The number of k-faces of a simple d-polytope

Anders Björner*
Department of Mathematics
Royal Institute of Technology
S-100 44 Stockholm, SWEDEN
bjorner@math.kth.se

Svante Linusson*
Department of Mathematics
Stockholm University
S-106 91 Stockholm, SWEDEN
linusson@matematik.su.se

Abstract

Consider the question: Given integers $k < d < n$, does there exist a simple d-polytope with n faces of dimension k? We show that there exist numbers $G(d,k)$ and $N(d,k)$ such that for $n > N(d,k)$ the answer is yes if and only if $G(d,k)$ divides n. Furthermore, a formula for $G(d,k)$ is given, showing that e.g. $G(d,k) = 1$ if $k \geq \lfloor \frac{d+1}{2} \rfloor$ or if both d and k are even, and also in some other cases (meaning that all numbers beyond $N(d,k)$ occur as the number of k-faces of some simple d-polytope).

This question has previously been studied only for the case of vertices ($k = 0$), where Lee [Le] proved the existence of $N(d,0)$ (with $G(d,0) = 1$ or 2 depending on whether d is even or odd), and Prabhu [P2] showed that $N(d,0) \leq cd\sqrt{d}$. We show here that asymptotically the true value of Prabhu's constant is $c = \sqrt{2}$ if d is even, and $c = 1$ if d is odd.

1 Introduction

An integer n will be called (d,k)-*realizable* if there is a simple d-polytope with n faces of dimension k. For terminology and basic properties of polytopes we refer to the literature, see e.g. [Z].

We show, see Theorem 7, that there exist numbers $G(d,k)$ and $N(d,k)$ such that

- if n is (d,k)-realizable then $G(d,k)$ divides n;
- if $G(d,k)$ divides n and $n > N(d,k)$ then n is (d,k)-realizable.

*Supported by EC grant CHRX-CT93-0400 and by the Mathematical Sciences Research Institute (Berkeley, CA).

The $G(d,k)$-divisible numbers that are not (d,k)-realizable will be called (d,k)-*gaps*. Thus there are only finitely many gaps for all $d > k \geq 0$. In this paper we study the numbers $G(d,k)$ and $N(d,k)$. Our proofs rely on the g-theorem.

To give some feeling for the results, let us discuss a few special cases. The parity restrictions that exist for each dimension k are easiest to understand for the case of vertices ($k = 0$). Namely, the graph of a simple d-polytope is d-regular, so if the polytope has n vertices then it has $\frac{dn}{2}$ edges. Hence, if d is odd n must be even. This is in fact the only constraint, and we have

$$G(d,0) = \begin{cases} 1, & d \text{ even} \\ 2, & d \text{ odd.} \end{cases}$$

This result is due to Lee [Le], who initiated the study of properties of vertex-count numbers of simple polytopes. Via the regular graph property this also implies the result for edge-count numbers:

$$G(d,1) = \begin{cases} \frac{d}{2}, & d \text{ even} \\ d, & d \text{ odd.} \end{cases}$$

For $1 < k < \lfloor \frac{d+1}{2} \rfloor$ the situation gets more complicated and the answer is different for k even and k odd. For instance,

$$G(d,2) = \begin{cases} 2, & d \equiv 1 \pmod 4 \\ 1, & \text{otherwise.} \end{cases}$$

The modulus $G(d,k)$ can get arbitrarily large in this range; for instance, $G(d,k) = d - k + 1$ whenever k is odd and $d - k + 1$ is a prime. Then, for $k \geq \lfloor \frac{d+1}{2} \rfloor$ the situation simplifies again to $G(d,k) = 1$. Theorem 2 gives the general formula for $G(d,k)$.

It is also of interest to study the magnitude of the numbers $N(d,k)$ (defined as the smallest possible ones for which the above statement is true). Again, this has been studied for the case of vertices by Prabhu [P2], who showed that $N(d,0) \leq cd\sqrt{d}$. We prove that asymptotically the true value of Prabhu's constant is $c = \sqrt{2}$ if d is even, and $c = 1$ if d is odd, see Section 5. We also give an upper bound for $N(d,k)$ in the general case, Theorems 10 and 11, but leave open the determination of its true asymptotic growth.

2 Preliminaries

Given a d-dimensional polytope P, we will call $\mathbf{f} := (f_0, f_1, \ldots, f_{d-1})$ the *f-vector* of P, where f_i is the number of faces of dimension i.

For any integers $n, s \geq 1$, there is a unique way of writing

$$n = \binom{a_s}{s} + \binom{a_{s-1}}{s-1} + \cdots + \binom{a_i}{i},$$

so that $a_s > a_{s-1} > \cdots > a_i \geq i \geq 1$. Then define:

$$\partial^s(n) := \binom{a_s - 1}{s-1} + \binom{a_{s-1} - 1}{s-2} + \cdots + \binom{a_i - 1}{i-1}.$$

Also let $\partial^s(0) := 0$.

A nonnegative integer sequence $(n_0, n_1, n_2, \dots)$ is called an *M-sequence* if

$$n_0 = 1 \quad \text{and} \quad \partial^s(n_s) \leq n_{s-1} \quad \text{for all } s \geq 1.$$

Two simple facts we will need about M-sequences is that if there is a zero in the sequence then all the following entries are also zeros, and that any sequence satisfying $n_0 = 1$ and $n_1 \geq n_2 \geq n_3 \geq \dots$ is an M-sequence.

An alternative definition of M-sequence, due to Macaulay and Stanley [S1], says that a sequence is a M-sequence if and only if it is the f-vector of a multicomplex. See [Li] and [Z] for examples of other interpretations of M-sequences. Let $\lfloor x \rfloor$ and $\lceil x \rceil$ denote the largest integer less than or equal to x and the smallest integer larger than or equal to x, respectively.

