Journal of Algebraic Combinatorics, 17, 171–180, 2003

Gröbner Bases for Complete Uniform Families

GÁBOR HEGEDŰS
LAJOS RÓNYAI ronyai@sztaki.hu
Computer and Automation Institute, Hungarian Academy of Sciences and Budapest University of Technology and Economics, Hungary

Received November 14, 2001; Revised August 9, 2002

Abstract. We describe (reduced) Gröbner bases of the ideal of polynomials over a field, which vanish on the set of characterisic vectors of the complete unifom families $\binom{[n]}{d}$. An interesting feature of the results is that they are largely independent of the monomial order selected. The bases depend only on the ordering of the variables. We can thus use past results related to the *lex* order in the presence of degree-compatible orders, such as *deglex*. As applications, we give simple proofs of some known results on incidence matrices.

Keywords: Gröbner basis, uniform family, inclusion matrix, Hilbert function

1. Introduction

First we introduce some notation. Let n be a positive integer and $[n]$ stand for the set $\{1, 2, \ldots, n\}$. The family of all subsets of $[n]$ is denoted by $2^{[n]}$. For an integer $0 \leq d \leq n$ we denote by $\binom{[n]}{d}$ the family of all d element subsets of $[n]$.

Let K be a field. As usual, $K[x_1, \ldots, x_n]$ denotes the ring of polynomials in variables $x_1, \ldots, x_n$ over K. For a subset $F \subseteq [n]$ we write $x_F = \prod_{j \in F} x_j$, and $x^F = \prod_{j \in F}(x_j - 1)$. In particular, $x_\emptyset = x^\emptyset = 1$.

Let $v_F \in \{0, 1\}^n$ denote the characteristic vector of a set $F \subseteq [n]$. For a family of subsets $\mathcal{F} \subseteq 2^{[n]}$, let $V(\mathcal{F}) = \{v_F : F \in \mathcal{F}\} \subseteq \{0, 1\}^n \subseteq K^n$. A polynomial $f \in K[x_1, \ldots, x_n] = S$ can be considered as a function from $V(\mathcal{F})$ to K in the straightforward way.

Several interesting results on finite set systems $\mathcal{F} \subseteq 2^{[n]}$ can be naturally fomulated as statements concerning *polynomial functions on* $V(\mathcal{F})$. For instance, certain inclusion matrices (see Section 3) can be viewed naturally in this setting. Also, the approach to the complexity of Boolean functions, initiated by Smolensky [13] and developed further by Bernasconi and Egidi [8], leads to such questions.

To study the polynomial functions on $V(\mathcal{F})$, it is natural to consider the ideal $I(V(\mathcal{F}))$:

$$I(V(\mathcal{F})) := \{f \in S : f(v) = 0 \quad \text{whenever } v \in V(\mathcal{F})\}.$$

In fact, substitution gives rise to a K-homomorphism from S to the ring of K-valued functions on $V(\mathcal{F})$. This homomorphism is seen to be surjective by an easy interpolation argument, and the kernel is exactly $I(V(\mathcal{F}))$. This way one can identify $S/I(V(\mathcal{F}))$ with the space of K valued functions on $V(\mathcal{F})$. In particular, $\dim_K S/I(V(\mathcal{F})) = |\mathcal{F}|$.

Our aim here is to describe Gröbner bases for the ideals $I_d = I(V(\binom{[n]}{d}))$, i.e. when $\mathcal{F}$ is the full family of d-sets of $[n]$.

1.1. Gröbner bases and standard monomials

We recall now some basic facts concerning Gröbner bases in polynomial rings. A total order $\prec$ on the monomials composed from variables $x_1, x_2, \dots, x_m$ is a *term order*, or *monomial order*, if 1 is the minimal element of $\prec$, and $uw \prec vw$ holds for any monomials u, v, w with $u \prec v$. Two important term orders are the lexicographic order $\prec_l$ and the deglex order $\prec_{dl}$. We have

$$x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \prec_l x_1^{j_1} x_2^{j_2} \cdots x_m^{j_m}$$

iff $i_k < j_k$ holds for the smallest index k such that $i_k \neq j_k$. As for deglex, we have $u \prec_{dl} v$ iff either $\deg u < \deg v$, or $\deg u = \deg v$, and $u \prec_l v$.

