Annales Univ. Sci. Budapest., Sect. Comp. 29 (2008) 175-198

ON THE HILBERT FUNCTION OF COMPLEMENTARY SET FAMILIES

D. Pintér and L. Rónyai
(Budapest, Hungary)

Dedicated to Professor Imre Kátai on the occasion of his 70th birthday

Abstract. We prove a relation connecting the Hilbert function of a set family $\mathcal{F} \subseteq 2^{[n]}$ to the Hilbert function of the complementary family $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$. Our argument works over ground rings including all fields and the rings $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. The result gives a min-max characterization of the smallest degree of a nontrivial polynomial that vanishes on the set of incidence vectors of $\mathcal{F}$. As an application, we give a new lower bound on the weak degree over $\mathbb{Z}_6$ of the Boolean function $\neg MOD_6$.

1. Introduction

$\mathbb{N}$ denotes the set of nonnegative integers, $\mathbb{Z}$ the integers. For a positive integer n let $[n]$ stand for the set $\{1, 2, \ldots, n\}$. The family of all subsets of $[n]$ is denoted by $2^{[n]}$.

Throughout the paper R denotes a commutative ring, whose identity element is denoted by 1. We shall also assume that R has a finite length

Research supported in part by OTKA grants T42706, T42481, NK63066, and the Center for Applied Mathematics and Computational Physics of the BUTE. Part of this work was done during the Special Semester on Gröbner Bases, 2006, organized by RICAM, Austrian Academy of Sciences and RISC, Johannes Kepler University, Linz, Austria.

as an R-module. We denote this length by ℓ. We write $\ell(M)$ for the length of an R-module M.

For the main results we need stronger assumptions on R. Let t be a positive integer and let R^t be the free R-module over R which we identify now with the set of vectors $(\alpha_1, \ldots, \alpha_t)$, $\alpha_i \in R$. Let $(,) : R^t \times R^t \to R$ be the standard bilinear form on R^t: for $u = (\alpha_1, \ldots, \alpha_t)$ and $v = (\beta_1, \ldots, \beta_t)$ we set $(u, v) := \sum_{j=1}^{t} \alpha_j \beta_j$.

For a submodule $K \leq R^t$ we define the orthogonal $K^\perp \leq R^t$ in the usual way:

$$K^\perp = \{u \in R^t : \ (u, v) = 0 \text{ for every } \ v \in K\}.$$

We call a ring R as above a *D-ring*, if $K^{\perp\perp} = K$ holds for every positive integer t and submodule $K \leq R^t$. Our duality theorem will hold over D-rings. Please note that any field is a D-ring. We will show in Section 3 that the modulo m residue class rings $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ (here m is a positive integer) are D-rings as well. More generally, rings of the form R^*/I are D-rings, where R^* is a principal ideal domain and I is a nonzero ideal in R^*.

We denote by $S = R[x_1, \ldots, x_n]$ the ring of polynomials in variables $x_1, \ldots, x_n$ over R.

For a subset $F \subseteq [n]$ we write $x_F = \prod_{j \in F} x_j$. In particular, $x_\emptyset = 1$.

Let

$$v_F = (v_1, v_2, \ldots, v_n) \in \{0, 1\}^n$$

denote the characteristic vector of a set $F \subseteq [n]$. We have $v_i = 1$ iff $i \in F$. For a family of subsets $\mathcal{F} \subseteq 2^{[n]}$, let $V(\mathcal{F}) = \{v_F : F \in \mathcal{F}\} \subseteq \{0, 1\}^n \subseteq R^n$. A polynomial $f \in S = R[x_1, \ldots, x_n]$ can be considered as a function from $V(\mathcal{F})$ to R in the straightforward way. Let $T_j(\mathcal{F})$ be the set of functions from $V(\mathcal{F})$ to R which can be represented as polynomials from S of degree at most j (here $j = 0, 1 \ldots$). Clearly $T_j(\mathcal{F})$ is an R-module.

The study of polynomial functions from $V(\mathcal{F})$ to R has become an important approach in extremal combinatorics, in the case when R is a field. We refer to Babai, Frankl [4] and Alon [1] for results of this type.

We call the numerical sequence $\ell(T_0(\mathcal{F})), \ell(T_1(\mathcal{F})), \ldots$ the *Hilbert function of* $\mathcal{F}$. We shall write $h(\mathcal{F}, k)$ instead of $\ell(T_k(\mathcal{F}))$. If $R = \mathbb{F}$ is a field, then $h(\mathcal{F}, k)$ is just the dimension of $T_k(\mathcal{F})$ over $\mathbb{F}$.

We note next that every function from $V(\mathcal{F})$ to R can be obtained as a polynomial of degree at most n, hence

$$T_n(\mathcal{F}) = T_{n+1}(\mathcal{F}) = \cdots \text{ a free module of rank } \ |\mathcal{F}|, \tag{1}$$

and in particular $\ell(T_n(\mathcal{F})) = |\mathcal{F}|\ell$. Indeed, it suffices to observe that the characteristic function χ_F of a set $F \subseteq [n]$ (which is 1 on v_F and 0 on all other 0-1-vectors) is a polynomial function of degree at most n. If $v_F = (v_1, \dots, v_n)$, then

$$\chi_F = \prod_{i=1}^{n} \frac{x_i - \bar{v}_i}{v_i - \bar{v}_i},$$

where $\bar{v}_i$ is defined by $\bar{v}_i = 1 - v_i$. Note that the denominator is ± 1, hence we have a polynomial over R. We remark that the degree n we obtained for the polynomial representing χ_F can not be decreased. This may be proved by an easy counting argument.

In the combinatorial literature the quantities $h(\mathcal{F}, k)$ are usually expressed in terms of inclusion matrices, at least in the case $R = \mathbb{F}$. 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 ($F \in \mathcal{F}, G \in \mathcal{G}$).

Inclusion matrices and their ranks are quite useful in the combinatorics of finite set families. In Chapter 7 of [4] there is an excellent treatment of this subject which highlights the importance of inclusion matrices $I(\mathcal{F}, \mathcal{G})$ with $\mathcal{G} = \binom{[n]}{m}$ and $\mathcal{G} = \binom{[n]}{\leq m}$ (the family of all m-element subsets of $[n]$, and the collection of all sets $H \subseteq [n]$, where $|H| \leq m$, respectively).

It is a simple matter to verify that in the case $R = \mathbb{F}$

$$h(\mathcal{F}, k) = \operatorname{rank}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{\leq k}\right). \tag{2}$$

We refer to [4], [6], [10], [11], [9] for the computation of the Hilbert function of interesting set families and applications to discrete mathematics and computer science.

The main result of the paper is a duality type statement which connects the Hilbert functions of complementary set families.

Theorem 1.1. *Suppose that R is a D-ring, and let $\mathcal{F} \subseteq 2^{[n]}$ and $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$. We have*

$$h(2^{[n]}, k) = |\mathcal{G}|\ell + h(\mathcal{F}, k) - h(\mathcal{G}, n - 1 - k)$$

for every $k = 0, 1, \dots, n$.

Remarks. 1. The statement is valid when $\mathcal{F}$ or $\mathcal{G}$ is empty, if we agree to put $h(\emptyset, k) = 0$ for every k.

2. We set $h(\mathcal{F}, -1) = 0$.

3. We shall see (Proposition 2.2 and Lemma 2.4) that $h(2^{[n]}, k) = \sum_{j=0}^{k} \binom{n}{j} \ell$.

The statement of Theorem 1.1 was proved by Tadahito Harima for much more general point sets in the case when $R = \mathbb{F}$ is a field. In formula (3.1.5) of [8] the result is given for two disjoint finite point sets $\mathbb{X}, \mathbb{Y} \subset \mathbf{P}^n(\mathbb{F})$ in the projective n-space over $\mathbb{F}$, instead of $V(\mathcal{F})$ and $V(\mathcal{G})$, such that $\mathbb{X} \cup \mathbb{Y}$ is a complete intersection. The formula was used in his characterization of the Hilbert functions of Artinian Gorenstein algebras with the weak Stanley property.

Here we focus on 0,1-vectors only, but over more general ground rings, including the rings $\mathbb{Z}_m$, which are important in some recent applications to computer science. Also, our approach is quite elementary, it is based on direct computations with polynomial functions.

Theorem 1.1 allows us to formulate a min-max relation, which, we believe, may be interesting on its own right. We call a polynomial $f \in R[x_1, \ldots, x_n]$ *reduced*, if $f = \sum_{H \le [n]} \alpha_H x_H$ with $\alpha_H \in R$. Let $\mathcal{F} \subset 2^{[n]}$ be a family different from $\emptyset$ and $2^{[n]}$. Let $a(\mathcal{F})$ stand for the smallest degree of a nonzero reduced polynomial from S which vanishes on $V(\mathcal{F})$. We have $1 \le a(\mathcal{F}) \le n$.