Let $\delta := \lfloor \frac{d}{2} \rfloor$ and let $M_d = (m_{ik})$ be the $(\delta+1) \times d$-matrix with entries

$$m_{ik} = \binom{d+1-i}{k+1} - \binom{i}{k+1}, \quad \text{for } 0 \leq i \leq \delta,\ 0 \leq k \leq d-1.$$

For example,

$$M_{10} = \begin{pmatrix} 11 & 55 & 165 & 330 & 462 & 462 & 330 & 165 & 55 & 11 \\ 9 & 45 & 120 & 210 & 252 & 210 & 120 & 45 & 10 & 1 \\ 7 & 35 & 84 & 126 & 126 & 84 & 36 & 9 & 1 & 0 \\ 5 & 25 & 55 & 70 & 56 & 28 & 8 & 1 & 0 & 0 \\ 3 & 15 & 31 & 34 & 21 & 7 & 1 & 0 & 0 & 0 \\ 1 & 5 & 10 & 10 & 5 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Our proofs will rely on the g-theorem, conjectured by McMullen. Sufficiency was proved by Billera and Lee [BL], and necessity by Stanley [S2] and later by McMullen [M], see [Z]. We will use the following matrix reformulation of the g-theorem, given by Björner [B1, B2], see also [Z]. We have here reformulated the statement from simplicial polytopes to simple polytopes, which just correspond to reading the f-vector backwards.

Theorem 1 **[The g-theorem]** *The matrix equation*

$$\mathbf{f} = \mathbf{g} \cdot M_d$$

gives a one-to-one correspondence between f-vectors $\mathbf{f}$ of simple d-polytopes and M-sequences $\mathbf{g} = (g_0, g_1, \dots, g_\delta)$. □

3 The modulus $G(d,k)$

The modulus mentioned in the introduction is defined as follows

$$G(d,k) := \gcd(m_{1,k}, m_{2,k}, \ldots, m_{\delta,k}), \tag{1}$$

the greatest common divisor for the elements in the k-th column and below the top row of the matrix M_d. In this section we will give simple and explicit formulas for $G(d,k)$. The role of $G(d,k)$ as the period for the possible numbers of k-faces of d-polytopes will be shown in the next section.

Theorem 2 *(i) If $k \geq \lfloor \frac{d+1}{2} \rfloor$, then $G(d,k) = 1$.*

(ii) If $k < \lfloor \frac{d+1}{2} \rfloor$ is even, let e be the integer such that $2^e \leq k+1 < 2^{e+1}$. Then

$$G(d,k) = \begin{cases} 2, & \text{if } d-k+1 \equiv 0 \ (\text{mod } 2^{e+1}) \\ 1, & \text{otherwise.} \end{cases}$$

(iii) If $k < \lfloor \frac{d+1}{2} \rfloor$ is odd, let $p_1, \ldots, p_t$ be the primes smaller than or equal to $k+1$, and let $e_i \geq 1$ be the integers such that $p_i^{e_i} \leq k+1 < p_i^{e_i+1}$. Then

$$G(d,k) = \frac{d-k+1}{\gcd(d-k+1, p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t})}.$$

For the proof we will need some facts about binomial coefficients modulo powers of a prime, that will be developed in a sequence of lemmas. Binomial coefficients modulo prime powers have been much studied, see e.g. [G] and the references therein, and the following lemma (which summarizes the properties that we need) is probably known. We have however not been able to find it in the literature, so we include a proof.

Lemma 3 *Let $k, e \geq 0$ and let p be a prime such that $p^e \leq k+1 < p^{e+1}$. Then for all $r \geq 1$ we have*

(i) $d \equiv d' \pmod{p^{e+r}}$ *implies* $\binom{d}{k+1} \equiv \binom{d'}{k+1} \pmod{p^r}$;

(ii)

$$\binom{p^{e+r}+k-i}{k+1} \equiv (-1)^{k+1} \binom{i}{k+1} \pmod{p^r},$$

for all $i = 0, 1, \ldots, p^{e+r}+k$;

(iii) the unique longest run of zeros in the period is $\binom{d}{k+1} \equiv_{p^r} 0$ for all $p^{e+r} \leq d \leq p^{e+r}+k$.

Part *(ii)* shows that if k is odd then the period extended by k is symmetric (mod p^r), and if k is even then it is antisymmetric. The lemma is illustrated by the following modular Pascal triangle.

1
1 1
1 2 1
1 3 3 1
1 0 2 0 1
1 1 2 2 1 1
1 2 3 0 3 2 1
1 3 1 3 3 1 3 1
1 0 0 0 2 0 0 0 1
1 1 0 0 2 2 0 0 1 1
1 2 1 0 2 0 2 0 1 2 1
1 3 3 1 2 2 2 2 1 3 3 1
1 0 2 0 3 0 0 0 3 0 2 0 1
1 1 2 2 3 3 0 0 3 3 2 2 1 1
1 2 3 0 1 2 3 0 3 2 1 0 3 2 1
1 3 1 3 1 3 1 3 3 1 3 1 3 1 3 1
1 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 1
1 1 0 0 0 0 0 0 2 2 0 0 0 0 0 0 1 1
1 2 1 0 0 0 0 0 2 0 2 0 0 0 0 0 1 2 1
1 3 3 1 0 0 0 0 2 2 2 2 0 0 0 0 1 3 3 1
1 0 2 0 1 0 0 0 2 0 0 0 2 0 0 0 1 0 2 0 1
1 1 2 2 1 1 0 0 2 2 0 0 2 2 0 0 1 1 2 2 1 1
1 2 3 0 3 2 1 0 2 0 2 0 2 0 2 0 1 2 3 0 3 2 1
1 3 1 3 3 1 3 1 2 2 2 2 2 2 2 2 1 3 1 3 3 1 3 1
1 0 0 0 2 0 0 0 3 0 0 0 0 0 0 0 3 0 0 0 2 0 0 0 1
1 1 0 0 2 2 0 0 3 3 0 0 0 0 0 0 3 3 0 0 2 2 0 0 1 1
1 2 1 0 2 0 2 0 3 2 3 0 0 0 0 0 3 2 3 0 2 0 2 0 1 2 1
1 3 3 1 2 2 2 2 3 1 1 3 0 0 0 0 3 1 1 3 2 2 2 2 1 3 3 1
1 0 2 0 3 0 0 0 1 0 2 0 3 0 0 0 3 0 2 0 1 0 0 0 3 0 2 0 1

Pascal's triangle (mod 4).