The *leading monomial* $\mathrm{lm}(f)$ of a nonzero polynomial $f \in S$ is the largest (with respect to $\prec$) monomial which appears with nonzero coefficient in f when written as a linear combination of monomials.

Let I be an ideal of S. A finite subset $G \subseteq I$ is a *Gröbner basis* of I if for every $f \in I$ there exists a $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. In other words, the leading monomials of the polynomials from G generate the semigroup ideal of monomials $\{\mathrm{lm}(f) : f \in I\}$. From the properties of the order $\prec$ it follows that G is actually a basis of I, i.e. G generates I as an ideal of S. It is a fundamental fact (cf. [10, Chapter 1, Corollary 3.12] or [1, Corollary 1.6.5, Theorem 1.9.1]) that every nonzero ideal I of S has a Gröbner basis.

A monomial $w \in S$ is called a *standard monomial for* I if it is not a leading monomial of any $f \in I$. Let $\mathrm{sm}(I)$ stand for the set of all standard monomials of I. It follows from the definition and existence of Gröbner bases (see [10, Chapter 1, Section 4]) that for a nonzero ideal I of S the set of monomials $\mathrm{sm}(I)$ is downward closed: if $w \in \mathrm{sm}(I)$, u, v are monomials from S such that $w = uv$ then $u \in \mathrm{sm}(I)$. Also, $\mathrm{sm}(I)$ is a basis of the K-vectorspace S/I. More precisely, every $g \in S$ can be written uniquely as $h + f$ where $f \in I$ and h is a unique K-linear combination of monomials from $\mathrm{sm}(I)$.

A Gröbner basis $\{f_1, \dots f_m\}$ of I is *reduced* if the coefficient of $\mathrm{lm}(f_i)$ is 1, and no nonzero monomial in f_i is divisible by any $\mathrm{lm}(f_j)$, $j \neq i$. By a theorem of Buchberger ([1, Theorem 1.8.7]) a nonzero ideal has a unique reduced Gröbner basis with respect to any term order $\prec$.

The *initial ideal* $in(I)$ of I is the ideal in S generated by the monomials $\{\mathrm{lm}(f) : f \in I\}$.

1.2. The main result

The main contribution of the paper is an explicit description of the reduced Gröbner bases for the ideals $I(V(\binom{[n]}{d}))$.

Let t be a integer, $0 < t \leq n/2$. We define $\mathcal{H}_t$ as the set of those subsets $H = \{s_1 < s_2 < \cdots < s_t\}$ of $[n]$ for which t is the smallest index j with $s_j < 2j$. Thus, the elements of $\mathcal{H}_t$

are t-subsets of $[n]$. We have $H \in \mathcal{H}_t$ iff $s_1 \geq 2, \dots, s_{t-1} \geq 2t-2$ and $s_t < 2t$. It follows that $s_t = 2t-1$, and if $t > 1$, then $s_{t-1} = 2t-2$.

For the first few values of t it is easy to give $\mathcal{H}_t$ explicitly: we have $\mathcal{H}_1 = \{\{1\}\}$, $\mathcal{H}_2 = \{\{2,3\}\}$, and $\mathcal{H}_3 = \{\{2,4,5\},\{3,4,5\}\}$, and

$$\mathcal{H}_4 = \{\{2,4,6,7\},\{2,5,6,7\},\{3,4,6,7\},\{3,5,6,7\},\{4,5,6,7\}\}.$$

For a subset $J \subseteq [n]$ and an integer $0 \leq i \leq |J|$ we denote by $\sigma_{J,i}$ the i-th elementary symmetric polynomial of the variables x_j, $j \in J$:

$$\sigma_{J,i} := \sum_{T \subseteq J, |T| = i} x_T \in K[x_1, \dots, x_n].$$

In particular, $\sigma_{J,0} = 1$.

