BOLYAI SOCIETY
MATHEMATICAL STUDIES, 2

Combinatorics,
Paul Erdős is Eighty (Volume 2)
Keszthely (Hungary), 1993
Budapest, 1996, pp. 173–192.

PRIMITIVE PARTITION IDENTITIES

P. DIACONIS, R. L. GRAHAM and B. STURMFELS

Let us call a subset $A \subseteq (\mathbb{Z}^n, +)$ *primitive* if:

(i) $\sum_{a \in A} a = \overline{0}$, the all-zero vector;

(ii) If B is a nonempty proper subset of A then $\sum_{b \in B} b \neq \overline{0}$.

In general, we allow repeated elements in A and B.

In this note we investigate properties of primitive subsets of various sets in $\mathbb{Z}^n$. For example, if $A \subset \{1, \ldots, n\} \subset \mathbb{Z}$ is primitive then $|A| \leq 2n - 1$, and this is best possible. Similarly, if $A \subset \{(1, i, i^2, \ldots, i^d) : 1 \leq i \leq n\} \subset \mathbb{Z}^{d+1}$ then $|A| \leq c_d n^{\binom{d+1}{2}}$ for a suitable constant c_d depending only on d (which is also best possible up to the choice of c_d).

1. INTRODUCTION

This paper offers generalizations of the identity $1+1 = 2$. To begin, consider identities of the form $a_1 + \cdots + a_k = b_1 + \cdots + b_l$ with $0 < a_i, b_j \leq n$ and all parts integers. Such identities arise in the study of Gröbner bases, computational statistics, and integer programming as explained below. Such an identity is called *primitive* if no subset sum of terms on the left equals a subset sum of terms on the right. Thus, $1 + 1 = 2$ is primitive with largest part 2. We show that there are only finitely many primitive partition identities with largest part n. In particular, the number of terms is bounded by $k + l \leq 2n - 1$ and this is sharp.

The main results are proved for vector summands. Let $\mathcal{A}$ be a finite spanning subset of the integer lattice $\mathbb{Z}^d$. By a *partition identity with parts in $\mathcal{A}$* we mean any identity of vector sums

$$a_1 + a_2 + a_3 + \cdots + a_k \quad = \quad b_1 + b_2 + b_3 + \cdots + b_l, \tag{1.1}$$

where $a_1, \ldots, a_k, b_1, \ldots, b_l \in \mathcal{A}$ (generally not distinct). The number $k + l$ is called its *degree.* The partition identity (1.1) is called *primitive* if there is no proper subidentity

$$a_{i_1} + a_{i_2} + \cdots + a_{i_r} \quad = \quad b_{j_1} + b_{j_2} + \cdots + b_{j_s}, \tag{1.2}$$

where $1 \le r + s \le k + l - 1$. If $k = l$ then the identity (1.1) is called *homogeneous.* It is *homogeneous primitive* if, in addition, no proper subidentity (1.2) with $r = s$ exists. The homogeneous case can be reduced to the inhomogeneous case by adding an extra coordinate 1 to each vector in $\mathcal{A}$.

Our main results give bounds on the size of the set of primitive identities.

Theorem 1. *Let $\mathcal{A}$ be a spanning subset of $\mathbb{Z}^d$ of cardinality n. Let $D(\mathcal{A})$ denote the largest absolute value of the determinant of any $d \times d$-minor of the integer $n \times d$-matrix $(a : a \in \mathcal{A})$. Then any primitive partition identity (1.1) satisfies*

$$k + l \; \le \; (2d)^d (d+1)^{d+1} \cdot D(\mathcal{A}). \tag{1.3}$$

Earlier work on this problem is in Sturmfels [14] who proved $k + l \le n \cdot (n - d) \cdot D(\mathcal{A})$. This is better than (1.3) for large d, but not as effective when d is fixed and n grows. Our proof of Theorem 1 uses results of Lagarias and Ziegler [11] on lattice polytopes, and of Grinberg and Sevast'yanov [9] on the Steinitz constant of a finite-dimensional normed space. These ideas and the proof of Theorem 1 are explained in Section 3.

Theorem 1 is a general result. Specializing to the opening example, take $d = 1$ and $\mathcal{A} = \{1, 2, 3, \ldots, n\}$. Then $D(\mathcal{A}) = n$ and the bound from Theorem 1 gives $k + l \le 8n$. In Section 2 we improve this to $k + l \le 2n - 1$ and show that this is sharp. We also show that when $d = 1$ and $\mathcal{A} = \{1, 2, 3, \ldots, n\}$, any homogeneous primitive identity satisfies $k + l \le n - 1$ and this is sharp. In Section 4 we carry out a more careful study when

$$\mathcal{A} \; = \; \{(1, i, i^2, \ldots, i^d) : i = 1, 2, \ldots, n\} \; \subset \; \mathbb{Z}^{d+1}.$$

This is the classical number theory problem of multigrades. It also arises in statistical applications.

The present paper began in applied work. Three applications are described in Section 5. The first uses Theorem 1 to give a bound on the maximum degree for a universal Gröbner basis of the toric ideal generated by the set $\mathcal{A}$. The second gives an application to statistics: the primitive identities give the steps for a random walk on a class of contingency tables arising in logistic regression. The third gives an application to integer programming: the primitive partition identities give a minimal set of moves for checking feasible solutions for knapsack problems.

2. Scalar partition identities

Fix a positive integer n. A *scalar partition identity* is an identity (1.1) where a_i, b_j are integers between 1 and n. It is *primitive* if no proper subidentity (1.2) exists. To illustrate these concepts we list all primitive scalar partition identities for $n = 5$. The primitive partition identities for all smaller values of n appear in the beginning.

$1+1=2,\quad 2+2=1+3,\ 2+2+2=3+3,\ 1+2=3,\ 1+1+1=3,$
$3+3=2+4,\ 3+3+3=1+4+4,\ 3+3+3+3=4+4+4,\ 2+3=1+4,$
$2+3+3=4+4,\ 2+2=4,\ 1+3=4,\ 3+3=1+1+4,\ 1+1+2=4,$
$1+1+1+1=4,\quad 4+4=3+5,\ 4+4+4=2+5+5,$
$4+4+4+4=1+5+5+5,\quad 4+4+4+4+4=5+5+5+5,$
$3+4=2+5,\ 3+4+4=1+5+5,\ 3+4+4+4=5+5+5,\ 3+3=1+5,$
$3+3+4=5+5,\ 3+3+3=4+5,\ 3+3+3=2+2+5,\ 3+3+3+3=2+5+5,$
$3+3+3+3+3=5+5+5,\ 2+4=1+5,\ 2+4+4=5+5,\ 2+3=5,$
$2+2+4=3+5,\ 2+2+2=1+5,\ 2+2+2+4=5+5,\ 2+2+2+2=3+5,$
$2+2+2+2+2=5+5,\ 1+4=5,\ 1+3+3=2+5,\ 1+3+3+3=5+5,$
$4+4=1+2+5,\ 1+2+2=5,\ 3+4=1+1+5,\ 4+4+4=1+1+5+5,$
$1+1+3=5,\ 4+4=1+1+1+5,\ 1+1+1+2=5,\ 1+1+1+1+1=5.$

Table 1. Primitive partition identities for $n \leq 5$.

