}$$

Now, choose for any elements of E, an arbitrary value of $g(x)$ with the sole condition that $\sum_{x \epsilon E} g(x) = f(\rho_0)$. For any X we define $g(X) = f(\rho_X) - \sum_{x \epsilon X} f(x) - f(\rho_0)$ which achieves the proof.

Remark: Suppose now that we discover that ρ_0 was *not* really the finest equivalence relation, but that there exists a still finer one, ρ'_0 differing from it only by the fact that in ρ'_0 the class (X) is split into (X') and (X''). Every equivalence relation ρ'_i, less fine than ρ_0 either is $> \rho_0$ or is of the form $(X'), (X''), (U), (V) \ldots (W)$—*i.e.* is identical on $E - X$ to some $\rho_i > \rho_0$.

Thus in this case $(\rho'_0, \rho'_i) \sim (\rho_0, \rho_i)$

and $$f(\rho'_i) = f(\rho_i) + f(\rho'_0) - f(\rho_0)$$

and $f(\rho')$ will be of the form needed if, having chosen arbitrarily $g(X')$, we take $g(X'') = g(X) - g(X') + f(\rho'_0) - f(\rho_0)$.

Suppose now that $\rho' < \rho$ entails $f(\rho) \leqslant f(\rho') \leqslant f < \infty$ and that we find some finite ρ_0 such that $f - f(\rho_0) \leqslant \varepsilon$ and for all classes Y of $\rho_0 = 0 < |g(Y)| < \eta$. Then the same condition may be made to hold for ρ'_0; for instance by taking

$$0 < g(X'') = g(X') = \tfrac{1}{2}\{f(\rho'_0) - f(\rho_0) + g(X)\} < \varepsilon + \eta/2$$

This remark would lead to the possibility of extending Theorem I to general E, under a proper definition of what is meant by an equivalence relation with infinitely many classes and corresponding restrictions on f.

Reverting to our main purpose—which is to measure information—we shall postulate that:

Condition I: The measure of the information $H(\rho_i)$ attached to the observer is a valuation on the set (lattice) R of all equivalence relation on E.

What this means exactly seems a fair enough requirement. If Ω_i differs from Ω_j by the same ability in finer distinctions as Ω_k does from Ω_e, we ask that the differences $H(\rho_i) - H(\rho_j)$ and $H(\rho_k) - H(\rho_e)$ be equal.

If one prefers, this condition may be interpreted in an equivalent way by assimilating H to a cost of equipment, and requiring that the expenses, involved in the addition of a special gadget, intended to perform some finer analysis, be independent from the total cost of the other parts of the observational machinery.

From *Theorem I*, we know only that if the number of states is finite, this implies that $H(\rho)$ be a sum of terms depending only on the classes of ρ. Of course, so broad a definition is not enough to determine H in a really interesting way, and we shall further postulate:

Condition II: If $\rho < \rho'$ in such a way that for a class U of ρ', $\rho \equiv \rho'[E-U]$ (*i.e.* if Ω differs from Ω' only by a further splitting of one of the classes), then

$$H(\rho) = H(\rho') + P(U)H(\rho'')$$

where $H(\rho'')$ is the measure of information attached to $\rho'' = \rho[U]$ for an observer knowing that the state ξ pertains to the subset U. To this condition we add:

Condition III: The probabilities $P(X) = x \neq 0$ are elements of some topological communitative ring* $\mathbf{a}$ and $H(\rho)$ a continuous functional in the $x, y \ldots$.

Condition IV: $\mathbf{a}$ is such, that if for all $a, b \in \mathbf{a}$, $a + b = 1$, $ab \neq 0$, h_i is a continuous functional satisfying

(1) $h_1(a + b) = h_1(a) + h_1(b)$ then $h_1(x) = \Delta(x)$

(2) $h_2(ab) = h_2(a) + h_2(b)$ then $h_2(x) = \Delta \log x$

where Δ is a semi-linear functional and log is some fixed function within the ring of functions of $\mathbf{a}$.

Theorem II: Under IV, the necessary and sufficient condition for $H(\rho)$ to satisfy I, II, III, is that it has the form:

$$H(\rho) = \sum_x x \, \Delta \log x$$

where the summation runs over classes X of ρ, and Δ is any continuous semi-linear functional.

Proof: The sufficiency is a matter of straightforward verification. As to the necessity, Condition I implies that:

$$H(\rho) = \Sigma g'(x) = \Sigma\, x \,.\, g(x) \text{ for some } g(X) = g'(x)/x.$$

Consider an equivalence relation with four classes: $\rho = (X)(Y)(Z)(T)$. Condition II with $U = Y + Z + T$ implies:

$$\begin{aligned} H(\rho) &= xg(x) + yg(y) + zg(z) + tg(t) \\ &= xg(x) + (y + z + t)g(y + g + t) \\ &\quad + (y + z + t)\left\{\frac{y}{y + z + t}\, g\left(\frac{y}{y + z + t}\right)\right. \\ &\quad \left. + \frac{z}{y + z + t}\, g\left(\frac{z}{y + z + t}\right) + \frac{t}{y + z + t}\, g\left(\frac{t}{y + z + t}\right)\right\} \end{aligned}$$

* *i.e.* very roughly speaking, a set in which abstract operations $+$ and $\times$ are defined, so as to satisfy the usual conditions except that it may happen that $ab = 0$ even when $a \neq 0$ and $b \neq 0$.

Let us transform this by writing: $1 - x = y + z + t$; $y' = y(1 - x)^{-1}$; $z' = z(1 - x)^{-1}$; $t' = t(1 - x)^{-1}$ and $k(a; b) = g(ab) - g(a) - g(b)$. Then after regrouping the terms we get

$$yk(y'; 1 - x) + zk(z'; 1 - x) + tk(t'; 1 - x) = 0$$

in particular, if t were zero, x and y keeping the same values, one would have

$$yk(y'; 1 - x) + (z + t)k(z' + t'; 1 - x) = 0$$

Then, by subtraction of the last two equations, one obtains:

$$(z' + t')k(z' + t'; 1 - x) = z'k(z'; 1 - x) + t'k(t'; 1 - x)$$

Hence after IV (1), since $ak(a; b)$ is additive in its first argument: $ak(a; b) = \Delta(a)$ where Δ may depend on b, but not on a. But $k(a, b)$ is symmetrical in a and b; this, in turn, implies that $k(a; b) = 1/ab\ \Delta'(ab)$ and the above equation gives $\Delta'(y'(1 - x)) + \Delta'((z' + t')(1 - x)) = \Delta'(y) + \Delta'(z + t) = 0$ where y and $z + t$ are restricted only by $y + z + t \leqslant 1$. Since Δ' is additive, this means that $\Delta'(u) = 0$ for all $u (0 < u < 1)$ so that one has $h(a; b) = g(ab) - g(a) - g(b) = 0$ for all $a, b \in \mathfrak{a}$; $a + b < 1$; $ab \neq 0$. Now, by Condition IV (2) this gives $g(a) = \Delta \log a$ which achieves the proof of the theorem.

Remark (1): The two successive steps *I* and *II* involved in the above axiomatic could be replaced by the single postulate *I'* (under Conditions III and IV and finite *E*).

I': For all $\rho = (X)(Y)(Z)$; $\rho_1' = (X)(Y + Z)$; $\rho_1'' = \rho\,[E - X] = (Y)(Z)$ $\rho_2' = (X + Y)(Z)$; $\rho_2'' = (X)(Y)$ one has:

$$H(\rho_1') + P(X)H(\rho_1'') = H(\rho_2') + P(Z)H(\rho_2'')$$

Indeed, it can be shown by recurrence that *I'* implies *I*. This formulation which does not require the concept of valuation may be interpreted as a principle of 'virtual decomposition of the observations into successive dichotomies', since it requires that the information attached to the distinction of ξ between X, Y, Z may be computed on the sole basis of the information attached to the dichotomies ρ' and ρ''.

Remark (2): When one confines oneself to information depending only on the numerical values of the $P(X)$, as is the case in communication theory, the Condition II may be replaced by additivity for the composition of independent variates (Woodward). Then, if a valuation is continuous and depends only on the $P(X)$, a necessary and sufficient condition for it to be additive *for the composition of independent variates is that it should have the form*: $\Sigma x \log x$.

Proof: Let η and ζ be two independent variates, taking respectively the states $Y_1 Y_2 Y_3$ and $Z_1 Z_2 Z_3$. Let $\xi = \eta \times \zeta$ be their abstract product, taking the 3×3 states X_{ij} $(i, j = 1, 2, 3)$. Let η^{α} (respectively $\zeta^{\star}$) be the variates obtained from η (respectively ζ) by confounding the states numbered 2 and 3. Since H is assumed to be a valuation, the information $H(\eta \times \zeta)$ on ξ is a sum: $H(\eta \times \zeta) = \sum_{ij} x_{ij} g(x_{ij})$ which by hypothesis is equal to

$$H(y) + H(\zeta) = \sum_i y_i g(y_i) + \sum_j z_j g(z_j)$$

DISCUSSION

One has

$$\begin{aligned} D &= H(\eta \times \zeta) - H(\eta \times \zeta^\star) - H(\eta^\star \times \zeta) + H(\eta^\star \times \zeta^\star) \\ &= (H(\eta) + H(\zeta)) - (H(\eta) + H(\zeta^\star)) - (H(\eta^\star) + H(\zeta)) \\ &\quad + (H(\eta^\star) + H(\zeta^\star)) \\ &= 0 \text{ identically} \end{aligned}$$

and, on the other hand, supposing that $z_2 = z_3 = z$ and writing $g(ab) - g(2ab) = k(a, b)$:

$$D = y_2 k(y_2, z) + y_3 k(y_3, z) - (y_2 + y_3) k(y_2 + y_3;\ z) = 0$$

which implies, since continuity is postulated, that $k(y_i, z)$ be independent from y_i.

But $k(y_i, z)$, again, is symmetrical in y_i and z, so that it is a constant K, and we obtain finally, letting $u = y_i, z$

$$g(u) - g(2u) = K \quad \text{for all} \quad 0 \leqslant u \leqslant 1$$

The theorem follows, since this is Schröder's equation, which is known[7] to have as its only solutions $g(u) = K \log u$. Observe that the proof would have failed if we had not assumed that g and k are numerical functions, for we could not have proved that $k(a, b)$ is a constant. Indeed, in the more general case, not only information, but the results of applying any linear operation to them (*i.e.* expressions of the form $\Sigma\, \Delta_1 P(X) \Delta_2 \log P(X)$) satisfy the requirements of additivity for the composition of independent variates.

REFERENCES

[1] Bartlett, M. S. In *Proc. London Symp. Information Theory*, p. 81, London; Ministry of Supply, 1950

[2] Darmois, G. *Rev. Inst. Int. Stat.* (1945) 132

[3] Fisher, R. A. *Phil. Trans. R. Soc.*, A. 22 (1921) 309

[4] Frechet, M. *Rev. Inst. Int. Stat.*, 3/4 (1942) 182

[5] Kullback, S. *Ann. Math. Stat.*, 2 (1954) 745

[6] Rao, G. Q. *Bull. Calcutta Math. Soc.*, 37 (1945) 81

[7] Schröder, K. *Math. Ann.*, 3 (1871) 296

[8] Schützenberger, M. P. *Pub. Inst. Stat. Univ. Paris*, 3 (1953) 27

[9] Wald, A. *Sequential Analysis*, N.Y.; J. Wiley and Son, 1947

[10] Woodward, P. M. and Davies, I. L. *Proc. Institute of Electrical Engineers*, III, 99 (1952) 37

[11] For further details, see the forthcoming book *Decision et Informations* by B. Mandelbrot and M. P. Schützenberger.

DISCUSSION

J. C. R. Licklider: As I understand it, Shannon's measure H, would be 'just another measure' if it did not lead to the Channel-Capacity Theorem. The fact that H leads to that remarkable insight gives H a definite status. In problems concerning coding of information for efficient transmission through restricted channels H is the natural measure.

If it is true that measures are noteworthy insofar as they lead to new orderings and relations of facts, then the question arises: do the other measures you have discussed lead to discoveries comparable with the Channel-Capacity Theorem?

DISCUSSION

R. Syski: The author has formulated his results in terms of lattice theory, and postulated that the amount of information $H(\rho)$ is the valuation on the modular lattice R of all equivalence relations on the set E.

I think that a formulation in terms of measure theory could be possible. In fact, some particular cases to which the author refers admit such a formulation. Shannon's entropy is defined as an integral of a certain measurable function, taken with respect to the probability measure, over the measure space with appropriate Borel field. Similarly, the concept of sufficient statistic was discussed by Halmos with the help of the Radon-Nikodym theorem (*Ann. Math. Stat.*, 20 (1949) 225.) Since the measure on sets is also the valuation on lattices (Boolean algebra), the author's approach and the measure theory approach are closely related. I should like to ask, therefore, what are the advantages in using lattice theory here?

Secondly, Dr. McMillan recently used metric informational lattices (*Bull. Amer. Math. Soc.*, 60 (1954) 558). Is his treatment related to that of the author's as far as the selective information is concerned?

M. P. Schützenberger in reply: I would answer Dr. Licklider: partly, yes. The Frechet-Darmois-Cramer- Rao and the Wald-Wolfowitz theorems are the counterpart of the Channel-Capacity Theorem; the first applies when the signal is of a continuous nature and the loss function is quadratic and provides a basis for Tuller's inequality; the second when a fixed signal has to be detected with as few elementary observations as possible. Both give an upper limit to the efficiency of a given transmission set-up. This may be shown under proper restrictions to be attained asymptotically when a long enough delay is allowed.

In reply to Mr. Syski, measure theory could be used as well. The point here is that the lattice under consideration is not Boolean nor modular so that the present approach (where the aim is quite different from McMillan's) seems to me to be more direct.

ALGÈBRE ET THÉORIE DES JEUX. — *Jeux de Nim et solutions.* Note (*) de MM. **Claude Berge** et **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

A l'aide d'une fonction de Grundy définie dans une Note antérieure (1) et pouvant avoir comme valeur un nombre ordinal transfini, on étudiera des propriétés d'un jeu de Nim généralisé dont on donnera des applications à la théorie des « solutions » au sens de Von Neumann et Morgenstern.

On appellera ici *jeu de Nim* tout jeu de mat alternatif à deux joueurs, compétitif, et symétrique par rapport aux deux joueurs (2). Une position de jeu sera le produit d'un élément x appelé *diagramme* et d'un indice i représentant le joueur ayant le trait au moment considéré. L'ensemble des positions pouvant succéder à une position $x.1$ sera désigné par $(\Gamma x).2$; il existera dans l'ensemble X des diagrammes deux ensembles K et L tels que

$$K \cap L = \emptyset, \qquad K \cup L = X_0 = \{x : \Gamma x = \emptyset\},$$
$$(K.1) \cup (L.2) = K_1; \qquad (L.1) \cup (K.2) = K_2.$$

(K_1 et K_2 désignent les *positions gagnées* pour les joueurs 1 et 2.)

Un tel jeu sera désigné par (Γ, K, L), et dans tout ce qui va suivre, on considérera un graphe orienté comme un jeu de Nim particulier du type $(\Gamma, \emptyset, X_0)$.

On dira qu'une fonction $g(x)$ sur X est une *fonction de Grundy* du jeu (Γ, K, L) si : $x \in L$ implique $g(x) = 0$; $x \in K$ implique $g(x) = 1$; $x \in CK \cap CL$ implique que $g(x)$ est le plus petit des nombres ordinaux ne figurant pas dans $\{g(y) : y \in \Gamma x\}$.

On voit, comme dans la Note précédente, que si le jeu (Γ, K, L) est localement fini, il existe une fonction de Grundy et une seule, que l'on déterminera par induction transfinie. Le théorème de Grundy se généralise :

Théorème I. — *Si, dans un jeu de Nim* (Γ, K, L), *il existe une fonction de Grundy* $g(x)$, *et si la position en cours est* $x.2$, *telle que* $g(x) = 0$, *le joueur* 1 *peut être sûr de gagner ou d'empêcher la partie de se terminer.*

En effet, le diagramme suivant y sera tel que $g(y) \neq 0$, et par conséquent, si $y \in K$, le joueur 1 aura gagné, et si $y \notin K$, le joueur 1 pourra choisir au coup suivant un diagramme z tel que $g(z) = 0$.

THÉORÈME II. — *Si un jeu* (Γ, K, L) *admet une fonction de Grundy* $g(x)$ *telle que* $\Gamma^+\{x/g(x) \neq 0,1\} = \emptyset$, *le jeu de qui-perd-gagne associé* (Γ, L, K) *admet une fonction de Grundy* $g'(x)$, *qui sera égale à zéro quand* $g(x) = 1$, *à* 1 *quand* $g(x) = 0$ *et à* $g(x)$ *quand* $g(x) \neq 0,1$.

1° Si $\Gamma x \neq \emptyset$ et si $\lambda < g'(x)$, il existe dans Γx un y tel que $g'(y) = \lambda$.
En effet si $g'(x) = 1$, on a $g(x) = 0$; donc, puisque :

$$\Gamma^+\{x; g(x) \neq 0,1\} \neq \emptyset,$$

on a un y dans Γx tel que $g(y) = 1$, c'est-à-dire $g'(y) = 0$; si, par ailleurs, $g'(x) > 1$, on a $g'(x) = g(x)$, et il existera encore un y tel que $g(y) = \lambda$.

2° Il n'existe pas dans Γx un y tel que $g'(y) = g'(x)$, car cela entraînerait $g(y) = g(x)$.
Enfin, on étendra le raisonnement de Grundy au cas cyclique pour démontrer :

THÉORÈME III. — *Si, pour des jeux* $(\Gamma^k, \emptyset, L^k)$, *il existe une fonction de Grundy, il existera également une fonction de Grundy pour le produit de composition d'ordre* 1, $(\Pi^{(1)}\Gamma^k, \emptyset, \Pi L^k)$, *où*

$$(\Pi^{(1)}\Gamma^k)x^1.x^2\ldots x^m = (\Gamma^1 x^1).x^2\ldots x^m \cup x^1.(\Gamma^2 x^2).x^3\ldots x^m \cup \ldots.$$

Cette fonction sera donnée par la règle « Nim-Sum » de Grundy.

Application. — Soit X l'ensemble des imputations d'un jeu à n personnes; si $x \in X$, on désignera par Γx l'ensemble des imputations qui peuvent dominer x. On posera $X_0 = \{x/\Gamma x = \emptyset\}$, et l'on considérera un sous-ensemble A de X_0.
Un ensemble S_A dans X sera par définition une *solution relativement* à A si l'on a

1° $x, y \in S_A$, entraîne $y \notin \Gamma x$;
2° $x \notin S_A$, $x \notin A$ entraîne l'existence d'un y dans S_A tel que $y \in \Gamma x$.

$S_\emptyset$ sera une *solution forte*, au sens de J. Von Neumann-O. Morgenstern [3]; S_{X_0} sera une *solution faible*, c'est-à-dire l'ensemble maximal de tous les éléments x qui dominent tout élément pouvant être dominé. On remarque que si le jeu de Nim $(\Gamma, A, X_0 - A)$ admet une fonction de Grundy $g(x)$, l'ensemble $\{x/g(x) = 0\} = S_A$ est une solution relativement à A.

CONSÉQUENCE 1. — *Si le graphe* (Γ, X) *est localement fini, à tout sous-ensemble* A *de* X_0 *correspondra une solution* S_A *et une seule.*

En effet, dans ce cas, il existe une fonction de Grundy et une seule pour le jeu $(\Gamma, A, X_0 - A)$. Dans le cas où $A = \emptyset$, on retrouve un résultat de Von Neumann-Morgenstern.

Conséquence 2. — *S'il existe une solution* S_A *engendrée par une fonction de Grundy* $g(x)$ *telle que* $\Gamma^{+}\{x/g(x) \neq 0, 1\} = \emptyset$, *il existe une solution* $S'_B = S'_{X_0 - A}$ *et l'on a* : $S_A \cap S'_B = \emptyset$. Cela se déduit du théorème II.

Il résulte en particulier que, dans ce cas, la solution forte et la solution faible sont des ensembles disjoints.

(*) Séance du 19 mars 1956.

(1) *Comptes rendus*, **242**, 1956, p. 1404.

(2) Pour la terminologie, *cf.* C. Berge, *J. Math. pures et appl.*, **32**, 1953, p. 129. Cette définition du jeu de Nim contient celle de E. H. Moore (*Ann. of Math.*, 1909) et celle de P. M. Grundy (*Eureka*, **2**, 1939).

(3) *Theory of Games and Economic behaviour*, Princeton, 1947, p. 587.

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*, t. **242**, p. 1672-1674, séance du 26 mars 1956).

GAUTHIER-VILLARS,
ÉDITEUR-IMPRIMEUR-LIBRAIRE DES COMPTES RENDUS DES SÉANCES DE L'ACADÉMIE DES SCIENCES
149793-56 Paris. — Quai des Grands-Augustins, 55.

SÉANCE DU 18 JUIN 1956. 2907

ALGÈBRE. — *Sur une représentation des demi-groupes.*

Note de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

On a défini antérieurement la notion de demi-groupe fondamental d'un processus régénératif ou d'un code (1). Le problème d'indécomposabilité ergodique pour ces structures revient à caractériser les demi-groupes A possédant un seul idéal à droite (2) dont le groupe Γ (défini plus bas) est réduit à son élément neutre ε. Sa solution repose sur une représentation nouvelle qui sera seule discutée ici.

Notations. — Soit A sans zéro satisfaisant à la condition minimale. Soient $C_i (i \in I)$ et $C^j (j \in J)$ respectivement ses idéaux minimaux à droite et à gauche. $C = \bigcup_{i \in I} C_i = \bigcup_{j \in J} C^j$. Si $C_i^j = C_i \cap C^j$ possède un élément unité e_i^j — ce que l'on supposera toujours — on sait (3) qu'il existe un groupe Γ, des constantes γ_j^i dans Γ et une application $a \to \bar{a}$ de C dans Γ tels que $ab = c$, $a \in C_i^j$ et $b \in C_k^l$ entraînent $\bar{a}\,\gamma_j^k\,\bar{b} = \bar{c}$. On peut supposer que $\gamma_1^i = \gamma_j^1 = \varepsilon$.

Définition. — On appellera « *ergodique à droite* » la représentation de tout $x \in A$ par une matrice carrée X à indices dans J et à éléments dans $\Gamma \cup o$ ($o\Gamma = \Gamma o = o$) dont l'élément $\xi_j^{j'}$ est égal à $\bar{u}$ si $e_1^j x = u \in C_1^{j'}$ et à o ailleurs. Si ρ_i est une équivalence régulière sur Γ on désignera par φ_i l'homorphisme de A associé à son « extension ergodique à droite », cette dernière étant définie par : $x \rho y$, si et seulement si $\xi_{j'}^j \rho \eta_{j'}^j$ pour tout $j, j' \in J$. En particulier φ désignera l'homomorphisme $x \to X$ et φ_0 l'homomorphisme associé à ρ_0, la plus fine des équivalences sur Γ telles que $\gamma_j^i \rho \gamma_{j'}^{i'}$ pour tout i, i', j.

Proposition 1. — *Une condition nécessaire et suffisante pour que $\varphi_i x \in \varphi_i C$ est qu'il existe deux indices j et k dans J et $\beta \in \Gamma$ tels que $\xi_{j''}^{j''} = \gamma_{j''}^k \beta$ si $j'' = j$ et $\xi_{j''}^{j''} = o$ si $j'' \neq j$.*

Il suffit de calculer la matrice Y d'un élément générique de C pour voir que la condition est nécessaire. Réciproquement, si $\xi_{j''}^{j''} = o$ pour tout $j'' \neq j$ ces relations doivent exister car $y = xe_1^j$ appartient à C et Y = X d'après les hypothèses faites sur les γ_j^i.

Proposition 2. — *ρ_0 est la plus fine des équivalences ergodiques telles que φA ne possède qu'un seul idéal minimum à droite.*

D'après les calculs précédents $e_i^1 \rho\, e_{i'}^1$ entraîne $\gamma_j^i \rho \gamma_{j'}^{i'}$ pour tout $j \in J$; d'autre part, pour tout i, si $j \neq j'$, $\varphi_0 e_i^j \neq \varphi_0 e_i^{j'}$.

Proposition 3. — *Soit une équivalence régulière à droite dont les classes $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\alpha, \ldots$ sont telles que $\emptyset \neq \mathfrak{C}_\alpha = C \cap \mathfrak{A}_\alpha \neq C \cap \mathfrak{A}_{\alpha'} = \mathfrak{C}_{\alpha'} \neq \emptyset$ pour tout $\alpha \neq \alpha'$. La représentation ergodique à droite est isomorphe à la représentation à droite de A sur les classes $\mathfrak{A}_\alpha$.*

X = Y est équivalent à $Cx = cy$ pour tout $c \in C$ puisque $c \in C_i^j$ entraîne

$ce_1^j = c$ et $ce_1^j x = cu$ avec $u \subset C^j$. D'autre part : $\mathfrak{C}_\alpha x \neq \emptyset$ pour tout α. Donc $\mathfrak{A}_\alpha x \cap \mathfrak{A}_\alpha y = \emptyset$ est équivalent à : $\mathfrak{C}_\alpha x \cap \mathfrak{C}_\alpha y = \emptyset$.

Soit en particulier la relation χ, fermeture de transitivité de χ_0 définie par $x \chi_0 y$, si et seulement si, pour quelques q, $q' \in Q \cup \emptyset$: $x = qt$; $y = q't$. Soit $\bar{\chi}$ la relation : pour tout $z \in A$, $zx \chi zy$.

PROPOSITION 4. — *Si* A *possède un sous-demi-groupe* Q *net à droite* (2), *unitaire à gauche* (2), *la représentation ergodique à droite est une représentation isomorphe du quotient de* A *par* $\bar{\chi}$. *En particulier si* A *est syntactiquement simple* (4) *par rapport à* Q, *la représentation ergodique à droite est une représentation isomorphe de* A.

Q, net à droite, contient tous les e_i^j $(i \in I)$ pour au moins un $j_0 \in J$. Donc $\bar{\chi}$ vérifie les conditions de la proposition 3 car à tout $x \in A$, il correspond au moins un $c \in C$ — par exemple $e_1^{j_0} x$ — tel que $c \chi x$. Si A est syntactiquement simple les classes pour χ coïncident par hypothèse avec les classes pour l'équivalence principale à droite (2) attachée à Q.

(1) M. P. SCHÜTZENBERGER, *Comptes rendus*, **242**, 1956, p. 862.

(2) P. DUBREIL, *Mém. Acad. Sc.*, **63**, 1941, p. 8 et *Rend. Matem.*, 5e série, **10**, 1951, p. 195.

(3) SUSCHKEVITSCH, *Math. Ann.*, **99**, 1928, p. 30.

(4) L'équivalence appelée « syntactique » dans (1) avait déjà été définie et étudiée par M. TEISSIER, *Comptes rendus*, **232**, 1951, p. 1987.

ALGÈBRE. — *Sur deux représentations des demi groupes finis.* Note (*)
de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

Soit Σ un demi groupe (1) d'applications d'un ensemble fini E dans lui-même. A tout $\sigma \in \Sigma$ on fait correspondre dans certains problèmes l'application « inverse » $\overset{-1}{\sigma}$ définie sur $F = \mathfrak{P}(E)$ par $\overset{-1}{\sigma}x = \{ \cup y : \sigma y \subset x \}$. Les $\overset{-1}{\sigma}$ fournissent une représentation de Σ anti-isomorphe de la première. Attachons à tout σ les deux matrices carrées à indices dans F suivantes :

$$S_\sigma : \quad S_\sigma(x;y) = 1 \quad \text{si} \quad \sigma x = y; \qquad S_\sigma(x;y) = 0 \quad \text{si} \quad \sigma x \neq y,$$
$$S'_\sigma : \quad S'_\sigma(x;y) = 1 \quad \text{si} \quad x = \overset{-1}{\sigma} y; \qquad S'_\sigma(x;y) = 0 \quad \text{si} \quad x \neq \overset{-1}{\sigma} y.$$

S'_σ est la transposée de la matrice d'application attachée à $\overset{-1}{\sigma}$ et S_σ est la matrice correspondant à l'extension de σ à F. Supposant que Σ est le demi groupe de toutes les applications de E dans lui-même, nous donnerons une base du module $\mathfrak{B}$ des matrices carrées à indices dans F telles que

$$(1) \qquad S_\sigma B = B S'_\sigma \quad \text{pour tout} \quad B \in \mathfrak{B} \quad \text{et} \quad \sigma \in \Sigma.$$

Notations. — On utilisera les matrices particulières suivantes dont les éléments sont égaux à 0 ou à 1. (On a indiqué pour chacune d'elles ci-dessous la partie de $F \times F$ correspondant aux éléments non nuls).

$$T : \ x = E - y; \qquad B_0 : \ x = \emptyset; \qquad B_1 : \ \emptyset \neq x \subset y; \qquad B_2 = B_1 T : \ \emptyset \neq x \subset E - y.$$
$$B_3 : \ x \cap y \neq \emptyset \neq x \cap (E - y); \qquad C_0 : \ x = y = \emptyset; \qquad C_3 = TC_0 : \ E - x = y = \emptyset;$$
$$B'_1 = B_0 + B_1; \qquad C'_1 = B'^{-1}_1; \qquad C'_2 = (B_0 + B_2)^{-1} = C'_1 T; \qquad B'_0 = B_0 + B_1 + B_2 + B_3$$

Proposition. — *Les matrices* B_0, B_1, B_2, B_3 *constituent une base indépendante de* $\mathfrak{B}$.

Démonstration. — Pour un σ donné, (1) s'écrit :

$$(1') \qquad \sum_{y \in F} S(x;y) B(y;z) = \sum_{y \in F} B(x;y) S'(y;z) \qquad \text{pour tout} \quad x, z \in F.$$

Soit encore puisque $S(x;y)$ et $S'(x;y)$ ne diffèrent de zéro que si $\sigma x = y$ et $x = \overset{-1}{\sigma} y$

$$(1'') \qquad \text{pour tout } x, z \in F : \quad B(\sigma x; z) = B\left(x; \overset{-1}{\sigma} z\right).$$

Or, pour tout σ, $z \cap \sigma x = \emptyset$ est équivalent à $x \cap \sigma^{-1} z = \emptyset$. Le système $(1'')$ d'équations se décompose donc en quatre sous systèmes tels que chaque $B(x;y)$ ne figure que dans un seul d'entre eux et ceux-ci correspondent aux cas suivants :

$$\begin{aligned}
&(1'')_0 : \quad x \cap z = \emptyset = x \cap (E - z), && \text{c'est-à-dire} && x = \emptyset.\\
&(1'')_1 : \quad x \cap z \neq \emptyset = x \cap (E - z), && \text{»} && \emptyset \neq x \subset z.\\
&(1'')_2 : \quad x \cap z = \emptyset \neq x \cap (E - z), && \text{»} && \emptyset \neq xE - z.\\
&(1'')_2 : \quad x \cap z \neq \emptyset \neq x \cap (E - z).
\end{aligned}$$

Montrons maintenant que si $B(x;y)$ et $B(x';y')$ figurent dans le même sous-système, ils sont égaux.

$(1'')_0$: Quel que soit $z \neq \emptyset$, E, on peut trouver σ et σ' tels que $\sigma^{-1} z = \emptyset$ et $\sigma'^{-1} z = E$. Donc $B(\emptyset; z) = B(\emptyset; \sigma^{-1} z) = B(\emptyset; \emptyset)$, d'une part, et, d'autre part, $B(\emptyset; z) = B(\emptyset; \sigma'^{-1} z) = B(\emptyset; E)$.

$(1'')_1$: Si $\emptyset \neq x \subset z$, on peut trouver σ tel que $\sigma E = x$ et $\sigma^{-1} z = E$. Donc, $B(x; z) = B(\sigma E; z) = B(E; \sigma^{-1} z) = B(E; E)$.

$(1'')_2$: Quels que soient σ et z, on a $\sigma^{-1} z = E - \sigma^{-1}(E - z)$. Donc, comme pour $(1'')_1$, $B(x, z) = B(E; \emptyset)$.

$(1'')_3$: Nous désignons par $|u|$ le nombre d'éléments de E contenus dans $u \in F$. Sous l'hypothèse $(1'')_3$, il existe plusieurs y tels que

$$0 < |x \cap z| \leq |y| \leq |E| - (|x| - |x \cap z|) < |E|. \tag{2}$$

En outre, pour tout semblable y, on peut trouver un σ tel que $\sigma y = x \cap z$ et $\sigma(E - y) = x - x \cap z$; c'est-à-dire

$$\sigma E = \sigma y \cup \sigma(E - y) = x \qquad \text{et} \qquad \sigma^{-1} z = E - \sigma^{-1}(E - z) = y.$$

Donc $B(x; z) = B(E; y)$, pour tout y satisfaisant (2).

Proposition. — *Si le corps de base de* $\mathfrak{B}$ *est commutatif, le déterminant* β *de* $B = \lambda_0 B_0 + \lambda_1 B_1 + \lambda_2 B_2 + \lambda_3 B_3$ *est égal à* $\lambda_0 (\lambda_1 - \lambda_2)^m (\lambda_1 + \lambda_2 - 2\lambda_3)^{m-1}$ ou $n = |E|$ *et* $m = 2^{n-1}$.

Démonstration. — λ_0 est un facteur simple de β. Formons les combinaisons suivantes de colonnes de B :

1° « Colonne z » — « colonne $(E - z)$ » pour tous les z tels que $|z| < |E|/2$ et si $|E|$ est paire pour tous les z contenant un élément fixe de E quand $|z| = |E|/2$. $B(x; z) - B(x; E - z) = 0$ si $x = \emptyset$; $= \lambda_1 - \lambda_2$ si $x \neq \emptyset$.

2° « Colonne $\emptyset$ » — « colonne E » — « colonne z » — « colonne $(E - z)$ » pour tous les $z \neq \emptyset$, E. $B(x; \emptyset) + B(x; E) - B(x; z) - B(x; E - z) = 0$ si $x = \emptyset$; $= \lambda_1 + \lambda_2 - 2\lambda_3$ si $x \neq \emptyset$.

PROPOSITION. — *Toute matrice* C *telle que* $CS_\sigma = S'_\sigma C$, *identiquement, est de la forme* $C = \mu_0 C_0 + \mu_1 C'_1 + \mu_2 C'_2 + \mu_3 C'_3$ *et* $BC = 1$ *si et seulement si*

$$\lambda_0(\mu_0+\mu_1+\mu_2+\mu_3)=1, \qquad (\lambda_1-\lambda_2)(\mu_1-\mu_2)=1,$$
$$(\lambda_1+\lambda_2-2\lambda_3)(\mu_1+\mu_2)=1, \qquad \lambda_1\mu_3+\lambda_2\mu_0+\lambda_3(\mu_1+\mu_2)=0.$$

Démonstration. — C_0 et C_3 satisfont manifestement la relation précédente de même que $(B_0+B_1)^{-1}$ et $(B_0+B_2)^{-1}$; le résultat en découle puisque ces quatre matrices sont linéairement indépendantes.

On trouve de même l'expression générale des matrices D (resp. D′) satisfaisant identiquement $S_\sigma D = DS_\sigma$ (resp. $S'_\sigma D' = D'S'_\sigma$) :

$$D = \delta_0 I + \delta_1(B_0+B_2)B'^{-1} + \delta_2 C_0 + \delta_3 B'_0 C_0 \qquad \text{et} \qquad D' = \delta'_0 I + \delta' T + \delta'_2 B_0 + \delta_3 T B_0.$$

(*) Séance du 22 octobre 1956.

(1) P. DUBREIL, *Algèbre*, Gauthier-Villars, 1946, p. 34.

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*, t. **243**, p. 1385-1387, séance du 5 novembre 1956.)

GAUTHIER-VILLARS,
ÉDITEUR-IMPRIMEUR-LIBRAIRE DES COMPTES RENDUS DES SÉANCES DE L'ACADÉMIE DES SCIENCES
15079S-56 Paris. — Quai des Grands-Augustins, 55.

Année 1957

Bibliographie

[1] Marcel-Paul Schützenberger. $\overline{\mathcal{D}}$ représentation des demi-groupes. *C. R. Acad. Sci. Paris*, 244 :1994–1996, 1957.

[2] Marcel-Paul Schützenberger. Applications des $\overline{\mathcal{D}}$ représentations à l'étude des homomorphismes des demi-groupes. *C. R. Acad. Sci. Paris*, 244 :2219–2221, 1957.

[3] Marcel-Paul Schützenberger. Sur une propriété combinatoire des demi-groupes libres. *C. R. Acad. Sci. Paris*, 245 :16–18, 1957.

[4] Marcel-Paul Schützenberger. Nouvelle démonstration du théorème de Schreier sur les sous-groupes d'un groupe libre par son extension au cas des demi-groupes. In *Séminaire Dubreil-Pisot, année 1957-58*, Exposé No. 6, 6 pages. Inst. H. Poincaré, Paris, 1957.

[5] Marcel-Paul Schützenberger. On some measure of "information" used in statistics. –, 1957. Traduit en russe.

[6] Marcel-Paul Schützenberger. Sur une généralisation de l'inégalité minimax. *Cahiers du bureau universitaire de recherche opérationnelle*, Cahier No 2 :2–7, 1957. Institut de Statistique de l'Université de Paris, Inst. H. Poincaré, Paris.

[7] Marcel-Paul Schützenberger. La théorie de l'information. In *Cahiers d'actualité et de synthèse, Encyclopédie française*, pages 9–21. Société Nouvelle de l'Encyclopédie Française, Paris, 1957. (Supplément à la réédition de 1957 du tome I : "L'outillage mental" (édition originale 1937)).

ALGÈBRE. — *$\overline{\mathcal{D}}$ représentation des demi-groupes.* Note (*)
de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

La $\overline{\mathcal{D}}$-classe D (1) du demi-groupe (1) S sera dite de type « élémentaire » si l'on a identiquement dans D : $\overline{\mathcal{L}} \cap \mathcal{R} = \mathcal{L} \cap \overline{\mathcal{R}} = \overline{\mathcal{H}}$ et l'on montrera que sous cette hypothèse, il est possible d'associer à D deux représentations de S par des matrices dont les éléments non nuls appartiennent à un groupe Γ déterminé par D. Ceci généralise à la totalité de S une construction analogue de D.D. Miller et A. H. Clifford (3) valable pour les seuls éléments de D et une autre représentation décrite antérieurement (4).

Proposition 1. — *Si s, $\bar{s}$ et $a \in S$ sont tels que $as\bar{s} = a$, l'application $x \to xs$ est une application biunivoque compatible avec $\overline{\mathcal{R}}$ de Sa sur Sa' ($a' = as$). En particulier, si* K *est une $\overline{\mathcal{H}}$-classe de* S *et si* $Ks \cap K \neq \emptyset$ *alors* $Ks = K$, *biunivoquement.*

Démonstration. — 1° Pour tout $b \in Sa$, $bs\bar{s} = b$ car $b = ua$ implique $bs\bar{s} = uas\bar{s} = ua = b$. Donc la translation à droite $s\bar{s}$ ($\bar{s}s$) est une application identique de Sa (Sa') sur lui-même. 2° $\mathcal{L}$ étant régulière à droite, $Sas \subset Sa'$ et $Sa'\bar{s} \subset Sa$; donc $Sas\bar{s} \subset Sa'\bar{s} \subset Sa$. 3° Pour tout $b \in Sa$, $b' = bs$, on a $b\overline{\mathcal{R}}b'$ car $b = b'\bar{s}$. Donc si $c\overline{\mathcal{R}}b$ ($c, b \in Sa$) on a $cs = c'\overline{\mathcal{R}}c$, $bs = b'\overline{\mathcal{R}}b$ et, en raison de la transitivité de $\overline{\mathcal{R}}$: $c'\overline{\mathcal{R}}b'$. 4° Si $ks = k'$ ($k, k' \in K$, c'est-à-dire $k\overline{\mathcal{L}} \cap \overline{\mathcal{R}}k'$), il existe par hypothèse $\bar{s}$ tel que $k'\bar{s} = k$. Donc s applique biunivoquement K sur une certaine $\overline{\mathcal{H}}$ classe K′ et $K' = K$ puisque $K' \cap K \neq \emptyset$.

Proposition 2. — *Soit* K *une $\overline{\mathcal{H}}$ classe de* S; $G = K^{(-1)}K = \{ s : Ks \cap K \neq \emptyset \}$; $G' = KK^{(-1)}$; $\varphi(\varphi')$ *l'homomorphisme de* $G(G')$ *induit par la représentation de ce sous-demi-groupe par des translations à droite* (*à gauche*) *sur* K. *On a* $\varphi(G) = \varphi'(G') =$ *un groupe* Γ.

Démonstration. — On choisit un élément fixe $\underline{k}$ de K; si s et s' sont tels que $\underline{k}s = \underline{k}s' \in K$, on a $\varphi(s) = \varphi(s')$ car il existe $\bar{s}$ tel que $\underline{k}s\bar{s} = \underline{k}$, ce qui entraîne $\underline{k}s'\bar{s} = \underline{k}$, donc $ks\bar{s} = ks'\bar{s}$ pour tout $k \in K$ et enfin $ks = ks'$ pour tout $k \in K$. Donc : 1° $\varphi(G)$ et $\varphi'(G')$ sont des groupes. 2° Il existe une correspondance biunivoque entre les $k \in K$, les $\alpha \in \varphi(G)$ et les $\alpha' \in \varphi'(G')$ définie par :

$\varphi'(\alpha')\underline{k} = \underline{k}\,\tilde{\varphi}(\alpha)$. On peut identifier $\varphi(G)$ et $\varphi'(G')$ et l'on écrira indifféremment : $k = \underline{k}^{\alpha} = \tilde{\varphi}'(\alpha)\underline{k} = \underline{k}\,\tilde{\varphi}(\alpha)$ ou $\alpha = \tilde{\varphi}(k)$. On conviendra que $\tilde{\varphi}(x) = 0$ si $x \notin K$. Soit maintenant D, la $\overline{\mathcal{D}}$ classe de K décomposée de la façon habituelle en ses $\overline{\mathcal{L}}$-, $\overline{\mathcal{R}}$- et $\overline{\mathcal{H}}$-classes : $D = \bigcup_{i\in I} L^i = \bigcup_{j\in J} R_j = \bigcup_{i\in I,\, j\in J} K^i_j$ avec $K^i_j = R_j \cap L^i$ et $K = K^1_1$. Par hypothèse, il existe des éléments $u^i, \bar{u}^i (i \in I)$, $v_j, \bar{v}_j (j \in J)$ satisfaisant les relations : $\underline{k}u^i \in L^i$; $\underline{k}u^i\bar{u}^i = \underline{k}$; $v_j\underline{k} \in R_j$; $\bar{v}_j v_j \underline{k} = \underline{k}$. D'après la proposition 2, les applications $K \to v_j K u_i$ et $K^i_j \to \bar{v}_j K^i_j \bar{u}^i$ sont biunivoques et inverse-l'une de l'autre.

Nous supposons désormais que D est de type élémentaire et nous considérons l'expression $d_i(s) = \underline{k}u^i s$. Ou bien $d_i(s) \notin R$ [et dans ce cas $d_i(st) \notin R$ pour tout $t \in S$], ou bien $d_i(s)$ appartient à une certaine $\overline{\mathcal{H}}$-classe $K^{i'}_j$. Comme $d_i(s)\overline{\mathcal{L}} \cap \mathcal{R}\underline{k}$, $j = 1$ et $\underline{k}u^i s\bar{u}^{i'}$ est un certain élément k de K. Nous posons $m^{i'}_i(s) = \tilde{\varphi}(k)$ et $m^{i''}_i(s) = 0$ pour tout $i'' \neq i'$ $(i'' \in I)$. Nous désignerons par $M(s)$ la $I \times I$ matrice dont les éléments $m(s)$ viennent d'être définis et l'on conviendra que $0\Gamma = \Gamma 0 = 0$. On définirait de la même manière une $J \times J$ matrice $N(s)$ avec au plus un élément non nul par colonne : $n^j_{j'}(s) = \tilde{\varphi}(\bar{v}_{j'} s v_j)$ si $s v_j \in R_{j'}$ et $= 0$, autrement.

Proposition 3. — *La représentation $s \to M(s)$ est équivalente à la restriction à* D *de la représentation de* S *par des translations à droite.*

Démonstration. — Il suffit de montrer que $M(st) = M(s)M(t)$ identiquement. Or $m^{i'}_i(st) = 0$ si et si seulement $L^i st \cap D \neq \emptyset$, c'est-à-dire, ou bien si $L^i s \cap D \neq \emptyset$, ou bien si $L^i s = L^{i''}$ et $L^{i''} t \neq L^{i'}$. Dans le cas contraire on a

$$m^{i'}_i(st) = \tilde{\varphi}(\underline{k}u^i st\bar{u}^{i'}) = \tilde{\varphi}(\underline{k}u^i s\bar{u}^{i''} u^{i''} t\bar{u}^{i'}) = m^{i''}_i(s)\, m^{i'}_{i''}(t).$$

Nous considérons maintenant la $I \times J$ matrice P d'éléments $p^j_i = \tilde{\varphi}(\underline{k}u^i v_j \underline{k})$.

Proposition 4. — *Pour tout $s \in S$ on a identiquement :*

$$M(s)P = PN(s) = Q(s).$$

Démonstration. — On pose $q^j_i(s) = \tilde{\varphi}(\underline{k}u^i s v_j \underline{k}) = \tilde{\varphi}(\underline{k}u^i s\bar{u}^{i''} v_j \underline{k}) = \tilde{\varphi}(\underline{k}u^i v_j, \bar{v}_j, s v_j \underline{k})$ et l'on vérifie que la $I \times J$ matrice $Q(s)$ ainsi construite est bien la valeur commune de $M(s)P$ et de $PN(s)$.

Proposition 5. — *A des transformations par des matrices diagonales près,* $M(s)$ *est indépendante du choix des u^i, v_j et de $\underline{k} \in D$.*

Démonstration. — Supposons les u^i remplacés par les u'^i. On a $\underline{k}u'\bar{u} = \underline{k}^{\lambda}$ et $\underline{k}u^i\bar{u}'^i = \underline{k}^{\bar{\lambda}^i}$ avec $\lambda_i\bar{\lambda}_i = \varepsilon = \varepsilon^2$ puisque $\underline{k}u'^i\bar{u}'^i = \underline{k}$. Donc $m'^{i'}_i(s)\lambda_{i'} = \lambda_i m^{i'}_i(s)$. D'autre part, $M(s)$ ne change pas quand on remplace $\underline{k}$ par $\underline{k}' = wk \in K^1_j$.

Enfin, $M(s)$ ne change pas non plus si l'on remplace simultanément $\underline{k}$ par $\underline{k}' = \underline{k}u^{i\star}$ et les u^i par les $u'^i = \overline{u}^{i\star}u^i$.

Remarque. — Si D n'est pas régulière au sens de (3), P est identiquement nulle ainsi que les $M(s)$ et les $N(s)$ pour tout $s \in D$. Si D est régulière

$$M(s) = P\overline{M}(s) \qquad \text{et} \qquad N(s) = \overline{M}(s)P \qquad \text{pour tout } s \in D,$$

$\overline{M}(s)$ étant la matrice ne contenant qu'un seul élément non nul définie par D. D. Miller et A. H. Clifford (3). Si D est la réunion des idéaux minimaux (à droite et à gauche) de S et si $u^i = e^i_1$; $v_j = e^1_j$; $\overline{u}^i = \overline{v}_j = e^1_1 = \underline{k}$, on retrouve la représentation définie dans (4).

(*) Séance du 25 mars 1957.