Now let $0 < t \leq n/2$, $0 \leq d \leq n$ and $H \in \mathcal{H}_t$. Put

$$H' = H \cup \{2t, 2t+1, \dots, n\} \subseteq [n].$$

We write

$$f_{H,d} = f_{H,d}(x_1, \dots, x_n) := \sum_{k=0}^{t} (-1)^{t-k} \binom{d-k}{t-k} \sigma_{H',k}.$$

Specifically, we have $f_{\{1\},d} = x_1 + x_2 + \cdots + x_n - d$, and

$$f_{\{2,3\},d} = \sigma_{U,2} - (d-1)\sigma_{U,1} + \binom{d}{2},$$

where $U = \{2, 3, \dots, n\}$.

Our main result follows. We denote the ideal $I(V(\binom{[n]}{d}))$ by I_d.

Theorem 1.1 *Let d, n be integers, $n > 0$ and $0 \leq d \leq n/2$. Let K be a field, and $\prec$ be an arbitrary term order on the monomials of $S = K[x_1, \dots, x_n]$ for which $x_n \prec x_{n-1} \prec \cdots \prec x_1$. Then the following set $\mathcal{G}$ of polynomials is a Gröbner basis with respect to $\prec$ of the ideal I_d of S:*

$$\mathcal{G} = \{x_1^2 - x_1, \dots, x_n^2 - x_n\} \cup \left\{x_J \;:\; J \in \binom{[n]}{d+1}\right\}$$
$$\cup \{f_{H,d} \;:\; H \in \mathcal{H}_t \text{ for some } 0 < t \leq d\}.$$

Similarly, the set $\mathcal{G}^*$ below is a Gröbner basis of I_{n-d}:

$$\mathcal{G}^* = \{x_1^2 - x_1, \dots, x_n^2 - x_n\} \cup \left\{x^J \;:\; J \in \binom{[n]}{d+1}\right\}$$
$$\cup \{f_{H,n-d} \;:\; H \in \mathcal{H}_t \text{ for some } 0 < t \leq d\}.$$

A partial result in this direction was obtained in [4], which is based on the notion of order shattering. Here we recall only the facts that are relevant to our discussion. Let K be a field.

Theorem 1.2 (Anstee, Rónyai, Sali, [4]) *Let* $0 \leq d \leq n/2$ *and denote by* $\mathcal{M} = \mathcal{M}_d$ *the set of all monomials* x_G *such that* $G = \{s_1 < s_2 < \cdots < s_j\} \subset [n]$ *for which* $j \leq d$ *and* $s_i \geq 2i$ *holds for* $1 \leq i \leq j$. *Then* $\mathcal{M}$ *is the set of standard monomials for* I_d *as well as for* I_{n-d} *with respect to the lexicographic order* $\prec_l$. *In particular*, $|\mathcal{M}| = \binom{n}{d}$ *and* $\mathcal{M}$ *constitutes a* K *basis of the space of functions from* $V\binom{[n]}{d}$ *to* K (*from* $V\binom{[n]}{n-d}$ *to* K, *resp.*).

For proofs the reader is referred to Theorem 4.3, Lemmas 2.2 and 2.3 in [4].

Theorem 1.1 allows us to describe the initial ideals and reduced Gröbner bases of the ideals I_d. Let n, K and $\prec$ be as in Theorem 1.1. It will be convenient to treat separately the (trivial) cases $d = 0$ or $d = n$. It is immediate that $\text{in}(I_0) = \text{in}(I_n) = (x_1, \ldots, x_n)$, and this is a minimal generating set. Similarly, $\{x_1, x_2, \ldots, x_n\}$ and $\{x_1 - 1, x_2 - 1, \ldots, x_n - 1\}$ are the reduced Gröbner bases of I_0 and I_n, respectively.

