Énumération des fonctions booléennes 1-résilientes

Jean-Marie Le Bars

GREYC, Université de Caen

Alfredo Viola

Université de la República, Uruguay

Rencontres Aléa 2007 19-23 mars 2007, CIRM, Luminy

Plan de l’exposé

Construction récursive des fonctions booléennes

Construction des classes

Énumération et dénombrement

Algorithmes

Bornes inférieures et supérieures

Perspectives

Plan de l’exposé

Construction récursive des fonctions booléennes

Construction des classes

Énumération et dénombrement

Algorithmes

Bornes inférieures et supérieures

Perspectives

Définition d'une fonction booléenne

- une application $f_n : \{0,1\}^n \to \{0,1\}$.
- un mot $b_0 \dots b_{2^n-1}$

$$f_n(x_1, \dots, x_n) = b_k, \text{ avec } k = \sum_{i=1}^{n} x_i \, 2^{i-1}.$$

Poids de Hamming : Nombre de 1 dans le mot $b_0 \dots b_{2^n-1}$.

Nombre de fonctions booléennes à n variables : 2^{2^n}.

Pour $n = 8$, $2^{2^8} = 10^{77}$
Nombre d'atomes dans l'univers 10^{80}

Fonctions sans corrélation d'ordre 1

Définitions

1. Une fonction f_n de poids de Hamming $2m$ est sans corrélation d'ordre 1 lorsque pour toute variable x_i

   $f_n|_{x_i=0}$ et $f_n|_{x_i=1}$ sont de poids de Hamming m.

2. Une fonction f_n est équilibrée lorsqu'elle est de poids 2^{n-1} (autant de 1 que de 0)

3. Une fonction f_n est 1-résiliente lorsqu'elle est sans corrélation d'ordre 1 et équilibrée

Nombre de fonctions 1-résilientes

n	Fonctions booléennes	Fonctions 1-résilientes
2	16	2
3	256	8
4	65536	222
5	4294967296	807980
6	$1.84\ 10^{19}$	95259103924394
7	$3.40\ 10^{38}$	?
8	$1.15\ 10^{77}$	?

Motivations pour l'étude des fonctions 1-résilientes

- Cryptographie symétrique :
  primives cryptographiques utilisées en chiffrement à flot ou par blocs

- Théorie de l'information :
  quelle quantité d'information est nécessaire pour capturer la classe de ces fonctions

Concaténation de deux fonctions booléennes

Soient f^1_{n-1} et f^2_{n-1} deux fonctions booléennes à $n-1$ variables.
On construit une fonction booléenne à n variables f_n

$$\begin{aligned} f_n(x_1,\ldots,x_n) &= f^1_{n-1}(x_1,\ldots,x_{n-1}) \text{ lorsque } x_n = 0 \\ &= f^2_{n-1}(x_1,\ldots,x_{n-1}) \text{ lorsque } x_n = 1 \end{aligned}$$

$$\left\{ \begin{array}{l} f^1_{n-1} = b^1_0 \ldots b^1_{2^{n-1}-1} \\ f^2_{n-1} = b^2_0 \ldots b^2_{2^{n-1}-1} \end{array} \right. \Longrightarrow f_n = b^1_0 \ldots b^1_{2^{n-1}-1} b^2_0 \ldots b^2_{2^{n-1}-1}$$

La concaténation sera notée $\star$

$$f_n = f^1_{n-1} \star f^2_{n-1}.$$

Exemple

On considère la fonction booléenne à trois variables suivante :

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Exemple

On considère la fonction booléenne à trois variables suivante :

f_2^1

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Exemple

On considère la fonction booléenne à trois variables suivante :

					f_2^2			
f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Exemple

On considère la fonction booléenne à trois variables suivante :

$$f_1^1$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Exemple

On considère la fonction booléenne à trois variables suivante :

$$f_1^2$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Exemple

On considère la fonction booléenne à trois variables suivante :

f_1^3

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Exemple

On considère la fonction booléenne à trois variables suivante :

