AAECC 2, 55–79 (1991)

AAECC
Applicable Algebra in Engineering, Communication and Computing

On the Number of Term Orders*

Gunter Ritter and Volker Weispfenning

Fakultät für Mathematik und Informatik der Universität, W-8390 Passau, Federal Republic of Germany

Received October 11, 1990; revised version February 15, 1991

Abstract. By an admissible order on a finite subset Q of $\mathbb{Q}^n$ we mean the restriction to Q of a linear order on $\mathbb{Q}^n$ compatible with the group structure of $\mathbb{Q}^n$ and such that $\mathbb{N}^n$ is contained in the positive cone of the order. We first derive upper and lower bounds on the number of admissible orders on a given set Q in terms of the dimension n and the cardinality of Q. Better estimates are possible if the set Q enjoys symmetry properties and in the case where Q is a discrete hyperbox of the form $\prod_{k=1}^{n} [1, d_k]$. In the latter case, we also give asymptotic results as $\min_{1 \leqq k \leqq n} d_k \to \infty$ for fixed n. We finally present algorithms which compute the set of admissible orders that extend a given binary relation on Q and their number. The algorithms are useful in connection with the construction of universal Gröbner bases.

Keywords: Term order, Separating hyperplane, Gröbner basis, Universal Gröbner basis

1. Introduction

During the last years, the method of Gröbner bases (cf. Buchberger [2]) has been well established as one of the most useful and versatile tools in the algorithmic theory of polynomial ideals and of polynomial equations. Let $R = K[X_1, \ldots, X_n]$ be a multivariate polynomial ring over a field K. The construction of a Gröbner basis $G \subseteq R$ from a finite set F of polynomials in R depends in an essential way on a term order $<$ on the set T of terms (i.e., power products of the indeterminates $X_1, \ldots, X_n$) in R. On the one hand, the complexity of the construction of G from F is crucially influenced by the choice of the order $<$ to the extent that computation

* AMS Classification: primary 06F20
secondary 06-04, 11N25

times may vary between a few minutes and several days. On the other hand, many applications of Gröbner bases require a specific (e.g. lexicographic) term order that may be a bad choice from the point of view of complexity. This raises the problem of choosing an appropriate term order for every given input F and the given application.

Whereas there are a continuum of different such term orders $<$ (cf. Robbiano [8] or Weispfenning [12]) every single Gröbner basis construction uses only the restriction of $<$ to a *finite* set T' of terms involved in the construction. In fact, T' depends only on the order $<$, the number n of indeterminates, and the finite set $T(F)$ of terms occurring in the polynomials of the set F. The restriction of $<$ to T' can be conveniently described by a linear form with positive rational coefficients (see Subsect. 2.3).

In fact, there is a much stronger result (cf. Schwartz [9], Weispfenning [13], Mora and Robbiano [7]), viz.: For given n and $T(F)$ there are finitely many rational linear forms describing partial term orders such that any Gröbner basis calculation from F with respect to an arbitrary term order $<$ is identical with a Gröbner basis computation from F with respect to one of these partial term orders. As a consequence, one can construct from F a *universal* Gröbner basis, i.e., a finite set $G \subseteq R$ that is a Gröbner basis for *all* term orders on T. The crux of this construction is the following problem:

Given a finite set T' of terms, determine a set $LF(T')$ of rational linear forms that make up a system of distinct representatives for all restrictions to T' of term orders on T.

The solution of this problem is also of interest from the point of view of combinatorial geometry: Notice that a term $t = X_1^{e_1} \cdot \cdots \cdot X_n^{e_n} \in T$ is determined by its n-tuple $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{N}^n$ of exponents and any term order $<$ on T induces a linear order $\prec$ on $\mathbb{N}^n$ with least element $\mathbf{0}$; we will call these orders on $\mathbb{N}^n$ *admissible*. Now, any nonzero linear form $\mathbf{a} = (a_1, \ldots, a_n)$ $(a_i \in \mathbb{Q})$ on the space $\mathbb{Q}^n$ partitions $\mathbb{Q}^n$ into a hyperplane and two halfspaces. Let us call the halfspace $H_{\mathbf{a}} = \{\mathbf{x} \in \mathbb{Q}^n : \mathbf{a} \cdot \mathbf{x} > 0\}$ the *positive halfspace* associated with $\mathbf{a}$. Given a subset Q of $\mathbb{N}^n$ (Q corresponds to the set T' above), we call two linear forms $\mathbf{a} \neq \mathbf{0}$ and $\mathbf{b} \neq 0$ whose associated hyperplanes intersect $Q - Q := \{\mathbf{y} - \mathbf{x} : \mathbf{x}, \mathbf{y} \in Q\}$ at the origin only *equivalent with respect to Q* if

$$(Q - Q) \cap H_{\mathbf{a}} = (Q - Q) \cap H_{\mathbf{b}}.$$

Let LF_n denote the set of all linear forms in n variables with positive, rational coefficients. We will show that the original problem above is equivalent to the following problem of *combinatorial geometry*:

Let Q be a finite subset of $\mathbb{N}^n$. Determine a subset $LF_n(Q)$ of LF_n that forms a system of distinct representatives for LF_n with respect to the above equivalence relation induced by Q.

In more intuitive terms the problem is to determine all different "cuts" of $Q - Q$ induced by hyperplanes H with $H \cap (Q - Q) = \{0\}$ that are represented by linear forms in LF_n.

The present paper is divided into two parts where we deal with the following two problems.

1. We compute upper and lower bounds on the number $LF(T')$.
2. We describe algorithms for computing $LF(T')$ from n and T'.

In the first, analytical, part we actually deal with the more general situation where Q is a finite, nonempty subset of $\mathbb{Q}^n$ (Sect. 4); in the second, algorithmic, part we treat the even more general case where additional side conditions are specified (Sect. 5). Our main technique is an inductive step that reduces the n-dimensional problem to one in $n-1$ dimensions (Proposition 2.8). A different approach appears in Schwarz [10].

In the analytical part we use this step recursively to derive first an *upper* bound for the number $\alpha(Q)$ of distinct representatives in terms of $\#Q$ and the dimension n; it is given in Theorem 4.6. For a general set Q the only *lower* bound in these terms is 1 (cf. the remark preceding Lemma 4.7). We therefore restrict matters to Cartesian products of one-dimensional, point-symmetric sets in this case and derive lower bounds in terms of the cardinalities of the *factors* and the dimension n.

More precise estimates are possible in the case of an n-dimensional lattice hyperbox $Q = \prod_{i=1}^{n} [1, d_i]$ $(d_i \geqq 2)$. For $M \subseteqq \{1, \ldots, n\}$, $\#M = r$, let $\varphi(r, \mathbf{d}_M)$ be the number of relatively prime n-tuples in the discrete hyperbox $\prod_{i \in M} [1, d_i]$. We derive upper and lower bounds for $\alpha(Q)$ in terms of the numbers $\varphi(r, \mathbf{d}_M)$ $(M \subseteqq \{1, \ldots, n\})$ and the dimension n (Theorem 4.13 and Lemma 4.10(c)). Using the asymptotic result for $\varphi(n, \mathbf{d})$ given in Proposition 3.2 we also obtain asymptotic results for $\alpha(Q)$ as $\min_{1 \leqq k \leqq n} d_k \to \infty$, n fixed (Theorem 4.15). Here, the Riemann ζ-function plays a certain rôle.

In the algorithmic part we will deal with the following situation: Besides the finite subset Q of $\mathbb{Q}^n$ let there be given a binary relation $\mathscr{C}$ on Q. Then the algorithms will determine a set of linear forms on $\mathbb{Q}^n$ that uniquely represent all admissible extensions of $\mathscr{C}$ on Q.

This is exactly the problem that arises in any construction of a universal Gröbner basis G when one attempts to generate the necessary partial term orders efficiently: Indeed, during the construction of G, the finite set T' of terms on which one wants to determine all term orders will grow, say, from T' to T''. Instead of recomputing the term orders on T'' from scratch it is more efficient to find all extensions of the term orders on T' since these have already been computed.

The corresponding problem for the exponents reads as follows: Suppose we are given finite subsets $Q \subset \tilde{Q}$ of $\mathbb{Q}^n$ and a set LF of distinct representatives in $\mathscr{L}(Q)$ of $\Pi(Q)$ (cf. Subsect. 2.3). Compute from LF a set of distinct representatives $LF^{\sim}$ in $\mathscr{L}(\tilde{Q})$ for $\Pi(\tilde{Q})$. Using our more general algorithms, this problem can be solved in the following manner: For a linear form $\mathbf{a} \in LF$, let $\mathscr{C}_{\mathbf{a}}$ be the admissible order on Q induced by the linear form $\mathbf{a}$. Then it suffices to determine for each $\mathbf{a} \in LF$ a set $LF_{\mathbf{a}}$ of linear forms on $\mathbb{Q}^n$ that uniquely represent all admissible extensions of $\mathscr{C}_{\mathbf{a}}$ on $\tilde{Q}$ and to define $LF^{\sim}$ as the union of all these sets $LF_{\mathbf{a}}$.

2. Term Orders and Admissible Orders

2.1 Explanations. Let $R = K[X_1, \ldots, X_n]$ be the polynomial ring in n indeterminates $X_1, \ldots, X_n$ over a field K. A *term* in R is a power product $t = X_1^{e_1} \cdots X_n^{e_n}$

($e_i \in \mathbb{N}$) of the n indeterminates. The set T of all terms forms a monoid under multiplication with neutral element $1 = X_1^0 \cdots X_n^0$. A *term order* $<$ on the set T is a linear order that turns T into an ordered monoid with smallest element 1. In other words, $<$ is a linear order on T such that, for all $s, t, u \in T$, we have

(i) $1 \leqq s$,

(ii) $s < t \Rightarrow s \cdot u < t \cdot u$.

By passing to exponents any term order can be regarded as a linear order $\prec$ on the additive monoid $\mathbb{N}^n$ satisfying the conditions

(iii) $\mathbf{0} \leqq \mathbf{x}$,

(iv) $\mathbf{x} \prec \mathbf{y} \Rightarrow \mathbf{x} + \mathbf{z} \prec \mathbf{y} + \mathbf{z}$

for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{N}^n$.

Any such order has a unique extension to a linear order on the additive groups $\mathbb{Z}^n$ and $\mathbb{Q}^n$ satisfying the conditions

(v) $\mathbf{0} \leqq \mathbf{x}$ for all $\mathbf{x} \in \mathbb{Q}_+^n := \{(y_1, \ldots, y_n) \in \mathbb{Q}^n : y_k \geqq 0 \ (1 \leqq k \leqq n)\}$,

(vi) $\mathbf{x} \prec \mathbf{y} \Rightarrow \mathbf{x} + \mathbf{z} \prec \mathbf{y} + \mathbf{z}$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{Q}^n$.

We shall call these orders on $\mathbb{Z}^n$ and $\mathbb{Q}^n$ *admissible.*

2.2 Representation of Admissible Orders by Linear Forms. By the results in [8] and [12], admissible orders on $\mathbb{Q}^n$ can be characterized by linear forms: Let $S = \mathbb{R}[Z]$ be the ordered polynomial ring over $\mathbb{R}$ in the indeterminate Z ordered in such a way that $r < Z$ for all $r \in \mathbb{R}$. Then any n-tuple $\mathbf{a} = (a_1, \ldots, a_n) \in S^n$ with (strictly) positive and rationally independent entries a_i induces an admissible order $\prec$ on $\mathbb{Q}^n$ in the following way:

(i) $\mathbf{x} \prec \mathbf{y} \Leftrightarrow \mathbf{a} \cdot \mathbf{x} < \mathbf{a} \cdot \mathbf{y} \quad (x, y \in \mathbb{Q}^n)$,

where $\mathbf{a} \cdot \mathbf{x} = \sum_{i=1}^{n} x_i a_i \quad (\in S) \quad (\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Q}^n)$ and on the right hand side the order is taken in S. Conversely, any admissible order on S is induced by such a linear form. Moreover, the mapping $\mathbb{Q}^n \to S$ defined by $\mathbf{x} \to \mathbf{a} \cdot \mathbf{x}$ is an embedding of the admissibly ordered group $\mathbb{Q}^n$ into the ordered polynomial ring S. In particular, $\mathbb{Q}^n$ and $\mathbf{a} \cdot \mathbb{Q}^n = \{\mathbf{a} \cdot \mathbf{x} : \mathbf{x} \in \mathbb{Q}^n\}$ are isomorphic *qua* linearly ordered groups.