Also, we define $b(\mathcal{F})$ to be the smallest integer k such that $h(\mathcal{F}, k) = |\mathcal{F}|\ell$. In other words, $b(\mathcal{F})$ is the smallest degree k such that every function from $V(\mathcal{F})$ to R can be represented by a polynomial from S of degree at most k. We have $0 \le b(\mathcal{F}) \le n$.

Using our earlier remark that the degree of any polynomial from S representing the characteristic function χ_v of a point $v \in \{0,1\}^n$ is at least n, it is immediate that

$$a(\mathcal{F}) + b(2^{[n]} \setminus \mathcal{F}) \ge n. \tag{3}$$

Theorem 1.1 implies that, in fact, we have an equality here.

Corollary 1.2. *Let $\mathcal{F} \subset 2^{[n]}$ and $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$. Assume that both $\mathcal{F}$ and $\mathcal{G}$ are nonempty. Then we have*

$$a(\mathcal{F}) + b(\mathcal{G}) = n.$$

Theorem 1.1 and Corollary 1.2 are proved in Section 2. In Section 3 we collected some simple facts for the reader's convenience, which easily imply that the rings $\mathbb{Z}_m$, where $m > 1$ is an integer, are actually D-rings. In Section 4 we give an application related to the complexity of Boolean functions. Corollary 4.1 presents an improved lower bound on the weak degree of the

function $\neg MOD_6$ over the ring $\mathbb{Z}_6$ (we refer to Subsection 4.1 for the relevant definitions). This Corollary will follow from the bound $b(\mathcal{F}) \leq \frac{5}{8}n + 2$, where $V(\mathcal{F})$ is the set of vectors from $\{0,1\}^n$ for which the number of 1 coordinates is divisible by 6 (Theorem 4.1).

2. The duality theorem

We shall work with graded rings A (which are graded with $\mathbb{N}$)

$$A = A_0 \oplus A_1 \oplus \cdots \oplus A_k \oplus \cdots \tag{4}$$

such that $A_0 = R$ and all the homogeneous components A_j have finite length as R-modules.

We shall often use the following basic facts (see e.g. pp. 92-93 in Matsumura [13]): if I is an ideal of A generated by homogeneous elements, then I and A/I are graded as well. We have

$$I = I_0 \oplus \cdots \oplus I_k \oplus \cdots$$

with some R-submodules $I_k \leq A_k$, and

$$A/I = B_0 \oplus B_1 \oplus \cdots \oplus B_k \oplus \cdots,$$

where $B_k \cong A_k/I_k$, for $k \geq 0$.

Proposition 2.1. *Let A be a graded ring as in (4). Suppose that $z \in A_1$ is a regular element (in the sense that z is not a zero divisor in A). Let $I = zA$ be the ideal generated by z in A. Then for*

$$A/I = B_0 \oplus B_1 \oplus \cdots \oplus B_k \oplus \cdots$$

we have $\ell(B_0) = \ell(A_0)$ and $\ell(B_i) = \ell(A_i) - \ell(A_{i-1})$ for $i > 0$. Here $\ell(M)$ denotes the length of an R-module M.

Proof. As z is homogeneous of degree 1, clearly we have $B_i \cong A_i/zA_{i-1}$ for $i > 0$ and $B_0 \cong A_0$. To conclude, it suffices to note that the map

$$A_{i-1} \xrightarrow{\cdot z} A_i \text{ which is given by } a \mapsto a \cdot z$$

is injective, hence then $\ell(A_{i-1}) = \ell(zA_{i-1})$. The injectivity of the map is equivalent to the regularity of z. We have

$$\ell(B_i) = \ell(A_i) - \ell(zA_{i-1}) = \ell(A_i) - \ell(A_{i-1})$$

whenever $i > 0$.

Let $\mathbb{X}$ denote the set of 0-1-vectors in R^{n+1} whose first coordinate is 1. We have $|\mathbb{X}| = 2^n$. We can consider the polynomials from the polynomial ring $S^* = R[z, x_1, \ldots, x_n]$ in the $n+1$ variables $z, x_1, \ldots, x_n$ as functions on $\mathbb{X}$. We shall also work with the polynomial ring $S = R[x_1, \ldots, x_n]$.

Recall that $v_F \in \{0,1\}^n \subseteq R^n$ is the characteristic vector of a set $F \subseteq [n]$. We shall also need the extended characteristic vector $w_F \in \mathbb{X} \subseteq R^{n+1}$, which is obtained as $w_F = (1, v_1, \ldots, v_n)$, where $(v_1, \ldots, v_n) = v_F$.

Let $\mathcal{F} \subseteq 2^{[n]}$ be a nonempty set family. In analogy with the notation $V(\mathcal{F})$ we put

$$W(\mathcal{F}) := \{w_F : \ F \in \mathcal{F}\} \subseteq \{0,1\}^{n+1}.$$

We have $V(\mathcal{F}) \subseteq R^n$ and $W(\mathcal{F}) \subseteq R^{n+1}$.

Let $Id(\mathcal{F})$ stand for the ideal of S^* which is generated by the homogeneous polynomials that vanish on $W(\mathcal{F})$. We have

$$Id(\mathcal{F}) = I_0(\mathcal{F}) \oplus I_1(\mathcal{F}) \oplus \cdots,$$

and

$$S^*/Id(\mathcal{F}) = U_0(\mathcal{F}) \oplus U_1(\mathcal{F}) \oplus \cdots, \tag{5}$$

where $U_j(\mathcal{F}) \cong S_j/I_j(\mathcal{F})$. Here S_j is the R-submodule of S^* consisting of the homogeneous polynomials of degree j and $I_j = Id(\mathcal{F}) \cap S_j$.

Recall that $T_j(\mathcal{F})$ is the set of functions from $V(\mathcal{F})$ to R which can be represented as polynomials from S of degree at most j.

Proposition 2.2. *As R-modules we have $T_j(\mathcal{F}) \cong U_j(\mathcal{F})$, for $j = 0, 1, \ldots$.*

Proof. Let $f(z, x_1, \ldots, x_n) \in S_j$ be a homogeneous polynomial of degree j. We map f to the function from $V(\mathcal{F})$ to R induced by the polynomial $f(1, x_1, \ldots, x_n) \in S$. Clearly this function is in $T_j(\mathcal{F})$. We defined a map $\phi : S_j \to T_j(\mathcal{F})$ which is an R-homomorphism. It is surjective: if a function g is induced by a polynomial $h(x_1, \ldots, x_n)$ of degree at most j, then $f(z, x_1, \ldots, x_n) := z^j h(x_1/z, \ldots, x_n/z)$ is in S_j and $\phi(f) = g$. Moreover, we have $\phi(f) = 0$ iff $f(1, x_1, \ldots x_n)$ vanishes on $V(\mathcal{F})$ iff $f(z, x_1, \ldots, x_n)$ vanishes on $W(\mathcal{F})$, iff $f \in I_j(\mathcal{F})$. This completes the proof.

Theorem 2.3. *Let $\mathcal{F} \subseteq 2^{[n]}$ be a nonempty set family. Then the image y of z in $S^*/Id(\mathcal{F})$ is regular. For*

$$S^*/(z, Id(\mathcal{F})) = P_0 \oplus P_1 \oplus \cdots \oplus P_n \oplus \cdots$$

we have $\ell(P_0) = h(\mathcal{F}, 0)$ *and* $\ell(P_i) = h(\mathcal{F}, i) - h(\mathcal{F}, i-1)$ *for* $i > 0$. *Moreover,* $\ell(S^*/(z, Id(\mathcal{F}))) = |\mathcal{F}|\ell$.