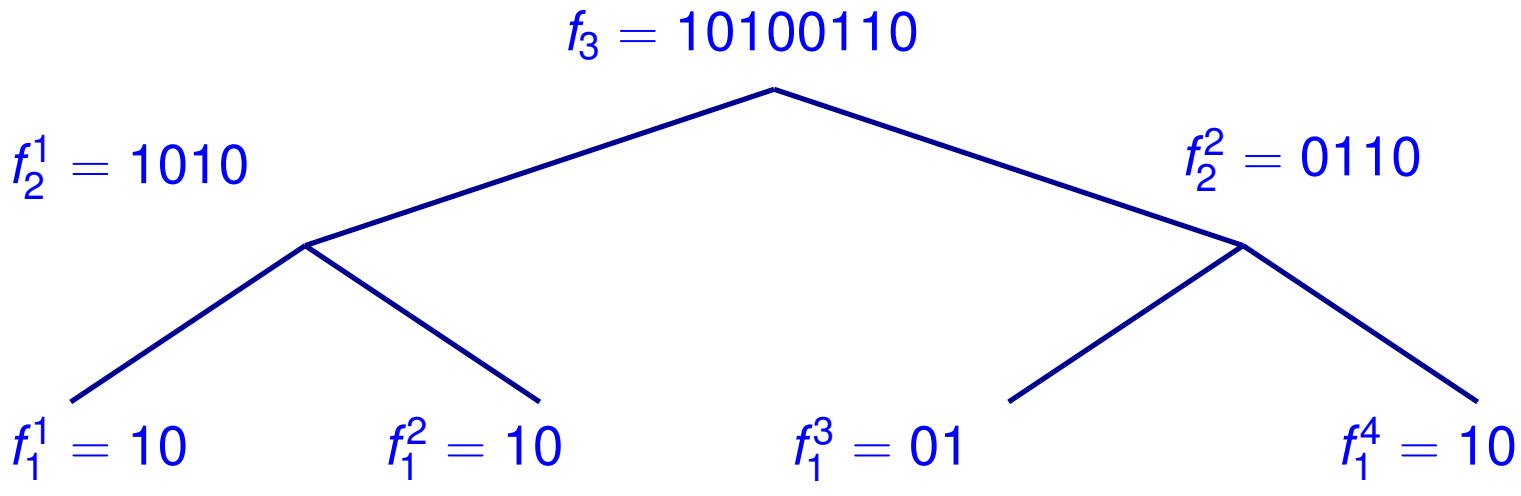
f_1^4

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Arbre de décomposition de f_3

$$f_3 = f_2^1 \star f_2^2$$

$$f_2^1 = f_1^1 \star f_1^2 \qquad f_2^2 = f_1^3 \star f_1^4$$



Construction d'une classe

Pour tout $i = 1 \ldots n$, on considère les différences de poids de Hamming

$$w_H(f_3 \mid_{x_i=0}) - w_H(f_3 \mid_{x_i=1})$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Poids de Hamming : 4

$\Omega(f_3) = \langle 4, \quad , \quad , \quad \rangle$

Construction d'une classe

Pour tout $i = 1 \ldots n$, on considère les différences de poids de Hamming

$$w_H(f_3 \mid_{x_i=0}) - w_H(f_3 \mid_{x_i=1})$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Poids de Hamming : 2

$\Omega(f_3) = \langle 4, \quad , \quad , \quad \rangle$

Construction d'une classe

Pour tout $i = 1 \ldots n$, on considère les différences de poids de Hamming

$$w_H(f_3 \mid_{x_i=0}) - w_H(f_3 \mid_{x_i=1})$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Poids de Hamming : 2

$\Omega(f_3) = \langle 4, 0, \quad , \quad \rangle$

Construction d'une classe

Pour tout $i = 1 \ldots n$, on considère les différences de poids de Hamming

$$w_H(f_3 \mid_{x_i=0}) - w_H(f_3 \mid_{x_i=1})$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Poids de Hamming : 2

$\Omega(f_3) = \langle 4, 0, \quad , \quad \rangle$

Construction d'une classe

Pour tout $i = 1 \ldots n$, on considère les différences de poids de Hamming

$$w_H(f_3 \mid_{x_i=0}) - w_H(f_3 \mid_{x_i=1})$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Poids de Hamming : 2

$\Omega(f_3) = \langle 4, 0, 0, \quad \rangle$

Construction d'une classe

Pour tout $i = 1 \ldots n$, on considère les différences de poids de Hamming

$$w_H(f_3 \mid_{x_i=0}) - w_H(f_3 \mid_{x_i=1})$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Poids de Hamming : 3 $\Omega(f_3) = \langle 4, 0, 0, \quad \rangle$