Let $\mathcal{D}_d$ denote the collection of subsets $U \subset [n]$, where $U = \{u_1 < \cdots < u_{d+1}\}$ and $u_j \geq 2j$ holds for $j = 1, \ldots, d$.

Corollary 1.3 *Assume that* $0 < d \leq n/2$. *The set of monomials*

$$\cup_{t=1}^{d}\{x_H : H \in \mathcal{H}_t\} \cup \{x_U : U \in \mathcal{D}_d\} \cup \left\{x_i^2 : i = 2, \ldots, n\right\}$$

minimally generates in$(I_d) =$ *in*(I_{n-d}).

It turns out that a subset of $\mathcal{G}$ ($\mathcal{G}^*$ resp.) is the reduced Gröbner basis of I_d (I_{n-d} resp.).

Corollary 1.4 *Let* n, K, *and* $\prec$ *as in Theorem* 1.1, *and* $0 < d \leq n/2$. *Then the following set of polynomials is the reduced Gröbner basis with respect to* $\prec$ *of the ideal* I_d:

$$\left\{x_2^2 - x_2, \ldots, x_n^2 - x_n\right\} \cup \{x_J : J \in \mathcal{D}_d\} \cup \{f_{H,d} : H \in \mathcal{H}_t \textit{ for some } 0 < t \leq d\}.$$

Similarly, the following set is the reduced Gröbner basis of I_{n-d}:

$$\left\{x_2^2 - x_2, \ldots, x_n^2 - x_n\right\} \cup \{x^J : J \in \mathcal{D}_d\} \cup \{f_{H,n-d} : H \in \mathcal{H}_t \textit{ for some } 0 < t \leq d\}.$$

The functions $f_{H,d}$ play a prominent role in our discussion. Next we provide an alternative description for them. Let $H \in \mathcal{H}_t$, and $H' = H \cup \{2t, 2t+1, \ldots, n\} \subseteq [n]$, as before. Let $l_{H'} = l_{H'}(x_1, \ldots, x_n) := \sum_{j \in H'} x_j$ and denote by $g_{H,d}$ the linear combination of squarefree monomials obtained from

$$\prod_{j=0}^{t-1}(l_{H'} - d + j)$$

by application of the relations $x_i^2 = x_i$.

Proposition 1.5 *Let* $0 \le d \le n$ *and* $H \in \mathcal{H}_t$ *for some* $0 < t \le n/2$. *Assume that* $\operatorname{char} K = 0$, *or* $\operatorname{char} K > t$. *Then we have* $f_{H,d} = (1/t!)g_{H,d}$.

In Section 2 we prove the preceding statements. These are followed by some consequences and concluding remarks.

2. Proofs

We write $I_d = I(V(\binom{[n]}{d}))$.

Lemma 2.1 *Assume that* $0 < t \le n/2$, $H \in \mathcal{H}_t$, *and* $0 \le d \le n$. *Then* $f_{H,d} \in I_d$.

Proof: Let $D \in \binom{[n]}{d}$ and let $v = v_D$ be the characteristic vector of D. The set $H' = H \cup \{2t, \dots, n\}$ has $n - t + 1$ elements, hence

$$|D \cap H'| \in \{d, d-1, \dots, d-t+1\}. \tag{1}$$

Now

$$f_{H,d}(v) = \sum_{k=0}^{t} (-1)^{t-k} \binom{d-k}{t-k} \sigma_{H',k}(v) = \sum_{k=0}^{t} (-1)^{t-k} \binom{d-k}{t-k} \binom{|D \cap H'|}{k}.$$

We intend to use the following identity involving binomial coefficients

$$\binom{x-d+t-1}{t} = \sum_{k=0}^{t} (-1)^{t-k} \binom{x}{k} \binom{d-k}{t-k}, \tag{2}$$

valid for every $x \in \mathbb{C}$, $d \in \mathbb{Z}$ and $t \in \mathbb{Z}^+$. From (2) we infer that

$$f_{H,d}(v) = \binom{|D \cap H'| - d + t - 1}{t},$$

which is indeed 0 because of (1).