Proof. If a homogeneous polynomial $f \in S^*$ does not vanish on $W(\mathcal{F})$, then neither does zf, because the value of z is 1 on all vectors from $\mathbb{X}$, hence y is indeed regular. Next we write just U_j instead of the precise $U_j(\mathcal{F})$. By Proposition 2.1 we have $\ell(P_0) = \ell(U_0)$ and $\ell(P_i) = \ell(U_i) - \ell(U_{i-1})$ for $i > 0$. This gives the claim for $\ell(P_i)$ by Proposition 2.2. In particular by observation (1) we have $\ell(P_j) = 0$ and thus $P_j = (0)$ for $j > n$. We have therefore

$$\ell(S^*/(z, Id(\mathcal{F}))) = \sum_{i=0}^{n} \ell(P_i) = \ell(U_0) + \sum_{i=1}^{n} (\ell(U_i) - \ell(U_{i-1})) = \ell(U_n) = |\mathcal{F}|\ell.$$

We need more details in the case $\mathcal{F} = 2^{[n]}$, or in terms of incidence vectors, $W(\mathcal{F}) = \mathbb{X}$. Let $I = Id(\mathbb{X})$ denote the ideal of S^* generated by the homogeneous polynomials vanishing on $\mathbb{X}$. We write simply U_j instead of the more precise $U_j(\mathbb{X})$ (see (5)). Thus,

$$S^*/I = U_0 \oplus U_1 \oplus \cdots \oplus U_k \oplus \cdots.$$

Lemma 2.4. *We have*

$$I = (x_1^2 - x_1 z, x_2^2 - x_2 z, \ldots, x_n^2 - x_n z).$$

Moreover, U_k *is a free* R*-module with basis* $\{z^{k-|H|} x_H : H \subseteq [n],\ |H| \leq k\}$, *for* $k = 0, 1, \ldots$. *(For simplicity, we denote by* z *and* x_H *the image of* z *and* x_H *with respect to the canonical map* $S^* \to S^*/I$.*)*

Proof. Let J denote the ideal of S^* generated by the polynomials $x_i^2 - x_i z$. These polynomials are homogeneous and obviously vanish on $\mathbb{X}$, hence $J \subseteq I$. Let now $f \in S^*$ be a homogeneous polynomial of degree k. After subtracting from f suitable multiples of the $x_i^2 - x_i z$ we obtain an expression of the form

$$f = g + \sum_{H \subseteq [n],\ \ |H| \leq k} \alpha_H z^{k-|H|} x_H, \tag{6}$$

where $g \in J$ and $\alpha_H \in R$. It suffices to show now, that if f vanishes on $\mathbb{X}$, then $\alpha_H = 0$ for every $H \subseteq [n]$. Assume for contradiction, that there is an H with $\alpha_H \neq 0$. Let H^* be a minimal such subset of $[n]$ and substitute $w = w_{H^*}$ into f. From (6) and $f(w) = g(w) = 0$ we obtain that $\alpha_{H^*} = 0$, a contradiction which shows that $f \in J$, hence $I \subseteq J$.

The very same argument shows that for $H \subseteq [n]$, $|H| \leq k$ the monomials $z^{k-|H|}x_H \in S^*/I$ are linearly independent over R. In view of (6) they span U_k as an R-module. This completes the proof.

Put

$$Q = S^*/(z, I) = Q_0 \oplus \cdots \oplus Q_k \oplus \cdots . \tag{7}$$

Theorem 2.5. *We have $Q_j = (0)$ for $j > n$ and $\ell(Q) = \ell 2^n$. Moreover Q_k is a free R-module with free generators $\{x_H : H \subseteq [n],\ |H| = k\}$, hence $\ell(Q_k) = \binom{n}{k}\ell$ for $0 \leq k \leq n$.*

Proof. $\ell(Q) = \ell 2^n$ follows from Theorem 2.3 applied to $\mathcal{F} = \mathbb{X}$. Also, $Q_j = (0)$ holds for $j > n$, see the proof of Theorem 2.3. Note next that $Q_k \cong U_k/zU_{k-1}$. This holds also for $k = 0$ if we set $U_{-1} = (0)$. By Lemma 2.4 we obtain that (the image of) $\{x_H : H \subseteq [n],\ |H| = k\}$ spans Q_k as an R-module, and then $\ell(Q_k) \leq \ell\binom{n}{k}$.

Comparing lengths gives

$$\ell 2^n = \ell(Q) = \sum_{k=0}^{n} \ell(Q_k) \leq \sum_{k=0}^{n} \binom{n}{k}\ell = \ell 2^n.$$

We must have equality here, hence $\ell(Q_k) = \ell\binom{n}{k}$ for $k = 0, 1 \ldots, n$. Q_k has maximal length compared to the number of R-generators, therefore it is free and $\{x_H : H \subseteq [n],\ |H| = k\}$ is a system of free generators.

2.1. Orthogonals and annullators

In this subsection we assume that R is a D-ring: it is a commutative ring with 1, it has a finite length ℓ, and for any finitely generated free module R^t and R-submodule $M \leq R^t$ we have $M^{\perp\perp} = M$.

Let M and N be free modules isomorphic to R^t for some positive integer t. Let $m_1, \ldots, m_t$ and $n_1, \ldots, n_t$ be fixed R-bases of M and N respectively. We define the bilinear form $(,)$ from $M \times N$ to R as follows: for $u = \sum_{i=1}^{t} \alpha_i m_i$ and $v = \sum_{i=1}^{t} \beta_i n_i$ we put $(u, v) = \sum_{i=1}^{t} \alpha_i \beta_i$.

For a submodule $K \leq M$ we define the orthogonal $K^\perp \leq N$ in the usual way: $K^\perp = \{v \in N : (u, v) = 0 \text{ for every } u \in K\}$. Similarly we can speak about the orthogonal $L^\perp \leq M$ of a submodule of $L \leq N$.

Proposition 2.6. *Suppose that R is a D-ring. Then $K^{\perp\perp} = K$ and $L^{\perp\perp} = L$ hold for every submodule $K \leq M$ and $L \leq N$. Moreover, we have $\ell(K) + \ell(K^{\perp}) = t\ell$ and $\ell(L) + \ell(L^{\perp}) = t\ell$, whenever $K \leq M$ and $L \leq N$.*

Proof. We observe that the maps which send $(\alpha_1, \ldots, \alpha_t)$ to $\sum_{i=1}^{t} \alpha_i m_i$ and $(\beta_1, \ldots, \beta_t)$ to $\sum_{i=1}^{t} \beta_i n_i$ induce an isomorphism from $R^t \times R^t$ to $M \times N$ which preserves $(,)$. The first statement is then a direct consequence of the definition of D-rings.

The second statement follows from the first. The maps $K \mapsto K^{\perp}$ and $L \mapsto L^{\perp}$ are order reversing isomorphisms among the lattices of submodules of M and N.

We turn now to the ring Q defined in (7). We know that Q is a free R-module with basis $\{x_H : H \subseteq [n]\}$. We define an R-bilinear form on Q. For $q_1, q_2 \in Q$ we let (q_1, q_2) be the coefficient of $x_{[n]}$ in the product $q_1 q_2$.

Proposition 2.7. *Let K be an R-submodule of Q.*

1. *We have $\ell(K) + \ell(K^{\perp}) = 2^n \ell$.*
2. *Assume that $K \leq Q_k$ for some k. Then $\ell(K) + \ell(K^{\perp} \cap Q_{n-k}) = \binom{n}{k}\ell$.*

Proof. We apply Proposition 2.6 with $M = Q$ and $N = Q$. The basis elements are indexed with subsets of $[n]$. The basis $\{m_H : H \subseteq [n]\}$ of M is given by letting $m_H = x_H$. A corresponding basis $\{n_H : H \subseteq [n]\}$ of N is given by $n_H = x_{[n]\setminus H}$. The first statement now follows directly.

Concerning the second statement, we use Proposition 2.6 again, but now with $M = Q_k$ and $N = Q_{n-k}$.

For a nonempty family $\mathcal{F} \subseteq 2^{[n]}$ we denote by $J(\mathcal{F})$ the image of the ideal $Id(\mathcal{F}) \leq S^*$ in Q (with respect to the natural map $S^* \to Q$). We have

$$Q/J(\mathcal{F}) = (S^*/(z, I))/((z, Id(\mathcal{F}))/(z, I)) \cong S^*/(z, Id(\mathcal{F})) \tag{8}$$

by a standard isomorphism, hence by Theorem 2.3 we obtain

$$\ell(Q/J(\mathcal{F})) = |\mathcal{F}|\ell \quad \text{and} \quad \ell(J(\mathcal{F})) = \ell \cdot (2^n - |\mathcal{F}|). \tag{9}$$

We need also the notion of annullator $ann(X)$ of a subset $X \subset A$ in a ring A. Set

$$ann(X) = \{a \in A : ax = 0 \text{ for every } x \in X\}.$$

Proposition 2.8. *Let $\mathcal{F} \subseteq 2^{[n]}$ and $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$. Assume that both $\mathcal{F}$ and $\mathcal{G}$ are nonempty. Then in Q we have*

$$ann(J(\mathcal{F})) = J(\mathcal{F})^{\perp} = J(\mathcal{G}).$$

Proof. It is immediate that $ann(J(\mathcal{F})) \subseteq J(\mathcal{F})^{\perp}$. We note next that $Id(\mathcal{F})Id(\mathcal{G}) \subseteq I$, because if a form $f \in S^*$ vanishes on $W(\mathcal{F})$ and a $g \in S^*$ vanishes on $W(\mathcal{G})$, then fg vanishes on $\mathbb{X}$. Therefore in S^* we have

$$((z) + Id(\mathcal{F}))((z) + Id(\mathcal{G})) \subseteq (z) + Id(\mathcal{F})Id(\mathcal{G}) \subseteq (z) + I,$$

implying that $J(\mathcal{F})J(\mathcal{G}) = (0)$ in Q and hence

$$J(\mathcal{G}) \subseteq ann(J(\mathcal{F})) \subseteq J(\mathcal{F})^{\perp}. \tag{10}$$

Taking lengths, we obtain

$$\ell \cdot (2^n - |\mathcal{G}|) \leq \ell(ann(J(\mathcal{F}))) \leq \ell \cdot (2^n - (2^n - |\mathcal{F}|)) = \ell \cdot (2^n - |\mathcal{G}|). \tag{11}$$

Thus, we must have equalities in (11) and in (10) as well. This finishes the proof.