We computed this list up to $n = 13$ with the computer algebra system MACAULAY, using the technique to be described in Section 5. This computation suggested that the maximum degree should be $2n - 1$. Here is the proof of this result.

Theorem 2. *For $d = 1$ and $\mathcal{A} = \{1, 2, 3, \ldots, n\}$, any primitive partition identity (1.1) satisfies $k + l \leq 2n - 1$. This is sharp since*

$$\underbrace{n + n + n + \cdots + n}_{n-1\text{ terms}} \quad = \quad \underbrace{(n-1) + (n-1) + \cdots + (n-1)}_{n\text{ terms}}. \qquad (2.1)$$

is the unique primitive identity with $k + l = 2n - 1$.

Proof. Suppose that (1.1) is primitive. We may assume that n does not appear on the right hand side of (1.1). But it can appear on the left hand side. We run the following algorithm, starting with $x := 0$ and the multisets $\mathcal{P} := \{a_1, \ldots, a_k\}$ and $\mathcal{N} := \{b_1, \ldots, b_l\}$:

```
While P ∪ N is non-empty do
  if x ≥ 0
  then select an element ν ∈ N, set x := x − ν and N := N \ {ν}
  else select an element π ∈ P, set x := x + π and P := P \ {π}.
```

At each step in the while-loop the value of x is an integer between $1-n$ and $n-1$. Thus the total number of possible values for x is $2n-1$. Since (1.1) is primitive, no value can be attained more than once. Otherwise a proper subidentity (1.2) is created whenever a value is reached for the second time. Therefore the total number of iterations in our loop is at most $2n-1$, which proves the first part of Theorem 2.

The maximum degree $2n-1$ can be attained only if all possible values for x are attained in the above loop. We add the requirement that in each step the largest element ν in $\mathcal{N}$ or π in $\mathcal{P}$ is to be selected. Then $\pi = n-1$ in the first step. Otherwise the value $x = n-1$ will never be reached. The next time we enter the "then"-case, we must jump from $x = -1$ with $\pi = n-1$. Otherwise the value $x = n-2$ will never be reached. The next time we enter the "then"-case, we must jump from $x = -2$ with $\pi = n-1$. Otherwise the value $x = n-3$ will never be reached. Iterating this argument, we see that $b_1 = b_2 = \ldots = b_l = n-1$ and $l = n$. This proves that (2.1) is the only primitive identity of maximum degree. ■

The upper bound in Theorem 2 can be strengthened as follows:

Corollary 1. *Suppose that (1.1) is a scalar primitive partition identity when $d = 1$ and $\mathcal{A} = \{1, 2, 3, \ldots, n\}$. Then*

$$k + l \;\leq\; max\,\{a_i \,:\, i = 1, \ldots, k\} \,+\, max\,\{b_j \,:\, j = 1, \ldots, l\}.$$

Proof. Let a_{i_0} be the maximum of the a_i's and let b_{j_0} be the maximum of the b_j's. In our algorithm in the proof of Theorem 2, the value of x is always an integer between $-b_{j_0}$ and $a_{i_0} - 1$. So, the number of possible values for x equals $a_{i_0} + b_{j_0}$, which is the right hand side of the claim. ■

A *homogeneous scalar partition identity* is an identity (1.1) where $k = l$ and a_i, b_j are integers between 1 and n. It is *primitive* if no proper subidentity (1.2) with $r = s$ exists. We list all homogeneous primitive partition identities for $n \leq 6$.

Note that homogeneous primitive identities need not be primitive in the inhomogeneous sense. The identity $1+4+4 = 2+2+5$ shows this. Underlined are the four identities of maximum degree $10 = 2 \cdot 6 - 2$.

$2+2=1+3$,
$3+3=2+4$, $3+3+3=1+4+4$, $2+3=1+4$, $2+2+2=1+1+4$,
$4+4=3+5$, $4+4+4=2+5+5$, $4+4+4+4=1+5+5+5$,
$3+4=2+5$, $3+4+4=1+5+5$, $2+2+2+2=1+1+1+5$,
$2+4=1+5$, $2+2+3=1+1+5$, $1+4+4=2+2+5$, $3+3+3=2+2+5$,
$3+3=1+5$, $5+5=4+6$, $5+5+5=3+6+6$, $5+5+5+5=2+6+6+6$,
$\underline{5+5+5+5+5=1+6+6+6+6}$, $4+5=3+6$, $4+5+5=2+6+6$,
$4+5+5+5=1+6+6+6$, $4+4=2+6$, $4+4+4+4=1+3+6+6$,
$4+4+4=3+3+6$, $4+4+4+4=1+5+6$, $3+5=2+6$, $3+5+5=1+6+6$,
$3+3+4=2+2+6$, $2+5+5=3+3+6$, $\underline{4+4+4+4+4=1+1+6+6+6}$,
$2+5=1+6$, $3+3+5=1+4+6$, $3+4=1+6$, $3+3+3+5=1+1+6+6$,
$3+3+3=1+2+6$, $3+3+3+3=2+2+2+6$, $3+3+3+3=1+1+4+6$,
$\underline{3+3+3+3+3=1+1+1+6+6}$, $2+4+4=1+3+6$, $2+3+3=1+1+6$,
$2+4+4+4=1+1+6+6$, $2+2+4=1+1+6$, $2+2+2+3=1+1+1+6$,
$\underline{2+2+2+2+2=1+1+1+1+6}$, $1+5+5=2+3+6$, $1+4+5=2+2+6$,
$1+5+5+5=2+2+6+6$, $4+4+5=1+6+6$, $1+1+5+5=2+2+2+6$.

Table 2. Homogeneous primitive partition identities for $n \le 6$.

