DIMACS Technical Report 2001-03
January 2001

Constructing Set-Systems with Prescribed Intersection Sizes

by

Vince Grolmusz[1]
Department of Computer Science
Eötvös University, H-1053 Budapest
HUNGARY
E-mail: grolmusz@cs.elte.hu

[1]Special Year Visitor at DIMACS Center, Piscataway, NJ.

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Research Institute and Telcordia Technologies (formerly Bellcore).

DIMACS was founded as an NSF Science and Technology Center, and also receives support from the New Jersey Commission on Science and Technology.

ABSTRACT

Let f be an n variable polynomial with positive integer coefficients, and let $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$ be a set-system on the n-element universe. We define set-system $f(\mathcal{H}) = \{G_1, G_2, \ldots, G_m\}$, and prove that $f(H_{i1} \cap H_{i2} \cap \ldots \cap H_{ik}) = |G_{i1} \cap G_{i2} \cap \ldots \cap G_{ik}|$, for any $1 \le k \le m$, where $f(H_{i1} \cap H_{i2} \cap \ldots \cap H_{ik})$ denotes the value of f on the characteristic vector of $H_{i1} \cap H_{i2} \cap \ldots \cap H_{ik}$.

The construction of $f(\mathcal{H})$ is a straightforward polynomial–time algorithm from $\mathcal{H}$ and polynomial f. In this paper we use this algorithm for constructing set-systems with prescribed intersection sizes modulo an integer.

As a by-product of our method, some Ray-Chaudhuri–Wilson-like theorems are proved.

Keywords: set-systems, algorithmic constructions, multi-variate polynomials, diadic decomposition, matrix-rank

1 Introduction

Let $V = \{v_1, v_2, \ldots, v_n\}$ be a set of n elements (the "universe"). A set-system $\mathcal{H}$ on V is simply some subset chosen from all of the subsets of V, i.e., $\mathcal{H} \subset \mathcal{P}(V)$. Several fields of combinatorics deal with set-systems (theory of symmetric structures (finite geometries, block designs, Steiner-systems, etc.), hypergraph-theory, extremal set systems theory) see [HBc95]. We are particularly interested in set-systems with restricted intersections, mainly with restricted intersection sizes. A beautiful (but still unpublished) book of Babai and Frankl [BF92] covers plenty results related to this topic. Just to mention a few, bounds to the size of set-systems with restricted intersections play a main rôle in the refutation of Borsuk's conjecture [KK93], in results in combinatorial geometry, related to the Hadwiger problem [FW81], and yields the best known explicit Ramsey-graphs [FW81], [Gro00b].

Here we present a method for constructing set systems with prescribed intersections. Most of our results are for constructing set-systems with restricted intersections modulo an integer (mostly primes). In Section 4 a by-product of this method gives new upper bounds for the size of set-systems with restricted intersections. Surprisingly, this upper bound - together with the construction of [Gro00b] - can be used for giving lower bounds for the degree (or weight) of some mod 6 polynomials (see Corollary 29 (cf. [BBR94], [TB98], [Gro95]).

1.1 Set-systems with prescribed intersections

We are interested in the following

Problem 1 *There are given non-negative integers $a_{ij}, 1 \leq i \leq j \leq m$. Does there exist a set-system $\mathcal{H} = \{H_1, H_2, H_3, \ldots, H_m\}$ such that*

$$|H_i \cap H_j| \equiv a_{ij}, \quad 1 \leq i \leq j \leq m. \tag{1}$$

The answer is yes, if we allow the universe (or the vertex-set) to be much larger than m, and

$$a_{ii} \geq \sum_{j<i} a_{ji} + \sum_{i<j} a_{ij},$$

is also satisfied: For $i < j$, we put a_{ij} elements into the pairwise disjoint sets called G_{ij} (these sets will play the rôle of $H_i \cap H_j$), then we define

$$H_i = \bigcup_{j<i} G_{ji} \cup \bigcup_{i<j} G_{ij} \cup G_i,$$

where G_i contains those elements what are still needed to have $|H_i| = a_{ii}$.

The answer is always yes, without any further assumption, if we consider the modular version: (1) holds only modulo r for some positive integer r. Then every G_i and G_{ij} contains at most $r - 1$ elements, and the number of elements is $O(rm^2)$.