Construction d'une classe

Pour tout $i = 1 \ldots n$, on considère les différences de poids de Hamming

$$w_H(f_3 \mid_{x_i=0}) - w_H(f_3 \mid_{x_i=1})$$

f_3	1	0	1	0	0	1	1	0
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1

Poids de Hamming : 1 $\Omega(f_3) = \langle 4, 0, 0, 2 \rangle$

Codage d'une classe

f_n appartient à la classe

$$\omega = \langle m, \alpha_n, \ldots, \alpha_1 \rangle$$

lorsque :

f_n est de poids m

Codage d'une classe

f_n appartient à la classe

$$\omega = \langle m, \alpha_n, \ldots, \alpha_1 \rangle$$

lorsque :

- $m = w_H(f_n)$ f_n est de poids m

Codage d'une classe

f_n appartient à la classe

$$\omega = \langle m, \alpha_n, \ldots, \alpha_1 \rangle$$

lorsque :

- $m = w_H(f_n)$ f_n est de poids m
- $\alpha_i = w_H(f_n\,|_{x_i=0}) - w_H(f_n\,|_{x_i=1})$, pour $i = 1 \ldots n$

Classes des fonctions sans corrélation d'ordre 1

Une fonction f_n de poids de Hamming $2m$ est sans corrélation d'ordre 1 lorsque pour toute variable x_i

$f_n\,|_{x_i=0}$ et $f_n\,|_{x_i=1}$ sont de poids de Hamming m.

Conséquence

Toutes ces fonctions appartiennent à la classe

$$\langle 2m, 0, \ldots, 0 \rangle.$$

Cette classe sera notée Cor_n^m

Classe des fonctions 1-résilientes

Une fonction f_n est 1-résiliente lorsque :

- f_n est sans corrélation d'ordre 1
- f_n est équilibrée (de poids 2^{n-1})

Conséquence

Les fonctions 1-résilientes appartiennent à la classe

$$Res_n^1 = \langle 2^{n-1}, 0, \ldots, 0 \rangle.$$

Ω_1 ensemble des classes à 1 variable

f_1	$\omega(f_1)$
00	$\langle 0, 0 \rangle$
01	$\langle 1, -1 \rangle$
10	$\langle 1, 0 \rangle$
11	$\langle 2, 0 \rangle$

Remarque

Chaque classe contient exactement 1 fonction booléenne

Ω_2 ensemble des classes à deux variables

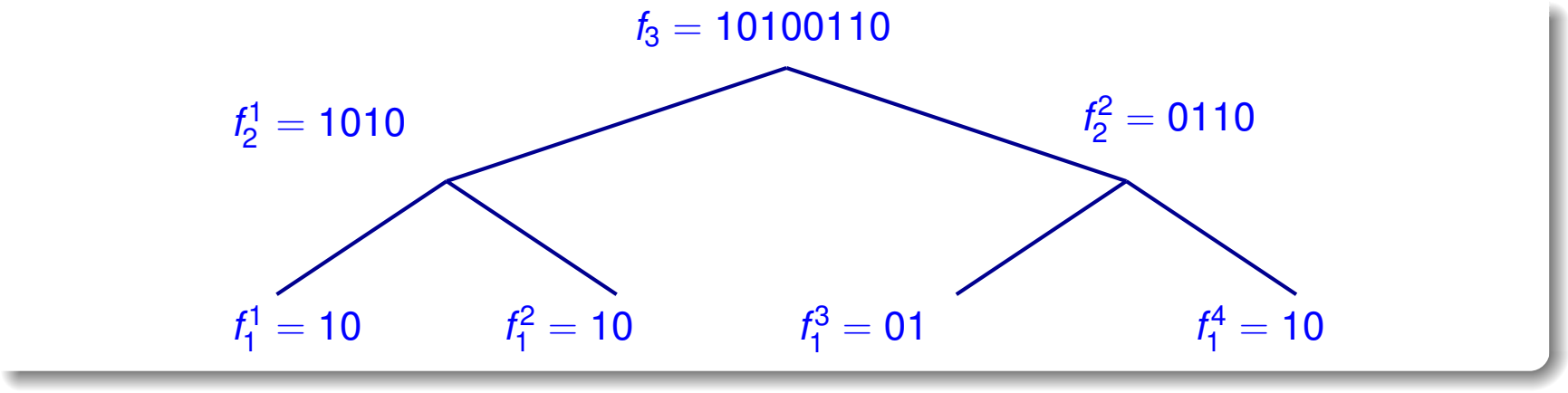
f_2	$\Omega(f_2)$	f_2	$\Omega(f_2)$
0000	$\langle 0,0,0\rangle$	1001	$\langle 2,0,0\rangle$
0001	$\langle 1,-1,1\rangle$	1010	$\langle 2,0,2\rangle$
0010	$\langle 1,-1,1\rangle$	1100	$\langle 2,2,0\rangle$
0100	$\langle 1,1,-1\rangle$	0111	$\langle 3,-1,-1\rangle$
1000	$\langle 1,1,1\rangle$	1011	$\langle 3,-1,1\rangle$
0011	$\langle 2,-2,0\rangle$	1101	$\langle 3,1,-1\rangle$
0101	$\langle 2,0,-2\rangle$	1110	$\langle 3,1,1\rangle$
0110	$\langle 2,0,0\rangle$	1111	$\langle 4,0\mathit{ill},0\rangle$