Remark. The preceding statement remains valid also in the case $\mathcal{F} = \emptyset$ or $\mathcal{G} = \emptyset$ if we agree to set $J(\emptyset) = Q$.

We are ready to prove the main result of the paper, a relation involving the Hilbert function of $\mathcal{F} \subseteq 2^{[n]}$ and $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$.

Proof of Theorem 1.1. Suppose that $0 \leq j \leq n$, and consider the j-th graded piece of $Q/J(\mathcal{F})$. By Theorems 2.3 and 2.5 and the isomorphism (8) we have

$$\ell(J(\mathcal{F}) \cap Q_j) = \binom{n}{j}\ell - h(\mathcal{F}, j) + h(\mathcal{F}, j-1).$$

Similarly, by looking at the $n-j$-th graded piece of $Q/J(\mathcal{G})$ we obtain

$$\ell(J(\mathcal{G}) \cap Q_{n-j}) = \binom{n}{j}\ell - h(\mathcal{G}, n-j) + h(\mathcal{G}, n-j-1).$$

From Propositions 2.6 and 2.8 we infer

$$\ell(J(\mathcal{F}) \cap Q_j) + \ell(J(\mathcal{G}) \cap Q_{n-j}) = \binom{n}{j}\ell,$$

hence

$$\binom{n}{j}\ell = h(\mathcal{F}, j) - h(\mathcal{F}, j-1) + h(\mathcal{G}, n-j) - h(\mathcal{G}, n-j-1), \tag{12}$$

for every $0 \leq j \leq n$. Next we add these equations up for $j = 0, \ldots, k$:

$$h(\mathbb{X}, k) = h(\mathcal{F}, k) + h(\mathcal{G}, n) - h(\mathcal{G}, n-k-1).$$

The Theorem follows now from $h(\mathcal{G}, n) = |\mathcal{G}|\ell$.

Remark. It was pointed out to us by Bálint Felszeghy, that Theorem 1.1 allows a short and elegant proof in the case $\ell = 1$, i.e. when R is a field. The approach involves the rudiments of the theory of Gröbner bases (see for example Subsection 1.1 of [10] for the notions not defined here). In fact let $\prec$ be an arbitrary degree comaptible term order on $S = \mathbb{F}[x_1, \ldots, x_n]$. Then one can readily verify that a monomial x_A is a standard monomial for $I(\mathcal{F})$ if and only if x_{A^c} is a leading term for $I(\mathcal{G})$. Here $A \subseteq [n]$, A^c stands for the set $[n] \setminus A$, and $I(\mathcal{F})$ (resp. $I(\mathcal{G})$) is the ideal of polynomials in S that vanish on $V(\mathcal{F})$ ($V(\mathcal{G})$, resp.). From this statement we immediately obtain equations (12) and hence Theorem 1.1.

We turn now to the proof of Corollary 1.2. Recall, that $a(\mathcal{F})$ stands for the smallest degree of a nonzero reduced polynomial from S which vanishes on $V(\mathcal{F})$. Also, $b(\mathcal{F})$ is the smallest integer k such that $h(\mathcal{F}, k) = |\mathcal{F}|\ell$.

Proof of Corollary 1.2. We intend to apply Theorem 1.1 with $k = a(\mathcal{F}) - 1$. Note first, that $k \geq 0$ and $h(\mathcal{F}, k) = h(2^{[n]}, k)$, because the reduced monomials of degree $\leq k$ are linearly independent over R, as functions on $V(\mathcal{F})$.

Theorem 1.1 gives now that $h(\mathcal{G}, n-k-1) = |\mathcal{G}|\ell$, hence $b(\mathcal{G}) \leq n-k-1 = n - a(\mathcal{F})$. This, together with (3) proves the assertion.

3. D-rings

Our objective here is to verify that the rings $\mathbb{Z}_m$ are D-rings. This is known to follow from Morita's theory of duality, see e.g. Example 4.4 and Section 7 of [17]. For the reader's convenience, here we give a simple direct proof. Our argument is not new, we merely collected some facts which are usually scattered and treated in greater generality in texts about the duality theory of modules.

Let R be a commutative ring with 1. A module M over a ring R is *injective*, if for every pair of R-modules $K \leq L$ and an R-homomorphism $\phi : K \to M$

there exists a homomorphism $\psi : L \to M$ which extends ϕ. It is a standard fact (see for example Proposition 18.7 in [3]) that M is injective iff M is a direct summand of K whenever $M \leq K$.

An R-module M is called a *cogenerator*, if every R-module N can be embedded into a suitable power M^X of M.

Proposition 3.1. *Let R be a commutative ring with 1. Suppose that R (as an R-module) is a cogenerator. Then for every positive integer t and $K \leq R^t$ we have $K^{\perp\perp} = K$.*

Proof. Let t be a positive integer. If $\phi : R^t \to R$ is an R-homomorphism, then there exists a $v \in R^t$ representing ϕ in the sense that $\phi(u) = (u, v)$ for every $u \in R^t$. Indeed, if $e^i \in R^t$ is the row vector with 1 in the i-th coordinate, and 0 elsewhere, then with $\beta_i = \phi(e^i)$ and $v = (\beta_1, \ldots, \beta_t)$ we have the claim.

Let now $K \leq R^t$. It is immediate that $K^{\perp\perp} \geq K$. In the other direction, let $x \in R^t \setminus K$ be an arbitrary element. R is a cogenerator, hence we have an injection $R^t/K \hookrightarrow R^X$. Taking a suitable projection $R^X \to R$ onto a coordinate, we obtain a map $\delta : R^t/K \to R$ such that $\delta(x+K) \neq 0$. Composing δ and the natural map $R^t \to R^t/K$, we obtain an R-homomorphism $\phi : R^t \to R$ such that $\phi(K) = (0)$ and $\phi(x) \neq 0$. For the element $v \in R^t$ representing ϕ we have $(v, K) = 0$ and $(v, x) \neq 0$, giving that $v \in K^\perp$ and $x \notin K^{\perp\perp}$. This finishes the proof.

We turn to the rings $R = \mathbb{Z}_m$, where $m > 1$ is an integer.

Proposition 3.2. *$\mathbb{Z}_m$ is injective as a $\mathbb{Z}_m$-module.*

Proof. Let M be a $\mathbb{Z}_m$-module with $\mathbb{Z}_m \leq M$. We have to prove that $\mathbb{Z}_m$ is a direct summand in M. Let N be a maximal submodule of M which intersects $\mathbb{Z}_m$ in (0). By factoring out N we may assume that every submodule of M intersects $\mathbb{Z}_m$ in a nonzero submodule. From this we have to conclude that $M = \mathbb{Z}_m$. Assume for contradiction that there exists an element $v \in M \setminus \mathbb{Z}_m$. By replacing v with a suitable integer multiple we may assume, that $v \notin \mathbb{Z}_m$ but $0 \neq u = pv \in \mathbb{Z}_m$ for some prime divisor p of m. We have $\frac{m}{p}u = \frac{m}{p}pv = mv = 0$, hence there exists a $v^* \in \mathbb{Z}_m$ such that $pv^* = u$. For $y = v - v^*$ we have $py = 0$, and $y \notin \mathbb{Z}_m$. The submodule generated by y intersects $\mathbb{Z}_m$ trivially. This contradiction proves the claim.

Proposition 3.3. *$\mathbb{Z}_m$ is a cogenerator as a $\mathbb{Z}_m$-module.*

Proof. For injective modules there is a very convenient cogenerator test: an injective R-module M is a cogenerator iff $\mathrm{Hom}_R(T, M) \neq (0)$ for every simple R-module T (Proposition 18.5 in [3]). In fact, $\mathbb{Z}_m$ is injective, and the simple $\mathbb{Z}_m$-modules are the modules $\mathbb{Z}_p$, where p is a prime divisor of m. We conclude by noting that for primes $p|m$ we have $\mathbb{Z}_p \cong \frac{m}{p}\mathbb{Z}_m \leq \mathbb{Z}_m$.

A combination of the preceding three statements gives the following

Corollary 3.4. *For $m > 1$ the rings $\mathbb{Z}_m$ are D-rings.*

The same reasoning gives *mutatis mutandis*, that R^*/I is a D-ring, where R^* is a principal ideal domain and I is a nonzero ideal of R^*.