(1) Modifiant légèrement les notations de J.A. Green(2) et supposant que S contient une unité on pose : $a\mathcal{L}b \rightleftharpoons Sa \subset Sb$; $a\mathcal{R}b \rightleftharpoons aS \subset bS$; $\overline{\mathcal{L}} = \mathcal{L} \cap \overline{\mathcal{L}}^{-1}$; $\overline{\mathcal{R}} = \mathcal{R} \cap \overline{\mathcal{R}}^{-1}$; $\overline{\mathcal{D}} = \overline{\mathcal{L}}.\overline{\mathcal{R}} = \overline{\mathcal{R}}.\overline{\mathcal{L}}$; $\overline{\mathcal{H}} = \overline{\mathcal{L}} \cap \overline{\mathcal{R}}$.

(1) P. Dubreil, *Algèbre*, Paris, p. 38.

(2) *Ann. Math.*, **54**, 1951, p. 163-172.

(3) *Trans. Am. Math. Soc.*, **82**, 1956, p. 270-280.

(4) *Comptes rendus*, **242**, 1956, p. 2907.

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*, t. **244**, p. 1994-1996, séance du 8 avril 1957.)

GAUTHIER-VILLARS,
ÉDITEUR-IMPRIMEUR-LIBRAIRE DES COMPTES RENDUS DES SÉANCES DE L'ACADÉMIE DES SCIENCES
151704-57 Paris. — Quai des Grands-Augustins, 55.

ALGÈBRE. — *Applications des $\overline{\mathcal{D}}$ représentations à l'étude des homomorphismes des demi-groupes.* Note (*) de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

La $\overline{\mathcal{D}}$ représentation d'un demi-groupe définie dans une Note antérieure (1) dont les notations seront utilisées ici, conduit à des résultats particulièrement simples quand S satisfait la condition J : Tout sous-demi-groupe U_d fermé (2) possède des idéaux minimaux à droite et à gauche. J, qui est préservée par les homomorphismes, entraîne, en particulier, $\mathcal{R} \cap \overline{\mathcal{L}}^{-1} = \overline{\mathcal{H}}$ et $\mathcal{R}\mathcal{L} \cap \overline{\mathcal{R}}^{-1}\overline{\mathcal{L}}^{-1} = \overline{\mathcal{D}}$. On désignera respectivement par δ^r_D, δ^l_D et $\delta^d_D = \delta^r_D + \delta^l_D$ les homomorphismes de S induits par sa $\overline{\mathcal{D}}$ représentation associée à D sur les demi-groupes de matrices $\{M(s)\}$, $\{N(s)\}$ et $\{M(s) + N(s)\}$ ($+$: la somme directe) et l'on montrera que les δ sont étroitement liés aux sous-demi-groupes unitaires définis et étudiés par P. Dubreil (3).

Proposition 1. — *S satisfaisant* J *et* θ *étant un homomorphisme de* S *sur* S′, *il correspond à toute $\overline{\mathcal{D}}$ classe* D′ *de* S′ *une $\overline{\mathcal{D}}$ classe* D *de* S *et des homomorphismes* $\theta'^x (x = d, r, l)$ *tels que* $\delta^x_{D'}\theta = \delta^x_{D'}\theta'^x\delta^x_D$, *qui se réduisent à l'application identique pour les éléments de* $\delta^x_D S$ *n'appartenant pas à* $\delta^x_D D$.

Démonstration. — 1° $\mathcal{R}$ et $\mathcal{L}$ étant compatibles avec les homomorphismes, toute $\overline{\mathfrak{X}}$ classe de S ($\overline{\mathfrak{X}} = \overline{\mathcal{H}}$, $\overline{\mathcal{R}}$, $\overline{\mathcal{L}}$ ou $\overline{\mathcal{D}}$) est appliquée par θ dans une $\overline{\mathfrak{X}}$ classe de S′. Soient : $e' = e'^2 \in D'$; $Q_{e'} = \overline{\theta}^{-1}e'$, le « noyau » correspondant; $P_e = Q^{(-1)}_{e'} Q_{e'} \cap Q_{e'} Q^{(-1)}_{e'} = \left\{ \overline{\theta}^{-1} s' : s'e' = e's' = e' \right\}$, la U_d fermeture de celui-ci; D, la $\overline{\mathcal{D}}$ classe de S contenant les idéaux minimaux de $P_{e'}$; $e = e^2 \in Q_{e'} \cap D$. Comme $\theta D \cap D' \neq \emptyset$, on a $\theta D \subset D'$. Montrons que $\theta D = D'$: si s' appartient à la $\overline{\mathcal{R}}$ classe R′ de e', il existe $\bar{s}'$ tel que $e's's' = e'$. Donc $e\overline{\theta}^{-1}s'\overline{\theta}^{-1}\bar{s}' \ni f \in Q_e$ mais puisque D est de type élémentaire et que e' est dans l'idéal minimum de $Q_{e'}$, f appartient à la $\overline{\mathcal{R}}$ classe R de e et l'on a donc $\theta R = R'$. On montrerait de même que $\theta L = L'$ et $\theta K = K'$ pour les $\overline{\mathcal{L}}$ ou les $\overline{\mathcal{H}}$ classes de D. Par conséquent, $\delta^x_{D'}\theta S$ est une image homomorphe de $\delta^x_D S$ car, par exemple, $\delta^r_D s_1 = \delta^r_D s_2$ entraîne $\delta^r_{D'}\theta s_1 = \delta^r_{D'}\theta s_2$ puisque la première égalité signifie que pour tout $i \in I$, l'ensemble d'indices des $\overline{\mathcal{L}}$ classes de D, ou bien $eu^i s_1 = eu^i s_2 \in R$, ou bien $eu^i s_1 \cup eu^i s_2 \in S - R$.

2° Considérons la restriction de δ_D^x à D. Si D n'est pas régulière (4), $\delta_D^x D = 0$; si D est régulière, on peut choisir $\underline{k} = e$ et $u^i = eu^i \in R$. Donc, par exemple, δ_D^r est un isomorphisme pour R et, plus généralement, δ_D^x est idempotent. Si, en outre, D est de type élémentaire, $\delta_D^x S$ admet un seul idéal minimum différent de o qui est précisément $o \cup \delta_D^x D$. Par conséquent, toute application θ' de $\delta_D^x S$ qui est un homomorphisme pour $\delta_D^x D$ et l'application identique en dehors de cet ensemble est un homomorphisme de $\delta_D^x S$.

3° Enfin, $\theta' \delta_D^x = \delta_D^x$ si θ' est un homomorphisme de $\delta_D^x S$ se réduisant à un isomorphisme pour $\delta_D^x D$, ce qui achève la démonstration.

Remarque. — Supposons toujours D de type élémentaire. Si s appartient à la $\overline{\mathcal{L}}$ classe $L^{i'}$ de D, $eu^i s \in R$ entraîne que cet élément appartienne à $L^{i'}$ et l'on ne peut donc avoir $\delta_D^r s_1 = \delta_D^r s_2$ pour $s_1, s_2 \in D$ que si $s_1 = \varphi_j \bar{\varphi}^{-1}(\alpha_1) u^{i'}$ et $s_2 = \varphi_{j'} \bar{\varphi}^{-1}(\alpha_2) u^{i'}$ avec $\tilde{\varphi}(u^i \varphi_j) \alpha_1 = \tilde{\varphi}(u^i \varphi_{j'}) \alpha_2$ pour tout $i \in I$. δ_D^r ne diffère donc de D que par l'identification des $\overline{\mathcal{R}}$ classes R_j et $R_{j'}$ satisfaisant une relation du type précédent. Il en est de même dualement pour δ_D^l et les $\overline{\mathcal{L}}$ classes de D et les deux opérations commutent manifestement quand D est de type élémentaire. On écrira selon des notations évidentes $\delta_D^k = \delta_D^r \delta_D^l = \delta_D^l \delta_D^r$.

Proposition 2. — 1° *Soit* S *un demi-groupe quelconque,* $\{P_n\}$ *une famille de demi-groupes* U_{x_n} *fermés de* $S(x_n = r, l, d \text{ ou } k)$, θ *un homomorphisme de* S *sur* S′ *tel que les* $P'_n = \theta P_n$ *possèdent des idéaux minimaux à gauche et à droite, et que* $\theta_{s_1} = \theta_{s_2}$ *si, et seulement si,* $s_1 \equiv s_2 (P_n)$ *pour tout* n (5), *alors* S′ *est isomorphe à la somme directe* $\delta S'$ *des représentations* $\delta_{D'_n}^{x_n} S'$ *où* D'_n *est la* $\overline{\mathcal{D}}$ *classe contenant l'idéal minimum de* P'_n.

Réciproquement, soit $S' = \theta S = \delta S'$ *où* δ *est de la forme précédente. Soit* E′ *l'ensemble des idempotents contenus dans* $\bigcup_n D'_n$, *alors,* θ *est tel que* $\theta s_1 = \theta s_2$ *si et seulement si,* $s_1 \equiv s_2 (T_{e'})$ *pour tout* $T_{e'} (e' \in E')$ *où* $T_{e'}$ *est indifféremment le noyau de* e' *ou la* U_d *fermeture de celui-ci.*

Démonstration. — 1° Puisque $\bar{\theta}^{-1} P'_n = P_n$, tout homomorphisme θ' de S′ tel que $\theta' s'_1 = \theta' s'_2$ si, et seulement si, $s'_1 \equiv s'_2 (P'_n)$ pour tout n est un isomorphisme de S′. Donc les P'_n sont U_{x_n} fermés en même temps que les P_n. Soit $s'_1 \neq s'_2$; par hypothèse, il existe un P'_n tel que, par exemple, $y' s'_1 z' = p' \in P'$ et $y' s'_2 z' = q' \notin P'$. Choisissons un idempotent $C' \neq o$ dans l'idéal minimum de $P'_n \subset D'_n$.

(r) si $x_n = r$, $q' \notin P'$ entraîne $e' q' \notin P'$ et comme $e' y'$ et $e' p'$ appartiennent à la $\overline{\mathcal{R}}$ classe de e', on a $\delta_{D'_n}^r s'_1 \neq \delta_{D'_n}^r s'_2$;

(l) si $x_n = l$, on applique le même raisonnement en multipliant à droite par e' et $\delta_{D'_n}^l s'_1 \neq \delta_{D'_n}^l s'_2$; (d) : si $x_n = d$, (r) *ou* (l) sont vrais; (k) : si $x_n = k$, (r) *et* (l) sont vrais.

2° On a encore $s_1 \equiv s_2(\mathrm{T})$ si, et seulement si, $0s_1 \equiv 0s_2(0\mathrm{T})$. Supposons donc que $0s_1 \not\equiv 0s_2$. Par hypothèse il existe un idempotent e' tel que par exemple $e' \overline{\mathcal{R}} e' u'^{i} 0 s_1 = s'_1 \not\equiv s'_2 = e' u'^{i} 0 s_2$. Ou bien s'_1 et s'_2 appartiennent à la même $\overline{\mathcal{L}}$ classe et sont de la forme $\overline{\varphi}^{-1}(\alpha_1)u'' = s'_1$ et $\overline{\varphi}^{-1}(\alpha_2)u'' = s'_2$ avec $\alpha_1 \neq \alpha_2$ et alors $s_1 \not\equiv s_2(\mathrm{T}_{e'})$. Ou bien ils appartiennent à deux $\overline{\mathcal{L}}$ classes différentes et alors $s_1 \not\equiv s_2(\mathrm{T}_{f'})$ où f' est un idempotent de l'une de ces classes.

(*) Séance du 8 avril 1957.

(1) *Comptes rendus*, **244**, 1957, p. 1994.

(2) Rappelons que $\mathrm{X}^{(-1)}\mathrm{Y} = \{s : \mathrm{X}s \cap \mathrm{Y} \neq \emptyset\}$. Un sous-demi-groupe P est U_d fermé si $\mathrm{P}^{(-1)}\mathrm{P} \cap \mathrm{PP}^{(-1)} \subset \mathrm{P}$; U_r fermé (« unitaire à gauche ») si $\mathrm{P}^{(-1)}\mathrm{P} \subset \mathrm{P}$; U_l fermé (« unitaire à droite ») si $\mathrm{PP}^{(-1)} \subset \mathrm{P}$; U_k fermé si $\mathrm{P}^{(-1)}\mathrm{P} \cup \mathrm{PP}^{(-1)} \subset \mathrm{P}$.

(3) *Rend. Circ. Palermo.*, **81**, 1951, p. 289-306.

(4) D. D. Miller et A. H. Clifford, *Trans. Amer. Math. Soc*, **82**, 1956, p. 270-280.

(5) On pose après Mme Teissier (6) qui a étudié cette congruence : $s_1 \equiv s_2(\mathrm{P})$ si, et seulement si, pour tout $y, z \in \mathrm{S}$, $ys_1z \in \mathrm{A}$ entraîne $ys_2z \in \mathrm{P}$ et réciproquement.

(6) *Comptes rendus*, **232**, 1951, p. 1987.

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*, t. **244**, p. 2219-2221, séance du 24 avril 1957.)

GAUTHIER-VILLARS,
ÉDITEUR-IMPRIMEUR-LIBRAIRE DES COMPTES RENDUS DES SÉANCES DE L'ACADÉMIE DES SCIENCES
151778-57 Paris. — Quai des Grands-Augustins, 55.

ALGÈBRE. — *Sur une propriété combinatoire des demi-groupes libres.* Note (*) de M. **Marcel-Paul Schützenberger**, présentée par M. Georges Darmois.

Soit S le demi-groupe (2) libre engendré par $F=\{f_i\}$, fini. On pose pour tout $s\in S$: $|s|_i=$ le nombre de fois où f_i figure dans l'expression de s et $|s|=\sum_i |s|_i$. Deux sous-ensembles W et W′ de S seront dits « commutativement équivalents d'ordre $n\gg$ s'il existe une correspondance biunivoque $w_j\leftrightarrow w'_j$ entre les éléments de longueur inférieure à n de W et W′ telle que $\alpha w_j=\alpha w'_j$ dans toute image homomorphe commutative αS de S.

Proposition (1). — *Si* $P=P^2\subset S$ *satisfait les conditions* (U), P *est libre*, (N*), *il existe* $k<\infty$ *tel que pour tout* $s\in S$ *on puisse trouver* s', $s''\in S$ *avec* $|s'|+|s''|\leq k$ *et* $s'ss''\in P$, *alors, pour tout* $n<\infty$, *on peut construire* $P'=P'^2$, *commutativement équivalent d'ordre n à* P, *libre, et satisfaisant* (U_r), $P's\cap P'\neq\emptyset$ *entraîne* $s\in P'$ *et* (N_r), P′ *intersecte tous les idéaux à droite de* S [*d'après P. Dubreil* (2), P′ *est unitaire à gauche et net à droite et, d'après W. Feller*, P′ *correspond à un événement récurrent dont la probabilité n'est jamais zéro*].

On peut observer que (N*) est vérifiée notamment quand P satisfait (N), P intersecte tous les idéaux bilatères de S et (H), il existe un homomorphisme φ avec $\varphi^{-1}\varphi P=P$ tel que φS possède un idéal bilatère minimum fini. Donc, quand les éléments de l'ensemble Q des générateurs de P ont une longueur bornée, (N) est équivalent à (N*) (3).

On posera, pour tout $w\in W\subset S$,

$$\Pr(w)=\prod_i p_i^{|w|_i};\qquad \Phi_W(t)=\sum_{w\in W}\Pr(w)\,t^{|w|},$$

où $\mathfrak{X}=\{p_i\}$ est une distribution de probabilités sur les f_i avec $p_i>0$.

(T) [respectivement (T*)] sera la condition que pour au moins un $\mathfrak{X}$ (pour tout $\mathfrak{X}$) la racine τ de plus petit module de $\Phi_Q(t)=1$ soit égale à 1 et l'on rappellera la proposition suivante :

Proposition. — (N*) *et* (U) *entraînent* (T*); (N*) *et* (T) *entraînent* (U); (U) *et* (T) *entraînent* (N).

Démonstration. — Soient $c_1, c_2, \ldots$ des constantes strictement positives; $\overline{A}(n) = n^{-1}\sum_{n'=0}^{n} A(n')$ où $A(n) = \sum_{|s|=n} \nu(s)\Pr(s)$ est le coefficient de t^n dans $\Phi_P(t) = (1 - \Phi_Q(t))^{-1}$ et $\nu(s)$ le nombre de décompositions de s en un produit d'éléments appartenant à Q;

$$\overline{B}(n) = n^{-1}\sum_{n'=0}^{n} B(n) = n^{-1}\sum_{|s|\leq n;\, s\in P} \Pr(s).$$

(U) est équivalent à $A(n) = B(n)$, identiquement, et, comme $\overline{B}(n) \leq 1$, (U) entraîne $\tau \geq 1$. Inversement si $\nu(p) \geq 2$ pour au moins un $p \in P$, $\overline{A}(n) \geq (1 + c_1)^n B(n)$.

(N*) entraîne que tout s soit un diviseur d'au moins un $p \in P$ avec $s| \leq |p| \leq |s| + k$. Donc

$$\overline{A}(n) \geq \overline{B}(n) \geq c_2 \sum_{n'=n}^{n+k} B(n') \geq c_3 \sum_{|s|=n} \Pr(s) = c_3 \quad \text{et} \quad \tau \leq 1.$$

Inversement, s'il existait $s \in S$ avec $SsS \cap P = \emptyset$, on aurait $B(n) < (1 - \Pr(s))^{c_4 n}$.

Par conséquent, (U) et (N*) entraînent $\tau \geq 1$ et $\tau \leq 1$ pour tout $\mathfrak{X}$. Comme (N*) implique $\overline{B}(n) = c_5 + o(1)$, on ne peut avoir $A(n)(B(n))^{-1} > (1 + c_1)^n$ quand $\tau = 1$ puisqu'alors $\overline{A}(n) < (1 + c_6)^n$ pour tout c_6. Enfin, comme $\tau = 1$ entraîne $\overline{A}(n) > (1 - c_7)^n$ pour tout c_7 et que (U) implique $\overline{A}(n) = \overline{B}(n)$ on ne peut pas avoir $SsS \cap P = \emptyset$.

Démonstration de la proposition principale. — Soit $\Phi_Q(t) = \sum_{n=1}^{\infty} C(n)t^n$. Les $C(n)$ non nuls sont des polynomes homogènes en les p_i de degré n et ayant tous leurs coefficients entiers et non négatifs. En outre $\sum_{n=1}^{\infty} C(n) = 1$ identiquement quand $\sum_i p_i = 1$. Supposons d'abord que la longueur maxima n^* des éléments de Q soit bornée. Il suffira évidemment de montrer que sous les hypothèses précédentes $\Phi_Q(t)$ est identique à $\Phi_{Q'}(t)$ où Q', l'ensemble des générateurs de P', satisfait (U'_r), si $q, q' \in Q'$ et $qs = q'$, alors $q = q'$ et (N'_r), pour tout $s \in S$, ou bien $qs' = s$, ou bien $ss' = q$, avec $q \in Q'$ et $s' \in S$. Ceci est facilement vérifié quand $n^* \leq 2$. Supposons-le établi pour $n^* \leq n_0$ et soit Q avec $n^* = n_0 + 1$. Il résulte des conditions que $C(n_0 + 1)$ peut être écrit sous la forme $C''(n_0)(\Sigma p_i)$ où $C''(n_0)$ de degré n_0 satisfait encore les mêmes conditions. Par hypothèse il correspond donc à $\Phi_{Q''}(t) = \Phi_Q(t) - C(n_0 + 1)t^{n_0+1} + C''(n_0)t^n$ un ensemble Q'' avec les propriétés voulues. Définissons maintenant Q' comme l'union des éléments de Q'' de longueur $n_0 - 1$, des éléments correspondants

aux termes de $C(n_0)$ et des éléments de longueur n_0+1 formés en faisant suivre par l'une des lettres f_i les éléments correspondants aux termes de $C''(n_0)$. On vérifie sans peine que Q' est bien l'ensemble cherché.

Si Q n'est pas de longueur bornée, on considère pour tout n, l'ensemble tronqué Q_n correspondant à la fonction génératrice

$$\Phi_{Q_n}(t) = \Psi_n(t) + \Phi_Q(1) - \Psi_n(1))\, t^{n_0+1},$$

où $\Psi_n(t)$ est le polynome en t de degré n_0 identique aux n premiers termes de $\Phi_Q(t)$. Comme $Q'_{n-1} \cap Q'_n \subset Q'_{n+1}$ où Q' est l'ensemble obtenu à partir de Q par la construction précédente, la proposition est établie.

(*) Séance du 12 juin 1957.

(1) Ceci justifie la conjecture de R. S. Markus (*Quart. Prog. Rep. R. L. E.*, avril 1957) selon laquelle les codes « sans délai » [satisfaisant (U'_r)] sont strictement admissibles quels que soient les coûts des symboles élémentaires. La démonstration est d'ailleurs, comme on le verra, basée sur la méthode de D. Huffman (*I. R. E. Proc.*, 40, 1952, p. 1098) pour construire ces codes quand les $Pr(q)$ $(q \in Q)$ sont des valeurs numériques données. L'admissibilité asymptotique pour des coûts égaux est un corollaire immédiat des théorèmes de C. Shannon ainsi que l'a noté B. Mandelbrojt (*Proc. Symp. Inf. Networks*, New York, 1954, p. 210). Une généralisation facile mais longue des remarques précédentes permet de vérifier l'admissibilité stricte pour des coûts quelconques des transitions de degré arbitraire fixe fini.

(2) *Mém. Acad. Sc. Inst. Fr.*, 63, 1941, p. 1-51. Sous l'hypothèse (H), (U_r) entraîne d'ailleurs (N_r) quand (N) et N_r entraîne (U_r) quand (U).

(3) Mais même en présence de (U_r), (N^*) n'entraîne pas nécessairement (H).

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*, t. 245, p. 16-18, séance du 1er juillet 1957.)

GAUTHIER-VILLARS,
ÉDITEUR-IMPRIMEUR-LIBRAIRE DES COMPTES RENDUS DES SÉANCES DE L'ACADÉMIE DES SCIENCES
152101-57 Paris. — Quai des Grands-Augustins, 55.

Faculté des Sciences de Paris
-:-:-:-
Séminaire P. DUBREIL,
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1957/58
-:-:-:-

6-01

16 décembre 1957

NOUVELLE DÉMONSTRATION DU THÉORÈME DE SCHREIER SUR LES SOUS-GROUPES D'UN GROUPE LIBRE PAR SON EXTENSION AU CAS DES DEMI-GROUPES LIBRES.

par M.P. SCHÜTZENBERGER.

1. Dans cet exposé, on fera toujours l'hypothèse que les demi-groupes considérés contiennent un élément unité e (sont des "monoïdes") et par "sous demi-groupe" on entendra "sous-demi-groupe contenant e" (c'est-à-dire "sous monoïde").

Le théorème de Schreier peut être formulé de la façon suivante :

(1) Une condition nécessaire et suffisante pour que le sous-demi-groupe H du groupe libre G soit un groupe libre est qu'il satisfasse la condition U_d :

$$U_d : \forall_G^s \; sH \cap Hs \cap H \neq \emptyset \Rightarrow s \in H .$$

En effet, dans les conditions de l'énoncé, U_d signifie simplement que H est non seulement un sous-demi-groupe mais un sous-groupe de G . (Car si $s \in H$, on a $s\,s^{-1} = s^{-1}s = e \in H$ et, donc, $s^{-1} \in H$).

Par contre, la proposition analogue concernant les demi-groupes :

(1') Une condition nécessaire et suffisante pour que le sous-demi-groupe A du demi-groupe libre F soit un demi-groupe libre, est qu'il satisfasse U_d ,

peut être prouvée beaucoup plus directement (cf, par exemple, M.P. SCHÜTZENBERGER [6]) ou comme un corollaire d'un théorème de F. Levi ou, encore, comme un cas particulier d'un énoncé sur les produits libres de demi-groupes.

Le but de cet exposé est de montrer que la version "groupe" (1), du théorème de Schreier peut être déduite très simplement de la version "demi-groupe" (1') moyennant quelques corollaires des théorèmes généraux de la théorie des demi-groupes unitaires de P. Dubreil [1] (Section 2 ci-dessous) et une remarque combinatoire (section 3 ci-dessous) qui présente elle-même une certaine utilité pour un problème de mathématiques appliquées (celui de la marche au hazard sur un groupe libre).

2. Dans cette section, on considère un demi-groupe libre F , un groupe G (avec

6-02

élément neutre e') et un homomorphisme φ de F sur G .

ROPOSITION 2.1. - Si H est un sous-groupe de G , $A = \overline{\varphi}^{1} H$ est un sous-demi-upe libre de F .

ÉMONSTRATION. - H est "unitaire" dans G (cf. P. DUBREIL [1]) (c'est-à-dire il satisfait $U_k : \forall^{s}_{G}\ HsH \cap H \neq \emptyset \Rightarrow s \in H$). Donc A dans F satisfait U_k et, ortiori, U_d , D'où le résultat, d'après (1').

EMARQUE. - On peut démontrer 2.1 directement en utilisant seulement le fait que est libre et que A satisfait U_k . Soit $A_1 = (A - e) - (A - e)^2$ l'ensemble érateur de A . Il suffit de montrer que tout $x \in A - e$ a une représentation que comme produit de $a \in A_1$. Supposons donc que $x = ab = a'b' \in A$ avec $a' \in A_1$ (et donc b , $b' \in A$, d'après U_k). Ou bien a est un diviseur à iche de a' ou bien, l'inverse. Dans le premier cas, a' = aa" et la condition implique que $a'' \in A$. Comme $a' \in A_1$ ceci n'est possible que si a" = e = suite vide et, donc, a = a' . Etc.

ROPOSITION 2.2. - Si H est un sous-groupe normal de G , A satisfait en re aux deux conditions équivalentes suivantes :

: $\forall^{x,y}_{F}\ xy \in A \Leftrightarrow yx \in A$ (A est "symétrique au sens de P. DUBREIL [1])

: Deux quelconques des trois relations ci-dessous entraînent la troisième :

$$xyz \in A \ ; \ xz \in A \ ; \ y \in A .$$

A intersecte tous les idéaux de F .

ÉMONSTRATION. - Il suffit de vérifier que les conditions sont satisfaites pour - G .

ROPOSITION 2.3. - Réciproquement, si le sous-demi-groupe E de F intersecte s les idéaux bilatères de F et satisfait U_n (ou U_d et S), il existe un omorphisme φ de F sur un groupe G tel que $\overline{\varphi}^{1} e' = E$.

ÉMONSTRATION. - On vérifie facilement que U_d et S entraînent U_n (et U_k). ersement (R.R. STOLL [7]) si E satisfait U_n et si $xy \in E$, on a y $\in E$ et par conséquent $yx \in E$ (puisque $xyxy = x(yx)y$). L'implication $\Rightarrow U_k$ est triviale.

oit donc E satisfaisant les conditions de l'énoncé et φ l'homomorphisme ocié à la relation d'équivalence sur F définie par $x \equiv y\ (E)$ si et seulement

6-03

pour tout z , $t \in F$

$$zxt \in E \Leftrightarrow zyt \equiv E .$$

n vérifie successivement :

. $x \equiv y(E)$ pour tout x , $y \in E$.

onc, φE est un élément idempotent e' de φF .

i. Pour tout $x \in F$, il existe au moins un $x' \in F$ tel que $\varphi x \varphi x' = \varphi x' \varphi x = e'$.
isque E intersecte tous les idéaux bilatères, il correspond à tout x au
ns une paire y , z avec $yxz \in E$ et, d'après S , $(zy)x$ et $x(zy)$ appartien-
t à E).

es deux remarques prouvent que $G = \varphi F$ est un groupe et que E est bien le
eau de φ .

ROPOSITION 2.3. - Dans les mêmes conditions 2.2., si φ' est un homomorphisme de
sur un groupe G'' (d'élément neutre e'') et si $\varphi^{-1} e' = E \subset E'' = \varphi^{-1} e''$,
existe un homomorphisme χ de G sur G'' telque $\varphi' = \chi \circ \varphi$.

ÉMONSTRATION. - Il suffit évidemment de montrer que $x \equiv y$ (E) entraîne
y (E'') . Or, si la première relation est vérifiée et si $zxt \in E''$, il existe
avec $xtzu \in E$, donc, $ytzu \in E \subset E''$. Mais, $xtz \in E''$ et $xtzu \in E \subset E''$
liquent $u \in E''$ et, d'après U_k , ytz (et donc zyt) $\in E''$.

ROPOSITION 2.4. - L'ensemble des sous-demi-groupes de F qui satisfont U_n
me un treillis $L(F)$ complet et, si F' est un sous-demi-groupe quelconque
F , $A \in L(F)$ entraîne $A \cap F' \in L(F')$.

a démonstration est une paraphrase de l'énoncé.
es propositions 2,i et leurs démonstrations sont les cas particuliers de
orèmes établis par P. DUBREIL [1][2], F. LEVI [3][4] et R.R. STOLL [7].

Dans cette section on considère encore un demi-groupe libre F engendré par
nsemble $F_1 = \{f\}$ et une application involutive fixe $f \to f^*$ de F_1 sur lui-
e. Cette application est étendue de façon naturelle à un antiisomorphisme
F par $e^* = e$; $(xy)^* = y^* x^*$.

se décompose en deux sous-ensembles :
, consistant en tous les $f \in F_1$ tels que $f = f^*$
, consistant en toutes les paires (f , f') telles que $f^* = f' \neq f = f'^*$.

6-04

On suppose que l'on a su choisir un élément dans chacune de ces paires et on ésigne par G_1 l'ensemble de ces éléments.

Enfin on dénote par F_2 l'ensemble formé par l'union de F_1' et des produits * où $f \in F_1''$.

Soit maintenant G le groupe libre engendré par G_1 . On définit une application de F_1 sur $\{G_1 \cup e'\}$ par les règles suivantes :

i $f \in F_1'$, $\theta f = e'$

i $f \in G_1$, $\theta f = f$

i $f = f'^*$ et $f' \in G_1$, $\theta f = f'^{-1}$.

Puisque F est libre, θ peut être étendue de façon naturelle à un homomorphisme e F sur G dont le noyau $\theta^{-1}e'$ sera désigné par E .

PROPOSITION 3.1. – Si $x \in E$ est de la forme fyf' avec f , $f' \in F_1$ et $f^* \neq f'$, lors $x = zt$ où z et t appartiennent tous les deux à $E - e$.

DÉMONSTRATION. – Pour simplifier, nous utilisons le résultat bien connu que E st l'ensemble des suites finies de symbole $\{f\}$ qui peuvent être réduites à la uite vide e par cancellation répétée de paires d'éléments appartenant à F_2 . i donc les conditions de l'énoncé sont remplies, la dernière cancellation ne eut être celle de ff' puisque ce produit n'appartient pas à F_2 . Donc x doit voir la forme $fy'f^*y''f'$ où $z = fy'f^* \in E$ n'est pas la suite vide. D'après a , $t = y''f'$ appartient aussi à $E - e$.

PROPOSITION 3.2. – Le noyau E peut être défini de façon équivalente comme e plus petit sous-demi-groupe $E' \subset L(F)$ qui contienne F_2 ou, E'' qui contienne e sous ensemble F^* des $x \in F$ tels que $x = x^*$.

DÉMONSTRATION. – Que E soit le plus petit sous-demi-groupe contenant F_2 est ne conséquence directe de 2.3 et 2.4 quand E est défini comme $\theta^{-1}e'$ où ' est l'élément neutre du groupe libre G . Réciproquement, E' , d'après 2.2, st le noyau d'un homomorphisme sur un groupe (la condition accessoire ue E intersecte tous les idéaux bilatères est automatiquement satisfaite uisque pour tout x , $xx^* \in E$, d'après S) et ce groupe est libre d'après a proposition 2.3 et le caractère minimal de E .

D'autre part, si $E'' \in L(F)$ contient F^* , il contient en particulier F_2 car pour tout x , $(xx^*)^* = x^{**}x^* = xx^*$) et réciproquement, $E' = E''$.

effet, en raisonnant par récurrence sur la longueur $|x|$ de x, le résultat
; vrai par hypothèse quand $|x| \leq 2$. Quand $|x| > 2$, et $x = x^*$, x a la forme
* où $f \in F_1$ et y, de longueur $|x| - 2$, appartient à E'' puisqu'il
isfait $y = y^*$.

EMARQUE. – Dans l'application évoquée au début de cet exposé, on doit
sidérer l'ensemble générateur E_1 de E consistant en les $x \in E$ tels que
yz, $y \in E - e$ implique $z = e$ et $y = x$. Les deux propositions précédentes
mettent de montrer que E_1 est en correspondance biunivoque avec l'ensemble
on de F_1' et des suites de la forme $xyztx^*$ avec $|x| \geqslant 1$ et, soit $yzt = e$,
t y et z appartenant à E_1 et étant respectivement de la forme $y = fy'$
$z = z'f'$ avec f, $f' \in F_1$ et $f^* \neq f'$ (et évidemment, toujours, $z \in E$).

DÉMONSTRATION du théorème de Schreier (1). – Soit maintenant, avec les notations
la section 3, H un sous-groupe de G.
n a les résultats suivants :
. D'après 1.1, $A = \theta^{-1} H$ est un demi-groupe libre.
i. Puisque $e' \in H$, $E \subset A$ et, d'après 2.4, $E \in L(A)$.
ii. E est le noyau de la restriction de θ à A.
v. Puisque $aa^* \in E$, a et a^* appartiennent en même temps à A. Donc, en
ant $A_1 = (A - e) - (A - e)^2 =$ l'ensemble générateur de A (cf. la remarque
la section précédente), la restriction de * à A_1 est une application involutive
cet ensemble sur lui-même et l'on peut définir A_1', A_1'', etc. pour $(A, ^*)$
me on l'a fait pour $(F, ^*)$. En particulier, soit K le plus petit sous-
i-groupe de $L(A)$ qui contienne A_2.

l est immédiat que $K \subset E$ et, d'après 3.2, le théorème de Schreier sera
uvé si l'on peut montrer que $K = E$ puisqu'alors $H = \theta A$ sera l'image du
i-groupe libre A par un homomorphisme θ dont le noyau a les propriétés
imales voulues.

oit donc $x \in E$. Si $|x| \leq 2$, il est certain que $x \in K$. Supposons donc
bli pour tous les éléments de longueur $\leq n$ que $x \in E$ entraîne $x \in K$ et
t maintenant $x \in E$ de longueur $n + 1$.

i x est de la forme fyf^*, y appartient à E (d'après U_n) et, par
othèse à K puisque $|y| = n - 1$. D'autre part, comme $E \subset A$, x appartient
A ainsi que xx^*. Mais, $(xx^*)^* = xx^*$ et, par conséquent, $xx^* \in K$ (proposition
2). En particulier, ff^* appartient à K, (puisqu'à E) pour tout $f \in F_1$.

6-06

Donc, en appliquant U_n à $xx^* = fyf^*fy^*f = fy(f^*f)(y^*)f^*$ (où les éléments i appartiennent à K et qui peuvent être éliminés sont mis entre parenthèses) trouve $fyf^* = x \in K$.

Ceci achève la démonstration, puisque, d'après la proposition 3.1, si x n'était s de la forme précédente, on aurait $x = yz$ avec $y, z \in E - e$ et par nséquent de longueur au plus égale à n, et, donc enfin, par hypothèse, , $z \in K$ et $x = yz \in K$.

BIBLIOGRAPHIE

] DUBREIL (Paul). - Contribution à la théorie des demi-groupes, Mem. Acad. Sc. Inst. France, t. 63, n° 3, 1941, p. 1-52.

] DUBREIL (Paul). - Contribution à la théorie des demi-groupes (II), Univ. Roma, Rendic. Mat.., Série 5, t. 10, 1951, p. 183-200.

] LEVI (F.W.). - On semi-groups, Bull. Calcutta math. Soc., t. 36, 1944, p. 141-146.

] LEVI (F.W.). - On semi-groups II, Bull. Calcutta math. Soc., t. 38, 1946, p. 123-124.

] SCHREIER (Otto). - Die Untergruppen der freien Gruppen, Abh. math. Sem. Hamb. Univ., t. 5, 1927, p. 161-183.

] SCHUTZENBERGER (M.P.). - Une théorie algébrique du codage, Séminaire Dubreil et Pisot, 9e année, 1955/56, exposé n° 15.

] STOLL (R.R.). - Homomorphisms of a semigroup onto a group, Amer. J. of Math., t. 73, 1951, p. 475-481.

ТЕОРИЯ ПЕРЕДАЧИ СООБЩЕНИЙ

(Труды Третьей международной конференции)

СБОРНИК СТАТЕЙ

Под редакцией
чл.-корр. АН СССР
В. И. СИФОРОВА

ИЗДАТЕЛЬСТВО
ИНОСТРАННОЙ ЛИТЕРАТУРЫ
МОСКВА, 1957

ПРЕДИСЛОВИЕ

Теория передачи сообщений (теория информации) изучает общие закономерности, присущие как самим сообщениям, так и их передаче при наличии помех. В силу своей весьма большой общности эта теория имеет большое значение для самых разнообразных областей науки и техники. К таким областям относятся, например, радиосвязь, проводная связь, радиолокация, радиотелеуправление, автоматика и телемеханика, техника вычислительных машин, телевидение, физиология, языкознание и т. д.

Теория передачи сообщений является одной из основ современной техники связи, и ее применение к этой области, несомненно, позволит значительно продвинуть решение таких сложных проблем, как повышение эффективности и надежности связи в условиях помех.

Начало общей теории передачи сообщений было положено в работе В. А. Котельникова „О пропускной способности „эфира“ и проволоки в электросвязи“, написанной в 1933 г., в которой автор сформулировал ряд положений и теорем, важных для последующего развития теории передачи сообщений. В 1935 г. была опубликована работа Д. В. Агеева, доказавшая принципиальную возможность увеличения числа каналов радиосвязи в заданном диапазоне частот. В 1947 г. вышла в свет новая работа В. А. Котельникова, где было введено понятие о потенциальной помехоустойчивости. Кроме того, в ней были рассмотрены еще и способы улучшения защиты линий радиосвязи от действия помех.

Наиболее бурное развитие теории передачи сообщений наблюдалось после ставших теперь уже классическими работ американского ученого Клода Шеннона (1947—1948 гг.). За последние восемь лет эта теория стала зрелой и весьма разветвленной отраслью науки, причем общее число научных работ в мировой литературе, посвященных этой теории и ее разнообразным приложениям, уже давно превысило тысячу.

Обсуждению достигнутых результатов и путей решения различных трудных проблем теории передачи сообщений был посвящен ряд международных совещаний ученых различных стран.

В сентябре 1955 г. в Лондоне состоялся третий международный симпозиум по теории передачи сообщений, на котором мне довелось присутствовать. В работе этой конференции приняли участие около 250 ученых Англии, СССР, США, Франции, Голландии, Италии, Федеративной Республики Германии, Швеции, Швейцарии, Дании и других стран. Участники этого совещания обсудили около 50 докладов по различным вопросам теории передачи сообщений и ее применения к электро- и радиосвязи, теории математических машин, физиологии, языкознанию и т. д.

В настоящий сборник включены наиболее интересные из прочитанных на этом совещании зарубежными учеными доклады по общей теории передачи сообщений и теории кодирования, а также по применению этих теорий к технике связи и некоторым проблемам структуры языка и статистики.

Ценность публикуемых докладов заключается не только в том, что в них изложены новые результаты, но также и в том, что в них сформулированы вопросы и проблемы, которые должны быть как можно скорее разрешены совместными усилиями ученых. Попутно нельзя не отметить, что ряд выдвинутых в этих докладах положений еще остается спорным, подлежит дискуссии и требует критического подхода со стороны читателя.

В. И. Сифоров.

I. ОБЩИЕ ВОПРОСЫ ТЕОРИИ ПЕРЕДАЧИ СООБЩЕНИЙ

О НЕКОТОРЫХ МЕРАХ „ИНФОРМАЦИИ", ИСПОЛЬЗУЕМЫХ В СТАТИСТИКЕ [1])

Шютценбергер М. П.

I

Хорошо известно, что понятия информации, которыми пользуются в статистике и в теории связи, различаются как по своему формальному выражению, так и по существу.

В статистике, где задача состоит в оценке значения неизвестного параметра θ путем наблюдения состояния ξ физической системы, априорная вероятность которого $P(\xi/\theta)$ зависит от θ, приходят к выражению

$$F = \sum \left[\frac{\partial P(x/\theta)}{\partial \theta}\right]^2 \frac{1}{P(x/\theta)},$$

где суммирование производится по всем возможным значениям x величины ξ. Целое семейство теорем [2, 4, 6] связывает при различных условиях регулярности величину F с нижней границей дисперсии разности $\theta - \hat{\theta}$ между истинным значением параметра θ и его оценкой $\hat{\theta}$.

С другой стороны, в теории связи количество информации о самой величине ξ обычно оценивается выражением

$$H = -\sum P(x) \log P(x).$$

Интересно, что именно это выражение привлекло к себе значительное внимание, а не более старое выражение для F, введенное Рональдом Фишером еще в 1921 г. [3] и лишь мимоходом рассматривавшееся специалистами по связи.

Однако величины F и H не являются единственными мерами информации по отношению к тому, что содержится в эксперименте, включающем априорную вероятность. Вторая основная задача статистики — проверка на основании информации о величине ξ, какая из гипотез $\theta = \theta_0$ или $\theta = \theta_1$ верна, — естественно приводит к выражению

$$W(\theta_0, \theta_1) = \sum P(x/\theta_1) \log \frac{P(x/\theta_0)}{P(x/\theta_1)}.$$

[1]) Schützenberger M P, On Some Measures of „Information" Used in Statistics (Paris, 1955).

А. Уолд [9] показал, что, каков бы ни был метод проверки (метод последовательного анализа или какой-либо другой), математическое ожидание числа независимых испытаний, необходимых для достижения заданного доверительного уровня, не может быть меньше K/W, где K зависит от вероятности ошибки, определяющей доверительный уровень. Следовательно, W можно назвать *мерой доставляемой через* ξ *информации о дилемме* $\theta = \theta_0$ *или* $\theta = \theta_1$.

Действительно, между F, H и W существует очень тесная связь. Следуя Бартлетту [1], рассмотрим видоизмененное выражение

$$H' = -\sum P(x/\theta) \log P(x/\theta + \varepsilon)$$

и предположим, что $\log P(x/\theta + \varepsilon)$ можно разложить в ряд по возрастающим степеням ε. После некоторых упрощений получим

$H' = H + \varepsilon^2 F +$ члены высшего порядка по ε.

Аналогично, если $\theta_0 = t + \varepsilon$ и $\theta_1 = t - \varepsilon$, где ε бесконечно мало, то можно показать, что случайная переменная

$$z(x) = \log \frac{P(x/\theta_0)}{P(x/\theta_1)},$$

математическое ожидание которой при $\theta = \theta_1$ есть $W(\theta_0, \theta_1)$, имеет распределение со средним значением $2\varepsilon^2 F$ и дисперсией $4\varepsilon^2 F$, с точностью до членов высшего порядка по ε. Более общие соотношения между F и W недавно исследовал Каллбэк [5].

Цель настоящей работы, так же, как и статьи [8], — показать, что эти аналогии имеют глубокие корни в самой природе того, что мы готовы называть „мерой информации". Основной принцип аксиоматики, которую мы попытаемся дать, представляет собой в большей или меньшей степени развитие подхода Вудворда [10] к той же задаче. А именно, производя полное определение ξ, можно остановиться на промежуточном уровне и получить полную информацию путем сложения:

а) члена, соответствующего информации, полученной до этого момента;

б) члена, соответствующего последующей информации, взвешенной подходящими условными вероятностями.

Однако мы ограничимся постулированием этого „принципа Гюйгенса" только для такого промежуточного момента, который наверняка исключает некоторые возможности, и не будем требовать справедливости принципа для всех промежуточных моментов, как это имеет место у Вудворда.

В таком ослабленном виде задача допускает чисто алгебраическое рассмотрение, которое дает, кроме „обычного" H, выражения для F и W как частные случаи более полного решения; это более полное решение можно выразить в явном виде при определенных условиях регулярности.

Для простоты доказательство разбито на две части. Первая часть (условие I и теорема I) применима не только к информации. Она приводит к абстрактному эквиваленту принципа разделения переменных. Вторая часть (условие II и теорема II) определяет специфический характер информации, т. е. вводит функцию $\log P(x)$.

Условия регулярности III и IV, по-видимому, можно ослабить введением другого постулата, выполненного для H, F и W, а именно, условия неотрицательности информаций. Здесь нужны дальнейшие исследования, о чем мы только упомянем вместе с возможностью распространить теорему I на предельный случай при соответствующих ограничениях.

II

Прежде всего заметим, что мы ищем не меру информации, получаемой из *одного* данного результата наблюдений, а меру того количества информации, которое может быть получено *в среднем* с помощью данных средств наблюдения.

Чтобы представить себе общую картину, рассмотрим физическую систему, состояние которой ξ неизвестно. Для простоты будем считать, что ξ может принимать только одно из конечного множества E значений $x, y, z, \ldots$ Практически такое квантование можно предполагать всегда, если бы даже ξ было непрерывной переменной, так как люббе реальное измерение может быть сделано только с конечной точностью.

Априорные вероятности, с которыми ξ может принимать состояния $x, y, \ldots$, будем обозначать через $P(x)$, $P(y), \ldots$, считая при этом, что они являются функциями некоторых неизвестных параметров, обозначаемых через θ.

По отношению к физической системе наблюдатель Ω_i характеризуется степенью точности, с которой он способен распознать ξ. Например, пусть ξ — числовая переменная с возможными значениями $E\{0, 1, 2, 3\}$. Наблюдатель Ω_1 может оказаться не в состоянии узнать о ξ больше, чем то, является ли оно нулем или нет; другой же наблюдатель Ω_2 может оказаться в состоянии лишь установить, является ли ξ четным или нет и т. д.

Поэтому каждому наблюдателю Ω_i соответствует отношение эквивалентности ρ_i между возможными состояниями ξ, или, другими словами, разбиение множества E на такие непересекающиеся подмножества $(X), (Y), (Z), \ldots$, что Ω_i не может различить два состояния, когда они принадлежат к одному и тому же компоненту $(X), (Y), \ldots$, т. е. к одному и тому же „классу эквивалентности" отношения ρ_i [1]).

[1]) Об отношениях эквивалентности см. П. С. Александров, Введение в общую теорию множеств и функций, ОГИЗ — Гостехиздат, М. — Л., 1948, гл. 1, §§ 3, 5. — *Прим. ред.*

Между отношениями эквивалентности на E существует обычное отношение частичного упорядочения $\rho' < \rho$ (ρ' „тоньше" чем ρ, т. е. каждый класс отношения ρ' содержится в каком-либо классе отношения ρ). Оно означает, что наблюдатель Ω' способен обнаружить все те различия между состояниями, что и Ω. Далее, если $\rho' < \rho$ и если X есть класс отношения ρ, то мы обозначим через $\rho'[X]$ („сужение ρ' к X") отношение эквивалентности, индуцируемое отношением ρ' в подмножестве X множества E. Если для некоторого подмножества X $\rho'[X] = \rho''[X]$, мы будем писать $\rho' \equiv \rho''(X)$ („ρ' и ρ'' тождественны на X"). Вооружившись этими понятиями, мы можем теперь сравнить наблюдателей или, вернее, пары наблюдателей.