2.3 Characterization of Finite Restrictions of Admissible Orders by Positive Blocks. We will deal with restrictions of admissible orders to *finite, nonempty* subsets Q of $\mathbb{Q}^n$. We refer to such a restriction as an *admissible order on* Q and denote the set of all admissible orders on Q by $\mathscr{A}(Q)$. By the results in [7] and [12], any admissible order on a finite subset Q of $\mathbb{Q}^n$ is characterized as above in 2.2(i) by a linear form $\mathbf{a} = (a_1, \ldots, a_n)$ on $\mathbb{Q}^n$ with (*strictly*) *positive, rational* coefficients a_i satisfying the condition of weak independence $\mathbf{a} \cdot \mathbf{z} \neq 0$ for all $\mathbf{0} \neq \mathbf{z} \in Q - Q$. We denote the set of these linear forms $\mathbf{a}$ by $\mathscr{L}(Q)$. Similarly as in 2.2, any linear form $\mathbf{a} \in \mathscr{L}(Q)$ induces an embedding $Q \ni \mathbf{x} \to \mathbf{a} \cdot \mathbf{x} \in \mathbb{Q}$ of the linearly ordered set Q into the ordered group $\mathbb{Q}$. In particular, the admissibly ordered set Q is isomorphic with its image $\mathbf{a} \cdot Q = \{\mathbf{a} \cdot \mathbf{x} : \mathbf{x} \in Q\} \subseteqq \mathbb{Q}$.

For a linear form $\mathbf{a} \in \mathscr{L}(Q)$ let $H_{\mathbf{a}}$ be the open, positive half space $\{\mathbf{x} \in \mathbb{Q}^n : \mathbf{a} \cdot \mathbf{x} > 0\}$. For any finite, nonempty subset Q of $\mathbb{Q}^n$ and any linear form $\mathbf{a} \in \mathscr{L}(Q)$ we define the *positive block* $\pi_{\mathbf{a}}(Q) \subseteqq Q - Q$ as the intersection

$\pi_{\mathbf{a}}(Q) = (Q-Q) \cap H_{\mathbf{a}}$, that is,

$$\pi_{\mathbf{a}}(Q) = \{\mathbf{z} \in Q - Q : \mathbf{a} \cdot \mathbf{z} > 0\};$$

we denote the set of all these positive blocks by $\Pi(Q)$. Notice that

$\{\pi_{\mathbf{a}}(Q), -\pi_{\mathbf{a}}(Q), \{0\}\}$ is a partition of $Q - Q$.

We will repeatedly use the following elementary properties of $\mathbf{a} \in \mathscr{L}(Q)$ and $\pi_{\mathbf{a}}(Q)$, sometimes without mentioning:

(a) If $Q_0 \subseteq Q$ then $\mathbf{a} \in \mathscr{L}(Q_0)$.
(b) If $\bar{Q} \supseteq Q$ is finite then $\mathbf{a} \in \mathscr{L}(Q)$ can be modified to $\bar{\mathbf{a}} \in \mathscr{L}(\bar{Q})$ in such a way that $\pi_{\bar{\mathbf{a}}}(Q) = \pi_{\mathbf{a}}(Q)$.

(First represent $\pi_{\mathbf{a}}$ by a linear form with rationally independent coefficients and then approximate it by a linear form $\bar{\mathbf{a}} \in \mathscr{L}(\bar{Q})$ with the same positive block in $Q - Q$.).

2.4 Proposition. *For any positive block $\pi \in \Pi(Q)$ let $\prec_\pi$ be the binary relation on Q defined by $\mathbf{x} \prec_\pi \mathbf{y} \Leftrightarrow \mathbf{y} - \mathbf{x} \in \pi$; for any admissible order $\prec$ on Q let $\pi_\prec$ be the subset of $Q - Q$ defined by $\pi_\prec = \{\mathbf{y} - \mathbf{x} : \mathbf{x}, \mathbf{y} \in Q, \mathbf{x} \prec \mathbf{y}\}$. Then we have*
(a) $\prec_\pi \in \mathscr{A}(Q)$ and $\pi_\prec \in \Pi(Q)$.
(b) The maps $\Pi(Q) \to \mathscr{A}(Q)$ and $\mathscr{A}(Q) \to \Pi(Q)$ defined by $\pi \to \prec_\pi$ and $\prec \to \pi_\prec$, respectively, are mutually inverse bijections.

Proof. Any positive block $\pi \in \Pi(Q)$ is of the form $\pi = \pi_{\mathbf{a}}(Q)$ for some linear form $\mathbf{a} \in \mathscr{L}(Q)$. It follows from 2.2(i) that the relation $\prec_\pi$ is the admissible order on Q induced by this linear form, hence $\prec_\pi \in \mathscr{A}(Q)$. On the other hand, any order $\prec \in \mathscr{A}(Q)$ is induced by a linear form $\mathbf{a} \in \mathscr{L}(Q)$. Then, by the definition of $\pi_\prec$ and by 2.2(i), we have $\pi_\prec = \pi_{\mathbf{a}}(Q) \in \Pi(Q)$. In order to show Part (b), notice that any admissible order on Q represented by the linear form $\mathbf{a}$ is determined by the positive block $\pi_{\mathbf{a}}(Q)$. Using this fact it is now easy to see that the two maps are mutually inverse. □

2.5 Projections of Admissible Orders. Let the projection $\mathbb{R}^n \to \mathbb{R}^{n-1}$ of an n-tuple onto its first $(n-1)$ coordinates be denoted by a prime, i.e., $(a_1, \ldots, a_n)' = (a_1, \ldots, a_{n-1})$. The objective of this section is to determine, from any finite subset Q of $\mathbb{Q}^n$, a finite subset Q^* of $\mathbb{Q}^{n-1}$ such that, roughly speaking, any admissible order on Q can be reconstructed in a perspicuous way from its projection regarded as an admissible order on the projection Q' of Q on $\mathbb{Q}^{n-1}$. Recall from 2.3 that, for any linear form $\mathbf{a} \in \mathscr{L}(Q)$, $\pi_{\mathbf{a}}(Q)$ denotes its positive block in $Q - Q$. Central to our investigation are the two subsets Q_1, Q_2 of $\mathbb{Q}^{n-1}$ defined for any finite subset $Q \subseteq \mathbb{Q}^n$ as follows:

$$Q_1 = \{\mathbf{z}' : \mathbf{z} \in Q - Q, z_n = 0\}$$

$$Q_2 = \left\{ \frac{\mathbf{z}'}{z_n} : \mathbf{z} \in Q - Q, z_n \neq 0 \right\}.$$

Notice that Q_1 is always symmetric in the sense that $-Q_1 = Q_1$ and that $\mathbf{0} \in Q_1$, while Q_2 and $-Q_2$ may differ.

For any finite subset $R \subseteq \mathbb{Q}^{n-1}$ and any linear form $\mathbf{c}$ on $\mathbb{Q}^{n-1}$ we put as before $\mathbf{c} \cdot R = \{\mathbf{c} \cdot \mathbf{u} : \mathbf{u} \in R\}$. If $\mathbf{d}$ is another linear form on $\mathbb{Q}^{n-1}$ we will say that $a \in \mathbb{R}$ and

$b \in \mathbb{R}$ *realize corresponding cuts* in $\mathbf{c} \cdot R$ and $\mathbf{d} \cdot R$, respectively, if

$$a \notin \mathbf{c} \cdot R, \quad b \notin \mathbf{d} \cdot R \quad \text{and}$$
$$\mathbf{c} \cdot \mathbf{u} > a \Leftrightarrow \mathbf{d} \cdot \mathbf{u} > b \quad (\mathbf{u} \in R).$$

2.6 *Lemma. Let Q be a finite subset of $\mathbb{Q}^n$ and let $a_i, b_i > 0$ $(1 \leqq i \leqq n)$. The following are eqivalent:*

(a) $\mathbf{a}, \mathbf{b} \in \mathscr{L}(Q)$ *and* $\pi_{\mathbf{a}}(Q) = \pi_{\mathbf{b}}(Q)$;
(b) $(\mathbf{a} \cdot (\mathbf{y} - \mathbf{x}))(\mathbf{b} \cdot (\mathbf{y} - \mathbf{x})) > 0$ *for all* $\mathbf{x}, \mathbf{y} \in Q$, $\mathbf{x} \neq \mathbf{y}$;
(c) (i) $(\mathbf{a}' \cdot \mathbf{u})(\mathbf{b}' \cdot \mathbf{u}) > 0$ *for all* $\mathbf{u} \in Q_1 \setminus \{\mathbf{0}\}$ *and*
(ii) $(\mathbf{a}' \cdot \mathbf{v} + a_n)(\mathbf{b}' \cdot \mathbf{v} + b_n) > 0$ *for all* $\mathbf{v} \in Q_2$;
(d) (iii) *the origin* $0 \in \mathbb{R}$ *realizes corresponding cuts in the sets* $\mathbf{a}' \cdot (Q_1 \setminus \{0\})$ *and* $\mathbf{b}' \cdot (Q_1 \setminus \{0\})$,
(iv) *the numbers* $-a_n$ *and* $-b_n$ *realize corresponding cuts in the sets* $(\mathbf{a}' \cdot Q_2)$ *and* $(\mathbf{b}' \cdot Q_2)$.

Proof. The equivalence of (a) and (b) is plain and (iii) and (iv) are just reformulations of the analytic expressions (i) and (ii), respectively. In order to prove the implication (b)$\Rightarrow$(c) let $\mathbf{u} \in Q_1$, $\mathbf{u} \neq \mathbf{0}$ be given by $\mathbf{u} = (\mathbf{y} - \mathbf{x})'$ with $\mathbf{x}, \mathbf{y} \in Q$, $\mathbf{x} \neq \mathbf{y}$ and $x_n = y_n$. Then $\mathbf{a}' \cdot \mathbf{u} = \mathbf{a} \cdot (\mathbf{y} - \mathbf{x})$ and $\mathbf{b}' \cdot \mathbf{u} = \mathbf{b} \cdot (\mathbf{y} - \mathbf{x})$ and (i) ensues from (b). Next, let $\mathbf{v} \in Q_2$ be given by $\mathbf{v} = \mathbf{z}'$,

$$\mathbf{z} = \left(\frac{\mathbf{y}' - \mathbf{x}'}{y_n - x_n}, 1 \right),$$

where $\mathbf{x}, \mathbf{y} \in Q$ and $x_n \neq y_n$. Dividing (b) by $(y_n - x_n)^2$ we immediately obtain $(\mathbf{a}' \cdot \mathbf{v} + a_n)(\mathbf{b}' \cdot \mathbf{v} + b_n) = (\mathbf{a} \cdot \mathbf{z})(\mathbf{b} \cdot \mathbf{z}) > 0$, i.e., (ii).

Let us now prove the opposite implication (c)$\Rightarrow$(b) and let $\mathbf{x}, \mathbf{y} \in Q$, $\mathbf{x} \neq \mathbf{y}$. If $x_n = y_n$, then $\mathbf{u} = (\mathbf{y} - \mathbf{x})' \in Q_1 \setminus \{0\}$, and so, by (i), $(\mathbf{a} \cdot (\mathbf{y} - \mathbf{x}))(\mathbf{b} \cdot (\mathbf{y} - \mathbf{x})) = (\mathbf{a}' \cdot \mathbf{u})(\mathbf{b}' \cdot \mathbf{u}) > 0$. If $x_n \neq \mathbf{y}_n$ put $\mathbf{z} = \left(\frac{\mathbf{y}' - \mathbf{x}'}{y_n - x_n}, 1 \right)$; then $\mathbf{v} = \mathbf{z}' \in Q_2$, and so, by (ii), $(\mathbf{a} \cdot \mathbf{z})(\mathbf{b} \cdot \mathbf{z}) = (\mathbf{a}' \cdot \mathbf{v} + a_n)(\mathbf{b}' \cdot \mathbf{v} + b_n) > 0$; after multiplication by $(y_n - x_n)^2$ we obtain again $(\mathbf{a} \cdot (\mathbf{y} - \mathbf{x})) \cdot (\mathbf{b} \cdot (\mathbf{y} - \mathbf{x})) > 0$. □

2.7. Notations. *For any finite subset $Q \subseteqq \mathbb{Q}^n$, Q^* will stand for the union*

$$Q^* = Q_1 \cup Q_2$$

and for any subset M of $\mathbb{R}$, $M_- = \{m \in \mathbf{M} : m < 0\}$ denotes the strictly negative part of M.

The following basic proposition reduces any admissible order on Q to an admissible order on Q^* induced by some linear form $\mathbf{c} \in \mathscr{L}(Q^*)$ and a cut in the finite subset $(\mathbf{c} \cdot Q_2)_- \subseteqq \mathbb{Q}$. It is the key to all main results in this paper. If $\mathbf{a} = (a_1, \ldots, a_{n-1}) \in \mathbb{Q}^{n-1}$ and $b \in \mathbb{Q}$ then $\mathbf{a} * b$ stands for the concatenation $(a_1, \ldots, a_{n-1}, b) \in \mathbb{Q}^n$.

