Embedding Divisor and Semi-Prime Testability in $f$-Vectors of Polytopes

Eran Nevo

Received: 26 October 2021 / Revised: 13 September 2022 / Accepted: 16 September 2022 / Published online: 20 October 2022

Abstract

We obtain computational hardness results for $f$-vectors of polytopes by exhibiting reductions of the problems DIVISOR and SEMI-PRIME TESTABILITY to problems on $f$-vectors of polytopes. Further, we show that the corresponding problems for $f$-vectors of simplicial polytopes are polytime solvable. The situation where we prove this computational difference (conditioned on standard conjectures on the density of primes and on $P \neq NP$) is when the dimension $d$ tends to infinity and the number of facets is linear in $d$.

Keywords  Polytopes · $f$-vector · Computational complexity

Mathematics Subject Classification  52B05

1 Introduction

The $f$-vector $(f_0(P), f_1(P), \ldots, f_{d-1}(P))$ of a $d$-polytope $P$ records the number of faces $P$ has: $f_i(P)$ faces in dimension $i$. The $f$-vectors of polytopes of dimension at most 3 were characterized by Steinitz, and the conditions, which are linear equalities and inequalities on the entries of the $f$-vector, are then easy to check; see e.g. [10, Sect. 10.3]. In contrast, the $f$-vectors of $d$-polytopes for $d \geq 4$ are not well understood; see e.g. [10, Sect. 10.4] and the fatness parameter [25] for $d = 4$, while the case $d > 4$ is even less understood. The set of $f$-vectors of the important subfamily of simplicial
polytopes is characterized by the $g$-theorem, conjectured by McMullen [13] and proved by Stanley [20] and Billera–Lee [6]. While this well-understood set may be regarded as complicated from some viewpoints (e.g. it is not a semi-algebraic set of lattice points, for any $d \geq 6$, see [18]), yet deciding membership in it is computationally easy, see [14, Thm. 1.4]. The analogous computational problem for the set of $f$-vectors of $d$-polytopes is unsolved, see [14, Problem 1.5], and we conjecture it to be NP-hard. It is known to be decidable in time double exponential in the input size, see e.g. [14, Sect. 1.2].

We exhibit two variants of the above membership problem and show that they are computationally hard for $f$-vectors of polytopes (given standard conjectures in complexity theory), but are efficiently solvable for $f$-vectors of simplicial polytopes.

**Problem 1.1** (fiber count) Given $d$, a subset of integers $S \subseteq [0, d-1]$, and values $f_i$ for all $i \in S$, let $f_c = f_c(d, (f_i)_{i \in S})$ be the number of $f$-vectors of $d$-polytopes with the given values for the $S$-coordinates. What is the computational complexity (as a function of the input size):

(i) of computing $f_c$?
(ii) of deciding whether $f_c = 1$?

For example, a recent result of Xue [23], verifying Grünbaum’s lower bound conjecture for general polytopes, implies that for all integers $d \geq 2$, $1 \leq i \leq d - 2$, and $d + 1 \leq a \leq 2d$, for $S = \{0, i\}$,

$$f_c \left(d, \left( f_0 = a, f_i = \left( \binom{d + 1}{i + 1} + \binom{d}{i + 1} - \binom{2d + 1 - a}{i + 1} \right) \right) \right) = 1.$$  

Thus, to obtain a hardness result in (ii) where $S$ is a two element subset containing 0, we must have $f_0 \geq 2d + 1$; see Lemma 1.2 (ii) below.

The problem of computing the number of divisors of a given integer, or even of deciding if a given integer is the product of exactly two primes (Semiprime Testability), is believed to be as hard as FACTORING, namely, as factoring the integer into a product of primes; see e.g. Terry Tao’s answer at MathOverflow [17]. From a structural result of McMullen on $d$-polytopes with $d + 2$ facets [12], specialized to the case $f_0 = 2d + 1$ (see also [16]), we conclude:

**Lemma 1.2** (i) The number of $f$-vectors of $d$-polytopes with $f_0 = 2d + 1$ and $f_{d-1} = d + 2$ equals $\lfloor D(d)/2 \rfloor$, where $D(d)$ is the number of divisors of $d$ in the interval $[2, d-1]$.
(ii) In particular, $f_c \left(d, \left( f_0 = 2d + 1, f_{d-1} = d + 2 \right) \right) = 1$ iff $d$ either is a semiprime or equals $p^3$ for some prime $p$.