Определение. *Две пары отношений эквивалентности* (ρ_i, ρ_j) *и* (ρ_k, ρ_l), *где* $\rho_i < \rho_j$ *и* $\rho_k < \rho_l$, *будем считать находящимися в отношении* $\sim$ *тогда и только тогда, когда существует разбиение* E *на два таких непересекающихся подмножества* E' *и* E'', *что*

$$\rho_i \equiv \rho_k(E'), \quad \rho_j \equiv \rho_l(E'), \quad \rho_i \equiv \rho_j(E''), \quad \rho_k \equiv \rho_l(E'').$$

Например, пусть $E = \{a, b, c, d, e, f, g\}$ и

$$\rho_i = (abc)(d)(e)(fg); \quad \rho_j = (abc)(d)(efg);$$
$$\rho_k = (ab)(cd)(e)(fg); \quad \rho_l = (ab)(cd)(efg).$$

Тогда $(\rho_i, \rho_j) \sim (\rho_k, \rho_l)$. Действительно, положив $E' = (efg)$ и $E'' = (abcd)$, получим:

$$\rho_i[E'] = \rho_k[E'] = (e)(fg); \qquad \rho_j[E'] = \rho_l[E'] = (efg);$$
$$\rho_i[E''] = \rho_j[E''] = (abc)(d); \quad \rho_k[E''] = \rho_l[E''] = (ab)(cd).$$

Легко показать, что символ $\sim$ является опять *отношением эквивалентности для множества всех упорядоченных пар, составленных из отношений эквивалентности.* Для этого достаточно заметить, что E'' однозначно определяется из ρ_i и ρ_j $(\rho_i < \rho_j)$ как объединение тех классов, которые являются одновременно классами отношения ρ_i и отношения ρ_j. Заметим, между прочим, что если также $\rho_j < \rho_l$, то $\rho_i < \rho_k$ и $(\rho_i, \rho_k) \sim (\rho_j, \rho_l)$. Поэтому отношение $\sim$ выглядит как абстрактная формулировка отношения равенства между двумя дробями.

Теперь для заданного конечного E рассмотрим множество R всех отношений эквивалентности на E и функцию $f(\cdot)$, отображающую R в некоторую аддитивную группу $\mathfrak{A}$.

Определение. *Функция* $f(\cdot)$ *будет называться нормировкой на* R, *если каждая четверка отношений* $(\rho_i, \rho_j) \sim (\rho_k, \rho_l)$ *влечет* $f(\rho_i) - f(\rho_j) = f(\rho_k) - f(\rho_l)$.

Теорема I. *Любая нормировка* $f(\cdot)$ *множества всех отношений эквивалентности на конечном* E *может быть записана в виде*

$f(\rho) = \sum g(X)$, *где суммирование производится по всем классам* X *отношения* ρ.

Доказательство. Для любого отношения эквивалентности с K классами $\rho = (X)(Y)\ldots(T)$ рассмотрим два других отношения: а) ρ_X — наиболее „тонкое" среди отношений эквивалентности, допускающих класс (X); б) $\rho_{\overline{X}}$ — наиболее „тонкое" среди отношений эквивалентности, допускающих классы $(Y)\ldots(T)$. Пусть ρ_0 — наиболее „тонкое" среди всех отношений эквивалентности, тогда $(\rho_0, \rho_X) \sim (\rho_{\overline{X}}, \rho)$, т. е. если $f(\cdot)$ есть оценка, то $f(\rho) = f(\rho_X) + f(\rho_{\overline{X}}) - f(\rho_0)$. Следовательно, если теорема доказана для всех отношений эквивалентности не более чем с $K-1$ классами, то она доказана для отношений с K классами, так как

$$f(\rho) = \Big[\sum_{x\in X} g(x) + g(Y) + g(Z) + \ldots + g(T)\Big] + \Big[g(X) + \sum_{x\in E-X} g(x)\Big] - \sum_{x\in E} g(x).$$

Выберем для элементов множества E произвольные значения функций $g(x)$ с тем единственным условием, что

$$\sum_{x\in E} g(x) = f(\rho_0),$$

и положим для любого X

$$g(X) = f(\rho_X) - f(\rho_0) - \sum_{x\in X} f(x).$$

Тем самым теорема доказана.

Замечание. Предположим, что на самом деле ρ_0 оказалось не самым „тонким" отношением эквивалентности, а существует еще более „тонкое" отношение ρ_0', отличающееся от ρ_0 только тем, что в ρ_0' класс (X) разбит на (X') и (X''). Каждое отношение эквивалентности ρ_i', менее „тонкое" чем ρ_0', всегда или $> \rho_0$, или имеет вид $(X')(X'')(U)(V)\ldots(W)$, т. е. совпадает на $E-X$ с некоторым $\rho_i > \rho_0$.

Следовательно, в этом случае

$$(\rho_0', \rho_i') \sim (\rho_0, \rho_i) \quad \text{и} \quad f(\rho_i') = f(\rho_i) + f(\rho_0') - f(\rho_0),$$

и $f(\rho_i')$ принимает искомый вид, если выбрав произвольное $g(X')$, положить

$$g(X'') = f(\rho_0') - f(\rho_0) - g(X') + g(X).$$

Предположим теперь, что из $\rho' < \rho$ следует $f(\rho) \leqslant f(\rho') \leqslant f < \infty$, и пусть можно найти такое конечное ρ_0, что $f - f(\rho_0) \leqslant \varepsilon$ и для всех классов Y отношения ρ_0

$$0 < g(Y) \leqslant \eta$$

Тогда такое же условие можно распространить на ρ_0', взяв, например,

$$0 < g(X'') = g(X') = \frac{1}{2}\left[f'(\rho_0') - f(\rho_0) + g(X)\right] < \frac{\varepsilon + \eta}{2}.$$

Это замечание приводит к возможности распространения теоремы I на любое E при соответствующем определении того, что понимается под отношением эквивалентности с бесконечным множеством классов, и при соответствующих ограничениях на $f(\cdot)$.

Возвращаясь к основной цели — измерению информации, мы постулируем следующее условие.

Условие I. *Мера информации $H(\rho_i)$, отнесенной к наблюдателю, является нормировкой на множестве (структуре) R всех отношений эквивалентности на E.*

Точное значение этого условия представляет довольно сильное требование. Именно, если Ω_i отличается от Ω_j такой же способностью к более тонким различениям, как Ω_k от Ω_l, то разности $H(\rho_i) - H(\rho_j)$ и $H(\rho_k) - H(\rho_l)$ должны быть равны. Если угодно, условие I можно истолковать также, уподобляя H стоимости оборудования и требуя, чтобы дополнительные расходы на вспомогательные приспособления, предназначенные для выполнения более тонкого анализа, не зависели от общей стоимости других частей наблюдательного механизма.

Из теоремы I следует только, что если число состояний конечно, то $H(\rho)$ есть сумма членов, зависящих только от классов отношения ρ. Конечно, столь широкое определение не позволяет задать H действительно интересным образом, и мы выставим дальнейшие постулаты.

Условие II. *Если $\rho < \rho'$ и притом для класса V отношения ρ' $\rho \equiv \rho'(E - V)$ (т. е. если Ω отличается от Ω' только дальнейшим разбиением одного из классов), то*

$$H(\rho) = H(\rho') + P(V)\,H(\rho''),$$

где $H(\rho'')$ — мера информации, отнесенной к $\rho'' = \rho[V]$ для наблюдателя, которому известно, что состояние ξ принадлежит к подмножеству V.

К этому условию мы присоединяем:

Условие III. *Вероятности $P(X) = x \neq 0$ суть элементы некоторого топологического коммутативного кольца $\mathfrak{A}$* [1]*, а $H(\rho)$ — непрерывный функционал от x, y, ...*

Условие IV. *Кольцо $\mathfrak{A}$ таково, что, если h_i есть непрерывный функционал, удовлетворяющий для всех a, $b \in \mathfrak{A}$ ($a + b = 1$, $ab \neq 0$) условиям:*

[1]) Грубо говоря, топологическое коммутативное кольцо есть множество, в котором абстрактные операции $+$ и $\times$ определены так, чтобы удовлетворялись обычные условия, за исключением равенства $ab = 0$, которое здесь может оказаться справедливым даже при $a \neq 0$ и $b \neq 0$.

1) $h_1(a+b)=h_1(a)+h_1(b)$, *то* $h_1(\cdot)=\Delta(\cdot)$, *где* $\Delta(\cdot)$ — *линейный функционал*;

2) $h_2(ab)=h_2(a)+h_2(b)$, *то* $h_2(\cdot)=\Delta\log(\cdot)$, *где* $\Delta(\cdot)$ — *линейный функционал*, а $\log(\cdot)$ — *некоторая заданная функция внутри кольца функций над* $\mathfrak{A}$.

Теорема II. *При условии IV необходимым и достаточным условием того, чтобы* $H(\rho)$ *удовлетворяло условиям I, II и III, является равенство*

$$H(\rho)=\sum_x x\,\Delta\log(x),$$

где суммирование производится по классам X *отношения* ρ, *а* Δ *есть любой непрерывный линейный функционал.*

Доказательство. Достаточность является предметом непосредственной проверки. Что же касается необходимости, то условие I влечет

$$H(\rho)=\sum g'(x)=\sum xg(x)$$

для некоторого $g(X)=\frac{1}{x}g'(x)$.

Рассмотрим отношение эквивалентности с четырьмя классами $\rho(X)(Y)(Z)(T)$.

Из условия II при $V=(Y\dot{+}Z\dot{+}T)$ следует

$$H(\rho)=xg(x)+yg(y)+zg(z)+tg(t)=xg(x)+$$
$$+(y+z+t)\,g(y+z+t)+(y+z+t)\left[\frac{y}{y+z+t}\,g\left(\frac{y}{y+z+t}\right)+\right.$$
$$\left.+\frac{z}{y+z+t}\,g\left(\frac{z}{y+z+t}\right)+\frac{t}{y+z+t}\,g\left(\frac{t}{y+z+t}\right)\right].$$

Введем обозначения $y+z+t=s$, $y'=ys^{-1}$, $z'=zs^{-1}$, $t'=ts^{-1}$ и $k(a;\ b)=g(ab)-g(a)-g(b)$. Тогда после перегруппировки членов получим

$$yk(y';\ s)+zk(z';\ s)+tk(t';\ s)=0.$$

В частности, при $t=0$ и тех же значениях x и y

$$yk(y';\ s)+(z+t)\,k(z'+t';\ s)=0.$$

Из двух последних уравнений вычитанием получим

$$(z'+t')\,k(z'+t';\ s)=z'k(z';\ s)+t'k(t';\ s).$$

Следовательно, так как $ak(a,\ b)$ аддитивно по первому аргументу, то, в силу условия IV (1), $ak(a;\ b)=\Delta(a)$, где Δ может зависеть от b, но не от a. Однако $k(a;\ b)$ симметрично по a и b.

Это в свою очередь влечет $k(a; b) = \frac{1}{ab}\Delta_1(ba)$, и приведенное выше уравнение дает

$$\Delta_1(y's) + \Delta_1(z' + t')s = \Delta_1(y) + \Delta_1(z + t),$$

где y и $z + t$ ограничены единственным условием $y + z + t < 1$. Так как Δ_1 аддитивно, то отсюда вытекает $\Delta_1(u) = 0$ для всех $0 < u < 1$, так что

$$k(a; b) = g(ab) - g(a) - g(b) = 0$$

для всех $a, b \in \mathfrak{A}$, $a + b < 1$, $ab \neq 0$.

Теперь ввиду условия IV(2) получим $g(a) = \Delta \log a$, что завершает доказательство.

Замечание 1. Два последовательных условия I и II, содержащиеся в приведенной выше аксиоматике, можно заменить одним постулатом I′ (при выполнении условий III и IV и при конечном E).

Условие I′. Для всех $\rho = (X)(Y)(Z)$, $\rho_1' = (X)(Z \dot{+} Y)$, $\rho_1'' = \rho[E - X] = (Y)(Z)$, $\rho_2' = (X \dot{+} Y)(Z)$, $\rho_2'' = (X)(Z)$ справедливо соотношение $H(\rho_1') + P(X)H(\rho_1'') = H(\rho_2') + P(Z)H(\rho_2'')$.

В самом деле, можно показать, что условие I′ включает условие I. Эта формулировка, которая не содержит понятия нормировки, может быть истолкована как „принцип виртуального разложения наблюдений в последовательные дихотомии", так как она требует, чтобы информация, связанная с различением между принадлежностью ξ к X, Y, Z, могла быть вычислена только лишь на основании информации, связанной с дихотомиями ρ' и ρ''.

Замечание 2. Если ограничиться информацией, зависящей только от численных значений $P(X)$, как в случае теории связи, то условие II можно заменить аддитивностью для сочетания независимых переменных (Вудворд). Тогда, *если оценка непрерывна и зависит только от* $P(X)$, *необходимым и достаточным условием ее аддитивности* для сочетания независимых переменных является ее представимость в виде

$$\sum x \log x.$$

Доказательство. Пусть η и ζ суть две независимые переменные, принимающие соответственно значения $Y_1Y_2Y_3$ и $Z_1Z_2Z_3$, и пусть $\xi = \eta \cdot \zeta$ есть их абстрактное произведение, принимающее 3×3 значений X_{ij} $(i, j = 1, 2, 3)$. Пусть η^* (соответственно ζ^*) есть переменная, полученная из η (соответственно из ζ) путем смешения значений № 2 и № 3. Так как предполагается, что H является нормировкой, то информация $H(\eta \cdot \zeta)$ о величине ξ является суммой $H(\eta \cdot \zeta) = \sum_{ij} x_{ij}\, g(x_{ij})$, которая по предположению равна

$$H(\eta) + H(\zeta) = \sum_i y_i g(y_i) + \sum_j z_j g(z_j).$$

Далее,

$$D = H(\eta \cdot \zeta) - H(\eta \cdot \zeta^*) - H(\eta^* \cdot \zeta) + H(\eta^* \cdot \zeta^*) =$$
$$= H(\eta) + H(\zeta) - [H(\eta) + H(\zeta^*)] - [H(\eta^*) +$$
$$+ H(\zeta)] + H(\eta^*) + H(\zeta^*) = 0.$$

С другой стороны, положив $x_{ij} = P(X_{ij})$, получим

$$D = x_{22}g(x_{22}) + x_{23}g(x_{23}) + x_{32}g(x_{32}) + x_{33}g(x_{33}) -$$
$$- [(x_{22} + x_{23})\, g(x_{22} + x_{23}) + (x_{32} + x_{33})\, g(x_{32} + x_{33}) +$$
$$+ (x_{22} + x_{32})\, g(x_{22} + x_{32}) + (x_{23} + x_{33})\, g(x_{23} + x_{33})] +$$
$$+ (x_{22} + x_{23} + x_{32} + x_{33})\, g(x_{22} + x_{23} + x_{32} + x_{33}) = 0.$$

Предположим теперь, что $z_2 = z_3 = z$. После перегруппировки членов последнее уравнение дает

$$y_2[2g(y_2z) - 2g(2y_2z)] + y_3[2g(y_3z) - 2g(2y_3z)] -$$
$$- (y_2 + y_3)\{2g[(y_2 + y_3)z] - 2g[2(y_2 + y_3)z]\} = 0.$$

Воспользовавшись обозначением $g(ab) - g(2ab) = k(a;\ b)$, получим равенство

$$y_2k(y_2;\ z) + y_3k(y_3;\ z) = (y_2 + y_3)\, k(y_2 + y_3;\ z),$$

из которого следует (так как непрерывность постулирована), что $k(y_i;\ z)$ не зависит от y_i.

Так как $k(y_i;\ z)$ симметрична по y_i и z, то она является постоянной K. Положив $u = y_iz$, окончательно получим

$$g(u) - g(2u) = K \quad \text{для всех} \quad 0 \leqslant u < 1.$$

Отсюда следует справедливость теоремы, так как мы получили уравнение Шрёдера, имеющее, как известно [7], единственное решение

$$g(u) = K \log u.$$

Заметим, что доказательство не удалось бы, если бы мы не предположили, что g и k суть числовые функции, так как нельзя было бы доказать, что $k(a;\ b)$ является постоянной. Действительно, в более общем случае не только информация, но и результаты применения линейных операций к ней (т. е. выражения вида $\sum \Delta_1(x\, \Delta_i \log x)$) удовлетворяют требованию аддитивности для сочетания независимых переменных.

III

Теперь, когда мы получили общее выражение для меры информации, необходимо связать оператор Δ с тем, к чему относится соответствующая информация и что пока еще не было нами определено. Мы не намного продвинулись в этом направлении, но

приводимые ниже соображения могут послужить намеками на полный ответ.

Теорема. *Если имеется такая функция* $\tau(\xi) = \zeta$, *что для всех* ξ (*условные*) *значения* $P(\xi/\zeta)\,\Delta \log P(\xi/\zeta)$ *равны нулю, то* Δ*-информации о* ξ *и о* ζ *равны.*

Доказательство. Достаточно убедиться, что формула для условных информаций справедлива в общем случае, т. е. если ξ и η — две переменные, а $H(\xi \cdot \eta)$ — информация о ξ и η, то

$$H(\xi \cdot \eta) = H(\eta) + E_\eta H(\xi/\eta)$$

(где правая часть есть сумма информации о η и математического ожидания условной информации о ξ при известном η). Если теперь $\zeta = \eta$ функционально связана с ξ, то

$$H(\xi \cdot \zeta) = H(\xi) = H(\zeta),$$

так как, по предположению, $H(\xi/\zeta) = 0$.

Например, пусть Δ есть оператор $[\ ]_{\theta=\theta_1}^{\theta=\theta_0}$ (значение при $\theta = \theta_0$ минус значение при $\theta = \theta_1$, где θ — неизвестный параметр, от которого зависит $P(\xi)$). С его помощью описывается информация W. Предположим, что распределение ξ можно представить в виде

$$P(\xi = \xi_0) = P(\zeta = \zeta_0)\,P(\zeta' = \zeta'_0),$$

где ζ — функция от ξ, а $P(\zeta' = \zeta_0)$ имеет одинаковые значения для $\theta = \theta_0$ и $\theta = \theta_1$. Хорошо известно, что в этом случае ζ представляет „*достаточную статистику*" для проверки $\theta = \theta_0$ или $\theta = \theta_1$.

Информация *T*. Следующий пример будет рассмотрен несколько подробнее, так как он является единственным примером подлинной „информации", если не считать классических H, F и W.

Пусть дано множество переключателей $a_1 a_2 \ldots a_i \ldots\ i \in I$, которые могут быть разомкнуты ($a_i = 0$) или замкнуты ($a_i = 1$) независимо друг от друга, причем вероятность разомкнутого состояния одинакова для всех и равна ω.

Рассмотрим множество произведений

$$A_1 = \prod_{i \in I_1} a_i, \quad A_2 = \prod_{i \in I_2} a_i, \ \ldots, \ A_k = \prod_{i \in I_k} a_i,$$

где I_j суть заданные подмножества множества I. Наблюдение заключается в проверке одновременного выполнения равенств $A_1 = A_2 = \ldots = A_k = 0$.

Нужно определить, для какого числа (ν) переключателей можно *доказать* с помощью такого наблюдения, что они в среднем разомкнуты. Конечно, если мы знаем только, что *не все* A_j равны нулю, то ничего *доказать* нельзя. Обозначим вероятность этого случая через Q.

Наоборот, если *все* $A_j = 0$ (с априорной вероятностью $P = 1 - Q$), то по крайней мере некоторые из A_i должны быть разомкнуты, причем их минимальное количество зависит от комбинаций, в которых a_i входят в множество произведений A_j. Например, если $A_1 = a_1a_2a_3$, $A_2 = a_1a_4a_5$, $A_3 = a_2a_4$, то ν равно двум, что соответствует трем возможностям:

$$a_1 = a_2 = 0; \qquad a_1 = a_4 = 0; \qquad a_2 = a_4 = 0.$$

Введем оператор Δ^* — произведение ω на частную производную по ω при $\omega = 0$:

$$\Delta^* = \left[\omega \frac{\partial}{\partial \omega}\right]_{\omega=0}$$

Соответствующая информация равна

$$T = P\Delta^* \log P + Q\Delta^* \log Q.$$

Так как событие вероятности Q может случиться даже, когда все a_i замкнуты, то Q имеет вид $1 - \omega^\alpha R$, где R — многочлен с ненулевым постоянным членом, так что

$$\Delta^* \log Q = \left[\frac{-\omega(\omega^\alpha R' + \alpha\omega^{\alpha-1}R)}{1-\omega^\alpha R}\right]_{\omega=0} = 0.$$

С другой стороны, $P = \omega^\alpha R$, где α в точности равно тому минимальному числу переключателей (ν), которые должны быть разомкнуты для того, чтобы удовлетворялось равенство $A_1 = A_2 = \ldots = A_k = 0$.

В этом легко убедиться прямым вычислением. Тогда

$$\Delta^* \log P = \left[\omega\left(\frac{\alpha}{\omega} + \frac{R'}{R}\right)\right]_{\omega=0} = \alpha = \nu,$$

а T в точности равно среднему значению νP этого минимального числа.

С познавательной точки зрения интересно отметить, что T представляет собой промежуточное понятие между случаем отсутствия шумов, когда H служит рациональным инструментом, и случаем наличия шумов, когда ведущую роль играет W или F, в соответствии с функцией стоимости, которая задается внутренней топологией „сообщений" (последние при наличии шума суть параметры θ, а не ξ).

В самом деле, T введено в „полудетерминистическом случае", когда только некоторые сообщения (в данном случае сообщение „все $A_j = 0$") допускают абсолютно безусловную интерпретацию.

ЛИТЕРАТУРА

1. Bartlett M. S., *Proc. London Symp. Inf. Theory*, p. 81 (1950).
2. Darmois G., *Rev. Inst. Int.* Stat. (1945).
3. Fisher R. A., *Phil. Trans. Roy. Soc.*, A 22, 309 (1921).
4. Frechet M., *Rev. Inst. Int. Stat.*, (3/4) p. 182 (1942).
5. Kullback, *Ann. Math. Stat.*, 2, 745 (1954).
6. Rao G. Q., *Bull. Calcutta Math. Soc.*, 37, 81 (1945).
7. Schröder, *Math. Ann.*, 3, 296 (1871).
8. Schützenberger M. P., *Pub. Inst. Stat. Univ. Paris*, 3, 27 (1953).
9. Wald A., Sequential Analysis, Wiley and Son, N. Y. (1947).
10. Woodward, *Proc. IEE* (1952).

INSTITUT DE STATISTIQUE
DE L'UNIVERSITÉ DE PARIS

CAHIERS DU BUREAU UNIVERSITAIRE DE RECHERCHE OPÉRATIONNELLE

Cahier n° 2

1957
PARIS
INSTITUT HENRI POINCARÉ

SUR UNE GÉNÉRALISATION DE L'INÉGALITÉ MINIMAX

par

Marcel-Paul SCHÜTZENBERGER

INTRODUCTION

Soit donné un ensemble : $A = (a_j^i)$ $(i = 1, 2, \ldots, n\ ;\ j = 1, 2, \ldots, m)$ de $(n.m)$ valeurs numériques .

L'inégalité dite "minimax" :

$$\operatorname{Min}_i \operatorname{Max}_j a_j^i \geqslant \operatorname{Max}_j \operatorname{Min}_i a_j^i$$

joue un rôle fondamental dans la théorie des jeux et la recherche opérationnelle. Or cette inégalité ne fait appel, pour sa démonstration, qu'aux propriétés les plus élémentaires des opérations associées à la relation $(\leqslant)$ entre grandeurs. Il peut donc présenter un certain intérêt de savoir dans quelle mesure elle se généralise quand on substitue aux opérations "Min" et "Max" des opérations consistant à prendre non plus seulement le premier (min) et le dernier (max) d'un ensemble d'éléments rangés dans l'ordre des grandeurs croissantes mais, plus généralement, le "p-ième". Ce que nous noterons par $\overset{(p)}{M}$. On a : Min = $\overset{(1)}{M}$; Max = $\overset{(N)}{M}$ (si N est le nombre des éléments de l'ensemble).

Comme les a_j^i n'interviennent que par leur grandeur relative il est sans importance de les remplacer par les $n.m$ valeurs $1, 2, \ldots, n.m$ et les raisonnements seront sans doute plus faciles à suivre si nous examinons d'abord l'exemple numérique ci-dessous.

EXEMPLE

Soit A =

$$\begin{vmatrix} 20 & 14 & 1 & 4 & 17 \\ 6 & 10 & 19 & 18 & 16 \\ 15 & 3 & 7 & 13 & 5 \\ 2 & 8 & 9 & 11 & 12 \end{vmatrix}$$

4

A partir de A construisons les deux tableaux B = Col. A et C = Lig. A obtenues en réarrangeant par ordre de grandeurs les éléments de chaque colonne (ligne) :

$$B = \begin{vmatrix} 2 & 3 & 1 & 4 & 5 \\ 6 & 8 & 7 & 11 & 12 \\ 15 & 10 & 9 & 13 & 16 \\ 20 & 14 & 19 & 18 & 17 \end{vmatrix} \qquad C = \begin{vmatrix} 1 & 4 & 14 & 17 & 20 \\ 6 & 10 & 16 & 18 & 19 \\ 3 & 5 & 7 & 13 & 15 \\ 2 & 8 & 9 & 11 & 12 \end{vmatrix}$$

Réarrangeons maintenant B par ligne et C par colonne. Nous obtenons

$$D = \text{Lig. } B = \text{Lig. Col. } A = \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 11 & 12 \\ 9 & 10 & 13 & 15 & 16 \\ 14 & 17 & 18 & 19 & 20 \end{vmatrix}$$

$$E = \text{Col. } C = \text{Col. Lig. } A = \begin{vmatrix} 1 & 4 & 7 & 11 & 12 \\ 2 & 5 & 9 & 13 & 15 \\ 3 & 8 & 14 & 17 & 19 \\ 6 & 10 & 16 & 18 & 20 \end{vmatrix}$$

Désignant par des lettres minuscules les éléments des tableaux correspondants il résulte de la construction même et selon des notations évidentes :

$$(1) \qquad b_k^i = \overset{k}{M}\, a_j^i \; ; \; c_j^h = \overset{h}{M}\, a_j^i \; ; \; d_k^h = \overset{h}{M}_i\, b_k^i = \overset{h}{M}_i\, \overset{k}{M}_j\, a_j^i \; ; \; e_k^h = \overset{k}{M}_j\, c_j^h = \overset{k}{M}_j\, \overset{h}{M}_i\, a_j^i$$

Il apparaît sur l'exemple choisi un phénomène remarquable : les éléments de D situés dans l'angle supérieur droit sont systématiquement plus petits que les éléments correspondants de E et l'inverse est vrai pour l'angle inférieur gauche.

En particulier on retrouve bien :

$$\operatorname{Max}_j \operatorname{Min}_i a_j^i \leqslant \operatorname{Min}_i \operatorname{Max}_j a_j^i$$

(soit ici $5 < 12$)

Le lecteur pourra d'ailleurs vérifier en prenant au hasard des valeurs a_j^i que ces particularités n'ont rien d'exceptionnel et le problème se pose donc de savoir quelles sont les conditions nécessaires et suffisantes pour que

$$(2) \qquad \overset{(h)}{M}_{(i)}\, \overset{(k)}{M}_{(j)}\, a_j^i \leqslant \overset{(k)}{M}_{(j)}\, \overset{(h)}{M}_{(i)}\, a_j^i$$

CALCUL DE $\overset{h}{M}_i$

Il est bien connu que, N quantités numériques u^i étant données, la fonction latticielle symétrique $\overset{(h)}{M}_i u_i$ est obtenue aussi bien par l'une que par l'autre des deux formules suivantes :

(3) $\overset{(\alpha)}{M}_i u^i$ = "Somme" de tous les "produits" $(N-\alpha+1)$ à $(N-\alpha+1)$ des u^i

(3') $\overset{\alpha}{M}_i u^i$ = "Produit" de toutes les "sommes" α à α des u^i.

Les mots "Somme" et "Produits" devant être entendus dans leur sens latticiel, c'est-à-dire que :

- "Somme" des éléments d'un ensemble X = les plus grands éléments de X,
- "Produit" des éléments de X = le plus petit élément de X.

Par exemple : Si $[x \leqslant y \leqslant z \leqslant t] = X$ on a :

$\overset{1}{M}X = xyzt = x = \text{Min } X =$ Produit de x, y, z et t

$\overset{2}{M}X = xyz + xyt + xzt + yzt = x + x + x + y = y$

ou $= (x+y)(x+z)(x+t)(y+z)(y+t)(z+t) = yztyyz = y$

$\overset{3}{M}X = xy + xz + xt + yz + yt + zt = x + x + xy + y + z = z$

ou $(x+y+z)(x+y+t)(x+z+t)(y+z+t) = zttt = z$

$\overset{4}{M}X = x + y + z + t = t = \text{Max } X =$ "Somme" de x, y, z et t

On sait que les opérations "Somme" et "Produit" sont à la fois associatives, commutatives, absorbantes ($x(x+y) = x + xy = x$) et distributives ($x(x+z) = xy + xz$; $(x+y)(x+z) = x+yz$) et on observera que la définition (3) ou (3') donne un sens à $\overset{\alpha}{M}$ même quand plusieurs des quantités considérées sont égales entre elles. Par exemple, si $x = y$: $\overset{1}{M}X = \overset{2}{M}X$ = la valeur commune de x et de y.

CALCUL DES $\overset{\alpha}{M}_i \overset{\beta}{M}_j$

D'après (3) on a pour un β fixé :

$d^{\alpha}_{\beta} = \overset{\alpha}{M}_i \overset{\beta}{M}_j a^i_j$ = "Somme" des "Produits" $(n-\alpha+1)$ à $(n-\alpha+1)$ des b^i_{β}

et encore d'après (3) pour un i fixé :

b^i_{β} = "Somme" des "Produits" $(n-\beta+1)$ à $(n-\beta+1)$ des a^i_j

Donc, en vertu de la distributivité des deux opérations l'une sur l'autre et compte tenu de leur associativité :

6

d^{α}_{β} = "Somme" de tous les "Produits" d_k de tous les éléments appartenant à un ensemble D_k obtenu lui-même en choisissant un ensemble A_k de $n-\alpha+1$ colonnes de A et dans chacune de celles-ci $m-\beta+1$ éléments a^i_j.

k parcourt un ensemble K comprenant $\begin{bmatrix} n \\ n-\alpha+1 \end{bmatrix}$ $\begin{bmatrix} m \\ m-\beta+1 \end{bmatrix}$ indices distincts et :

$$(4) \qquad d^{\alpha}_{\beta} = \sum_{k \in K} d_k \qquad \text{où} \qquad d_k = \prod_{a^i_j \in D_K} a^i_j$$

$$(4') \qquad e^{\alpha}_{\beta} = \prod_{\ell \in L} e_\ell \qquad \text{où} \qquad e_\ell = \sum_{a^i_j \in E\ell} a^i_j$$

E_ℓ étant obtenu en choisissant α éléments a^i_j dans chacune des β lignes d'un ensemble B_ℓ ($\ell \in L$).

Pour la suite, nous aurons avantage à introduire encore les notations suivantes relatives à un $k \in K$ et un $\ell \in L$ fixés :

$A_1 = a^i_j$ tel que: $i \in A_k$ $j \in B_\ell$

$A_2 = a^i_j$ " $i \in A_k$ $j \notin B_\ell$

$A_3 = a^i_j$ " $i \notin A_k$ $j \in B_\ell$

Donc : $D_k \subset A_1 \cup A_2$; $E_\ell \subset A_1 \cup A_3$

CONDITIONS DE VALIDITÉ IDENTIQUE DE L'INÉGALITÉ (2)

Il est bien connu que quelque soient x, y et z on a identiquement : $xy \leqslant x \leqslant x+z$ les opérations ayant évidemment leur sens latticiel. En particulier, quelque soient les u^i [3] implique $M^{\alpha}_i u^i \leqslant M_i u^i$ et, d'autre part, si $u^i \leqslant v^i$ pour tout i, alors $M^{\alpha}_i u^i \leqslant M_i v^i$.

Donc si $\alpha \leqslant \alpha'$ et $\beta \leqslant \beta'$:

$$M^{\alpha}_i M^{\beta}_j a^i_j \leqslant M^{\alpha'}_i M^{\beta'}_j a^i_j$$

ce qui s'interprète immédiatement sur les tableaux D et E. Revenons à l'inégalité (2). Celle-ci s'écrit :

$$d^{\alpha}_{\beta} = \sum d_k \leqslant e^{\alpha}_{\beta} = \prod e_\ell$$

et est donc satisfaite sauf si $e_{i_1} \leqslant d_{k_1}$ pour au moins un couple d'indices $k_1 \in K$ et $l_1 \in L$. Mais si les ensembles D_k et E_i possédaient un élément $a^{i_1}_{j_1}$

commun on aurait $d_k \leqslant a^{i}_{j_1} e_1$ et, par conséquent, (2) ne peut se trouver en défaut que si les deux conditions suivantes sont satisfaites :

(5) Il existe au moins un couple (D_{k_1}, E_{l_1}) tel que $D_{k_1} \cap E_{l_1} = 0$

(6) $d_{k_1} = \mathrm{Min}\, D_{k_1}, e_{l_1} = \mathrm{Max}_{l_1}$

En particulier, puisque D_k contient $(n-\alpha+1)(m-\beta+1)$ éléments et $E, \alpha\beta$, il sera possible de satisfaire à (5) si :

(7) $(n-\alpha+1)(m-\beta+1) + \alpha\beta > n + (n-\alpha+1)\, m - \beta(n-\alpha+1)$ c'est-à-dire si :

(7') $(\beta-1)(n-\alpha) > 1$

puisque le membre de droite de (7) est le nombre des cases de l'ensemble $A_1 \cup A_2 \cup A_3$. On trouve ainsi une généralisation de l'inégalité Minimax :

(2) $\mathrm{Max}_i \overset{\beta}{M}_j a^{i}_{j} \leqslant \overset{\beta}{M}_j \mathrm{Max}_i \leqslant a^{i}_{j}$ pour tout β $(1 \leqslant \beta \leqslant m)$

$\overset{\alpha}{M}_i \mathrm{Min}_j a^{i}_{j} \leqslant \mathrm{Min}_j \overset{\alpha}{M}_i a^{i}_{j}$ pour tout α $(1 \leqslant \alpha \leqslant n)$.

Supposons maintenant que $\beta \neq 1$ et $\alpha \neq n$ et montrons que l'on peut satisfaire à (5), A_k et B_ℓ étant fixés.

En effet, dans chaque colonne de A_k, $m-\beta+1$ éléments a^{i}_{j} seulement figurent dans D_k. On peut donc choisir cet ensemble de telle façon que $m-\beta+1-(m-\beta) =$ un seul a^{i}_{j} par colonne se trouve dans A_1 et de même pour les lignes. D'où le résultat puisque A_1 étant un rectangle qui comporte au moins deux lignes et deux colonnes il est possible de faire en sorte que ces deux derniers ensembles de a^{i}_{j} soient disjoints.

Comme (6) peut toujours être satisfaite, il en résulte que (2) est le seul cas où (2) soit identiquement vérifié. Exemple : $n = m = 4$. Pour le tableau suivant on a :

$$8 = \overset{3}{M}_i \overset{2}{M} a^{i}_{j} > \overset{2}{M}_j \overset{3}{M}_i a^{i}_{j} = 7$$

(A_k : les colonnes 2 et 4 ; B_{l_1} les lignes 2 et 3)

$$A = \begin{vmatrix} 11 & 8 & 16 & 13 \\ 3 & 14 & 1 & 7 \\ 6 & 2 & 5 & 9 \\ 4 & 12 & 10 & 15 \end{vmatrix} \quad B = \begin{vmatrix} 3 & 2 & 1 & 7 \\ 4 & 8 & 5 & 9 \\ 6 & 12 & 10 & 13 \\ 11 & 14 & 16 & 15 \end{vmatrix} \quad C = \begin{vmatrix} 8 & 11 & 13 & 16 \\ 1 & 3 & 7 & 14 \\ 2 & 5 & 8 & 9 \\ 14 & 10 & 12 & 15 \end{vmatrix}$$

$$D = \begin{vmatrix} 1 & 2 & 3 & 7 \\ 4 & 5 & 0 & 9 \\ 6 & 10 & 12 & 13 \\ 11 & 14 & 15 & 16 \end{vmatrix} \quad E = \begin{vmatrix} 1 & 3 & 6 & 9 \\ 2 & 5 & 0 & 14 \\ 4 & 10 & 12 & 15 \\ 8 & 11 & 13 & 16 \end{vmatrix}$$

8

Validité limite de (2)

Il apparaît cependant vraisemblable pour des raisons de symétrie que si β/m est plus petit que α/n (2) doit être "généralement vraie" dans un sens qui reste à préciser. Nous le ferons ici très simplement sous les hypothèses suivantes :

1°- $n = m$ tend vers l'infini

2°- $\beta = n-\alpha+1$ est l'entier le plus voisin de λn ou λ est une constante finie $\ll 1/2$

3°) Les $(n^2)!$ permutations possibles des a_j^i sont équiprobables.

$\overset{\beta}{M}$ est donc le "λ-ième quantile inférieur" $\overset{\lambda}{M}$ et nous chercherons à prouver que si λ est assez petit, zéro est la limite quand $n \to \infty$ de la probabilité P que :

(2°) $\overset{1-\lambda}{M}_i \; \overset{\lambda}{M}_j \; a_j^i > M_j \; \overset{1-\lambda}{M}_i \; a_j^i$

quand les a_j^i sont tirés au sort indépendamment et selon une seule et même loi de probabilité.

Appelons $E_{k,\ell}$ l'événement consistant en ce que (6) soit vérifié pour un couple (D_k, E_ℓ). On a :

(8) $P < \Sigma \Pr(E_{k,\ell})$ où la sommation est étendue à tous les couples (D_k, E_ℓ) tels que $D_k \cap E_\ell = \emptyset$. En raison de la symétrie (8) peut s'écrire :

(8') $P \begin{bmatrix} n \\ \lambda n \end{bmatrix}^2 \times Q \times P_o$ où :

$P_o = \Pr(E_{k,\ell})$ est indépendant des indices k et l.

Q est le nombre des façons de choisir D_k et E_ℓ disjoints quand A_k et B_ℓ sont fixés.

$\begin{bmatrix} n \\ n\lambda \end{bmatrix}^2$ = est le nombre des façons de choisir A_k et B_ℓ.

La seule difficulté réside dans le calcul de Q. En effet, D_k et E_ℓ étant fixés et contenant chacun $n' = \lambda n\,(n-\lambda+1)$ éléments la probabilité pour que (6) soit vraie est :

(9) $P_o = \begin{bmatrix} 2n' \\ n \end{bmatrix}^{-1} = \exp\left(-n^2(\lambda - \lambda^2)\, 2 \operatorname{Log} 2 + O(n^2)\right)$.

Au lieu de calculer Q nous calculerons Q' qui en est une estimation grossière pour λ voisin de $1/2$ mais suffisante pour λ petit.

Q' = Nombre des façons de prendre deux ensembles D' et E' de n' éléments chacun de telle sorte que $D' \subset A_1 \cup A_2$; $E' \subset A_1 \cup A_3$ et $D' \cap E' = \emptyset$.

Supposons qu'en outre il soit fixé que X éléments de D' et Y éléments de E' sont dans A_1 qui contient $\lambda^2 n^2$ cases, on a :

$$Q'_{ky} = \frac{(\lambda^2 n^2)!}{X!\,Y!\,(\lambda^2 n^2 - X - Y)!} \begin{bmatrix} n^2(\lambda-\lambda^2) \\ n'-X \end{bmatrix} \begin{bmatrix} n^2(\lambda-\lambda^2) \\ n'-Y \end{bmatrix} \quad \text{Donc :}$$

$Q' = \sum Q'_{x,y}$ où la sommation est étendue à toutes les valeurs de X et de Y telles que $X+Y \leqslant \lambda^2 n^2$. Posons

$$X = x\,\lambda^2 n^2 \quad \text{et} \quad Y = y\,\lambda^2 n^2$$

$$H(u) = u \log 1/u + (1-u) \operatorname{Log} 1/(1-u) ;$$

$$H(x,y) = x \operatorname{Log} 1/x + y \operatorname{Log} 1/y + (1-x-y) \operatorname{Log} 1/(1-x-y)$$

il vient

$$\operatorname{Log} Q'_{xy} = n^2 \lambda^2 H(x,y) + n^2(\lambda-\lambda^2)\left(H\left(\frac{x\lambda}{1-\lambda}\right) + H\left(\frac{y\lambda}{1-\lambda}\right)\right) + o(n^2)$$

$$= n^2(\lambda-\lambda^2)\, F_\lambda(x,y) + o(n^2)$$

Q'_{xy} étant exponentiellement convexe en x et en y tend pour n croissant vers $(\exp n^2(\lambda-\lambda^2)F_\lambda)$ ou F_λ est le maximum en x,y de $F_\lambda(x,y)$.

D'après (8') et (9) le résultat sera donc établi quand on pourra prouver que :

$$F_\lambda < 2 \operatorname{Log} 2 \tag{10}$$

Observons d'abord que $F(x,y)$ n'atteint son maximum que si $x = y$. Dans ce cas : $F_\lambda(x,x) = 2H\left(\frac{x\lambda}{1-\lambda}\right) + \frac{2\lambda}{1-\lambda} \times L\,2 + \frac{\lambda}{1-\lambda} H(2x)$ qui pour $x = 1/2$ est certainement plus grand que 2 log 2 quand λ est voisin de $1/2$. Par contre, $F_\lambda(x,x)$ croissant en λ, tend uniformément vers zéro avec cette quantité. Il existe donc une valeur λ_0 finie telle que (2°) soit satisfaite à la limite quand $n \longrightarrow \infty$ si $\lambda < \lambda_0$.

Références sur les treillis

G. BIRKHOFF. Lattice Theory, New York 1948, Chap. III.

M. L. DUBREIL-JACOTIN, , L. LESIEUR et R. CROISOT - Theorie des Treillis (Paris 1953).

ENCYCLOPÉDIE FRANÇAISE

CAHIERS D'ACTUALITÉ ET DE SYNTHÈSE

LA CYBERNÉTIQUE

par L. COUFFIGNAL et M.P. SCHÜTZENBERGER

CONSTRUCTION SÉMANTIQUE DE LA LOGIQUE

par E. W. BETH

MATHÉMATIQUES

mises à jour détaillées rédigées sous la direction de Paul MONTEL

I

SOCIÉTÉ NOUVELLE DE L'ENCYCLOPÉDIE FRANÇAISE
Dépositaire Général : Librairie Larousse *13-21, rue du Montparnasse, PARIS VI^e^*

LA CYBERNETIQUE

2. - *La théorie de l'information*

INTRODUCTION

Il est classique de comparer à l'énergétique la théorie de l'information. La première aurait pour but l'étude des systèmes dans lesquels une certaine quantité d'énergie se produit ou se transforme — la seconde aurait le même rôle, mais relativement à une nouvelle grandeur : l'*information*. A l'énergétique appliquée correspondraient les machines qui ont été le triomphe de la technologie du XIX^{e} siècle : locomotive ou alternateur électrique. A la théorie de l'information reviendrait de faire les plans de ces mécanismes nouveaux que sont les calculatrices électroniques, les appareils de télévision, etc.

On peut ainsi poursuivre ces analogies assez loin, jusqu'au point même où les deux théories se rencontrent parce que l'on doit discuter les rapports mutuels entre les quantités d'énergie et d'information simultanément mises en jeu dans certains processus. Cependant une différence irréductible subsiste. Les deux théories correspondent à des idéalisations opposées de la réalité et comme nous le montrerons en détail plus loin, la seconde commence à ce point précis où sont postulées négligeables les quantités qui étaient l'objet même des recherches de la première.

Dans une perspective entièrement différente, des auteurs, moins techniciens que philosophes peut-être, ont voulu trouver dans la théorie nouvelle les fondements d'une science radicalement originale qui livrerait les clés de la signification et on a tenté ainsi, plus ou moins sérieusement, de rattacher la sémantique aux résultats des spécialistes en télécommunications.

Entre ces deux points de vue extrêmes, sinon dans leur but, tout au moins dans leur dépassement des possibilités actuelles, il nous semble

préférable (*) de ne conserver de la première analogie que le principe des démarches de la physique théorique et de ne garder de la seconde que la présence d'entités nouvelles et notamment de « *sujets* » dont il faudra avant toute chose élucider les comportements.

Enfin, on ne saurait oublier que la théorie des communications, en tant que discipline appliquée, a une fonction normative : non contente de théoriser ce qui est ou ce qui peut être, elle doit fournir à l'ingénieur des critères raisonnables de décision qui, par nature, sont partiellement absolus, mais aussi partiellement arbitraires. En ceci encore, elle se distinguera donc des autres théories physiques auxquelles nous emprunterons le schéma initial d'analyse :

— décomposition de l'objet étudié en une série d'éléments plus simples ;

— fixation des principes de fonctionnement de chacune de ces parties ;

— calcul d'approximation permettant la synthèse des éléments constitutifs relativement à un principe extrémal d'optimalité.

LES ELEMENTS D'UN DISPOSITIF DE COMMUNICATION

Prenons, pour fixer les idées, l'exemple le plus courant d'un réseau télégraphique :

En suivant, depuis le début, la marche des opérations, nous y rencontrerons les articulations suivantes :

Emission

1) *L'expéditeur* compose le texte du télégramme.

Codage

2) L'agent du poste émetteur transforme la suite des lettres et signes typographiques, en une suite d'impulsions électriques qui sont envoyées sur un circuit électrique (matériel ou non).

Transmission

3) Les impulsions cheminant sur ce circuit sont soumises à des perturbations diverses (distorsion, « fading », parasites atmosphériques ou autres).

Décodage

4) Un second agent déchiffre les indications reçues et recompose en caractères typographiques usuels un texte qui est remis au destinataire.

Réception

5) Au reçu du télégramme, ce dernier prend une certaine décision, telle qu'aller attendre son correspondant à la gare à une certaine heure, effectuer telle ou telle opération commerciale, etc.

Enfin :

Bilan

6) Un bilan est établi qui chiffre d'une part le coût du télégramme, d'autre part le bénéfice ou la perte qu'a fait réaliser effectivement sa transmission plus ou moins rapide et correcte.

Si on le voulait, on pourrait voir, dans ce schéma un « modèle canonique de communication » et, en effet, les étapes que l'on vient d'énumérer se retrouvent quoique avec une importance variable dans tout processus de communications concevable. Nous conviendrons en outre de décomposer tout échange d'information (un dialogue par exemple) en une série de tels cycles dans lesquels le même individu peut d'ailleurs changer de rôle d'un cycle à un autre. L'identification est au demeurant toujours assez facile encore que l'opération « bilan » puisse paraître assez artificielle. C'est pourtant elle, comme nous le verrons plus loin, qui est la clé de voûte de toute la théorie.

1) L'émission. — Par hypothèse, un « émetteur » choisit un message à expédier dans une certaine liste de messages possibles. L'émetteur est le premier « sujet » que nous ayons à introduire. Par ce terme nous entendons d'ailleurs pour le moment une propriété négative : le comportement de l'émetteur ne *peut* pas être prévu exactement, car en effet si l'on savait quel message va être choisi il n'y aurait pas besoin de communication du tout. Ceci dit, l'émetteur peut être soit *passif*, c'est-à-dire considéré comme choisissant au hasard selon des probabilités fixes et connues, les différents messages, soit *actif*, c'est-à-dire agissant de façon entièrement autonome et imprévisible. Le cas du sujet actif sera traité plus en détails quand nous parlerons des principes de comportement.

Le deuxième aspect important de l'émission est l'existence d'une liste finie ou infinie, mais en tous cas *connue* de messages possibles : c'était l'ensemble des suites de signes typographiques composant un texte français dans notre exemple initial, mais ce serait aussi bien :

— l'ensemble des plages lumineuses plus ou moins éclairées formant une image susceptible d'être vue par une caméra de télévision ;

— l'ensemble de 3 lettres et 4 chiffres composant le numéro d'appel à un standard téléphonique ;

— une valeur numérique dans ce processus informationnel très spécial qu'est la mesure d'une grandeur physique (longueur, poids, voltage, etc.) ;

— un symbole dichotomique (« oui » ou « non ») fourni par un dispositif avertisseur par exemple.