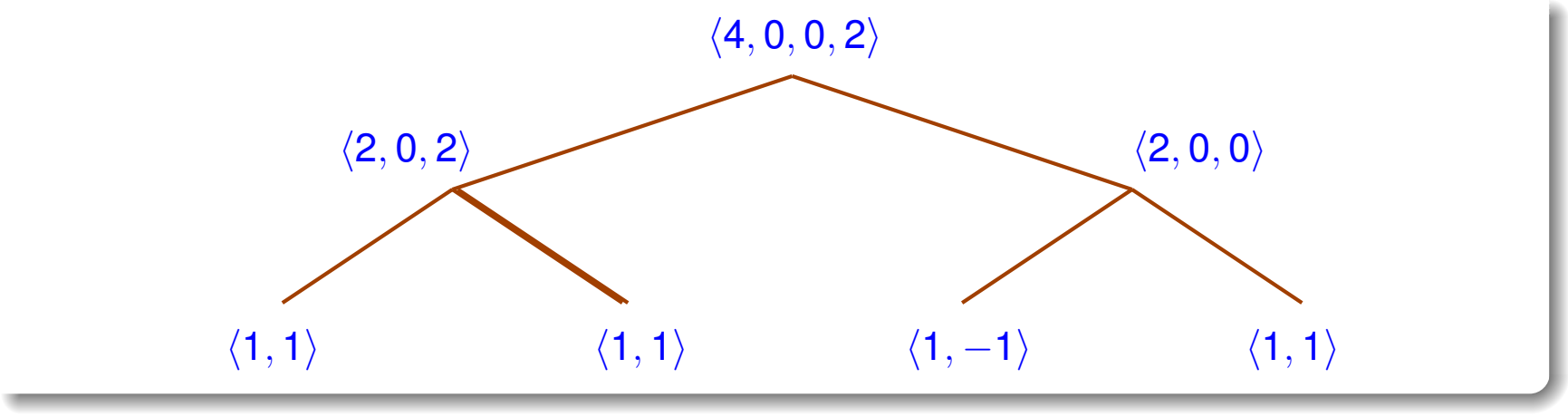
Ω_2 ensemble des classes à deux variables

f_2	$\Omega(f_2)$	f_2	$\Omega(f_2)$
0000	$\langle 0,0,0\rangle$	1001	$\langle 2,0,0\rangle$
0001	$\langle 1,-1,1\rangle$	1010	$\langle 2,0,2\rangle$
0010	$\langle 1,-1,1\rangle$	1100	$\langle 2,2,0\rangle$
0100	$\langle 1,1,-1\rangle$	0111	$\langle 3,-1,-1\rangle$
1000	$\langle 1,1,1\rangle$	1011	$\langle 3,-1,1\rangle$
0011	$\langle 2,-2,0\rangle$	1101	$\langle 3,1,-1\rangle$
0101	$\langle 2,0,-2\rangle$	1110	$\langle 3,1,1\rangle$
0110	$\langle 2,0,0\rangle$	1111	$\langle 4,0\mathit{ill},0\rangle$