One can in fact characterize the commutative Artinian rings R (rings with the minimum condition for ideals) for which the conclusion of Proposition 3.1 holds. These are precisely the finite direct sums of Gorenstein Artinian rings. The sufficiency is outlined in Remark 1.3 of [17]. The necessity is very easy: if a local Artinian ring is not Gorenstein, then the conslusion of Proposition 3.1 fails even for $t = 1$.

4. An application: the weak degree of a Boolean function

4.1. Boolean functions and set families

As an application of the preceding results, we give a lower bound on the weak degree of the Boolean function $\neg MOD_6$ over the ring $\mathbb{Z}_6$. Recall that the Boolean function $\neg MOD_6 : \{0,1\}^n \to \{0,1\}$ gives 1 on the Boolean vector $v \in \{0,1\}^n$ if the Hamming weight $\mathrm{Ham}(v)$ of v is not divisible by 6, and $\neg MOD_6(v) = 0$ otherwise. Following [5] we say that the polynomial $p \in \in R[x_1, \ldots, x_n]$ *weakly represents* the Boolean function $F : \{0,1\}^n \to \{0,1\}$ over the ring R if $F(v) = 0$ holds iff $p(v) = 0$ for all $v \in \{0,1\}^n$. The *weak degree* $\delta(F)$ of F is the minimal degree of those polynomials that weakly represent F.

We refer to [5] and [16] for a background on and the significance of modular representations of Boolean functions. In the sequel we do not distinguish $\mathcal{F}$ from $V(\mathcal{F})$, both will be denoted simply by $\mathcal{F}$.

We set

$$\mathcal{F} := \{v \in \{0,1\}^n : 6 \mid \mathrm{Ham}(v)\}\,,\ \mathcal{G} := \{0,1\}^n \setminus \mathcal{F}.$$

The main result of this section is the following

Theorem 4.1. *Assume that $R{=}\mathbb{Z}_6$. Then $b(\mathcal{F}) \le \frac{5}{8}n{+}2$ and consequently $a(\mathcal{G}) \ge \frac{3}{8}n - 2$. Also $b(\mathcal{F}) \ge \frac{1}{2}n + O(\log n)$ and hence $a(\mathcal{G}) \le \frac{1}{2}n + O(\log n)$.*

We observe that $a(\mathcal{G}) \le \delta(\neg MOD_6)$. This gives the lower bound below, which strengthens Theorem 3.2 from [5] and Theorem 4.4 of [16] in the case $m = 6$:

Corollary 4.1. *We have $\delta(\neg MOD_6) \ge \frac{3}{8}n - 2$.*

Remark. It is easy to compute the weak degree of $\neg MOD_p$ over the ring $\mathbb{Z}_p$, when p is a prime. Here let $\mathcal{F}$ consist of those 0-1 vectors of length n whose Hamming-weight is divisible by p, and put $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$ as usual. The polynomial $\left(\sum_{i=1}^{n} x_i\right)^{p-1} - 1$ shows that $a(\mathcal{G}) \leq \delta(\neg MOD_p) \leq p-1$ as this latter polynomial vanishes on each $v \in \mathcal{G}$. On the other hand, suppose that $n > 2p-4$. We show that the degree of the characteristic function (in $\mathcal{F}$) of any vector $v \in \mathcal{F}$ is at most $n-p+1$ which implies that $b(\mathcal{F}) \leq n-p+1$. To see this, let us fix a vector $v \in \mathcal{F}$, $\mathrm{Ham}(v) := k$ with $p \mid k$. Assume, that $k \leq n-p+1$ (similar consideration works when $n-k \leq n-p+1$, with the roles of 0 and 1 reversed). Without loss of generality we suppose that $v_1 = \ldots = v_k = 1, v_{k+1} = \ldots = v_n = 0$. The polynomial

$$g = \prod_{i=1}^{k} x_i \cdot \prod_{j=k+1}^{n-p+1} (1 - x_j)$$

has degree $n-p+1$ and it gives 1 if we substitute v but $g(w) = 0$ for $w \in \mathcal{F}$, $w \neq v$. We obtain that g is the characteristic function of v (in $\mathcal{F}$). Now by Corollary 1.2 we have $n = a(\mathcal{G}) + b(\mathcal{F}) \leq p - 1 + n - p + 1 = n$, hence $b(\mathcal{F}) = n-p+1$ and $a(\mathcal{G}) = \delta(\neg MOD_p) = p-1$.

4.2. Proof of Theorem 4.1

4.2.1. The inequality $b(\mathcal{F}) \leq \frac{5}{8}n + 2$

Our first observation is that it is sufficient to prove a slightly stronger inequality for $6 \mid n$ only. Indeed, let us suppose that we can prove

$$b(\mathcal{F}_n) \leq \frac{5}{8}n \text{ for all } n \text{ such that } 6 \mid n \tag{13}$$

(henceforth in the notation $\mathcal{F}_n$ the subscript n indicates that the vectors in $\mathcal{F}$ have n coordinates). Let $v \in \mathcal{F}_{n+i}$ for some i with $i \in \{1, \ldots, 5\}$. Without loss of generality we may assume that $v_{n+1} = \cdots = v_{n+i} = 0$. Let w be the vector obtained from v by deleting the last i coordinates. Let χ_w be the characteristic function of w in $\mathcal{F}_n$. Then

$$\chi_v = \chi_w \cdot \prod_{j=1}^{i} (1 - x_{n+j})$$

gives χ_v. We infer that

$$b(\mathcal{F}_{n+i}) \leq \frac{5}{8}n + i = \frac{5}{8}(n+i) + \frac{3}{8}i < \frac{5}{8}(n+i) + 2$$

as $i \leq 5$. Indeed it suffices to prove (13).

We assume now that $6|n$. We use symmetric polynomials to estimate $b(\mathcal{F})$. Let σ_i^n denote the ith elementary symmetric polynomial of the variables $x_1, \ldots, x_n$ $(0 \leq i \leq n,\ i \in \mathbb{N})$,

$$\sigma_i^n := \sum_{1 \leq j_1 < \ldots < j_i \leq n} x_{j_1} \ldots x_{j_i} \quad \text{for} \quad i > 0, \quad \sigma_0^n := 1.$$

We construct a polynomial $\chi_{\underline{0}}$ which is the characteristic function in $\mathcal{F}$ of the vector v with $v_1 = \ldots = v_n = 0$ such that $\deg(\chi_{\underline{0}})$ is small. By the Chinese Remainder Theorem it is enough to construct $\chi_{\underline{0}}$ over $\mathbb{Z}_2[x_1, \ldots, x_n]$ and over $\mathbb{Z}_3[x_1, \ldots, x_n]$ since by taking a suitable linear combination we obtain $\chi_{\underline{0}}$ over $\mathbb{Z}_6[x_1, \ldots, x_n]$. Indeed, if q_2 represents $\chi_{\underline{0}}$ over $\mathbb{Z}_2[x_1, \ldots, x_n]$ and q_3 over $\mathbb{Z}_3[x_1, \ldots, x_n]$ then $3q_2 + 4q_3$ represents $\chi_{\underline{0}}$ over $\mathbb{Z}_6[x_1, \ldots, x_n]$.

To construct $\chi_{\underline{\mathbf{0}}}$ over $\mathbb{Z}_3[x_1, \ldots, x_n]$, we use only those σ_i^n for which $3 \mid i$, $i \leq \frac{n}{2}$. In fact, an integer linear combination of $\sigma_0^n, \sigma_3^n, \ldots, \sigma_{n/2}^n$ gives $\chi_{\underline{\mathbf{0}}}$ (mod 3). Similarly, to construct a polynomial representation of $\chi_{\underline{\mathbf{0}}}$ over $\mathbb{Z}_2[x_1, \ldots, x_n]$ it is sufficient to use the σ_i^n for which $2 \mid n$, $i \leq \frac{n}{3}$, i.e. $\sigma_0^n, \sigma_2^n, \ldots, \sigma_{n/3}^n$ over $\mathbb{Z}_3$ will give $\chi_{\underline{\mathbf{0}}}$ (mod 2).

Observe that $\sigma_i^n(v) = \binom{\mathrm{Ham}(v)}{i}$ holds for any $v \in \{0,1\}^n$. Since the number of the possible values of $\mathrm{Ham}(v)$ is $\frac{n}{6} + 1$, the dimension over $\mathbb{Z}_3$ of the space of symmetric functions from $\mathcal{F}$ to $\mathbb{Z}_3$ is at most $\frac{n}{6} + 1$. On the other hand, there are $\frac{n}{6} + 1$ different functions σ_i^n, where $0 \leq i \leq \frac{n}{2}$, with $3 \mid i$.