(And of course $f_c \left(d, \left( f_0 = 2d + 1, f_{d-1} = d + 2 \right) \right) = 0$ iff $d$ is a prime, which can be decided in polytime in $\log d$ by the celebrated PRIMES is in P result [1, 2].)

As a corollary, we can reduce Semiprime Testability to a decision problem on fiber count, namely Problem 1.1 (ii). Here the bit length of the input is $O(\log d)$, while the full $f$-vector clearly has bit length of size $\Omega(d)$ (in fact $\Omega(d \log d)$). Nevertheless, the corresponding problem for $f$-vectors of simplicial polytopes can be solved efficiently:

Springer
Let $f_{cs} = f_{cs}(d, (f_i)_{i \in S})$ be the number of $f$-vectors of simplicial $d$-polytopes with the given values for the $S$-coordinates.

**Theorem 1.3** Given as input positive integers $d, a, b$ of total bit length $O(\log d)$, and $b$ of order $O(d)$:

(i) It can be decided in polylog($d$)-time whether $f_{cs}(d, f_0 = a, f_{d-1} = b) = 1$.

(ii) Deciding whether $f_{cs}(d, f_0 = a, f_{d-1} = b) = 1$ is at least as hard as Semiprime Testability for $d$.

The problem DIVISOR, asking whether given three integers $L < U < d$, $d$ has a divisor in the interval $[L, U]$, is believed to be NP-complete, see e.g. Sudan’s survey [22]. In fact, it is NP-complete if for any large enough real number $x$ there exists a prime in the interval $[x, x + \text{polylog}(x)]$, see e.g. the answers by Peter Shor and Boaz Barak in StackExchange [7] to a question of Michaël Cadilhac. Cramér’s conjecture [8, 9] implies that for any $\epsilon > 0$ the interval $[x, x + (1 + \epsilon)\log^2 x]$ suffices for $x$ large enough. DIVISOR remains NP-complete if we require $\sqrt{d} \in [L, U]$ (under the assumption above on the existence of primes in short intervals), by a reduction from a variant of SUBSET SUM of real numbers where the target sum is approximately half the sum of all input numbers.

**Lemma 1.4** Given three integers $L < U < d$, with $\sqrt{d} \in [L, U]$, denote $M = M(L, U, d) = \max(L + d/L, U + d/U)$. Then there exists a divisor $x$ of $d$ such that $L \leq x \leq U$ iff there exists a $d$-polytope $P$ whose $f$-vector satisfies $f_0(P) = 2d + 1$, $f_{d-1}(P) = d + 2$ and $f_1(P) \in [d^2 + d(1 + d - M)/2, d^2 + d(1 + d - 2\sqrt{d})/2]$.

Again, we show that the corresponding problem for simplicial polytopes is polytime-solvable, despite the fact that the input is of size logarithmic in $d$, the number of coordinates in the $f$-vector. Combined, it reads as follows.

**Theorem 1.5** Given as input positive integers $d, a, b, L, U$ of total bit length $O(\log d)$, such that $L \leq U$ and $b$ is of order $O(d)$, then:

(i) It can be decided in polylog($d$)-time whether there exists a simplicial $d$-polytope $P$ whose $f$-vector satisfies $f_0(P) = a$, $f_{d-1}(P) = b$, and $f_1(P) \in [L, U]$.

(ii) Deciding whether there exists a $d$-polytope $P$ whose $f$-vector satisfies $f_0(P) = a$, $f_{d-1}(P) = b$, and $f_1(P) \in [L, U]$ is at least as hard as DIVISOR for $d$.

**Remarks** (1) Sjöberg and Ziegler [19] characterized the pairs $(n, m)$ such that there exists a $d$-polytope $P$ with $(f_0(P), f_{d-1}(P)) = (n, m)$ for even $d$ whenever $n + m \geq \binom{3d+1}{d/2}$ (and they proved similar but weaker results for $d$ odd); however our interest is in the region $m + n \in O(d)$ where the behaviour is different and not well understood. If one fixes $d \geq 5$ and let $m + n$ tend to infinity, the results [19, Thms. 3.2 and 3.3] show that deciding whether $(n, m)$ equals $(f_0(P), f_{d-1}(P))$ for some $d$-polytope is polytime-solvable for $d$ even, but may still be hard for $d$ odd.