2.8 Proposition. *Let Q be a finite subset of $\mathbb{Q}^n$ and let $\mathbf{c}_i \in \mathscr{L}(Q^*)$ $(1 \leqq i \leqq m)$ be complete in $\mathscr{L}(Q^*)$* in the following sense:

(i) $\{\pi_{\mathbf{c}_1}(Q^*), \ldots, \pi_{\mathbf{c}_m}(Q^*)\} = \Pi(Q^*)$.

Realize every cut S_{ij} in $(\mathbf{c}_i \cdot Q_2)_-$ $(0 \leqq j \leqq \#(\mathbf{c}_i \cdot Q_2)_-)$ by a negative, rational number $-d_{ij}$ and put $\mathbf{d}_{ij} = \mathbf{c}_i * d_{i,j}$. Then

(a) $\mathbf{d}_{ij} \in \mathscr{L}(Q)$ *and*

(b) $\{\pi_{\mathbf{d}_{ij}}(Q): 1 \leqq i \leqq m,\ 0 \leqq j \leqq \#(\mathbf{c}_i \cdot Q_2)_-\} = \Pi(Q)$.

Proof. (a) is a consequence of Lemma 2.6, (d)$\Rightarrow$(a) with $\mathbf{a} = \mathbf{b} = \mathbf{d}_{ij}$. It remains to show that for any $\pi \in \Pi(Q)$ there exist two indices $1 \leqq i \leqq m$, $0 \leqq j \leqq \#(\mathbf{c}_i \cdot Q_2)_-$, such that $\pi_{\mathbf{d}_{ij}}(Q) = \pi$. By 2.3, we may assume that $\pi = \pi_{\mathbf{a}}(Q)$ for some linear form $\mathbf{a} \in \mathscr{L}(Q \cup Q^* \times \{0\})$ (cf. 2.3(b)). Since $\mathbf{a}' \in \mathscr{L}(Q^*)$ and by Hypothesis (i), there exists some i, $1 \leqq i \leqq m$, such that $\pi_{\mathbf{c}_i}(Q^*) = \pi_{\mathbf{a}'}(Q^*)$. Recall that $\mathbf{0} \in Q_1$. Since $\mathbf{a}', \mathbf{c}_i \in \mathscr{L}(Q_1)$, no $\mathbf{u} \in Q_1 \setminus \{0\}$ is annihilated by $\mathbf{a}'$ or $\mathbf{c}_i$ and since $\pi_{\mathbf{a}'}(Q_1) = \pi_{\mathbf{c}_i}(Q_1)$, we have $\mathbf{a}' \cdot \mathbf{u} > 0 \Leftrightarrow \mathbf{c}_i \cdot \mathbf{u} > 0$ $(\mathbf{u} \in Q_1,\ \mathbf{u} \neq 0)$; i.e., 2.6(iii) is satisfied with $\mathbf{b}' = \mathbf{c}_i$. On the other hand, since $\mathbf{a}', \mathbf{c}_i \in \mathscr{L}(Q_2 \cup \{0\})$,both maps

$$(Q_2 \cup \{0\}, <_{\mathbf{a}'}) \ni \mathbf{u} \to \mathbf{a}' \cdot \mathbf{u} \in \mathbf{a}' \cdot (Q_2 \cup \{0\}) \quad \text{and}$$
$$(Q_2 \cup \{0\}, <_{\mathbf{c}_i}) \ni \mathbf{u} \to \mathbf{c}_i \cdot \mathbf{u} \in \mathbf{c}_i \cdot (Q_2 \cup \{0\})$$

are order isomorphisms, where $<_{\mathbf{a}'}$ and $<_{\mathbf{c}_i}$ stand for the orders on $Q_2 \cup \{0\}$ induced by $\mathbf{a}'$ and $\mathbf{c}_i$, respectively. Since $\pi_{\mathbf{a}'}(Q_2 \cup \{0\}) = \pi_{\mathbf{c}_i}(Q_2 \cup \{0\})$, these orders on $Q_2 \cup \{0\}$ coincide and the map

$$\mathbf{a}' \cdot (Q_2 \cup \{0\}) \ni \mathbf{a}' \cdot \mathbf{u} \to \mathbf{c}_i \cdot \mathbf{u} \in \mathbf{c}_i \cdot (Q_2 \cup \{0\}), \tag{1}$$

too, is an order isomorphism. By Lemma 2.6, applied to $\mathbf{b} = \mathbf{a}$, we see that $-a_n$ realizes a cut in the set $\mathbf{a}' \cdot Q_2$. Hence there exists j such that $-a_n$ and $-d_{ij}$ realize corresponding cuts in $\mathbf{a}' \cdot Q_2$ and $\mathbf{c}_i \cdot Q_2$, respectively. We have now established 2.6(d) for the linear forms $\mathbf{a}$ and $\mathbf{b} = \mathbf{d}_{ij}$; thus 2.6(a) is satisfied, i.e., we have $\pi_{\mathbf{d}_{ij}}(Q) = \pi_{\mathbf{a}}(Q) = \pi$. □

3. The Number of Relatively Prime Lattice Points

3.1 Historical Remarks and Notations. In our asymptotic analysis of the number of term orders we shall need upper and lower bounds on the number $\varphi(n, d)$ $(n \geqq 2)$ of *relatively prime* n-tupels $\mathbf{x}$ in the lattice hypercube $[1, d]^n$ as $d \to \infty$. For $n = 2$, a slightly modified problem was treated for the first time by Dirichlet [3]. Dirichlet was interested in the number $\psi(d)$ of relatively prime pairs in the triangular lattice $\{(x, y) \in \mathbb{Z}^2 : 1 \leqq x \leqq d,\ 1 \leqq y \leqq x\}$; he showed, that

$$2\psi(d) - \frac{d^2}{\zeta(2)} = 0(d^\gamma) \quad (d \to \infty),$$

where $\zeta(\alpha) = \sum_{m=1}^{\infty} m^{-\alpha}$ $(\alpha > 1)$ is the Riemann ζ-function and γ is the solution of $\zeta(\gamma) = 2$. (γ is a real number strictly between $\frac{3}{2}$ and 2.) Mertens [6], Problem 1, sharpened Dirichlet's result by proving

$$\left| 2\psi(d) - \frac{d^2}{\zeta(2)} \right| < d(\ln d + C + \tfrac{5}{4}) + 2. \tag{1}$$

Here and in the sequel, $C = \lim_{m\to\infty}\left(\sum_{k=1}^{m}\frac{1}{k} - \ln m\right) = 0.57721\ldots$ is Euler's constant. Of course, since there are no relatively prime pairs on the diagonal of the square $[1,d]^2$ other than $(1,1)$, the relation between $\psi(d)$ and $\varphi(2,d)$ is given by

$$2\psi(d) = \varphi(2,d) + 1. \tag{2}$$

We now state and prove an analogue of Mertens' result for n-dimensional lattice hyperboxes. For integers $d \leqq e$ we let $[d,e]$ denote the discrete interval $\{x\in\mathbb{Z}: d \leqq x \leqq e\}$ and for $\mathbf{d} = (d_1,\ldots,d_n), \mathbf{e} = (e_1,\ldots,e_n)\in\mathbb{Z}^n$, where $d_i \leqq e_i (1 \leqq k \leqq n)$, $[\mathbf{d},\mathbf{e}]$ denotes the n-dimensional *lattice hyperbox* $[\mathbf{d},\mathbf{e}] = \prod_{i=1}^{n}[d_i,e_i]$. $\varphi(n,\mathbf{d})$ stands for the number of relatively prime n-tuples in the discrete hyperbox $[\mathbf{1},\mathbf{d}]$.

The proof of Part (a) of the following proposition is as in Mertens, loc.cit.; cf. also Knuth [5], Exercise 10, pp. 337 and 595. For the reader's convenience we reproduce it here. $\mu:\mathbb{N}\to\{-1,0,1\}$ is the *Möbius function*, i.e., $\mu(k) = 0$ if k is divisible by a prime square, and $\mu(k) = (-1)^r$ if k is the product of r distinct primes; in particular, $\mu(1) = (-1)^0 = 1$. $[\ ]$ denotes the integer part of a real number.

3.2 Proposition. *We have for* $n \geqq 1$

(a) $\varphi(n,\mathbf{d}) = \sum_{k=1}^{\min d_i}\mu(k)\prod_{i=1}^{n}\left[\frac{d_i}{k}\right]$;

(b) $\varphi(1,\mathbf{d}) = 1$,

$$\left|\varphi(n,\mathbf{d}) - \frac{\prod_i d_i}{\zeta(n)}\right| < \begin{cases} 2\max_i d_i\left(\ln\min_i d_i + C - \frac{1}{2} + \frac{1}{\min_i d_i}\right) & (n=2), \\ \frac{\prod_i d_i}{\min_i d_i}\left(n(\zeta(n-1)-1) + \frac{1}{(n-1)(\min_i d_i)^{n-2}}\right) & (n\geqq 3); \end{cases}$$

in particular, for each $n \geqq 1$, we have

(c) $\frac{\varphi(n,\mathbf{d})}{\prod_i d_i} \to \frac{1}{\zeta(n)}$ as $\min_i d_i \to \infty$.

Proof. In order to prove Part (a) let, for any finite set R of prime numbers, D_R be the set of n-tupels $\mathbf{x}\in[\mathbf{1},\mathbf{d}]$ such that all x_j are divisible by all primes in R; of course, $D_\varnothing = [\mathbf{1},\mathbf{d}]$. Furthermore, let

$$\phi(n,\mathbf{d}) = \{\mathbf{x}\in[\mathbf{1},\mathbf{d}]: x_1,\ldots,x_n \text{ relatively prime}\}$$

be the set of all $\mathbf{x} = (x_1,\ldots,x_n)$ in the considered hyperbox such that the only common divisor of $x_1,\ldots,x_n$ is 1. Then $\varphi(n,\mathbf{d}) = \#\phi(n,\mathbf{d})$ and

$$\phi(n,\mathbf{d}) = [1,\mathbf{d}] \Big/ \bigcup_{p\,\text{prime}} D_{\{p\}};$$

hence, by Sylvester–Poincaré's sieve formula, we have

$$\varphi(n,\mathbf{d}) = \prod_i d_i - \#\bigcup_{p\,\text{prime}} D_{\{p\}} = \sum_R (-1)^{\#R}\#D_R. \tag{1}$$

Now note that $(-1)^{\#R} = \mu(\alpha_R)$ and $\#D_R = \prod_i \left[\frac{d_i}{\alpha_R}\right]$, where α_R is the product of the primes in R ($\alpha_\varnothing = 1$). Part (a) now ensues from (1).

To obtain the estimate in (b) we start with the identity

$$\sum_{k \geqq 1} \frac{\mu(k)}{k^n} = \frac{1}{\zeta(n)} \tag{2}$$

(cf. Titchmarsh [11], Formula 1.1.4) and use (a) to write

$$\begin{aligned} \left|\varphi(n, \mathbf{d}) - \frac{\prod d_i}{\zeta(n)}\right| &= \left|\sum_{k=1}^{\min d_i} \mu(k) \prod_i \left[\frac{d_i}{k}\right] - \left(\prod_i d_i\right) \sum_{k \geqq 1} \mu(k) \frac{1}{k^n}\right| \\ &= \left|\sum_{k=2}^{\min d_i} \mu(k) \prod_i \left[\frac{d_i}{k}\right] - \left(\prod_i d_i\right) \sum_{k \geqq 2} \mu(k) \frac{1}{k^n}\right| \\ &\leqq \left|\sum_{k=2}^{\min d_i} \left(\prod_i \left[\frac{d_i}{k}\right] - \prod_i \frac{d_i}{k}\right)\right| + \left(\prod_i d_i\right) \sum_{k > \min d_i} \frac{1}{k^n}. \end{aligned} \tag{3}$$

The first summand on the right side of (3) is majorized by

$$\begin{aligned} &\sum_{k=2}^{\min d_i} \left(\prod_i \frac{d_i}{k} - \prod_i \left[\frac{d_i}{k}\right]\right) \\ &= \sum_{k=2}^{\min d_i} \sum_{j=1}^{n} \left(\frac{d_j}{k} - \left[\frac{d_j}{k}\right]\right) \left(\prod_{i=1}^{j-1} \left[\frac{d_i}{k}\right]\right) \prod_{i=j+1}^{n} \frac{d_i}{k} \\ &\leqq n \cdot \frac{\prod d_i}{\min d_i} \sum_{k=2}^{\min d_i} \frac{1}{k^{n-1}} \\ &< \begin{cases} 2 \max d_i \left(\ln \min d_i + C - 1 + \dfrac{1}{\min d_i}\right) & (n = 2), \\ n(\zeta(n-1) - 1) \dfrac{\prod d_i}{\min d_i} & (n \geqq 3). \end{cases} \end{aligned} \tag{4}$$