L'existence de cette liste ne semble pas une restriction a priori puisque la liste peut être aussi longue et aussi complexe que l'on veut, mais elle a cependant une conséquence fondamentale : nous pouvons, dès le début, assigner à chacun des messages possibles un numéro d'ordre (au sens usuel

(*) Le point de vue qui sera adopté ici est celui qui avait guidé un séminaire sur la théorie des informations organisé en 1954-1955 dans le cadre de la chaire de Calcul des Probabilités de M. le Pr. G. DARMOIS par B. MANDELBROT et M. P. SCHÜTZENBERGER. Bien que ce dernier soit seul responsable de la forme donnée ici à cet exposé, son contenu reflète un point de vue commun développé au cours de longues et amicales discussions.

ou dans un sens généralisé) et considérer que la communication ne porte que sur ce numéro d'ordre, à l'exclusion de tout contenu sémantique du message qu'il repère. Ainsi – et c'est là qu'est la restriction essentielle — la théorie de l'information ne porte-t-elle que sur les « *signifiants* » et non sur les « *signifiés* » pour reprendre la distinction fameuse de SAUSSURE. Tout comme le nombre « 245 » désigne les propriétés collectives de tout ensemble formé de 245 objets distincts indépendamment de leur nature propre, le système de communication dont l'ensemble des messages possibles est « oui » ou « non » peut être étudié en soi sans tenir compte de ce que signifient ce oui et ce non.

Du même coup, il apparaît que la notion d'information n'existe qu'en relation avec la structure explicite de cette liste. Ce dernier point méritera toute notre attention, car son oubli est la source de bien des erreurs d'interprétation, dont la théorie a été l'objet.

2) Codage. – Même sous la forme d'un numéro d'ordre, le message n'est pas en général propre à être transmis tel quel :

Les images lumineuses doivent être transformées en modulations électriques avant d'être radiodiffusées, la pensée doit se traduire en mots, en gestes avant d'être perçue par autrui, le discours doit être écrit pour que la communication en soit possible au-delà du cercle des auditeurs, etc.

Le codage a pour but de faire correspondre à chaque message un autre symbole encore plus abstrait mais appartenant cette fois à la liste des *messages susceptibles d'être transmis* ou « *signaux* ».

Naturellement dans la pratique, ce codage est en réalité une série de codages successifs (de la pensée à la phrase, aux mots, aux phonèmes, aux ondes sonores, etc.), bien que nous l'envisagions ici comme une opération unique, dont le caractère essentiel est seulement d'être effectué selon des règles fixes, connues, et qui permettent le décodage ultérieur.

3) La ligne de transmission. — Ici encore, il s'agit d'une idéalisation à laquelle peuvent s'identifier les réalités les plus diverses depuis la page imprimée jusqu'à l'onde hertzienne. Son trait distinctif est d'être le lieu où s'introduit l'incertitude dans la communication.

Par une généralisation du langage des radiotransmissions, on appelle « *bruit* » toute perturbation au hasard du message transmis : par exemple sera réputé paradoxalement « bruit » le fait que le circuit téléphonique soit coupé pendant une conversation à condition que cette interruption soit :

1) imprévisible de façon autre que statistique ;

2) indépendante du message initial transmis.

(La censure n'est pas de la nature d'un « bruit » à proprement parler !)

Par conséquent, les distorsions qui peuvent en principe être rigoureusement corrigées (par exemple un affaiblissement de certaines fréquences) ne sont pas du bruit, car elles ne se produisent pas au hasard.

Elles ne sont pas « aléatoires » ou « stochastiques » (ces deux expressions étant pratiquement synonymes).

C'est en général une des données du problème que la structure du bruit et celle-ci s'exprime par des probabilités indiquant quelles sont les chances d'une transmission correcte ou incorrecte des différents signaux.

Observons d'ailleurs que le bruit peut dans certains cas être nul ou négligeable : c'est le cas le plus simple et sa théorie nous occupera tout spécialement.

4), 5), 6). — Décodeur. Récepteur. Bilan. Il n'y a que peu de choses à dire pour le moment du décodeur et du récepteur, dont les fonctions sont évidentes et dont les principes d'action seront discutés plus loin. La notion de bilan, par contre, mérite un examen détaillé : supposons donc que nous soyons dans un cas où des évaluations monétaires précises aient un sens et voyons quels sont les « postes » qui doivent figurer à ce bilan.

Nous trouvons :

1) *Les frais d'équipement :* pour réaliser le codage, la transmission et le décodage, un certain matériel a dû être mis en place quel que soit l'usage ultérieur qui en sera fait. C'est donc l'une des tâches de théoriciens des communications que d'indiquer comment les mécanismes doivent être réalisés de la façon la plus simple pour des niveaux d'exactitude et de rapidité donnés.

2) *Les frais de fonctionnement :* ceux-ci dépendent à la fois du message émis et des opérations ultérieures. Il nous faut distinguer encore. D'une part il y a les coûts de codage, de transmission et de décodage qui varient selon le degré de minutie avec lequel ces opérations sont réalisées et, d'autre part se trouve le « *coût d'erreur* » qui est la clé de voûte de tout l'édifice. Par cette fonction, nous entendons ce qu'il en coûte au récepteur pour chaque message émis d'avoir pris sa décision en fonction d'un message plus ou moins tronqué ou incorrect.

Il n'est pas facile d'ailleurs de trouver des exemples naturels simples où le calcul de ce bilan soit tant soit peu rigoureux : en dehors d'opérations industrielles très précises il est hautement arbitraire de « taxer » monétairement les inconvénients de tel ou tel type d'erreur. Aussi avons-nous là comme une sorte de contradiction dans la théorie :

D'un côté, sans notion de bilan celle-ci devient triviale, car si les erreurs étaient sans importance, il serait inutile de communiquer quoi que ce soit, et de même si la transmission ne coûtait rien, il suffirait de répéter un très grand nombre de fois

pour être à peu près sûr du résultat. Mais, d'autre part, dans chaque application, l'établissement de ce bilan est une affaire d'appréciations personnelles impossibles à chiffrer : comment trouver une commune mesure entre le coût en temps et en argent d'un long télégramme et le risque que son contenu trop elliptique soit incompréhensible pour le destinataire?

Comment comparer l'inconvénient d'une image télévisée plus ou moins floue avec l'avantage d'un prix de revient moindre d'un appareillage simplifié?

C'est donc d'abord à ce niveau que la théorie devra être normative en choisissant arbitrairement des critères raisonnables de coût, avec l'espoir souvent justifiable que la contradiction sera levée par ce fait mathématique que si les opérations sont répétées un très grand nombre de fois, le résultat pratique et peu sensible à des changements de critères tant que ceux-ci ont à peu près les mêmes propriétés qualitatives.

Voici des exemples de normes parmi les plus fréquemment utilisées :

Coût d'installation. — On dispose d'un stock de pièces détachées, toutes censées avoir le même prix et il s'agit d'en faire la synthèse de dispositif, en utilisant le plus petit nombre d'unités.

Coût de fonctionnement. — Un petit intervalle de temps est pris comme une unité à laquelle on ramène toutes les opérations que l'on cherche évidement à effectuer avec des délais minimum. Ou bien : l'énergie mise en jeu sur la ligne est prise comme unité de coût. Ou bien : cette même énergie est taxée à un tarif infime tant qu'elle est en dessous d'un certain palier et à un tarif infiniment élevé au-dessus.

Fonction d'erreur. — Les messages possibles étant en nombre fini, une « unité de gain » est enregistrée si et seulement si le message émis est correctement identifié, les erreurs étant toutes considérées comme égales en coût. Ou bien : les messages possibles étant restreints à deux (*oui* ou *non*), une taxation élevée oblige à rendre très faible la fréquence des « oui » reçus, comme « non » et l'on minimise la fréquence des « non » reçus comme « oui ». (1)

Les messages possibles étant des grandeurs (intensité, voltage, distance, etc.), on mesure la précision par une fonction simple de la différence $|\xi - \hat{x}|$ entre la grandeur émise ξ et la grandeur reçue $\hat{x}$ (2).

Ce choix fait pour chacune des parties, il sera le plus souvent suffisant au stade de l'application pratique de fixer des limites à tous les coûts, sauf un sur lequel on fera porter l'effort d'optimalisation : quitte d'ailleurs à reposer le problème sous un autre angle par la suite. Ainsi par exemple, dans le développement du téléphone, a-t-on pu voir successivement les ingénieurs s'efforcer de diminuer les coûts d'erreurs (l'objectif premier étant obtention d'une reproduction correcte de la voix parlée), puis les coûts d'installation (l'objectif étant la simplification des appareillages), puis maintenant en fonction d'exigences spéciales, les coûts de fonctionnement (la réduction des « largeurs de bande »).

Enfin, au-delà des techniques, l'introduction du bilan et de la fonction de coût d'erreur a une signification profonde pour toute la théorie, car c'est elle qui restitue aux messages émis ou reçus leur valeur concrète : le message initial était, nous l'avons vu, un simple numéro d'ordre sur une liste : au plus avait-il comme caractéristique sa probabilité plus ou moins grande d'être émis. La fonction d'erreur nous oblige, sinon à tenir compte intégralement de sa signification, tout au moins à considérer l'aspect de celle-ci qui retentit sur le bilan de la transmission : par exemple, si le bruit est tel que les messages dont les numéros d'ordre sont voisins ont plus de chance d'être confondus les uns avec les autres, il sera désirable d'éloigner par le codage les messages entre lesquels l'erreur est la plus grave. C'est là, si l'on veut, une possibilité de définition intrinsèque du degré de synonymie : deux messages sont d'autant plus synonymes que la confusion de l'un avec l'autre a un coût plus faible.

On observera d'ailleurs, à ce propos, que la relation de synonymie n'est pas nécessairement symétrique : confondre A et B n'a pas toujours la même importance, selon que c'est A ou B qui a été émis (cf. les dispositifs d'alarme évoqués plus haut).

LES PRINCIPES DE COMPORTEMENT

Ayant mis en place les acteurs et les décors, il nous faut maintenant fournir aux personnages des mobiles d'actions.

Le codeur et le décodeur sont par hypothèses de simples figurants : agissant selon des règles fixes connues de tous, ils sont mécanisables et mécanisés par principe.

Le bruit, lui est un acteur indépendant, mais nous avons convenu de le restreindre à n'agir que les yeux bandés sans savoir quels sont les messages qu'il déforme ou qu'il mutile.

Par contre, l'émetteur et le récepteur peuvent avoir des personnalités plus riches. Il suffit en ce qui concerne le premier d'évoquer le cas où l'émetteur est un avion ennemi ; les « messages émis » étant sa position et sa direction instantanée de vol. Le dispositif de communication a alors pour but d'informer le récepteur — qui est

(1) Par exemple un dispositif avertisseur d'alarme : on augmente d'abord sa sensibilité jusqu'à ce que les chances qu'il manque à fonctionner en cas d'accidents soient infimes (plus petites que 1/100 000 disons), puis dans un deuxième temps, on s'efforce d'empêcher au maximum qu'il donne l'alarme sans cause.

(2) Le plus souvent, le carré $|\xi - \hat{x}|^2$ de cette différence : c'est la méthode des « moindres carrés » connue des astronomes et des géodésiens depuis un siècle et demi et le « RMS criterium » des électroniciens modernes.

une batterie de D. C. A. — des éléments nécessaires au réglage du tir.

Il n'est évidemment pas possible de considérer que l'avion se déplace au hasard, car tout au contraire il dirige son vol de façon à rendre le plus difficile possible le pointage des pièces ennemies : il est *adversaire du récepteur* et il nous faut trouver une formulation mathématique de cette possibilité.

C'est la théorie des jeux — autre branche de la cybernétique — qui nous fournira les outils analytiques indispensables pour cette étude.

Pour l'instant, il nous suffit de savoir que l'émetteur adversaire peut dans des cas très généraux être considéré comme un sujet passif (c'est-à-dire choisissant au hasard), à condition que les probabilités en cause soient convenablement calculées.

Or, cette situation est beaucoup plus générale qu'il ne paraît : si, au lieu d'un adversaire subjectivement animé d'intentions hostiles, le récepteur avait en face de soi un sujet passif, mais dont il ignore les normes de conduite, ce pourrait être une politique raisonnable que d'agir comme à l'égard d'un ennemi déclaré.

Pour la seconde fois, la théorie des communications doit faire apparaître un principe normatif : en présence d'un émetteur dont il ignore les caractéristiques, le récepteur se conformera au principe « Minimax », c'est-à-dire qu'il manœuvrera comme si ces caractéristiques inconnues étaient les plus défavorables pour lui. Ceci nous amène alors à conclure que l'attitude du récepteur n'est en aucune façon différente de celle d'un statisticien. Pour ce dernier, en effet, une certaine grandeur inconnue a été « choisie » par la nature et ne lui est révélée qu'à travers un système de prises d'échantillons dont l'élément aléatoire peut être assimilé à un bruit. Par exemple le problème type suivant de la statistique peut être retraduit en termes de théorie des communications :

La longueur ξ comprise entre 99 et 101 cm d'un certain étalon est inconnue et non mesurable. On a reproduit 10 copies de cet étalon dont les mesures sont x_1, $x_2 \ldots$ x_{10} et l'on sait que des écarts — inévitables — dans le processus de copies sont distribués selon une loi connue Φ. Que peut-on dire de ξ connaissant les x_i ?

TRADUCTION

La liste des messages possibles est l'ensemble de tous les nombres entre 99 et 101. Le message émis ξ est codé en envoyant 10 fois un courant d'une intensité égale à ξ. Il existe un bruit qui ajoute ou soustrait à chacun des signaux une petite quantité distribuée selon une loi connue.

On pourrait donc considérer si l'on voulait que toute la statistique mathématique n'est autre chose que la théorie du récepteur dans les communications avec bruit si cette formulation ne subordonnait pas de façon un peu artificielle une discipline ancienne et largement développée à une autre encore dans l'enfance. Il n'en reste pas moins que la théorie de l'information ne se conçoit pas sans la statistique mathématique et il est assez intéressant du point de vue de l'histoire des sciences de constater que les ingénieurs des communications ont redécouvert en toute innocence des résultats et des principes bien connus depuis longtemps dans l'autre domaine.

LES GRANDS PROBLÈMES DE LA THÉORIE DE L'INFORMATION

La statistique mathématique ayant pour domaine propre le comportement du récepteur, il est clair que les résultats les plus nouveaux de la théorie de l'information se rencontrent à l'autre extrémité du cycle et tout spécialement dans l'étude du codage (3).

COMMUNICATIONS SANS BRUIT

Nous partirons du cas le plus simple et le plus typique où sont réunies les particularités suivantes :

i) la liste des messages élémentaires M_1, $M_2 \ldots M_n$ est *finie* et l'émetteur se borne à les choisir au hasard avec des probabilités fixes connues ;

ii) la ligne est exempte de bruit ;

iii) les signaux élémentaires qui peuvent être transmis sont en nombre fini et ont tous le même coût (calculé en unité de temps).

iv) aucune erreur n'est tolérée. (C'est-à-dire : le coût d'une erreur est infini !)

Sans grande perte de généralité on pourra supposer qu'il existe seulement deux signaux élémentaires, disons « + » ou « — », et le problème d'optimalité se formulera donc ainsi :

Comment faire correspondre à chacun des M_1, $M_2 \ldots$ une suite de + ou de —, de façon telle que cette correspondance permette un décodage sans erreur et qu'en moyenne le nombre des signaux élémentaires utilisés (« la longueur moyenne des messages du code ») soit le plus faible possible? Par exemple les messages à transmettre sont les suivants : M_1 « en avant », M_2 « en arrière », M_3 « à gauche », M_4 « à droite », M_5 « stop » avec des fréquences respectives de 1/8, 1/8, 1/8, 1/8 et 1/2. Comme nous n'avons à notre disposition

(3) On observera que l'opération appelée ici « codage » n'est pas inconnue de la statistique. Le soin de préparer les questions, c'est-à-dire les expériences ou les observations, de telle sorte que la « nature » y réponde le plus explicitement possible constitue ce que l'on appelle le « design of experiment » et tend à être un des chapitres les plus vivants de cette discipline. Il existe cependant des différences essentielles quant à la souplesse possible du codage qui est considérablement plus grande en théorie des communications.

que 2 signaux élémentaires + et − , il faut coder les M_i par des suites de + et de − . Supposons que l'on ait pris :

$$M_1 = + \; ; \; M_2 = - \; + \; ; \; M_3 = - - + \; ;$$
$$M_4 = - - - + \; ; \; M_5 = - - - -$$

Ceci est un code correct (sans ambiguïté à la lecture). Voyons quel serait son coût moyen. On trouve :

$$1\times 1/8 + 2\times 1/8 + 3\times 1/8 + 4\times 1/8 + 4\times 1/2 = 26/8 = 3{,}25.$$

Naturellement il semblerait plus logique d'attribuer au message « stop » qui est de loin le plus fréquent la suite la plus courte de signaux élémentaires et nous pouvons essayer, par exemple, le code suivant :

$$M_1 = + + + \; ; \; M_2 = + + - \; ; \; M_3 = + - + \; ;$$
$$M_4 = + - - \; ; \; M_5 = - -$$

de coût moyen :

$$3/8 + 3/8 + 3/8 + 3/8 + 1/2 = 16/8 = 2$$

donc beaucoup plus économique.

La question se pose d'elle-même de savoir si l'on ne pourrait encore faire mieux et c'est là l'objet du premier théorème de la théorie de l'information que nous formulerons ainsi :

« Dans les conditions décrites plus haut, le nombre moyen des signaux élémentaires ne peut pas descendre au-dessous de la valeur H, qui a l'expression suivante :

$$H = \Sigma p_i \operatorname{Log}_2 1/p_i$$

(p_i est la probabilité a priori du i-ème message).

$\operatorname{Log}_2 1/p_i$ est le logarithme de base de 2 de $1/p_i$, c'est-à-dire le nombre x tel que $(1/2)^x = p_i$).

Dans notre exemple : $p_1 = p_2 = p_3 = p_4 = 1/8$ et $\operatorname{Log}_2 8 = 3$; $p_5 = 1/2$ et $\log_2 2 = 1$, donc

$$H = 1/8\times 3 + 1/8\times 3 + 1/8\times 3 + 1/8\times 3 + 1/2\times 1 = 2.$$

D'autre part, un second théorème — plus profond que le précédent d'ailleurs — affirme que :

Il est possible de trouver au moins un codage tel que le nombre moyen de signaux élémentaires soit plus petit que H + 1.

Ces deux énoncés corrélatifs montrent que la quantité H a une liaison essentielle avec le problème. Nous l'appellerons la *quantité d'information de Hartley* et nous discuterons plus en détail sa signification dans les paragraphes suivants.

L'INFORMATION DE HARTLEY

La signification de cette quantité sera plus claire sans doute si nous considérons ce que devient H dans deux cas limites très simples.

D'abord quand une seule des probabilités n'est pas nulle (et est donc égale à 1). On trouve que H est nul et qu'il est différent de zéro pour tout autre système de valeur — ce que nous pouvons résumer par : l'information de Hartley est nulle si, et seulement si le message était connu à l'avance. Voyons maintenant l'autre cas extrême, celui où il existe N messages, tous également probables : un calcul facile montre que dans ce cas H a la valeur $\operatorname{Log}_2 N$ et que c'est pour ce choix des probabilités que celle-ci est maximum. A priori ce résultat n'a rien que de très intuitif : supposons pour simplifier que N soit une puissance de 2 — (2, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$ ... etc.), soit 2^h. D'après la définition qui a été donnée, H est précisément égal à h. Or il existe exactement 2^h — suites différentes formées de h symboles consécutifs + ou —. Si donc nous voulons faire correspondre à chaque suite un seul message, il faudra donc employer toutes ces suites et leur longueur moyenne (qui est leur longueur commune) sera bien h. D'autre part, nous ne saurions rien gagner en utilisant des suites de longueurs différentes, comme on peut le vérifier sans peine.

Le fait que pour un nombre donné N de messages, la quantité H atteigne un maximum quand ceux-ci sont tous aussi probables les uns que les autres correspond d'ailleurs bien à l'intuition : que ce cas est celui où l'incertitude est la plus grande possible. — C'est d'ailleurs sur des considérations de cette nature que s'était basé Hartley dès 1923 pour étudier cette question avant la formulation plus abstraite et plus systématique qu'en a donné C. Shannon en 1949 dans un mémoire qui à la fois fonde et popularise la notion d'information.

Nous aurons cependant avantage à utiliser une deuxième interprétation de H qui en montre plus directement l'usage et nous prendront l'exemple schématique suivant : un objet appartient à l'une des 5 catégories C_1, C_2, C_3, C_4, C_5 dont les fréquences respectives sont 1/8, 1/8, 1/8, 1/8 et 1/2 et qui sont caractérisées par les propriétés suivantes :

	C_1	C_2	C_3	C_4	C_5
Taille	grand	grand	petit	petit	petit
Forme	long	court	long	long	long
Couleur	vert	vert	vert	vert	blanc
Poids	lourd	lourd	léger	lourd	léger

Supposant que toutes les observations ont le même coût, comment organiser au mieux le diagnostic (c'est-à-dire l'identification de la classe à laquelle appartient un objet)?

Nous empruntons aux systématiciens botanistes ou zoologistes leurs « clefs de diagnose » et nous construisons le schéma suivant :

Catégorie

Couleur { vert : Taille { grand : Forme { long : C_1 ; court : C_2 } ; petit : Poids { léger : C_3 ; lourd : C_4 } } ; blanc : G_5 }

Celui-ci conduit à 2,00 observations en moyenne. Serait-il possible de faire mieux?

LA CYBERNETIQUE

La théorie nous permet déjà de répondre *non :* en effet, le problème est rigoureusement le même que celui discuté plus haut une fois que l'on a introduit par exemple le code suivant :

1er symbole : + = vert ; − = blanc ;

2e symbole : + = grand ; − = petit ;

3e symbole : + = long ou léger ; − = court ou long

et un diagnostic plus rapide en moyenne signifierait un codage plus efficace, ce qui est impossible pour les valeurs données des fréquences.

Mais nous pouvons aller plus loin :

H correspondant aux valeurs (1/8, 1/8, 1/8, 1/8, 1/2) nous donne une sorte de mesure de ce que nous savons a priori sur l'objet en nous fournissant une estimation du nombre minimum d'indices qu'il faut recueillir pour l'identifier. Si nous savions que l'objet est « petit », les catégories C_1 et C_2 seraient exclues et les probabilités des autres catégories deviendraient 1/6, 1/6 et 4/6. A cet ensemble de valeurs correspond une quantité d'informations :

$H = 1/6 \log_2 6 + 1/6 \log 6 + 4/6 \log 6/4 = 1.2526\ldots$

On peut donc considérer que la connaissance du fait que « l'objet est petit » apporte une quantité d'information chiffrée par la différence :

$$2{,}00 - 1{,}252 \ldots \neq 0{,}748\ldots$$

Si au contraire nous savions que l'objet est grand, les seules catégories possibles seraient C_1 et C_2 avec une valeur de H correspondante égale à $H'' = 1/2 \log_2 + 1/2 \log_2 2 = 1{,}00$, soit une différence de $2{,}00 - 1{,}00 = 1{,}00$.

Finalement à l'observation portant sur la taille, il est logique d'associer la valeur moyenne de ces différences, soit :

$$1/4\,(H - H'') + 3/4\,(H - H') \neq 0{,}811 = \bar{\bar{H}}$$

que nous appelons la *valeur moyenne de l'information apportée par l'observation de la taille.*

La signification de $\bar{\bar{H}}$ est claire : cette quantité exprime de façon approchée la réduction du nombre moyen d'observation restant à faire quand la taille est connue par rapport à la valeur correspondante quand la taille est inconnue.

C'est ici qu'intervient un phénomène mathématique de la plus haute importance dû au choix particulier qui a été fait pour l'expression analytique de H :

$\bar{\bar{H}}$ est précisément la quantité d'information attachée au simple diagnostic de l'objet entre les deux groupes de catégories « grand » ou « petit ». Autrement dit, nous aurions pu faire l'économie de tout le calcul précédent et évaluer $\bar{\bar{H}}$ simplement comme

$\bar{\bar{H}} = 1/4 \log_2 4 + 3/4 \log_2 4/3 = 0{,}811\ldots$ (probabilité $C_1 + C_2$ (grand) = 1/8 + 1/8 probabilité $C_3 + C_4 + C_5$ (petit) = 1/8 + 1/8 + 1/2).

En particulier nous voyons qu'en première approximation une observation isolée sera d'autant meilleure que la valeur de $\bar{\bar{H}}$ correspondante sera plus élevée. D'après ce que nous avons dit au début, ceci rejoint parfaitement l'intuition, car la question la plus « informative » est celle à laquelle toutes les réponses sont le plus également probables a priori.

Les remarques précédentes ont sans doute montré l'utilité de l'information de HARTLEY, mais il est nécessaire de ne pas perdre de vue ses limitations et surtout le fait qu'elle dépend des probabilités a priori des différentes catégories. Ainsi, si nous voulions savoir quelle est la quantité d'information apportée par une lettre de l'alphabet, nous ne pourrions donner de réponse que dans le cadre d'un système de référence précis qui pourrait être par exemple :

soit l'ignorance complète sur cette lettre (comme ce serait le cas si elle était l'indicatif de série d'un billet de loterie). On trouve alors :

$$H_1 = 26 \times 1/26 \times \log_2 26 = 4{,}70,$$

soit la seule connaissance du fait que cette lettre appartient à un texte français. Ici :

$$H_2 = \text{à peu près } 2{,}5$$

d'après les données statistiques établies empiriquement,

soit la connaissance quelle est la première lettre d'un verbe français rimant avec « rouge » :

$$H = 0$$

car la seule possibilité est b (de « bouge » ; cf. A. DE MUSSET). Si ces probabilités sont inconnues ou trop mal connues, l'information de HARTLEY ne sert plus guère qu'à formuler cette trivialité dont abusent les vulgarisateurs, à savoir que pour reconnaître un objet entre 2^h catégories ou plus, il faut au moins h observations dichotomiques.

La même mise en garde vaut pour la réalisation effective d'un programme de diagnostic : si les probabilités a priori des différentes catégories sont connues et si leur nombre est faible, il existe une méthode directe (due à HUFFMAN) permettant de construire un programme optimal sans utiliser H qui n'est en définitive qu'une fonction d'approximation. Par exemple, on présente parfois la solution du célèbre « problème de 12 pièces » (trouver en trois pesées une pièce fausse parmi 12) comme une application de la théorie de l'information et c'est là le type d'une prétention un peu exagérée.

La théorie permet bien de calculer qu'a priori il n'y a pas d'impossibilité en ce qui la concerne, mais la possibilité effective est de nature purement combinatoire. Ainsi si l'on savait qu'une pièce dans un lot de trois est plus lourde que les deux autres, la théorie de l'information montrerait qu'il n'est possible de la reconnaître par une

seule observation qu'à condition que cette dernière soit susceptible de donner 3 réponses différentes : cette condition est nécessaire, mais non suffisante. Par exemple, l'opération est évidemment irréalisable avec une balance de type habituel.

Cependant, et c'est là l'aspect important, répétons-le, s'il s'agissait de reconnaître n pièces plus lourdes parmi 3n pièces, la deuxième partie du théorème montrerait que sous des conditions très larges on pourrait s'approcher proportionnellement autant que l'on veut de l'optimum à condition que n soit assez grand.

C'est d'ailleurs parce que H est une approximation et non pas une expression rigoureusement égale à la fonction de coût de fonctionnement que son efficacité est si grande comme nous le verrons plus loin.

PROBLEMES DE SCANSION

Nous n'avons envisagé jusqu'ici qu'un seul message. En général il s'agit plutôt de suites indéfinies de messages élémentaires, même si la liste de ceux-ci est finie. Par exemple, on doit considérer le cas où l'émetteur guiderait constamment un engin en dictant sans interruption une suite d'ordres tels que : en avant, à gauche, stop, stop, etc., etc., et un nouveau problème, algébrique celui-ci, se pose à l'ingénieur. Comment le décodeur va-t-il reconnaître que tel signal + ou − est un début ou une fin de *mot* (4) à moins de précautions spéciales. Par exemple, si le code avait été composé des mots suivants :

$M_1 = + + +$; $M_2 = - + +$; $M_3 = + - +$;

$M_4 = - - +$; $M_5 = - -$

(c'est-à-dire l'inverse de celui donné plus haut). La suite d'ordres « droite arrière stop » ($M_4 M_2 M_5$) serait inutilisable car elle serait transmise sous la forme $- - + - + + -$ et avant le dernier signe le récepteur ne pourrait savoir s'il ne s'agit pas de la suite « stop stop gauche... » ($M_5 M_5 M_3$) qui commence de la même manière. Ce problème n'est d'ailleurs pas purement théorique et il suffit d'avoir essayé de lire, par exemple, un texte classique javanais où aucun signe n'indique la fin des mots, pour apprécier ce genre de difficultés.

A ceci, plusieurs remèdes sont possibles : le plus naturel consiste à réserver un symbole spécial à la séparation des messages élémentaires successifs : c'est dans notre typographie ce signe spécial qu'est l'absence de tout autre signe et B. MANDELBROT en a fait la théorie dès 1952. Une autre technique consiste à n'employer que des unités de longueur fixe, les débuts de mots se retrouvant alors régulièrement.

Enfin, il est des classes de codes pour lesquels le délai d'attente entre la réception d'un symbole et celle de contexte nécessaire pour l'interpréter est réduite au minimum : ce sont les codes *unitaires*.

Dans le cas général, le problème de trouver les fins de mots, de *scander* le message conduit à l'introduction de notions intéressantes, notamment celle d'équivalence syntaxiques : (M. P. SCHÜTZENBERGER) les suites de symboles élémentaires a et a′ sont syntaxiquement équivalentes si, quelles que soient les suites x et y, les suites composées xay et xa′y sont en même temps des messages corrects, c'est-à-dire composés d'une suite de mots.

Il y a là une analogie avec les parties du discours : (deux mots sont équivalents si on peut les substituer l'un à l'autre sans altérer la correction de la phrase, par exemple : deux adjectifs masculins singuliers, en français, ou en anglais : deux adjectifs quelconques) dont on a ainsi une sorte d'image algébrique formelle.

On observera au passage que la théorie des communications apporte une contribution à la discussion sur le sens des termes « équivalent » ou « échangeable » en linguistique . Nous avons parlé plus haut de synonymie (= équivalence du point de vue de la fonction de coût d'erreur) — l'équivalence syntaxique définie a rapport à la structure et non pas au contenu du message et en est donc qualitativement différente.

COMMUNICATIONS AVEC BRUIT

Nous conservons les mêmes hypothèses que plus haut, à cela près que nous ne supposons plus que la ligne de transmission soit exempte de bruit. La fonction d'erreur sera le nombre des identifications correctes toutes les erreurs étant également pénalisées. Prenons l'exemple très simple suivant :

Les messages à transmettre $M_1 M_2 M_3 M_4$ ont les mêmes probabilités a priori — 1/4. La ligne admet deux signaux + et −, mais pour chacun d'eux il y a une chance sur 10 pour que la transmission l'altère à tel point qu'il devienne impossible à reconnaître :

Ainsi ayant codé de la façon la plus économique, les messages par le tableau ci-dessous :

$M_1 = + +$
$M_2 = + -$
$M_3 = - +$
$M_4 = - -$

nous pouvons calculer que si M_1 est émis, il y a :

81 chances pour cent pour qu'il arrive correctement (+ +) ;

18 chances pour que l'un des symboles soit ininterprétable (le message reçu est ? + ou + ?) ;

1 chance pour cent pour que les deux symboles soient brouillés (? ?).

Dans les cas douteux, le récepteur pourra tirer au sort sa décision entre les deux possibilités qui existent (par exemple, s'il a reçu + ? c'est que soit + + = M_1, soit + − = M_2 avaient été émis.

(4) On appelle « mot » la suite de signaux élémentaires correspondant à un seul message élémentaire.

En moyenne on trouve que le résultat final sera correct dans :

$$\frac{81}{100} + \frac{1}{2}\,\frac{18}{100} + \frac{1}{4}\,\frac{1}{100} = 90{,}25\%$$ des cas ou plus.

Naturellement si un code plus long était utilisé, les résultats seraient meilleurs : par exemple avec

$$M_1 = + + + + + \; ; \; M_2 = + + - - - \; ;$$
$$M_3 = - - - + + \; ; \; M_4 = - - - - -$$

les chances sont beaucoup plus faibles pour que le message reçu soit ambigu : + + ? +, par exemple, ou même + ? ? + ne peuvent provenir que de M_1. Le même calcul que plus haut conduit à prédire un résultat correct dans 99,0025 des cas.

Il est intuitif qu'à condition d'augmenter suffisamment le nombre des symboles employés n'importe quel degré de certitude prescrit à l'avance pourrait être atteint et ceci quelle que soit d'ailleurs l'intensité du bruit à corriger.

Cependant ceci nous oblige à employer des codes parfois très longs et en tous cas ne réalisant pas le critère d'économie maximum permis par le théorème fondamental en l'absence de bruit. Les codes « antibruit » sont comme on dit *redondants* en ce sens qu'ils sont en moyenne plus longs que les codes optimaux correspondants.

Le problème se pose donc de savoir ce qui subsiste de la théorie dans ce cas et ceci est l'objet d'un théorème énoncé initialement par SHANNON puis démontré rigoureusement par FEINSTIEN, théorème qui constitue pour l'instant le résultat le plus important de toute la théorie de l'information.

Nous ne saurions ici en donner une expression rigoureuse, mais il est possible de montrer simplement en quoi il consiste :

Si nous revenons à l'exemple de tout à l'heure, nous constatons que quand 4 symboles sont consacrés à chaque message, il serait possible de transmettre non pas seulement 4 messages, mais 8 sans diminuer beaucoup la sécurité : par exemple le code :

$$M_1 = + + + + \; ; \; M_2 = + + - - \; ;$$
$$M_3 = + - + - \; ; \; M_4 = + - - + \; ;$$
$$M_5 = - + + - \; ; \; M_6 = - + - + \; ;$$
$$M_7 = - - + - \; ; \; M_8 = - - - -$$

donne 97,2 % de transmission correcte soit avec différence de 2 % à peine avec le code précédent alors que le nombre de messages utilisables est double.

Il y a donc très généralement une balance entre la sécurité permise par un code et le nombre de messages distincts qu'il contient ; balance dont les exemples courants sont nombreux. Typiquement : toute chose égale d'ailleurs, une augmentation de la sensibilité d'une émulsion photographique se paye par une diminution de la finesse des images ; il s'agit donc de trouver une quantité ne dépendant que de la ligne, c'est-à-dire du bruit, qui puisse servir en quelque sorte, de coefficient à cette équation et c'est là le rôle de la *capacité*.

LA CAPACITE

Nous avons caractérisé la ligne et le bruit par les probabilités avec lesquelles les signaux élémentaires sont transmis correctement ou, au contraire, sont altérés au point d'être confondus les uns avec les autres. Il est clair que si ces probabilités sont différentes, il y aura avantage à employer proportionnellement plus fréquemment ceux des symboles que le bruit affecte le moins, c'est-à-dire d'adapter en probabilités le codage à la ligne. La capacité est précisément la valeur moyenne du gain d'information réalisé quand cette adaptation est effectuée de façon optimale. Un calcul relativement simple permet d'en trouver la valeur et du même coup de fixer une limite supérieure au rendement de tout codage concevable pour un niveau de bruit donné.

C'est là l'extension du premier théorème que nous avons donné dans la section précédente. La seconde partie, elle aussi, est beaucoup plus profonde : elle indique qu'il existe sûrement un code qui permet à la limite (c'est-à-dire pour des messages extrêmement longs) d'atteindre cet optimum (c'est-à-dire de transmettre cette quantité d'information).

Le phénomène mathématique curieux est que le théorème affirme l'existence d'un tel code sans donner aucune indication sur la manière de le construire (5). D'ailleurs jusqu'à une date très récente on ne connaissait aucun code qui approchât même d'assez loin cet optimum théorique.

Revenant à la première partie du théorème, il est impossible de ne pas mentionner son application au cas très important dans la pratique où les messages sont codés par la modulation d'un système périodique (modulation en fréquence ou en amplitude) : une théorie spéciale permet de fixer une limite infranchissable à la multiplicité des signaux reconnaissables pour une largeur de bande ou une énergie données et naturellement sur le plan pratique l'existence de cette limite est un guide précis pour la construction des appareillages.

C'est même à ce chapitre de la théorie que sont consacrés le plus grand nombre des travaux qui se publient chaque jour, mais leur nature essentiellement technique nous interdit d'y consacrer plus que ces brèves remarques.

INFORMATION DE WALD

A l'opposé en quelque sorte de la théorie précédente se situe le cas où deux messages seulement sont à distinguer, mais où l'accent est mis

(5) La situation est analogue à la suivante : nous pesons ensemble 50 caisses censées contenir chacune 100 kg. Le poids total est 4 950 kg, donc l'une des caisses n'est pas complètement remplie ! mais nous ne savons pas évidemment de laquelle il s'agit.

tout spécialement sur l'économie de codage des signaux et ceci nous donnera l'occasion de parler d'un autre type d'information, *l'information de Wald*.

Si le décodage des signaux élémentaires est très coûteux, il est certain que le récepteur pourra procéder de façon plus économique en arrêtant celui-ci aussitôt qu'il s'estimera assez sûr du résultat.

Par exemple, dans le premier code discuté plus haut, si le récepteur a la chance que les trois premiers symboles aient été transmis sans brouillage (+ + +, par exemple), il n'a nul besoin du quatrième pour être sûr que le message émis était M_1. Le quatrième symbole ne sert qu'au cas où l'un des signaux antérieurs aurait fourni une indication douteuse. Ceci est très typiquement la démarche même que nous employons chaque jour où, pour vérifier une hypothèse, nous renouvelons les observations et les expériences jusqu'à ce que la balance penche indiscutablement d'un côté ou d'un autre.

L'emploi systématique de cette méthode constitue ce que l'on appelle « l'analyse séquentielle » et cette théorie, due au mathématicien A. WALD, constitue un des développements les plus brillants de la statistique dans les dernières décades. Son application à la théorie des communications est encore dans l'enfance, mais il nous semble important de la mentionner ici, car elle repose sur l'emploi d'une certaine quantité W (6) qui généralise l'information H de HARTLEY et qui permet a priori de limiter inférieurement le nombre minimum des signaux à décoder.

PROBLEMES DE TRANSMISSION CONTINUE. INFORMATION DE FISHER

Jusqu'ici nous avons toujours supposé que les messages pouvaient être arrangés sur une liste finie ou tout au moins que l'on pouvait leur donner un numéro d'ordre 1, 2... n.

Les considérations précédentes deviennent inappliquables si les messages sont des grandeurs continues comme cela se rencontre souvent dans la pratique.

Une technique très simple employée par exemple dans le Pulse Code Modulation consisterait à se ramener au cas précédent en *quantifiant* ces messages, c'est-à-dire en faisant choix d'une unité assez petite et en négligeant de transmettre les fractions de cette unité. C'est ce que font les chauffeurs de taxis qui tarifent leurs courses en *hectomètres* et non pas de façon exactement proportionnelle au chemin parcouru.

Cependant, sur le plan théorique aussi bien que pratique, il n'est pas sans intérêt de discuter en lui-même le cas d'un message continu et les statisticiens, dans les cinquante dernières années, ont élaboré des techniques analytiques très raffinées pour traiter ce problème.

Ici encore, selon le schéma logique, qui semble de règle, nous rencontrerons :

1) Une quantité ayant les propriétés formelles d'une information, c'est-à-dire telle qu'on puisse aussi bien soit la calculer globalement a priori, soit déterminer étape par étape le gain apporté par chaque observation. (C'est ici l'information de FISHER (7).)

2) Un théorème fixant une limite inférieure au nombre minimum d'observations nécessaires pour obtenir une précision donnée. (C'est l'objet du théorème dit de CRAMER - FRECHET - DARMOIS - RAO d'après les noms des auteurs qui l'ont successivement généralisé.)

3) Un second théorème montrant que si des observations très nombreuses sont permises, il est possible de les combiner de telle sorte que cette limite soit approchée d'aussi près que l'on veut.

Ici encore le sujet est essentiellement mathématique et il nous serait impossible d'entrer dans plus de détails sans recourir à un appareil analytique compliqué.

On mentionnera seulement que les « diverses quantités informatives » qui ont été introduites successivement, peuvent être fondées dans une large mesure à partir de principes axiomatiques très généraux sans faire appel à leur fonction spécifique (M. P. SCHÜTZENBERGER).

LES APPLICATIONS DE LA THÉORIE DE L'INFORMATION

THEORIE DE L'INFORMATION ET PHYSIQUE

L'expression formelle de l'information H de HARTLEY est identique à celle d'une des grandeurs fondamentales de la thermodynamique, à savoir l'entropie.

Il a donc semblé très vite qu'une liaison profonde devait exister entre ces deux notions ; liaison à laquelle d'ailleurs paraissait convier directement leur contenu intuitif :

d'une part une mesure de notre connaissance sur le système,

(6) Soient p_i et p'_i les probabilités respectives pour que le signal élémentaire i ait été reçu selon que M ou M' a été émis.
Soit $W = \Sigma p_i \operatorname{Log} p_i/p'_i$.
Alors, si M a été émis, il faudra décoder en moyenne au moins K/W signaux élémentaires par où K ne dépend pas de la ligne, mais seulement du niveau de sécurité que l'on désire atteindre.

(7) Si $f(x_i \theta)$ est la probabilité que l'observation donne le résultat x_i quand le message a la valeur θ, on a :

$$F = \Sigma_i \; f(x_i : \theta) \; \partial^2/\partial\theta^2 \operatorname{Log} f(x_i : \theta).$$

d'autre part, puisque c'est là l'interprétation habituelle de l'entropie, une mesure de degré de désordre de ce même système.

Et, en effet, dans un travail assez peu remarqué à son époque, le physicien SZILARD avait déjà étudié en 1923 une relation analogue avant même que fût introduit le concept d'information. Pour exposer cette question, il nous faut ouvrir une brève parenthèse et rappeler ce qu'est un «démon» de MAXWELL :

C'est un postulat fondamental de la physique que l'impossibilité du mouvement perpétuel. Supposons cependant qu'une boîte remplie de gaz soit divisée en deux parties par une cloison munie d'une porte.

Toujours d'après les principes fondamentaux, les molécules de gaz sont en mouvement et leur vitesse est inégale, la valeur moyenne seule de celle-ci restant constante et caractérisant la température.

Par conséquent, si un « démon » posté près de la porte ouvrait et fermait judicieusement celle-ci, ce qu'il pourrait faire en ne dépensant qu'une énergie très faible, il parviendrait petit à petit à trier les molécules en ne laissant par exemple entrer dans l'une des parties que les molécules en mouvement rapide et dans l'autre celles en mouvement lent.

Au bout d'un certain temps, il aurait donc réalisé une différence de température entre ces deux parties, différence susceptible d'être convertie en énergie en violation apparente du principe de l'impossibilité d'un « perpetuum mobile ».

Naturellement ce paradoxe n'a de valeur que théorique, mais sa réfutation a suscité de nombreux travaux et notamment l'application la plus importante de la théorie de l'information à la physique :

Quel est en effet le résultat de l'action du «démon»: en classant les molécules il diminue leur désordre, c'est-à-dire qu'il diminue l'entropie. Or, ceci n'a été possible que parce qu'une certaine information a été obtenue sur les molécules.

Par conséquent, si nous identifions (au signe + ou − près) l'information et l'entropie comme le suggère leur analogie formelle, nous retrouvons bien un bilan total nul ainsi que le veut la théorie : le «démon» n'a pu acquérir de l'information sur les molécules qu'aux dépens d'une certaine augmentation d'entropie qui doit compenser exactement la diminution de cette même quantité qu'il a provoquée dans la boîte.

En développant plus en détails les calculs, BRILLOUIN a réussi à montrer qu'effectivement un semblable «démon» est impossible et à exorciser ainsi le paradoxe de MAXWELL.

Cette identification peut d'ailleurs être poussée plus loin et l'on retrouve en théorie de l'information des formules parallèles aux célèbres relations d'incertitude de HEISENBERG qui dominent la physique quantique.

Il y a là tout un domaine de recherches nouveau étudié notamment par GABOR et dont les principes mêmes sont encore loin d'être éclaircis, car étant donné que les énoncés purement mathématiques, sur lesquels se basent les deux développements, sont rigoureusement les mêmes, on peut se demander si cette assimilation de l'information à l'entropie est plus qu'un parallélisme formel. Peut-être d'ailleurs que cette question elle-même est vide de sens, puisqu'en toute rigueur les deux théories correspondent au départ à deux idéalisations opposées.

THEORIE DE L'INFORMATION ET SCIENCES HUMAINES

Il était naturel que le nom seul de théorie de l'information suscite un grand enthousiasme parmi les spécialistes des sciences humaines, comme contenant la promesse d'un instrument mathématique rigoureux pour traiter de concepts jusque-là rebelles à l'analyse numérique.

Il faut cependant admettre que les résultats n'ont peut-être pas encore égalé les espérances dans tous les domaines envisagés, et notre exposé sera par nécessité moins cohérent qu'on ne le souhaiterait.

Applications à la sémantique et à la psychologie. — CARNAP et d'autres logiciens comme MACKAY ont cherché à appliquer l'information de HARTLEY (ou à introduire des expressions analogues) afin d'étudier des cas plus généraux : jusqu'ici les résultats ont été surtout formels puisque comme nous l'avons vu, il n'a d'intérêt que si des probabilités explicites figurent au départ. Il n'en reste pas moins qu'une lacune grave existe : il n'existe actuellement aucune façon qui ne soit pas artificielle d'évaluer le « gain d'information » (au sens large comme opposé au sens étroit utilisé dans les chapitres précédents) réalisé par l'accomplissement d'un calcul ou d'un raisonnement logique : si par exemple nous voulons savoir quel est le plus petit nombre x tel que $x^2 - 14x + 12 = 0$, c'est intuitivement un « gain d'information » que d'apprendre que x est égal à 7 moins la racine carrée de 37. Cependant, du point de vue de la théorie de l'information, il n'y a aucun gain de réalisé. De façon tout aussi négative, aucune mesure intéressante ne permet d'estimer le progrès réalisé à chacune des étapes intermédiaires d'un Sorite.

L'intérêt d'un concept mathématique applicable à ces cas serait cependant considérable puisqu'il permettrait sans doute de fixer des limites aux nombres d'opérations élémentaires à effectuer pour arriver au bout d'un calcul.

Les seuls résultats connus sont, soit purement formels, soit obtenus par des méthodes d'épuisement de tous les cas possibles, soit des approximations extrêmement sommaires.

Ceci souligne, une fois de plus, s'il en était besoin, à quel point est erronée l'opinion trop répandue qui considère la théorie comme traitant de l'« information » au sens courant du terme et non pas seulement d'une certaine quantité appelée « information » (de HARTLEY, de WALD, de FISHER, etc.) définie dans un contexte rigoureux, quantité qui est d'ailleurs, en effet, parfois identifiable partiellement à ce que suggère son nom, mais sans que pour autant les résultats analytiques de la théorie soient valables plus loin que ce contexte (8) étroit.

A un niveau plus concret la théorie de l'information a cependant apporté des résultats encore que fragmentaires :

Les plus remarquables sont sans doute ceux de MAC CALLOCH et PITTS qui, dans le cadre plus large de la physiologie nerveuse, ont systématiquement étudié le nerf comme un système destiné à transmettre de l'information. Dans la même ligne de recherches, d'autres travaux ont mis à profit ces méthodes pour essayer de donner une théorie des organes des sens et notamment de l'audition.

Sur le plan expérimental on ne peut pas négliger les recherches récentes de H. QUASTLER qui a cherché à mesurer quelle quantité d'information par seconde le cortex humain était capable d'utiliser : des résultats convergents basés aussi bien sur l'observation de dactylographes hautement qualifiées que de musiciens entraînés déchiffrant à leur vitesse maximum, ont permis de trouver un palier correspondant approximativement à une douzaine de choix dichotomiques par seconde. Ceci correspond — grossièrement — aussi à la quantité reçue dans une lecture rapide et on entrevoit des applications nombreuses de ces recherches en plein développement.