(2) For $d = 4$, all the two-projection pairs $(f_i(P), f_j(P))$, $0 \leq i < j \leq 3$, are characterized, in a series of works, see Grünbaum [10, Thms. 10.4.1 and 10.4.2], Barnette–Reay [4, Thm. 10], and Barnette [3, Thm. 1]. It follows that these pairs are polytime decidable. Polytime decidability holds also for the pairs $(f_0(P), f_1(P))$.
of 5-polytopes $P$, characterized independently by Kusunoki–Murai [11, Thm. 1.2] and Pineda-Villavinecio et al. [15, Thm. 7.2]. However, whether $f$-vectors of 4-polytopes can be decided in polynomial time is an open problem which we expect to be NP-hard.

**Outline:** Section 2 sets notation and collects the background results we need on $f$-vectors of polytopes. In Sect. 3 we prove the computational hardness results above, for general polytopes, namely Theorems 1.3 (ii) and 1.5 (ii). In Sect. 4 we prove the computational efficiency results above, for simplicial polytopes, namely, Theorems 1.3 (i) and 1.5 (i). Section 5 ends with open problems.

## 2 Preliminaries

For the basics on face enumeration and on polytopes needed here we refer to e.g. the textbooks by Grünbaum [10] and Ziegler [24].

### 2.1 Faces of Polytopes

A $d$-polytope is a polytope of dimension $d$. Its faces of dimension $k$ are called $k$-faces. Faces of dimension 0, 1, $d - 1$ are called vertices, edges, facets, respectively. A polytope is simplicial if all its proper faces are simplices. Denote by $f_k(P)$ the number of $k$-faces of a $d$-polytope $P$. The $f$-vector of $P$ is $f(P) = (1 = f_{-1}(P), f_0(P), f_1(P), \ldots, f_{d-1}(P))$. The following lower bound result of McMullen is crucial for our computational hardness results. Let

$$
\Phi_j(v, d) = \min \{ f_j(P) : P \text{ is a } d\text{-polytope, } f_0(P) = v \}.
$$

**Theorem 2.1** [12, Thm. 2]

- $\Phi_{d-1}(d + 1, d) = d + 1$, achieved by the $d$-simplex only.
- If $d + 2 \leq v \leq \lfloor d(d + 8)/4 \rfloor$, then either
  
  (i) $\Phi_{d-1}(v, d) = d + 2$, and a $d$-polytope that achieves this must be of the form $T^{r,s,t} := a t$-fold pyramid over the cartesian product of an $r$-simplex and an $s$-simplex. Thus $v = (r + 1)(s + 1) + t$, $d = r + s + t$, $t \geq 0$, and $r, s \geq 1$, for some integers $r, s, t$ in this case.
  
  (ii) Or else, $\Phi_{d-1}(v, d) = d + 3$.

### 2.2 Face Numbers of Simplicial Polytopes

Assume that the $d$-polytope $P$ is simplicial. Then the $f$-vector and $h$-vector of $P$ determine each other by a polynomial equation in the ring $\mathbb{Z}[x]$:

$$
\sum_{i=0}^{d} f_{i-1}x^{d-i} = \sum_{i=0}^{d} h_i(x + 1)^{d-i}.
$$
Define the $g$-vector $g(P) = (g_0, \ldots, g_{\lfloor d/2 \rfloor})$ by setting $g_0 = 1$ and $g_i = h_i - h_{i-1}$ for $1 \leq i \leq d/2$. The celebrated $g$-theorem [6, 20] asserts what follows.

**Theorem 2.2** ($g$-theorem) $f = (1, f_0, \ldots, f_{d-1})$ is the $f$-vector of a simplicial $d$-polytope iff

(i) the corresponding $h$-vector satisfies Dehn–Sommerville relations: $h_i = h_{d-i}$ for all $0 \leq i \leq \lfloor d/2 \rfloor$; and

(ii) the corresponding $g$-vector is an $M$-sequence, namely $0 \leq g_i$ for all $1 \leq i \leq d/2$ and it satisfies Macaulay inequalities $g_i^{(i)} \geq g_{i+1}$ for all $1 \leq \langle i \rangle \leq \lfloor d/2 \rfloor - 1$.

See e.g. [21] for the definition of the functions $m \mapsto m^{(i)}$ and for further background on the $g$-theorem.

## 3 Reductions

Here we prove our computational hardness results, Theorems 1.3 (ii) and 1.5 (ii), via Lemmas 1.2 and 1.4, respectively. As observed in [16], plugging $v = 2d + 1$ into Theorem 2.1 gives the following, as then $d = sr$.

**Corollary 3.1** (i) If $d$ is a prime then $\Phi_{d-1}(2d + 1, d) = d + 3$.

(ii) If $d$ is the product of exactly two primes, or equals a prime cubed, then $\Phi_{d-1}(2d + 1, d) = d + 2$, achieved by a unique minimizer polytope.