Seule la classe des fonctions 1-résilientes contient deux fonctions

Arbre de décomposition sur les classes





Opérateur $\star$ sur les classes

Exemple précédent

$$\langle 2, 0, 0\rangle \star \langle 2, 0, 2\rangle = \langle 4, 0, 0, 2\rangle$$

Cas général

$$\langle p, \beta_n, \ldots, \beta_1\rangle \star \langle q, \gamma_n, \ldots, \gamma_1\rangle = \langle m, \alpha_n, \ldots, \alpha_1\rangle$$

Opérateur $\star$ sur les classes

Exemple précédent

$$\langle 2, 0, 0\rangle \star \langle 2, 0, 2\rangle = \langle 4, 0, 0, 2\rangle$$

Cas général

$$\langle p, \beta_n, \ldots, \beta_1\rangle \star \langle q, \gamma_n, \ldots, \gamma_1\rangle = \langle m, \alpha_n, \ldots, \alpha_1\rangle$$

- $p + q = m$

Opérateur $\star$ sur les classes

Exemple précédent

$$\langle 2, 0, 0\rangle \star \langle 2, 0, 2\rangle = \langle 4, 0, 0, 2\rangle$$

Cas général

$$\langle p, \beta_n, \ldots, \beta_1\rangle \star \langle q, \gamma_n, \ldots, \gamma_1\rangle = \langle m, \alpha_n, \ldots, \alpha_1\rangle$$

- $p + q = m$
- $\alpha_n = \beta_{n-1} - \gamma_{n-1}$

Opérateur $\star$ sur les classes

Exemple précédent

$$\langle 2, 0, 0\rangle \star \langle 2, 0, 2\rangle = \langle 4, 0, 0, 2\rangle$$

Cas général

$$\langle p, \beta_n, \ldots, \beta_1\rangle \star \langle q, \gamma_n, \ldots, \gamma_1\rangle = \langle m, \alpha_n, \ldots, \alpha_1\rangle$$

- $p + q = m$
- $\alpha_n = \beta_{n-1} - \gamma_{n-1}$
- $\alpha_i = \beta_i + \gamma_i$, pour $i = 1 \ldots n - 1$

Plan de l’exposé

Construction récursive des fonctions booléennes

Construction des classes

Énumération et dénombrement

Algorithmes

Bornes inférieures et supérieures

Perspectives

Énumération des fonctions d'une classe

- Ω_n : ensemble des classes à n variables.
- Ω_n^m : ensemble des classes à n variables de poids m.

Théorème (Énumération)

Soit $\omega \in \Omega_n^m$.

$$\omega = \bigcup_{\omega_1 \star \omega_2 = \omega} \omega_1 \times \omega_2,$$

où $\omega_1 \times \omega_2 = \{f_n \mid f_n = f_{n-1}^1 \star f_{n-1}^2, f_{n-1}^1 \in \omega_1 \text{ et } f_{n-1}^2 \in \omega_2\}$.

Calcul de la cardinalité d'une classe

Corrolaire (Dénombrement)

Soit $\omega \in \Omega_n^m$.

$$card(\omega) = \sum_{\omega_1 \star \omega_2 = \omega} card(\omega_1) \times card(\omega_2).$$

Classe miroir

Soit $\omega = \langle m, \alpha_n, \ldots, \alpha_1 \rangle$ la classe de Ω_n^m.

La classe miroir de ω est

$$\overline{\omega} = \langle m, -\alpha_n, \ldots, -\alpha_1 \rangle.$$

On passe de $f_n \in \omega$ à $\overline{f_n} \in \overline{\omega}$ avec

$$\overline{f_n}(x_1, \ldots, x_n) = f_n(1 - x_1, \ldots, 1 - x_n).$$

La classe miroir vérifie

$$\omega \star \overline{\omega} = Cor_n^m.$$

Énumération des fonctions sans corrélation d'ordre 1

Soit Cor_n^m la classe sans corrélation d'ordre 1 à n variables de poids $2m$.