For the last term on the right side of (3) we use the estimate

$$\sum_{k > a} \frac{1}{k^n} < \int_a^\infty \frac{dx}{x^n} = \frac{1}{(n-1)a^{n-1}} \tag{5}$$

valid for all integers $a \geqq 1$. This concludes the proof of Part (b) and Part (c) ensues from it. □

In the special case of a lattice hyper*cube* $[1, d]^n$ ($d \geqq 1$) the estimates given in Proposition 3.2 can be improved. We formulate this as

3.3 Proposition. *Let $n \geqq 2$ and $d \geqq 1$. For the number $\varphi(n, d)$ of relatively prime*

n-tupels in the discrete hypercube $[1,d]^n$ *we have the estimate*

$$\left|\left(\varphi(n,d)-\frac{d^n}{\zeta(n)}\right)+\frac{n}{2}(\varphi(n-1,d)-d^{n-1})\right|<\begin{cases} d(\ln d+C)+1 & (n=2),\\ \dfrac{n}{2}(\zeta(n-1)-1)d^{n-1}+\dfrac{d}{n-1} & (n\geqq 3).\end{cases}$$

Proof. Applying Identity 3.2(2) again we have

$$\begin{aligned}(1)\qquad &\left|\left(\varphi(n,d)-\frac{d^n}{\zeta(n)}\right)+\frac{n}{2}(\varphi(n-1,d)-d^{n-1})\right|\\ &=\left|\sum_{k=2}^{d}\mu(k)\left(\left[\frac{d}{k}\right]^n-\left(\frac{d}{k}\right)^n+\frac{n}{2}\left[\frac{d}{k}\right]^{n-1}\right)-\sum_{k>d}\mu(k)\left(\frac{d}{k}\right)^n\right|\\ &\leqq\sum_{k=2}^{d}\left|\left[\frac{d}{k}\right]^n-\left(\frac{d}{k}\right)^n+\frac{n}{2}\left[\frac{d}{k}\right]^{n-1}\right|+d^n\sum_{k>d}\frac{1}{k^n}.\end{aligned}$$

In order to estimate the first term on the right side of (1) we use the convex inequality

$$\beta^n-\alpha^n=n\int_{\alpha}^{\beta}x^{n-1}dx\leqq\frac{n}{2}(\beta-\alpha)(\beta^{n-1}+\alpha^{n-1}),$$

valid for all real numbers $n\geqq 2$, $0\leqq\alpha\leqq\beta$, and infer from $0\leqq\frac{d}{k}-\left[\frac{d}{k}\right]<1$

$$\left|\left[\frac{d}{k}\right]^n-\left(\frac{d}{k}\right)^n+\frac{n}{2}\left[\frac{d}{k}\right]^{n-1}\right|\leqq\frac{n}{2}\left(\frac{d}{k}\right)^{n-1}.$$

Therefore, the first term on the right side of (1) is majorized by

$$(2)\qquad \frac{n}{2}d^{n-1}\sum_{k=2}^{d}\frac{1}{k^{n-1}}\leqq\begin{cases} d\left(\ln d+C-1+\dfrac{1}{d}\right) & (n=2),\\ \dfrac{n}{2}(\zeta(n-1)-1)d^{n-1} & (n\geqq 3).\end{cases}$$

The estimates (1), (2), and 3.2(5), now imply the proposition. □

Summarizing the results of Propositions 3.2 ($n\geqq 3$) and 3.3 ($n=2$) we obtain in the case of a lattice hypercube the following

3.4 Corollary.

$$\left|\varphi(n,d)-\frac{d^n}{\zeta(n)}\right|<\begin{cases} d(\ln d+C+1) & (n=2),\\ n(\zeta(n-1)-1)d^{n-1}+\dfrac{d}{n-1} & (n\geqq 3).\end{cases}$$

3.5. Discussion. (a) For a hypercube of dimension $n\geqq 3$ sharper estimates than those given in 3.4 can be derived from Proposition 3.3, at least for large values of d; e.g., the coefficient of d^{n-1} in the bound for $\left|\varphi(n,d)-\frac{d^n}{\zeta(n)}\right|$ is no greater than $\frac{n}{2}\left(\frac{1}{\zeta(n-1)}+\zeta(n-1)\right)$.

(b) In the case $n=2$, the estimates given in Proposition 3.3 is slightly sharper than Mertens' estimate 3.1(1). Indeed, by 3.1(2), we have

$$\left|2\psi(d)-\frac{d^2}{\zeta(2)}\right| \leqq \left|\varphi(2,d)+1-\frac{d^2}{\zeta(2)}\right| = \left|\varphi(2,d)+\varphi(1,d)-\frac{d^2}{\zeta(2)}\right|$$
$$< d(\ln d + C + 1) + 1.$$

(c) The asymptotic in 3.2(c) also holds if $\varphi(n,\mathbf{d})$ is interpreted as the number of relatively prime lattice points in a shifted hyperbox $\mathbf{x}+[1,\mathbf{d}]$, where the x_i's are nonnegative integers.

(d) The results in this section can be given a *probabilistic interpretation*, viz.: If one conducts n independent Laplace experiments by picking random integers $X_1 \in [1,d_1],\ldots,X_n\in[1,d_n]$ then the probability of obtaining a relatively prime n-tupel $(X_1,\ldots,X_n)$ is, asymptotically as $\min_i d_i \to \infty$, $\frac{1}{\zeta(n)}$. Indeed, by independence and since the random integers $X_1,\ldots,X_n$ are uniformly distributed on $[1,d_1],\ldots,[1,d_n]$, respectively, the joint random lattice point $(X_1,\ldots,X_n)\in[\mathbf{1},\mathbf{d}]$, too, is uniformly distributed on $[\mathbf{1},\mathbf{d}]$, i.e. the probability of relative primitivity of $(X_1,\ldots,X_n)$ is given by the relative frequency $\frac{\#\phi(n,\mathbf{d})}{\#[\mathbf{1},\mathbf{d}]}=\frac{\varphi(n,\mathbf{d})}{\prod_i d_i}$. Similar statements are true also for other distributions on $\mathbb{Z}^n$ than the uniform distribution on $[1,\mathbf{d}]$ but we shall not go into details here.

(e) Let $(d_i)_{i\geqq 1}$ be *any* sequence of integers $\geqq 2$ and let $(X_i)_{i\geqq 1}$ be an independent sequence of uniformly distributed random integers $X_i:(\Omega,P)\to[1,d_i]$. For each prime factor p of X_1 there is P-a.s. an index $i\geqq 2$ such that p does not divide X_i; i.e., P-almost surely, the sequence (X_i) does not possess a common prime factor. Moreover, since $n(\zeta(n)-1)=0(2^{-n})$, Proposition 3.2(b) provides the asymptotic result

$$\left|P[(X_1,\ldots,X_n) \text{ is relatively prime}]-\frac{1}{\zeta(n)}\right| = 0(2^{-n}).$$

4. Upper and Lower Bounds for the Number of Term Orders

We combine now the results of Sects. 2 and 3 to give proofs of the main results stated in Sect. 1. For any finite subset $Q\subseteqq\mathbb{Q}^n$, we denote by $\alpha(Q)$ the *number of admissible orders* on Q. We need the following special classes of subsets Q of $\mathbb{Q}^n$.

4.1 Definition. *We call the set Q point symmetric if*

$$Q=-Q$$

and we call Q symmetric with respect to all coordinates, if

$$(x_1,\ldots,-x_i,\ldots,x_n)\in Q$$

for all $(x_1,\ldots,x_i,\ldots,x_n)\in Q$ and all indices i.

4.2 Remarks. (a) Symmetry with respect to all coordinates is inherited by Q_1, Q_2, and a fortiori, by Q^* from Q.
(b) If Q is symmetric with respect to all coordinates then Q is also point symmetric.

We first deal with upper estimates and infer from Proposition 2.8 the following reductive step.

4.3 Corollary. *Assume* $\#Q \geqq 2$.
(a) *We have* $\alpha(Q) \leqq \alpha(Q^*)\,(\#Q_2 + 1)$.
(b) *If* Q_2 *is point symmetric then we have* $\alpha(Q) \leqq \alpha(Q^*)\left(\left[\frac{\#Q_2}{2}\right] + 1\right)$.

Proof. By Proposition 2.8 and with the notation there we have at most as many admissible orders on Q as there are n-tuples $\mathbf{d}_{ij}$. But the number of cuts in $(\mathbf{c}_i \cdot Q_2)_-$ is at most $(\#Q_2 + 1)$ in the general case and at most $\left[\frac{\#Q_2}{2}\right] + 1$ if Q_2 is point symmetric. □

We next estimate the cardinalities of Q_1, Q_2, and Q^*. As in 2.5, Q' denotes the projection of $Q \subseteq \mathbb{R}^n$ to $\mathbb{R}^{n-1}$.

4.4 Lemma. (a) $\#Q_1 \leqq \#Q'(\#Q' - 1) + 1$;
(b) $\#Q_2 \leqq \binom{\#Q}{2}$;
(c) $\#Q^* \leqq \binom{\#Q}{2} + \binom{\#Q'}{2} + 1 \leqq \#Q(\#Q - 1) + 1$.

Proof. Claim (a) is obvious. In order to prove Claims (b) and (c) let $I_1 = \{(\mathbf{x}, \mathbf{y}) \in Q^2 : x_n = y_n\}$ and $I_2 = \{(\mathbf{x}, \mathbf{y}) \in Q^2 : x_n \neq y_n\}$. The obvious surjection $I_2 \to Q_2$ maps the two elements $(\mathbf{x}, \mathbf{y}), (\mathbf{y}, \mathbf{x}) \in \mathbf{I}_2$ to the same element in Q_2, whence we have

$$\#I_2 \geqq 2\#Q_2 \tag{1}$$

and Claim (b).

The obvious surjection $I_1 \to Q_1$ maps all $\#Q$ elements of the diagonal of Q^2 to the zero vector, hence we have

$$\#I_1 \geqq \#Q_1 + \#Q - 1. \tag{2}$$

Noting that Q^2 is the disjoint union of I_1 and I_2 and using (a), (2), and (1), we finally obtain

$$\begin{aligned} 2\#Q^* \leqq 2\#Q_1 + 2\#Q_2 &\leqq \#Q'(\#Q' - 1) + 1 + \#I_1 - \#Q + 1 + \#I_2 \\ &= \#Q'(\#Q' - 1) + \#Q(\#Q - 1) + 2, \end{aligned}$$

i.e., Estimate (c). □

4.5 Sharpness of the Estimates in Lemma 4.4. In order to assess sharpness of the estimates in Lemma 4.4 we let $u_0 < \cdots < u_{q-1}$ be a rationally independent q-tupel of real numbers. Then, by rational independence, all differences $u_j - u_i$ $(i \neq j)$ are

pairwise different; moreover all quotients

$$\frac{u_j - u_i}{3^k - 3^h} \quad (j > i, k > h)$$

are pairwise different: If $\frac{u_s - u_r}{3^w - 3^v} = \frac{u_j - u_i}{3^k - 3^h}$ $(s > r,\ w > v)$ then, again by rational independence, we must have $s = j$ and $r = i$ and hence $3^w - 3^v = 3^k - 3^h$. But each integer has a unique representation as a linear combination of powers 3^i with coefficients in the set $\{\pm 1, 0\}$. It follows that we have also $w = k$ and $v = h$. Now approximate $(u_0, \ldots, u_{q-1})$ by a q-tupel $(\bar{u}_0, \ldots, \bar{u}_{q-1})$ of *rational* numbers so that the differences $\bar{u}_j - \bar{u}_i$ and the quotients $(\bar{u}_j - \bar{u}_i)/(3^k - 3^h)$ are still pairwise different and consider $n = 2$ and the set $Q = \{\bar{u}_0, \ldots, \bar{u}_{q-1}\} \times \{1, 3, 3^2, \ldots, 3^{q-1}\} \subseteqq \mathbb{Q}^2$. In this case, $\#Q = q^2$, $\#Q' = q$ and, as shown above, $\#Q_1 = q(q-1)+1$ and $\#Q_2 = 2\binom{q}{2}^2 + 1$; thus the coefficients of the highest powers of q in $\#Q_1$, $\#Q_2$, and $\#Q^*$ coincide with those in the estimates of 4.4. This example can be extended to n dimensions with the same sharpness of bounds.

4.6 Theorem. *Let $n \geqq 1$ and let $Q \subseteqq \mathbb{Q}^n$ be finite and such that $\#Q \geqq 2$.*

(a) *We have* $\alpha(Q) \leqq \dfrac{(\#Q)^{2^n - 2}}{2^{n-1}}$.