In the next table we present a count by degree of all homogeneous primitive partition identities for $n \le 12$:

degree	4	6	8	10	12	14	16	18	20	22	total #
$n=3$	1										1
$n=4$	3	2									5
$n=5$	7	7	2								16
$n=6$	13	22	12	4							51
$n=7$	22	54	36	13	2						127
$n=8$	34	118	110	54	18	6					340
$n=9$	50	230	276	155	60	23	4				798
$n=10$	70	418	646	406	182	78	24	6			1830
$n=11$	95	710	1374	965	462	207	74	25	4		3916
$n=12$	125	1150	2788	2260	1228	602	264	108	34	10	8569

Table 3. Degree distribution of homogeneous primitive partition identities

This table suggests that the maximum degree should be $2n - 2$. Here is the proof.

Theorem 3. *For $d = 2$ and $\mathcal{A} = \{(1,1),(2,1),\ldots,(n,1)\}$, any primitive partition identity (1.1) satisfies $k = l \leq n-1$. This is sharp since*

$$\underbrace{1+1+\cdots+1}_{n-2\text{ terms}} + n \quad = \quad \underbrace{2+2+\cdots+2}_{n-1\text{ terms}}$$

There are exactly $\phi(n-1)$ (the Euler phi-function) such maximal identities. For $n \geq 5$, there are $n + 2\phi(n-1) + 2\phi(n-2) - 6$ primitive identities with $k = l = n-2$.

Proof. We sort the left and right hand sides of (1.1) as follows:

$$a_1 \leq a_2 \leq a_3 \leq \ldots \leq a_k \qquad \text{and} \qquad b_1 \leq b_2 \leq b_3 \leq \ldots \leq b_k.$$

Consider the differences $\delta_i := a_i - b_i$, $i = 1,\ldots,k$. In the equation

$$\delta_1 + \delta_2 + \ldots + \delta_k \quad = \quad 0 \tag{2.2}$$

we separate the positive terms and the negative terms. The result is an inhomogeneous primitive partition identity of degree k. Let $\Delta_+ = max\{\delta_i : \delta_i > 0\}$ and $\Delta_- = max\{-\delta_j : \delta_j < 0\}$. By Corollary 1 applied to (2.2) we have $k \leq \Delta_+ + \Delta_-$.

We now choose indices i_0 and j_0 such that $b_{i_0} - a_{i_0} = \Delta_-$ and $a_{j_0} - b_{j_0} = \Delta_+$. We distinguish two cases. If $i_0 < j_0$ then

$$1 + \Delta_- \;\leq\; a_{i_0} + \Delta_- \;=\; b_{i_0} \;\leq\; b_{j_0} \;=\; a_{j_0} - \Delta_+ \;\leq\; n - \Delta_+. \tag{2.3}$$

If $i_0 > j_0$ then

$$n - \Delta_- \;\geq\; b_{i_0} - \Delta_- \;=\; a_{i_0} \;\geq\; a_{j_0} \;=\; b_{j_0} + \Delta_+ \;\geq\; 1 + \Delta_+. \tag{2.4}$$

In either case we have $\Delta_+ + \Delta_- \leq n-1$, and therefore

$$\text{degree of (1.1)} \quad = \quad 2k \quad \leq \quad 2(\Delta_+ + \Delta_-) \quad \leq \quad 2n-2. \tag{2.5}$$

This proves the first part of the claim.

To establish the second part of Theorem 3, we must characterize all primitive identities of maximal degree $2n-2$. Let $e_1, e_2, \ldots$ denote the positive δ_i's and let $f_1, f_2, \ldots$ denote the negated negative δ_i's. Thus (2.2) is written as $e_1 + e_2 + \ldots = f_1 + f_2 + \ldots$. This is a primitive identity. We apply the add-subtract algorithm from the proof of Theorem 2. Since equality holds in (2.5), the variable x must attain each integer value between

$-\Delta_-$ and $\Delta_+ - 1$ exactly once. In fact, this must be the case for <u>every</u> permutation of $e_1, e_2, \ldots$ and of $f_1, f_2, \ldots$ respectively.

We claim that $e_1 = e_2 = \ldots$ and $f_1 = f_2 = \ldots$. We assume the contrary, say $e_1 \neq e_2$. For our add-subtract algorithm we permute the e_i's so that e_2 is last and e_1 is second to last. Between the addition step with $\pi = e_1$ and the addition step with $\pi = e_2$ there may be several intermediate subtraction steps, say $\nu = f_1, f_2, \ldots, f_t$. Let $S \geq 0$ be the x-value immediately after the addition of $\pi = e_2$. At this point the variable x has visited each integer between $-\Delta_-$ and 0 and each integer between S and $\Delta_+ - 1$ exactly once, and it only has to run down from S to 0. The last negative value visited in this run equals $x = S - e_2$. We now change the positions of e_1 and e_2 in the permutation of the e_i's. Otherwise we leave the permutations untouched. Running the algorithm again, after the addition step with $\pi = e_2$ there is only one more negative value left to be visited. It is the same one as before, namely, $x = S - e_2$. Therefore we have precisely the same subtraction steps $\nu = f_1, f_2, \ldots, f_t$ between the addition of $\pi = e_2$ and the later addition of $\pi = e_1$. This implies $e_1 = e_2$ and the claim is proved.

The equations $e_1 = e_2 = \ldots$ and $f_1 = f_2 = \ldots$ show that every homogeneous primitive identity of maximum degree must have the form

$$\underbrace{1 + 1 + \cdots + 1}_{n-\ell-1 \text{ terms}} + \underbrace{n + n + \cdots + n}_{\ell \text{ terms}} = \underbrace{(\ell+1) + (\ell+1) + \cdots + (\ell+1)}_{n-1 \text{ terms}} \tag{2.6}$$

for some integer ℓ between 1 and $n-1$. The homogeneous identity (2.6) is seen to be primitive if and only if $\gcd(n-1-\ell, \ell) = 1 = \gcd(n-1, \ell)$. The number of integers ℓ with these properties equals $\phi(n-1)$, the value of the Euler phi-function. A similar (but more complicated) argument applies to give the result we state for degree $2n-4$.

We remark that the slightly more complicated construction in the first part of Theorem 3 is really needed. Direct reduction to Theorem 1 for the inhomogeneous identity (2.2) is not possible: it would give only $k \leq 2(n-1) - 1$ and hence the degree bound $2k \leq 4n - 6$, which is off by a factor of two.

The results above bound the number of terms in primitive scalar identities. It is also useful to have bounds on their number. The upper bound in the following result is due to Noga Alon.

Theorem 4. *For $d = 1$ and $\mathcal{A} = \{1, 2, 3, \ldots, n\}$, let $g(n)$ denote the number of primitive partition identities (1.1). Then there exist absolute constants*

c_1, c_2 such that

$$e^{c_1\sqrt{n}} < g(n) < e^{c_2\sqrt{n}(\log n)^{3/2}}$$

for all $n \geq 2$.