Consequently, we should ask the following

Question: *Does there exist a set-system, satisfying (1) on a "small" vertex set? And, if there exists such a set-system, can we construct it?*

We are also interested in restrictions in multiple intersection-sizes. For any $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \{0,1\}^m$, and for $\mathcal{H}$, let

$$a_\alpha = |\bigcap_{i:\alpha_i=1} H_i|.$$

Now we can formulate the following problem:

Problem 2 *There are given non-negative integers a_α for $\alpha \in \{0,1\}^m$. Does there exists a set-system $\mathcal{H} = \{H_1, H_2, H_3, \ldots, H_m\}$ such that*

$$a_\alpha = |\bigcap_{i:\alpha_i=1} H_i| \tag{2}$$

The modular case is easier again: It is easy to see, that one can always find such a set-system $\mathcal{H}$, if (2) is satisfied modulo r. Indeed, starting with the longest intersections (i.e., with the intersections of the maximum number of H_i's), one can add at most $r-1$ new vertices into each intersections to fullfill requirements (2); this results an $\mathcal{H}$ on at most $(r-1)2^m$ elements. For the non-modular version, the same method works if numbers a_α satisfy for all α:

$$a_\alpha \geq \sum_{\beta \leq \alpha} a_\beta,$$

where $\beta \leq \alpha$ is a coordinate-wise inequality.

Consquently, the interesting question is again whether does there exists a set-system, satisfying the multiple-intersection properties (2) on a small vertex set?

In this paper, we give some partial answers to these questions, see Theorems 20, 21, 22, 23.

Extremal set theory also addresses these questions, and there are deep and nice results in this field. One of these questions is giving upper bounds for the size of the set-systems with certain pairwaise intersection sizes. There are non-modular and modular results; see the famous papers of Ray-Chaudhuri and Wilson [RCW75], Frankl-Wilson [FW81], and Deza, Frankl, and Singhi [DFS83], or the book of Babai and Frankl [BF92]. Another question is the existence and constructions of set-systems with given intersections sizes, which meets the above mentioned upper bounds (extremal set-systems). We should mention here the results of Frankl and Füredi [FF86] and the survey paper of Füredi [Für91]. The extremal set-systems have remarkable structure, sometimes they are finite geometries. Our point of interest in the present work is the constructions of set-systems with given intersection properties, preferably on a small vertex-set, but we do not want to find the extremal structures.

In theoretical computer science, there are applications of existence arguments or constructions of set-systems with restricted intersections sizes. Let us mention the papers [BMRV00] and [NW94].

By the author's best knowledge, until the present results, there were no general algorithms known for constructing set systems with prescribed intersection sizes.

The main goal of the present paper is to show that one can define arithmetical operations on set-systems which have interesting properties for the intersecting properties of set-systems. With these operations we can construct other set-systems with prescribed intersection-sizes, and the construction can be done in polynomial time in the size of the initial set system, of the size of the universe and in the size of the polynomial, used in the construction. We remark, that if the polynomial has only few non-zero coefficients, then the size of the universe will be small, it can be even smaller than the size of the original universe.

2 Preliminaries

2.1 Set-systems and Polynomials

We define the *dream-product* of matrices of same dimensions. The reason for calling it *dream* is that the typical undergraduate student would dream of such a matrix-product, where the product of two matrices is a matrix with each entry is a product of two corresponding entries of the matrices. More exactly:

Definition 3 *Let $A = \{a_{ij}\}$ and $B = \{b_{ij}\}$ two $u \times v$ matrices over a ring R. Their* dream-product *is an $u \times v$ matrix $C = \{c_{ij}\}$, denoted by $A \odot B$, and is defined as $c_{ij} = a_{ij}b_{ij}$, for $1 \leq i \leq u$, $1 \leq j \leq v$.*

As usual, we make difference between hypergraphs and set systems over a universe V. A hypergraph is a collection of several subsets of V, where some subsets may be present with a multiplicity, greater than 1 (called multi-edges). A set system may, however, contain each subset of V at most once.