To show that $\sigma_0^n, \sigma_3^n, \ldots, \sigma_{n/2}^n$ form basis for the symmetric functions over $\mathbb{Z}_3$, it suffices to verify that they are independent (over $\mathbb{Z}_3$) as functions on $\mathcal{F}$. This amounts to proving that $3 \nmid \det A$ where $A_{ij} = \sigma_i^n(v_j) = \binom{6j}{3i}$ $(i, j = 0, \ldots, n/6)$, and $v_j \in \{0,1\}^n$ with $\mathrm{Ham}(v_j) = 6j$.

$$A = \begin{pmatrix} \binom{0}{0} & \binom{6}{0} & \binom{12}{0} & \cdots & \binom{n}{0} \\ \binom{0}{3} & \binom{6}{3} & \binom{12}{3} & \cdots & \binom{n}{3} \\ \binom{0}{6} & \binom{6}{6} & \binom{12}{6} & \cdots & \binom{n}{6} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{0}{n/2} & \binom{6}{n/2} & \binom{12}{n/2} & \cdots & \binom{n}{n/2} \end{pmatrix}$$

We prove a more general statement.

Lemma 4.2. *Let p be a prime and let l, m, α be positive integers. Let B be the $(m+1) \times (m+1)$ matrix with $B_{ij} = \binom{jlp^\alpha}{ip^\alpha}$ $(i, j = 0, 1, \ldots, m)$. Then $p \not| \det B$ if and only if $(p, l) = 1$.*

$$B = \begin{pmatrix} \binom{0}{0} & \binom{lp^\alpha}{0} & \binom{2lp^\alpha}{0} & \cdots & \binom{mlp^\alpha}{0} \\ \binom{0}{p^\alpha} & \binom{lp^\alpha}{p^\alpha} & \binom{2lp^\alpha}{p^\alpha} & \cdots & \binom{mlp^\alpha}{p^\alpha} \\ \binom{0}{2p^\alpha} & \binom{lp^\alpha}{2p^\alpha} & \binom{2lp^\alpha}{2p^\alpha} & \cdots & \binom{mlp^\alpha}{2p^\alpha} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{0}{mp^\alpha} & \binom{lp^\alpha}{mp^\alpha} & \binom{2lp^\alpha}{mp^\alpha} & \cdots & \binom{mlp^\alpha}{mp^\alpha} \end{pmatrix}$$

Proof. Lucas' Theorem ([12], Problem 1.2.6/10e) states that for any prime p and integers $0 \le a_i, b_i \le p-1$ we have

$$\binom{a_k p^k + \ldots + a_1 p + a_0}{b_k p^k + \ldots + b_1 p + b_0} \equiv \binom{a_k}{b_k} \ldots \binom{a_1}{b_1} \binom{a_0}{b_0} \pmod{p}.$$

We infer that $\binom{ip^\alpha}{jp^\alpha} \equiv \binom{i}{j} \pmod{p}$ for any nonnegative integers i, j. Therefore, it is sufficient to prove that $\det C$ is nonzero $\pmod{p}$ iff $(p, l) = 1$, where C is the $(m+1) \times (m+1)$ matrix with $C_{ij} = \binom{jl}{i}$ $(i, j = 0, 1, \ldots, m)$.

$$C = \begin{pmatrix} \binom{0}{0} & \binom{l}{0} & \binom{2l}{0} & \cdots & \binom{ml}{0} \\ \binom{0}{1} & \binom{l}{1} & \binom{2l}{1} & \cdots & \binom{ml}{1} \\ \binom{0}{2} & \binom{l}{2} & \binom{2l}{2} & \cdots & \binom{ml}{2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{0}{m} & \binom{l}{m} & \binom{2l}{m} & \cdots & \binom{ml}{m} \end{pmatrix}$$

To this end we compute the exact value of $\det C$. Let x be a variable and k be a positive integer. The binomial expression $\binom{x}{k}$ is a polynomial of degree k and its leading coefficient is $\frac{1}{k!}$. It is obvious that $\binom{x}{0}, \binom{x}{1}, \ldots, \binom{x}{k}$ form a basis of the subspace of polynomials in $\mathbb{Q}[x]$ whose degree is at most k. In particular, there exist coefficients $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Q}$ such that

$$\sum_{i=0}^{k-1} a_i \binom{x}{i} + \binom{x}{k} = \frac{1}{k!} x^k.$$

As a consequence, by adding a suitable linear combination of the first $i-1$ rows (of C) to the ith row $(i = m+1, m, \ldots, 2)$, we obtain $\frac{1}{i!}0^i, \frac{1}{i!}l^i, \ldots, \frac{1}{i!}(lm)^i$ in the ith row. We end up with the following matrix D as i runs through $m+1, m, \ldots, 2$:

$$D = \begin{pmatrix} \frac{0^0}{0!} & \frac{l^0}{0!} & \frac{(ml)^0}{0!} \\ \frac{0^1}{1!} & \frac{l^1}{1!} & \frac{(ml)^1}{1!} \\ \vdots & \vdots & \vdots \\ \frac{0^m}{m!} & \frac{l^m}{m!} & \frac{(ml)^m}{m!} \end{pmatrix}$$

After taking out $\prod_{i=0}^{m} \frac{1}{i!}$ we obtain a Vandermonde matrix, hence

$$\det D = \prod_{i=0}^{m} \frac{1}{i!} \cdot \prod_{0 \le i < j \le m} (lj - li) = \prod_{i=0}^{m} \frac{1}{i!} \cdot l^{\binom{m+1}{2}} \cdot \prod_{i=0}^{m} i! = l^{\binom{m+1}{2}}.$$

This latter is not divisible by p iff $(p, l) = 1$, so the proof of the lemma is complete.

$$\det \begin{pmatrix} \binom{0}{0} & \binom{lp^\alpha}{0} & \binom{mlp^\alpha}{0} \\ \binom{0}{p^\alpha} & \binom{lp^\alpha}{p^\alpha} & \binom{mlp^\alpha}{p^\alpha} \\ \vdots & \vdots & \vdots \\ \binom{0}{mp^\alpha} & \binom{lp^\alpha}{mp^\alpha} & \binom{mlp^\alpha}{mp^\alpha} \end{pmatrix} =$$

$= \#$ point-disjoint path-systems

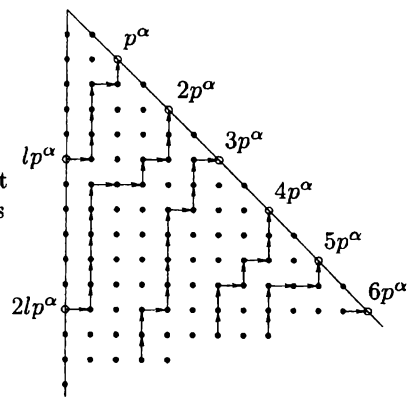

Fig. 1. The Gessel-Viennot theorem applied to B

Remark. By the Gessel-Viennot theorem ([2], [7]) $\det B$ has a combinatorical interpretation: it is the number of special point disjoint path-systems on the xy coordinate-plane. From $ip^\alpha \leq ilp^\alpha$ $(i = 0, 1, \ldots, m)$ we know that this number is always positive hence $\det B > 0$.

We apply Lemma 4.2 with $p = 3,\ l = 2,\ \alpha = 1$ and $m = n/6$, to obtain that the degree of $\chi_{\underline{\mathbf{0}}}$ over $\mathbb{Z}_3[x_1, \ldots, x_n]$ is at most $n/2$. Similarly, applying Lemma 4.2 with $p = 2,\ l = 3, \alpha = 1$ and $m = n/6$ we obtain that the degree of $\chi_{\underline{\mathbf{0}}}$ over $\mathbb{Z}_2[x_1, \ldots, x_n]$ is at most $n/3$. Putting these two facts together, there is a polynomial of degree at most $n/2$ that represents $\chi_{\underline{\mathbf{0}}}$ over $\mathbb{Z}_6$.

Note also, that if we have a polynomial g representing $\chi_{\underline{\mathbf{0}}}$, then we automatically have a polynomial g' representing $\chi_{\underline{\mathbf{1}}}$ with the same degree (here $\underline{\mathbf{1}}$ denotes the vector with 1 in each coordinate), if we substitute $1 - x_i$ in the place of x_i in g. More generally, from a representation of χ_v $v \in \mathcal{F}$ we have a representation of $\chi_{\underline{\mathbf{1}}-v}$, if in χ_v we substitute $1 - x_i$ for x_i.

With $\chi_{\underline{\mathbf{0}}}$ and $\chi_{\underline{\mathbf{1}}}$ at hand, we construct a polynomial for the characteristic function of a given vector $v \in \mathcal{F}$. Let $H(v) \subseteq \{1, \ldots, n\}$ denote the index set of 1-coordinates in v. We use induction on $|H(v)|$. If this number is 0 then $v = \underline{\mathbf{0}}$ and we are done. To construct χ_v for $\mathrm{Ham}(v) > 0$, we employ three basic steps:

- we find a polynomial $p(\mathbf{x})$ which is 0 on $w \in \{0,1\}^n$ if $6 \not| |H(v) \cap H(w)|$, and ± 1 if $H(v) \cap H(w) = H(v)$ (i.e. if a coordinate of v is 1, so is the same coordinate of w),
- we multiply $p(\mathbf{x})$ by $\chi_{\underline{\mathbf{0}}}^{\underline{\mathbf{1}}-v}$ (here the superscript $\underline{\mathbf{1}} - v$ means that we consider vectors in $\{0,1\}^{n-\mathrm{Ham}(v)}$ and variables indexed with the 0-coordinates of v),
- from the polynomial $p(\mathbf{x})\chi_{\underline{\mathbf{0}}}^{\underline{\mathbf{1}}-v}$ we subtract suitable scalar multiples of (already represented) characteristic functions of vectors $w \in \{0,1\}^n$ for which $\mathrm{Ham}(w) < \mathrm{Ham}(v)$, such that we obtain χ_v.