Applications à la Linguistique. — C'est ici certainement que les résultats les plus riches et les plus encourageants ont été obtenus, jusqu'à présent. Nous distinguerons parmi ceux-ci deux groupes : les résultats d'observation et les résultats théoriques.

1) *Résultats d'observation.* Il est difficile de savoir les rôles respectifs joués par la théorie de l'information et les simples nécessités de la pratique des communications.

Le fait est néanmoins que la phonétique ayant amené des esprits de formation plus scientifique que littéraire à reconsidérer les problèmes de langage, divers faits nouveaux ont été découverts qui n'avaient pas attiré l'attention des grammairiens.

Essentiellement il s'agit de la structure statistique du langage, étude qui encore une fois décolle du plan de la réalité de la signification pour s'intéresser exclusivement à la façon dont cette signification est transmise.

Comme nous l'avons vu déjà, toute étude d'un système de communication doit être précédée d'une analyse de la fréquence des divers messages :

Ainsi, de façon assez grossière le code Morse reflète la composition moyenne par lettres de l'anglais (e, la lettre la plus fréquente est le « mot » le plus bref : un *point ;* q, très rare, demande sept fois plus de temps : *trait trait point trait*).

Cependant cette seule liste de fréquence des lettres ne caractérise pas — et de loin — un langage : il existe ce que l'on appelle des corrélations, c'est-à-dire, très simplement, que la fréquence des lettres n'est pas indépendante de la séquence qui précède son apparition : en français « q » entraîne presque automatiquement u, « x » est surtout une lettre finale. Les probabilités d'apparition des différents couples de lettres (les fréquences de « bigrammes ») forment donc une description plus fine du langage. Allant plus loin on peut étudier les fréquences des trigrammes, des quadrigrammes, quoique le décompte devienne vite inextricable, pratiquement en raison de la multiplicité des cas à considérer (9).

D'après ce que nous avons dit plus haut, l'existence de ces liaisons en probabilités diminue le contenu informationnel des lettres successives : A la question : quelle est la lettre suivante ?, nous sommes déjà le plus souvent capables de donner une réponse approchée alors qu'un codage optimal (du seul point de vue de l'économie) voudrait que toutes les 27 réponses possibles fussent aussi probables les unes que les autres.

Naturellement cette redondance n'est pas sans avantage : un texte partiellement altéré ou tronqué reste en partie compréhensible grâce aux contextes. La langue est un code anti-bruit très efficace (10).

Cette analyse statistique a révélé des aspects curieux bien qu'anecdotiques des langues parlées : le niveau de redondance est celui-là même qui permet l'existence de mots croisés ou encore est tel qu'un codage optimal n'utilisant que *deux* signes typographiques, permettrait de traduire à peu près tout texte dans un autre de même longueur. Une manière pittoresque de présenter ce dernier résultat est de dire qu'une phrase de n signes peut — en général — être devinée au moyen de n questions bien choisies dont la réponse est limitée à oui ou non.

(8) Comme l'extrapolation abusive qui voudrait appliquer le théorème des «forces vives» à l'« énergie » d'un général d'armée.

(9) Voici des exemples de ce que l'on peut obtenir en tirant au sort les lettres successives selon les fréquences des trigrammes : « PROSEJOURS DE MAIS LE QUE DONNENT TROIRE A BLEMER » (français), « UALLIS MINIET/LETAUDATORUM NUOS ET BINIBUS NONEMAE RESCENT » (Latin).

(10) Des recherches expérimentales ont d'ailleurs montré l'étendue étonnante des distorsions ou des mutilations que supporte un discours sans cesser d'être intelligible alors qu'assez vite disparaît la possibilité de reconnaître l'identité de l'orateur : il y a une marge extrêmement grande entre reproduction parfaite et reproduction utilisable dont la technique la plus avancée cherche à tirer profit pour simplifier les appareillages ou réduire les largeurs de bande utilisées.

LA CYBERNETIQUE

De façon plus sérieuse, des considérations analogues peuvent être développées au sujet de l'analyse des phénomènes : combien d'oppositions élémentaires (vocalisé/non vocalisé ; nasal/non nasal, etc.) sont nécessaires pour identifier un phonème d'une langue donnée? Une équipe de chercheurs autour de JAKOBSON travaille activement cette question qui a des rapports évidents avec la réalisation d'une machine capable de traduire en un texte *écrit* un message *parlé*.

D'autres recherches expérimentales ont étudié la répartition des accents d'intensité, la longueur des phrases, etc. et il y a là comme nous le disions plus haut, un point de vue nouveau qui ne peut que féconder le développement de la linguistique.

2) *Recherches théoriques*. Bien qu'elles soient en marge de la théorie de l'information au sens strict, il est impossible de ne pas citer ici les recherches suscitées par le problème de la mécanisation des opérations de traductions.

Si l'on veut dépasser le stade primitif d'une simple mécanisation de dictionnaire, il est certain que les structures grammaticales doivent être interprétées dans un esprit nouveau : au lieu d'une aide à la *compréhension* d'une langue ou d'un recueil de principes énonçant les règles de la civilité verbale et écrite, la grammaire opérationnelle doit être un manuel rigide prescrivant les démarches à effectuer pour identifier les parties de discours et leurs accidents ou pour faire l'inverse.

La rédaction de semblables grammaires est en train pour les langues principales, et déjà on commence à apercevoir des possibilités d'analyse structurelle radicalement différentes de celles jusqu'ici classiques, notamment l'existence d'« unités sémantiques » moins complexes que les phrases, mais plus abstraites que les mots.

Ici encore, les travaux en cours sont extrêmement prometteurs.

Beaucoup plus liée à l'aspect mathématique est par contre la théorie de B. MANDELBROT sur laquelle nous nous étendrons plus longuement.

Nous avons mentionné plus haut ce fait que si aucun signe spécial n'articulait les fins de mots, la lecture du message serait beaucoup plus délicate, voire même impossible en cas de perturbations altérant un ou plusieurs symboles.

Plus généralement cette division en unités sémantiques, cette quantification de la description du monde, que permet l'existence de ces atomes de discours que sont les mots, se révèle une nécessité à peu près absolue quand le langage doit être plus qu'un simple code référant à un système fixe de messages étroitement délimités à l'avance.

Mais si l'on admet ce postulat, il s'ensuit que les méthodes usuelles d'optimalisation du codage ne sont plus applicables brutalement et le problème se pose de savoir quelles devraient être la longueur et la fréquence relative des différents mots pour que ce codage envisagé reste le plus économique parmi ceux qui appartiennent au même temps.

En résolvant mathématiquement cette question, on découvre qu'il doit exister une relation très simple entre, d'une part : la fréquence relative de chacun des mots et, d'autre part : le nombre des mots plus fréquents que celui considéré.

Or, il se trouve que ces répartitions statistiques avaient été déjà compilées empiriquement par ZIPF sur des échantillons très longs de langues aussi diverses que l'anglais de T. S. ELIOTT, celui de James JOYCE, l'hébreu moderne, certaines formes de latin d'église, etc., sans parler des langues classiques.

L'accord entre la théorie et les observations est excellent et les cas exceptionnels s'interprètent d'une façon qui confirme la validité générale de la théorie.

Nous avons donc là un des premiers exemples d'application complète des méthodes des sciences physiques aux sciences humaines : un modèle mathématique est construit sur la base d'un principe d'optimalité et les calculs à eux seuls permettent à la fois de retrouver les régularités empiriques et d'expliquer les cas de non-concordance.

Mais il y a plus. Les structures mathématiques employées relèvent d'une théorie plus profonde dont B. MANDELBROT a étudié d'autres applications : on retrouve là des problèmes thermodynamiques spéciaux — ceux-là mêmes que la théorie habituelle néglige — comme ne correspondant pas aux approximations naturelles de l'interprétation énergétique classique, mais dont l'intérêt n'est pas pour autant moins grand : par exemple les nombres de genres et d'espèces dans lesquels se subdivisent des groupes aussi variés et aussi étendus que les algues, les coléoptères, etc., suivant certaines relations empiriques (« Loi de WILLIS ») de façon à peu près vigoureuse, relations qui déterminent statistiquement la fréquence relative des genres possédant n espèces pour toutes les valeurs de n. B. MANDELBROT a montré que cette loi pouvait précisément s'interpréter comme une conséquence d'un principe.

M. P. SCHÜTZENBERGER.

Année 1958

Bibliographie

[1] Marcel-Paul Schützenberger. A propos de l'inégalité de Fréchet-Cramer. *Publ. Inst. Statist. Univ. Paris*, 7(3/4) :3–6, 1958.

[2] Marcel-Paul Schützenberger. Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées. In *Séminaire Dubreil-Pisot, année 1958-59*, Exposé No. 1, 11 décembre 1958, 22 pages. Inst. H. Poincaré, Paris, 1958.

[3] Marcel-Paul Schützenberger. Sur la représentation monomiale des demi-groupes. *C. R. Acad. Sci. Paris*, 246 :865–867, 1958.

[4] Marcel-Paul Schützenberger. Sur les homomorphismes d'un demi-groupe sur un groupe. *C. R. Acad. Sci. Paris*, 246 :2442–2444, 1958.

[5] Marcel-Paul Schützenberger. On the quantization of finite dimensional messages. *Information and Control*, 1 :153–158, 1958.

[6] Marcel-Paul Schützenberger. La méthode des modèles dans les sciences humaines. In *La méthode dans les sciences modernes*, Hors série de "Travail et Méthodes", pages 195–197. Éditions sciences et industries, Paris, 1958.

A PROPOS DE L'INÉGALITÉ DE FRÉCHET-CRAMER

Marcel Paul SCHUTZENBERGER

1/ - Le but de cette note (1) est de montrer comment l'inégalité classique de Fréchet-Cramer s'applique au cas de l'estimation de Bayes, c'est-à-dire à celui où le paramètre à estimer, x, possède une densité de probabilité à priori f(x). Comme dans le cas habituel, nous supposons que la fonction de coût d'erreur est quadrique et qu'un nombre constant N de variables y_i est observé. Les y_i sont distribués indépendament avec la densité conditionnelle $g(\frac{y}{x})$ et l'ensemble des N valeurs observées est désigné par le vecteur z. On supposera que la densité :

$$h(z;x) = f(x) \prod_i g(\frac{y_i}{x})$$

est presque partout différentiable et ne s'annule pour aucune valeur finie de ses arguments. On posera : $f^*(z)$ = la densité de probabilité de z ; $g^*(\frac{x}{z})$ = la densité de probabilité (à posteriori) de x pour z observé.

2/ - Etablissement de l'inégalité.

Pour toute fonction d'estimation $x \# (z)$ on a :

$$E\,(x - x\,\#\,(z))^2 \geqslant \left(\frac{1}{F + N\,E_x G(x)}\right) \qquad (2)$$

où E_u (resp. E) désigne la valeur moyenne par rapport à u (resp. par rapport à x et à z) et où

$$F = E_x\left(\frac{f'(x)}{f(x)}\right)^2 \; ; \; G(x) = E_y\left(\frac{\delta}{\delta x}\,\frac{g(\frac{y}{x})}{g(\frac{y}{x})}\right)^2$$

---

(1) Je tiens à signaler que cette extension a été obtenue par plusieurs auteurs indépendamment : Mr D. Slepian (de la Cie Bell) communication personnelle; Mr J. Dard (article à paraître dans "Annals of Mathematical Statistics"). Aucun de nous n'a publié autre chose que des résumés de ses résultats.

Démonstration.

On part du résultat classique :

$$E(x - x\,\#(z))^2 = E(x - \bar{x}(z))^2 + E(\bar{x}(z) - x\,\#\,(z))^2 > E_z\, v(z)$$

où $\bar{x}(z)$ et $v(z)$ sont respectivement la moyenne et la variance de $g^*(\frac{x}{z})$.

D'après l'inégalité de Weyl, $v(z) \geqslant \frac{1}{G^*(z)}$ (où $G^*(z)$ est la valeur moyenne du carré de la dérivée logarithmique de $g^*(\frac{x}{z})$) donc, par convexité :

$$E_z\, v(z) \geqslant (E\ v(z)^{-1}\ )^{-1} \geqslant (E_z\, G^*(z))^{-1}.$$

Comme d'autre part en calculant la valeur moyenne du carré de la dérivée logarithmique (par rapport à x) de h(z;x) on obtient l'identite :

$$E_z\, G^*(z) = F + N\, E_x\, G(x) \quad ,$$ le résultat est établi.

(2) ne diffère de l'inégalité classique que par la présence de F.

3/ - Conditions d'égalité.

Reprenant le raisonnement précédent, on voit que trois conditions sont nécessaires et, dans l'ensemble, suffisantes pour que l'on ait égalité dans (2). Ce sont :

1) $x\,\#\,(z) = \bar{x}(z)$

2) $v(z)\, G^*(z) = 1$,

pour presque toutes les valeurs de z, c'est-à-dire : $g^*(\frac{x}{z})$, une distribution de Laplace-Gauss pour presque toutes les valeurs de z.

3) $v(z)$, une constante.

Il en résulte, en inversant les données du problème, qu'à toute densité $f^*(y)$ et à toute fonction $b(y)$ fixant arbitrairement la régression de x sur y, correspondent des fonctions $f(x)$ et $g(\frac{y}{x})$ donnant lieu à l'égalité dans (2).

Considérons maintenant le cas qui présente un certain intérêt pratique où y est en régression dure sur x, c'est-à-dire où y est la somme d'une fonction certaine a(x) et d'un bruit de densité de probabilité indépendante de x.

On va voir que sous cette condition en apparence très faible il ne peut y avoir égalité dans (2) que si la distribution simultanée de x et y est une distribution de Laplace Gauss à deux variables, tout au moins quand on impose à a(x) d'être une fonction analytique de x.

Soit donc à résoudre l'équation fonctionnelle :

$$2\pi f(x)\, g(y - a(x)) = f^*(y) \exp - \frac{1}{2}(x - b(y))^2 \qquad (3)$$

où f, g et f* sont des densités de probabilité admettant des dérivées logarithmique du premier ordre. On obtient en dérivant :

$$\frac{f'(x)}{f(x)} - a'(x) \frac{g'(y - a(x))}{g(y - a(x))} = b(y) - x$$

$$\frac{g'(y - a(x))}{g(y - a(x))} = \frac{f^{*\prime}(y)}{f^*(y)} + b'(y)(x - b(y)).$$

On peut évidemment admettre que a'(x) n'est pas identiquement nulle car le contraire reviendrait à supposer que x et y sont indépendants. En éliminant $\frac{g'}{g}$ on obtient :

$$\left(\frac{f'(x)}{f(x)} + x\right)(a'(x))^{-1} + b(y)\, b'(y) - \frac{f^{*\prime}(y)}{f^*(y)} - \frac{b(y)}{a'(x)} + xb'(x) = 0. \qquad (4)$$

Désignons cette expression par K(x,y) et formons la différence :

K(x + h;y + h) - K(x+k;y) - K(x; y+h) + K(x;y), il vient :

$$(b(y + h) - b(y))\left(\frac{1}{a'(x + k)} - \frac{1}{a'(x)}\right)^{-1} + k(b'(y+h) - b'(y)) = 0.$$

Si b'(y) est une constante, il en est de même de a'(x) et en portant ces résultats dans (4), on vérifie que h(x;y) est une densité de Laplace-Gauss.

Si b'(y) est une fonction de y non réduite à une constante, la dernière équation reécrite sous la forme :

$$(b(y + h) - b(y))(b'(y+h) - b'(y))^{-1} = k\left(\frac{1}{a'(x+k)} - \frac{1}{a'(x)}\right)^{-1}.$$

Ceci implique que les deux membres soient égaux à une constante, donc que b(y) soit une fonction exponentielle et a(x) une fonction logarithmique ; portant ces résultats dans (4), on constate que les variables se séparent encore et l'on obtient finalement :

$$f(x) = C_1(x+\alpha)^{\frac{\beta}{\mu}} \exp - \frac{(x-\nu)}{2}$$

$$f^*(y) = C_2 \exp\{\beta y + \frac{1}{2}(\alpha + \nu + \lambda e^{\mu y})^2\}$$

$$g(y;x) = C_3 \exp\{\beta(y - \mu^{-1}\,\mathrm{Log}(x+\mu)) + \lambda e^{-\mu y + \mathrm{Log}(x+\alpha)}\}$$

ou $\alpha, \beta, \lambda, \mu$ et ν sont des constantes arbitraires et C_1, C_2, et C_3 des constantes fixées par normalisation.

BULLETIN

OF THE

AMERICAN MATHEMATICAL SOCIETY

EDITED BY

J. C. OXTOBY B. J. PETTIS

G. B. PRICE

VOLUME 63

JANUARY TO DECEMBER, 1957

PUBLISHED BY THE SOCIETY

MENASHA, WIS., AND PROVIDENCE, R.I.

321*t*. M. P. Schützenberger: *A generalization of the Fréchet-Cramér inequality to the case of Bayes estimation.*

Let $f(x)$ be the a priori density function of x; $g(y|x)$ the conditional density function of y. For fixed x, the set of n independent y-variates is represented by z. The density function of z is $f'(z)$ and $g'(x|z)$ is the a posteriori density function of x, for given z. The a posteriori variance of the Bayes estimate is $v_z^2 = \int (x-\bar{x})^2 g'(x|z)dx$ and $v^2 = E_z v_z^2 = \int v_z^2 f'(z)dz$ is its average over z. $F = \int (\partial f(x)/\partial x)^2 (f(x))^{-1}dx$; $G = E_z G_z$ with $G_z = \int ((\partial/\partial x)g(y|x))^2 (g(y|x))^{-1}dy$; $G' = E_z G_z'$ with $G_z' = \int ((\partial/\partial x)y'(x|z))^2 (g(x|z))^{-1}dx$. The usual assumptions on f and g, which insure that F, G_z, G_z' are finite are made. Since $0 = F' = \int ((\partial/\partial x)f'(z))^2 (f'(z))^{-1}dz$, it is easily seen that $F+nG = G'$ (Third London Symposium on Information Theory, 1955, p. 18). Furthermore, it is a classical result that $v_z^2 G_z' \geqq 1$. Thus $v^2 = E_z v_z^2 \geqq (E_z 1/v_z^2)^{-1} \geqq (E_z G_z')^{-1} = (F+nG)^{-1}$, which is the desired inequality that tends to the usual form when n goes to infinity. It reduces to an equality if and only if $v^2 = v_z^2 = (G_z')^{-1}$ for all z, that is, if and only if $g'(x|z)$ is gaussian with variance independent of z. If, furthermore, $y-x = t$ has a distribution $h(t)$ independent of x, this implies that $f(x)$ and $h(t)$ are also gaussian. (This work was supported in part by the Army (Signal Corps), the Air Force (Office of Scientific Research, Air Research and Development Command), and the Navy (Office of Naval Research).) (Received November 5, 1956.)

Séminaire Dubreil.
Algèbre et théorie
des nombres

MARCEL P. SCHÜTZENBERGER

Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, n° 1 (1958-1959), exp. n° 1, p. 1-23.

<http://www.numdam.org/item?id=SD_1958-1959__12_1_A1_0>

Faculté des Sciences de Paris
-:-:-
Séminaire P. DUBREIL
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1958/59
-:-:-

1-01

10 novembre 1958

SUR UNE PROPRIÉTÉ COMBINATOIRE DES ALGÈBRES DE LIE LIBRES POUVANT ÊTRE UTILISÉE DANS UN PROBLÈME DE MATHÉMATIQUES APPLIQUÉES

par Marcel P. SCHÜTZENBERGER

INTRODUCTION. - Le but de ces notes est de signaler la possibilité d'utiliser, dans un problème de Mathématiques appliquées ([1]), certaines propriétés combinatoires élémentaires des bases de Marshall HALL des algèbres de Lie libres.

Dans la section I, on rappelle divers résultats fondamentaux de Marshall HALL [9] et de ŠIRŠOV [17].

Dans la section II, on vérifie les propriétés cherchées, qui permettent d'ailleurs de donner une démonstration nouvelle d'un théorème de MEIER WUNDERLI [16].

Dans la section III, on complète les considérations précédentes en montrant que la méthode de Birkhoff donne une démonstration très simple de l'indépendance des bases de Marshall HALL.

Dans la section IV, on vérifie que le calcul des "shuffles" de CHEN, FOX et LYNDON [2], ou plutôt un cas particulier de celui-ci, s'applique encore aux bases considérées ici.

Je remercie M. NAZARD pour de nombreuses et utiles discussions.

([1]) consistant à construire des sous-demi-groupes (sous-monoïdes) G du demi-groupe (monoïde) libre F satisfaisant les deux conditions :

$\mathfrak{U}_z$: pour tout $f, f' \in F$, si $ff', f'f \in G$ alors $f, f' \in G$.

$\mathfrak{N}_\ell$: pour tout $f \in F$, $Ff \cap G \neq \emptyset$.

(G est "net à droite" selon la théorie de P. DUBREIL, cf. [3], [4], [5], [6]).

La signification de ce problème est discutée dans [8] et surtout dans [15], ce dernier ouvrage contenant une bibliographie très complète de la question, apparemment insoupçonnée des auteurs de [8].

1-02

I. Résultats préliminaires

I.1. Définitions préliminaires.

Soient A un ensemble, $D = D(A)$ le système algébrique libre à une seule opération (ne satisfaisant aucune identité) sur A (cf. [10]). Par définition, $D = A \cup D^+$, où D^+ est construit par induction comme l'ensemble des symboles $d = [d' , d'']$ avec $d' , d'' \in D$. On dira que d' (resp. d'') est le composant gauche (resp. droit) d'ordre un de d ; d sera le composant d'ordre zéro de soi-même.

Un composant gauche (resp. droit) d'ordre α d'un composant (gauche ou droit) d'ordre α' de d sera un composant gauche (rep. droit) d'ordre $\alpha + \alpha'$ de d.

Pour tout sous-ensemble $X \subset D$, on désignera par $\mathfrak{F}(X)$ le sous-demi-groupe (sous-monoïde) engendré par X du demi-groupe libre $S = \mathfrak{F}(D)$ engendré par D. 1 désignera l'élément neutre de S.

Soit $s = d_1 d_2 \cdots d_i \cdots d_n$ un élément de S factorisé de la façon indiquée en un produit d'éléments de D. On pose :

$$\delta_j s = s , \quad \text{si} \quad j \neq 1 , 2 , \cdots , i , \cdots , n \quad \text{ou si} \quad d_j \in A ;$$

$$\delta_i s = d_1 d_2 \cdots d_{i-1} d' d'' d_{i+1} \cdots d_n \quad \text{si} \quad d_i = [d' , d''] .$$

Les δ_j engendrent de façon naturelle un demi-groupe $\Delta = \{\delta\}$ d'opérateurs de S dans lui-même ; si $s' = \delta s$, on dira que s' est une décomposition de s. Les facteurs de s' sont, de façon bien déterminée (pour δ fixé) des composants des facteurs de s, ou, pour abréger, des composants de s.

Réciproquement on pose

$$\delta_j^{-1} s = s , \quad \text{si} \quad s \in D \quad \text{ou si} \quad j \neq 1 , 2 , \cdots , n$$

$$\delta_1^{-1} s = [d_n , d_1] d_2 \cdots d_i \cdots d_n , \quad \text{quand} \quad j = 1$$

et dans les autres cas :

$$\delta_i^{-1} s = d_1 \cdots d_{i-2} [d_{i-1} , d_i] d_{i+1} \cdots d_n$$

$\delta_i^{-1} s$ est une recomposition de s.

Tout $s \in S$ possède une décomposition unique notée $\delta^* s$ qui est un élément de $F (= \mathfrak{F}(A))$; δ^* est donc un endomorphisme de demi-groupe $S \to F$. La degré $|s|$ de s est la longueur de $\delta^* s$.

Pour tout sous-ensemble $X \subset S$ on pose

$$\mathfrak{Z}_p(X) = \{ s \in \mathfrak{F}(X) : s = x^p \quad (x \in X) ; \quad s \notin \mathfrak{Z}_{p+1>p}(X) \}$$

et

$$\mathfrak{Z}(X) = \bigcup_{1 \leq p < \infty} \mathfrak{Z}_p(X) \quad .$$

Si $s' = d_j\, d_{j+1} \cdots d_n\, d_1\, d_2 \cdots d_{j-1}$ se déduit de $s = d_1\, d_2 \cdots d_j \cdots d_n$ par une permutation circulaire de ses facteurs, s et s' seront dits π-conjugués (2).

Manifestement si $s \in \mathfrak{Z}_p(S)$ il en est de même de tous les éléments de sa π-classe (c'est-à-dire : de l'ensemble des éléments π-conjugués de s).

I.2. Monômes standards.

On suppose donnée une fois pour toute une relation d'ordre total $<$ sur D satisfaisant :

(H0) : si d' est un composant (gauche ou droit) d'ordre $\geqslant 1$ de d, alors $d' < d$.

On définit par induction un sous-ensemble $H = H(A)$ de D par les règles suivantes :

$A \subset H$ et si $d = [d', d''] \in D^+$, $d \in H$ si et seulement si

(H1) $\qquad d', d'' \in H$

(H2) $\qquad d' > d''$

(2) La relation de π-conjugaison introduite ici n'est évidemment rien d'autre que la restriction à S de la relation habituelle de conjugaison du groupe libre engendré par D. On notera que s et s' sont π-conjugués si et seulement s'il existe $s'' \in S$, tel que $ss'' = s''s'$. La théorie générale de ces équivalences est faite par R. CROISOT dans [3].

1-04

(H3) ou bien $d' \in A$ ou bien, si $d' = [d'', d'^{\vee}]$, $d'^{\vee} \leqslant d''$.

Ces définitions sont celles de Marshall HALL, sauf (H0) qui remplace la condition un peu plus stricte :

(H0)' si $|d'| < |d|$, alors $d' < d$ (cf. [9]).

Après ŠIRŠOV [17], on considère une partition $H = Q \cup P$ telle que $q < p$ pour tout $q \in Q$, $p \in P$. On appellera "partion de Širšov" toute partition de H satisfaisant cette condition.

A l'intérieur de P, on distingue le sous-ensemble

$$K = \{p \in P : p \in A \text{ ou } p = [d', d''] \text{ avec } d'' \in Q\}$$

Dans tout le reste de ces notes, sauf mention expresse du contraire, on supposera fixés une fois pour toutes P et Q. Les cas le plus intéressant sont évidemment ceux où $Q = H$ et $P = K = \emptyset$; ou, à l'opposé, où $Q = \emptyset$ $P = H$ et $K = A$.

PROPRIÉTÉ I.1. - Soit d_i un facteur de $s = d_1 \dots d_i \dots d_n$ où s est une décomposition d'un élément $\overline{s} \in \mathfrak{F}(H)$

1° $s \in \mathfrak{F}(H)$

2° si d_i est un composant gauche d'un facteur de $\overline{s}$, $d_i > d_{i+1}$.

3° si d_i est un composant droit d'un facteur h_j de $\overline{s}$ ou bien $d_{i-1} \leqslant d_i$ ou bien $d_{i-1} > d_i$ et alors $[d_{i-1}, d_i]$ est un composant de h_j.

DÉMONSTRATION. - Le 1° est une conséquence immédiate de (H1). Supposons le 2° et le 3° déjà établis pour s, et montrons qu'ils sont encore vrais pour $\delta_i\, s = d_1\, d_2 \dots d_{i-1}\, d'\, d''\, d_{i+1} \dots d_n$. Les seuls cas à considérer sont évidemment :

- d', d'' : d'après (H2), $d' > d''$, d' et d'' sont respectivement des composants gauches et droits d'un certain facteur h_j de $\overline{s}$ dont, par hypothèse, $d_i = [d', d'']$ est un composant (écentuellement d'ordre zéro !) ;

- si d_{i-1} (resp. d_{i+1}) est un composant droit (resp. gauche) ou d'ordre zéro le résultat subsiste ;

- si d_{i-1} est un composant gauche : par induction $d_{i-1} > d_i$ et, a fortiori, $d_{i-1} > d'$ d'après (H0) ;

- si d_{i+1} est un composant droit : on a toujours $d'' \leq d_{i+1}$, car, ou bien $d_i < d_{i+1}$, et a fortiori $d'' < d_{i+1}$ ou bien $d_i > d_{i+1}$; par induction, $[d_i , d_{i+1}]$ est un composant d'un certain $h_j \in H$ et l'on a $d'' \leq d_{i+1}$ d'après (H3).

On observera que l'énoncé subsiste si l'on suppose que les indices sont pris modulo la longueur du mot considéré (c'est-à-dire $d_{i+1} = d_1$ quand $i = n$, et $d_{i-1} = d_n$ quand $i = 1$).

Considérons en particulier $h \in H$ et ce que nous appellerons sa décomposition normale (à gauche) d'ordre p :

$$s = \delta_1^p h = \delta_1 (\delta_1^{p-1} h) = h_1^* h_2 \dots h_{p+1}$$

h_{p+1} étant le composant droit (d'ordre 1) de h, h_p, le composant droit (d'ordre 1) du composant gauche (d'ordre 1) de h, etc.

h_1^* est par définition le composant "d'extrême gauche" d'ordre p de h.

En appliquant la propriété 1, on obtient immédiatement

$$h_1^* > h_2 \leq h_3 \leq \dots \leq h_{p+1} .$$

Tenant compte de (H0) et du fait que tout composant propre c'est-à-dire d'ordre $\neq 0$), non d'extrême gauche de h, est composant de l'un des h_i $(2 \leq i \leq p+1)$ il en résulte que seuls les composants d'extrême-gauche de h peuvent être en relation $\geqslant$ avec son composant droit d'ordre un.

PROPRIÉTÉ I.2. (ŠIRŠOV). - Tout $p \in P$ admet une et une seule décomposition dont tous les facteurs appartiennent à K. Inversement, tout $p \in P$ appartient à K, si et seulement si aucun de ses composants propres, non d'extrême gauche, appartient à K.

DÉMONSTRATION.

1° si $h \in A$, la propriété est trivialement vérifiée. Soit donc $p = [h' , h'']$; si $p \in K$, $h'' \in Q$, et comme toute décomposition de p admet comme facteurs ceux d'une décomposition de h'', p ne peut pas être décomposé de la façon indiquée ; si $p \notin K$, $h'' \in P$ et a fortiori (d'après (H2)) $h' \in P$; par induction chacun des facteurs de $\delta_1 p = h'h''$ admet une décomposition du type indiqué.

2° Si $p \in P$ admet un composant propre non d'extrême-gauche k appartenant à K, le composant droit d'ordre un, h'' de p est tel que $h'' \geqslant k$; donc $h'' \in P$ et $p \notin K$.

3° Supposons déjà établi que pour tous les $p' \in P$ tels que $|p'| < |p|$, $p' \in K$ si aucun des composants non d'extrême-gauche de p', appartient à K, et soit $p = [h', h'']$ ayant cette propriété; celle-ci est encore vérifiée pour h'' donc (par l'hypothèse d'induction), h'' lui-même appartiendrait à K s'il appartenait à P, comme ceci est exclu par hypothèse, $h'' \in Q$ et donc $p \in K$.

PROPRIÉTÉ I.3. - Si $P \neq \emptyset$ à tout $q \in Q$ il correspond au moins un $k \in K$ dont q est un composant d'extrême-droite.

DÉMONSTRATION. - D'après la propriété 2, $P \neq \emptyset$ entraîne $K \neq \emptyset$. Le résultat est trivialement vrai quand $K \cap A \neq \emptyset$ ou quand K contient un $k = [k_1', k_1]$ avec $k_1 \leqslant q$ car, d'après (H3), $[k, q] \subset H$ (et donc $[K, q] \in K$) puisque $k > q$. Considérons $k \in K$, quelconque et une décomposition "normale à droite" de k :

$$k = h_1' h_2' \ldots h_i' h_i^* \quad \text{avec} \quad k = [h_1', h_1] ; \quad h_1^* = [h_2', h_2^*] ; \quad h_{i-1}^* = [h_i', h_i^*]$$

Supposons le résultat déjà établi pour tous les $q' \in Q$ tels que $h_i^* \leqslant q'$ où h_i^* est le plus petit (selon $\leqslant$) composant d'extrême-droite de h tel que $h_i^* > q$:

Si $h_i^* \in A$, $q_1 = [h_i, q] \in H$ d'après (H3) ;

Si $h_i^* = [h_{i+1}', h_{i+1}^*]$, par hypothèse $h_{i+1}^* \leqslant q$ et donc, encore d'après (H3), $q_1 = [h_i^*, q] \in H$.

Dans les deux cas, $q_1 > h_i^*$ et q_1 admettant q comme composant droit d'ordre un, le résultat est établi par induction.

REMARQUE I.1. - Il résulte de la propriété I.2 qu'à tout $d \in \mathfrak{F}(D(P))$ ($D(P)$: l'ensemble des éléments de D admettant une décomposition dont tous les facteurs sont dans P), correspond une et une seule décomposition que l'on notera $\delta_P d$ et dont tous les facteurs sont dans K.

Après ŠIRŠOV, on dira que d et d' ($d, d' \in \mathfrak{F}(D(P))$) ont le même "P-contenu" si $\gamma \delta_P d = \gamma \delta_P d'$ où γ désigne l'homomorphisme canonique (de demi-groupe)

de $\mathcal{F}(K)$ dans le demi-groupe commutatif libre engendré par K.

Manifestement, si d et d' ont le même P-contenu, d et d' ont aussi le même P'-contenu pour toute partition de Širšov : $H = Q' \cup P'$, telle que $P' \supset P$. On dira que d est en relation ρ_P avec d' quand :

1° d et d' ont le même P'-contenu pour tout $P' \supset P$, $P' \neq P$

2° si $\gamma \delta_P d = k_1^{n_1} k_2^{n_2} \dots k_m^{n_m} \dots$; $\gamma \delta_P d' = k_1^{n'_1} k_2^{n'_2} \dots k_m^{n'_m} \dots$ où $k_1 < k_2 < k_3 < \dots < k_m < \dots$ sont les éléments de K et si pour un certain m :

$$n_m > n'_m \quad \text{et} \quad \sum_{i=m+1}^{\infty} n_i = \sum_{i=m+1}^{\infty} n'_i$$

ρ_P est une relation de préordre et la relation $\gg$ définie par

$$d \gg d'$$

si et seulement s'il existe une partition de Širšov $H = Q'' \cup P''$ telle que $d \rho_{P''} d'$ est une relation d'ordre total sur D.

On notera que $d \rho_P d'$ entraîne $[d , d''] \rho_P [d' , d''']$ pour toutes les paires $d'' , d''' \in D(P)$ ayant le même P-contenu.

REMARQUE I.2. - Il sera commode d'utiliser la notation suivante : la paire (h , h') sera dite "légale" si :

1° $h , h' \in Q \cup K$

2° ou bien $h \leqslant h'$, ou bien $[h , h'] \in Q \cup K$, ou bien $h , h' \in K$.

On utilisera le fait que si (h , h') est légale, il en est de même pour (h , h''), quand $h' \leqslant h''$ et $h'' \in Q \cup K$.

En effet, puisque $h \in Q \cup K$:

- si $h'' \in K$: ou bien $h \leqslant h''$ ou bien $h \in K$

- si $h'' \in Q$: ou bien $h \leqslant h''$ ou bien $h > h''$, et alors soit $h \in A$, soit $h = [h''' , h^{IV}]$ avec $h^{IV} \leqslant h'$, donc $h^{IV} \leqslant h''$; dans les deux cas,

$$[h , h''] \in H$$

et d'après la propriété 2

$$[h , h''] \in Q \cup K .$$

II. Théorème de Meier-Wunderli.

II.1. Recompositions légales.

Soit $s = h_1 h_2 \cdots h_i \cdots h_n$; $s \in \mathfrak{F}(H)$.

s sera dit "légal" (resp. π-légal, resp. complètement légal) si toutes les paires (h_{i-1}, h_i), avec $i = 2, \ldots, n$ (resp. avec $i = 1, 2, \ldots, n$, les indices étant pris modulo n ; resp. toutes paires $(h_i, h_{i'})$ avec $i < i'$), sont légales.

Manifestement, s est π-légal si et seulement si $s^2 = ss$ est légal ou, de façon équivalente, si tous les éléments de sa π-classe sont légaux.

On notera les cas particuliers suivants qui définissent en même temps des notations utilisées plus loin :

1° Tous les mots de F, $T = \mathfrak{F}(K)$; $\mathfrak{F}(Q)$ sont à la fois π-légaux et complètement légaux.

2° Soit $V \in \mathfrak{F}(Q)$ l'ensemble des Q-mots non décroissants ($v \in V$; si $v = e$ ou si $v \notin Q$ ou si $v = v_1 v_2 \cdots v_n$ avec $v \in \mathfrak{F}(Q)$ et $v_1 \leqslant v_2 \leqslant \cdots \leqslant v_n$) .

3° W : l'ensemble des mots de la forme vt ($v \in V$; $t \in T$) . Tous les mots de W et de V sont complètement légaux (mais en général non π-légaux).

D'autre part on dira que le facteur h_i de s est "critique" si :

(C1) $\qquad h_i \in Q$;

(C2) $\qquad h_{i-1} > h_i \leqslant h_{i+1}$

(les indices étant pris modulo n :

$h_{i+1} = h_1$ pour $i = n$;

$h_{i-1} = h_n$ pour $i = 1$).

Une recomposition δ_i^{-1}, où d_i est un facteur critique, sera dite "légale".

1-09

PROPRIETE II.1. - Si s est π-conjugué d'une décomposition de $\bar{s} \in T \cup \mathcal{F}(Q)$ une condition nécessaire et suffisante pour qu'il ne possède aucun facteur critique est qu'il soit π-conjugué de $\bar{s}$ lui-même.

Réciproquement quel que soit le facteur critique h_i de s, $\delta_i^{-1} s$ est π-conjugué d'une décomposition de $\bar{s}$ et dans les mêmes conditions quand s est une décomposition de $\bar{s}$, $\delta_i^{-1} s$ est aussi une décomposition de cet élément.

DEMONSTRATION.

Si $\bar{s} \in T$, il en est de même de sa π-classe et aucun de ses facteurs ne satisfait (C1).

Si $\bar{s} \in \mathcal{F}(Q)$, ou bien $\bar{s} = q$ $(q \in Q)$ ou bien $\bar{s} = q^p$: dans les deux cas (C2) n'est pas satisfaite.

Soit d'abord $s \in \mathcal{F}(K \cup Q)$ quelconque. Si $s \notin \mathcal{F}(Q) \cup \mathcal{F}(T)$, s possède au moins deux facteurs différents, et donc au moins un facteur satisfaisant (C2) ; supposons que h_i soit précisément le plus petit (selon $\leq$) facteur de s : s'il appartenait à K il en serait de même de tous les autres facteurs de s (puisque $q < k$ pour tout $q \in Q$ et $k \in K$). Or ceci est impossible, dans les conditions de l'énoncé, car si s est π-conjugué d'une décomposition non triviale de $\bar{s}$, s admet au moins deux facteurs h_{j-1}, h_j tels que $[h_{j-1}, h_j] \in K \cup Q$: donc (d'après la propriété I.1) $h_{j-1} > h_j$ (et donc $s \notin \mathcal{F}(Q) \cup T$) et donc (d'après la propriété I.2) $h_j \in Q$, ce qui achève la preuve que h_i est critique. On a montré du même coup que tout $s \in \mathcal{F}(K \cup Q)$, $s \notin \mathcal{F}(Q) \cup T$ admet au moins un facteur critique.

RECIPROQUE. - Soit h_i, un facteur critique de s ;

1° h_i n'est pas un composant d'ordre zéro d'un facteur de $\bar{s}$ car : $h_{i-1} > h_i$ d'après (C2), ce qui exclut le cas où $\bar{s} \in \mathcal{F}(Q)$; $h_i \in Q$ (d'après (C1)), ce qui exclut le cas ou $\bar{s} \in T$.

2° h_i n'est pas un composant gauche d'après la proposition I.1 et l'inégalité $h_i \leq h_{i+1}$; donc, d'après la même propriété, $[h_{i-1}, h_i]$ est un composant de $\bar{s}$ puisque $h_{i-1} > h_i$.

Si $s = \delta \bar{s}$, le facteur h_1 (le premier facteur à gauche) de s ou bien appartient à K ou bien, toujours d'après la proposition I.1, satisfait $h_1 > h_2$;

h_i n'est donc jamais un facteur critique et $\delta^*(\delta_i^{-1} s) = \delta^* \bar{s}$ pour tout facteur critique h_i de $s = \delta\bar{s}$.

Soit $\bar{s}' = \delta_s^{-1*}$ un élément sans facteur critique obtenu par une suite de recomposition légales, effectuées dans un ordre quelconque à partir de $s = \delta\bar{s}$ (resp. d'un élément π-conjugué de $s = \delta\bar{s}$) , et en particulier à partir de $s = \delta^* \bar{s} \in F$ (resp. d'un mot s de la π-classe de $\delta^* \bar{s}$) . On vient de voir que tous les facteurs de $\bar{s}'$ sont des composants de $\bar{s}$; $\bar{s}'$ est une décomposition de $\bar{s}$ mais, d'une part $\bar{s}' \in T \cup \mathcal{Z}(Q)$ (puisque $\bar{s}'$ n'a pas de facteur critique), d'autre part on sait qu'aucune décomposition propre de $\bar{s} \in T \cup \mathcal{Z}(Q)$ n'appartient à cet ensemble. $\bar{s}'$ est donc identique à $\bar{s}$ (resp. est π-conjugué de $\bar{s}$).

PROPRIETE II.2 (MEIER-WUNDERLI [16]). - δ^* établit, pour tout $p \geqslant 1$, une application bijective de l'ensemble des π-classes de $\mathcal{Z}_p(T) \cup \mathcal{Z}_p(Q)$ sur celui des π-classes de $\mathcal{Z}_p(F)$.

DEMONSTRATION. - Montrons d'abord que si s est π-légal il en est de même de $\delta_i^{-1} s$, si et seulement si h_i est un facteur critique : en effet, d'après la propriété I.2 et (H2) , la condition (C1) et l'inégalité $h_{i-1} > h_i$ sont nécessaire et suffisantes (puisque s est π-légal par hypothèse) pour que $h = [h_{i-1} , h_i]$ appartienne à $K \cup Q$. Considérons la paire (h , h_{i+1}) : puisque, par construction, $h \notin A$, (h , h_{i+1}) est légale (d'après (H3)) si et seulement si $h_i \leqslant h_{i+1}$. Considérons la paire (h_{i-2} , h) ; ou bien $h_{i-2} \leqslant h$ ou bien, dans le cas contraire, $[h_{i-2} , h] \in K \cup Q$, car $h_{i-2} > h$ implique, a fortiori, $h_{i-2} > h_i$, donc $[h_{i-2} , h_i] \in K \cup Q$ puisque, par hypothèse, s est π-légal, donc, a fortiori, soit $[h_{i-2} , h] \in K \cup Q$, soit $h_{i-2} , h \in K$.

Soit maintenant $f = f'^p \in \mathcal{Z}_p(F)$; d'après la propriété II.1, il correspond à f' un élément $\bar{s}' \in \mathcal{Z}_1(T) \cup \mathcal{Z}_1(Q)$ dont la π-classe est bien déterminée et qui est tel que $\delta^* \bar{s}'$ soit π-conjugué de f' . Considérons $\bar{s}'^p$; $\delta^* \bar{s}'^p$ est π-conjugué de f et donc $\delta^{-1*} f$ est un élément de la π-classe de $\bar{s}'^p$.

Ainsi que l'a montré MEIER WUNDERLI, cette propriété permet de retrouver la formule de WITT [18] (une fois établi que H correspond biunivoquement à une base (indépendante) de l'algèbre de Lie libre sur A) en utilisant un résultat combinatoire dû au Colonel MOREAU [13] .

PROPRIETE II.3. - δ^* établit une application bijective de W (cf. définition supra) sur F .

DEMONSTRATION. - Nous considérons, F , D , H , P , etc. comme des sous-ensembles des systèmes correspondants construits à partir de $A^* = A \cup a^*$ où a^* est un nouvel élément. Il est compatible avec (HO) de supposer que, dans $D(A \cup a^*)$, on a $h < a^*$ pour tout $h \in D = D(A)$; par hypothèse on a donc $a^* \in K(A \cup a^*)$.

Soit maintenant $f \in F(A)$, et considérons $\delta^{-1*}(a^* f) = \overline{s}^*$; manifestement

$$\overline{s}^* \in \mathfrak{F}_1(T(A \cup a^*)) \cup \mathfrak{F}_1(Q(A \cup a^*))$$

et, d'après la propriété II.1, $\delta^* \overline{s}^* = a^* f$. On a donc :

- soit $\overline{s}^* = a^* \overline{s}$ avec $\overline{s} \in T \vee \mathfrak{F}(Q)$ et donc $\overline{s} \in W(A)$.

- soit $\overline{s}^* = k^* \overline{s}'^*$ avec $k^* \in K(A \cup a^*)$ et $\overline{s}' \in T(A)$. Considérons dans ce cas la décomposition normale à gauche $a^* h_1 h_2 \dots h_n$ de k^* ; d'après les remarques faites à la fin de la propriété I.1, $h_1 \leq h_2 \leq \dots \leq h_n$, c'est-à-dire $h_1 h_2 \dots h_n \in V$ et par conséquent $\overline{s} = \delta^{-1**} f = h_1 h_2 \dots h_n \overline{s}' \in W$. et $\delta^* \overline{s} = f$. Réciproquement, si $w \in W$ est de la forme vt avec $t \in T$ et $v = h'_1 h'_2 \dots h'_n$ de longueur non nulle $[a^* h'_1] h'_2] \dots] h'_n] \in K(A \cup a^*)$ et δ^* et δ^{-1**} sont donc bien inverses l'un de l'autre.

REMARQUE II.1. - La propriété II.3 peut aussi être établie en considérant des facteurs "c-critique" d_i définis par

(C'1) $\qquad d_i \in Q$;

(C'2) $\qquad d_i$ est critique et $i = 2, \dots, n-1$ ou $d_i = d_n$ et $d_{n-1} > d_n$

(C'3) $\qquad d_i \leq d_{i'}$ pour tout $i' \geq i$.

W est alors l'ensemble des $s \in \mathfrak{F}(Q \cup K)$ n'admettant aucun facteur c-critique et on montre comme plus haut que si s est complètement légal, il en est de même de $\delta_i^{-1} s$ si et seulement si d_i est c-critique.

PROPRIETE II.4. - L'application $\delta^* : T \to F$ est un monomorphisme et $G = \{\delta^* t : t \in T\}$ satisfait les conditions $\mathfrak{U}_2$ et $\mathfrak{V}_\ell$.

DEMONSTRATION.

1° Que δ^* est un monomorphisme est une conséquence immédiate de la propriété II.1, car la restriction de δ^* à T admet comme on l'a vu, un inverse δ^{-1**} G est donc un sous-demi-groupe libre de F .

2° Soit $ff' = \delta^* t$ et $f'f = \delta^* t'$ ($f , f' \in F$; $t , t' \in T$) . Puisque ff' et f'f sont π-conjugués, il en est de même de t et de t' ; considérons la recomposition légale de ff' , $h_1 h_2 \dots h_n$ qui est de longueur minimale parmi celles possèdant la propriété que $\delta^*(h_1 h_2 \dots h_i) = f$ et $\delta^*(h_{i+1} h_{i+2} \dots h_n) = f'$. Comme t' est π-conjugué de t , les facteurs $h_1 , h_2 , \dots , h_n$ sont des composants de t' ; en particulier, h_{i+1} est un composant gauche (ou d'ordre zéro) et n'est donc pas un facteur critique ; la même remarque vaut pour h_1 et, puisque par hypothèse la recomposition $h_1 \dots h_i h_{i+1} \dots h_n$ est de longueur minimale avec les propriétés indiquées, elle n'admet pas de facteur critique. Tous les facteurs h_i appartiennent donc à K et par conséquent $\delta^{-1*} f$, $\delta^{-1*} f' \in T$ ce qui achève de montrer que G satisfait $\mathfrak{U}_z$.