For each prime p define the valuation $v_p : \mathbb{Z} \setminus \{0\} \to \boldsymbol{N}$ by $v_p(n) = s$, where p^s is the highest power of p that is a divisor to n. We will frequently use that

$$v_p(n+m) = v_p(n) \quad \text{if } v_p(n) < v_p(m); \tag{2}$$

in particular, $v_p(n + p^x) = v_p(n)$ if $|n| < p^x$.

Lemma 4 *Let k, e and p be as in Lemma 3. Then*

$$v_p\left[(k+1)\binom{k}{j}\right] \leq e, \quad \textit{for all } 0 \leq j \leq k.$$

Proof The proof hinges on the following fact: *Among all products of $x \leq p^e(p-1)$ consecutive integers in the interval $1, 2, \ldots, p^{e+1} - 1$ the maximum valuation is attained by the string that starts with p^e.* To show this, assume that $r, r+1, \ldots, r+x-1$ is such a string of integers. If $r > p^e$, say $ap^e < r \leq (a+1)p^e$, then the string beginning with $r - ap^e$ has the same valuation. Thus we may assume that $r \leq p^e$.

If $r < p^e$, let s be the least number such that $r < s \leq p^e$ and $v_p(r) < v_p(s)$. Then it is easy to see that $v_p(r(r+1)\cdots(r+x-1)) \leq v_p(s(s+1)\cdots(s+x-1)$, and the claim follows.

We may assume that $j \leq \frac{k}{2}$. Then $j+1 \leq p^e(p-1)$, and what was just shown implies that $v_p((k-j+1)(k-j+2)\cdots(k+1)) \leq v_p(p^e(p^e+1)\cdots(p^e+j)) = e + v_p(j!)$, which is equivalent to the stated formula. $\square$

Proof of Lemma 3 We know from Pascal's triangle that $\binom{d}{k+1} \pmod{p^r}$ is completely determined by the values of $\binom{j}{0} = 1, j \geq 0$, and $\binom{d'+i}{i} \pmod{p^r}$ for any $d' \geq 0$ and all $i = 1, \ldots, k+1$. Therefore it suffices to show that

$$\binom{p^{e+r}-1+i}{i} \equiv_{p^r} 0, \tag{3}$$

for all $i = 1, \ldots, p^{e+1}-1$, to establish the first part of the lemma. We have that $v_p(p^{e+r}+s) = v_p(s)$ for all $s = 1, \ldots, p^{e+r}-1$. So the expansion of the binomial coefficient

$$\binom{p^{e+r}-1+i}{i} = \frac{(p^{e+r}+i-1)(p^{e+r}+i-2)\cdots p^{e+r}}{i(i-1)(i-2)\cdots 2\cdot 1}$$

gives $v_p(\binom{p^{e+r}-1+i}{i}) = e + r - v_p(i) \geq r$, if $i < p^{e+1}$, which proves (3).

The second part of the lemma is obvious when $0 \leq i \leq k$, since both sides are zero (for the left-hand side this follows from (i)). Therefore, assume that $k < i < p^{e+r}$. For each $j \neq 0$ write $j = p^{\min\{v_p(j),e\}} q_j$. Then, for $0 < j < p^{e+r}$:

$$q_{p^{e+r}-j} \equiv_{p^r} q_{-j} = -q_j. \tag{4}$$

We have the equality

$$\binom{i}{k+1}\frac{(k+1)!}{p^{v_p((k+1)!)}} = \frac{i(i-1)\cdots(i-k)}{p^{v_p((k+1)!)}} =$$

$$p^{\sum_{j=0}^{k}\min\{v_p(i-j),e\}-v_p((k+1)!)}\prod_{j=0}^{k} q_{i-j} = p^{\alpha}\prod_{j=0}^{k} q_{i-j},$$

and similarly

$$\binom{p^{e+r}+k-i}{k+1}\frac{(k+1)!}{p^{v_p((k+1)!)}} = \frac{(p^{e+r}-i)(p^{e+r}-i+1)\cdots(p^{e+r}-i+k)}{p^{v_p((k+1)!)}} =$$

$$p^{\sum_{j=0}^{k}\min\{v_p(p^{e+r}-(i-j)),e\}-v_p((k+1)!)}\prod_{j=0}^{k} q_{p^{e+r}-(i-j)} = p^{\beta}\prod_{j=0}^{k} q_{p^{e+r}-(i-j)}.$$

We claim that

$$\beta = \alpha \geq 0.$$

The equality follows from (2), and the inequality will soon be proved. The two identities therefore give, using (4):

$$\binom{i}{k+1}\frac{(k+1)!}{p^{v_p((k+1)!)}} \equiv_{p^r} (-1)^{k+1}\binom{p^{e+r}+k-i}{k+1}\frac{(k+1)!}{p^{v_p((k+1)!)}}.$$

Since $\frac{(k+1)!}{p^{v_p((k+1)!)}}$ is invertible in $\mathbb{Z}_{p^r}$ this implies (ii).