- **Énumération de Cor_n^m**

$$Cor_n^m = \bigcup_{\omega_1 \in \Omega_{n-1}^m} \omega_1 \times \overline{\omega_1}.$$

- **Cardinalité de Cor_n^m**

$$card(Cor_n^m) = \sum_{\omega_1 \in \Omega_{n-1}^m} card(\omega_1)^2.$$

Plan de l’exposé

Construction récursive des fonctions booléennes

Construction des classes

Énumération et dénombrement

Algorithmes

Bornes inférieures et supérieures

Perspectives

Algorithme 1 – Programme Maple

$$x_0^m\, x_1^{\alpha_1} \ldots x_n^{\alpha_n} \iff \omega = \langle m, \alpha_n, \ldots, \alpha_1 \rangle$$

On définit les séries génératrices suivantes :

- $\varphi(0) = 1 + x_0$
- $\varphi(n) = [x_0 \to x_0 * x_n]\, \varphi(n-1) * [\, x_0 \to x_0/x_n]\, \varphi(n-1)$

$[x_0 \to y]\, \varphi(n-1)$: chaque occurrence de x_0 est remplacée par y.

$$Res_n^1 = [x_0^{2^{n-1}} x_n^0 \ldots x_1^0\,]\varphi(n).$$

Algorithme 1 – Programme Maple

```
f := proc(n) options remember;
if n = 0 then (1 + x[0])
else subs(x[0] = x[0] * x[n], f(n − 1)) * subs(x[0] = x[0]/x[n], f(n − 1))
fi end;
f := proc(n) option remember;
if n = 0 then 1 + x[0]
else subs(x[0] = x[0] * x[n], f(n − 1)) * subs(x[0]y = x[0]/x[n], f(n − 1))
end if end proc
g := proc(n) options remember;
subs(x[0] = x[0] * x[n], f(n − 1)) end;

convert(map(x− > x * x, [coeffs(coeff(expand(collect(g(n), x[0])), x[0], 2^(n − 2)))]), ' + ');
```

n	5	6
Temps de calcul	0.1s	1 h 33 mn

Algorithme 2 – Réduction du nombre de classes

Propriété

$$|\langle m, \alpha_n, \ldots, \alpha_1 \rangle| \quad = \quad |\langle m, |\alpha_n|, \ldots, |\alpha_1| \rangle|$$

Preuve.

$$\begin{array}{c|c|c} x_i = 0 & \longleftrightarrow & x_i = 1 \\ \alpha_i & & -\alpha_i \end{array}$$

$\Longrightarrow$ *On ne calcule que les cardinalités des classes* $\langle m, \alpha_n, \ldots, \alpha_1 \rangle$, *avec* $\alpha_i \geq 0$.

Algorithme 2 – Réduction du nombre de classes

n	5	6
Res_n^1	807980	95259103924394
Temps de calcul	0.032 s	0.380 s

n	7
Res_n^1	2347801575478885443949762268929 6
Temps de calcul	25 mn 49 s

Algorithme 3 – Classes normalisées

Definition

Une classe normalisée vérifie
$\langle m, \alpha_n, \ldots, \alpha_1 \rangle$, avec $0 \leq \alpha_n \leq \alpha_{n-1} \leq \ldots \leq \alpha_1$.

Propriété

Pour toute permutation σ *de* $\{1, \ldots, n\}$,

$$card(\langle m, \alpha_n, \ldots, \alpha_1 \rangle) = card(\langle m, \alpha_{\sigma(n)}, \ldots, \alpha_{\sigma(1)} \rangle)$$

Preuve.

$$\begin{array}{c|c|c} x_i & & x_j \\ \alpha_i & \longleftrightarrow & \alpha_j \end{array}$$

$\Longrightarrow$ *On ne calcule que les cardinalités des classes normalisées*

Algorithme 3 – Classes normalisées

n	5	6	7	8
Res_n^1	807980	$9.52\ 10^{13}$	$2.34\ 10^{31}$	$4.05\ 10^{67}$
Temps de calcul	0.086 s	0.104 s	50 s	1 j 14 h18 mn