3° Le résultat est trivial si $\delta^{-1**} f \in T$; si $\delta^{-1**} f = qt$ ($q \in Q$, $t \in T$) , on sait trouver (d'après la propriété I.3) $k , k' \in K$ tels que $\delta^* k' = (\delta^* k)(\delta^* q)$; on a donc $\delta^{-1**}((\delta^* k)f) \in T$ et, par conséquent, $F f \cap t \neq \emptyset$.

Si $\delta^{-1**} f = vt$, $v = q_1 q_2 \dots q_n \in V$ et s'il existe un $h' \in H$ tel que $k = [h' , q_1] \in K$ on a encore $\delta^{-1**}((\delta^* h')f) = [[h' q_1] q_2] \dots] q_n] t \in T$ (et donc $F f \cap G \neq \emptyset$) puisque en raison des inégalités $q_1 \leq q_2 \leq \dots \leq q_n < k$, l'élément $[h' , q_1] q_2] \dots] q_n]$ appartient à K .

On peut donc par double induction supposer que le résultat est déjà établi pour tous les f' tels que $\delta^{-1**} f' = q'_1 q_2 \dots q_n t$ avec $q'_1 > q_1$ et comme en utilisant la propriété I.3 on sait trouver un h' tel que $[h' , q_1] \in Q \cup K$ le résultat est établi dans tous les cas.

REMARQUE II.2. - Il existe au moins un autre type de sous-demi-groupes G de F satisfaisant $\mathfrak{U}_z$ et $\mathfrak{U}_\ell$, ce sont les idéaux à droite J ($JF = F$) qui satisfont la condition :

$\mathfrak{U}_\ell$: pour tout $f \in F$: si $f J \cap J \neq \emptyset$ alors $f \in J$. (qui sont "unitaires à gauche" dans la théorie de P. DUBREIL [4] , [5] , [6]).

Ceci est notamment le cas desidéaux J de la forme $\overline{f}F$, où $\overline{f}$ est un mot fixe de F, ne pouvant pas être écrit sous la forme $f'f''f'$, avec $f', f'' \in F$ et f' de longueur non nulle (cf. [15], pour une théorie de ces problèmes et de leurs liens avec la notion probabiliste "d'événement récurrent"); j'ignore s'il existe encore d'autres types de sous-demi-groupes satisfaisant $\mathcal{U}_z$, et ne pouvant pas être obtenus comme l'intersection de sous-demi-groupes de l'un des deux types décrits ou de leurs opposés.

REMERQUE II.3. - Il ressort de la démonstration que pour un ensemble K donné il existe un entier naturel n tel que quel que soit $f \in F$, il y ait au moins un $f' \in F$ de longueur inférieure à n et tel que $f'f \in \delta^* T$. Il en découle, par une application élémentaire de la théorie des demi-groupes unitaires et nets d'un seul côté ([4], [5], et [6]), que, si A contient $m < \infty$ éléments la fonction entière de la variable λ

$$1 - \sum_{k \in K} \lambda^{|k|} \qquad (|k| : \text{le degré de } k)$$

admet la racine $1/n$.

REMARQUE II.4. - $\mathcal{U}_z$ est évidemment triviale dans le cas des groupes. La condition suivante $\mathcal{U}'_z$ est équivalente à $\mathcal{U}_z$ dans le cas des demi-groupes libres mais non dans le cas des groupes.

Soient F et F' deux demi-groupes (resp. groupes) libres δ^* un homomorphisme $\delta^* : F' \to F$:

$\mathcal{U}'_z$ si $f'_1, f'_2 \in F'$ sont tels qu'il existe un $f \in F$ de longueur non nulle vérifiant $f(\delta^* f'_1) = (\delta^* f'_2) f$, alors il existe un $f' \in F'$ de longueur non nulle vérifiant $f'f'_1 = f'_2 f'$.

III. Indépendance des bases de Marshall Hall.

III.1. Notations. - On garde les notations précédentes, et on convient que pour tout $X \subset S$, $\overline{X}$ désigne le $\mathbb{Z}$-module libre dont X est une base. On convient aussi que les opérations $(x, y) \to xy$ et $(x, y) \to [x, y]$ sont bilinéaires. Donc, en particulier, $\overline{F}$ (resp. $\overline{D}$) peut être considéré comme la $\mathbb{Z}$-algèbre associative (resp. sans identité) libre sur A_o. L'élément neutre 1 de S est considéré comme l'élément unité de $\overline{S}$ et il sera commode de poser :

1-14

$[n , d] = [d , n] = [0 , d] = [d , 0] = 0$ pour tout $n \in \underset{\sim}{Z}$ et $d \in D$.

On définit en outre un homomorphisme (de $\underset{\sim}{Z}$-algèbre associative) $\lambda : \overline{S} \longrightarrow \overline{F}$ par :

$$(s + s')^{\lambda} = s^{\lambda} + s'^{\lambda} \quad ; \quad (ss')^{\lambda} = s^{\lambda} s'^{\lambda} \quad ; \quad [s , s']^{\lambda} = s^{\lambda} s'^{\lambda} - s'^{\lambda} s^{\lambda} \quad .$$

Chaque élément d^{λ} $(d \in D)$ est donc égal à un élément, que l'on désignera par le même symbole, de l'algèbre de Lie libre $\overline{L}(A)$ engendrée par A .

PROPRIÉTÉ III.1 (Marshall HALL, ŠIRŠOV). - $(\overline{D}(P))^{\lambda} \subset \overline{F}^{\lambda}$.

DÉMONSTRATION. - Soient, plus généralement, h et h' deux éléments quelconques de H ; puisque $[h , h']^{\lambda} + [h' , h]^{\lambda} = 0$, on peut supposer que $h \succ h'$, si $[h , h'] \in H$, on a a fortiori $[h , h'] \in P$ quand $h' \in P$; si $[h , h'] \notin H$, nous considérons la partition de Širšov $Q' \cup P'$ de H définie par $\overline{h} \in P'$ si et seulement si $\overline{h} \not\succ h'$. Soit $K' = K'(h')$, $(K' \ni h')$ l'ensemble correspondant défini comme dans I.2 ; naturellement si h appartient à P , P' est un sous-ensemble de P .

Soit $\delta_{P'} h = k'_1 \ldots k'_n$ la décomposition de h dont tous les facteurs appartiennent à K' (cf. Remarque I.1). Supposons déjà établi, pour toutes les paires (h , h') telles que le H-contenu de $[h , h']$ (par rapport au cas particulier où $Q = \emptyset$; $P = H$ et $K = A$) soit inférieur à celui de $\overline{h}\,\overline{h'}$, que $[h h']^{\lambda}$ est égal à une somme de termes $\pm h_i^{\lambda}$ où tous les h_i figurant dans la somme :

1° ont le même P'-contenu que $[h , h']$

2° ont leurs deux composants d'ordre un en relation $\succ$ avec h' .

3° admettent h' comme composant droit.

Si $\overline{h} = [\overline{h}_1 \; \overline{h}_2]$ et, par hypothèse $\overline{h}_1 \succ \overline{h}_2 \succ \overline{h'}$, on a d'après l'identité de Lie :

$$[\overline{h} , \overline{h'}]^{\lambda} = [[\overline{h}_1 , \overline{h'}] , \overline{h}_2]^{\lambda} - [[\overline{h}_2 , \overline{h'}] , \overline{h}_1]^{\lambda}$$

Suivant l'hypothèse d'induction, $[\overline{h}_1 \; \overline{h'}]^{\lambda}$ et $[\overline{h}_2 \; \overline{h'}]^{\lambda}$ sont égaux à des sommes dont tous les termes ont les propriétés voulues et donc, en particulier sont en relation $\succ$ avec $\overline{h'}$; le résultat en découle immédiatement puisqu'il n'y a qu'un nombre fini d'éléments de H ayant un P'-contenu donné.

REMARQUE III.1. - Soient $<$ satisfaisant (HO)' , $H_{m,n}$ l'ensemble des $h \in H$ de degré m dont les deux composants d'ordre un sont de degré $\geqslant n$, $\alpha : \overline{H} \to \overline{H}$ la transformation linéaire induite par une transformation linéaire α_1 de A dans lui-même. La propriété III.1 permet facilement de vérifier que $\alpha \overline{H}_{m,n} \subset \overline{H}_{m,n}$ pour tout n , n . Cette propriété d'invariance des bases de Marshall HALL n'est pas partagée par les bases de CHEN, FOX et LYNDON ([2] , [14]

REMARQUE III.2. - Soient h , h' et $\overline{h}$ trois éléments de H , $\overline{h}$ admettant au moins un composant égal à h ; l'élément $\overline{h}'$ de D , obtenu en subsituant h' à h (une fois) dans l'écriture de $\overline{h}$, n'appartient pas nécessairement à H ; d'après la propriété III.1, on peut trouver une somme $\sum \pm h_i$ telle que $\overline{h}'^{\lambda} = \sum \pm h_i^{\lambda}$; on va montrer que si $h \gg h'$ (où ρ est la relation d'ordre total définie dans la remarque I.1), $\overline{h} \gg h_i$ pour tous les h_i figurant avec un coefficient non nul dans la somme $\overline{h}'^{\lambda}$.

Par hypothèse, il existe une partition de Širšov $H = Q \cup P$ telle que $h , h' \in P$ et que $h \rho_P h'$; P contient certainement les composants droits h_1 et h_1' d'ordre un de h et de h' car sinon, désignant par h_1^* le plus petit de ces deux éléments et par $Q^* \cup P^*$ la partition de Širšov définie par $h'' \in P^*$, si et seulement si $h_1^* \leqslant h''$, on aurait $\gamma\delta_{P^*} h = \gamma\delta_{P^*} h'$ et donc, comme on le vérifie aisément $h = h'$. Le résultat en découle immédiatement par induction car, si $[h , h''] \in H$ ou $[h'' , h] \in H$, h'' est $\gg$ le composant droit d'ordre un de h . Donc, $h'' \in P$ et, comme le P-contenu de tous les termes h_i apparaissant dans la somme $[h' , h'']$ ou $[h'' , h']$ est le même que celui de $[h' , h'']$, on a $[h , h''] \rho_P h_i$ d'après les propriétés de régularité de la relation $\gg$.

Nous considérons maintenant de nouveau une partition de Širšov $F1 = Q \cup P$ fixe et les ensembles T , W , etc. définis au début de la section II. On rappelle que $\overline{F}$ est la Z-algèbre libre engendrée par A .

PROPRIÉTÉ III.2 (G. BIRKHOFF, E. WITT). - $\overline{W}^{\lambda}$ est une base (indépendante) de $\overline{F}$ ([1] , [18]).

DEMONSTRATION. - On suit la méthode de "straightning" de G. BIRKOFF [1] .

Soit U l'ensemble des mots complètement légaux de S . Par définition $F \subset U \subset \mathcal{F}(K \cup Q)$. On définit une application linéaire σ de $\overline{U}$ dans $\overline{W}$ par :

$(u + u')^{\sigma} = u^{\sigma} + u'^{\sigma}$; $u^{\sigma} = u$, si $u \in W$; $(u' u)^{\sigma} = (u' u^{\sigma})^{\sigma}$

et pour tout u appartenant à l'ensemble U' des mots de la forme $u' = hw$ avec $h \in H$, $w \in W$, $w = h_1 w'$; $w' \in W$ et (h , h_1) légal, on pose :

$$(h w)^{\sigma} = h w \quad , \text{ si } h \leqslant h_1 \quad \text{(puisqu'alors } hw \in W\text{)}$$

$$= ([h h_1] w')^{\sigma} + h_1 (h w')^{\sigma} \text{ , si } h \succ h_1 .$$

la définition permet effectivement une construction par induction car, si $h \succ h_1$,

1° les deux termes $[h , h_1] w'$ et hw' sont de longueur strictement inférieure à celle de $h w$.

2° Puisque (h , h_1) est légale, et que $w' = h_2 w''$ avec $h_1 \leqslant h_2$, $(h_1 h_2)$ est légale a fortiori et donc $[h , h_1] w' \in U'$

3° Pour les mêmes raisons, $hw' \in U'$. Par une induction facile on vérifie que le premier facteur à gauche de tous les w_i figurant dans la somme $\sum w_i = (h w')^{\sigma}$ est toujours en relation $\succ$ avec h ou h_2 (selon que $h \leqslant h_2$ ou $h \succ h_2$) et donc, a fortiori, en relation $\succ$ avec h_1 .

On note d'autre part :

4° Que hw , $[h , h_1] w'$ et $h_1 h w'$ ont le même H-contenu

5° que $(h h_1)^{\lambda} = [h , h_1]^{\lambda} + (h_1 h)^{\lambda}$.

Il s'ensuit par induction que pour tout $u \in U$, $(u^{\sigma})^{\lambda} = u^{\lambda}$ ce qui achève la démonstration. On remarquera, qu'il résulte de la construction que pour tout $f \in F$, f^{σ} est une somme dont les coefficients sont non négatifs.

Etant donné (Propriété II.3) qu'il existe une correspondance bijective, conservant le contenu, entre F et W , III.2 montre que W^{λ} est une base indépendante de $\overline{F}$. Donc,

1° Les h^{λ} $(h \in H)$ sont linéairement indépendants et forment une base de l'algèbre de Lie libre engendrée par A (Marshall HALL).

2° Les t^{λ} $(t \in T)$ engendrent une sous-algèbre associative libre de $\overline{F}$ (ŠIRŠOV) puisque les $\delta^{*} t$ $(t \in T)$ engendrent un sous-demi-groupe libre de F (propriété II.4).

Soient R un corps, $\overline{X}$ désignant maintenant le R-module libre engendré par X et $\varphi : \overline{L}(A) \longrightarrow \overline{L}'$, un épimorphisme de $\overline{L}(A)$ la R-algèbre de Lie libre.

REMARQUE III.3. - Quel que soit la base de Marshall HALL, H, il existe un sous-ensemble $Q \subset H$ tel que φQ soit une base (indépendante) de L' et qu'en outre Q contienne tous les composants de ses éléments.

DÉMONSTRATION. - Il est évident que φH est une base (non indépendante) de L' ; définissons une suite $h_1^*, h_2^*, \ldots, h_n, \ldots$ d'éléments de H par les règles suivantes

1° $h_{i+1}^* \in Q(h_i^*)$ où $Q(h_i^*)$ est le sous-ensemble de H formé des éléments dont aucun des composants n'est un $h_{i'}^*$, $(i' \leq i)$.

2° h_{i+1}^* est le plus petit élément de $Q(h_i^*)$ (h_1^* est le plus petit élément de H) selon l'ordre $\gg$ tel que φh_{i+1}^* appartienne au sous-module de L' engendré par tous les φh avec $h \ll h_{i+1}^*$.

Soit maintenant $Q = \bigcap_i Q(h_i^*)$ et $H = Q \cup P$ la partition correspondante de H, Par construction, Q contient tous les composants de ses éléments et les φq, $q \in Q$, sont indépendants ; comme d'après la remarque III.2, $\varphi h \in \varphi Q$ pour tout $h \in P$, le résultat est établi.

On observera que si, ayant défini une nouvelle relation d'ordre $<'$ sur D, satisfaisant (HO) et $h <' h'$, si $h, h' \in Q$ et $h < h'$ ou si $h \in Q$ et $h' \notin Q$, on construit la base de Marshall HALL correspondante H', on a :

$$Q \subset H \cap H'$$

et il existe une partition de Širšov $Q \cup P'$ de H' telle que $\overline{P}'^{\lambda} = \overline{P}^{\lambda}$.

IV. Algèbre de "Shuffle"

Soit $\langle s , s' \rangle$ la forme bilinéaire symétrique sur $\overline{S} \times \overline{S}$ définie à partir de $\langle s , s' \rangle = 1$ ou $= 0$, selon que $s = s'$ ou $s \neq s'$ $(s , s' \in S)$. Le théorème de Poincaré-Birkhoff-Witt peut s'écrire sous la forme :

$$s = \sum_{w \in W} \langle w , s^{\sigma} \rangle w^{\lambda}$$

et et nous allons donner une formule un peu différente pour calculer $\langle w , s^{\sigma} \rangle$ Afin de simplifier les énoncés on suppose désormais que $P = \emptyset$, c'est-à-dire que $H = Q$ et $W = V$.

1-18

On va munir le $\underset{\sim}{Z}$-module $\overline{F}$ d'une structure $\overline{F}_{\top}$ d'algèbre de "shuffle" qui est un cas très particulier des structures de même nom introduites par R. C. LYNDON [14] et dont la théorie est exposée dans [2].

Soit $\top$ une opération linéaire $\overline{F} \times \overline{F} \longrightarrow \overline{F}$ définie par prolongement à partir des règles suivantes :

(S1) $\qquad 1 \top f = 0 \top f = f \top 0 = 0 \; ; \quad f \top 1 = f$ pour tout $f \in F$

et, par induction :

(S2) $\qquad$ si $f = af' \quad (a \in A \; , \quad f' \in F)$,

$$f \top f'' = a(f' \top f'' + f'' \top f') \quad \text{pour tout} \quad f'' \in \overline{F}$$

Posons pour abréger $x \overline{\top} y = x \top y + y \top x$, pour tout x , y et considérons la double identité :

(S0) $\qquad (x \top y) \top z = (x \top z) \top y = x \top (y \overline{\top} z)$.

Il résulte immédiatement de (S0) que $\overline{\top}$ est non seulement commutative mais encore associative car, à cause de la distributivité :

$$(x \overline{\top} y) \overline{\top} z = (x \top y) \top z + (y \top x) \top z + z \top (x \top y) + z \top (y \top x)$$

avec, d'après (S0) :

$$(x \top y) \top z = x \top (y \overline{\top} z) \; ; \quad (y \top x) \top z = (y \top z) \top x \; ;$$

$$z \top (x \top y) + z \top (y \top x) = z \top (y \overline{\top} x) = (z \top y) \top x$$

et par conséquent :

$$\begin{aligned}(x \overline{\top} y) \overline{\top} z &= x \top (y \overline{\top} z) + (y \top z) \top x + (z \top y) \top x \\ &= x \top (y \overline{\top} z) + (y \overline{\top} z) \top x \\ &= x \overline{\top} (y \overline{\top} z) \; .\end{aligned}$$

D'autre part, (S0) est identiquement vérifiée par l'opération $\top$ définie par (S1) et (S2) car (S0) est trivialement vraie si $x = 1$ et, par induction, si (S0) est vraie pour x , y , z $(x \; , \; y \; , \; z \in F)$ et si $a \in A$,

on a, pour ax, y et z :

$$(ax \top y) \top z = (a(x \bar{\top} y)) \top z = a((x \bar{\top} y) \bar{\top} z)$$

$$= a(x \bar{\top} (y \bar{\top} z)) = (ax) \top (y \bar{\top} z)$$

$$= a((x \bar{\top} z) \bar{\top} y) = (ax \top z) \top y$$

Pour tout f, $f' \in F$, $f \bar{\top} f' = \sum f_i$ $(f_i \in F)$ où le contenu de chacun des f_i apparaissant dans cette somme est le même que celui de ff'.

Les f_i sont les "shuffles" de R. C. LYNDON correspondant au cas particulier où la longueur du "shuffle" est la somme de celle des éléments "shuffled" f et f'.

On observera que $\bar{F}_\top$ est la Z-algèbre libre $\bar{Y}$ sur A satisfaisant (S0) ; en effet, on vérifie facilement que si $\bar{Y}$ satisfait cette identité, tout $y \in \bar{Y}$ est une somme finie de termes "normés" c'est-à-dire de la forme $a_1 \top (a_2 \top (a_3 \top (\ldots))$ avec $a_1, a_2, \ldots, a_i \in A$; or, si $\bar{Y} = \bar{F}_\top$, d'après (S2), $a_1 \top (a_2 \top (a_3 \top (\ldots))) = a_1 a_2 a_3 \ldots \in F$ et le résultat découle immédiatement de ce que F est une base indépendante de $\bar{F}$.

Soit maintenant $\tilde{\upsilon} : \bar{W} \to \bar{F}$ l'application définie par les règles suivantes :

1° $a^{\tilde{\upsilon}} = a$ pour tout $a \in A$

2° $h^{\tilde{\upsilon}} = (\delta_1^* h)^{\tilde{\upsilon}}$ pour tout $h \in H$ (où, on le rappelle, $\delta_1^* h$ est la décomposition normale gauche de h).

3° $w^{\tilde{\upsilon}} = (\prod n_i!)^{-1} w^{\bar{\tilde{\upsilon}}} = (\prod n_i!)^{-1} h_1^{\tilde{\upsilon}} \bar{\top} h_1^{\tilde{\upsilon}} \ldots \bar{\top} h_2^{\tilde{\upsilon}} \ldots \bar{\top} h_x^{\tilde{\upsilon}}$ pour tout $w = h_1^{n_1} h_2^{n_2} \ldots h_i^{n_i} \ldots h_x^{n_x}$ avec $w^{\tilde{\upsilon}}$ défini récursivement par $(w h_j)^{\tilde{\upsilon}} = w^{\tilde{\upsilon}} \bar{\top} h_j^{\tilde{\upsilon}}$.

4° $(w + w')^{\tilde{\upsilon}} = w^{\tilde{\upsilon}} + w'^{\tilde{\upsilon}}$.

PROPRIÉTÉ IV.1. - Pour tout $w \in \bar{W}$ et $f \in \bar{F}$,

$$\langle w^{\tilde{\upsilon}}, f \rangle = \langle w, f^{\sigma} \rangle$$

DÉMONSTRATION. - Il suffit évidemment de démontrer le résultat pour $w \in W$ et $f \in F$. Supposons-le déjà établi pour $f' \in F$, et soit $f = af'$, $a \in A$.

1-20

On a :

$$\langle w , (af')^{\sigma} \rangle = \sum_{w' \in W} \langle w , (aw')^{\sigma} \rangle \langle w' , f'^{\sigma} \rangle$$

Soit $w' = h_1^{n_1} h_2^{n_2} \dots h_i^{n_i}$; d'après les résultats de III, on vérifie facilement que

$$\langle w , (aw')^{\sigma} \rangle = 0 ,$$

sauf si w a l'une des formes

$$w = aw' \quad \text{(et alors } a < h_1\text{)}$$

$$w = h_1^{n_1'+1} h_2^{n_2'} \dots h_i^{n_i} \quad \text{(et alors } h_1 = a\text{)}$$

$$w = h_1^{n_1} h_2^{n_2} \dots h_i^{n_i}$$

où les n_i sont reliés aux n_i' par la condition suivante : pour un certain i^*

1° $n_i = n_i' - \nu_i$ $(\nu_i \geqslant 0)$ quand $i < i^*$

2° $n_{i^*} = n'_{i^*} + 1$ et $\delta_i^* h_{i^*} = a h_1^{\nu_1} h_2^{\nu_2} \dots h_{i^*}^{\nu_{i^*-1}}$

3° $n_i = n_i'$ quand $i > i^*$

Dans ce cas,

$$\langle w , (aw')^{\sigma} \rangle = \prod_{i \leq i^*} \left[\begin{matrix} n_i' \\ \nu_i \end{matrix} \right] \quad ([\ ] : \text{le coefficient binomial}).$$

Considérons maintenant w^{τ} ; on a, en raison du fait que $\bar{\tau}$ est associative et commutative et des identités (S1) (S2)

$$w^{\tau} = \left(\prod n_i!\right)^{-1} \sum_{i^*} n_{i^*} \left(\prod \nu_j!\right)^{-1} a'_{i^*} \top (w'_{i^*})^{\bar{\tau}}$$

où la somme est étendue à tous les h_{i^*} distincts figurant dans w et où on a posé

1° $\delta_1^* h_{i^*} = a'_{i^*} h_i^{\nu_1} h_2^{\nu_2} \dots h_{i-1}^{\nu_{i-1}}$

2° w' = l'élément de W, $w' = h_1^{n_1'} h_2^{n_2'} \dots h_i^{n_i'}$

avec

$$n_i' = n_i + \nu_i \ , \quad \text{pour} \quad i < i^*$$

$$n'_{i^*} = n_{i^*} - 1 \ , \quad \text{pour} \quad i = i^*$$

$$n_i' = n_i \ , \quad \text{pour} \quad i > i^*$$

Donc,

$$\langle w^\tau , af' \rangle = (\prod n_i!)^{-1} \sum_{i^*} n_i^* (\prod \nu_i!)^{-1} \langle a_{i^*} \top w^{\tilde{\tau}}_{i^*} , af' \rangle$$

$$= (\prod n_i!)^{-1} \sum_{i^*} n_i^* (\prod \nu_i!)^{-1} \prod (n_i + \nu_i)! \langle w^\tau_{i^*} , f' \rangle$$

où la sommation est étendue à tous les i^* tels que $a_{i^*} = a$.

Comme par hypothèse $\langle w'^{\tau}_{i^*} , f' \rangle = \langle w_{i^*} , f'^{\sigma} \rangle$ le résultat découle immédiatement de la comparaison de cette formule avec $\langle w_1 (a\, w')^{\sigma} \rangle$.

REMARQUE. - Soit $W_{(n)}$ le sous-ensemble de W formé par les w de la forme $f'h$ où $f' \in F$ et $h \in H$ et où h est de degré n .

Soit d'autre part $\mu : \overline{F} \to \overline{F}$ l'homomorphisme de $\overline{F}$ induit par la substitution de $1 + a_i$ à a_i pour tout $a_i \in A$. On vérifie facilement que pour tout $f \in F$ la composante homogène de degré m de μf est déterminée par la seule donnée des $\langle w^\tau , f \rangle$ avec $w \in W_{(n)}$ $n \leq m$. Il en résulte la possibilité de retrouver les relations de "shuffle" et en particulier le fait que si $f \in F$ est de degré n_1 en a_1 , n_2 en a_2 , ... , n_i en a_i $(n_1 \geqslant n_2 \geqslant \dots \geqslant n_i)$, les inégalités existant entre les coefficients font que f est déterminé par la donnée des $\langle w^\tau , f \rangle$ avec $w \in W_{(n)}$, $n \leq n_2 + 1$.

Les formules utilisant les bases de Marshall HALL semblent cependant moins bien adaptées à ce calcul que celles qui reposent sur les bases de CHEN, FOX et LYNDON.

Mentionnons pour terminer la formule suivante qui se déduit facilement des calculs qui viennent d'être développés :

Si $w = h_1^{\nu_1} h_2^{\nu_2} \dots h_i^{\nu_i}$, le coefficient $N(w) = \langle w^\tau , (\sum a_i)^n \rangle$ est égal à :

1-22

$$(\sum \nu_i |h_i|)!\ \prod_i (\nu_i!)^{-1} (N(h_i)/|h_i|)^{\nu_i}$$

où $|h_i|$ est le degré de h_i $(n = \sum \nu_i |h_i|)$ est où $N(h_i)$ est défini inductivement par $N(h_i) = N(w')$ quand $\delta_1^* h_i = a\, w'$ $(a \in A)$.

En particulier, si h est multilinéaire de degré n

$$\langle h^{\nu}, (\sum a_i)^n \rangle = (n-1)!\ (\prod |h_i|)^{-1}$$

où le produit est étendu à tous les composants propres de h qui ne sont pas des composants gauches.

BIBLIOGRAPHIE

[1] BIRKHOFF (Garrett). - Representability of Lie algebras and Lie groups by matrices, Annals of Math., Series 2, t. 38, 1937, p. 526-532.

[2] CHEN (K. T.), FOX (R. H.) and LYNDON (R. C.). - Free differential calculus, IV : The quotient groups of the lower central series, Annals of Math., Series 2, t. 68, 1958, p. 81-95.

[3] CROISOT (Robert). - Automorphismes intérieurs d'un semi-groupe, Bull. Soc. math. France, t. 82, 1954, p. 161-194.

[4] DUBREIL (Paul). - Contribution à la théorie des demi-groupes, I., Mém. Acad. Sc. Inst. France, t. 63, 1941, 52 p.

[5] DUBREIL (Paul). - Contribution à la théorie des demi-groupes, II., Univ. Roma Ist. naz. alta Mat. Rend. Mat. e Appl., t. 10, Série 5, 1951, p. 183-200

[6] DUBREIL (Paul). - Contribution à la théorie des demi-groupes, III., Bull. Soc. math. France, t. 81, 1953, p. 289-306.

[7] FOX (Ralph H.). - Free differential calculus, I : Derivation in the free group ring, Annals of Math., Series 2, t. 57, 1953, p. 547-560.

[8] GOLOMB (S. W.), GORDON (B.) and WELCH (L. R.). - Comma free codes, Canadian J. of Math., t. 10, 1958, p. 202-210.

[9] HALL (Marshall). - A basis for free Lie rings and higher commutators in free groups, Proc. Amer. math. Soc., t. 1, 1950, p. 575-581.

[10] KUROŠ (A. G.). - Neassociativnye svobodnye algebry i svobodnye proizvedenija algebr (Non-associative free algebras and free products of algebras), Recueil math. Soc. math. Moscou (Mat. Sbornik), N. S., t. 20 (62), 1947, p. 239-262.

[11] LAZARD (Michel). - Sur les algèbre enveloppantes universelles de certaines algèbres de Lie, Publ. scient. Univ. Alger, Série A, t. 1, 1954, p. 281-294.

[12] LAZARD (Michel). - Lois de groupes et analyseurs, Ann. scient. Ec. Norm. Sup., Série 3, t. 72, 1955, p. 299-400.

[13] LUCAS (Edouard). - Théorie des nombres. - Paris, Gauthier-Villars, 1891.

[14] LYNDON (R. C.) - On Burnside's problem, I., Trans. Amer. math. Soc., t. 77, 1954, p. 202-215.

[15] MANDELBROT (Benoit). - Logique et langage. - Paris, Presses universitaires de France, 1957.

[16] MEIER-WUNDERLI (H.). - Note on a basis of P. Hall for the higher commutators in free groups, Comment. Math. Helvet., t. 26, 1952, p. 1-5.

[17] ŠIRŠOV (A. I.). - Podalgebry svobodnykh lievykh algebr, Recueil math. Soc. math. Moscou (Mat. Sbornik), N. S., t. 33 (75), 1953, p. 441-452.

[18] WITT (Ernest). - Treue Darstellung Liescher Ringe, J. für reine und ang. Math., t. 177, 1937, p. 152-160.

ALGÈBRE. — *Sur la représentation monomiale des demi-groupes.*

Note de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

On applique aux demi-groupes avec unité (monoïdes) la méthode utilisée en théorie des groupes pour définir les représentations monomiales.

Notations. — Soient A et B deux demi-groupes commutant d'applications dans lui-même de l'ensemble $\Sigma^\star = \{\sigma\}$. Il sera commode de supposer que A et B sont les images homomorphes αS et βS d'un certain demi-groupe S avec unité (e) et d'écrire $s\sigma s'$ au lieu de $\sigma.\alpha s'.\beta s = \sigma.\beta s.\alpha s'$.

On utilisera les relations suivantes sur $\Sigma^\star \times \Sigma^\star$:

$$\sigma' \mathfrak{C}_A \sigma \rightleftharpoons \sigma' \in \sigma S; \qquad \sigma' \mathfrak{C}_B \sigma \rightleftharpoons \sigma' \in S\sigma; \qquad \sigma' \mathfrak{C}_S \sigma \rightleftharpoons \sigma' \in S\sigma S;$$
$$\overline{\mathfrak{C}}_A = \mathfrak{C}_A \cap \mathfrak{C}_A^{-1}; \qquad \overline{\mathfrak{C}}_B = \mathfrak{C}_B \cap \mathfrak{C}_B^{-1}; \qquad \overline{\mathfrak{C}}_S = \mathfrak{C}_S \cap \mathfrak{C}_S^{-1}; \qquad \overline{K} = \overline{\mathfrak{C}}_A \cap \overline{\mathfrak{C}}_B.$$

On sait [J. A. Green (1)] que $\overline{\omega} = \overline{\mathfrak{C}}_A \circ \overline{\mathfrak{C}}_B = \overline{\mathfrak{C}}_B \circ \overline{\mathfrak{C}}_A \subset \overline{\mathfrak{C}}_S$ est une équivalence et l'on dira qu'une partie Σ' de $\Sigma^\star$ est « A-élémentaire » si l'on a identiquement sur Σ' : $\mathfrak{C}_A^{-1} \cap \mathfrak{C}_B = \overline{\mathfrak{C}}_A \cap \mathfrak{C}_B$. Une $\overline{\mathfrak{C}}_S$ classe qui est à la fois A- et B-élémentaire se réduit à une seule $\overline{\omega}$-classe et sera dite « élémentaire ».

Définition de la représentation. — On considère désormais une $\overline{\omega}$-classe, Σ, fixe et l'on désigne respectivement par $\Sigma^i (i \in I)$; $\Sigma_j (j \in J)$; $\Sigma_j^i = \Sigma^i \cap \Sigma_j$ ses $\overline{\mathfrak{C}}_B$-, $\overline{\mathfrak{C}}_A$- et $\overline{K}$-classes. On choisit arbitrairement des éléments σ_1^i et σ_j^1 dans chacune des $\overline{K}$-classes Σ_1^i et Σ_j^1. D'après la définition même de $\overline{\mathfrak{C}}_A$ et $\overline{\mathfrak{C}}_B$, il existe deux systèmes $\{a_1, a_i^1\}$ et $\{b_j^1, b_1^j\}$ tels que

$$\sigma_1^1 a_1^i = \sigma_1^i; \qquad \sigma_1^i a_i^1 = \sigma_1^1; \qquad b_j^1 \sigma_1^1 = \sigma_j^1; \qquad b_1^j \sigma_j^1 = \sigma_1^1.$$

On fera usage de la remarque suivante :

(★) *Si* $\sigma s = \sigma s' = \sigma' \in \Sigma^{i'}$ *pour un* $\sigma \in \Sigma^i$ *alors* $\sigma'' s = \sigma'' s' = \sigma''' \in \Sigma^{i'}$ *pour tous les* $\sigma'' \in \Sigma^i$.

En effet, il existe $b, b' \in B$ tels que $b\sigma = \sigma''$ et $b'\sigma'' = \sigma$. Donc

$$\sigma'' s = b\sigma s = b\sigma s' = \sigma'' s' = \sigma''' \qquad \text{et} \qquad b'\sigma''' = b'\sigma'' s = \sigma s = \sigma'.$$

Si $A^i = \{s : \Sigma^i s \cap \Sigma^i \neq \emptyset\} = \{s : \Sigma^i s \subset \Sigma^i\}$, la restriction à Σ^i de la représentation $(\Sigma^\star, A^i)$ induit un homomorphisme $\varphi_i : A^i \to \overline{A}^i$. Comme $\sigma_1^1 a_1^i a_i^1 = \sigma_1^1$ et

$\sigma_1^i a_i^1 a_1^i = \sigma_1^i$ il résulte de la remarque précédente (★) que $\varphi_1 a_1^i a_i^1 = \varphi_1 e$ et $\varphi_i a_i^1 a_1^i = \varphi_i e$. Les applications de A^i dans A^1 et de A^1 dans A^i :

$$a \to a_1^i a a_i^1 \quad (a \in A^i) \qquad \text{et} \qquad a \to a_i^1 a a_1^i \quad (a \in A^1)$$

sont donc des isomorphismes entre $\bar{A}^i$ et $\bar{A}^1$.

On désigne par o un nouvel élément servant de zéro au demi-groupe $\bar{A}^\star = \bar{A}^1 \cup O$, et, à tout $s \in S$, on attache la $I \times I$ matrice $M(s)$ définie par

$$m_i^{i'}(s) = \varphi_1(a_1^i s a_{i'}^1) \quad \text{si } \sigma_1^i s \in \Sigma^{i'}; \qquad = o \quad \text{si } \sigma_1^i s \notin \Sigma^{i'}.$$

On a évidemment $M(s)M(s') = M(ss')$ identiquement, et l'on définirait de façon duale les $J \times J$ matrices $N(s)$ n'ayant cette fois qu'un élément non nul au plus par colonne.

D'après (★), l'équation en $\bar{x}$, $\bar{a}\bar{x} = \bar{a}'$, entre éléments de $\bar{A}^\star$ possède au plus une solution. Soit $\bar{\bar{A}}$ le sous-ensemble des $\bar{x} \in \bar{A}^\star$ tels que pour au moins un $\bar{x}'$, $\bar{x}\bar{x}' = \bar{e}(= \varphi_1 e)$. $\bar{\varphi}_1^{-1}\bar{\bar{A}}$ coïncide avec l'ensemble

$$\{ s \in S : \Sigma_1^1 s \cap \Sigma_1^1 \neq \emptyset \} = \{ s \in S : \Sigma_1^1 s = \Sigma_1^1 \}$$

et est un groupe puisque tout élément de $\bar{\bar{A}}$ possède un inverse unique. Enfin $\tilde{A} = \bar{A}^\star - (O \cup \bar{\bar{A}})$ est vide si et seulement si Σ est A-élémentaire et, sinon, $\bar{A}^\star$ (et par conséquent A), contiennent une suite infinie d'idéaux à droite $\{a^n A\}(a \in \tilde{A})$ tous distincts.

Dans tous les cas (2), si $\bar{\bar{B}}$ est le groupe défini de façon duale dans $\bar{B}_1$, la correspondance $\sigma_1^1 a = b \sigma_1^1$ établit un isomorphisme entre $\bar{\bar{A}}$ et $\bar{\bar{B}}$.

Il s'en déduit (3) la possibilité de montrer que $M(s)$ ne dépend pas du choix des σ_1^i (à une transformation près par des matrices diagonales à coefficients dans $\bar{\bar{A}}$).

Relation entre les deux représentations. — On suppose désormais que Σ est une $\bar{\bar{\mathfrak{S}}}_S$-classe élémentaire. On peut représenter par un élément unique σ_0 l'ensemble $S\Sigma S - \Sigma$ et l'on fait l'hypothèse que les a_1^i et les b_j^1 peuvent être choisis de telle façon que $\sigma_1^1 a_1^i b_j^1 = a_1^i b_j^1 \sigma_1^1$, identiquement. On désigne par R la $I \times J$ matrice dont les éléments sont les $a_1^i b_j^1 (\in \bar{\bar{A}} \cup O)$ et par $U = \{ s : \bigvee^{i,j} a_1^i s b_j^1 \sigma_1^1 = \sigma_1^1 a_1^i s b_j^1 \}$.

On a donc pour tout $u \in U$: $M(u)R = RN(u) = R(u)$ puisque $r_i^j(u)$ est la valeur commune dans $\bar{\bar{A}} \cup O$ de

$$\sigma_1^1 a_1^i u b_j^1 = m_i^{i'}(u) \sigma_1^1 a_1^{i'} b_j^1 \qquad \text{et} \qquad a_1^i u b_j^1 \sigma_1^1 = a_1^i b_{j'}^1 \sigma_1^1 n_{j'}^j(u),$$

i' et j' étant les indices (uniques s'ils existent) tels que $m_i^{i'}(u)$ et $n_{j'}^j(u)$ ne soient pas nuls. Il résulte de cette équation que U est un demi-groupe ainsi que le

sous-ensemble V (qui peut être vide) des $\varphi \in U$ tels qu'il existe une $J \times I$ matrice $T(\varphi)$ satisfaisant $M(\varphi) = RT(\varphi)$ et $N(\varphi) = T(\varphi)R$. En particulier, si Σ est identifiable à S lui-même et si Σ correspond à une $\overline{\mathcal{D}}$ classe élémentaire et régulière D de S, $S = U$, V contient D et $T(\varphi)$ est la représentation de Clifford (4) avec la multiplication $T(\varphi)RT(\varphi') = T(\varphi\varphi')$.

(1) *Ann. Math.*, 54, 1951, p. 163-172.
(2) G.-B. Preston, *Bull. Am. Math. Soc.*, 63, 1957, Abst., n° 651.
(3) *Comptes rendus*, 244, 1957, p. 1994 et 2219.
(4) *Trans. Amer. Math. Soc.*, 82, 1956, p. 270-280.

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*, t. 246, p. 865-867, séance du 10 février 1958.)

GAUTHIER-VILLARS,
ÉDITEUR-IMPRIMEUR-LIBRAIRE DES COMPTES RENDUS DES SÉANCES DE L'ACADÉMIE DES SCIENCES
153256-58 Paris. — Quai des Grands-Augustins, 55. Imprimé en France.

ALGÈBRE. — *Sur les homomorphismes d'un demi-groupe sur un groupe.*

Note de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

En vue de leur utilisation dans un problème de mathématiques appliquées on déduit des théories générales développées dans (1), (2), (3) deux caractérisations de ces homomorphismes.

Notations. — S, $R = RS$, $L = SL$ désigneront toujours un demi-groupe (2) avec l'élément neutre e et deux de ses idéaux. $\tilde{\xi}$ étant une équivalence sur S, ${}_R\xi_L$ désignera l'homomorphisme naturel associé à la congruence $a\,{}_R\tilde{\xi}_L\,b \rightleftharpoons \forall_{R,L}^{r,l}\, ral\,\tilde{\xi}\,rbl$; si $\tilde{\xi}$ n'a que deux classes X et $S - X$ [*cf.* (1)] et que $R = L = S$, on écrira φ_X au lieu de ${}_S\xi_S$; si $T \subset S$, $[\tilde{\xi}]^T$ désignera la restriction de $\tilde{\xi}$ à $T \times T$; on utilisera les remarques suivantes : 1° [*cf.* (1), section IV], soit $\psi : S \to S'$, un épimorphisme, $\tilde{\xi}'$ une équivalence sur S', $R' = \psi R$, $L' = \psi L$; le demi-groupe quotient ${}_{R'}\xi'_{L'}S'$ est isomorphe à ${}_R\xi_L S$ où $\tilde{\xi}$ est définie par $a\tilde{\xi}b \rightleftharpoons \psi a\tilde{\xi}'\psi b$; en particulier si S' est un groupe avec zéro ${}_R\xi_L S = {}_S\xi_S S = {}_{R'}\xi'_{L'}S'$ dès que $\psi LR \neq 0$. 2° En tant que partie de $S \times S$, ${}_R\tilde{\xi}_L$ contient l'union de toutes les congruences $\tilde{\varphi}$ telles que $[\tilde{\varphi}]^{RL} \subset [\tilde{\xi}]^{RL}$ et lui est donc égale quand $[{}_R\tilde{\xi}_L]^{RL} \subset [\tilde{\xi}]^{RL}$; cette condition est vérifiée quelle que soit $\tilde{\xi}$ quand R et L sont des unions d'idéaux principaux idempotents, donc quand $R = L = S$ (3); elle entraîne que l'image de $\tilde{\xi}$ par ${}_R\xi_L$ soit une équivalence $\tilde{\xi}' = {}_R\xi_L\tilde{\xi}$ sur $S' = {}_R\xi_L S$ et que ${}_{R'}\xi'_{L'}$ soit l'application identique de S' sur lui-même.

I. *Soit* $\emptyset \neq Y \subset S$; *il existe un homomorphisme* γ *de* S *sur un groupe avec* $\bar{\gamma}^1\gamma Y = Y$, *si et seulement si, pour tout* $s \in S$, $Ss \cup sS$ *contient un* n *tel que* $ab \in Y \rightleftharpoons anb \in Y$.

Démonstration. — Considérons plus généralement une équivalence $\tilde{\xi}$ et soit $N = \mathfrak{N}(\tilde{\xi}) = \{n \in S : ab\,\tilde{\xi}\,anb\}$ [*cf.* (1), section V]; N satisfait (★) : si $n \in N$, $xy \in N \rightleftharpoons xny \in N$, ce qui entraîne que $\varphi_N N$ soit un élément unique e' de $S' = \varphi_N S$; e' est un élément neutre puisque $e \in N$; comme $\varphi_N s = 0 \rightleftharpoons SsS \cap N = \emptyset$, il y a pour tout $s' \in S' - 0$ au moins une paire r', l' avec $r's'l' = e'$; S' n'a donc pas d'idéaux bilatères propres sauf 0. Considérons sa représentation par des

translations à droite; si $r'l' = e'$, r' correspond à une injection et l' à une surjection; réciproquement si l' correspond à une surjection, il existe r' avec $r'l' = e'$; donc la $\overline{\mathcal{K}}$, $\overline{\mathcal{R}}$ et $\overline{\mathcal{L}}$-classe de e' correspondent respectivement au groupe G′ des bijections, au demi-groupe simplifiable à droite des injections qui appartiennent à la $\overline{\mathcal{D}}$-classe de e', au demi-groupe simplifiable à gauche des surjections. On en conclut que S′, qui n'est pas nécessairement un groupe (6), se réduit à $G' \cup o$ quand il admet un idéal à droite minimal en dehors de o ($\rightleftharpoons$ un s' tel que $s's'' \neq o \Rightarrow s' \in s's''S'$) ou quand $s' \neq o \Rightarrow e' \in S's' \cup s'S'$. Soit $T = S - \overline{\varphi}_N^{-1} o; \tilde{\eta}$ l'équivalence telle que $[\tilde{\eta}]_T = [\tilde{\xi}]^T$ admettant la classe $S - T$; $M = \mathfrak{N}(\tilde{\eta})$; $\tilde{\xi}' = {}_S\xi_S\tilde{\xi}$; on a : $\mathfrak{N}(\tilde{\xi}') = {}_S\xi_S N$ et, si $\varphi_N S$ est un groupe avec zéro, ce que nous supposons désormais, $[\tilde{\varphi}]^T \subset [\tilde{\xi}]^T$; $N \subset M$; $SsS \cap M \neq \emptyset \rightleftharpoons s \in T$; ${}_S\tilde{\xi}_S \subset \tilde{\varphi}_N \subset {}_S\tilde{\eta}_L = \tilde{\varphi}_M$. D'où le résultat énoncé puisque alors $S' = G'$ et $\tilde{\eta} = \tilde{\xi}$.

Remarque. — Moyennant des hypothèses d'une nature différente, (★) peut être affaiblie; soit $A \subset S$ intersectant tous les idéaux bilatères et tel que $\varphi_A S$ admette des bi-idéaux minimaux. $\varphi_A S$ est un groupe si et seulement si :

$A^2 \subset A$ et $a \in A \;\&\; xay \in A \Rightarrow xy \in A$; ou bien (2) :

$A(S-A)A \subset S-A$ et $a \in A \;\&\; xy \in A \Rightarrow xay \in A$ (3), (4). Ces trois propriétés s'établissent directement au moyen de la représentation de Miller et Clifford (5) en observant que tout homomorphisme ψ de $B = SBS$ *dans* un groupe avec zéro G′ peut être étendu de façon unique à un homomorphisme (se réduisant à ψ sur B) de tout S *dans* G′.