It remains to show that $\alpha \geq 0$. If $v_p(i-j) \leq e$ for all $j = 0, \ldots, k$, then $\alpha = v_p(\binom{i}{k+1}) \geq 0$. If not, then since $k+1 < p^{e+1}$ there is exactly one s, with $i-k \leq s \leq i$, such that $v_p(s) > e$. In that case we have

$$\alpha + v_p((k+1)!) = v_p((i-k)\cdots s \cdots i) - v_p(s) + e =$$

$$v_p((i-k)\cdots(s-1)) + v_p((s+1)\cdots i) + e = v_p((s-(i-k))!) + v_p((i-s)!) + e,$$

where the last equality uses (2) twice. Thus, using Lemma 4,

$$\alpha = -v_p((k-(i-s)+1)(k-(i-s)+2)\cdots(k+1)) + v_p((i-s)!) + e =$$

$$-v_p\left((k+1)\binom{k}{i-s}\right) + e \geq 0.$$

To prove (iii) assume that $\binom{d+i}{k+1} \equiv_{p^r} 0$, for some $d \geq k+1$ and all $i = 0, \ldots, k$. Then $\binom{d}{j} \equiv_{p^r} 0$, for $j = 1, \ldots, k+1$. Especially, $\binom{d}{p^s} \equiv_{p^r} 0$ for $0 \leq s \leq e$, which gives that $v_p(\binom{d}{p^s}) \geq r$. In particular, $v_p(d) \geq r$. We will now show that $v_p(d) \geq r+s$ for all $0 \leq s \leq e$, by induction on s. Assume that $v_p(d) \geq r+s-1$. Then $r \leq v_p(\binom{d}{p^s}) = v_p(d(d-1)\cdots(d-(p^s-1))) - v_p(1 \cdot 2 \cdots (p^s-1)p^s) = v_p(d) + v_p((p^s-1)!) - v_p((p^s-1)!) - v_p(p^s) = v_p(d) - s$. Hence, a run of $k+1$ consecutive zeros must begin with $\binom{d}{k+1}$ for some d divisible by p^{e+r}. On the other hand, the 1's along the left boundary of Pascal's triangle show that there cannot be a run of more than $k+1$ zeros of the form $\binom{i}{k+1}$. This proves the lemma. □

We can now proceed toward the proof of Theorem 2.

Lemma 5 *For each $k < \lfloor \frac{d+1}{2} \rfloor$, $G(d,k)$ is a divisor of $\frac{d-k+1}{\gcd(d-k+1, p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t})}$, where $p_1, \ldots, p_t$ are the primes $\leq k+1$ and $p_i^{e_i} \leq k+1 < p_i^{e_i+1}$.*

Proof Take a prime p dividing $G(d,k)$ and let $x := v_p(G(d,k)) \geq 1$. Write $k+1$ in base p, $k+1 = k_0 + k_1 p + \cdots + k_e p^e$, where $0 \leq k_i < p$ and $k_e \neq 0$. Notice that

$$v_p\left(\frac{d-k+1}{\gcd(d-k+1, p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t})}\right) = \begin{cases} v_p(d-k+1) - e & \text{if } v_p(d-k+1) \geq e, \\ 0 & \text{otherwise,} \end{cases}$$

so it will suffice to show that $v_p(d-k+1) - e \geq x$ in the first case and obtain a contradiction in the second.

Since $p^x | G(d,k)$ we get that $\binom{d+1-i}{k+1} \equiv_{p^x} \binom{i}{k+1}$, for all $i = 1, \ldots, \delta$. Especially we must have $\binom{d+1-i}{k+1} \equiv_{p^x} 0$, for $i = 1, \ldots, k$ and $\binom{d-k}{k+1} \equiv_{p^x} 1$. From

$$(d-2k)\binom{d+1-k}{k+1} = \binom{d-k}{k+1}(d-k+1),$$

we get $v_p(d-k+1) - v_p(d-2k) = v_p(\binom{d+1-k}{k+1}) \geq x \geq 1$. Hence by (2), $v_p(k+1) = v_p(d-k+1-(d-2k)) = v_p(d-2k) < v_p(d-k+1)$.

There are now two cases: First assume that $v_p(d-k+1) \geq e$. If $k+1 = k_e p^e$ we are done, since we have shown that $v_p(d-k+1) - v_p(k+1) \geq x$. Assume that $k+1 > k_e p^e$. From $d-k+1 \geq k+1 > k_e p^e$ we conclude that $v_p(d-k+1-k_e p^e) \geq e$, which implies $v_p(d-k+1-k_e p^e - i) = v_p(i)$, for all $i = 1, \ldots, k+1-k_e p^e < p^e$. This in turn implies that

$$v_p\left(\frac{(d-k-k_e p^e)!}{(d-2k)!}\right) = v_p((k-k_e p^e)!) = v_p\left(\frac{(d+1-k_e p^e)!}{(d+1-k)!}\right).$$

Using the equality

$$\frac{(d-k-k_e p^e)!}{(d-2k)!}\binom{d+1-k_e p^e}{k+1} = \binom{d+1-k}{k+1}\frac{(d+1-k_e p^e)!}{(d+1-k)!},$$

we get that $v_p(\binom{d+1-k_e p^e}{k+1}) = v_p(\binom{d+1-k}{k+1})$. This together with the identity

$$(d-k+1-k_e p^e)\binom{d+2-k_e p^e}{k+1} = \binom{d+1-k_e p^e}{k+1}(d+2-k_e p^e)$$

gives

$$x \leq v_p(m_{k_e p^e - 1, k}) = v_p\left(\binom{d+2-k_e p^e}{k+1}\right) \leq$$

$$v_p\left(\binom{d+1-k_e p^e}{k+1}\right) - e + v_p(d+2-k_e p^e) =$$

$$v_p\left(\binom{d-k+1}{k+1}\right) - e + v_p(k+1-k_e p^e) = v_p(d-k+1) - e.$$

Here the last equality comes from $v_p(k+1-k_e p^e) = v_p(k+1) = v_p(d-2k)$ and $v_p(\binom{d-k+1}{k+1}) = v_p(d-k+1) - v_p(d-2k)$, established above.