Definition 4 *Let $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$ be a hypergraph of m edges (sets) over an n element universe $V = \{v_1, v_2, \ldots, v_n\}$, and let $U = \{u_{ij}\}$ be the $n \times m$ 0-1* incidence-matrix *of hypergraph $\mathcal{H}$, that is, the columns of U correspond to the sets (edges) of $\mathcal{H}$, the rows of U correspond to the elements of V, and $u_{ij} = 1$ if and only if $v_i \in H_j$. The $n \times 1$ incidence-matrix of a single subset $A \subset V$ is called the* characteristic vector *of A.*

2.2 Arithmetic operations on set systems

Note, that every member of a set system is different; so there are no identical columns in an incidence matrix of a set system, but there may be identical columns in an incidence matrix of a hypergraph in case of multi-edges. If U is a 0-1 matrix with no identical columns, then U is an incidence matrix of a set system.

Definition 5 *Let $\mathcal{F} = \{F_1, F_2, \ldots, F_m\}$ be a set system with an $n \times m$ incidence-matrix U and $\mathcal{G} = \{G_1, G_2, \ldots, G_m\}$ be a set-system with $n' \times m$ incidence-matrix W. Then* *we define $\mathcal{F}_U + \mathcal{G}_W$ as a set-system on the $n + n'$ element universe, and its incidence matrix is the $(n+n') \times m$ matrix T, where T contains the union of the rows of U and W. We define $\mathcal{F}_U\mathcal{G}_W$ as a hypergraph on the nn'-element universe, and its $nn' \times m$ incidence matrix Y is defined as the union of all the nn' pairwise dream-products of the rows of U and W.*

In other words, $\mathcal{F}_U + \mathcal{G}_W$ consists of sets $F_i \cup G_i$, $i = 1, 2, \ldots, m$ if the universes of $\mathcal{F}$ and $\mathcal{G}$ are disjoint, and if the universes are not disjoint, first we make them disjoint, and then make the pairwise unions.

The universe of $\mathcal{F}_U\mathcal{G}_W = \{K_1, K_2, \ldots, K_m\}$ consists of all (u, v) pairs of vertices, where u is a vertex of $\mathcal{F}$ and v is a vertex of $\mathcal{G}$. Moreover, $(u, v) \in K_i$ if and only if $u \in F_i$, $v \in G_i$.

Consequently, the product and sum of two hypergraphs depend on the particular choice of the incidence-matrices, and it is easy to construct such set-systems whose product contains multiple edges. Note also, that both $\mathcal{F} + \mathcal{G}$ and $\mathcal{F}\mathcal{G}$ contains m sets, exactly as $\mathcal{F}$ or $\mathcal{G}$.

Definition 6 *Let $f(x_1, x_2, \ldots, x_n) = \sum_{I\subset\{1,2,\ldots,n\}} a_I x_I$ be a multi-linear polynomial, where $x_I = \prod_{i\in I} x_i$. Let $w(f) = |\{a_I : a_I \neq 0\}|$ and let $\mathrm{L}_1(f) = \sum_{I\subset\{1,2,\ldots,n\}} |a_I|$.*

Definition 7 *Let $\mathcal{H}$ be a set-system on the n element universe $V = \{v_1, v_2, \ldots, v_n\}$ and with $n \times m$ incidence-matrix U, and let $f(x_1, x_2, \ldots, x_n) = \sum_{I\subset\{1,2,\ldots,n\}} a_I x_I$ be a multi-linear polynomial with non-negative integer coefficients or from coefficients from $\mathbf{Z}_r$. Then $f(\mathcal{H}_U)$ is a hypergraph on the $\mathrm{L}_1(f)$-element vertex-set, and its incidence-matrix is the $\mathrm{L}_1(f) \times m$ matrix W. The rows of W correspond to x_I's of f; there are a_I identical rows of W, corresponding to the same x_I. The row, corresponding to x_I is defined as the dream-product of those rows of U, which correspond to $v_i, i \in I$.*

Example 8 *Let $f(x_1, x_2, x_3, x_4) = x_1 + x_2 + 2x_3x_4$, and let the incidence-matrix U of $\mathcal{H}$ be*

$$U = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccc} H_1 & H_2 & H_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Then the incidence-matrix of $f(\mathcal{H})$ is

$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3x_4 \\ x_3x_4 \end{array} \begin{array}{c} \begin{array}{ccc} \hat{H}_1 & \hat{H}_2 & \hat{H}_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Lemma 9 *Suppose, that in Definition 7 the coefficients of $x_1, x_2, \ldots, x_n$ are non-0's in f. Then the resulting hypergraph $f(\mathcal{G})$ is a set system.*