(b) *If, in addition, Q is symmetric with respect to all coordinates then*

$$\alpha(Q) \leqq \frac{(\#Q)^{2^n - 2}}{4^{n-1}}.$$

Proof. We proceed by induction on n and prove first Part (a). Note that 4.4(b) and $\#Q \geqq 2$ together imply

$$\#Q_2 + 1 \leqq \frac{(\#Q)^2}{2}. \tag{1}$$

For $n = 1$ we clearly have $\alpha(Q) = 1$. For $n > 1$, we distinguish between the two cases $\#Q^* = 1$ and $\#Q^* \geqq 2$. In the former case we have by Corollary 4.3(a)

$$\alpha(Q) \leqq \alpha(Q^*)(\#Q_2 + 1) \leqq \alpha(Q^*)(\#Q^* + 1) = 2 \leqq 2^{1-n} 2^{2n-2} \leqq \frac{(\#Q)^{2^n - 2}}{2^{n-1}}.$$

In the latter case, Corollary 4.3 (a), the inductive assumption, (1), and Lemma 4.4(c) yield

$$\begin{aligned} \alpha(Q) &\leqq \alpha(Q^*)(\#Q_2 + 1) \\ &\leqq 2^{2-n}(\#Q^*)^{2^{n-1}-2}(\#Q_2 + 1) \\ &\leqq 2^{1-n}(\#Q)^{2^n - 4}(\#Q)^2. \end{aligned}$$

Turning to the proof of Part (b) we first note that 4.4(b) and $\#Q \geqq 2$ together imply

$$\left[\frac{\#Q_2}{2}\right] + 1 \leqq \frac{(\#Q)^2}{4}. \tag{2}$$

To carry out the inductive step we suppose $n > 1$ and note that, by 4.2, Q_2 is point symmetric and hence 4.3(b) is applicable. We distinguish again between the two cases $\#Q^* = 1$ and $\#Q^* \geqq 2$. In the former case we may estimate

$$\alpha(Q) \leqq \alpha(Q^*)\left(\left[\frac{\#Q_2}{2}\right]+1\right) = \alpha(Q^*) = 1 \leqq 4^{1-n}2^{2n-2} \leqq \frac{(\#Q)^{2n-2}}{4^{n-1}}.$$

In the latter case observe that the assumptions of Part (b) are satisfied with n replaced by $n-1$ and Q replaced by Q^* (cf. Remark 4.2(a)). We may therefore use Corollary 4.3(b), the inductive assumption, (2), and Lemma 4.4(c) to estimate

$$\begin{aligned}\alpha(Q) &\leqq \alpha(Q^*)\left(\left[\frac{\#Q_2}{2}\right]+1\right)\\ &\leqq 4^{2-n}(\#Q^*)^{2^{n-1}-2}\left(\left[\frac{\#Q_2}{2}\right]+1\right)\\ &\leqq 4^{2-n}(\#Q)^{2^{n-4}}\frac{(\#Q)^2}{4}. \quad \square\end{aligned}$$

We next deal with lower estimates. Considering the subset $Q = (\mathbf{1},\ldots,\mathbf{q}) \in \mathbb{Q}^n$, we see that the only lower estimate of $\alpha(Q)$ valid for a *general*, finite subset $Q \subseteqq \mathbb{Q}^n$ and based solely on the number of Q is $\alpha(Q) \geqq 1$. Therefore, in order to obtain nontrivial lower estimates we require that Q satisfy additional assumptions. Similar to the reductive step for the upper bound given in Corollary 4.3 we have for the lower bound the following

4.7 Lemma. *Let $n \geqq 2$ and let Q be a finite subset of $\mathbb{Q}^n$ such that*
(α) *Q_2 is point symmetric and*
(β) *for all $\mathbf{x}', \mathbf{y}' \in Q'$ there exists $z \in \mathbb{Q}$ such that $(\mathbf{x}', z), (\mathbf{y}', z) \in Q$.*

Then $\alpha(Q) \geqq \alpha(Q')\left(\left[\frac{\#Q_2}{2}\right]+1\right)$.

Proof. Let $\Pi(Q') = \{\pi_1,\ldots,\pi_r\}$ with pairwise different π_i's and choose $\mathbf{c}_i \in \mathscr{L}(Q^* \cup Q')$ such that $\pi_i = \pi_{\mathbf{c}_i}(Q')$ for $1 \leqq i \leqq r$. Let $\mathbf{d}_{ij}$, $1 \leqq i \leqq r$, $0 \leqq j \leqq \#(\mathbf{c}_i \cdot Q_2)_-$, be defined as in Proposition 2.8. Then, as in 2.8(a), we have $\mathbf{d}_{ij} \in \mathscr{L}(Q)$. Moreover, by Hypothesis (α) and since $\#(\mathbf{c}_i \cdot Q_2) = \#Q_2$ (cf. 2.3), we have

$$\#\{\mathbf{d}_{ij} : 1 \leqq i \leqq r,\ 0 \leqq j \leqq \#(\mathbf{c}_i \cdot Q_2)_-\} = r \cdot \left(\left[\frac{\#Q_2}{2}\right]+1\right),$$

and plainly $r = \alpha(Q')$. It suffices therefore to show that $\pi_{\mathbf{d}_{ij}}(Q) \neq \pi_{\mathbf{d}_{hk}}(Q)$ if $(i,j) \neq (h,k)$. If $i \neq h$ then π_i and π_h are distinct and there exist elements $\mathbf{x}', \mathbf{y}' \in Q'$ such that $(\mathbf{c}_i \cdot (\mathbf{y}' - \mathbf{x}'))(\mathbf{c}_h \cdot (\mathbf{y}' - \mathbf{x}')) < 0$. By Hypothesis (β) the $(n-1)$-tupels $\mathbf{x}'$ and $\mathbf{y}'$ can be extended to $\mathbf{x}, \mathbf{y} \in Q$ such that $x_n = y_n$, whence $(\mathbf{d}_{i,j} \cdot (\mathbf{y} - \mathbf{x}))(\mathbf{d}_{h,k} \cdot (\mathbf{y} - \mathbf{x})) < 0$. If $i = h$, then $j \neq k$, and hence d_{ij} and d_{ik} realize different cuts in $(\mathbf{c}_i \cdot Q_2)_-$ and, a fortiori, in $\mathbf{c}_i \cdot Q_2$. Thus, by Lemma 2.6, $\pi_{\mathbf{d}_{ij}}(Q) \neq \pi_{\mathbf{d}_{hk}}(Q)$. $\square$

Using the foregoing lemma we can derive a lower bound for Cartesian products Q of symmetric subsets of $\mathbb{Q}$. Since such a set Q satisfies the hypotheses of Theorem

4.6(b), we can also give an upper bound. Both bounds are in terms of the cardinalities of the factors of Q.

4.8 Theorem. *Let $R_k \subseteq \mathbb{Q}$ be point symmetric and finite and contain at least two elements ($1 \leq k \leq n$, $n \geq 1$). Then for the Cartesian product $Q = \prod_{k=1}^{n} R_k$ we have*

$$\prod_{k=2}^{n} (\#R_k)^{k-1} \leq \alpha(Q) \leq \frac{(\#Q)^{2^n-2}}{4^{n-1}}.$$

(Note that the best lower bound is achieved by arranging $\#R_1, \ldots, \#R_n$ in increasing order.)

Proof. The set Q is symmetric with respect to all coordinates; hence Theorem 4.6(b) establishes the upper bound. In order to prove validity of the lower estimate we first show

$$\alpha(Q) \geq (\#Q')\alpha(Q') \tag{1}$$

if $n \geq 2$. Let a_k be the smallest element of R_k with respect to the natural order of $\mathbb{Q}$ and let $b_n \in R_n$, $b_n \neq a_n$. For any element $\mathbf{x}' \in Q' = \prod_{k=1}^{n-1} R_k$ we have $(\mathbf{x}', \pm b_n) \in Q$ and we also have $(\mathbf{a}', \pm a_n) \in Q$, where $\mathbf{a}' = (a_1, \ldots, a_{n-1})$. Hence we have $\pm \dfrac{\mathbf{x}' - \mathbf{a}'}{b_n - a_n} \in Q_2$. The minimal property of $\mathbf{a}'$ implies that the subsets

$$\left\{ \frac{\mathbf{x}' - \mathbf{a}'}{b_n - a_n} : \mathbf{x}' \in Q' \right\} \quad \text{and} \quad \left\{ -\frac{\mathbf{y}' - \mathbf{a}'}{b_n - a_n} : \mathbf{y}' \in Q',\ \mathbf{y}' \neq \mathbf{a}' \right\}$$

of Q_2 are disjoint and we have thus found $2\#Q' - 1$ distinct elements of Q_2. Notice that the set Q satisfies the hypotheses of Lemma 4.7. We therefore obtain

$$\alpha(Q) \geq \alpha(Q')\left(\left[\frac{Q_2}{2} \right] + 1 \right) \geq \alpha(Q')(\#Q')$$

as desired.

Induction on n with the aid of (1) now shows that $\alpha(Q) \geq \prod_{k=1}^{n-1} (\#R_k)^{n-k}$. The upper bound in the statement of the theorem is obtained by reversing the order of the sets R_k. □

In the case of a discrete hyperbox $Q = [\mathbf{1}, \mathbf{d}]$ Theorem 4.8 states that

$$\prod_{k=2}^{n} d_k^{k-1} \leq \alpha(Q) \leq \frac{(\prod d_k)^{2^n-2}}{4^{n-1}}$$

and for a discrete hypercube $Q = [1, d]^n$ ($d \geq 2$) we obtain

$$d^{(n^2-n)/2} \leq \alpha(Q) \leq \frac{d^{n(2^n-2)}}{4^{n-1}}.$$

We can, however, say more in these special cases by applying the results of Sect. 3 which we are now going to take up.

4.9 Notations. *Let* $n \geqq 2$, $\mathbf{0} \leqq \mathbf{d} \in \mathbb{Z}^n$ *and let* $Q = [\mathbf{0}, \mathbf{d}]$. *For every subset* $M \subseteqq \{1, \ldots, n\}$ *containing* n, $M = \{i_1, \ldots, i_r\}$ with $r \geqq 1$, $i_1 < \cdots < i_r = n$, *we let*

$$\mathbf{d}_M = (d_{i_1}, \ldots, d_{i_r}) \in \mathbb{Z}^r.$$

The number $\varphi(n, \mathbf{d})$ *is defined as in Subsect. 3.1 as the number of relatively prime n-tupels in the discrete hypercube* $[\mathbf{1}, \mathbf{d}]$. *For* $1 \leqq d \in \mathbb{Z}$, *the number* $\varphi(n, d)$ *is defined as in Subsect. 3.1 as the number of relatively prime n-tupels in the discrete hypercube* $[1, d]^n$.

4.10 Lemma. *Let* $n \geqq 2$, $\mathbf{1} \leqq \mathbf{d} \in \mathbb{Z}^n$ *and let* $Q = [\mathbf{0}, \mathbf{d}]$. *Then*

(a) $Q_1 \subseteqq Q_2$, $Q^* = Q_2$;

(b) Q^* *is symmetric with respect to all coordinates*;

(c) $$\#Q_2 = \sum_{r=1}^{n} 2^{r-1} \sum_{\substack{M \subseteqq \{1,\ldots,n\} \\ n \in M, \#M = r}} \varphi(r, \mathbf{d}_M) =: \sigma(n, \mathbf{d}).$$

Proof. Claim (a) follows from $Q_1 = [-\mathbf{d}', \mathbf{d}']$ and the fact that any element $\mathbf{z} \in [-\mathbf{d}', \mathbf{d}']$ can be represented in the form

$$\mathbf{z} = \frac{\mathbf{x}' - \mathbf{y}'}{x_n - y_n} \in Q_2,$$

where $\mathbf{x} = (\mathbf{z}^+, 1) \in Q$ and $\mathbf{y} = (\mathbf{z}^-, 0) \in Q$ $(\mathbf{z}^{\pm} = (z_1^{\pm}, \ldots, z_{n-1}^{\pm}))$.