The second case is if $a := v_p(d-k+1) < e$. The same argument can be applied again; however, now replacing $k_e p^e$ everywhere by $k_a p^a + \cdots + k_e p^e$ and replacing e by a. We then get $x \leq v_p(d-k+1) - a = 0$, a contradiction. $\square$

Lemma 6 *$G(d,k)$ is a divisor to $m_{0,k} = \binom{d+1}{k+1}$.*

PROOF If for a prime p we have that p^r divides $G(d,k)$ and $p^e \leq k+1 < p^{e+1}$, then Lemma 5 implies that p^{r+e} divides $d-k+1$. Hence $v_p(\binom{d+1}{k+1}) = v_p(\binom{d+1}{k}) + v_p(d-k+1) - v_p(k+1) \geq r$. □

PROOF OF THEOREM 2. The first statement follows from the fact that $m_{d-k,k} = 1$ for $k \geq \left\lfloor \frac{d+1}{2} \right\rfloor$.

Let $k < \left\lfloor \frac{d+1}{2} \right\rfloor$. We have from the definition of $m_{i,k}$ that for every prime p and every $r \geq 1$:

$$p^r | G(d,k) \iff \binom{d+1-i}{k+1} \equiv_{p^r} \binom{i}{k+1}, \text{for } i = 0, 1, \ldots, \left\lfloor \tfrac{d+1}{2} \right\rfloor. \tag{5}$$

Actually, the definition supports this only for $i = 1, \ldots, \delta = \left\lfloor \frac{d}{2} \right\rfloor$ on the right hand side, but $i = 0$ can be added because of Lemma 6 and $i = \left\lfloor \frac{d+1}{2} \right\rfloor$ (for d odd) gives a trivially true identity.

Case 1: k even. Assume that $G(d,k) \neq 1$, and that $p^r | G(d,k)$. Since by Lemma 3 there is a unique longest run of $k+1$ zeros in the period of $\binom{i}{k+1}$ (mod p^{e+r}) we get from (5) that $d-k+1 \equiv_{p^{e+r}} 0$. Therefore, Lemma 3 and (5) give

$$\binom{k+1}{k+1} \equiv_{p^r} \binom{d-k}{k+1} \equiv_{p^r} \binom{p^{e+r}-1}{k+1} \equiv_{p^r} -\binom{k+1}{k+1},$$

which implies $p = 2$ and $r = 1$. Hence, $G(d,k) = 2$, and this happens only if $d-k+1 \equiv_{2^{e+1}} 0$. On the other hand, if $d-k+1 \equiv_{2^{e+1}} 0$ then $2 | G(d,k)$ can be concluded from Lemma 3 and (5).

Case 2: k odd. Let p^r be a divisor of $\frac{d-k+1}{\gcd(d-k+1, p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t})}$. By Lemma 5 it suffices to show that $p^r | G(d,k)$. The assumption implies that p^{r+e} divides $d-k+1$, where as usual e is defined by $p^e \leq k+1 < p^{e+1}$. Hence by Lemma 3

$$\binom{d+1-i}{k+1} \equiv_{p^r} \binom{i}{k+1}, \quad \text{for all } i = 0, \ldots, d+1,$$

which via (5) shows that $p^r | G(d,k)$.

This finishes the proof of the theorem. □

EXAMPLE We want to calculate $G(116, 9)$. Since $k = 9$ is odd we calculate the greatest common divisor of $116 - 9 + 1 = 108$ and $2^3 \cdot 3^2 \cdot 5 \cdot 7$ which is 36. We get $G(116, 9) = 118/36 = 3$. □

4 Periodicity of (d,k)-realizable numbers

We will now show the general theorem about the ultimately stable periodic distribution of the (d,k)-realizable numbers.

Theorem 7 *Fix $0 \leq k < d$, and let $G(d,k)$ be the number defined in equation (1). Then there exists an integer N such that for all $n > N$:*

$$n \text{ is the number of } k\text{-faces of a simple } d\text{-polytope}$$

$$\Longleftrightarrow$$

$$n \equiv 0 \pmod{G(d,k)}$$

Proof We will prove the theorem with the last statement replaced by $n \equiv m_{0,k} \pmod{G(d,k)}$. Lemma 6 shows that $m_{0,k}$ is divisible by $G(d,k)$, so this reformulation is equivalent.

$\Longrightarrow$ This direction is clear from Theorem 1.

$\Longleftarrow$ Write

$$G(d,k) = \sum_{i=1}^{\delta} \lambda_i m_{i,k}, \qquad \lambda_i \in \mathbb{Z}.$$

Suppose $m_{1,k} = C \cdot G(d,k)$. Define

$$g_\delta := \begin{cases} (C-1)|\lambda_\delta|, & \text{if } \lambda_\delta < 0 \\ 0, & \text{otherwise;} \end{cases}$$

and recursively

$$g_i := g_{i+1} + (C-1)(|\lambda_i| + |\lambda_{i+1}|), \qquad 0 < i < \delta.$$

Let $N := m_{0,k} + \sum_{i=1}^{\delta} g_i m_{i,k}$, and let $g_i^{(p)} = g_i + p\lambda_i$, for $p = 0, 1, \ldots$

Then $g^{(p,q)} = (1, g_1^{(p)} + q, g_2^{(p)}, \ldots, g_\delta^{(p)})$ is nonnegative and decreasing after the first entry for all $q \geq 0$ and all $0 \leq p < C$, and hence is an M-sequence. The f_k values corresponding to these g-vectors are

$$f_k^{(p,q)} = N + qCG(d,k) + pG(d,k).$$

It is clear from the construction that all numbers $N + j \cdot G(d,k), j = 0, 1, \ldots$ are of the form $f_k^{(p,q)}$ for suitable $q \geq 0$ and $0 \leq p < C$. $\square$

Corollary 8 *If the $m_{i,k}$ are relatively prime, then all numbers from some point on are (d,k)-realizable. Furthermore, Theorem 2 shows that this happens precisely in the following cases:*

(i) if $k \geq \lfloor \frac{d+1}{2} \rfloor$;

(ii) if $k < \lfloor \frac{d+1}{2} \rfloor$ is even, unless $d - k + 1 \equiv 0$ (mod 2^{e+1});

(iii) if $k < \lfloor \frac{d+1}{2} \rfloor$ is odd, unless $d-k+1$ fails to divide $p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$. $\square$

Now, define $N(d,k)$ to be the least number N for which Theorem 7 is true. Note that $N(d,d-1) = d$, so in what follows we may assume that $k < d-1$.