Proof: If the coefficients of $x_1, x_2, \ldots, x_n$ are non-0's in f, then the corresponding rows of the incidence-matrix of $f(\mathcal{G})$ are the same as the rows of $\mathcal{G}$. Since $\mathcal{G}$ was a set-system, its incidence-matrix does not contain identical columns, so the same holds for the incidence-matrix of $f(\mathcal{G})$. $\square$

Remark 10 *Let $f = (x_1 + x_2 + \cdots + x_n)$. Then, for any $\mathcal{H}_U$, $f(\mathcal{H}_U) = \mathcal{H}_U$. Let $f = (x_1 + x_2 + \cdots + x_n)^2$. Then, for any $\mathcal{H}_U$, $f(\mathcal{H}_U) = \mathcal{H}_U\mathcal{H}_U$. If $\mathcal{H}_U$ is a set-system, then $f(\mathcal{H}_U)$ is also a set-system.*

The most remarkable property of $f(\mathcal{H}_U)$ is given by the following theorem.

Theorem 11 *Let $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$ be a set-system, and let U be their $n \times m$ incidence-matrix. Let f be a multi-linear polynomial with non-negative integer coefficients, or from coefficients from $\mathbf{Z}_r$. Let $f(\mathcal{H}) = \{\hat{H}_1, \hat{H}_2, \ldots, \hat{H}_m\}$. Then, for any $1 \le k \le m$ and for any $1 \le i_1 < i_2 < \ldots < i_k \le m$:*

$$f(H_{i_1} \cap H_{i_2} \cap \ldots \cap H_{i_k}) = |\hat{H}_{i_1} \cap \hat{H}_{i_2} \cap \ldots \cap \hat{H}_{i_k}|. \tag{3}$$

Proof: Consider a monomial $x_I = \prod_{j \in I} x_j$ of polynomial f. This monomial adds 1 to the left hand side of (3) exactly when $\forall j \in I : v_j \in H_{i_1} \cap H_{i_2} \cap \ldots \cap H_{i_k}$, but, this happens exactly when vertex x_I is an element of $H_{i_1} \cap H_{i_2} \cap \ldots \cap H_{i_k}$. $\square$

The next theorem gives relations between arithmetic operations on polynomials and set systems.

Theorem 12 *Let f and g be two multi-linear polynomials of n variables and with non-negative integer coefficients, and let $\mathcal{H}$ be a set-system on the n-element universe. Then*

(i) $(f + g)(\mathcal{H}) = f(\mathcal{H}) + g(\mathcal{H})$.

(ii) Let h denote the unique multi-linear polynomial equals to fg over set $\{0,1\}^n$. Then $h(\mathcal{H}) = f(\mathcal{H})g(\mathcal{H})$.

Proof: (i): The proof is obvious.

(ii): Let us remark, that the rows of the incidence matrix of $h(\mathcal{H})$ correspond to the monomials of h which, in turn, correspond to the products of the monomials of f and g; the row, corresponding to

$$\prod_{i \in I \cup J} x_i$$

is the dream-product of rows, corresponding to

$$\prod_{i \in I} x_i \text{ and } \prod_{i \in J} x_i.$$

$\square$

2.3 Corollaries for Intersection Matrices

After giving some natural definitions, we will get some corollaries for the intersection-matrices of of set-system $f(\mathcal{H})$.

Definition 13 *The* self-intersection matrix *(or simply, the* intersection-matrix*) of $\mathcal{H}$, denoted by* $\mathrm{I}(\mathcal{H})$ *is an $m \times m$ matrix, such that each entry of this matrix is a length-n 0-1 vector: the entry in row i and column j is the characteristic vector w_{ij} of set $H_i \cap H_j$, or, in other words, the dream-product of column i and column j of U. The* intersection-size matrix $\mathrm{IS}(\mathcal{H})$ *is simply $U^T U$, that is, it contains $|H_i \cap H_j|$ in column j of row i.*

In other words, if we write $H_i \cap H_j$ for characteristic vector w_{ij}:

$$\mathrm{I}(\mathcal{H}) = \begin{pmatrix} H_1 & H_1 \cap H_2 & \cdots & H_1 \cap H_m \\ H_2 \cap H_1 & H_2 & \cdots & H_2 \cap H_m \\ \vdots & \vdots & \ddots & \vdots \\ H_m \cap H_1 & H_m \cap H_2 & \cdots & H_m \end{pmatrix}$$

and

$$\mathrm{IS}(\mathcal{H}) = \begin{pmatrix} |H_1| & |H_1 \cap H_2| & \cdots & |H_1 \cap H_m| \\ |H_2 \cap H_1| & |H_2| & \cdots & |H_2 \cap H_m| \\ \vdots & \vdots & \ddots & \vdots \\ |H_m \cap H_1| & |H_m \cap H_2| & \cdots & |H_m| \end{pmatrix}. \tag{4}$$