Proof. For the lower bound, any value $c_1 < \pi\sqrt{2/3}$ can be chosen since we can take all identities of the form

$$n = b_1 + b_2 + \cdots + b_r$$

where the right-hand side runs over all $p(n)$ partitions of n, and it is known that

$$p(n) \sim e^{\pi\sqrt{\frac{2n}{3}}}/4n\sqrt{3}$$

(e.g., see [12]).

For the upper bound, we give the argument of Alon. Suppose

$$a_1 + \cdots + a_r = b_1 + \cdots + b_s, 1 \leq a_i, b_j \leq n$$

is a primitive partition identity. Let $\mathcal{C}$ denote the set of *distinct* elements among the a_i and suppose $|\mathcal{C}| > c_3 n^{1/2}(\log n)^{1/2}$ for a large constant c_3. A result of Freiman [8] then implies that the set of subset sums from $\mathcal{C}$ contains, for some $d \leq 3n/|\mathcal{C}|$, a run of at least $c_4|\mathcal{C}|^2$ consecutive multiples of d centered about $1/2 \sum_{a\in\mathcal{C}} a$.

On the other hand, by grouping the b_i together in (disjoint) sets B_j where $S_j = \sum_{b\in B_j} b \equiv 0 \pmod{d}$, we see that the multi-subset sums of $b_1, b_2, \ldots$ contain $S_1, S_1 + S_2$, $S_1 + S_2 + S_3, \ldots$ (which are all multiples of d). Since $|S_i| \leq nd$ and $n < c_4|\mathcal{C}|^2 = c_4 c_3 n \log n$ for large n, then some (proper) subset sum from $\mathcal{C}$ is equal to a multi-subset sum for $\{b_1, \ldots b_s\}$, which is a contradiction to primitivity.

Thus we must have $|\mathcal{C}| \leq c_3 n^{1/2}(\log n)^{1/2}$. Since $r + s \leq 2n - 1$ then a simple calculation shows that there are at most $e^{c\sqrt{n}(\log n)^{3/2}}$ choices for the a_i and b_j, for a suitable constant c. This bound also applies to the homogeneous case (for a different value of c). ■

It would be interesting to know if $g(n) < e^{c'\sqrt{n}}$ for some constant c'.

3. Vector partition identities

In this section we consider vector partition identities with parts in an arbitrary set of lattice points. Our main result is Theorem 1. For its proof we need two lemmas. The first is a basic property of convex sets which is an easy consequence of a result due to Lagarias and Ziegler [11]. Let $\mathcal{A}$ be any spanning subset of $\mathbb{Z}^d$. We abbreviate

$$\mathcal{A}^* \quad = \quad \mathcal{A} - \mathcal{A} \quad = \quad \{\, a_i - a_j \,:\, a_i, a_j \in \mathcal{A}\},$$

and we write $\mathrm{vol}(\mathcal{A}^*)$ for the (usual d-dimensional Euclidean) volume of its convex hull.

Lemma 1. *For all finite subsets $\mathcal{A} \subset \mathbb{Z}^d$, we have the inequality*

$$\mathrm{vol}(\mathcal{A}^*) \quad \leq \quad 2^d (d+1)^{d+1}/d! \;\cdot D(\mathcal{A}). \qquad (3.1)$$

Proof. Let P and P^* denote the convex hulls of $\mathcal{A}$ and $\mathcal{A}^*$ respectively. The polytope P^* is centrally symmetric and it has dimension d. However, P may have dimension $d-1$. In that case we replace $\mathcal{A}$ by $\mathcal{A} \cup \{0\}$ to get $\dim(P) = d$ as well.

Let S be a d-simplex of maximal volume in P. Lagarias and Ziegler [11, Thm. 3] prove the following result about this simplex:

(1) The d-simplex S may be chosen to have vertices in $\mathrm{vert}(P) \subset \mathcal{A}$.

(2) After a translation we have the inclusion $P \subset d \cdot S$.

(3) After a translation we have the inclusion $-P \subset (d+2) \cdot S$.

Properties (2) and (3) imply $\mathrm{vol}(\mathcal{A}^*) = \mathrm{vol}(P^*) \leq (2d+2)^d \cdot \mathrm{vol}(S)$. Property (1) implies that S can be covered by the union of at most $d+1$ d-simplices, each having the origin as a vertex and its other d vertices in $\mathcal{A}$. Consequently $\mathrm{vol}(S)$ is bounded above by $\frac{d+1}{d!} \cdot D(\mathcal{A})$. Combining both inequalities we get (3.1). ∎

The second lemma needed for our proof of Theorem 1 is due to Grinberg and Sevast'yanov [9]. We include its proof for completeness. For other references on the Steinitz constant, the reader is referred to [2].

Lemma 2. (Grinberg and Sevast'yanov, 1980) *Let $x_1, x_2, \ldots, x_n$ be vectors in $\mathbb{R}^d$ such that $x_1 + x_2 + \ldots + x_n = 0$. Then there exists a permutation π in S_n such that*

$$x_{\pi(1)} + \cdots + x_{\pi(k)} \in d \cdot \mathrm{conv}\{x_1, x_2, \ldots, x_n\} \qquad \textit{for all } k = 1, 2, \ldots, n. \qquad (3.2)$$

Proof. We will construct a decreasing chain of index sets $\{1,2,\ldots,n\} = A_n \supset A_{n-1} \supset A_{n-2} \supset \cdots \supset A_{d+1} \supset A_d$ and numbers λ_{ik}, $k = d,\ldots,n$, $i \in A_k$ such that

$$\#(A_k)=k,\ 0\leq \lambda_{ik}\leq 1,\ \sum_{i\in A_k} \lambda_{ik}=k-d, \text{ and } \sum_{i\in A_k} \lambda_{ik}x_i=0, \text{ for all } i,k. \quad (3.3)$$

We start the construction for $k = n$ by setting $A_n := \{1,2,\ldots,n\}$ and $\lambda_{in} := (n-d)/n$ for all $i \in A_n$.