Before going into the details, we need some notation: from now on let $\sigma_i^{a..b}$ denote the ith elementary symmetric polynomial over the polynomial ring $\mathbb{Z}_6[x_a, x_{a+1}, \ldots, x_b]$ $(1 \leq a \leq b \leq n$ integers). Similarly, $\chi_v^{a..b}$ denotes the characteristic function of the vector $v \in \{0,1\}^{b-a+1}$ over $\mathbb{Z}_6[x_a, x_{a+1}, \ldots, x_b]$.

Let us suppose first, that $\mathrm{Ham}(v) = 6$. By relabeling the coordinates we may assume that $v_1 = \ldots = v_6 = 1$. Our key polynomial is $\sum_{i=0}^{5}(-1)^i\sigma_i^{1\ldots6}$. It gives 1 on w if $w_1 = w_2 = \cdots = w_6 = 0$, and it is -1 if $w_1 = \ldots w_6 = 1$, and it is 0 otherwise. As a consequence,

$$g = -\left(\sum_{i=0}^{5}(-1)^i\sigma_i^{1\ldots6}\right)\chi_{\underline{\mathbf{0}}}^{7..n} + \chi_{\underline{\mathbf{0}}}^{1..n}$$

gives a polynomial representation of $\chi_v^{1..n}$. Indeed, as explained above,

$$\sum_{i=0}^{5}(-1)^i\sigma_i^{1\ldots6}$$

gives a nonzero value on w iff $w_1 = \ldots = w_6$, and if so (this fact ensures that the number of 1-coordinates among $w_7, \ldots, w_n$ is divisible by 6), then $\chi_{\underline{\mathbf{0}}}^{7..n}$ gives nonzero substitution value iff $w_7 = \ldots = w_n = 0$. Hence, the product of these two polynomials is nonzero iff $w = v$ or $w = \underline{\mathbf{0}}$. This latter case is corrected by the additional term $\chi_{\underline{\mathbf{0}}}^{1..n}$.

The idea described above can be used for computing χ_v if $\mathrm{Ham}(v) = 12$ with only a slight modification. By relabeling the coordinates we assume that $v_1 = \ldots = v_{12} = 1$. Based on the argument above, the polynomial

$$p_{12}(\mathbf{x}) = \left(\sum_{i=0}^{5}(-1)^i\sigma_i^{1\ldots6}\right)\left(\sum_{i=0}^{5}(-1)^i\sigma_i^{7\ldots12}\right)\chi_{\underline{0}}^{13\ldots n}$$

is nonzero (on w) only if $w_1 = \ldots = w_6$ AND $w_7 = \ldots = w_{12}$ AND $w_{13} = \ldots = w_n = 0$. Equivalently, $p_{12}(\mathbf{x})$ can be nonzero only if we substitute $\underline{\mathbf{0}}, v, t$ or u where $t_1 = \ldots = t_6 = 1$, $t_7 = \ldots = t_n = 0$ and $u_1 = \ldots = u_6 = 0$, $u_7 = \ldots = u_{12} = 1$, $u_{13} = \ldots = u_n = 0$. As the Hamming-weight of $\underline{\mathbf{0}}, u, t$ is at most 6, we already have their characteristic function, therefore we can express χ_v with $p_{12}(\mathbf{x})$ and with the already constructed characteristic functions:

$$\chi_v = \left(\sum_{i=0}^{5}(-1)^i\sigma_i^{1\ldots6}\right)\left(\sum_{i=0}^{5}(-1)^i\sigma_i^{7\ldots12}\right)\chi_{\underline{0}}^{13\ldots n} - \chi_{\underline{0}}^{n} + (\chi_u + \chi_t).$$

Turning to the general case, let us suppose that $\mathrm{Ham}(v) = l$ for some l with $6 \mid l$, and $v_1 = \ldots = v_l = 1$. Our method is quite similar: we consider the polynomial

$$p_l(\mathbf{x}) = \left(\prod_{j=1}^{l/6}\sum_{i=0}^{5}(-1)^i\sigma_i^{6j-5\ldots6j}\right)\chi_{\underline{0}}^{l+1..n},$$

which is nonzero on $w \in \mathcal{F}$ if and only if $\mathrm{Ham}(w) \leq \mathrm{Ham}(v)$. Using the induction hypothesis, we can modify $p_l(\mathbf{x})$ in order to produce χ_v.

Next we determine the degree of our polynomial representative for χ_v. By following the inductive procedure above, it can easily be seen that the degree of χ_v is the degree of $p_{\mathrm{Ham}(v)}$ since the "correcting" polynomials have smaller degree. Indeed, if $\mathrm{Ham}(v) = l$ $(l = 0, 6, \ldots, \frac{n}{2})$, then $\deg(p) = \frac{5}{6}l + \frac{1}{2}(n-l) = = \frac{1}{2}n + \frac{1}{3}l$ which is strictly increasing in l, therefore the degree of χ_w is smaller if $\mathrm{Ham}(w) < \mathrm{Ham}(v)$. We obtain that the degree for the representation of χ_v is $\frac{1}{2}n + \frac{1}{3}l$. In particular, the degree will be maximal if $\mathrm{Ham}(v) = \frac{1}{2}n$, when it is $\frac{1}{2}n + 2 \cdot \frac{1}{12}n = \frac{2}{3}n$.

By applying a slight modification of the above construction we may decrease the degree of χ_v. In fact, the above inductive procedure should not be carried out completely. At the beginning of the induction, the number of zero coordinates of v is n and the degree for χ_v is $n/2$. While decreasing the number of zero coordinates (increasing the Hamming weight) the degree of the representing polynomial increases. An interesting moment occurs when the number of zero coordinates of v gets smaller or equal to the degree of χ_v for the first time. If the Hamming-weight of v is l at this time then

$$n - l \leq \frac{1}{2}n + \frac{1}{3}l$$

which implies

$$\frac{3}{8}n \leq l.$$

Without loss of generality we may assume that $v_1 = \ldots = v_l = 1$. At this point, for each $w \in \{0,1\}^n$ with $\mathrm{Ham}(w) < \mathrm{Ham}(v)$ we have $n - \mathrm{Ham}(w) > \deg(\chi_w)$ but $n - \mathrm{Ham}(v) \leq \deg(\chi_v)$. It is immediate that the polynomial

$$g = \prod_{i=l+1}^{n} (1 - x_i) - \sum \chi_w$$

represents χ_v, where the summation is for $w \in \mathcal{F}$, $\mathrm{Ham}(w) < \mathrm{Ham}(v)$ and $w_{l+1} = \ldots = w_n = 0$. Moreover, for the degree we have

$$\deg(g) \leq \max\{n - l, \max\{\deg(\chi_w) \mid \mathrm{Ham}(w) < \mathrm{Ham}(v)\}\} \leq \frac{5}{8}n.$$

For vectors $v \in \mathcal{F}$ of Hamming weight larger than l, we use induction on $\mathrm{Ham}(v)$. The polynomial

$$\prod_{i=\mathrm{Ham}(v)+1}^{n} (1 - x_i) - \sum \chi_w$$

represents χ_v, where the summation is for all $w \in \mathcal{F}$ with $\mathrm{Ham}(w) < \mathrm{Ham}(v)$ and $w_{\mathrm{Ham}(v)+1} = \ldots = w_n = 0$. For the degree we obtain

$$\max\{n - \mathrm{Ham}(v), \max\{\deg(\chi_w) \mid \mathrm{Ham}(w) < \mathrm{Ham}(v)\}\}$$

which is at most $\frac{5}{8}n$.

4.2.2. The inequality $b(\mathcal{F}) \geq \frac{1}{2}n + O(\log n)$

We give two different arguments. The first one is based on a simple counting and it is nonconstructive. It is well known (see for example [15, p.76]) that the size of $\mathcal{F}$ is

$$\sum_{i=0}^{\lfloor n/6 \rfloor} \binom{n}{6i} = \frac{1}{6}2^n + o(2^n),$$

hence there are $6^{\frac{1}{6}2^n + o(2^n)}$ functions from $\mathcal{F}$ to $\mathbb{Z}_6$. On the other hand, the number of polynomial functions over $\mathbb{Z}_6$ which contain only (squarefree) monomials of degree at most k is not larger than $6^{\sum_{i=0}^{k}\binom{n}{i}}$. Thus, in order to have a representing polynomial for each function, an inequality

$$\frac{1}{6}2^n + o(2^n) \leq \sum_{i=0}^{k} \binom{n}{i}$$

must hold. It is also known [14, Theorem 3, p.156] that the above inequality implies $k \geq \frac{1}{2}n - \Theta(\sqrt{n})$. The upper bound on $a(\mathcal{G})$ follows now from Corollary 1.2.