Approximation : on ne calcule pas la cardinalité de toutes les classes

Plan de l’exposé

Construction récursive des fonctions booléennes

Construction des classes

Énumération et dénombrement

Algorithmes

Bornes inférieures et supérieures

Perspectives

Méthode utilisée jusqu'à présent

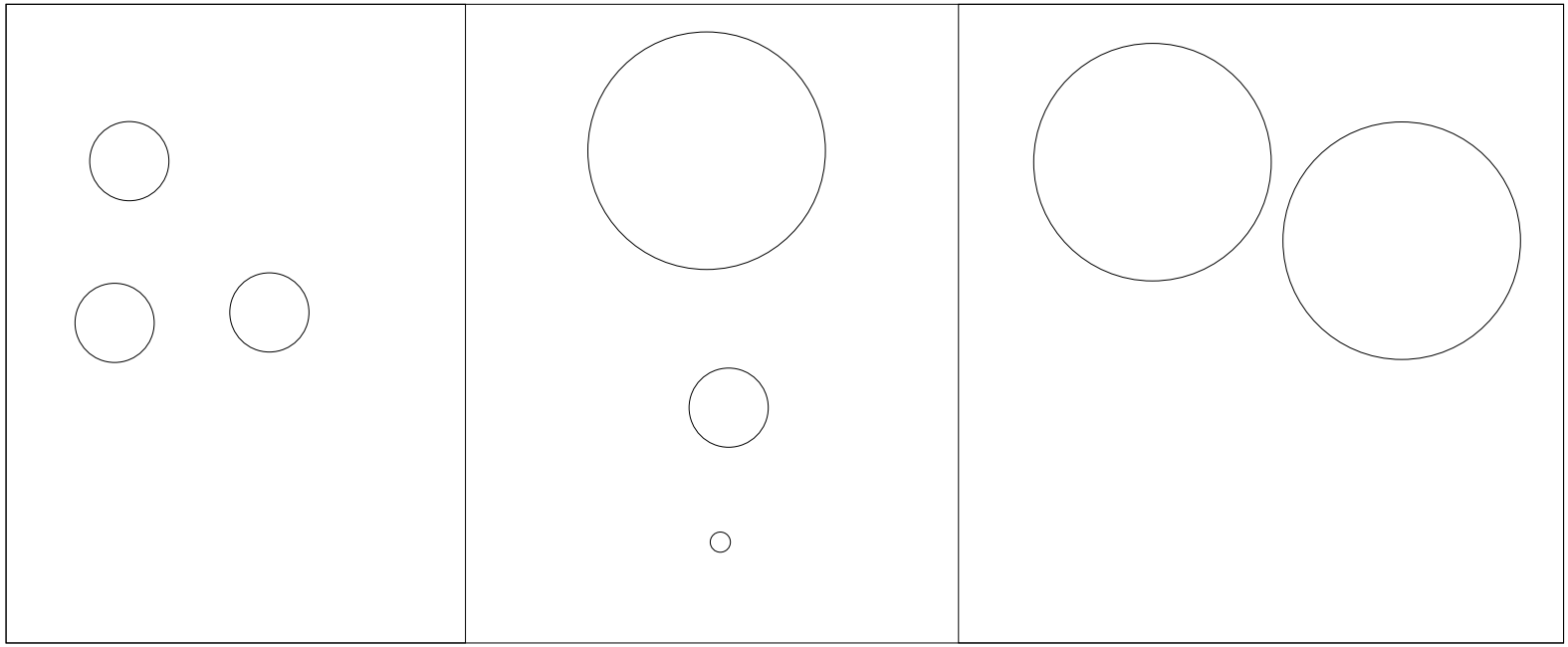
On veut calculer le nombre d'éléments d'une classe de fonction booléennes.

Bornes inférieures	Bornes supérieures
on compte moins de fonctions	on compte plus de fonctions
sous-classe	classe plus grande

Notre méthode

On fait varier la répartition des cardinalités des classes :

Borne inférieure Répartition réelle Borne supérieure



Borne inférieure déjà connue

Maitra et Sarkar (2000) : dénombrement des fonctions booléennes 1-résilientes connues.

$$\binom{2^{n-1}}{2^{n-2}} + 2^{2^{n-2}} + \binom{2^{n-2}}{2^{n-3}}\left(\binom{2^{n-2}}{2^{n-3}} - 2\right) - 2^{2^{n-3}} + \binom{2^{n-3}}{2^{n-4}}$$