The inductive step $(k+1 \to k)$ goes as follows. Consider the convex polytope

$$P_{k+1} \;=\; \{\,(\mu_i : i \in A_{k+1}) \mid 0 \leq \mu_i \leq 1,\ \sum_{i\in A_{k+1}} \mu_i = k-d,\ \sum_{i\in A_{k+1}} \mu_i x_i = 0\,\}.$$

This polytope lies in $\mathbb{R}^{k+1}$. It is non-empty, e.g., take $\mu_i = \frac{k-d}{k+1-d}\cdot\lambda_{k+1,i}$ for $i \in A_{k+1}$. The polytope P_{k+1} lies in a subspace of dimension $\geq k-d$ inside $\mathbb{R}^{k+1}$, and inside this space it is defined by $2k+2$ linear inequalities. Let $\bar{\mu} = (\bar{\mu}_i : i \in A_{k+1})$ be any vertex of P_{k+1}. Then at least $k-d$ of the $2k+2$ inequalities $\mu_i \geq 0$ and $\mu_i \leq 1$ are binding for $\bar{\mu}$. Since $\sum_{i\in A_{k+1}} \bar{\mu}_i = k-d$, this implies that there exists an index j with $\bar{\mu}_j = 0$. We put $A_k := A_{k+1} \setminus \{j\}$ and $\lambda_{k,i} = \bar{\mu}_i$ for $i \in A_k$, which completes the inductive step.

To complete the proof of Lemma 2, we define the permutation π by requiring $\{\pi(k)\} = A_k \setminus A_{k-1}$ for $k = d+1,\ldots,n$ and $\{\pi(1),\ldots,\pi(d)\} = A_d$ in any ordering. For $k \leq d$ the desired conclusion is obvious. For $k \geq d+1$ we have

$$\sum_{i=1}^{k} x_{\pi(i)} \quad = \quad \sum_{i\in A_k} (1-\lambda_{ik})\cdot x_i \quad \in \quad d\cdot \mathrm{conv}\,\{x_1,\ldots,x_n\}$$

because $\sum_{i\in A_k}(1-\lambda_{ik}) = k-(k-d) = d$. ■

Proof of Theorem 1. The primitive partition identity (1.1) can be rewritten as

$$x_1 + x_2 + \ldots + x_{k+l} \;=\; 0 \qquad \text{with } x_i \in \mathcal{A}^*.$$

Since the identity is primitive, the partial sums $x_1 + x_2 + \ldots + x_i$ must be distinct for different values of i. After a permutation as in Lemma 2, we may assume that $x_1 + x_2 + \ldots + x_i \in d\cdot \mathrm{conv}(\mathcal{A}^*)$ for all i. Therefore the degree $k+l$ of (1.1) is bounded above by the number of lattice points in the convex polytope $d \cdot \mathrm{conv}(\mathcal{A}^*)$, which can be bounded above by $d!$ times the volume of that polytope (by a result of Blichfeldt [3]). But $\mathrm{vol}(d \cdot \mathrm{conv}(\mathcal{A}^*)) = d^d \cdot \mathrm{vol}(\mathcal{A}^*)$, and consequently Lemma 7 gives

$$k + l \le d^d d! \ \mathrm{vol}(\mathcal{A}^*) \le (2d)^d (d+1)^{d+1} D(\mathcal{A})$$

as desired. ∎

4. Multigrades

A *multigrade of type* (d,n) is a pair of multisets of non-negative integers not exceeding n, say $\{i_1, i_2, \ldots, i_k\}$ and $\{j_1, j_2, \ldots, j_k\}$, such that

$$i_1^\nu + i_2^\nu + \cdots + i_k^\nu \quad = \quad j_1^\nu + j_2^\nu + \cdots + j_k^\nu \qquad \text{for } \nu = 0, 1, 2, \ldots, d. \tag{4.1}$$

We abbreviate (4.1) by

$$i_1, i_2, \ldots, i_k \quad \stackrel{d}{=} \quad j_1, j_2, \ldots, j_k \tag{4.2}$$

The multigrade (4.2) is *primitive* if no proper sub-multisets have the same property. Here is a little example: there are precisely seven primitive multigrades for $n = 5, d = 2$.

$$1,1,1,3,3,3,3,3,3 \stackrel{2}{=} 2,2,2,2,2,2,2,2,5$$
$$1,1,3,3,3,4 \stackrel{2}{=} 2,2,2,2,2,5$$
$$1,3,3,3 \stackrel{2}{=} 2,2,2,4$$
$$1,4,4,4,4,4,4,4,4 \stackrel{2}{=} 3,3,3,3,3,3,5,5,5$$
$$1,4,4,4,4,4 \stackrel{2}{=} 2,3,3,3,5,5$$
$$1,4,4 \stackrel{2}{=} 2,2,5$$
$$2,4,4,4 \stackrel{2}{=} 3,3,3,5$$

Table 4. The seven primitive multigrades for $n = 5, d = 2$.

Multigrades of order $d = 1$ are precisely the homogeneous scalar partition identities studied in Section 2. Multigrades of any higher order fit into the general framework of Section 3: they correspond to the partition identities with parts in the set

$$\mathcal{A} \quad = \quad \mathcal{A}_{n,d} := \{(1, i, i^2, \ldots, i^d) : i = 1, 2, \ldots, n\} \subset \mathbb{Z}^{d+1}.$$

The classical results on multigrades can be found in [10]. Our main result is Theorem 5. Our proof proceeds in two parts, first the upper bound (which is now easy) and then the lower bound (which is harder).

Theorem 5. *For each integer $d \geq 0$ there exist constants c_d and $\tilde{c}_d$ (depending on d but not on n) such that*

$$c_d \cdot n^{\binom{d+1}{2}} \quad \leq k \leq \quad \tilde{c}_d \cdot n^{\binom{d+1}{2}}$$

where k denotes the maximum number of terms on each side in any primitive multigrade (4.1).

Proof (upper bound). By Theorem 1, it suffices to show that

$$D(\mathcal{A}_{n,d}) \quad \leq \quad c_d n^{\binom{d+1}{2}} \qquad \text{for some constant } c_d. \tag{4.3}$$

To see this inequality, we note that $D(\mathcal{A}_{n,d})$ is equal to

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ i_0 & i_1 & i_2 & \ldots & i_d \\ i_0^2 & i_1^2 & i_2^2 & \ldots & i_d^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ i_0^d & i_1^d & i_2^d & \ldots & i_d^d \end{vmatrix} \quad = \quad \prod_{0 \leq r < s \leq d} (i_s - i_r) \tag{4.4}$$

for some $(d+1)$-tuple of indices $1 \leq i_0 < i_1 < \ldots < i_d \leq n$. The Vandermonde determinant (4.4) clearly satisfies the inequality (4.3). ∎

Proof (lower bound). We need to exploit specific arithmetic properties of the set $\mathcal{A}_{n,d}$ for our lower bound. To begin, we require the following elementary result:

Fact. There is a function $f : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ satisfying

(i) $f(k) \leq k^3$ for all k;

(ii) All slopes determined by the points $(i, f(i)) \in \mathbb{R}^2$ are distinct.