It remains to verify (2). One may start out with a version of the familiar Vandermonde identity ([12], pp. 169–170)

$$\binom{x+s}{t} = \sum_{k=0}^{t} \binom{x}{k} \binom{s}{t-k},$$

which holds for all $x, s \in \mathbb{C}$ and $t \in \mathbb{Z}^+$. By negating the upper index s on the right-hand side we obtain

$$\binom{x+s}{t} = \sum_{k=0}^{t} \binom{x}{k} (-1)^{t-k} \binom{t-s-k-1}{t-k},$$

from which the substitution $s = t - d - 1$ gives (2). □

Lemma 2.2 *Assume that* $0 < t \le n/2$, $H \in \mathcal{H}_t$ *and* $0 \le d \le n$. *Then* $f_{H,d}$ *can be written as a linear combination of squarefree monomials*

$$f_{H,d} = \sum_{U \subseteq H',\ |U| \le t} \alpha_U x_U, \tag{3}$$

where $\alpha_U \in K$. *The leading monomial of* $f_{H,d}$ *with respect to* $\prec$ *is* x_H *and the leading coefficient is* $\alpha_H = 1$. *Also we have* $x_H \notin \mathcal{M}$, *but* $x_U \in \mathcal{M}$ *for any other nonzero term* x_U *of* (3).

Proof: The statement about the form (3) follows from the fact that the (elementary) symmetric polynomials $\sigma_{H',i}$ $(0 \le i \le t)$ are linear combinations of monomials x_U with $U \subset H'$ and $|U| \le t$. Let $U = \{u_1 < \cdots < u_j\}$ be any such subset and write $H = \{s_1 < \cdots < s_t\}$. By the definition of H' we have $s_i \le u_i$ for $i = 1, \ldots, j$, hence $x_U \preceq x_{s_1} \cdots x_{s_j} \preceq x_H$. Also, the coefficient of x_H in $f_{H,d}$ is $(-1)^{t-t}\binom{d-t}{t-t} = 1$. These imply that x_H is the leading monomial of $f_{H,d}$.

It is immediate that $x_H \notin \mathcal{M}$ because $s_t = 2t - 1$. Finally, if $U \ne H$, then $2i \le s_i \le u_i$ hold for $i \le \min\{j, t-1\}$, giving the last statement for $j < t$. If $j = t$ then from $U \ne H$ we infer additionally that $u_t > s_t = 2t - 1$. The proof is complete. □

Proof of Theorem 1.1: Let d, n be integers, $n > 0$ and $0 \le d \le n/2$. It is immediate that $x_i^2 - x_i \in I_d$ and $x_J \in I_d$ if $|J| = d + 1$, hence by Lemma 2.1 $\mathcal{G} \subseteq I_d$. Similarly we obtain that $\mathcal{G}^* \subseteq I_{n-d}$.

To show that $\mathcal{G}$ is a Gröbner basis of I_d we use the following characterization of Gröbner bases (see Theorem 3.10 in Chapter 1 of [10], or Theorem 1.9.1 in [1]):

A nonempty set $\mathcal{G}$ *of polynomials is a Gröbner basis of the ideal* I *generated by* $\mathcal{G}$ *iff every* $f \in I$ *reduces to zero with respect to* $\mathcal{G}$.

Here *reduction* means that we possibly repeatedly replace monomials in f by smaller ones (with respect to $\prec$) as follows: if w is a monomial occurring in f and $\mathrm{lm}(g)$ divides w for some $g \in \mathcal{G}$ (i.e. $w = \mathrm{lm}(g)u$ for some monomial u), then we replace w in g with $u(\mathrm{lm}(g) - g)$. Clearly the monomials in $u(\mathrm{lm}(g) - g)$ are $\prec$-smaller than w.

Obviously we can reduce any monomial which is divisible by x_i^2 for some i. We can thus assume that f contains only squarefree monomials x_U, $U \subseteq [n]$. We can also eliminate those x_U for which $|U| > d$.