Borne inférieure asymptotique :

$$\sqrt{\frac{2}{\pi}}\, 2^{-2^{n-2}}\, 2^{2^{n-1}}$$

Nouvelle borne inférieure

Nombre de fonctions 1-résilientes

Nombre de *variables*	Borne de Maitra et Sarkar	nouvelle borne
5	17876	128500
6	$7.66\ 10^{8}$	$1.468\ 10^{12}$
7	$2.19\ 10^{18}$	$4.625\ 10^{28}$
8	$2.73\ 10^{37}$	$2.597\ 10^{63}$
9	$6.34\ 10^{75}$	$3.445\ 10^{136}$
10	$5.05\ 10^{152}$	$5.107\ 10^{285}$

Ordre partiel

Definition

Soient $\omega_1 = \langle m, \alpha_n, \ldots, \alpha_1 \rangle$ et $\omega_2 = \langle m, \beta_n, \ldots, \beta_1 \rangle$

On a $\omega_1 \prec \omega_2$ lorsque

$$\begin{cases} \alpha_i \geq \beta_i, & \text{pour tout } i \\ \alpha_j > \beta_j, & \text{pour au moins un } j \end{cases}$$

Théorème

$$\omega \prec \omega' \implies |\omega| < |\omega'|.$$

Distance d'une fonction aux classes sans corrélation d'ordre 1

Soit $\omega = \langle m, \alpha_n, \ldots, \alpha_1 \rangle$ la classe d'une fonction f_n.

$$\delta(\omega) = \sum_{i=1}^{n} \alpha_i.$$

$\delta_{max}(n-1)$: δ maximum pour une fonction équilibrée à $n-1$ variables.

$$\delta_{max}(n-1) = \left\lceil \frac{n-1}{2} \right\rceil \binom{n-1}{\lceil \frac{n-1}{2} \rceil}.$$

Majoration du nombre de classes équilibrées

Notons $U(n-1)$ le nombre de classes équilibrées à $n-1$ variables.

$$U(n-1) \leq \binom{\delta_{max}(n-1)/2 + n - 1}{n-1} 2^{n-1}.$$

Nouvelle borne inférieure asymptotique

Le nombre de fonctions 1-résilientes est inférieure à

$$\frac{\binom{2^{n-1}}{2^{n-2}}^2}{U_{n-1}}.$$

On en déduit la borne inférieure asymptotique suivante :

$$BIA(n) = 2^{2^n - n^2 + \frac{\ln 2}{2}\, n \ln n + \Theta(n)}.$$

Nous avons l'encadrement suivant avec la borne supérieure de Schneider :

$$2^{-n^2} < \Pr(f_n \text{ est 1-résiliente }) < 2^{-\frac{n^2}{4}+\frac{n}{4}}$$

Comparaisons entre les bornes asymptotiques

n	8	9	10	11	12	13	14
$Maitra(n)$	10^{37}	10^{75}	10^{152}	10^{306}	10^{614}	10^{1231}	10^{2463}
$BIA(n)$	10^{63}	10^{136}	10^{288}	10^{588}	10^{1199}	10^{2426}	10^{4885}
$Sch(n)$	10^{71}	10^{147}	10^{299}	10^{606}	10^{1221}	10^{2452}	10^{4916}
$SchU(n)$	10^{72}	10^{148}	10^{301}	10^{608}	10^{1223}	10^{2454}	10^{4918}

Borne inférieure du nombre de fonctions k-résilientes

Soient $k \geq 2$ et $n > k$, une fonction f_n est k-résiliente si elle reste équilibrée lorsque l'on fixe k variables.

Notons $\mathcal{R}es_n^k$ la classe des fonctions k-résiliente.

À partir de toute fonction de $\mathcal{R}es_{n-k+1}^1$, on construit une fonction de $\mathcal{R}es_n^k$.

On obtient la première borne inférieure significative :

$$card(\mathcal{R}es_n^k) \geq card(\mathcal{R}es_{n-k+1}^1)).$$

Plan de l’exposé

Construction récursive des fonctions booléennes

Construction des classes

Énumération et dénombrement

Algorithmes

Bornes inférieures et supérieures

Perspectives

Perspectives

- Bornes inférieures et supérieures des fonctions k-résilientes
- Bornes asymptotiques par l'étude des séries génératrices
- Génération aléatoire dans une classe de fonctions booléennes
- Construction de fonctions booléennes avec plusieurs critères (résilience, degré algébrique, non linéarité. . .)