What can be said about the magnitude of $N(d,k)$? We will here give a general upper bound, and then we will determine the exact asymptotic growth for the special case $N(d,0)$ in the following section.

Define

$$L(d,k) := \min \max_{i=1}^{\delta} |\lambda_i|,$$

with the minimum taken over all ways to represent $G(d,k)$ on the form

$$G(d,k) = \sum_{i=1}^{\delta} \lambda_i m_{i,k}, \qquad \lambda_i \in \mathbb{Z}.$$

Lemma 9 *For all $0 \le k \le d-2$, we have $L(d,k) < m_{1,k}$.*

Proof Assume $G(d,k) = \sum_{i=1}^{\delta} \lambda_i m_{i,k}$, with $|\lambda_s| \ge m_{1,k}$ and $m_{s,k} \ne 0$. By symmetry we may assume that λ_s is positive, that is $\lambda_s \ge m_{1,k}$. Since $G(d,k) < m_{1,k} m_{s,k}$, there has to be a t such that $\lambda_t < 0$ and $m_{t,k} \ne 0$. Let

$$\lambda_i' = \begin{cases} \lambda_s - m_{t,k} & \text{if } i = s, \\ \lambda_t + m_{s,k} & \text{if } i = t, \\ \lambda_i & \text{otherwise.} \end{cases}$$

We get $G(d,k) = \sum_{i=1}^{\delta} \lambda_i' m_{i,k}$. Since $|\lambda_s'| < |\lambda_s|$, $|\lambda_t'| < |\lambda_t|$ or else $|\lambda_t'| < m_{s,k}$, and all other $|\lambda_i'|$ are unchanged, we can continue this process until $|\lambda_i| < m_{1,k}$, for all i. $\square$

Theorem 10 $N(d,k) < \frac{1}{2} d^2 \binom{d}{k+1}^3$

Proof Referring to the proof of Theorem 7, with an optimal choice of the λ_i-s, we have

$$N(d,k) \le \sum_{i=0}^{\delta} g_i m_{i,k} \le \binom{d+1}{k+1} + L(d,k)(C-1) \sum_{i=1}^{\delta} (2\delta + 1 - 2i) \binom{d+1-i}{k+1}$$

$$\le \binom{d+1}{k+1} + L(d,k)(C-1)\delta(2\delta-1)\binom{d}{k+1} < 2L(d,k)\delta^2 \binom{d}{k+1}^2.$$

$\square$

For example, let $k = 0$. The general bound specializes to $N(d,0) \le \frac{1}{2} d^5$. This should be compared to the true asymptotic value $N(d,0) \sim c d^{3/2}$, which will be proved in the next section.

For $k \ge \lfloor \frac{d+1}{2} \rfloor$ we can improve on the general bound significantly.

Theorem 11 *Suppose $k \geq \lfloor \frac{d+1}{2} \rfloor$. Then $N(d,k) < \binom{d+1}{d-k}(d-k)(k+1)(d+1)/2$.*

Since $G(d,k) = 1$ for such k this implies that for every $n \geq \binom{d+1}{d-k}(d-k)(k+1)(d+1)/2$ there is a simple d-polytope with n faces of dimension k.

To prove this we need a more technical construction than before. First we extend the definition of ∂^s. Define for $p \leq s$:

$$\partial_p^s(n) := \binom{a_s - p}{s - p} + \binom{a_{s-1} - p}{s - 1 - p} + \cdots + \binom{a_i - p}{i - p},$$

where n is written in the unique expansion

$$n = \binom{a_s}{s} + \binom{a_{s-1}}{s-1} + \cdots + \binom{a_i}{i},$$

as in Section 2. Also let $\partial_p^s(0) := 0$. We will allow p to be negative, which corresponds to the natural "inverse" of ∂_p^s for positive p. Thus, for $p > 0$, $\partial_{-p}^s(n)$ is the greatest number such that $\partial_p^s(\partial_{-p}^s(n)) = n$. We will continue to write just ∂^s for ∂_1^s.

Now, fix d and $k \geq \lfloor \frac{d+1}{2} \rfloor$. Define a vector $\mathbf{g} := (g_0, g_1, \ldots, g_{d-k})$ inductively as follows.

- Let $g_{d-k} := 0$.
- Assume we have defined $g_{d-k}, g_{d-k-1}, \ldots, g_i$, for some $0 < i \leq d-k$. Let

  $g_{i-1} := \partial^i(x_i)$, where x_i is the smallest integer such that $x_i \geq g_i$ and

$$\sum_{s=i}^{d-k} \left(\partial_{i-s}^i(x_i) - g_s\right) m_{s,k} \geq m_{i-1,k} - 1. \tag{6}$$

This is an M-sequence by construction.

Lemma 12 *Given the g-vector above, define $N := \sum_{i=0}^{d-k} g_i m_{i,k}$. Then there are no (d,k)-gaps larger than or equal to N.*

Proof Adding any positive integer to g_1 in an M-sequence gives another M-sequence. Thus we only have to prove that it is possible to form all the $m_{1,k} - 1$ integers following N with legal g-vectors. This will imply the lemma.