Proof. Define $f(0) = 0$, $f(1) = 1$ and suppose $f(0), \ldots f(k-1)$ have been defined. Then $f(k) = v$ needs to be chosen so that

$$\frac{v - f(i)}{k - i} \neq \frac{f(r) - f(s)}{r - s}, \qquad 0 \leq i,\ r \neq s \leq k - 1\,.$$

Since there are fewer than k^3 choices for i, r, and s then some value for $v = f(k)$ in $\{0, \dots, k^3\}$ must be valid. ■

Assume now for convenience that $n = (d+2)N$, $N \in \mathbb{Z}$, and define

$$X_k := kN + f(k), \qquad 0 \le k \le d+1 \; .$$

We want to form a primitive multigrade of the form

$$\underbrace{X_0, \dots, X_0}_{a_0}, \underbrace{X_2, \dots, X_2}_{a_2}, \; \dots \quad \stackrel{d}{=} \quad \underbrace{X_1, \dots, X_1}_{a_1}, \underbrace{X_3, \dots, X_3}_{a_3}, \; \dots$$

where the a_i are positive integers. Now, the condition that this is a multigrade is equivalent to the set of linear equations

$$a_0 X_0^j \quad = \quad \sum_{i=1}^{d+1} (-1)^{i-1} a_i X_i^j, \quad 0 \le j \le d \; . \tag{4.5}$$

Solving this system of linear equations in $a_1, \dots, a_{d+1}$, we find by (4.4) that

$$a_k = (-1)^{k-1} \frac{P_k(X_0)}{P_k(X_k)} a_0 \tag{4.6}$$

where $P_k(x) := (X_{d+1} - x)(X_d - x) \cdots (X_{k+1} - x)(x - X_{k-1}) \cdots (x - X_1)$. Since $X_0 < X_1 < \cdots < X_{d+1}$, all the a_k are positive if a_0 is.

We now fix d and consider N very large. The basic idea will be to show that the integers $P_k(X_0)$ and $P_k(X_k)$ have relatively small gcd's, as do $P_k(X_k)$ and $P_l(X_l)$, so that a_0 must be very large if each a_k is to be integer. Now,

$$\begin{aligned} & \gcd(X_i - X_j, X_k - X_l) \\ \le \;& \gcd((k-l)(X_i - X_j), (i-j)(X_k - X_l)) \\ = \;& \gcd((k-l)(X_i - X_j) - (i-j)(X_k - X_l), (i-j)(X_k - X_l)) \\ = \;& \gcd((k-l)(f(i) - f(j)) - (i-j)(f(k) - f(l)), (i-j)(X_k - X_l)) \; . \end{aligned}$$

By the definition of f,

$$(k-l)(f(i) - f(j)) - (i-j)(f(k) - f(l)) \neq 0 \; .$$

Thus,

$$\gcd(X_i - X_j, X_k - X_l) \le |(k-l)(f(i) - f(j)) - (i-j)(f(k) - f(l))| \le d^4 \tag{4.7}$$

for $i \neq j$, $k \neq l$. Let

$$x_{k,i} := (X_k - X_i)/\gcd(X_k - X_i,\ P_k(X_0)), \quad \text{for } i < k\ .$$

By (4.7) we have

$$x_{k,i} \geq (X_k - X_i)/d^{4d}\ . \tag{4.8}$$

Since each $x_{k,i}$ divides a_0 and

$$\gcd(x_{k,i}, x_{l,j}) \leq \gcd(X_k - X_i, X_l - X_j) \leq d^4 \text{ for } i \leq k, j \leq l, (i,k) \neq (j,l)$$

by (4.7), we conclude by (4.8) that

$$\begin{aligned} a_0 &\geq \prod_{1\leq i<j\leq d+1} x_{j,i}/d^{4\binom{d+1}{2}} \\ &\geq \prod_{1\leq i<j\leq d+1} (X_j - X_i)/(d^{4d})^{\binom{d+1}{2}} \cdot d^{4\binom{d+1}{2}} \\ &\geq d^{-2d(d+1)^2} \prod_{1\leq i<j\leq d+1} \left((j-i)\frac{n}{d} + f(i) - f(j)\right) \\ &\geq \widehat{c}_d n^{\binom{d+1}{2}} \end{aligned} \tag{4.9}$$

for a suitable constant $\widehat{c}_d$. Finally, we choose for a_0 the *smallest* positive value so that all the a_k are integers. Thus, the corresponding multigrade will be primitive, which shows by (4.9) that

$$\sum_{i=0}^{d+1} a_i \quad > \quad a_0 \quad \geq \quad \widehat{c}_d n^{\binom{d+1}{2}}$$

and the theorem is proved. ■

In view of the lower bound in Theorem 5, it is natural to wonder whether the analogous lower bound holds even in the general situation of Theorem 1. The subsequent remark shows that this is not the case: the upper bound $\gamma_d \cdot D(\mathcal{A})$ is best possible for multigrades (of fixed order d) but is not best possible for general sets $\mathcal{A}$.

Remark. There does not exist any constant c_d such that, for all finite subsets $\mathcal{A}$ of $\mathbb{Z}^d$ there is a primitive partition identity of degree $\geq c_d \cdot D(\mathcal{A})$.

Proof. Let $d = 1$. Linearly order the set of all prime numbers $p_1 < p_2 < p_3 < p_4 < \ldots$, and set $p^{(n)} := p_1 p_2 \cdots p_n$. Let $\mathcal{A}^{(n)} = \{a_1, a_2, \ldots, a_n\} \subset \mathbb{Z}$ where $a_i = p^{(n)}/p_i$. The only primitive partition identities in this case are

$$\underbrace{a_i + a_i + \cdots + a_i}_{p_i \text{ summands}} = \underbrace{a_j + a_j + \cdots + a_j}_{p_j \text{ summands}}. \tag{4.10}$$

Then the maximum degree of a primitive partition identity is $p_n + p_{n-1}$ while $D(\mathcal{A}^{(n)}) = p^{(n)}/p_1 = p_2 p_3 \cdots p_n$. The ratio $D(\mathcal{A}^{(n)})/(p_n + p_{n-1})$ is unbounded as $n \to \infty$. ■

5. Applications

In this section we present applications of our combinatorial results to questions in Gröbner bases theory, in statistics, and integer programming. These applications are interconnected by the sampling algorithms introduced in [6], and the Gröbnerian methods for integer programming introduced in Conti & Traverso [4] and Thomas [15].