Claim (b) follows from (a) and the representation

$$Q_2 = \left\{ \frac{\mathbf{x}'}{x_n} : \mathbf{x} \in [-\mathbf{d}, \mathbf{d}],\ x_n \geqq 1 \right\}. \tag{1}$$

In order to prove Part (c) we put

$$Q_3 := \{\mathbf{x} \in [-\mathbf{d}, \mathbf{d}] : x_n \geqq 1 \text{ and } \gcd(x_1, \ldots, x_n) = 1\}.$$

Now (1) implies that the map $\mathbf{x} \to \dfrac{\mathbf{x}'}{x_n}$ provides a bijection between the sets Q_3 and Q_2; we hence have

$$\#Q_2 = \#Q_3. \tag{2}$$

For every subset $M \subseteqq \{1, \ldots, n\}$ containing n we let

$$Q_{3M} := \{\mathbf{x} \in Q_3 : \text{support}(x) = M\}$$

and

$$\mathbf{Q}_{3M}^+ := \{\mathbf{x} \in Q_{3M} : \mathbf{x} \geqq \mathbf{0}\}.$$

Notice that for any such $M, \#M = r \geqq 1$, we have

$$\#Q_{3M} = 2^{r-1} \#Q_{3M}^+. \tag{3}$$

By dropping zeros in elements of Q_{3M}^+ we get a bijection between Q_{3M}^+ and the set $\{x \in [\mathbf{1}, \mathbf{d}_M] : \gcd(x_{i_1}, \ldots, x_{i_r}) = 1\}$ whence we have

$$\#Q_{3M}^+ = \varphi(\mathbf{r}, \mathbf{d}_M). \tag{4}$$

Since Q_3 is the disjoint union of all the sets Q_{3M} for $n \in M \subseteqq \{1, \ldots, n\}$, Claim (c) now follows from (2)–(4).

For a discrete hypercube $Q = [0, d]^n$ we obtain the following

4.11 Corollary. *Let $n \geqq 2$, $d \geqq 1$, and let $Q = [0, d]^n$. Then*

$$\#Q_2 = \sum_{r=1}^{n} 2^{r-1} \binom{n-1}{r-1} \varphi(r, d) =: \sigma(n, d).$$

4.12 Lemma. (a) $1 + \left[\frac{\sigma(n, \mathbf{d})}{2}\right] = \frac{1 + \sigma(n, \mathbf{d})}{2}$;

(b) $2^{n-1}\varphi(n, \mathbf{d}) \leqq \sigma(n, \mathbf{d}) \leqq d_n \prod_{k=1}^{n-1} (1 + 2d_k)$;

(c) $2^{n-1}\varphi(n, \mathbf{d}) \leqq \sigma(n, \mathbf{d}) \leqq d(1 + 2d)^{n-1}$;

(d) $\frac{\sigma(n, \mathbf{d})}{\prod_i d_i} \to \frac{2^{n-1}}{\zeta(n)}$ as $\min_i d_i \to \infty$;

(e) $\frac{\sigma(n, d)}{d^n} \to \frac{2^{n-1}}{\zeta(n)}$ as $d \to \infty$.

Proof. The numbers $\sigma(n. \mathbf{d})$ are odd whence we have Claim (a). The lower estimate in (b) is plain and the upper estimate follows from 4.10(c) and 4.10(1). Claim (d) follows from Proposition 3.2. Claims (c) and (e) ensue from (b) and (d), respectively.

We are now ready to prove the main results of this paper. We first deal with upper and lower estimates.

4.13 Theorem. *Let $n \geqq 2$, $\mathbf{1} \leqq \mathbf{d} \in \mathbb{Z}^n$, $1 \leqq d \in \mathbb{Z}$.*
(a) *For the number of admissible orders on the n-dimensional discrete hyperbox $[\mathbf{0}, \mathbf{d}]$ we have the estimates*

$$\frac{\prod_{r=2}^{n} (1 + \sigma(r, (d_1, \ldots, d_r)))}{2^{n-1}} \leqq \alpha([\mathbf{0}, \mathbf{d}]) \leqq \frac{\sigma(n, \mathbf{d})^{2^{n-1}-2}(1 + \sigma(n, \mathbf{d}))}{2^{2n-3}}.$$

(*Note that the best lower bound is achieved by arranging the d_i's in decreasing order.*)
In particular, we have for a rectangle $\alpha([0, d_1] \times [0, d_2]) = 1 + \varphi(2, \mathbf{d})$.
(b) *For the number of admissible orders on the n-dimensional discrete hypercube $[0, d]^n$ we have the estimates*

$$\frac{\prod_{r=2}^{n} (1 + \sigma(r, d))}{2^{n-1}} \leqq \alpha([0, d]^n) \leqq \frac{\sigma(n, d)^{2^{n-1}-2}(1 + \sigma(n, d))}{2^{2n-3}}.$$

In particular, we have for a square $\alpha([0, d]^2) = 1 + \varphi(2, d)$.

Proof. The estimates for the cube are direct consequences of those for the box. To derive the upper bound in Part (a) we combine Corollary 4.3(b), Lemma 4.10, Lemma 4.12(a), and Theorem 4.6(b) to estimate

$$\alpha([\mathbf{0}, \mathbf{d}]) \leqq \alpha([\mathbf{0}, \mathbf{d}]^*) \frac{1 + \sigma(n, \mathbf{d})}{2} = \frac{\sigma(n, \mathbf{d})^{2^{n-1}-2}(1 + \sigma(n, \mathbf{d}))}{4^{n-2} \cdot 2}.$$

In order to derive the lower bound put $Q := [\mathbf{0}, \mathbf{d}]$ and denote the projection of

$\mathbf{x} \in \mathbb{Z}^n$ and Q on the first $n-k$ coordinates by $\mathbf{x}^{(k)}$ and $Q^{(k)}$. Using repeatedly Lemma 4.7 and Lemma 4.12(a) we estimate

$$\alpha(Q) \geqq \alpha(Q^{(1)})\left(1+\left[\frac{\#Q_2}{2}\right]\right) \geqq \alpha(Q^{(2)})\left(1+\left[\frac{\#(Q^{(1)})_2}{2}\right]\right)\left(1+\left[\frac{\#Q_2}{2}\right]\right) \geqq \cdots$$

$$\geqq \alpha(Q^{(n-1)}) \prod_{k=0}^{n-2}\left(1+\left[\frac{\#Q^{(k)}}{2}\right]\right) = \prod_{k=0}^{n-2}\left(1+\left[\frac{\sigma(n-k, \mathbf{d}^{(k)})}{2}\right]\right)$$

$$= \frac{\prod_{k=0}^{n-2}(1+\sigma(n-k, \mathbf{d}^{(k)}))}{2^{n-1}} = \frac{\prod_{r=2}^{n}(1+\sigma(r, \mathbf{d}^{(n-r)}))}{2^{n-1}}. \quad \square$$

4.14. Remark. (a) In the case of a square $[0,d]^2$ we obtain immediately from 4.13(b) and 4.11

$$\alpha([0,d]^2) = 1 + \varphi(2,d).$$

In this case we obtain for $1 \leqq d \leqq 20$ the following list:

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\alpha([0,d]^2)$	2	4	8	12	20	24	36	44	56	64	84	92	116	128	144	160	192	204	240	256

(b) In cases where it is not possible to compute the numbers $\sigma(r,d)$ (if r or the d_i's are too large) we have recourse to the estimates given in Lemma 4.12(b), (c) and to the estimates in Propositions (3.2), (3.4), and in Corollary 3.5. We will not explicitly expose the somewhat clumsy estimates for $\alpha([\mathbf{0},\mathbf{d}])$ and $\alpha([0,d]^n)$ which we would obtain.

We next derive asymptotic upper and lower bounds as $\min_i d_i$ tends to infinity for fixed n.

4.15 Theorem. *Let $n \geqq 2$ and define*

$$b_n := \frac{2^{(n-1)(n-2)/2}}{\prod_{k=2}^{n}\zeta(k)}, \quad c_n := \begin{cases} \dfrac{1}{\zeta(2)} & n=2 \\ \dfrac{2^{(n-1)2^{n-1}-3n+4}}{\sqrt{e}} & n \geqq 3. \end{cases}$$

(a) *For any $\varepsilon > 0$ we have*

$$(1-\varepsilon) b_n d_n^{n-1} \prod_{k=1}^{n-1} d_k^k \leqq \alpha([\mathbf{0},\mathbf{d}]) \leqq (1+\varepsilon) c_n \left(\prod_{k=1}^{n} d_k\right)^{2^{n-1}-1}$$

if $\min_i d_i$ is sufficiently large. (The best lower bound is achieved by arranging the numbers d_i in increasing order.)

(b) *For any $\varepsilon > 0$ we have*

$$(1-\varepsilon) b_n d^{(n^2+n-2)/2} \leqq \alpha([0,d]^n) \leqq (1+\varepsilon) c_n d^{n(2^{n-1}-1)}$$

for eventually all $d \in \mathbb{N}$.

Proof. Part (b) follows immediately from Part (a). We first deal with the upper

estimate in (a). By Theorem 4.13(a) and Lemma 4.12(d) we have

$$\limsup_{\min_k d_k \to \infty} \frac{\alpha([\mathbf{0},\mathbf{d}])}{\left(\prod_k d_k\right)^{2^{n-1}-1}} \leqq \frac{2^{(n-1)(2^{n-1}-1)}}{2^{2n-3}\zeta(n)^{2^{n-1}-1}} = \frac{2^{(n-1)2^{n-1}-3n+4}}{\zeta(n)^{2^{n-1}-1}}.$$

The upper bound in the case $n=2$ now follows. For $n \geqq 3$ we show that $\zeta(n)^{2^{n-1}-1} \geqq \sqrt{e}$: For $n=3$ this follows from $\zeta(3) > 1.19 > e^{1/6}$. For $n \geqq 4$ we have $\left(\frac{2k}{k+1}\right)^n \geqq 3$ $(k \geqq 2)$. It follows that

$$2^n \sum_{k \geqq 2} \frac{1}{k^n} = 1 + \sum_{k \geqq 3} \left(\frac{2}{k}\right)^n \geqq 1 + \sum_{k \geqq 2} \frac{3}{k^n},$$

i.e.,

$$\sum_{k \geqq 2} \frac{1}{k^n} \geqq \frac{1}{2^n - 3},$$

and

$$\zeta(n) \geqq 1 + \frac{1}{2^n - 3}.$$

Hence, using $\left(1 + \frac{1}{k}\right)^{k+1} \geqq e$, we have $\zeta(n)^{2^{n-2}} \geqq \left(1 + \frac{1}{2^n - 3}\right)^{2^{n-2}} \geqq e$, which is the desired estimate.

In order to derive the lower bound in (a) use 4.12(d) to see that

$$\frac{\prod_{r=2}^{n} (1 + \sigma(r,(d_1,\ldots,d_r)))}{2^{n-1} d_1^{n-1} \prod_{r=2}^{n} d_r^{n-r+1}} \to \frac{2^{(n-1)(n-2)/2}}{\prod_{r=2}^{n} \zeta(r)} = b_n \tag{1}$$

as $\min_i d_i$ tends to infinity. From (1) and Theorem 4.13(a) it follows that

$$\alpha([\mathbf{0},\mathbf{d}]) \geqq (1-\varepsilon) b_n d_1^{n-1} \prod_{r=2}^{n} d_r^{n-r+1}$$

if $\min_i d_i$ is sufficiently large. The lower estimate now follows by reversing the order of the numbers d_r. □

4.16 Remark. It is also possible to derive bounds for more general subsets $Q \subseteqq \mathbb{Q}^n$ than those considered so far in this section. If $\underline{Q}$ and $\bar{Q}$ are subsets of $\mathbb{Q}^n$ such that

$$\underline{Q} \subseteqq Q \subseteqq \bar{Q},$$

then plainly

$$\alpha(\underline{Q}) \leqq \alpha(Q) \leqq \alpha(\bar{Q}),$$

i.e., any upper bound of $\alpha(\bar{Q})$ is also an upper bound of $\alpha(Q)$ and any lower bound of $\alpha(\underline{Q})$ is a lower bound for $\alpha(Q)$. It is therefore sufficient to look for "large" sets

Q and "small" sets $\bar{Q}$ controlled by Theorems 4.8, 4.13, and 4.15. We conclude this section with a sample result analogous to Theorem 4.15(b) for sets Q related to terms of maximum total degree d. Other sets that could be well treated in this manner are norm balls of the form $\left\{x\in\mathbb{Z}^n: \sum_{k=1}^{n} |x_k|^p \leqq d^p\right\}$ for real numbers $p, d > 0$.

4.17 Corollary. *Let $n\geqq 2$, $d\geqq 1$, and let $Q=\left\{x\in\mathbb{Z}_+^n: \sum_{k=1}^{n} x_k \leqq d\right\}$. For any $\varepsilon>0$ we have the estimates*

$$(1-\varepsilon)b_n\left[\frac{d}{n}\right]^{(n^2+n-2)/2} \leqq \alpha(Q) \leqq (1+\varepsilon)c_n d^{n(2^{n-1}-1)}$$

for eventually all $d\in\mathbb{N}$. (b_n and c_n are the constants defined in Theorem 4.15.)

Proof. This follows from the inclusion $[\mathbf{0},\mathbf{g}]\subseteqq Q\subseteqq[0,d]^n$, where $g=\left[\frac{d}{n}\right]$.