(iii) If $d$ is the product of more than two primes, and not a prime cubed, then $\Phi_{d-1}(2d + 1, d) = d + 2$, and is achieved by $\lceil D/2 \rceil > 1$ minimizer polytopes, where $D$ is the number of divisors of $d$ in the interval $[2, d - 1]$. Each of these minimizers has a different number of edges, hence a different $f$-vector.

The only part of Corollary 3.1 that is not immediate from Theorem 2.1 is the claim on the different $f_1$ in (iii). However, a routine computation gives that

$$f_1(T^{r,s,t}) = d^2 + \frac{d(t + 1)}{2}$$

in this case (which is indeed an integer!), hence fixing $f_1$ determines $t$ which in turn determines $r$ and $s$ as $rs = d$ and $r + s = d - t$.

Lemma 1.2 immediately follows. Theorem 1.3 (ii) follows by plugging $a = 2d + 1$ and $b = d + 2$, and recalling that deciding if a given $d$ equals a prime cubed is polytime solvable: first one checks if $d^{1/3}$ is an integer in $O((\log d)^{1+\epsilon})$-time (for any fixed $\epsilon > 0$), see e.g. [5], and if the answer is YES, then one checks primality of $d^{1/3}$ in $O(\text{polylog}(d))$-time by [1].

To prove Lemma 1.4 we use again the expression for $f_1(T^{r,s,t})$: recall we assume that $\sqrt{d} \in [L, U]$. Note that the function $x \mapsto x + d/x$ has a unique extremal point for $x \geq 0$, which is a local minimum, at $x = \sqrt{d}$. Thus, there exists a divisor $r$ of $d$ with $L \leq r \leq U$ iff there exists $T^{r,s,t}$ with $d - t = r + s = r + d/r \in [2\sqrt{d}, M]$ for $M = M(d, L, U) := \max \{L + d/L, U + d/U\}$, equivalently with $t \in [d - M, d - 2\sqrt{d}]$. This happens, using Corollary 3.1, iff there exists a $d$-polytope $P$ with $f_0(P) = 2d + 1$, $f_{d-1}(P) = d + 2$, and $f_1(P) \in [d^2 + d(1 + d - M)/2, d^2 + d(1 + d - 2\sqrt{d})/2]$, as claimed. As before, Theorem 1.5 (ii) follows from the case $a = 2d + 1$ and $b = d + 2$. 
4 Efficient Computations for Simplicial Polytopes

Here we prove our computational efficiency results, Theorems 1.3 (i) and 1.5 (i) using the $g$-theorem. By a direct computation, the number of facets is expressed in terms of the $g$-vector as follows: for $d = 2k$ even

$$f_{d-1} = (d + 1) + (d - 1)g_1 + (d - 3)g_2 + \cdots + 3g_{k-1} + g_k,$$

and for $d = 2k + 1$ odd

$$f_{d-1} = (d + 1) + (d - 1)g_1 + (d - 3)g_2 + \cdots + 4g_{k-1} + 2g_k.$$

Now, combined with the $g$-theorem, if $f_{d-1}(P) = b \in O(d)$ then there exists a constant $C > 0$ s.t. $g_i(P) = 0$ for all $i > C$ and $0 \leq g_i(P) \leq C$ for all $0 \leq i \leq \lfloor d/2 \rfloor$; hence, there are only finitely many potential $g$-vectors to check. In each of them the Macaulay inequalities $g_i \geq g_{i+1}$ need to be checked only for $i < C$, so each such inequality is checked in constant time. Altogether, in constant time all the $g$-vectors whose $f_{d-1}$ equals $b$ are found. In particular, one checks in constant time if there exists exactly one such $g$-vector; this proves Theorem 1.3 (i).

Now, for each $g$-vector which passed the test above we compute $f_1 = g_2 + dg_1 + \binom{d+1}{2}$ in $O(\text{polylog}(d))$-time and then check whether $f_1 \in [L, U]$ in $O(\log(d))$-time, proving Theorem 1.5 (i).

5 Concluding Remarks

For fixed dimension we conjecture the following, which if correct would provide an explanation why when $d \geq 4$ the $f$-vectors of $d$-polytopes are poorly understood.

Conjecture 5.1 Let $d \geq 4$ be fixed. Then it is NP-hard to decide if a given $N$-bit vector $f = (1, f_0, \ldots, f_{d-1})$ of positive integers is the $f$-vector of a $d$-polytope.

Regarding the computational efficiency results,

Problem 5.2 Can the assumption $b \in O(d)$ in Theorems 1.3 (i) and 1.5 (i) be dropped and the same conclusions there hold?