5.A. Gröbner bases. This subsection addresses readers who are interested in computational commutative algebra. We assume familiarity with Gröbner bases and toric ideals; see [5], [7], [14] and the references given therein. We fix an n-element set of lattice points $\mathcal{A} = \{a_1, \ldots, a_n\}$ in $\mathbb{Z}^d$, and we introduce indeterminates $t_1, \ldots, t_d, x_1, \ldots, x_n$. Each point $a_i = (a_{i1}, a_{i2}, \ldots, a_{id})$ is identified with a Laurent monomial $\mathbf{t}^{a_i} := t_1^{a_{i1}} \cdots t_d^{a_{id}}$. Given any field K, we consider the K-algebra homomorphism

$$\begin{aligned} \phi \; : \; K[x_1, x_2, \ldots, x_n] &\to K[t_1, \ldots, t_d, t_1^{-1}, \ldots, t_d^{-1}] \\ x_i &\mapsto \mathbf{t}^{a_i} = t_1^{a_{i1}} t_2^{a_{i2}} \cdots t_d^{a_{id}}. \end{aligned} \tag{5.1}$$

The kernel of ϕ is denoted $I_\mathcal{A}$ and called the *toric ideal* associated with $\mathcal{A}$. It is well known (see e.g. [14, Lemma 2.5]) that $I_\mathcal{A}$ is spanned as a K-vector space by all binomials of the form

$$x_{i_1} x_{i_2} \cdots x_{i_k} - x_{j_1} x_{j_2} \cdots x_{j_l} \quad \text{where} \quad a_{i_1} + \cdots + a_{i_k} = a_{j_1} + \cdots + a_{j_k}. \tag{5.2}$$

In other words, the toric ideal $I_\mathcal{A}$ is spanned by all (binomially coded) partition identities with parts in $\mathcal{A}$. The following proposition is proved in [7]. Slightly different but essentially equivalent variants can be found in [14, Cor. 2.6] and [15, Thm. 3.2.3].

Proposition 1. (cf. [7]) *The set of binomial relations (5.1) arising from primitive partition identities is a universal Gröbner basis for the toric ideal $I_\mathcal{A}$.*

From Theorem 1 we get the following corollary.

Corollary 2. *For each integer d there exists a constant γ_d, depending only on $d = \dim(I_{\mathcal{A}})$, such that every reduced Gröbner basis of $I_{\mathcal{A}}$ has degree at most $\gamma_d \cdot D(\mathcal{A})$.*

Here $\dim(I_{\mathcal{A}})$ denotes Krull dimension of the residue ring $K[x_1, \dots, x_n]/I_{\mathcal{A}}$. The bound in Corollary 2 is better than the bound in Proposition 1 in the sense that it does not depend on n, the embedding dimension of the toric variety defined by $I_{\mathcal{A}}$. The statement becomes even more succinct when formulated for projective toric varieties. By a *projective toric variety* we will here mean an irreducible projective variety $X = X_{\mathcal{A}}$ in P^{n-1} whose homogeneous vanishing ideal is of the form $I_{\mathcal{A}}$. (For experts in algebraic geometry we note that such toric varieties X need not be normal.) Clearly, generators of homogeneous toric ideals correspond to homogeneous partition identities.

Corollary 3. *The maximum degree in any reduced Gröbner basis of the ideal of a projective toric variety X is bounded by* $\deg(X) \cdot \gamma(\dim(X))$, *for some function* $\gamma : \mathbb{N} \to \mathbb{N}$.

Corollary 3 follows from Theorem 1, Lemma 1, and the well-known fact that $\deg(X)$, the degree of X, is equal to the normalized volume of the polytope $P = \mathrm{conv}(\mathcal{A})$.

A projective toric variety of dimension 1 is called a *monomial curve.* For curves we have the following bound. Note that this bound is tight for all rational normal curves.

Corollary 4. *The maximum degree in any reduced Gröbner basis of the ideal of a monomial curve X is bounded above by the degree of X.*

Proof. Theorem 2 and Proposition 1 give the upper bound for the rational normal curve of degree $n-1$ in P^{n-1}. Every monomial curve X is obtained from a rational normal curve by a degree-preserving coordinate projection. Hence the upper bound for general X follows by the elimination property of the universal Gröbner basis. ■

5.B. Statistics. Another motivation for the study of the partition identities considered here comes from a problem in applied statistics. The statistical problem is called *binary logistic regression.* It involves fitting curves to predict binary outcomes based on an observable vector of covariates. The models are of the form

$$\begin{aligned} P\{Y = 1 \mid z\} &= e^{\theta \cdot z}/(1 + e^{\theta \cdot z}) \\ P\{Y = 0 \mid z\} &= 1/(1 + e^{\theta \cdot z}) \,. \end{aligned} \tag{5.3}$$

In (5.3), $\theta \in \mathbb{R}^d$ is a parameter to be estimated, and $z \in \mathbb{Z}^d$ is a known vector. As an example, if $z = (1, j)$, the model becomes

$$P\{Y = 1 \,|\, j\} \quad \propto \quad e^{\theta_1 + j\theta_2} .$$

This might be appropriate if the probability depends on a distance, dose or educational level, which arises in equally spaced intervals.

Going back to generalities, data consists of pairs (y_1, z_1),$(y_2, z_2), \ldots$, (y_N, z_N). Let

$$W(z) := |\{i : z_i = z\}|, \quad W_1(z) := |\{i : z_i = z, y_i = 1\}| .$$

The chance of seeing such data is

$$\begin{aligned} P\{Y_i = y_i, 1 \le i \le N \,|\, z_i, 1 \le i \le N\} &= \prod_i \frac{e^{\theta \cdot z_i y_i}}{(1 + e^{\theta \cdot z_i y_i})} \\ &= \left\{ \prod_z \frac{1}{(1 + e^{\theta \cdot z})^{W(z)}} \right\} e^{\theta \cdot \sum_z z W_1(z)} \end{aligned}$$

From this description we see that a sufficient statistic for θ is

$$\{W(z)\}_{z \in \mathbb{Z}} \quad \text{and} \quad t_1 = \sum_z z W_1(z) .$$

We will assume a fixed finite $\mathcal{A} \subset \mathbb{Z}^d$ such that all covariates z lie in $\mathcal{A}$. Set $n = \#(\mathcal{A})$. Data from these problems usually are summarized as a $2 \times n$-array

$$\begin{array}{c} \\ 0 \\ \\ 1 \end{array} \overset{\mathcal{A}}{\begin{pmatrix} W_0(z_1) \; W_0(z_2) \cdots W_0(z_n) \\ \\ W_1(z_1) \; W_1(z_2) \cdots W_1(z_n) \end{pmatrix}} \tag{5.4}$$

For inference, the task becomes one of generating random arrays with the same row and column sums, and the same value of $t_1 = \sum_z z W_1(z)$. Note that this automatically fixes $t_0 = \sum_z z W_0(z)$.