We will think of the elements in column k of M_d as weights which we combine to get the correct total weight.

Consider first the choice of $g_{d-k-1} := \partial^{d-k}(x_{d-k})$, where $x_{d-k} = m_{d-k-1,k} - 1$. All the vectors $(g_0, g_1, \ldots, g_{d-k-1}, i)$, $i = 0, \ldots m_{d-k-1,k} - 1$ are M-sequences, producing $N, N+1, \ldots, N + m_{d-k-1,k} - 1$ k-faces respectively. We here use the fact that $m_{d-k,k} = 1$. Similarly $(g_0, g_1, \ldots, g_{d-k-1} + j, i)$, for fixed j and $i = 0, \ldots m_{d-k-1,k} - 1$ gives $N + jm_{d-k-1,k}, N + jm_{d-k-1,k} + 1, \ldots, N + (j +$

$1)m_{d-k-1,k}-1$ k-faces. The definition of g_{d-k-2} allows us to have j sufficiently large to get all the numbers at least up to and including $N+m_{d-k-2,k}-1$.

Assuming inductively that we can form the sequence $N, N+1, \ldots, N+m_{i,k}-1$ by increasing only coordinates $i+1, \ldots, d-k$, the definition of $\mathbf{g}$ gives that we can form all the numbers $N, N+1, \ldots, N+m_{i-1,k}-1$ by increasing only coordinates $i, \ldots, d-k$ of $\mathbf{g}$. This proves the lemma □

EXAMPLE Take $d=10$ and $k=6$. We see from the matrix M_{10}, displayed in Section 2, that the weights are $330, 120, 36, 8$ and 1. We get $\mathbf{g}=(1,4,6,6,0)$ which gives $N(10,6)<1074$, showing that every $n \geq 1074$ is $(10,6)$-realizable.

PROOF OF THEOREM 11 First we show that $g_i \leq (d-k-i)(k+1)$ by reverse induction. It is trivially true for g_{d-k}. Assume it is true for g_i. Since $g_{i-1} = \partial^i(x_i) \leq x_i$, it suffices to bound x_i. The inequality (6) is true if $(x_i - g_i)m_{i,k} \geq m_{i-1,k}-1$. Since x_i is chosen to be minimal we get that

$$x_i \leq g_i + \left\lceil \frac{m_{i-1,k}-1}{m_{i,k}} \right\rceil = g_i + \left\lceil \frac{\binom{d+2-i}{k+1}-1}{\binom{d+1-i}{k+1}} \right\rceil \leq$$

$$\leq g_i + \left\lceil \frac{d+2-i}{d+1-i-k} - \frac{1}{\binom{d+1-i}{k+1}} \right\rceil \leq g_i + k + 1 \leq (k+1)(d-k-i+1).$$

Now,

$$N \leq \binom{d+1}{k+1} + (k+1)\sum_{i=1}^{d-k}(d-k-i)\binom{d+1-i}{k+1} \leq$$

$$\binom{d+1}{k+1} + (k+1)\binom{d}{k+1}\binom{d-k}{2} \leq \binom{d+1}{k+1}\left(1 + \frac{(k+1)(d-k-1)(d+1)}{2}\right).$$

This proves the theorem. □

Note that $m_{0,k}+1 = \binom{d+1}{d-k}+1$ is never (d,k)- realizable for $k < d-1$. This gives a trivial lower bound for $N(d,k)$ to be compared with the upper bounds in Theorems 10 and 11.

5 The case of vertices

The only case of (d,k)-realizability that seems to have been previously studied is for $k=0$, i.e., the number of vertices. We will make a more exact analysis of that case.

Lee showed in [Le, Corollary 4.4.15] that for each dimension d all sufficiently large numbers are $(d,0)$-realizable (with parity restrictions, see the Introduction). Prabhu [P1, P2] strengthened the result and proved that there exists a constant c such that every $n > cd\sqrt{d}$ is $(d,0)$-realizable (with parity restrictions). This gives an upper bound on the size $N(d,0)$ of the largest gap in each dimension — we are not aware of any published non-trivial lower bound. The exact result is previously known only for small dimensions, see [Le] where Lee lists all $(d,0)$-gaps for $d \leq 9$.

We will sharpen Prabhu's result in both directions and prove that one can use $c = \sqrt{2} + \epsilon$ as constant in his theorem for any $\epsilon > 0$ and sufficiently large even d (depending on ϵ). However, the statement is not true for $c < \sqrt{2}$.

Theorem 13 *If $d \geq 4$ is even, then there does not exist a simple d-polytope with $n = (d-1)(\lceil\sqrt{2d-4}\rceil - 2) + 4$ vertices.* □

Theorem 14 *For every even $d \geq 2$ and every $n > (d-1)(\sqrt{2d} + 2\sqrt{2\sqrt{2d}} + 5)$, there exists a simple d-polytope with n vertices.* □

Similarly, if we restrict our attention to d odd the true value for c is asymptotically equal to 1.

Theorem 15 *If $d \geq 3$ is odd, then there does not exist a simple d-polytope with $n = (d-1)(\lceil\sqrt{d-2}\rceil - 2) + 4$ vertices, but for every even integer $n > (d-1)(\sqrt{d} + 2\sqrt{2\sqrt{2d}} + 5)$, there exists a simple d-polytope with n vertices.* □