If x_U $(|U| \le d, U = \{u_1 < u_2 < \cdots < u_j\})$ is a monomial not in $\mathcal{M}_d$, then there is an index $i \le j$ such that $u_i < 2i$. Let t be the smallest such index i. Then

$$\{u_1 < \cdots < u_t\} =: H \in \mathcal{H}_t$$

and x_H divides x_U. By Lemma 2.2 x_H is the leading monomial of $f_{H,d} \in \mathcal{G}$, hence via $f_{H,d}$ we can reduce f further.

We have obtained so far that, using $\mathcal{G}$, any $f \in S$ can be reduced to a linear combination

$$\sum_{w \in \mathcal{M}_d} \alpha_w w, \tag{4}$$

where $\alpha_w \in K$. Let I be the ideal of S generated by $\mathcal{G}$. From (4) and Theorem 1.2 we deduce first that

$$\dim_K S/I \leq |\mathcal{M}_d| = \binom{n}{d} = \dim_K S/I_d. \tag{5}$$

On the other hand, Lemma 2.1 implies that $I \subseteq I_d$, hence we have $I = I_d$.

Finally, if we reduce an $f \in I_d$ into a form (4), then every α_w is zero by Theorem 1.2, because $\mathcal{M}_d$ is a basis of the space of functions from $V(\binom{[n]}{d})$ to K. This proves that $\mathcal{G}$ is a Gröbner basis of I_d.

Essentially the same argument works for I_{n-d}. Note that the leading term of a polynomial x^J, $|J| = d + 1$ is x_J and all other terms have degree at most d. These polynomials and $x_i^2 - x_i$ allow us to reduce any polynomial f into one of degree at most d. From here reduction via $f_{H,n-d}$ where $H \in \mathcal{H}_t$ and $0 < t \leq d$ and $x_i^2 - x_i$ gives a linear combination of type (4). If $f \in I_{n-d}$ then every α_w is zero by Theorem 1.2, therefore $\mathcal{G}^*$ is a Gröbner basis of I_{n-d}. □

Proof of Corollary 1.3: Let $\mathcal{W}$ denote the set of monomials given in the statement. Clearly we have $\mathcal{W} \subset \text{in}(I_d)$ and $\mathcal{W} \subset \text{in}(I_{n-d})$. To show that $\mathcal{W}$ is a generating set, it suffices then to verify, that any monomial $w \notin \mathcal{M}_d$ is divisible by an element of $\mathcal{W}$. This is immediate if x_1 divides w because $\{1\} \in \mathcal{H}_1$. Otherwise if w is not squarefree, then it is divisible by x_i^2 for some $2 \leq i \leq n$. We can therefore assume that $w = x_U$ for some $U = \{u_1 < \cdots < u_j\} \subseteq [n]$ and either there exists an $0 < i \leq d$ such that $u_i < 2i$, or $j > d$. If the first case occurs here, then let t be the smallest index i with $u_i < 2i$. Then for $H = \{u_1, \ldots, u_t\}$ we have $H \in \mathcal{H}_t$, hence $x_H \in \mathcal{W}$ and x_H divides w. If only the second case applies to w, then for $H = \{u_1, \ldots, u_{d+1}\}$ we have $H \in \mathcal{D}_d$, hence $x_H \in \mathcal{W}$, moreover x_H again divides w.

Minimality follows because there are no nontrivial divisibilities among the elements of $\mathcal{W}$. □

Proof of Corollary 1.4: From Corollary 1.3 we see that the leading terms of the sets of polynomials given in the statement are minimal generating sets of the initial ideals of I_d (I_{n-d} respectively). Reducedness follows from the fact that all other (i.e. non-leading) monomials in the polynomials are actually standard monomials for I_d (and for I_{n-d} as well). This has been proven for $f_{H,d}$ and $f_{H,n-d}$ in Lemma 2.2. Also, $x_i \in \mathcal{M}_d$ for $i = 2, \ldots, n$.