II. *Soit* $\emptyset \neq H \subset S$; *il existe un homomorphisme* γ *de* S *sur un groupe avec* $\gamma\overline{\gamma}^{-1}H = H$ et $\gamma H = h$, *un élément unique, si et seulement si :* (1) H *intersecte tous les idéaux bilatères* de S; (1′) $HSHS \cap H \neq \emptyset$;

$$(\star\star) \qquad xHy \cap H \neq \emptyset \;\Rightarrow\; xHy \subset H \;\&\; x(SHS - H)y \subset S - H \quad (9).$$

Démonstration. — Supposons seulement (1′) et (★★). $\varphi_H H$ étant réduit à un élément unique, on fera pour simplifier l'hypothèse que $\varphi_H S = S$; $H = h$; $\{s = o \rightleftharpoons h \notin SsS\}$. Soient a et b avec $hahb = h$; on a $hahbahb = h$, donc, d'après (★★), $hbah = h$; on pose $h' = bahba$ (5). Supposons qu'il existe x, y et k avec $xh = k$ et $ky = h$; on a $xhy = h$, donc $xhyh'xhy = h$, donc d'après (★★) $hyh'xh = h$; par conséquent $h = (hyh')k$ et $k = h(h'k)$; $D = SHS - o$ est donc une $\overline{\mathcal{D}}$ classe régulière élémentaire (5). Soit $f = f^2$; ou bien $fh = o$, ou bien $f^2h = fh$ et d'après (★★) $fh = h$ (10); en particulier, si f appartient à la $\overline{\mathcal{L}}$-classe de hh', on a $fhh' = f \neq o$, donc $fh = h$ et $f = hh'$. Observons maintenant que S est isomorphe à sa représentation à droite sur D et que, par conséquent hx et hy sont égaux si et seulement si $hxz = h \rightleftharpoons hyz = h$ pour tout $z \in Sh$; en particulier, si $hx = (hx)^2 \neq o$, on a $hx = hh'$, car, hx et hh' étant

les seuls idempotents de leurs $\overline{\mathcal{L}}$-classes, $hxz = h$, $z \in Sh$, n'est possible que si $z = h$; donc, finalement, h a un inverse unique h'.

Supposons maintenant au lieu de (1) que

$$SsS \cap H \neq \emptyset \Rightarrow H \cap (SHsS \cap SsHS) \neq \emptyset.$$

D se réduit au (x) $\overline{\mathcal{J}\mathcal{K}}$-classe (s) contenant h, h', hh' et $h'h$ et, en utilisant le fait que S est isomorphe à sa représentation à droite sur D, on vérifie que S est égal à D ou à D $\cup$ o. Dans les conditions de l'énoncé, S = D et D n'a qu'une seule $\overline{\mathcal{J}\mathcal{K}}$-classe puisque $h^2 \neq$ o.

Remarques. — 1° Si $RHL \cap H \neq \emptyset$, la condition « pour tout $(r, l) \in (R, L)$, si $rHl \cap H \neq \emptyset$ alors $rHl \subset H$ et $r(SHS - H)l \subset S - H$ » entraîne (★★). Ceci rapproche la propriété énoncée du théorème 18 de (1) et de la condition de F. W. Levi [(4) et *cf.* (7)] caractérisant les noyaux d'homomorphismes sur un groupe [$(xy \in N \Rightarrow xay \in N \Rightarrow a \in N)$].

2° Les démonstrations données peuvent aussi être basées sur l'observation suivante : soient $A_i (i \in I_R)$ les classes intersectant R pour l'équivalence : $x \overset{\sim}{\xi}_L y \Rightarrow \forall^l_L xl \overset{\sim}{\xi} yl$; $\mathbf{A}(s)$, la $I_R \times I_R$ matrice avec $\mathbf{a}^{i'}_i(s) = 1$ ou o selon que $A_i s \subset A_{i'}$ ou non; $\mathbf{B}(s)$ définie de façon symétrique pour ${}_R\overset{\sim}{\xi}(\forall^r_R : rx \overset{\sim}{\xi} ry)$; pour chaque classe X de $\overset{\sim}{\xi}$, $\mathbf{X}(s)$ la $I_R \times I_L$ matrice avec $\mathbf{x}^{i'}_i(s) = 1$ ou o selon que $A_i s B_{i'} \subset X$ ou non. On a identiquement $\mathbf{A}(s)\mathbf{X}(s') = \mathbf{X}(s)\mathbf{B}(s') = \mathbf{X}(ss')$ et les demi-groupes $\{\mathbf{A}(s)\}$ et $\{\mathbf{B}(s)\}$ sont isomorphes à ${}_R\xi_L S$. Ceci permet facilement d'établir la propriété suivante : une condition nécessaire et suffisante pour que $\varphi_H S$ soit un groupe avec zéro avec $\varphi_H H =$ un élément unique différent de zéro est que : 1° $RHL \cap H \neq \emptyset$, 2° $rHl \cap H \neq$ o $\Rightarrow rHl \subset H$; 3° $rl \in H$ & $r'l \in H$ & $rl' \in H \Rightarrow r'l' \in H$ [H est « fort » au sens de P. Dubreil (2) relativement à R, L]; 4° si $ral \in H \Rightarrow rbl \in H$ alors $ral \in H \Rightarrow rbl \in H$ (ceci exprime quand S est un groupe, que si H est un segment d'un préordre régulier, il est nécessairement une classe de la congruence associée); 5° $SsS \cap H \neq \emptyset \Rightarrow (SsH \cup HsS) \cap H \neq \emptyset$ (où, de façon équivalente ici, $SsS \cap H \neq \emptyset \Rightarrow HSsSH \cap H \neq \emptyset$).

(1) R. Croisot, *J. Math. Pures Appl.*, 36, 1997, p. 373-417.
(2) P. Dubreil, *Mem. Acad. Inst. France*, 63, 1941, p. 1-52.
(3) P. Dubreil, *Univ. Roma Rendic. Mat.*, 10, 1951, p. 183-200.
(4) F. W. Levi, *Bull. Calcutta Math. Soc.*, 36, 1944, p. 141-146.
(5) D. D. Miller et A. H. Clifford, *Trans. Amer. Math. Soc.*, 82, 1956, p. 270-280.
(6) G. B. Preston, *Bull. Amer. Mat. Soc.*, 5, 1958, Abst. 540 20.
(7) R. R. Stoll, *Amer. J. Mat.*, 73, 1951, p. 475-481
(8) M. Teissier, *Çomptes rendus*, 232, 1951, p. 1987.
(9) (★ ✶) est nécessaire [*cf.* (1), section V] car chacune des deux implications qu'elle comporte entraîne, quand S est un groupe, que H soit une classe d'un sous-groupe normal.
(10) Plus généralement $hx \neq$ o & $ux = x \Rightarrow hu = h$; et si $u \in Sh$; alors $u^2 = u$.

Reprinted from INFORMATION AND CONTROL, Volume 1, No. 2, May 1958
Academic Press Inc. *Printed in U.S.A.*

INFORMATION AND CONTROL **1,** 153–158 (1958)

On The Quantization of Finite Dimensional Messages[1]

MARCEL P. SCHÜTZENBERGER[2]

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts

Let L be the average value of a measure of quantization noise, and let H be the negentropy of the quantized signal. Some reciprocal relationship exists between these quantities, since, for example, increasing the number of possible quantized values reduces L but increases H. We give a lower bound to L as a function of H and show that it may be realized up to a constant factor. Roughly speaking, this shows that every bit added to H multiplies L by a factor depending on the dimensionality of the message and the measure of quantization noise used.

I. INTRODUCTION

Let the message ξ be an n-dimensional continuous variate with *a priori* probability density $f(\xi)$. Before it can be transmitted through a discrete channel it has to be replaced by a quantized signal $[\xi]$, that is, by some approximate quantity taking only a finite number of distinct values.

We assume here that the channel is perfectly noiseless so that the only source of error lies in the quantization $\xi \rightarrow [\xi]$. The accuracy is usually measured by the average L of some given nondecreasing function $\ell(\mid \xi - [\xi] \mid)$ over the *a priori* distribution of ξ. We shall consider only those functions ℓ which are of the form $c \mid \xi - [\xi] \mid^{\alpha} (\alpha > 0)$ and our results will consequently cover the case of the so-called rms criterion $(\alpha = 2)$.

Shannon's theory of noiseless communication indicates that the natural measure of the cost of transmission is the negentropy H of the quantized signal $[\xi]$. With these conventions, the optimum is obtained when, for a given value of H (or of L), the other quantity is as small as possible. Intuitively, some general relationship must presumably exist between H and L, since any action which tends to decrease one of them (for in-

[1] This work was supported in part by the U. S. Army (Signal Corps), the U. S. Air Force (Office of Scientific Research, Air Research and Development Command), and the U. S. Navy (Office of Naval Research).

[2] Present address: Faculté des Sciences de Poitiers, France.

stance the multiplication of the number of different values of $[\xi]$) has exactly the opposite effect on the other.

Under some broad conditions we give here a lower bound to the value of L as a function of H and we show that this bound may be reached up to a constant proportionality factor. Loosely speaking, these two results mean that every bit of information allows on the average a reduction of L by a factor no more but not less than $2^{-\alpha/n}$, whatever be the density function $f(\xi)$. In particular, $L \geqq KN^{-\alpha/n}$ with K, a constant, for every quantization with N different quantized values $[\xi]$.

II. HYPOTHESES

We state first our hypotheses:

A. The message is an n-dimensional variate ($n < \infty$) admitting a continuous, bounded density $f(\xi)$ in its domain of variation $E = \{\xi : f(\xi) > 0\}$

Further,

$$\left| \int_E f(\xi) \log f(\xi)\, d\xi \right| < \infty.$$

B. There exists a finite θ for which

$$\int_E |\xi|^{\alpha+\theta} f(\xi)\, d\xi < \infty.$$

A quantization $\xi \to [\xi]$ will be identified with a partition $W = \{E_i\}$ of E; each E_i is the set of the ξ's admitting the same quantized value $[\xi] = a_i$. For any W we define:

$$H(W) = -\sum P_i \log P_i$$

where

$$P_i = \int_{E_i} f(\xi)\, d\xi$$

and

$$L(W) = \int_E c\, |\xi - [\xi]|^{\alpha} f(\xi)\, d\xi = \sum P_i L_i'$$

where

$$L_i' = P_i^{-1} \int_{E_i} c\, |\xi - [\xi]|^{\alpha} f(\xi)\, d\xi.$$

Finally, we say that a sequence of quantizations $W_1 = \{E_{1,i}\}$, $W_2 =$

$\{E_{2i}\}\ \cdots$, $W_j = \{E_{ji}\}\ \cdots$, is *systematically convergent* if, for all j, every $E_{j+1,i}$ is entirely contained in some $E_{ji'}$ and if $\overline{\lim}_{j\to\infty} L(W_j) = 0$.

First inequality. If $f(\xi)$ satisfies A, there exists a constant K with the property that $L(W) \geqq K(\exp -\alpha/n)\, H(W)$ for all possible quantizations of ξ.

Second inequality. If $f(\xi)$ satisfies A and B, there exists a constant K' and a systematically convergent sequence $\{W_j\}$ with the property that $L(W_j) \leqq K'(\exp -\alpha/n)\, H(W_j)$ for all j.

III. PROOF OF THE INEQUALITIES

In what follows $g_1, g_2, \cdots$ denote geometric constants which are functions of α and n only; $k_1, k_2, \cdots$ denote nonzero finite constants whose values depend upon $f(\xi)$ but not upon the quantization considered.

We shall use twice the fact that for any partition $W = \{E_i\}$ the sum $|-\sum P_i \log f_i|$, where f_i is the value of $f(\xi)$ at some inner point of E_i, is uniformly bounded. This results immediately from the hypotheses by the following inequalities

$$|\sum P_i \log 1/f_i| = |\sum P_i \log f^*/f_i - \sum P_i \log f^*|$$

$$\leqq \sum P_i |\log f^*/f_i| + |\log f^*| < \int_E f(\xi)\, |\log f^*/f(\xi)|\, d\xi + |\log f^*|$$

$$\leqq \int_E f(\xi) \log 1/f(\xi)\, d\xi + 2|\log f^*|$$

where

$$f^* = \sup_{\xi\in E} f(\xi).$$

First Inequality

We take a fixed arbitrary number p $(0 < p < 1)$ and, for each E_i of W we define a value f_i and a subset E_i' of E_i by the relations:

$$E_i' = \{\xi\epsilon E_i\,;\, f(\xi) \geqq f_i\}; \qquad \int_{E_i'} f(\xi)\, d\xi = p\int_{E_i} f(\xi)\, d\xi = pP_i\,.$$

We have

$$P_i L_i' \geqq \inf_x \int_{E_i} c\,|\xi - x|^\alpha f(\xi)\, d\xi = c\int_{E_i} |\xi - x_i|^\alpha f(\xi)\, d\xi$$

$$\geqq c\int_{E_i'} |\xi - x_i|^\alpha f(\xi)\, d\xi \geqq cf_i \int_{E_i} |\xi - x_i|^\alpha d\xi = cf_i L_i''.$$

It is a classical result that for a fixed value of meas(E_i'), the sum L_i'' is a minimum when E_i' is an n-dimensional sphere with radius ρ_i centered at x_i. Consequently, $P_iL_i' \geqq cg_1f_i{\rho_i}^{n+\alpha}$ where ρ_i is defined by meas$(E_i') = g_2{\rho_i}^n$ and where g_1 and g_2 are geometric constants. If we now define $\bar{f}_i$ by the equality $\bar{f}_i$ meas$(E_i') = pP_i = \int_{E_i'} f(\xi)\, d\xi$, we can eliminate ρ_i and meas(E_i'). Thus we obtain

$$P_iL_i' \geqq {P_i}^{1+\alpha/n}cg_3p^{1+\alpha/n}f_i\bar{f}_i^{-1-\alpha/n}.$$

Taking into account the remark made at the beginning of this section, we find that

$$L_i' \geqq cg_3(p/f^*)^{1+\alpha/n}{p_i}^{\alpha/n}f_i$$

and

$$-\sum P_i \log L_i' \leqq \left(\frac{\alpha}{n}\right) H(W) + \log k_1 - \sum P_i \log f_i$$

$$\leqq \left(\frac{\alpha}{n}\right) H(W) - \log K.$$

This concludes the proof, since we have

$$L(W) = \sum P_iL_i' \geqq \exp - \sum P_i \log L_i' \quad [= K \exp - \alpha/nH(W)]$$

because of the convexity of the function $\log 1/x$.

SECOND INEQUALITY

The construction of a systematically convergent sequence can be carried out in many ways. We indicate here one method which is probably among the simplest ones. In the first place we observe that the classical inequality on the absolute moments

$$\left[\int_{E'} |\xi|^{\alpha} f(\xi)\, d\xi\right]^{1/\alpha} \leqq \left[\int_{E'} |\xi|^{\alpha+\theta} f(\xi)\, d\xi\right]^{(\alpha+\theta)^{-1}} \left[\int_{E'} f(\xi)\, d\xi\right]^{\theta(\alpha+\theta)^{-1}}$$

gives under the hypothesis B

$$\int_{E'} |\xi^{\alpha}| f(\xi)\, d\xi \leqq \left[\int_{E'} |\xi|^{\alpha+\theta} f(\xi)\, d\xi\right]^{\alpha(\alpha+\theta)^{-1}} \left[\int_{E'} f(\xi)\, d\xi\right]^{\theta(\alpha+\theta)^{-1}}$$

$$= k_2 \left[\int_{E'} f(\xi)\, d\xi\right]^{\theta(\alpha+\theta)^{-1}}$$

for any subset E' of E.

Let us take now an arbitrary length d and construct a connected domain F around the origin made up of the juxtaposition of n-dimensional cubes C_i, with d the length of the side of each cube. We can make F big enough so that

$$e = \int_{E-F} f(\xi)\, d\xi$$

satisfies the relation $e^{\theta/\alpha+\theta} \leqq d^{\alpha}$. We consider the quantization W in which, $[\xi] = x_i$, the center of C_i, when $\xi \epsilon C_i$ and $[\xi] = 0$ when $\xi \epsilon E - F$. We have

$$H(W) = -\sum P_i \log P_i - e \log e - P_i \log f_i + n \log 1/d - e \log e$$

(where, again, f_i is the value of $f(\xi)$ at some inner point of C_i), that is,

$$n \log 1/d \geqq H(W) - k_3 + e \log e.$$

Had we considered instead of F some domain F' for which

$$e' = \int_{E-F'} f(\xi)\, d\xi \leqq \int_{E-F} f(\xi)\, d\xi = e$$

the last inequality would still have been valid, for $x \log 1/x$ is a decreasing function of x. Consequently $d^n \leqq K'' \exp - H(W)$ for some K''. We compute now $L(W)$.

$$\sum P_i L_i' = c \int_{E-F} |\, \xi \,|^{\alpha} f(\xi)\, d\xi + \sum c \int_{C_i} |\, \xi - x_i \,|^{\alpha} f(\xi)\, d\xi$$

but, for any C_i:

$$\int_{C_i} |\, \xi - x_i \,|^{\alpha} f(\xi)\, d\xi \leqq \int_{C_i} \Big| \sup_{\xi \epsilon C_i} |\, \xi - x_i \,| \Big|^{\alpha} f(\xi)\, d\xi$$

$$\leqq g_4\, d^{\alpha} \int_{C_i} f(\xi)\, d\xi = g_4\, d^{\alpha}\, P_i$$

and

$$\int_{E-F} |\, \xi \,|^{\alpha} f(\xi)\, d\xi \leqq k_2 e^{\theta(\alpha+\theta)^{-1}} \leqq k_2\, d^{\alpha}.$$

Thus

$$L(W) = \sum P_i L_i' \leqq K''' d^{\alpha} \leqq K' \exp - \alpha/nH(W).$$

By construction the constant K' can be chosen such that it does not

depend upon W. We consider now the partition $W = W_1$ as the first term of the sequence $\{W_j\}$ and we take a second value d' such that d is equal to some multiple of d'.

We subdivide every C_i into smaller cubes C_i' with length of the side d' and we add new cubes of the same size around F so as to obtain a domain F' for which, as above,

$$\int_{E-F'} f(\xi)\, d\xi \leqq d'^{(\alpha+\theta)\alpha\theta^{-1}}.$$

Obviously the partition $W_2 = W'$ satisfies $L(W') \leqq L(W)$; $L(W') \leqq K' \exp - \alpha/nH(W')$, and this concludes the proof since we can choose, by iterating the same method, a sequence d, d', $\cdots$ converging to zero.

IV. REMARKS

i. The hypotheses A and B are sufficient but obviously not necessary for the validity of the results. In the same manner, the assumption that the "loss function" $\ell(r)$, $(r = |\xi - [\xi]|)$, has the form cr^α could be weakened and the results would hold substantially, in an asymptotic fashion, for any $\ell(r)$ with $\lim_{r\to 0} rd/dr \log \ell(r) = \alpha > 0$. But this would definitely not be true for arbitrary $\ell(r)$ (as, for example, $\exp -1/r$ or $r \log 1/r$) and the normalization function $H(W)$ does not seem then to play the same natural role.

ii. A more detailed computation allows one to get closer estimates of the constants K and K'. However, they remain different and their ratio tends to infinity with n. For $n = 2$, a better "second inequality" can be obtained by use of a covering of the plane with hexagons instead of squares. Our present ignorance concerning the most elementary properties of the coverings of the space for $n \geqq 3$ seems to lie at the root of the discrepancy between K and K'.

RECEIVED: September 6, 1957.

LA MÉTHODE DES MODÈLES DANS LES SCIENCES HUMAINES

Par **Paul-Marcel SCHUTZENBERGER**

C'est avec une certaine réserve, comme l'on sait, que les sciences humaines en sont venues à utiliser les méthodes scientifiques de recherche développées par les sciences de la nature.

Ainsi, jusqu'à une période fort peu éloignée et encore même de nos jours dans certains milieux, l'application des méthodes mathématiques au comportement humain apparaissait-il comme scandaleux, utopique, ou au mieux, puéril. S'il n'en est plus de même maintenant c'est que des courants multiples ont préparé progressivement les chercheurs eux-mêmes à utiliser des techniques que leurs devanciers ne savaient ni ne voulaient manier, bien plus à créer des techniques nouvelles telles que l'analyse factorielle par exemple.

Cependant pour beaucoup, l'usage du calcul dans les problèmes humains se limite encore étroitement à celui de la statistique : en économie, en démographie, plus récemment et avec des outils encore plus spécifiquement mathématiques en psychologie et en sociologie expérimentales, les évaluations chiffrées remplacent peu à peu les appréciations du type « dans la plupart des cas... » ou « il n'est pas rare que... » qui semblent un peu « littéraires » au spécialiste rompu à l'emploi des pourcentages. Bien plus, si ce dernier est formé à la discipline de la statistique mathématique il exigera que tout chiffre soit accompagné de son erreur standard ou de toute autre estimation de sa précision ou de la confiance qu'on peut lui accorder.

Bien des critiques sont pourtant formulées contre ce que d'autres ne considèrent que comme une manie de mesurer ce qui ne saurait l'être : la plus sérieuse est sans doute ce reproche que la poursuite de l'apparente précision des chiffres détourne les chercheurs de celles des « gros phénomènes », des modifications qualitatives, et des relations profondes qui les gouvernent. A coup sûr (je prends un exemple personnel pour ne heurter personne...) l'estimation pour une certaine population à $2{,}4 \pm 1{,}3$ ans de la différence d'âge au mariage pour les couples dont le mari est alcoolique est moins intéressante que ce fait impossible à formuler de façon plus précise : « plus souvent que les normaux, les alcooliques épousent des femmes plus âgées qu'eux ». Le premier chiffre indépendamment de toute fluctuation statistique *stricto sensu* ne vaut que pour une population donnée, il a évolué dans le temps, selon les milieux sociaux, selon l'âge au mariage lui-même, etc. Multiplier les observations pour obtenir une décimale supplémentaire ne servirait à peu près à rien. Au contraire, la loi tendancielle même purement qualitative, même irrégulièrement vérifiée, indique sans doute un phénomène psychologique qui mérite d'être étudié.

Ainsi, si l'on réduisait à la seule statistique l'emploi des mathématiques dans les sciences humaines, serait peut-être justifié en partie ce reproche

qu'on leur fait d'avoir influence parfois stérilisante ou de ne jouer qu'un rôle statutairement ancillaire pour aider à la mise au net des enquêtes et des expériences.

Une autre voie d'approche semble ouverte : à l'imitation des sciences physico-chimiques, chercher à représenter de façon semi-empirique les données expérimentales au moyen de fonctions plus ou moins classiques. Cependant, ici encore, on constate que les résultats n'ont pas toujours rejoint les espérances : en dehors de domaines très spéciaux — et d'ailleurs en général étroitement liés à la physico-chimie — les causes d'erreur ou de fluctuation incontrôlables jouent un rôle trop important en biologie et, a fortiori, dans les sciences humaines pour que les concordances entre les courbes théoriques et les courbes observées entraînent la conviction. Je crois qu'aucun biologiste ne me contredira si je prétends qu'en pharmacodynamie par exemple une « Constante » est une grandeur qui consent à ne varier que du simple au quintuple. Rares sont donc les cas où le matériel étudié permet des variations si étendues des conditions expérimentales qu'un accord sur les ordres de grandeurs traduise un phénomène remarquable. Bien plus — et c'est de là en partie que proviennent ces difficultés — ces courbes théoriques sont directement empruntées à la physique : elles sont motivées par des équations différentielles (c'est-à-dire de liaisons constantes et régulières entre des causes extrêmement faibles et leur effet) alors les mécanismes causaux à la base des phénomènes biologiques ou psychologiques étudiés n'admettent qu'un déterminisme largement affecté par le hasard — au niveau qui nous intéresse.

Il semble donc que l'emploi des mathématiques dans les sciences humaines ne puisse se faire que par le recours à des concepts et des techniques analytiques radicalement nouveaux par rapport à ceux qu'ont rendu familiers les mathématiques de l'ingénieur et c'est effectivement ce qui s'est produit dans les cas le plus remarquable.

Dans la méthode des modèles qui se développe de plus en plus, l'originalité ne réside en effet pas tellement dans le schéma général que dans ses modalités : traduire en langage mathématique des principes de fonctionnement (on dira plutôt ici : « de comportement »), choisir des hypothèses simplificatrices rendant possible le traitement mathématique, puis comparer avec les faits les résultats des déductions opérées par voie géométrique pour infirmer ou confirmer telle ou telle de ces hypothèses de structure ou de fonctionnement, il n'y a rien là qui ne soit courant dans les sciences de la matière inanimée.

Mais en psychologie ou en sociologie, les principes invoqués sont rarement de nature infinitésimale : le plus souvent ils sont globaux ou structurels ; le hasard est fréquemment introduit dans leur nature même et le traitement mathématique subséquent est donc rarement classique. Enfin, les conclusions que l'on cherchera à obtenir ne sont qu'incidemment numériques : typiquement ou montrera que tel ou tel phénomène *qualitatif* peut apparaître au détour des calculs malgré l'apparente pauvreté conceptuelle des hypothèses de base, que telle ou telle variation se fait dans un sens plutôt que dans un autre, etc.

Il n'est pas difficile de multiplier les exemples :

— Des « neurones abstraits » (c'est-à-dire n'ayant guère plus de propriétés que des relais électriques de modèle standard) sont interconnectés au hasard et doués selon des lois très simples de facultés d'auto-excitation : le calcul montre que s'ils sont très nombreux il se produit spontanément

comme une sorte d'organisation qui a pour résultat que le système possède plusieurs paliers d'activité stables caractérisés chacun par des oscillations assez régulières et de période relativement fixe.

— Un principe d'économie étant fixé, on cherche un modèle de « langage » transportant le maximum d'information tout en restant peu sensible à l'action des bruits « parasites » qui perturbent la transmission. Le calcul (B. Mandelbrot) fait apparaître que ce langage doit consister en « mots » (et non pas être continu comme l'est la musique) et que ces mots doivent satisfaire certaines lois statistiques qui sont celles-là même qui avaient été observées empiriquement.

Le plus bel exemple est peut-être pourtant le suivant :

Deux « machines » sont construites (sur le papier) de telle sorte qu'elles puissent jouer (bien ou mal) au poker. On fournit à chacune comme principe directeur de « rendre le plus faible possible la valeur moyenne de la perte qu'elle peut subir si l'autre joue au mieux ». Le calcul (von Neumann) montre que ces machines, avec une certaine fréquence, misent de forts enjeux alors qu'elles ont des jeux faibles ou bien font l'inverse. Disons qu'elles « bluffent » pour employer un langage anthropomorphique.

Comment interpréter ces résultats ? Signifient-ils qu'effectivement le cerveau est un tissu de neurones associés au hasard, qu'un comptable inconnu au milieu de notre matière grise pèse le coût et le rendement informationnel de chaque mot avant que nous le prononcions, que ces machines sont douées d'une conscience de Soi-Même et de l'Autre ?

Naturellement cette conclusion ne se dégage pas du tout nécessairement des faits. Mais la valeur de ceux-ci est pourtant certaine.

D'abord négativement : telle ou telle propriété du psychisme humain ou animal, tel ou tel phénomène sociologique *ne demande pas* pour son explication plus que les hypothèses introduites dans le modèle et il n'est donc pas nécessaire, sur ce point, de recourir à des forces ou des structures nouvelles *ad hoc*.

Comme presque toujours, cette assertion négative est la seule qui soit sûre. Mais ce n'est certes pas la plus utile. Quoique l'analogie soit grossière entre la réalité et le modèle, il se peut cependant, si celui-ci est heureusement construit, que les concordances aillent plus loin que le phénomène précis que l'on avait initialement en vue, que certains détails structurels soient non seulement analogues mais semblables.

Evidemment encore, il serait prématuré de voir là une preuve avant que d'autres expériences ou d'autres observations n'aient permis de trier entre ces hypothèses provisoires.

Mais de les avoir suggérées est le rôle heuristique du modèle et c'est là qu'on reconnaîtra la validité de cette méthode.

Année 1959

Bibliographie

[1] Marcel-Paul Schützenberger. A characteristic property of certain polynomials of E. F. Moore and C. Shannon. *Quarterly Progress Report of the Research Lab. of Electronics, MIT*, 66 :117–118, 1959.

[2] Marcel-Paul Schützenberger. Sur l'équation $a^{2+n} = b^{2+m}c^{2+p}$ dans un groupe libre. *C. R. Acad. Sci. Paris*, 248 :2435–2436, 1959.

[3] Marcel-Paul Schützenberger. Sur certains sous-demi-groupes qui interviennent dans un problème de mathématiques appliquées. *Publ. Sci. Univ. Alger Sér. A*, 6 :85–90, 1959.

[4] Marcel-Paul Schützenberger and R. S. Marcus. Full decodable code-word sets. *IRE Trans. Inf. Theory*, IT-5 :12–15, 1959.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

RESEARCH LABORATORY OF ELECTRONICS

QUARTERLY PROGRESS REPORT No. 55

October 15, 1959

Submitted by: J. B. Wiesner
G. G. Harvey
H. J. Zimmermann

(IX. PROCESSING AND TRANSMISSION OF INFORMATION)

C. A CHARACTERISTIC PROPERTY OF CERTAIN POLYNOMIALS OF E. F. MOORE AND C. E. SHANNON

Let $\overline{L}_n$ be the set of all Boolian functions, and L_n the subset of all Boolian functions not involving the negation operation, in the n variates $\alpha(i)$ $(i=1,2,\ldots,n)$. For any $\mu \in \overline{L}_n$, if the $\alpha(i)$ are random independent variates with $Pr(\alpha(i) = 1) = p$, then $Pr(\mu=1)$ is a polynomial (1), $h(\mu)$ in p. We give an elementary necessary and sufficient condition for the existence of at least a $\lambda \in L_n$ for which $h(\mu) = h(\lambda)$. As is well known (2), there is a natural one-to-one correspondence between L_n and the set of all simplicial complexes with, at most, n vertices. Consequently, this condition is also a characterization of the sequences of integers $\{a_j\}$ that can be the number of j-simplexes contained in a complex and its boundary. Because of this interpretation, it is unlikely that the condition is new, but I have not been able to find any relevant reference to it.

With the help of this condition and of the corresponding extremal functions $\omega(g)$ and $\Sigma P_{n-j}^{a_j}$, defined below, more elementary proofs can be given for Yamamoto's inequality (2) on the number of prime implicants of $\lambda \in L_n$ and for the Moore-Shannon lower bound (1) on the value of the derivative of $h(\lambda)$ $(\lambda \in L_n)$.

1. Notations

i. Let P_m^x be the set of the x first products of m of the variates $\alpha(i)$ when these products are taken in lexicographic order with respect to the indices i. We write P_m, instead of P_m^x, when x has its maximal value $\begin{bmatrix} n \\ m \end{bmatrix}$ and $P = \bigcup_m P_m$. For any subset $P' \subset P$, $\Sigma P'$ denotes the Boolian function (belonging to L_n) which is the sum of all the products, β, satisfying $\beta \leqslant \beta'$ for some $\beta' \in P'$. Conversely, for any $\lambda \in L_n$, $P_m\lambda$ is defined as the set of all the $\beta \in P_m$ that are such that $\beta \leqslant \lambda$. Thus, $\lambda = \Sigma P\lambda$ for any $\lambda \in L_n$. The set of all products, $\beta \in P'$, of the form $\beta = \beta'\alpha(i)$, with $\beta' \in P'$ and with $\alpha(i)$ not a factor of β', is denoted by $\Delta P'$ [cf. Yamamoto (2)].

ii. To every pair of positive integers x and m there corresponds one and only one strictly decreasing sequence of $m' \leqslant m$ positive integers: $y_1, y_2, \ldots, y_{m'}$ with the property that

$$x = \begin{bmatrix} y_1 \\ m \end{bmatrix} + \begin{bmatrix} y_2 \\ m-1 \end{bmatrix} + \ldots\ldots + \begin{bmatrix} y_{m'} \\ m - m' + 1 \end{bmatrix}$$

Consequently, the function

$$D_m(x) = \begin{bmatrix} y_1 \\ m-1 \end{bmatrix} + \begin{bmatrix} y_2 \\ m-2 \end{bmatrix} + \ldots\ldots + \begin{bmatrix} y_{m'} \\ m-m' \end{bmatrix}$$

(IX. PROCESSING AND TRANSMISSION OF INFORMATION)

is well determined for all non-negative integers x and m if we define $D_m(0)$ and $D_0(x)$ as zero.

For any x and m, $x + D_m(x) \geqslant D_{m+1}(x)$ (with a strict inequality if and only if $x > m + 1$). For all x, $D_m(x) + D_{m-1}(x') \geqslant D_m(x+x')$ if and only if $x' \leqslant D_m(x)$.

iii. For any $\mu \in \bar{L}_n$, we define the polynomial $g(\mu)$ as the product by $(1+t)^n$ of the function obtained when $(1+t)^{-1}$ is substituted for p in $h(\mu)$. The coefficient a_j of t^j in $g(\mu)$ is the number of monomials with $n - j$ asserted, and j negated, variates $\alpha(i)$ in the canonical expansion of μ; when $\mu \in L_n$, a_j is also the number of elements in $P_{n-j}\mu$.

2. Statement of the Condition

For any $\mu \in \bar{L}_{n'}$, a necessary and sufficient condition that there exist a $\lambda \in L_n$ for which $g(\mu) = g(\lambda)$ $\left(=a_o+a_1t+\ldots+a_mt^m\right)$ is that

$$\begin{bmatrix} n \\ j-1 \end{bmatrix} \geqslant a_{j-1} \geqslant D_j(a_j), \qquad \text{for all } j > 0$$

3. Verification

The condition is sufficient. since, for any polynomial $g(\mu)$ that fulfills it, we can define a function $\omega(g) \in L_n$ as

$$\omega(g) = \Sigma\left(\bigcup_j P_{n-j}^{a_j}\right)$$

and $\omega(g)$ satisfies $g(\omega(g)) = g$ because $\Delta P_m^x = P_{m+1}^{x'}$, when $x' = D_{n-m}(x)$.

It can be remarked that the functions $\Sigma P_{n-j}^{a_j}$ are the only functions in L_n for which $a_{j'-1} = D_{j'}(a_{j'})$ for all $j' \leqslant j$.

The condition is necessary. The first inequality is obvious. With respect to the proof of the second inequality it is enough to consider a truncated function $\lambda = \Sigma P_{n-j}\lambda$ with a_j prime implicants. Let α and α' be any two $\alpha(i)$'s. Then, λ can be written as $\alpha\alpha'A + \alpha(B+C) + \alpha'(B+C') + D$, where A, B, C, C', and D are sums of products not involving α and α', and where, furthermore, $P_{n-j+2}C$ and $P_{n-j+2}C'$ are disjoint sets. It is readily checked that the function $\lambda' = \alpha\alpha'A + \alpha(B+C+C') + \alpha'(B) + D$ is such that the set $P_{n-j}\lambda'$ has a_j elements and that the set $P_{n-j+1}\Delta\lambda'$ has, at most, as many elements as $P_{n-j+1}\Delta\lambda$. By taking successively $\alpha = \alpha(i)$ and $\alpha' = \alpha(i+1)$ for all i, we can reduce the function λ to a function $\Sigma P_j^{a_j}$ and the result is proved.

M. P. Schützenberger

References

1. E. F. Moore and C. E. Shannon, J. Franklin Inst. 262, 191-208; 281-297 (1956).
2. K. Yamamoto, J. Math. Soc. Japan 6, 343-353 (1954).

ALGÈBRE. — *Sur l'équation* $a^{2+n} = b^{2+m}c^{2+p}$ *dans un groupe libre.* Note de M. **Marcel Paul Schützenberger**, présentée par M. Georges Darmois.

En appliquant la théorie des demi-groupes (1), (2) (monoïdes) libres, on vérifie que cette équation (avec $n, m, p \in \mathrm{N}$), dans un groupe libre G, entraîne $bc = cb$, ce qui étend un théorème de R. C. Lyndon (3).

Notations. — Tous les calculs sont effectués dans F, le monoïde libre engendré par les générateurs de G et leurs inverses; $|f|$ désigne la longueur de f; $\varphi : \mathrm{F} \to \mathrm{G}$ est l'homomorphisme canonique; $f \to \bar{f}$, l'anti-automorphisme de F tel que $\varphi\bar{f} = (\varphi f)^{-1}$; $f \to f^*$, l'application de F sur $\mathrm{F}^* \subset \mathrm{F}$ telle que : 1° $\varphi f = \varphi f^*$; 2° $f^* = e_\mathrm{F}$ si $f = \bar{f}$; 3° $(fg)^* = (f^* g^*)^*$; $\pi(f) = \{ f''f' : f'f'' = f \}$; $\mathrm{F}^{**} = \{ f : f^2 \in \mathrm{F}^* \}$; F_1 désigne un sous-monoïde générique de rang unité.

On utilisera les remarques suivantes :

(1) Si $a^{2+n} = fbc'gc''bd'\bar{g}d''\bar{f} \in \mathrm{F}^*$ *et* $|b| \geqq |a|$, *alors* : $f = e_\mathrm{F}$; g *et* $\bar{g}$ *sont des facteurs de* a^2 *et de* b^2; $a, b, c'gc'', d'\bar{g}d'' \in \mathrm{F}_1$.

(2) *Si* $af b\bar{g} = gc\bar{f}a \in \mathrm{F}^*$ *et* $|a| > 0$, *alors* : $b = u\bar{f}g\varphi$; $c = \varphi\bar{g}fu$; $a = g(\varphi\bar{g}u\bar{f}g)^k\varphi\bar{g}$. D'où, par induction : *si* $af b\bar{f}c = c\bar{f}bfa \in \mathrm{F}^*$, *alors* : $f = e_\mathrm{F}$ *et* $a, b, c \in \mathrm{F}_1$.

(3) *Si* $a' \in \pi(a)$, $f' \in \pi(f)$, $a'f' \in \pi(a\bar{f})$, *tous ces éléments appartenant à* F^{**}, *alors* $f = f' = e_\mathrm{F}$ *et* $a, a' \in \mathrm{F}_1$.

(4) *Si* $a^{2+n} = g'(bf)^{1+m}b\bar{g}'g''c(\bar{f}c)^{1+p}\bar{g}''$ *avec* $a, b, c \in \mathrm{F}^{**}$ *et en outre* : $fg'g''$, $\bar{g}'g''\bar{f} \in \mathrm{F}^*$ (*cette dernière condition étant nécessaire*), *alors* $g' = g'' = f = e_\mathrm{F}$ *et* $a, b, c \in \mathrm{F}_1$.

L'énoncé résulte de façon à peu près immédiate de (1) si $|a| \leqq |(bf)^{1+m}|$ ou $\leqq |(\bar{f}c)^{1+p}|$ et l'on vérifie qu'une telle inégalité existe toujours sauf quand $n = 0$, ou $= 1$ et m (ou p) $= 0$.

Dans ces derniers cas, il faut appliquer préalablement (2) pour montrer que $a \in \pi(((\varphi u)^k\varphi f)^{1+m}\varphi u)$ et considérer séparément les cas $n = 1$, $m = 0$, $p \neq 0$; $n = 1$, $m = p = 0$; $n = 0$, $m \neq 0$; $n = m = 0$, $p \neq 0$; $n = m = p = 0$.

(5) *Si* $xa^{2+n}\bar{x} = b^{2+m}c^{2+p} \in \mathrm{F}^*$ *avec* $a, b, c \in \mathrm{F}^{**}$, *alors on a* $x = e_\mathrm{F}$ *et* $a, b, c \in \mathrm{F}_1$.

On déduit de l'équation trois relations $(a'a'')^{n'}a' = (c''c')^{p'}c''$; $(a''a')^{n''}a'' = (b'b'')^{m'}b'$; $(b''b')^{m''}b'' = (\bar{c}'\bar{c}'')^{p''}\bar{c}'$; $n' + n'' = 1 + n$; $m' + m'' = 1 + m$; $p' + p'' = 1 + p$. L'énoncé résulte à peu près immédiatement de (1) et (3) si n, m et p sont tous pairs ou si cinq des nombres $n', n'', m', m'', p', p''$ sont différents de zéro. Si, au contraire, deux de ces nombres sont nuls, on peut éliminer deux des six variables $a', a'', b', \ldots$ et se ramener à une équation du type (4) avec $g' = g'' = e_\mathrm{F}$.

Soit maintenant l'équation $\varphi(a'b'c') = e_\mathrm{G}$ où l'on a écrit pour abréger $a' = a^{2+n}, \ldots$. Cette équation peut, à un automorphisme intérieur près

de G, être transformée en : $a' = (xb'\bar{x}yc'\bar{y})^{\star}$ avec a', b', $c' \in \mathrm{F}^{\star\star}$; donc : ou bien $a' = xb'\bar{x}yc'\bar{y} \in \mathrm{F}^{\star}$ [ce qui est une équation du type (4) avec $f = e_{\mathrm{F}}$], ou bien, en supposant que $|xb'\bar{x}| \geqq |yc'\bar{y}|$, $xb'\bar{x} = a'y\bar{c}'\bar{y} \in \mathrm{F}^{\star}$. Dans ce dernier cas, si $|x| \geqq |a'|$, on pose $x = a'x'$ et, en simplifiant, on retrouve l'équation $y\bar{c}'\bar{y} = x'b'\bar{x}'\bar{a}' \in \mathrm{F}^{\star}$; si $|x| < |a'|$ et $|y|$, on pose $a' = xd$; $\bar{y} = \bar{y}'\bar{x}$, d'où $b' = a''y'\bar{c}'\bar{y}' \in \mathrm{F}^{\star}$ avec $a'' \in \pi(a')$; enfin, si $|y| \leqq |x| < |a'|$, on pose encore $a' = xd$ et $\bar{x} = \bar{x}'\bar{y}$, d'où $x'b'\bar{x}' = a''\bar{c}' \in \mathrm{F}^{\star}$ avec $a'' \in \pi(a')$, ce qui est une équation du type (5).

On observera qu'un carré peut être effectivement un produit de trois carrés [par exemple : $(yx)^2(xy)^2(xyx)^2 = (yxyxxyx)^2$] et que la remarque (1) permet aussi de vérifier que :

Si $(\varphi(b))^{-1}(\varphi(c))^{-1}\varphi(b)\varphi(c) = (\varphi(a))^{2+n}$, *alors* $\varphi a = e_{\mathrm{G}}$.

(1) P. Dubreil, *Mém. Acad. Inst. Fr.*, 63, 1941, p. 1-52.
(2) F. W. Levi, *Bull. Calcutta Mat. Soc.*, 36, 1944, p. 141-146.
(3) *Michigan Mat. J.*, 6, 1959, p. 89-95.

PUBLICATIONS SCIENTIFIQUES
DE L'UNIVERSITÉ D' ALGER

SÉRIE A

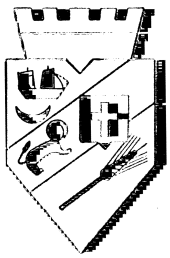
MATHÉMATIQUES

DÉCEMBRE 1959. — Tome VI.

EXTRAIT

M. P. SCHÜTZENBERGER

SUR CERTAINS SOUS-DEMI-GROUPES QUI INTERVIENNENT DANS UN PROBLÈME DE MATHÉMATIQUES APPLIQUÉES



IMPRIMERIE DURAND CHARTRES - 9, RUE FULBERT

Alger, Mathématiques.
Tome VI, 1959.

M. P. SCHÜTZENBERGER (Poitiers)

SUR CERTAINS SOUS-DEMI-GROUPES QUI INTERVIENNENT DANS UN PROBLÈME DE MATHÉMATIQUES APPLIQUÉES

Dans cette note on examine les relations existant entre deux systèmes de conditions qui peuvent caractériser certains sous-demi-groupes intervenant dans un problème d'algèbre appliquée (1).

On fera toujours l'hypothèse que l'élément neutre e du demi-groupe S est contenu dans le sous-demi-groupe P.

Les huit conditions U_x^y sont de la forme :

Si pour un $s \in S$, $U_x^y(s)$ intersecte P, alors s appartient à P, avec :

$$U_d^m(s) = sP \cap Ps; \quad U_r^m(s) = Ps; \quad U_l^m(s) = sP; \quad U_k^m(s) = PsP;$$
$$U_d^f(s) = sS \cap Ss; \quad U_r^f(s) = Ss; \quad U_l^f(s) = sS; \quad U_k^f(s) = SsS;$$

(1) L'intérêt pratique de ces conditions peut être rappelé brièvement comme suit : Soit S demi-groupe libre engendré par un ensemble dénombrable de symboles S_1; P un sous-demi-groupe de S engendré par un ensemble de mots P_1.

La condition U_d^m est nécessaire et suffisante pour que P_1 puisse être utilisé comme un « code » afin de transmettre des messages au moyen des signaux élémentaires en correspondance biunivoque avec les éléments de S_1; U_d^m étant supposée satisfaite, N_d^m devient une condition nécessaire et suffisante pour qu'il existe une distribution de probabilité pour laquelle ce code soit admissible du point de vue de la longueur moyenne des mots. Dans ce cas, N_d^f contrôle la distribution asymptotique du délai au décodage. Les codes unilatéraux (U_r^m) sont les plus importants pratiquement puisque pour eux ce délai est minimal. Et, parmi ceux-ci, les codes satisfaisant U_r^f présentent des caractères optimaux étudiés par B. Mandelbrot qui les a le premier définis. U_k^m signifie donc que le message peut être décodé sans délai aussi bien de droite à gauche que de gauche à droite, etc. (Cf. [8]).

Les huit conditions N_x^y sont de la forme :

Pour tout $s \in S$; $U_{x'}^{y'}(s)$ intersecte P avec $y' = m$ (ou f) quand $y = f$ (ou m) et x' correspondant à x de la façon suivante :

$$d' = k; \qquad r' = l; \qquad l' = r; \qquad k' = d.$$

Par exemple, P satisfait U_r^m et N_d^f si, pour tout $s \in S$, la relation $sp = p'$ avec p, $p' \in P$ entraîne $s \in P$ et si pour tout $s \in S$, il existe au moins une paire p'', $p''' \in P$ telle que $p''sp''' \in P$.

Puisque l'on a supposé que e appartient à P, on a pour $A = U$ ou N :

1) Quelque soit $x = d$, r, l ou k, A_x^f entraîne A_x^m;

2) Quelque soit $y = m$ ou f, si A_r^y ou A_l^y, alors A_d^y;

3) Quelque soit $y = m$ ou f, si A_r^y et A_l^y, alors A_k^y et réciproquement.

La plupart de ces conditions ont déjà été étudiées et définies par P. Dubreil [4, 5, 6] dans le cas plus général d'un sous-ensemble et non pas seulement d'un sous-demi-groupe. U_k^m : « *unitaire* »; U_r^m (U_l^m) « *unitaire à gauche (à droite)*; N_k^m (N_r^m, N_l^m) « *net* » *(à droite, à gauche);* U_r^f (U_l^f) « *consistant à droite* » *(à gauche)*; nous rappelons les propriétés les plus simples qui se déduisent de ces conditions :

U_d^m est une condition nécessaire et suffisante pour que P soit libre quand S est un demi-groupe libre; U_r^m est satisfaite de façon caractéristique par les sous-demi-groupes qui laissent fixe un point dans une représentation à droite de S; U_x^f (avec $x = r$, l) exprime que $S - P$ est un idéal (à droite, à gauche,) et se rattache à des notions de primalité; N_x^m ($x = d$, r, l, k) signifie que P intersecte tous les idéaux (bilatères, à droite, à gauche, *bi*-idéaux); N_x^f ($x = k$, l, r, d) est satisfaite quand P contient un idéal (bilatère, à droite, à gauche *bi*-idéal). Si S est un groupe ou un demi-groupe commutatif, A_x^y est équivalent à $A_{x'}$, pour $A = U$ ou N et y, x et x' quelconques. Plus particulièrement :

Quand S est un groupe, U_x^m est nécessaire et suffisante pour que P soit un sous-groupe et non pas seulement un sous-demi-groupe; N_x^m est satisfaite de façon triviale et A_x^f entraîne $P = S$.

Quand S est un treillis, A_x^m est équivalente à A_y^f; U_x^y est nécessaire et suffisante pour que P soit un idéal dual de S et N_x^y pour que P contienne le zéro de S.

Pour S quelconque, les seules relations qui existent entre ces conditions sont triviales mais pour une classe qui comprend en particulier tous les demi-groupes compacts il est possible de prouver la

PROPOSITION : *S'il existe un homomorphisme* φ *de* S *tel que* $P = \overset{-1}{\varphi}\varphi P$ *et que* φS *admette des bi-idéaux minimaux, toute paire de conditions* $(U_x^y, N_{x'}^{y'})$ *est équivalente à l'une des onze paires suivantes :*

1) (U_x^y, N_x^y) *avec* $y = m$ *ou* f *et* $x = d, r, l$ *ou* k.