A *partition identity* based on $\mathcal{A}$ is of the form

$$z_1 + \cdots + z_k = z_1'' + \cdots + z_l', \qquad z_i, z_i' \in \mathcal{A} \tag{5.5}$$

Such an identity is *primitive* if no proper subset sum of terms on the left-hand side equals a sum of terms on the right-hand side. The sum $k + l$ is called the *degree* of the identity (5.5). It is not regarded as fixed.

Let $\mathcal{G}(\mathcal{A})$ be the set of primitive partition identities based on $\mathcal{A}$. This gives a set of steps with which to run a random walk. The random walks takes values on the space of all tables with fixed values of $\{W(z)\}_{z\in\mathcal{A}}$ and $t_1 = \sum_z zW_1(z)$. If the walk is currently at the table x, it proceeds by picking an identity in $\mathcal{G}(z)$ at random (uniformly), choosing one of the two sides (left and right) at random with probability 1/2. Then $W_1(z) \to W_1(z) - 1$ for each z on the left-hand side, and $W_1(z) \to W_1(z) + 1$ for each z on the right-hand side. The counts $W_0(z)$ are then adjusted to preserve the column sums. If all these adjustments result in a table with nonnegative entries satisfying the constraints, the walk moves to the new table. If not, the walk stays at x.

In [6] it is shown that this walk is connected and aperiodic, and so converges to the uniform distribution on the space of tables. Modifications, similar to the Metropolis algorithm, are provided for generation using other classical distributions on the space of tables. It follows from [6, Corollary 4.2] and the results in [7] that this walk remains connected even if structural zeros are prescribed.

The present paper gives bounds on the maximum degree of any such identity. Obviously, such bounds are crucial to implementation. Further details and examples can be found in [6].

5.C. Integer Programming. We consider the following family of knapsack problems:

$$\begin{aligned} &\text{Minimize} \sum_{j=1}^{n} c_j \cdot x_j \\ &\text{subject to} \sum_{j=1}^{n} j \cdot x_j = \beta,\ x_i \text{ integral and } 0 \le x_i \le d_i \text{ for } i = 1, \dots, n, \end{aligned} \tag{5.6}$$

where $c_1, \dots, c_n, d_1, \dots, d_n$ and β are parameters ranging over the positive integers. A feasible solution $(x_1, \dots, x_n)$ to an instance of (5.6) can be written as a pair of partitions:

$$\begin{array}{ccc} \text{inside the knapsack} & & \text{outside the knapsack} \\ \underbrace{1,1,\dots,1}_{x_1}\,\underbrace{2,2,\dots,2}_{x_2}\dots\underbrace{n,n,\dots,n}_{x_n} & \Big| & \underbrace{1,1,\dots,1}_{d_1-x_1}\,\underbrace{2,\dots,2}_{d_2-x_2}\dots\underbrace{n,\dots,n}_{d_n-x_n} \end{array} \tag{5.7}$$

Each scalar partition identity (1.1) gets directed by the cost functional $(c_1, \dots, c_n)$ via

$$a_1, a_2, a_3, \cdots, a_k \to b_1, b_2, b_3, \cdots, b_l \text{ whenever } c_{a_1} + \cdots + c_{a_k} > c_{b_1} + \cdots + c_{b_l}, \tag{5.8}$$

provided lexicographic tie breaking is used if a tie occurs. We say that (5.7) *can be improved along* (5.8) if $a_1, a_2, \cdots, a_k$ appear on the left side ("inside the knapsack") and $b_1, b_2, \cdots, b_k$ appear on the right side ("outside the knapsack"). In this case the feasible solution (5.7) can be improved by the exchange step (5.8). We claim that the primitive scalar partition identities are a *universal test set* for the general knapsack problem (5.6).

Corollary 5. *Let the c_i, d_i and β be arbitrary integers. A feasible solution (5.7) to (5.6) is <u>not</u> optimal if and only it can be improved along some <u>primitive</u> partition identity.*

Corollary 5 is an immediate consequence of Proposition 1 and the known identification (see [4], [15]) of Gröbner bases for toric ideals and test sets for integer programs. For general background on test sets in integer programming see also [13, §17.3].

REFERENCES

[1] N. Alon, (personal communication).

[2] W. Banaszczyk, A note on the Steinitz constant of the Euclidean plane, *C. R. Math. Rep. Acad. Sci. Canada* **12**(1990), 97–102.

[3] H. F. Blichfeldt, Notes on geometry of numbers, *Bull. Amer. Math. Soc.* **27**(1921), 150–153.

[4] P. Conti ,and C. Traverso, Buchberger algorithm and integer programming, in: *Proceedings AAECC-9 (New Orleans),* Springer LNCS **539**(1991), 130–139.

[5] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms,* Springer-Verlag, New York, 1993.

[6] P. Diaconis and B. Sturmfels, Algebraic algorithms for sampling from conditional distributions, to appear in *Annals of Statistics.*

[7] B. Sturmfels and R. Thomas, Variations of cost functions in integer programming, Manuscript, 1994.

[8] G. A. Freiman, New analytical results in subset-sum problem, *Discrete Math.* **114**(1993), 205–218.

[9] V. S. Grinberg and S. V. Sevast'yanov, Value of the Steinitz constant, *Functional Analysis Appl.* **14**(1980), 125–126.

[10] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* Oxford Univ. Press, London, 4th ed., 1960.

[11] J. C. Lagarias and G. M. Ziegler, Bounds for lattice polytopes containing a fixed number of interior points in a sublattice, *Canadian J. Math.* **43**(1991), 1022–1035.

[12] H. Rademacher, On the partition function, *Proc. London Math. Soc.* **43**(1937), 241–254.

[13] A. Schrijver, *Theory of Linear and Integer Programming,* Wiley-Interscience, 1986.

[14] B. Sturmfels, Gröbner bases of toric varieties, *Tôhoku Math. J.* **43**(1991), 249–261.

[15] R. Thomas, A geometric Buchberger algorithm for integer programming, *Mathematics of Operation Research* **20**(1995), 864–884.

P. Diaconis
Harvard University,
Cambridge, MA 02138
USA

R. L. Graham
AT&T Bell Laboratories,
Murray Hill, NJ 07974
USA

e-mail: `rlg@research.att.com`

B. Sturmfels
University of California,
Berkeley, CA 97420
USA