Finally let us consider the polynomials x^J, where $J = \{j_1 < \cdots < j_{d+1}\} \in \mathcal{D}_d$. If $U = \{u_1 < \cdots < u_k\} \subset J$ with $k = |U| \leq d$, then $u_i \geq j_i \geq 2i$ holds whenever $1 \leq i \leq k$, hence $x_U \in \mathcal{M}_d$. We conclude that the non-leading monomials of x^J are standard monomials, and this completes the proof. □

Proof of Proposition 1.5: Simple direct calculation shows that

$$\frac{1}{t!} g_{H,d} = x_H + g_1,$$

where g_1 is a linear combination of squarefree monomials x_U, with $U \subseteq H'$, $|U| \leq t$ and $U \neq H$. We have $x_H \notin \mathcal{M}_d$, and as in Lemma 2.2, we infer that the monomials of g_1

are from $\mathcal{M}_d$. The same Lemma 2.2 gives that $f_{H,d} = x_H + g_2$, where g_2 is also a linear combination over $\mathcal{M}_d$.

Both $f_{H,d}$ and $g_{H,d}$ vanish on $V(\binom{[n]}{d})$, hence $g_1 - g_2 \in I_d$. The set of standard monomials $\mathcal{M}_d$ is linearly independent modulo I_d, giving that $g_1 = g_2$. □

3. Some consequences

Let I be an ideal of $S = K[x_1, \ldots, x_n]$. The *Hilbert function* of the algebra S/I is the sequence $h_{S/I}(0), h_{S/I}(0), \ldots$. Here $h_{S/I}(m)$ is the dimension over K of the factorspace $S_{\leq m}/I_{\leq m}$, where $S_{\leq m}$ ($I_{\leq m}$ resp.) is the set of elements of S (of I, resp.) with degree at most m (see [7, Section 9.3]).

In the case when $I = I(V(\mathcal{F}))$ for some set system $\mathcal{F} \subseteq 2^{[n]}$, then $h_{\mathcal{F}}(m) := h_{S/I}(m)$ is the dimension of the space of functions from $V(\mathcal{F})$ to K which can be represented as polynomials of degree at most m.

In the combinatorial literature these important quantities are expressed in terms of inclusion matrices, see for example [6]. For families $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ the *inclusion matrix* $I(\mathcal{F}, \mathcal{G})$ is a (0,1) matrix of size $|\mathcal{F}| \times |\mathcal{G}|$ whose rows and columns are indexed by the elements of $\mathcal{F}$ and $\mathcal{G}$, respectively. The entry at position (F, G) is 1 if $G \subseteq F$ and 0 otherwise ($F \in \mathcal{F}, G \in \mathcal{G}$). It is straightforward to verify that $h_{\mathcal{F}}(m) = \operatorname{rank}_K I(\mathcal{F}, \binom{[n]}{\leq m})$.

On the other hand, $h_{S/I}(m)$ is the number of standard monomials of degree at most m with respect to an arbitrary degree-compatible term order, for instance deglex.

By Theorem 1.1 the set of deglex standard monomials of $\binom{[n]}{d}$ is $\mathcal{M}_k$, where $k = \min\{d, n-d\}$. Now if $0 \leq m \leq k$, then the set of monomials from $\mathcal{M}_k$ of degree at most m is precisely $\mathcal{M}_m$. We have the following

Corollary 3.1 (Wilson [14]) *Let* $0 \leq d \leq n$, $0 \leq m \leq \min\{d, n-d\}$, *and* K *be an arbitrary field. Then we have*

$$h_{\binom{[n]}{d}}(m) = \binom{n}{m}. \tag{6}$$

As a further application we give a simple proof of a theorem of Frankl [11, Theorem 1.1]. Let p be a prime and $d \in \mathbb{Z}$. Let

$$\mathcal{F}_d := \{F \subseteq [n] : |F| \equiv d \pmod{p}\}.$$

Corollary 3.2 (Frankl) *Assume that* $0 \leq m < p$ *and* $m \leq n/2$. *Then over* $K = \mathbb{F}_p$ *we have*

$$h_{\mathcal{F}_d}(m) \leq \binom{n}{m}.$$

Proof: We work over the field $K = \mathbb{F}_p$. Let $0 < t \leq m$ and $H \in \mathcal{H}_t$. We observe that $f_{H,d} = f_{H,d'}$, as polynomials over $\mathbb{F}_p$, whenever $d \equiv d' \pmod{p}$. This follows because for $0 \leq k \leq t$ we have

$$\binom{d-k}{t-k} \equiv \binom{d'-k}{t-k} \pmod{p},$$

a consequence of $0 \leq t-k \leq m < p$.