2) (U_x^m, N_x^f) *avec* $x = d, r,$ *ou* l.

II. RELATIONS FORMELLES ENTRE LES CONDITIONS.

1° On vérifie directement que les huit paires suivantes — ou toute combinaison plus forte entraînent que P soit égal à S :

$(U_x^y, N_{x'}^{y'})$ avec $y \neq y'$ et (x, x') de la forme (d, k) ou (r, l).

D'autre part, certaines paires entraînent automatiquement une condition plus forte. Tenant compte de la symétrie gauche-droite, il suffit de vérifier les cas suivants :

2° Quand U_r^f, N_d^m est équivalent à N_r^f.

3° Quand N_r^m, U_d^f est équivalent à U_r^f.

4° Quand U_r^m, N_d^f est équivalent à N_r^f.

5° Quand N_r^f, U_d^m est équivalent à U_r^m.

Les démonstrations sont immédiates et le fait qu'aucune autre réduction ne se produit dans le cas général sera établi plus bas par des contre exemples.

III. DÉMONSTRATION DE LA PROPOSITION.

Toujours à cause de la symétrie, il suffira de prouver que sous les hypothèses faites l'on a :

1° Si U_r^m et N_d^m, alors N_r^m.

2° Si N_r^m et U_d^m, alors U_r^m.

3° Si U_d^f et N_d^m, alors N_d^f.

La condition $\overset{-1}{\varphi}\varphi P = P$ implique que φP satisfasse A_x^y dans φS en même temps que P satisfait la même condition dans S. On pourra donc supposer que S admet les *bi*-idéaux minimaux $K_j^i (i \in I, j \in J)$ dont l'union D est l'idéal bilatère minimum de S. On posera $R_j = \bigcup_{i \in I} K_j^i$ et $L^i = \bigcup_{j \in J} K_j^i$ et puisque toutes les conditions considérées sont plus fortes que N_d^m, on pourra supposer que $P \cap D$ contient $q \in K_{j_1}^{i_1}$.

Démonstration de 1°. Soit $s \in S$ quelconque; puisque q appartient à l'idéal à droite minimal R_{j_1}, il existe au moins un s' tel que $qss' = q$. Mais, à cause de U_r^m, cette relation implique que ss' appartienne à P. Donc, à tout $s \in S$ il correspond au moins un s' tel que $ss' \in P$ et c'est là la condition N_r^m.

Démonstration du 2°. On observe d'abord que pour tout $j \in J$, l'élément idempotent $e^{i_1}_j$ de $K^{i_1}_j$ appartient à P : en effet, N^m_r implique que pour tout $j \in J$ il existe au moins un élément, $q_j \in P \cap R_j$. On a $q_j q \in P$ et $(e^{i_1}_j q_j)\, q = q_j q = q_j (q e^{i_1}_j)$, c'est-à-dire, $e^{i_1}_j P \cap P e^{i_1}_j \cap P \neq \emptyset$; donc, d'après U^m_d, $e^{i_1}_j \in P$. Pour la même raison, l'inverse $\bar{q}$ de q dans $K^{i_1}_{j_1}$ appartient à P puisque $q\bar{q} = \bar{q}q = e^{i_1}_{j_1}$. Par conséquent, si $s \in R_{j_2}$ satisfait la relation $qs \in P \cap K^{i_2}_{j_1}$, il appartient aussi à P puisque l'on a $s = e^{i_1}_{j_2} e^{i_1}_{j_1} s = e^{i_1}_{j_2} \bar{q} q s$ et que $e^{i_1}_{j_2}$, $\bar{q}$ et qs appartiennent tous à P.

Soit maintenant t, un élément quelconque de S satisfaisant la relation $pt \in P$ pour au moins un élément $p \in P$. Multipliant à gauche par $P \cap D$, on obtient au moins une relation de la forme $q't = q''$ avec $q', q'' \in P \cap D$ et, par exemple $q'' \in K^{i_2}_j$. Puisque $qt = qte^{i_2}_j$, et, en tenant compte de la dernière remarque, $te^{i_2}_j = q'''$ appartient à P et l'on a finalement $(q'''q')t = q'''q'' = t(e^{i_2}_j q'')$ ce qui, d'après U^m_d entraîne $t \in P$. Donc $Pt \cap P \neq \emptyset$ entraîne $t \in P$ et c'est là la condition U^m_r.

Démonstration de 3°. Soit s un élément quelconque de $K^{i_1}_{j_1}$; $\bar{s}$ son inverse. Comme $e^{i_1}_{j_1} = s\bar{s} = \bar{s}s$ appartient à P ainsi que l'on vient de le voir, la condition U^f_d entraîne que s (et $\bar{s}$) appartienne à P. Donc, plus généralement, U^f_d implique que tout bi-idéal minimal qui intersecte P soit contenu dans P. Soit maintenant s quelconque, le produit $e^{i_1}_{j_1} s e^{i_1}_{j_1}$ appartient à $K^{i_1}_{j_1}$, donc à P; Donc, pour tout $s \in S$ $PsP \cap P \neq \emptyset$, ce qui est la condition N^f_d.

IV. Contre exemples.

C'est une conséquence immédiate des définitions que si $P_1 \subset S_1$ satisfait $A^{y_1}_{x_1}$ et $P_2 \subset S_2$ satisfait $A^{y_2}_{x_2}$ le produit direct $P_1 \times P_2 \subset S_1 \times S_2$ satisfait $A^{y_3}_{x_3}$ où y_3 et x_3 dépendent de x_1, x_2, y_1 et y_2 selon les tableaux suivants :

y_1 \ y_2	m	f
m	m	m
f	m	f

si $x_1 = x_2 = x_3$

x_1 \ x_2	d	r	l	k
d	d	d	d	d
r	d	r	d	r
l	d	d	l	l
k	d	r	l	k

si $y_1 = y_2 = y_3$

Avec l'aide de cette remarque, et en notant désormais par S′ un demi-groupe anti-isomorphique avec S, il est possible de réduire à six le nombre des contre-exemples nécessaires. On rappelle que e désigne toujours l'élément neutre.

Cas 1. $S = (e, a, b)$; $P = (e, a)$ avec $a = a^2 = ba$; $b = b^2 = ab$.

Cas 2. $S = (e, a, b, ab)$; $P = (e, a)$ avec $e = b^2$; $a = a^2 = ba$.

Cas 3. N'importe quel sous-groupe propre d'un groupe.

Les preuves sont de simples vérifications.

Soit maintenant Z l'ensemble des entiers naturels et S le demi-groupe consistant en l'application identique e et l'ensemble des injections de Z dans lui-même telles que :

$$\text{Card}\,(Z.s) = \text{Card}\,(Z - Z.s) = \text{Card}\,(Z).$$

Il est bien connu que $S - e$ est formé d'un idéal à droite unique et que l'équation en s : $xs = y \neq e$ admet toujours une solution (l); donc, dans les deux cas suivants, N_r^m sera toujours satisfaite.

Cas 4. Soit s_0 un élément fixe de $S - e$; $Z_0 = Z.s_0$ et P consistant en les $a \in S$ dont la restriction à Z_0 est une bijection de cet ensemble sur lui-même.

Puisque pour tout sous-ensemble Z′ de Z et tout s, $s' \in S$ on a $Z'.ss' \subset Z'.s'$, P ne peut pas satisfaire N_1^m. D'autre part, si $p \in P$, ps (ou sp) ne peuvent appartenir à P que s'il en est de même de s et, par conséquent, P satisfait U_k^m.

Cas 5. On écrit Inv (s) pour représenter le nombre cardinal de paires $(i, j) \in (Z, Z)$ telles que $i < j$ et $i.s > j.s$ et on considère $P = \{s : \text{Inv}\,(s) = 0\}$. Au moyen de la formule.

$$\text{Inv}(s) - \text{Inv}(s') \leqslant \text{Inv}(ss') \leqslant \text{Inv}(s) + \text{Inv}(s')$$

on vérifie que P satisfait U_l^m et non U_r^m. N_k^m est satisfaite puisque l'on peut trouver pour tout $s \in S$, s' et s'' tels que ss' et $s''s$ appartiennent à P.

Cas 6. Soit S le demi-groupe libre engendré par a et b; T_1, l'ensemble des mots de S de la forme $a^{l+m}b^{l+n}$; T, le sous-demi-groupe engendré par T_1; P_1, l'ensemble des mots de la forme $b^{|t|}ta^{|t|}$ où $t \in T$ et où $|t|$ désigne la longueur de t; P le demi-groupe engendré par P_1.

Quelque soit $s \in S$, le produit xsy où $x = b^{|s|+2}a$ et $y = ba^{|s|+2}$ appartient à P. Donc P satisfait N_2^m. Réciproquement, si $p \in P$ est de la forme $b^m a\ldots$, l'on sait que $p = p'p''$ où $p'' \in P$ et $p' = b^m asba^m$ avec, évidemment, $m = 2 + |s|$. Donc $ps \in P$ et $p \in P$ entraînent $s \in P$ et, par symétrie, U_k^m. Soit maintenant s un élément quelconque de S

tel qu'il existe à la fois x et y satisfaisant $xs \in P$ et $sy \in P$. On peut écrire s sous la forme $ps'p'$ avec $p,p' \in P$ maximaux du point de vue de la longueur. Si s' n'était pas le mot vide, il serait à la fois un diviseur à droite et un diviseur à gauche d'un certain élément $p'' \in P$, c'est-à-dire qu'il aurait la forme $b^n a \ldots b a^{n'}$ avec les conditions mutuellement contradictoires que $n \geqslant n' + 2$ et $n' \geqslant n + 2$. Donc s appartient à P et P satisfait U_a^l.

Remarque. — On observera que tous les contre-exemples, sauf le dernier, peuvent être construits au moyen de demi-groupes qui non seulement possèdent un idéal bilatère minimum, mais encore, de façon plus restrictive, consistent en l'union d'un élément unité et d'un demi-groupe d-simple selon la terminologie de Green et Clifford [3, 7].

RÉFÉRENCES

[1] R. Baer et F. Levi, *Sitzber. Heidelberg. Akad. Wiss*, **18**, 19, 1932.
[2] A. H. Clifford, *Am. J. Math.*, **70**, 521-526, 1948.
[3] A. H. Clifford, *Am. J. Math.*, **75**, 547-556, 1953.
[4] P. Dubreil, *Mem. Acad. Sci.*, Inst. France, **2**, 1-52, 1941.
[5] P. Dubreil, *Rend. Circ. Mat. Palermo*, **10**, 1-18, 1951.
[6] P. Dubreil, *Bull. Soc. Math. France*, 289-306, 1953.
[7] J. A. Green, *Ann. Math.*, **54**, 163-172, 1951.
[8] M. P. Schützenberger and R. S. Markus, *I. R. E. Trans. Inf. Theory*. 5, n° 1. 1959, pp. 12-15.

Manuscrit reçu en juin 1959.

M. P. SCHÜTZENBERGER
Maître de conférences
Faculté des Sciences de Poitiers.

12 IRE TRANSACTIONS ON INFORMATION THEORY March

Full Decodable Code-Word Sets*

M. P. SCHÜTZENBERGER† AND R. S. MARCUS‡

Summary— **This paper considers further how the decodability condition imposes restrictions on a set of code words. A generating function is defined that describes the composition of the code words. The relation between the generating function and a "full" set of code words is found. This relation shows that the sum of arbitrary probabilities associated with the words of a full set must be one. A full set of code words is one to which no code word can be added and still keep the set decodable. It is also shown that a full set is "completable." For a completable set of code words any string of symbols can be made into a sentence by adding a suitable prefix and a suffix.**

Introduction

SEVERAL authors have considered the restrictions that are imposed on the set of code words by the decodability condition.[1-5] (A code-word set is decodable if no string of symbols can be broken up into code words in more than one way.) Most of the results thus far have had to do with the *lengths* of the code words. This paper includes some conclusions relating to the more detailed *composition* of the code words.

It is important to consider the composition of the code words, as well as their lengths, when the symbols are not of the same cost. For example, in the Morse code the dot is shorter in time duration than the dash. The less costly dot, therefore, should be used more frequently for efficiency of information transmission.

In particular, this paper defines a generating function that describes the composition of the code words. The relation between this function and a "full" set of code words is found. A full set of code words is one to which no code words can be added and still keep the set decodable. It is also shown that a full set is "completable." For a completable set of code words, any string of symbols can be made into a sentence by adding a suitable prefix and a suffix.

* Manuscript received by the PGIT, July 25, 1958. This work was supported in part by the U. S. Army (Signal Corps), the U. S. Air Force (Office of Sci. Res., Air Res. and Dev. Com.), and the U. S. Navy (Office of Naval Research).

† Faculté des Sciences de Poitiers, France; formerly with Res. Lab. of Electronics, Mass. Inst. Tech., Cambridge, Mass.

‡ Res. Lab. of Electronics, Mass. Inst. Tech., Cambridge, Mass.

[1] A. A. Sardinas and G. W. Patterson, "A necessary and sufficient condition for unique decomposition of coded messages," 1953 IRE National Convention Record, pt. 8, pp. 104–108.

[2] B. Mandelbrot, "On recurrent noise limiting coding," *Proc. Symp. on Information Networks*, New York, N. Y.; 1954.

[3] B. McMillan, "Two inequalities implied by unique decipherability," IRE Trans. on Information Theory, vol. IT-2, pp. 115–116; December, 1956.

[4] M. P. Schützenberger, "On an application of semi-group methods to some problems in coding," IRE Trans. on Information Theory, vol. IT-2, pp. 47–60; September, 1956.

[5] R. S. Marcus, "Discrete noiseless coding," S. M. thesis, Dept. Elec. Eng., M. I. T., Cambridge, Mass.; January, 1957.

Statement of the Problem

Let us consider an information-carrying channel with D symbols, d_i, $j = 1, \cdots, D$. For any given string of symbols, s, we write $|s|_i \equiv$ the number of occurrences of symbol d_i in s, and $|s| \equiv$ the total number of symbols in s. Thus, $|s| = \sum_i |s|_i$. A *code word*, w_k, is a particular s. The *code-word set*, P_0, is a set of M code words. *Sentences* are strings of words and they form the infinite set $P = \{P_0\}$. It is always understood that the lengths of the code words are bounded. Without this hypothesis, the conclusions are somewhat different.

It is convenient to associate with the set $\{d_i\}$ an arbitrary set of probabilities, p_i ($\sum p_i = 1$, $p_i > 0$, $j = 1, \cdots, D$). Then we write $Pr(s) = \prod_i p_i^{|s|_i}$. We may now define the *generating function of the words*, $\phi_{P_0}(t)$:

$$\phi_{P_0}(t) = \sum_k Pr\,(w_k) t^{|w_k|} = \sum_{i=1}^{n_m} a_i t^i, \tag{1}$$

where

$$a_i = \sum_{|w_k| = i} Pr\,(w_k)$$

$$n_m = \max\{|\,w_k\,|\}.$$

Similarly, we define the *generating function of the sentences*, $\Phi_P(t)$:

$$\Phi_P(t) = \sum_{s \in P} \nu(s)\, Pr\,(s) t^{|s|} = \sum_n A_n t^n, \tag{2}$$

where

$$A_n = \sum_{|s| = n} \nu(s)\, Pr\,(s)$$

$\nu(s)$ = number of decompositions of s into words.

A code-word set, P_0, is then uniquely decodable or, let us say, just *decodable* (d), if $\nu(s) = 1$ for all s in P. (Of course, $\nu(s) = 0$, if s is not in P.) P_0 is said to be *full* (F) if no word can be added to P_0 to form a code-word set that is decodable. P_0 is said to be *completable* (C) if any string, s, can be made to fit in P by adding some suitable prefix and suffix. (Symbolically, we write: P_0 is C if $\forall\ s\ \exists\ x$ and y ϶ xsy ε P.)[6]

The four theorems that will be presented show that the four following statements are equivalent for decodable code-word sets:

I. P_0 is full.
II. P_0 is completable.
III. $\phi_{P_0}(1) = 1$ for some particular p_i set. (3)
IV. $\phi_{P_0}(1) \equiv 1$ for all p_i sets.

[6] The symbols xsy denote the string x, followed by the string s, followed by the string y. Here x and y may vary for different s's. $\forall$ means for all; $\exists$ means there exists; ϶ means with the property that; ε means belonging to.

THEOREMS

Theorem I: If P_0 is C, then $\phi_{P_0}(1) = 1$.

Method of Proof: Since the sentences are defined recursively, the A_n are given by a difference equation and are the sums of roots to the nth power, as shown in section 1). For P_0 completable, we show that the A_n cannot become vanishingly small, as shown in sections 2)–4). But for P_0 decodable, the A_n cannot become larger than one. Thus the root of minimum modulus, the real root, must be one.

Proof:

1)
$$A_n = \sum_{i=1}^{n_m} B_i T_i^{-n}, \tag{4}$$

where T_i are the roots of $\phi_{P_0}(t) = 1$
B_i are constants.

Eq. (4) is true, since A_n is given by

$$A_n = \sum_{i=1}^{n_m} a_i A_{n-i}. \tag{5}$$

The solution of the difference (5) is given by

$$A_n = \sum_{i=1}^{n_m} B_i \rho_i^n, \tag{6}$$

where ρ_i are roots of $\rho^{n_m} - a_1\rho^{n_m-1} - \cdots - a_{n_m} = 0$
B_i are constants.

Letting $T = \rho^{-1}$, we have

$$T^{-n_m} - a_1 T^{1-n_m} - a_2 T^{2-n_m} - \cdots - a_{n_m} = 0$$
$$= 1 - a_1 T - a_2 T^2 - \cdots - a_{n_m} T^{n_m}$$
$$= 1 - \phi_{P_0}(T).$$

This proves (4).

2) If P_0 is C, then the number of symbols in any prefix and suffix that is needed to make s in P is bounded. More specifically, we have

$$|x| + |y| \leq L = 2n_{m-1}. \tag{7}$$

This is obviously true, since if $|x| > n_m$ we could break up x into words and a string x' with the property that $|x'| < n_m$. This x' could serve as a suitable prefix; similarly for y.

3) If P_0 is C, then $\sum_{n=\alpha}^{\alpha+L} A_n > C_1 > 0$; (for any α). (8)

To prove this, let u_i be the $D^\alpha s \ni |s| = \alpha$. (See Fig. 1.)

Let u_i' be one $xu_iy \in P \ni |x| + |y| \leq L$. Hence,

$$\alpha \leq |u_i'| \leq \alpha + L.$$

Some of the u_i' may be the same but we can pick a set of distinct u_i', say v_j, with the property that each u_i can be expanded into at least one v_j. Let $u_{i,j}$ be the set of u_i that can be expanded into a given v_j.

Let

$$\sum_{u_i \in u_{i,j}} Pr(u_i) \equiv Pr(u_{i,j}).$$

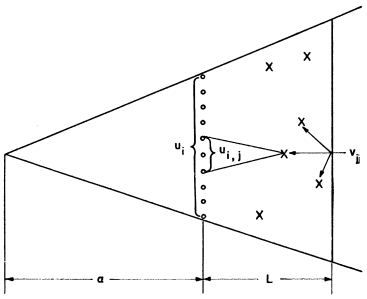


Fig. 1—Abstraction from code-word tree.

Then

$$\sum_j Pr(u_{i,j}) \geq \sum_i Pr(u_i) = 1.$$

Now from each $u_{i,j}$ pick the u_i (call it w_j) with the maximum $Pr(u_i)$. The maximum number of u_i in any $u_{i,j}$ is $|v_j| - \alpha + 1$. An upper bound on this number is $(\alpha + L) - \alpha + 1 = L + 1$. Thus $Pr(w_j) \geq [1/(L+1)]$ $Pr(u_{i,j})$. But $Pr(v_j) = Pr(x)\ Pr(w_j)\ Pr(y) \geq p_{\min}^L\ Pr(w_j)$, where $p_{\min} = \min\{p_i\}$. Hence,

$$\sum_{n=\alpha}^{\alpha+L} A_n \geq \sum_j Pr(v_j) \geq p_{\min}^L \sum_j Pr(w_j)$$
$$\geq \frac{p_{\min}^L}{L+1} \sum_j Pr(u_{i,j}) \geq \frac{p_{\min}^L}{L+1} \equiv C_1 > 0$$

This proves (8).

4) Hence, $\lim_{n\to\infty} A_n > C_1/(L+1) \equiv C_2 > 0$ (if the limit exists).

5) Hence, $|T_1| \leq 1$, where $|T_1|$ is the minimum modulus. If $|T_1| > 1$, $A_n \to 0$ as $n \to \infty$.

6) A_n must be bounded. If A_n were not bounded, then $\nu(s)$ would be greater than one for some s because

$$A_n = \sum_{|s|=n} \nu(s)\ Pr(s) \quad \text{and} \quad \sum_{|s|=n} Pr(s) = 1.$$

This would mean that P_0 is not d, contrary to the hypothesis that P_0 is C.

7) Hence, $|T_1| \geq 1$. Otherwise A_n would be unbounded.

8) Since all the coefficients of $\phi_{P_0}(t)$ are positive, $\phi_{P_0}(t)$ is monotonic and $\phi_{P_0}(t) = 1$ has one real root, and no other root has a modulus smaller than this.[7]

9) Hence, $|T_1| = T_1 = 1$.

10) Hence, $\phi_{P_0}(1) = 1$ (and this is true for all p_i sets).

Theorem II: If $\phi_{P_0}(1) = 1$ and P_0 is d, then P_0 is F.

Proof: If we add a word to P_0 to give P_0', then $\phi_{P'_0}(1) > 1$, and T_1', the real root of $\phi_{P'_0}(t) = 1$, is less than one. But by Theorem I, section 6), and Theorem I, section 7), this implies that P_0' is not d. Thus P_0 is F.

[7] The fact that the real root has the minimum modulus follows from Cauchy's theorem. Cf. Morris Marden, "The Geometry of the Zeros of a Polynomial in a Complex Variable," Mathematical Surveys No. III, American Mathematical Society, New York, N. Y.; 1949. See especially Theorem (27.1), p. 95.

Theorem III: If P_0 is d and $\phi_{P_0}(1) = 1$ for a given p_i, then P_0 is C.

Proof: Suppose P_0 is not C. Then $\exists\ s_0\ \mathfrak{s}\ \forall x, y\ xs_0y \notin P$. Since no s with s_0 as a prefix is in P, those strings in that part of the tree that "grows" from s_0 can be eliminated as possible s in P. This means that for $n \geq |s_0|$,

$$A_n \leq 1 - Pr\,(s_0).$$

Of those strings that do not begin with s_0, we can eliminate that fraction whose second $|s_0|$ symbols are s_0. Thus

$$A_n \leq [1 - Pr\,(s_0)]^2 \quad \text{for} \quad n \geq 2\,|\,s_0\,|.$$

Similarly,

$$A_n \leq [1 - Pr\,(s_0)]^m \quad \text{for} \quad n \geq m\,|\,s_0\,|.$$

Hence, $A_n \to 0$ as $n \to \infty$. But for given p_i, $T_1 = 1$ and $A_n > C_3 > 0$ for some $n > N$ for any N. Hence, we have a contradiction and P_0 is C.

Theorem IV: If P_0 is F, then P_0 is C.

Method of Proof: Assuming that P_0 is not completable, we consider the string, u, which cannot be completed. If we add u as a word to P_0, we obtain a new set, $\bar{P}_0$, which cannot be decodable. We then show that this implies that u has the same string of symbols in its beginning as at its end, as shown in section 14). But this leads to a contradiction.

Proof:

1) Assume that P_0 is F but not C.

2) Hence, $\exists\ u\ \mathfrak{s}\ \forall\ x, y\ xuy \notin P = \{P_0\}$.

3) Consider $\bar{P}_0 = P_0 \cup u$ and $\bar{P} = \{\bar{P}_0\}$.

4) Since $\bar{P}_0$ is not decodable, $\exists\ v$ with two decompositions in $\bar{P}$.

5) Choose v as a minimal doubly decomposable string (minimal d.d. string); that is, a string that cannot remain d.d. if any symbols are removed from its beginning and/or end.

6) Since P_0 is d and $\bar{P}_0$ is not, one of the decompositions of v must contain u as a word. Thus $v = x_1uy_1$, where $x_1, y_1\ \mathfrak{e}\ \bar{P}$.

7) Since u is not completable in P, $v \notin P$.

8) But $v\ \mathfrak{e}\ \bar{P}$.

9) Hence, the second decomposition of v also contains u, *i.e.*, $v = x_2uy_2$.

10) Assume that $|x_1| \leq |x_2|$. If this is not so, reverse designations.

11) $|x_2| \neq |x_1|$. If $|x_2| = |x_1|$, then $x_2 = x_1$, and for v to be d.d. either $x_1 = x_2$ is d.d. or $y_1 = y_2$ is d.d., contrary to the hypothesis that v is a minimal d.d. string.

12) Hence, $|x_1| < |x_2|$.

13) Let us so choose the second decomposition that $|x_2| < |x_1| + |u|$. (See Fig. 2.)

Otherwise, x_2 contains u and must be decomposed as $x_2 = x_3uy_3$ by the same reasoning that led to section 9). Thus we could have chosen to consider the first u as the word u in the second decomposition of v.

14) Thus $u = x_4u_2 = u_2y_4$. (See Fig. 3.)

15) We can find (as we shall show) a u' for which the equation of section 14) cannot be satisfied. Hence, the assumption that P_0 is F, but not C, which leads to this conclusion, is false and the theorem is proved.

16) To find u' we consider two cases that cover all the possibilities.

Case 1): $u = a^{|u|}$.

Case 2): $u = a^kby_5$; $0 < k < |u|$, $0 \leq |y_5|$.

We have arbitrarily called the first symbol in u "a" and the first symbol in u which is not a, if such a symbol exists, "b".

17) For case 1), let $u' = ub = a^{|u|}b$.

Clearly, u' cannot satisfy

$$u' = x_5w = wy_6; \qquad |\,y_6\,| > 0,$$

since w must start with a and end with b.

18) For case 2), let $u' = ub^{|u|}$.

$|w| \leq |u|$ is clearly impossible, for then w would have to start with "a" but consist only of b's.

But if $|w| > |u|$, we can write

$$w = x_6ab^{r+|u|},$$

where $0 \leq |x_6|$; $0 \leq r < |u|$.

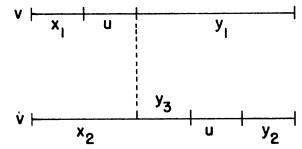


Fig. 2—Grouping of symbols in the string v.

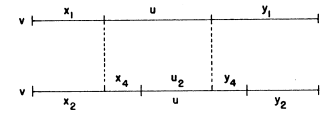


Fig. 3—Grouping of symbols in the string v.

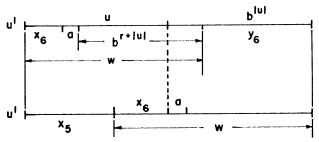


Fig. 4—Grouping of symbols in the string u'.

Then, as is apparent from Fig. 4, $u' = x_5w$ requires that the "a" in question occur in a position that must be a "b" from the fact that $u' = wy_6$. This contradiction shows that the given u' for case 2) does not satisfy section (14). Thus section 15) is proved and Theorem IV, in turn, is proved.

Conclusion

The four theorems, taken together, show the logical equivalence of the four properties of the statements of equation 3), as is indicated in Fig. 5.

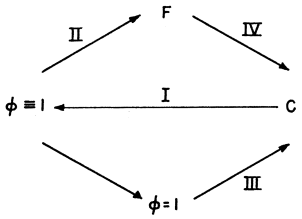


Fig. 5—Diagram showing the relations of the four theorems.

Sections 1)–5) of Theorem I then show that the probabilities associated with a full code-word set must sum at least to one. Sections 6) and 7) of Theorem I show that this sum must be no more than one if the code is decodable; that is, $\phi_{P_0}(1) \leq 1$ if P_0 is d. It can easily be shown that this inequality leads to the generalized Kraft[8] inequality

$$\sum_{k=1}^{M} 2^{-q_k} \leq 1,$$

where q_k is the normalized cost of word w_k.

Our discussion shows that the equality sign holds only when P_0 is full. This inequality was obtained by Marcus[5] by extending Mandelbrot's proof[2] for the equal-cost case. Mandelbrot used Shannon's Fundamental Theorem for Discrete Noiseless Channels[9] and pointed out that a similar inequality had been obtained previously by Szilard. McMillan[3] obtained a proof in the equal-cost case without using information-theory concepts. Note that the proofs of this paper are also independent of the Shannon theorem.

For the equal-cost case, the normalized cost is just $q_k = n_k \log D$, with $n_k = |w_k|$. Thus the inequality reads:

$$\sum_{k=1}^{M} D^{-n_k} \leq 1.$$

[8] L. G. Kraft, "A device for quantizing, grouping and coding amplitude modulated pulses," S. M. thesis, Dept. Elec. Eng., M. I. T. Cambridge, Mass.; 1949.

[9] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. J.*, vol. 27, pp. 379–423; July, 1948.

Année 1960

Bibliographie

[1] Marcel-Paul Schützenberger. Un problème de la théorie des automates. In *Séminaire Dubreil-Pisot, année 1959-60*, Exposé No. 3, 6 pages. Inst. H. Poincaré, Paris, 1960.

Séminaire Dubreil.
Algèbre et théorie
des nombres

MARCEL P. SCHÜTZENBERGER

Un problème de la théorie des automates

Séminaire Dubreil. Algèbre et théorie des nombres, tome 13, n° 1 (1959-1960), exp. n° 3, p. 1-6.

<http://www.numdam.org/item?id=SD_1959-1960__13_1_A3_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
13e année, 1959/60, n° 3

3-01

23 novembre 1959

UN PROBLÈME DE LA THÉORIE DES AUTOMATES

par Marcel P. SCHÜTZENBERGER

Un "one way, one tape" [2] automate A est un algorithme destiné à classer les mots du monoïde libre F_X engendré par $X = \{x\}$, fini, d'après le mécanisme suivant :

A est donné par

1° Un ensemble fini $S = \{s\}$ avec un élément s_0 et un sous-ensemble S_1, distingués.

2° Une application $(S, X) \longrightarrow S$ (notée sx).

Cette application se prolonge de façon naturelle en une représentation de F_X par un monoïde d'applications de S dans lui-même et on dit que $f \in F_X$ est accepté ou non selon que $s_0 f$ appartient ou non à S_1. L'ensemble F' des mots qui peuvent être acceptés par un automate fini a été caractérisé par S. C. KLEENE [1] au moyen d'opérations logiques.

Dans cet exposé, nous montrons que la somme formelle $\sum \{f : f \in F'\}$ peut, dans un certain sens, être considérée comme une fonction "rationnelle" des $x \in X$. Nous généralisons ensuite cette propriété en montrant que si S au lieu d'être fini est le produit direct d'un ensemble fini par Z (le groupe additif des entiers) et si l'application $(S, X) \longrightarrow S'$ et le sous-ensemble S_1 sont définis de façon convenable, alors la somme correspondante est dans un certain sens une fonction "algébrique".

Cette terminologie se justifie par le fait que si les variables x étaient des variables commutatives ordinaires, les sommes correspondantes seraient effectivement rationnelles ou algébriques.

Indépendamment de toute notion d'automate, les sous-ensembles $F' \subset F_X$ considérés peuvent être définis comme des unions finies des sous-ensembles tels que $F' = \varphi^{-1} g$ où g est un élément d'un certain monoïde quotient φF_X de F_X. Quand S est fini, φF_X l'est aussi ; la généralisation que nous proposons contient comme cas particulier celui où φF_X est l'extension de Z par un groupe fini.

NOTATION : Ω un anneau unital ; Ω_n l'anneau des $n \times n$ matrices sur Ω ;

3-02

Π_p le projecteur de $A_X(\Omega)$ sur le sous-module dont une base est l'ensemble des $f \in F_X$ de longueur $\leqslant p$.

On complète $A_X(\Omega)$ en une algèbre de série (infinies) $\bar{A}_X(\Omega)$ en posant ab = l'élément unique c tel que, pour tout p , $\Pi_p c = \Pi_p(\Pi_p a\ \Pi_p b)$. Si $a \in \bar{A}_X(\Omega)$ est tel que $\Pi_0 a = 0$, on définit $(1-a)^{-1}$ comme l'élément unique c tel que, pour tout p , $\Pi_p c = \Pi_p(1 + \sum_{p'=1}^{p} (\Pi_p c)^{p'})$. On vérifie que $(1-a)(1-a)^{-1} = (1-a)^{-1}(1-a) = 1$ et que $(1-a)b = 1$ ou $b(1-a) = 1$ entraînent $b = (1-a)^{-1}$.

On note $R_X(\Omega)$ la plus petite sous-algèbre de $\bar{A}_X(\Omega)$ qui contienne $A_X(\Omega)$ et qui soit telle que $r \in R_X(\Omega)$ entraîne $(1 + \Pi_0 r - r)^{-1} \in R_X(\Omega)$. On a la propriété suivante.

PROPRIÉTÉ 1. - Une condition nécessaire et suffisante pour que $r \in R_X(\Omega)$ est qu'il existe un homomorphisme γ_r de F_X dans Ω_n $(n < \infty)$ tel que

$$r = \Pi_0 r + \sum_{f \in F_X,\, f \neq e_{F_X}} f(\gamma_r f)_{1,n}$$

où $(\gamma_r f)_{1,n}$ désigne l'élément à l'intersection de la première ligne et de la n-ième colonne de la matrice $(\gamma_r f)$.

La condition est nécessaire. Ceci est évident quand $r \in A_X(\Omega)$. Supposons que le résultat soit vrai pour r et que $\Pi_0 r = 0$; si $s = (1-r)^{-1}$, on obtient γ_s comme l'homomorphisme prolongeant les applications $\gamma_s x$ $(x \in X)$ où $(\gamma_s x)$ est la $n \times n$ matrice, somme de $(\gamma_r x)$ et d'une matrice dont toutes les colonnes sont nulles sauf la première qui est égale à la n-ième colonne de $(\gamma_r x)$.

De la même manière, si $\gamma_r : F_X \to \Omega_n$; $\gamma_{r'} : F_X \to \Omega_{n'}$, $\Pi_0 r = \Pi_0 r' = 0$; $s = r\omega + r'\omega'$; $(\omega, \omega' \in \Omega)$; $t = rr'$, on obtient $\gamma_s : F_X \to \Omega_{n+n'+2}$ et $\gamma_t : F_X \to \Omega_{n+n'+1}$ en prolongeant les applications.

$$(\gamma_s x) = \begin{pmatrix} 0 & (\gamma_r x)_1 & (\gamma_{r'} x)_1 & \alpha \\ 0 & (\gamma_r x) & 0 & (\gamma_r x)^n \omega \\ 0 & 0 & (\gamma_{r'} x) & (\gamma_{r'} x)^{n'} \omega' \\ 0 & 0 & 0 & 0 \end{pmatrix} ; \quad (\gamma_t x) = \begin{pmatrix} (\gamma_r x) & (\gamma_r x)^n & 0 \\ 0 & 0 & (\gamma_{r'} x)_1 \\ 0 & 0 & (\gamma_{r'} x) \end{pmatrix}$$

(où les notations $(\ )_1$ et $(\ )^n$ (ou $(\ )^{n'}$) désignent respectivement la première ligne, la n-ième (ou la n'-ième) colonne de la matrice correspondante

3-03

La condition est suffisante. Soit U une $n \times n$ matrice (u_{ij}) dont les éléments sont n_2 indéterminés ; U' la matrice obtenue en supprimant la n-ième ligne et la n-ième colonne de U ;

$$W = I_n + \sum_{p>0} U^p \; ; \quad W' = I_{n-1} + \sum_{p>0} U'^p \quad .$$

On a : $w_{n,n} = (1 - u_{n,n} - \sum_{j,j'<n} u_{n,j}\, w'_{j,j'}\, u_{j',n})^{-1}$ et pour tout i , $i' < n$

$$w_{i,n} = (\sum_{j<n} w'_{i,j}\, u_{j,n})\, w_{n,n} \; ; \quad w_{n,i'} = w_{n,n}(\sum_{j'<n} u_{n,j'}\, w_{j',i'})$$

$$w_{i,i'} = w'_{i,i'} + w_{i,n}(w_{n,n})^{-1} w_{n,i'} \quad .$$

Tous les calculs étant effectués dans $R_{\{u_{i,j}\}}(\Omega)$.

Il en résulte immédiatement que si $U \in R_{\{u_{i,j}\}}$, chacune des entrées $(U)_{i,i'}$ de U appartient à R_Ω. Par conséquent, $1 + \sum_{f \in F_X, f \neq \ell_{F_X}} f(\gamma_r f)_{1,n}$ étant égal à $((1 - \sum_{x \in X} x(\gamma_r x)^{-1})_{1,n}$ appartient à $R_X(\Omega)$.

REMARQUE. - Soit R_X^{pos} le sous-ensemble de $\bar{A}_X(\mathcal{Z})$ défini à partir de X par les seules opérations d'addition, de multiplication et de l'opération $r \longrightarrow (1 - r)^{-1} - 1$ quand $r \in R_X^{pos}$, $\pi_0\, r = 0$. En utilisant l'identité : $(1 - a + b)^{-1} = (1 - a - b(1 - a)^{-1}\, b)^{-1}\, (1 - b(1 - a)^{-1})$ on vérifie que tout $s \in R_X(\mathcal{Z})$ peut être écrit sous la forme $s = r - r'$ avec r , $r' \in R_X^{pos}$. Par construction, si $r \in R_X^{pos}$, toutes les matrices $\gamma_r f$ $(f \in F_X)$ ont leurs entrées non négatives ; il existe donc un monoïde quotient fini $\varphi_r F_X$ tel que $(\gamma_r f)_{1,n} \neq 0$ si et seulement si $\varphi_r f$ appartient à un certain sous-ensemble de $\varphi_r F_X$.

II. - Soit $Y = X \cup U$ où $U = \{u_j\}_{j=1,2,\ldots,m}$.

Soient r_1 , r_2 , ... , $r_m \in R_Y(\Omega)$ tel que

$$r_1 = r_2 = \ldots = r_m = 0 \quad \text{quand} \quad x_1 = x_2 = \ldots = x_n = 0$$

et

$$r_1\, r_2 \ldots r_m \neq 0 \quad \text{quand} \quad u_1 = u_2 = \ldots = u_m = 0 \quad .$$

Dans ces conditions, si θ' est une application de U dans $\bar{A}_X(\Omega)$ telle que $\pi_0\, \theta' u = 0$, θ'_n l'application $\pi_n \circ \theta$ et θ et θ_n les homomorphismes $\bar{A}_Y(\Omega) \longrightarrow \bar{A}_X(\Omega)$ qui les prolongent, on a, pour tout n et $n' \geq n$,

u_j en les x peuvent donc être "résolues" en calculant par des opérations rationnelles les coefficients successifs $\Pi_p u_j$ et l'on dira que chacune de ces séries est un "élément algébrique" de $\bar{A}_X(\Omega)$. On désignera par $S_X(\Omega)$ la plus petite sous-algèbre de $\bar{A}_X(\Omega)$ qui contienne tous les éléments algébriques et qui soit telle que $s \in S_X(\Omega)$ entraîne $(1 + \Pi_0 s - s)^{-1} \in S_X(\Omega)$.

III. - Soit $\varphi : F_X \longrightarrow G$ un homomorphisme de F_X dans un monoïde fini et $\beta_1 : (G , X) \longrightarrow Z$ une application quelconque.

On prolonge β_1 en un "coset mapping" $\beta : (G , F_X) \longrightarrow Z$ en posant $\beta(g ; 0_{F_X}) = 0$ et inductivement

$$\beta(g ; fx) = \beta(g ; f) + \beta_1(g\varphi f ; x) \quad .$$

Les définitions précédentes déterminent sur (F_X , Z) une structure de monoïde avec $(f , a)(f' , a') = (ff' , a + \beta(\varphi f ; f') + a')$; $(f ; a) \equiv f' ; a')$ et seulement si $\varphi f = \varphi f'$ et $a = a'$.

Soit $h^+ = \sup \beta_1(g ; x)$; $h^- = \inf \beta_1(g , x)$ $(g \in G , x \in X)$, et pour tout $g , g' \in G$; $0 \leqslant a , b \leqslant h^+$ les éléments suivants de $\bar{A}_X(Z)$

$$B^+_{g,g'} = \sum \left\{ f : f \in F_X ; g\varphi f = g' ; \beta(g , f) = 0 ; \beta(g ; f') \geqslant 0 \right\}$$
pour tous les facteurs à gauche propres f' de f

$$A^+_{g,g'}(a , b) = \sum \left\{ f : f \in F_X ; g\varphi f = g' ; a + \beta(g , f) = b ; a + \beta(g , f') > 0 \right\}$$
pour tous les facteurs à gauche propres f' de f

On a les équations $(c = \inf(a , b))$

$$(1) \quad A^+_{g,g'}(a , b) = \sum_{0<a'<c} \sum_{g'',g'''} A^+_{g,g''}(a - a' , 0)\, B^+_{g'',g'''}\, A^+_{g''',g'}(0 , b - a') + \begin{cases} A^+_{g,g'}(0 , b - a) \text{ ou } A^+_{g,g'}(a - b , 0) \\ \text{selon que } b \gtrless 0 \text{ ou non.} \end{cases}$$

$$(2) \quad A^+_{g,g'}(0 , a) = \sum'_{x \in X^+_g} x\, A_{g\varphi x,g'}(\beta(g , x) , a)$$

où $X^+_g = \{x : x \in X ; \beta_1(g , x) > 0\}$.

$$(2)' \quad A^+_{g,g'}(a , 0) = \sum A_{g,g''}(a , b)\, x$$

où cette sommation est étendue à tous les triples $b \in Z$, $x \in X$, $y'' \in G$ tels que $-\beta_1(g'' , x) = b > 0$, $g''\varphi x = g'$.

3-05

d'indice est en correspondance biunivoque avec G et qui sont telles que $(B^+)_{g,g'} = B^+_{g,g'}$; $(A^+)_{g,g'} = A^+_{g,g'}(0\ ,\ 0)$; on a évidemment :

$$(B^+) = (I - (A^+))^{-1} \qquad (3)$$

Éliminant les $A^+_{g,g'}(a\ ,\ b)$ $(ab \neq 0)$ au moyen de (1), il résulte de (2), (2)' et (3) que les $A^+_{g,g'}(0\ ,\ b)$, les $A^+_{g,g'}(a\ ,\ 0)$, les $B^+_{g,g'}$ et finalement les $A^+_{g,g'}(a\ ,\ b)$ appartiennent tous à $S_X(Z)$.

Ceci naturellement vaudrait aussi bien pour les éléments $A^-_{g,g}(a\ ,\ b)$ $(h^- \leqslant a\ ,\ b \leqslant 0)$ ou $B^-_{g,g'}$ définis de façon symétrique.

Soit enfin $K = \{k\}$ un ensemble en correspondance biunivoque avec les paires $(g\ ,\ c)$, $g \in G$; $h^- \leqslant c \leqslant h^+$. On considère les $K \times K$ matrices (X) et (A) avec

$(X)_{k,k'} = x \in X$ si $k = (g\ ,\ c)$; $k' = (g'\ ,\ c')$ et $g\varphi x = g'$;
$cc' \leqslant 0$; $c \neq 0$; $c + \beta_1(g\ ,\ x) = c'$
$= 0$, autrement.

$(A)_{k,k'} = A^+_{g,g'}(a\ ,\ b)$ si $k = (g\ ,\ a)$; $k' = (g'\ ,\ b)$; $0 \leqslant a\ ,\ b \leqslant h^+$;
$= A^-_{g,g'}(a\ ,\ b)$ si $k = (g\ ,\ a)$: $k' = (g'\ ,\ b)$; $h^- \leqslant a\ ,\ b \leqslant 0$;
$= 0$ autrement.

Finalement si $(B) = (I - (A)(X))^{-1}$ tous les éléments de (B) appartiennent à $S_X(Z)$.

En particulier, ceci est vrai des sommes $B_{g'c} = \sum \{f \in F_X : \varphi f = g'\ ;\ \beta(e_{F_X}\ ,\ f) = c\}$ qui correspondent par construction à $k = (e_{F_X}\ ,\ 0)$; $k' = (g'\ ,\ c)$

REMARQUE. - Le résultat ne se généralise pas au cas où β serait un "coset mapping" de G, fini, dans un groupe abélien de dimension $\geqslant 2$ et où l'on chercherait la somme

$$\sum \{f : \varphi f = g\ ;\ \beta(e_{F_X}\ ,\ f) = 0\}$$

Considérons en effet le cas où φ est trivial ($\varphi f = e_G$ pour tout f) et où, X étant égal à $\{x_1\ ,\ x_2\ ,\ x_3\}$, on a :

$$\beta(x_1) = (0\ ,\ 1)\ ;\ \beta(x_2) = (1\ ,\ 0);\ \beta(x_3) = (-1\ ,\ -1) \quad .$$

Dans ce cas, si α désigne l'homomorphisme de $\bar{A}_X$ dans l'algèbre des séries formelles en les variables commutatives t_1, t_2 et t_3, on a :

3-06

$$\alpha_s = \alpha \Sigma \{ f : \beta(f) = 0 \} = (4\pi)^{-2} \int_0^{2\pi} \int_0^{2\pi} (1 - t_1 \exp iu - t_2 \exp iv - t_3 \exp -i(u+v))^{-1} \, du \, dv \quad ;$$

$$= 1 + \sum_{p>0} (3p)! \, (p!)^{-3} \, (t_1 \, t_2 \, t_3)^p \quad .$$

Quand $t_1 = t_2 = t_3 = 1/3 \, t$, cette fonction a, pour $t \longrightarrow 1$, une singularité non algébrique puisque

$$\frac{(3n)!}{(n!)^3 3^{3n}} \sim \frac{1}{2\pi n} \quad .$$

Donc, a fortiori, $s \notin S_X(Z)$.

BIBLIOGRAPHIE.

[1] KLEENE (S. C.). - Representation of events in nerve nets and finite automata, Automata studies, p. 3-41. - Princeton, Princeton University Press, 1956 (Annals of mathematical Studies, 34).

[2] RABIN (M. O.) and SCOTT (D.). - Finite automata and their decision problems, IBM Research J., t. 3, 1959, p. 114-117.

Table des matières

Tome IV

Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par Jean Berstel, Alain Lascoux et Dominique Perrin

Les treize tomes de cette édition contiennent l'ensemble des œuvres de Marcel-Paul Schützenberger qui ont fait l'objet d'une publication dans une revue scientifique ou un livre. Ses travaux couvrent une période de plus de 50 ans, depuis sa première note aux Comptes Rendus en 1943 jusqu'à son dernier article, paru en 1997.
Les publications sont présentées dans l'ordre chronologique. Chaque tome est précédé d'une courte introduction qui essaie d'éclairer certains des travaux, tant pour leur intérêt scientifique intrinsèque que pour l'écho qu'ils ont rencontré et les développements qu'ils ont suscités.

Tome 4 : 1956 – 1960

Durant cette période, Schützenberger publie une première série d'articles sur la théorie algébrique des codes et les monoides. L'article « Une théorie algébrique du codage » est un texte fondateur, exposé au séminaire d'algèbre de Paul Dubreil et suivi d'une publication comme note aux Comptes-Rendus. Il contient la présentation de la problématique du codage en termes algébriques et, notamment le fait que la propriété de décodage unique équivaut à celle d'une base d'un sous-monoïde libre. Une version en anglais est présentée à un colloque IRE au MIT « On the application of semigroup methods to some problems in coding ».
Une série de notes aux Comptes-Rendus traite de la structure de semigroupes, et contient la définition de ce que Clifford et Preston nommeront dans leur livre le « groupe de Schützenberger » d'une $\mathcal{H}$-classe et les « représentations de Schützenberger » relatives à une $\mathcal{D}$-classe.
L'article « Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées » est la première présentation des liens entre bases des algèbres de Lie libres, factorisations des monoïdes libres et codes comma-free.