Proof of Theorem 13 Let $d = 2\delta \geq 6$, so the first column of M_d will be $2\delta+1, 2\delta-1, \ldots, 3, 1$. We will look for the lowest possible value for f_0 such that $f_0 \equiv 4 \pmod{2\delta - 1}$. The entries of the first column will be the weights by which we seek to create the value of f_0. They are $2, 0, -2, -4, \ldots, -(2\delta-2) \pmod{2\delta-1}$. By the properties of M-sequences we have to take at least $k+2$ weights to obtain $f_0 \equiv 4 \equiv -2\delta + 5 \pmod{2\delta - 1}$, where

$$2 + \sum_{i=0}^{k} -2i \leq -(2\delta - 1) - (2\delta - 5),$$

corresponding to the M-sequence $\mathbf{g} = (1, 1, \ldots, 1, 1)$ with $k+2$ 1's. This is equivalent to

$$k(k+1) \geq 4\delta - 4.$$

Now, choose k such that $k \leq \sqrt{4\delta - 4} < k + 1$. We then get that

$$f_0 \geq 2\delta + 1 + \sum_{i=0}^{k} 2\delta - 1 - 2i = 2\delta + 1 + (2\delta - k - 1)(k+1) >$$

$$2\delta + 1 + (2\delta - 1)\left\lceil\sqrt{4\delta - 4}\right\rceil - \left(\left\lfloor\sqrt{4\delta - 4}\right\rfloor^2 + \left\lfloor\sqrt{4\delta - 4}\right\rfloor\right) >$$

$$(d-1)(\left\lceil\sqrt{2d-4}\right\rceil-2)+4.$$

Hence, $(d-1)(\lceil\sqrt{2d-4}\rceil-2)+4$ is a gap.

The result is easily seen to be true also for $d=4$. $\square$

Proof of Theorem 14 Let $d=2\delta\geq 4$ (the case $d=2$ is easily checked). As above the first column of M_d will be $2\delta+1, 2\delta-1, \ldots, 3, 1$. First we note that if $n+1, n+2, \ldots, n+d-1$ are all realizable then every integer larger then n is realizable since we can just add 1 to g_1 in the corresponding M-sequences.

As in the previous proof we let k_1 be such that $k_1\leq\sqrt{4\delta-4}<k_1+1$. We consider the M-sequences $1=g_0=g_1=\cdots=g_i$ and $0=g_{i+1}=g_{i+2}=\ldots$, for $0\leq i\leq k_1+1$. The corresponding values for f_0 constitute one sequence of odd residues and one sequence of even residues modulo $d-1$, with no distance being larger than $2(k_1-1)$. Now we choose k_2 such that

$$\sum_{i=0}^{k_2}-2i\leq-(2k_1-1)\Longleftrightarrow k_2+1>\sqrt{2(k_1-1)}.$$

It is clear that the M-sequences $1=g_0, 2=g_1=\cdots=g_j$, $1=g_{j+1}=g_{j+2}=\cdots=g_i$ and $0=g_{i+1}=g_{i+2}=\ldots$, for $0\leq j<i\leq k_1+1$ and $j\leq k_2$, give values for $f_0 \pmod{d-1}$ where no residue is more than $2(k_2-1)$ away from another residue of the same parity. Continuing this process, we choose integers $k_1, k_2, \ldots, k_s$, as small as possible such that $\sqrt{2(k_{i-1}-1)}<k_i+1$, for $2\leq i\leq s$. We stop when we have reached $k_s=1$. Hence, every possible value for $f_0 \pmod{d-1}$ can be obtained with an M-sequence that has coordinates satisfying $g_i\leq j$, whenever $k_{j+1}+1<i$.

So if f_0 is a gap then we must have

$$f_0<2\delta+1+\sum_{i=0}^{k_1}(2\delta-1-2i)+\sum_{i=0}^{k_2}(2\delta-1-2i)+\cdots+\sum_{i=0}^{k_s}(2\delta-1-2i)<$$

$$2\delta+1+(k_1+1+k_2+1+\cdots+k_s+1)(2\delta-1)<\text{[by induction]}$$

$$2\delta+1+(k_1+1+2(k_2+1))(2\delta-1)<(d-1)(\sqrt{2d-4}+2\sqrt{2\sqrt{2d-4}-2}+5).$$

This estimate suffices to show the theorem. $\square$

Proof of Theorem 15 The proof can be carried out in the same manner as the two previous proofs. $\square$

References

[BL] L.J. Billera and C.W. Lee, *A proof of the sufficiency of McMullen's conditions for f-vectors of simplicial convex polytopes,* J. Combinatorial Theory Ser. A **31** (1981), 237–255.

[B1] A. Björner, *Face numbers of complexes and polytopes,* in "Proceedings of the International Congress of Mathematicians, Berkeley, 1986", Amer. Math. Soc., 1987, pp. 1408-1418.

[B2] A. Björner, *Partial unimodality for f-vectors of simplicial polytopes and spheres*, in "Jerusalem Combinatorics '93" (eds. H. Barcelo and G. Kalai), Contemporary Math. Series, Vol. 178, Amer. Math. Soc., 1994, pp. 45–54.

[G] A. Granville, *Binomial coefficients modulo prime powers*, preprint, http://www.math.uga.edu/˜andrew/Binomial/index.html.

[Le] C. W. Lee, *Counting the faces of simplicial convex polytopes*, Ph.D. thesis, Cornell University, 1981.

[Li] S. Linusson, *The number of M-sequences and f-vectors*, in Ph.D. thesis "Studies in algebraic and topological combinatorics", KTH, Sweden, 1995, pp. 117–141.

[M] P. McMullen, *On simple polytopes*, Inventiones Math. **113** (1993), 419–444.

[P1] N. Prabhu, *Hamiltonian Simple Polytopes*, Discrete&Computational Geometry **14** (1995), 301–304 .

[P2] N. Prabhu, *Facet-numbers of simplicial polytopes*, Chapter 7 in Ph.D. thesis "Properties of Convex Polytopes", New York University, 1991.

[S1] R. P. Stanley, *Hilbert functions for graded algebras*, Advances in Math. **28** (1978), 57–83.

[S2] R.P. Stanley, *The number of faces of simplicial convex polytopes*, Advances in Math. **35** (1980), 236–238.

[Z] G. M. Ziegler, *Lectures on Polytopes*, GTM-series, Springer-Verlag, 1995.