Next we outline an alternative approach which gives $a(\mathcal{G}) \leq \frac{1}{2}n + O(\log n)$ directly, via a construction. Let us suppose that $n = 2 \cdot 3^k - 4$ for some integer $k > 1$. In the ternary number system we have $n = 122\ldots212$, and the number of digits of n is $k+1$. Let $l = \frac{n}{2} - 1 = 3^k - 3$. The shape of l in the ternary system is $l = 2\ldots20$. We consider the polynomial $p = \sigma_l - \sigma_{l+1} + \sigma_{l+2}$. For $v \in \{0,1\}^n$ we have

- $p(v) = 0$ if $\mathrm{Ham}(v) < l$,
- $p(v) = 1$ if $\mathrm{Ham}(v) = l$,
- $p(v) \equiv 0 \pmod 3$ if $\mathrm{Ham}(v) = l+1$ as $\binom{l+1}{l} - \binom{l+1}{l+1} = l \equiv 0 \pmod 3$,
- $p(v) \equiv 0 \pmod 3$ if $\mathrm{Ham}(v) = l+2$ as $\binom{l+2}{l} - \binom{l+2}{l+1} + \binom{l+2}{l+2} = \frac{l^2+l}{2} \equiv 0 \pmod 3$, and

- $p(v) \equiv 0 \pmod 3$ if $\mathrm{Ham}(v) > l + 2$.

It remains to verify the last of these congruences. Let $v \in \{0,1\}^n$ with

$$l + 2 = 3^k - 1 < \mathrm{Ham}(v) \leq 2 \cdot 3^k - 4 = n.$$

Suppose that the ternary representation of $\mathrm{Ham}(v)$ is

$$\mathrm{Ham}(v) = a_k 3^k + \ldots + a_1 3 + a_0.$$

A comparison to the ternary form of $l + 2$ and n gives that at least one of the digits $a_1, \ldots, a_{k-1}$ must be 0 or 1. By Lucas' theorem we have for $i = 0, 1, 2$

$$\binom{\mathrm{Ham}(v)}{l+i} = \binom{a_k 3^k + a_{k-1}3^{k-1} \ldots + a_1 3^1 + a_0 3^0}{0 \cdot 3^k + 2 \cdot 3^{k-1} + \ldots + 2 \cdot 3^1 + i} \equiv$$

$$\equiv \binom{a_k}{0}\binom{a_{k-1}}{2} \ldots \binom{a_1}{2}\binom{a_0}{i} \equiv 0 \pmod 3. \tag{14}$$

We obtain that $2p(v) \equiv 0 \pmod 6$ iff $\mathrm{Ham}(v) \neq l = \frac{n}{2} - 1$, i.e. $2p$ vanishes on $\mathcal{G}$, but not on $\{0,1\}^n$, as $6 \mid l$. From $\deg p = \frac{n}{2} + 1$ we obtain $a(\mathcal{G}) \leq \frac{n}{2} + 1$ whenever $n = 2 \cdot 3^k - 4$.

For a general n, we only have to write n as a sum of numbers of the form $2 \cdot 3^k - 4$, $k \in \mathbb{N}$, $k > 1$. The procedure is similar to computing the ternary representation of n. First we consider the largest k for which $2 \cdot 3^k - 4 \leq n$, here $2 \cdot 3^k - 4$ gives the first term of the sum. We then repeat the above step with $n' = n - (2 \cdot 3^k - 4)$, and so on, as long as we can.

We note first, that $4(2 \cdot 3^k - 4) > 2 \cdot 3^{k+1} - 4$, hence $2 \cdot 3^k - 4$ can occur at most three times in the decomposition of n, for each $k > 1$. It follows that we obtain at most $3 \log_3 n + 1$ terms. At the end of the procedure we are left with an integer $0 \leq l \leq 13$, because $k \geq 2$. For these remaining l coordinates we consider the polynomial $\prod_{i=n-l+1}^{n} (1 - x_i)$. Taking the product of the polynomials corresponding to each term, we obtain a polynomial that is not identically zero on $\{0,1\}^n$, and it gives nonzero value on $w \in \{0,1\}^n$ only if $6 \mid \mathrm{Ham}(w)$, and its degree is $\frac{n}{2} + O(\log n)$.

For example, for $n = 119$ we have $n = 50 + 50 + 14 + 5$, hence

$$p = 2 \cdot \left(\sigma_{24}^{1..50} - \sigma_{25}^{1..50} + \sigma_{26}^{1..50}\right) \cdot \left(\sigma_{24}^{51..100} - \sigma_{25}^{51..100} + \sigma_{26}^{51..100}\right) \cdot$$

$$\cdot \left(\sigma_6^{101..114} - \sigma_7^{101..114} + \sigma_8^{101..114}\right) \cdot \prod_{i=115}^{119} (1 - x_i). \tag{15}$$

We obtain that $a(\mathcal{G}) \leq \frac{n}{2} + O(\log n)$, and the proof of the theorem is complete.

Our methods can be used for an arbitrary m with at least two different prime divisors. For

$$\mathcal{F} := \{v \in \{0,1\}^n : \quad m|\mathrm{Ham}(v)\}$$

we obtain $b(\mathcal{F}) \leq c \cdot n$ where $c < 1$ depends only on m. For an arbitrary, non prime-power m we conjecture the following

Conjecture. $b(\mathcal{F}) = \frac{1}{2}n + o(n)$, and hence $a(\mathcal{G}) = \frac{1}{2}n + o(n)$.

Acknowledgement. We are grateful to Bálint Felszeghy and Gábor Hegedűs for their useful remarks and suggestions.

References

[1] **Alon N.,** Algebraic and probabilistic methods in discrete mathematics, *Visions in Mathematics, Towards 2000,* eds. N.Alon et al., Birkhäuser, 2000, 455-470.

[2] **Aigner M. and Ziegler G.M.,** *Proofs from THE BOOK,* Springer Verlag, 1998.

[3] **Anderson F.W. and Fuller K.R.,** *Rings and categories of modules,* GTM **13**, Springer Verlag, 1973.

[4] **Babai L. and Frankl P.,** *Linear algebra methods in combinatorics,* September 1992.

[5] **Barrington D.A.M., Beigel R. and Rudich S.,** Representing Boolean functions as polynomials modulo composite numbers, *Computational Complexity,* **4** (1994), 367-382.

[6] **Bernasconi A. and Egidi L.,** Hilbert function and complexity lower bounds for symmetric Boolean functions, *Information and Computation,* **153** (1999), 1-25.

[7] **Gessel I.M. and Viennot G.,** Binomial determinants, paths and Hook length formulae, *Advances in Mathematics,* **58** (1985), 300-321.

[8] **Harima T.,** Characterization of Hilbert functions of Gorenstein Artin algebras with the weak Stanley property, *Proc. Amer. Math. Soc.,* **123** (1995), 3631-3638.

[9] **Hegedűs G., Friedl K. and Rónyai L.,** Gröbner bases for complete ℓ-wide families, *Publ. Math. Debrecen* (to appear)

[10] **Hegedűs G. and Rónyai L.,** Gröbner bases for complete uniform families, *J. of Algebraic Combinatorics,* **17** (2003), 171-180.

[11] **Hegedűs G. and Rónyai L.,** Standard monomials for q-uniform families and a conjecture of Babai and Frankl, *Central European Journal of Mathematics,* **1** (2003), 198-207.

[12] **Knuth D.E.,** *The art of computer programming, Volume I,* Addison-Wesley, 1997.

[13] **Matsumura H.,** *Commutative ring theory,* Cambridge University Press, Cambridge, 1994.

[14] **Rényi A.,** *Probability theory,* Akadémiai Kiadó, Budapest, 1970.

[15] **Riordan J.,** *Combinatorial identities,* John Wiley & Sons, 1968.

[16] **Tsai S.C.,** Lower bounds on representing Boolean functions as polynomials in $\mathbb{Z}_m$, *SIAM Journal on Discrete Mathematics,* **9** (1996), 55-62.

[17] **Wood J.A.,** Duality for modules over finite rings and applications to coding theory, *American J. of Mathematics,* **121** (1999), 555-575.

D. Pintér and L. Rónyai
Computer and Automation Institute
of the Hungarian Academy of Sciences and
Department of Algebra
Budapest University of Technology and Economics