Now Lemma 2.1 implies that the polynomials $f_{H,d}$ vanish on $V(\mathcal{F}_d)$, whenever $H \in \mathcal{H}_t$ for some $0 < t \leq m$. Let $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a polynomial of degree at most m. Using the polynomials $f_{H,d}$ above, and $x_i^2 - x_i$, we can reduce f into a linear combination over $\mathbb{F}_p$ of monomials from $\mathcal{M}_m$, as in the proof of Theorem 1.1. This imples that

$$h_{\mathcal{F}_d}(m) \leq |\mathcal{M}_m| = \binom{n}{m}. \qquad \square$$

4. Concluding remarks

It would be desirable to obtain similar results for other families $\mathcal{F} \subseteq 2^{[n]}$, with possible applications to inclusion matrices and to the complexity of Boolean functions (see [8] for the latter). In particular, Gröbner bases for symmetric families (i.e., which are invariant under the action of the symmetric group on $[n]$) would be of interest.

Aigner [2] gave a remarkable explicit decomposition of $2^{[n]}$ into symmetric chains. The bottommost elements of the chains are exactly the sets $U \subset [n]$ for which $x_U \in \mathcal{M}_{\lfloor n/2 \rfloor}$, the set of standard monomials for $\binom{[n]}{\lfloor n/2 \rfloor}$. It would perhaps be interesting to obtain an algebraic explanation of the results in [2].

Acknowledgment

We are grateful to Kati Friedl for her useful remarks.

Research supported in part by OTKA and NWO-OTKA grants, and the EU-COE Grant of MTA SZTAKI.

References

1. W.W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, 1994.
2. M. Aigner, "Lexicographic matching in Boolean algebras," *Journal of Combinatorial Theory*, Ser. B **14** (1973), 187–194.
3. R.E.L. Aldred and R.P. Anstee, "On the density of sets of divisors," *Discrete Math.* **137** (1995), 345–349.
4. R.P. Anstee, L. Rónyai, and A. Sali, "Shattering news," *Graphs and Combinatorics* **18** (2002), 59–73.
5. R.P. Anstee and A. Sali, "Sperner families of bounded *VC*-dimension," *Discrete Math.* **175** (1997), 13–21.
6. L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics*, September 1992.
7. T. Becker and V. Weispfenning, *Gröbner Bases—A Computational Approach to Commutative Algebra*, Springer-Verlag, Berlin, 1993.
8. A. Bernasconi and L. Egidi, "Hilbert function and complexity lower bounds for symmetric Boolean functions," *Information and Computation* **153** (1999), 1–25.
9. T. Bier,"Remarks on recent formulas of Wilson and Frankl," *Europ. J. Combin.* **14** (1993), 1–8.

10. A.M. Cohen, H. Cuypers, and H. Sterk (Eds.), *Some Tapas of Computer Algebra,* Springer-Verlag, Berlin, 1999.
11. P. Frankl, "Intersection theorems and mod p rank of inclusion matrices," *J. Combin. Theory* A **54** (1990), 85–94.
12. R.L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics,* Addison-Wesley, 1989.
13. R. Smolensky, "On representations by low-degree polynomials," in *Proc. of the 34th IEEE Symposium on the Foundations of Computer Science*, 1993, pp. 130–138.
14. R.M. Wilson, "A diagonal form for the incidence matrices of t-subsets vs. k-subsets," *Europ. J. Combin.* **11** (1990), 609–615.