5. Algorithms

5.1 Explanations. In this section we sketch two algorithms for constructing a set of distinct representatives in $\mathscr{L}(Q)$ for $\Pi(Q)$, where Q is a finite subset of $\mathbb{Q}^n$. These algorithms are based on Proposition 2.8 which provides a recursive method for the construction of a finite set of representatives for $\Pi(Q)$.

In view of the applications indicated in the introduction, we treat the problem in greater generality: Let $\mathscr{A}(Q,\mathscr{C})$ be the set of all admissible orders on Q that extend a given set $\mathscr{C}\subseteqq Q^2$ of "side conditions", i.e., $\mathscr{A}(Q,\mathscr{C}):=\{\prec\in\mathscr{A}(Q): x\prec y$ for all $(x,y)\in\mathscr{C}\}$, and let $\Pi(Q,\mathscr{C})$ be the subset of $\Pi(Q)$ corresponding to $\mathscr{A}(Q,\mathscr{C})$ by Proposition 2.4. The following notion of inconsistency singles out those sets $\mathscr{C}$ for which $\mathscr{A}(Q,\mathscr{C})$ is void for a trivial reason. Let $\leqq$ denote the componentwise partial order on $\mathbb{Q}^n$. We call $\mathscr{C}\subseteqq(\mathbb{Q}^n)^2$ *inconsistent*, if there exists $(\mathbf{x},\mathbf{y})\in\mathscr{C}$ with $\mathbf{y}\leqq\mathbf{x}$. Notice that $\mathscr{A}(Q,\mathscr{C})=\varnothing$ for inconsistent $\mathscr{C}$.

We want to construct a set of distinct representatives in $\mathscr{L}(Q)$ for $\Pi(Q,\mathscr{C})$. Turning to our first algorithm we now determine a finite subset of $\mathbb{Q}^n$ such that each admissible order on Q is represented by at least one linear form in this subset. For a rational number $r=\frac{x}{y}$ with $x,y\in\mathbb{Z}$, $y\neq 0$, $\gcd(x,y)=1$, we define the *modulus* of r by $\mathrm{mod}(r):=\max\{|x|,|y|\}$. For $\mathbf{x}=(x_1,\ldots,x_n)\in\mathbb{Q}^n$, $\mathrm{mod}(\mathbf{x}):=\max\{\mathrm{mod}(x_i): 1\leqq i\leqq n\}$ and for a finite subset $Q\subseteqq\mathbb{Q}^n$, $\mathrm{mod}(Q):=\max\{\mathrm{mod}(\mathbf{x}):\mathbf{x}\in Q\}$.

The following inequalities are straightforward:

(i) For any finite subset $Q\subseteqq\mathbb{Q}^n$ we have

$$\mathrm{mod}(Q^*)\leqq 2(\mathrm{mod}(Q))^4.$$

(ii) If $\mathbf{c},\mathbf{x}\in\mathbb{Q}^n$ then

$$\mathrm{mod}(\mathbf{c}\cdot\mathbf{x})\leqq n(\mathrm{mod}(\mathbf{c}))^n(\mathrm{mod}(\mathbf{x}))^n.$$

(iii) If $\mathbf{x},\mathbf{y}\in\mathbb{Q}^n$ then

$$\mathrm{mod}\tfrac{1}{2}(\mathbf{x}+\mathbf{y})\leqq 2(\mathrm{mod}(\mathbf{x}))(\mathrm{mod}(\mathbf{y})).$$

5.2 Proposition. *Define the functions* $m_n: \mathbb{N} \to \mathbb{N}$ $(n \geqq 1)$ *recursively by* $m_1(q) := 1$,

(i) $m_{n+1}(q) := 2^{2n+1} n^2 q^{8n} m_n^{2n}(2q^4)$ $(q \in \mathbb{N})$.

Then:

(a) *For any nonempty, finite subset* $Q \subseteqq \mathbb{Q}^n$ *and any positive block* $\pi \in \Pi(Q)$ *there exists a linear form* $\mathbf{c} \in \mathscr{L}(Q)$ *representing* π *and such that*

$$\operatorname{mod}(\mathbf{c}) \leqq m_n(\operatorname{mod}(Q)).$$

(b) *For all* $q \geqq 1$, $n \geqq 2$ *we have*

$$2^{2^{2n-3}(n-1)!} q^{8^{n-1}(n-1)!} \leqq m_n(q) \leqq 2^{3^{2n-3}(n-1)!} q^{9^{n-1}(n-1)!}.$$

Proof. We first prove Part (a) and proceed by induction on n. Let Q be a nonempty, finite subset of $\mathbb{Q}^{n+1}$. By Proposition 2.8, any positive block $\pi \in \Pi(Q)$ for Q can be represented by a linear form $\mathbf{d} = \mathbf{c} * d$, where $\mathbf{c} \in \mathscr{L}(Q^*)$ can be chosen in such a way that

$$\operatorname{mod}(\mathbf{c}) \leqq m_n(\operatorname{mod}(Q^*)) \tag{1}$$

(inductive assumption) and $-d$ realizes a cut in the set $(\mathbf{c} \cdot Q_2)_-$. We may take d to be the arithmetic mean of two neighbors in the set $(\mathbf{c} \cdot Q_2)_- \cup \{0, 3 \cdot \min(\mathbf{c} \cdot Q_2)_-\}$. Therefore, by 5.1(iii) and (ii),

$$\operatorname{mod}(d) \leqq 2 \operatorname{mod}(\mathbf{c} \cdot Q_2)^2 \leqq 2n^2 (\operatorname{mod}(\mathbf{c}))^{2n} (\operatorname{mod}(Q_2))^{2n}. \tag{2}$$

Now, by (1), 5.1(i), and by monotonicity of the function m_n, we have

$$\operatorname{mod}(\mathbf{c}) \leqq m_n(2(\operatorname{mod}(Q))^4). \tag{3}$$

Furthermore, by 5.1(i),

$$\operatorname{mod}(Q_2) \leqq 2(\operatorname{mod}(Q))^4. \tag{4}$$

Combining (2), (3), and (4) we see that $\operatorname{mod}(d)$ is dominated by $m_{n+1}(\operatorname{mod}(Q))$. To conclude the proof note that

$$\operatorname{mod}(\mathbf{d}) = \max\{\operatorname{mod}(\mathbf{c}), \operatorname{mod}(d)\}$$

and that

$$\operatorname{mod}(\mathbf{c}) \leqq m(\operatorname{mod}(Q^*)) \leqq m_n(2(\operatorname{mod}(Q))^4) \leqq m_{n+1}(\operatorname{mod}(Q)).$$

We turn now to the proof of Part (b). We proceed again by induction on n and verify first the upper estimate. The cases $n = 2, 3$ are plain since $m_2(q) = 8q^8$, and $m_3(q) = 2^{51} q^{144}$. By the definition of m_{n+1} and the inductive hypothesis we have for $n \geqq 3$

$$\begin{aligned} m_{n+1}(q) &\leqq 2^{2n+1} n^2 q^{8n} [2^{3^{2n-3}(n-1)!} (2q^4)^{9^{n-1}(n-1)!}]^{2n} \\ &= 2^{[2n+1+8 \cdot 3^{2n-3} n!]} n^2 q^{[8n+8 \cdot 9^{n-1} n!]}. \end{aligned} \tag{5}$$

Now, for $n \geqq 3$, we have $2n + 1 + 2ldn \leqq 3^{2n-3} n!$ and for $n \geqq 2$ we have $8n \leqq 9^{n-1} n!$ so that (5) is majorized by $2^{3^{2n-1} n!} q^{9^n n!}$.

In the lower estimate the case $n = 2$ is plain. For $n \geqq 2$ the inductive hypothesis

implies

$$m_{n+1}(q) \geqq m_n^{2n}(2q^4) \geqq [2^{2^{2n-3}(n-1)!}(2q^4)^{8^{n-1}(n-1)!}]^{2n}$$
$$= 2^{[2\cdot 2^{2n-3}+2\cdot 2^{3n-3}]n!} q^{8^n n!} \geqq 2^{4\cdot 2^{2n-3}n!} q^{8^n n!}. \quad \square$$

5.3 Notations. *As before, let Q be a finite subset of $\mathbb{Q}^n$ and let $\mathscr{C} \subseteq Q^2$. We put $\mathscr{L}(Q,\mathscr{C}) = \{\mathbf{a}\in\mathscr{L}(Q): \mathbf{a}\cdot\mathbf{x} < \mathbf{a}\cdot\mathbf{y}$ for all $(\mathbf{x},\mathbf{y})\in\mathscr{C}\}$. So $\mathscr{L}(Q,\mathscr{C})$ consists exactly of the linear forms in $\mathscr{L}(Q)$ that represent admissible orders on Q which extend $\mathscr{C}$. We also put $\Pi(Q,\mathscr{C}) = \{\pi_{\mathbf{a}}(Q): \mathbf{a}\in\mathscr{L}(\mathbf{Q},\mathscr{C})\}$.*

We associate with $\mathscr{C}$ and Q two subsets $\mathscr{C}_l$, $\mathscr{C}_u$ of Q_2 and three subsets $\mathscr{C}_1, \mathscr{C}_2$ and $\mathscr{C}^*$ of Q_1, Q_2 and Q^*, respectively; the latter sets are formed in analogy to Q_1, Q_2 and Q^*:

$$\mathscr{C}_l = \left\{\frac{\mathbf{y}'-\mathbf{x}'}{y_n-x_n}\in\mathbb{Q}^{n-1}: (\mathbf{x},\mathbf{y})\in\mathscr{C} \text{ and } x_n > y_n\right\},$$

$$\mathscr{C}_u = \left\{\frac{\mathbf{y}'-\mathbf{x}'}{y_n-x_n}\in\mathbb{Q}^{n-1}: (\mathbf{x},\mathbf{y})\in\mathscr{C} \text{ and } x_n < y_n\right\},$$

$$\mathscr{C}_1 = \{(\mathbf{0},\mathbf{y}'-\mathbf{x}')\in(\mathbb{Q}^{n-1})^2: (\mathbf{x},\mathbf{y})\in\mathscr{C},\ x_n = y_n\},$$

$$\mathscr{C}_2 = \{(\mathbf{u},\mathbf{v})\in(\mathbb{Q}^{n-1})^2: \mathbf{u}\in\mathscr{C}_l,\ \mathbf{v}\in\mathscr{C}_u\},$$

$$\mathscr{C}^* = \mathscr{C}_1 \cup \mathscr{C}_2.$$

We prove next an analogue of Proposition 2.6.

5.4 Lemma. *Let Q be a finite subset of $\mathbb{Q}^n$ and let $\mathscr{C} \subseteq Q^2$. The following hold:*
(a) *If $\mathbf{a}\in\mathscr{L}(Q^*)$ and if $b\in\mathbb{Q}_+$ is such that $\mathbf{a}*b\in\mathscr{L}(Q,\mathscr{C})$, then*

(i) $\mathbf{a}\in\mathscr{L}(Q^*,\mathscr{C}^*)$ *and*
(ii) $\mathbf{a}\cdot\mathscr{C}_l < -b < \mathbf{a}\cdot\mathscr{C}_u$.

(b) *Suppose that $\mathbf{a}\in\mathscr{L}(Q^*,\mathscr{C}^*)$; then:*

(iii) $\mathbf{a}\cdot\mathscr{C}_l < \mathbf{a}\cdot\mathscr{C}_u$ *and*
(iv) *for any $b\in\mathbb{Q}^+$ such that $-b\notin\mathbf{a}\cdot Q_2$ and $\mathbf{a}\cdot\mathscr{C}_l < -b < \mathbf{a}\cdot\mathscr{C}_u$ we have $\mathbf{a}*b\in\mathscr{L}(Q,\mathscr{C})$.*

Proof. (a) By hypothesis $\mathbf{a}*b\in\mathscr{L}(Q,\mathscr{C})$, i.e., if $(\mathbf{x},\mathbf{y})\in\mathscr{C}$ then $(\mathbf{a}*b)\cdot\mathbf{x} < (\mathbf{a}*b)\cdot\mathbf{y}$, and so $\mathbf{a}\cdot(\mathbf{y}'-\mathbf{x}') > -b(y_n-x_n)$. If $y_n = x_n$, this implies $\mathbf{a}\cdot(\mathbf{y}'-\mathbf{x}') > 0 = \mathbf{a}\cdot\mathbf{0}$; if $x_n > y_n$, it implies $\mathbf{a}\cdot\dfrac{\mathbf{y}'-\mathbf{x}'}{y_n-x_n} < -b$, and if $x_n < y_n$, it implies $\mathbf{a}\cdot\dfrac{\mathbf{y}'-\mathbf{x}'}{y_n-x_n} > -b$. This shows in particular that for $\mathbf{u}\in\mathscr{C}_l$, $\mathbf{v}\in\mathscr{C}_u$, $\mathbf{a}\cdot\mathbf{u} < \mathbf{a}\cdot\mathbf{v}$, and hence that $\mathbf{a}\in\mathscr{L}(Q^*,\mathscr{C}^*)$.
(b) Let $\mathbf{u}\in\mathscr{C}_l, \mathbf{v}\in\mathscr{C}_u$. Then $(\mathbf{u},\mathbf{v})\in\mathscr{C}_2 \subseteq \mathscr{C}^*$, and so $\mathbf{a}\cdot\mathbf{u} < \mathbf{a}\cdot\mathbf{v}$.
Next let $b\in\mathbb{Q}_+$ satisfy $-b\notin\mathbf{a}\cdot Q_2$ and $\mathbf{a}\cdot\mathscr{C}_l < -b < \mathbf{a}\cdot\mathscr{C}_u$. Since $\mathbf{a}\in\mathscr{L}(Q^*,\mathscr{C}^*) \subseteq \mathscr{L}(Q_1)$, 2.6(iii) is satisfied with $\mathbf{a}'$ and $\mathbf{b}'$ replaced by $\mathbf{a}$. The condition $-b\notin\mathbf{a}\cdot Q_2$ implies that 2.6(iv) is satisfied with $a_n = b_n = b$ and $\mathbf{a}' = \mathbf{b}'$ replaced by $\mathbf{a}$. Lemma 2.6 implies that $\mathbf{a}*b\in\mathscr{L}(Q)$.