This means $b$ would be polynomial (rather than linear) in $d$, as the entire input is of size $O(\log d)$.

Acknowledgements I deeply thank Nathan Keller for pointing me to [5] and [17], Boaz Barak and Igor Pak for helpful discussions, Guillermo Pineda-Villavicencio for helpful comments on an earlier version, and the referees for helpful comments on the presentation.

References

1. Agrawal, M., Kayal, N., Saxena, N.: PRIMES is in P. Ann. Math. 160(2), 781–793 (2004)
2. Agrawal, M., Kayal, N., Saxena, N.: Errata: PRIMES is in P. Ann. Math. 189(1), 317–318 (2019)
3. Barnette, D.: The projection of the $f$-vectors of 4-polytopes onto the $(E, S)$-plane. Discrete Math. **10**, 201–216 (1974)
4. Barnette, D., Reay, J.R.: Projections of $f$-vectors of four-polytopes. J. Combin. Theory Ser. A **15**, 200–209 (1973)
5. Bernstein, D.J.: Detecting perfect powers in essentially linear time. Math. Comp. **67**(223), 1253–1283 (1998)
6. Billera, L.J., Lee, C.W.: A proof of the sufficiency of McMullen’s conditions for $f$-vectors of simplicial convex polytopes. J. Combin. Theory Ser. A **31**(3), 237–255 (1981)
7. Cadilhac, M., Barak, B., Shor, P.: An NP-complete variant of factoring (2011). Stack Exchange. https://cstheory.stackexchange.com/questions/4769/an-np-complete-variant-of-factoring
8. Cramér, H.: On the order of magnitude of the difference between consecutive prime numbers. Acta Arith. **2**, 23–46 (1936)
9. Granville, A.: Harald Cramér and the distribution of prime numbers. Scand. Actuar. J. **1995**(1), 12–28 (1995)
10. Grünbaum, B.: Convex Polytopes. Graduate Texts in Mathematics, vol. 221. Springer, New York (2003)
11. Kusunoki, T., Murai, S.: The numbers of edges of 5-polytopes with a given number of vertices. Ann. Comb. **23**(1), 89–101 (2019)
12. McMullen, P.: The minimum number of facets of a convex polytope. J. Lond. Math. Soc. **3**, 350–354 (1971)
13. McMullen, P.: The numbers of faces of simplicial polytopes. Israel J. Math. **9**, 559–570 (1971)
14. Nevo, E.: Complexity yardsticks for $f$-vectors of polytopes and spheres. Discrete Comput. Geom. **64**(2), 347–354 (2020)
15. Pineda-Villavicencio, G., Ugon, J., Yost, D.: The excess degree of a polytope. SIAM J. Discrete Math. **32**(3), 2011–2046 (2018)
16. Pineda-Villavicencio, G., Ugon, J., Yost, D.: Lower bound theorems for general polytopes. Eur. J. Combin. **79**, 27–45 (2019)
17. Rune, Tao, T.: How hard is it to compute the number of prime factors of a given integer? (2009). MathOverflow. https://mathoverflow.net/questions/3820/how-hard-is-it-to-compute-the-number-of-prime-factors-of-a-given-integer/10062#10062
18. Sjöberg, H., Ziegler, G.M.: Semi-algebraic sets of $f$-vectors. Israel J. Math. **232**(2), 827–848 (2019)
19. Sjöberg, H., Ziegler, G.M.: Characterizing face and flag vector pairs for polytopes. Discrete Comput. Geom. **64**(1), 174–199 (2020)
20. Stanley, R.P.: The number of faces of a simplicial convex polytope. Adv. Math. **35**(3), 236–238 (1980)
21. Stanley, R.P.: Combinatorics and Commutative Algebra. Progress in Mathematics, vol. 41. Birkhäuser, Boston (1996)
22. Sudan, M.: The P vs. NP problem (2010). http://people.csail.mit.edu/madhu/papers/2010/pnp.pdf
23. Xue, L.: A proof of Grünbaum’s lower bound conjecture for general polytopes. Israel J. Math. **245**(2), 991–1000 (2021)
24. Ziegler, G.M.: Lectures on Polytopes. Graduate Texts in Mathematics, vol. 152. Springer, New York (1995)
25. Ziegler, G.M.: Face numbers of 4-polytopes and 3-spheres. In: International Congress of Mathematicians (Beijing 2002), vol. 3, pp. 625–634. Higher Ed. Press, Beijing (2002)

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.