Now let $(\mathbf{x},\mathbf{y})\in\mathscr{C}$. If $y_n = x_n$ then $(\mathbf{0},\mathbf{y}'-\mathbf{x}')\in\mathscr{C}_1 \subseteq \mathscr{C}^*$ and so $(\mathbf{a}*b)\cdot(\mathbf{y}-\mathbf{x}) = \mathbf{a}\cdot(\mathbf{y}'-\mathbf{x}') > \mathbf{a}\cdot\mathbf{0} = 0$. If $x_n > y_n$ $(x_n < y_n)$ then $\mathbf{u} = \dfrac{\mathbf{y}'-\mathbf{x}'}{y_n-x_n}$ is in $\mathscr{C}_l$ (in $\mathscr{C}_u$) and hence $\mathbf{a}\cdot\mathbf{u} < -b$ $(\mathbf{a}\cdot\mathbf{u} > -b)$; therefore $\mathbf{a}\cdot(\mathbf{y}'-\mathbf{x}') > -b(y_n-x_n)$, and so $(\mathbf{a}*b)\cdot\mathbf{x} < (\mathbf{a}*b)\cdot\mathbf{y}$. $\square$

Our algorithms will use the following unspecified

5.5 Procedures

(a) *Check*: A procedure that checks a finite subset $\mathscr{C} \subseteqq (\mathbb{Q}^n)^2$ for consistency.

(b) *Compare*: A procedure that checks whether two blocks $\pi_{\mathbf{a}}(Q)$ and $\pi_{\mathbf{b}}(Q)$ generated by linear forms $\mathbf{a}, \mathbf{b} \in \mathscr{L}(Q)$ coincide. Here, as before, Q is a finite subset of $\mathbb{Q}^n$.

(c) *Reduce*: A procedure – based on (b) – that takes as input a finite subset $Q \subseteqq \mathbb{Q}^n$ and a finite subset $LF \subseteqq \mathscr{L}(Q)$ and outputs a complete set $LF' = \text{Reduce}\,(LF; Q)$ of representatives in LF for $\{\pi_{\mathbf{b}}(Q): \mathbf{b} \in LF\}$; i.e., LF' is a subset of LF such that for $\mathbf{a} \neq \mathbf{b} \in LF'$ we have $\pi_{\mathbf{a}}(Q) \neq \pi_{\mathbf{b}}(Q)$ and such that $\{\pi_{\mathbf{a}}(Q): \mathbf{a} \in LF'\} = \{\pi_{\mathbf{b}}(Q): \mathbf{b} \in LF\}$.

Our first algorithm is based mainly on Proposition 5.2(a).

5.6 Algorithm I: Repr_elem $(n, Q, \mathscr{C})$.

Input: $1 \leqq n \in \mathbb{N}$, a finite subset $Q \subseteqq \mathbb{Q}^n$, and $\mathscr{C} \subseteqq Q^2$.

Output: A finite set of distinct representatives in $\mathscr{L}(Q)$ of $\Pi(Q, \mathscr{C})$ if $\Pi(Q, \mathscr{C})$ is nonempty, and $\varnothing$ otherwise.

BEGIN
  $m := n$;
  $q :=$ mod (Q);
  stack $:= \varnothing$;
  WHILE $m > 1$ AND consistent $(\mathscr{C})$ DO
    $m := m - 1$;
    stack $:=$ PUSH$(q,$ stack$)$;
    $q := 2q^4$;
    $\mathscr{C} := \mathscr{C}^*$
  END;
  IF inconsistent $(\mathscr{C})$ THEN repr_elem $:= \varnothing$ {cf. 5.4(iii)}
  ELSE
    max_list $:=$ (1);
    WHILE $m < n$ DO
      q $:=$ POP(stack);
      max $:=$ CAR(max_list);
      max $:= 2^{2n+1} n^2 q^{8n}$ max^{2n};
      max_list $:=$ CONS(max, max_list);
      $m := m + 1$
    END
    $l$forms $:= \left\{ \left(1, \frac{x_2}{y_2}, \ldots, \frac{x_n}{y_n}\right) : |x_i| \leqq \max_i,\ 1 \leqq y_i \leqq \max_i \right.$
      $\left.$ for all $1 \leqq i \leqq n$, where $(\max_n, \ldots, \max_1) =$ max_list $\right\}$;
    repr_elem $:=$ reduce ($l$forms, Q)
  END
END.

5.7 Remark. For $n = 2$, the variable $\max_n$ in the above algorithm assumes the

value $8(\mathrm{mod}(Q))^8$ and for $n=3$ the value $2^{51}(\mathrm{mod}(Q))^{144}$. It seems unlikely that this algorithm is useful for $n \geqq 3$ even in the case $\mathrm{mod}(Q)=1$. We therefore design a second algorithm that exploits Proposition 2.8 in a more efficient and direct way. Using Lemma 5.4 we first state the following generalization of Proposition 2.8. Its proof is similar to that of Proposition 2.8, using the additional facts stated in Lemma 5.4.

5.8 Proposition. *Let Q be a finite subset of Q^n, let $\mathscr{C} \subseteq Q^2$, and let $\mathbf{c}_i \in \mathscr{L}(Q^*, \mathscr{C}^*)$ $(1 \leqq i \leqq m)$ be such that*

(i) $\{\pi_{\mathbf{c}_1}(Q^*), \ldots, \pi_{\mathbf{c}_m}(Q^*)\} = \Pi(Q^*, \mathscr{C}^*)$.

Then the following hold:

(a) $\mathbf{c}_i \cdot \mathscr{C}_l < \mathbf{c}_i \cdot \mathscr{C}_u$ *for* $1 \leqq i \leqq m$.
(b) *For every cut S_{ij} $(j \in J_i)$ in $(\mathbf{c}_i \cdot Q_2)_-$ that refines the pair $(\mathbf{c}_i \cdot \mathscr{C}_l, \mathbf{c}_i \cdot \mathscr{C}_u)$ pick $d_{ij} \in \mathbb{Q}_+ \setminus \{0\}$ such that $-d_{ij}$ realizes the cut S_{ij} and put $\mathbf{d}_{ij} = \mathbf{c}_i * d_{ij}$. Then*

(α) $\mathbf{d}_{ij} \in \mathscr{L}(Q, \mathscr{C})$ *and*
(β) $\{\pi_{\mathbf{d}_{ij}}(Q) : 1 \leqq i \leqq m, j \in J_i\} = \Pi(Q, \mathscr{C})$.

With the aid of the foregoing proposition we can now outline a more refined algorithm that computes for given $n, Q, \mathscr{C}$, by recursion on n, a set of distinct representatives in $\mathscr{L}(Q)$ for $\Pi(Q, \mathscr{C})$.

5.9 Algorithm II: Repr_recur $(n, Q, \mathscr{C})$.

Input: $1 \leqq n \in \mathbb{N}$, a finite subset $Q \subseteq \mathbb{Q}^n$, and $\mathscr{C} \subseteq Q^2$.

Output: A finite set of distinct representatives in $\mathscr{L}(Q)$ of $\Pi(Q, \mathscr{C})$, if $\Pi(Q, \mathscr{C})$ is nonempty, and $\varnothing$ otherwise.

```
BEGIN
  m:= n;
  stack:= ∅;
  WHILE m > 1 AND consistent (𝒞) DO
    m:= m − 1;
    stack:= PUSH((Q, Q₂, 𝒞_l, 𝒞_u), stack);
    Q:= Q*;
    𝒞:= 𝒞*
  END;
  IF inconsistent(𝒞) THEN repr_recur:= ∅                    {cf. 5.4(iii)}
  ELSE
    lforms:= {1};
    WHILE m < n DO
      (Q, Q₂, 𝒞_l, 𝒞_u):= POP(stack);
      new_lforms:= ∅;
      WHILE lforms ≠ ∅ DO
        c:= some element of lforms;
        lforms:= lforms\{c};
        D:= a set of elements d of ℚ₊\{0}, whose negatives
              −d realize all cuts in (c·Q₂)_ with c·𝒞_l < −d < c·𝒞_u;
```

```
            new_lforms:=new_lforms∪{c*d:d∈D}
        END;
        lforms:=reduce (new_lforms, Q);
        m:=m+1
    END;
    repr_recur:=lforms
  END
END.
```

5.10 Remarks. (a) The two algorithms described in this section determine, for a given triple $(n, Q, \mathscr{C})$, a *set* of representatives in $\mathscr{L}(Q)$ of the system $\Pi(Q, \mathscr{C})$ of positive blocks. If we are interested in the *cardinality* of $\Pi(Q, \mathscr{C})$ only, procedure *reduce*, which necessitates keeping in stick *all* positive blocks so far found, may be replaced by certain stochastic algorithms for duplicate-free counting known from the domain of data bases (cf. Astrahan–Schkolnick–Whang [1] for an overview and Flajolet [4] for a close analysis). These algorithms, based on hashing procedures, avoid keeping in stock *all* positive blocks so far encountered and the comparison of new linear forms with all of them. As it is the case with all stochastic algorithms the resulting gain in efficiency is at the expense of an approximation error and an uncertainty of the result; error and uncertainty can, however, be controlled by stochastic methods. The stochastic algorithms can be used in an obvious way in Algorithm I and in the last inductive step (dimension $n-1$) of Algorithm II. We will give more details in a forthcoming paper.

(b) Notice that recursions instead of stacks could be used in both algorithms.

References

1. Astrahan, M. M., Schkolnick, M., Whang. K.-Y.: Approximating the number of unique values on an attribute without sorting. Inf. Syst. **12**, 11 15 (1987)
2. Buchberger, B.: Gröbner bases: An algorithmic method in polynomial ideal theory. Chap. 6 In: Recent trends in multidimensional system theory. Bose, N. K. (ed.) Dordrecht: Reidel 1985
3. Dirichlet, P. G. L.: Über die Bestimmung der mittleren Werthe der Zahlentheorie. Abhandlungen der Berlin Akademie (1849)
4. Flajolet, Ph.: On adaptive sampling. INRIA Rapports de Recherche #1025 (1989)
5. Knuth, D. E.: The art of computer programming, Vol. 2. Addison-Wesley, Reading, MA 1981
6. Mertens, F.: Über einige asymptotische Gesetze der Zahlentheorie. J. Reine Angew. Math. **77**, 289–291 (1874)
7. Mora, T., L. Robbiano: The Gröbner fan of an ideal. J. Symb. Comp. **6**, 183 208 (1988),
8. Robbiano, L.: Term orderings on the polynomial ring. In EUROCAL '85, Caviness, B. F. (ed.) Lecture Notes in Computer Science, vol. 204, pp. 513–517. Berlin, Heidelberg, New York: Springer 1985
9. Schwartz, N.: Stability of Gröbner bases. J. Pure Appl. Algebra **53**, 171–186 (1988)
10. Schwarz, F.: Monomial orderings and Gröbner bases. ACM SIGSAM Bulletin 25 (1) 10–23 (1991)
11. Titchmarsh, E. C.: The theory of the Riemann zeta-function. 2nd ed., Oxford University Press, Oxford, 1986
12. Weispfenning, V.: Admissible orders and linear forms. ACM SIGSAM Bulletin 21 (2) 16–18 (1987)
13. Weispfenning, V.: Constructing Universal Gröbner Bases. In: Proc. AAECC-5, Menorca, 1987, Huguet, L., Poli, A. (eds). Lecture Notes in Computer Science, vol. 356, pp. 408–417. Berlin, Heidelberg, New York: Springer 1989