Definition 14 *Let $\mathcal{H}$ be a set-system. Then let*

$$\mathrm{L}(\mathcal{H}) = \{|H_i \cap H_j|, H_i \neq H_j, H_i, H_j \in \mathcal{H}\}.$$

Definition 15 *Let A and B be two sets, $f : A \to B$ a function and n and k two positive integers. Let $A^{n \times k}$ denote the set of $n \times k$ matrices with entries from A. Let $M \in A^{n \times k}$, $M = \{m_{ij}\}$. Then*

$$f[M] = \begin{pmatrix} f(m_{11}) & f(m_{12}) & \cdots & f(m_{1k}) \\ f(m_{21}) & f(m_{22}) & \cdots & f(m_{2k}) \\ \vdots & \vdots & \ddots & \vdots \\ f(m_{n1} & f(m_{n2}) & \cdots & f(m_{nk}) \end{pmatrix} \in B^{n \times k}.$$

Example 16 *Let $f = (x_1 + x_2 + \cdots + x_n)$. Then, for any $\mathcal{H}$ on the n-element universe: $f[\mathrm{I}(\mathcal{H})] = \mathrm{IS}(\mathcal{H})$.*

Corollary 17 *Let $\mathcal{F}$ and $\mathcal{H}$ be two set-systems, and let U and W be their $n \times m$ incidence-matrices. Let f be a multi-linear polynomial with non-negative integer coefficients, or from coefficients from $\mathbf{Z}_r$.*

Then

(i) $\mathrm{IS}(\mathcal{F}_U + \mathcal{H}_W) = \mathrm{IS}(\mathcal{F}_U) + \mathrm{IS}(\mathcal{H}_W)$.

(ii) $\mathrm{IS}(\mathcal{F}_U \mathcal{H}_W) = \mathrm{IS}(\mathcal{F}_U) \odot \mathrm{IS}(\mathcal{H}_W)$.

(iii) $\mathrm{IS}(f(\mathcal{H}_W)) = f[\mathrm{I}(\mathcal{H})]$.

(iv) *Suppose, that f is symmetric, that is, $f(x_1, x_2, \ldots, x_n)$ depends only on $\sum x_i = j$, and, consequently, it can be written as $f(j)$. Then:*

$$\mathrm{IS}(f(\mathcal{H}_W)) = f[\mathrm{IS}(\mathcal{H})].$$

Proof:

(i) $\mathrm{IS}(\mathcal{F}_U) = U^T U$, $\mathrm{IS}(\mathcal{H}_W) = W^T W$, and

$$\mathrm{IS}(\mathcal{F}_U + \mathcal{H}_W) = \begin{pmatrix} U^T & W^T \end{pmatrix} \begin{pmatrix} U \\ W \end{pmatrix} = U^T U + W^T W,$$

implying statement (i).

(ii) Let now $\mathcal{G}_X = \mathcal{F}_U \mathcal{H}_W$.. $G_i \cap G_j$ contains exactly those vertices (u, v) such that $u \in F_i \cap F_j, v \in H_i \cap H_j$, and there are exactly $|F_i \cap F_j||H_i \cap H_j|$ such (u, v) pairs.

(iii) The statement is an easy consequence of Theorem 11, with $k = 2$.

(iv) This follows trivially from (iii).

□

3 Polynomials and algorithmic constructions of set-systems

Lemma 18 *With the notations of Definition 7, the incidence matrix of set-system $f(\mathcal{H}_U)$ can be computed from the incidence matrix U of set-system $\mathcal{H}$ and polynomial f in*

$$O(\mathrm{L}_1(f)nm)$$

time.

□

3.1 Constructions with Interpolating Polynomials

Theorem 19 *Let f be an n-variable symmetric polynomial with non-negative integer coefficients, and let $\mathcal{F}$ be a set-system of size m on the n element universe. Suppose that*

$$\mathrm{L}(\mathcal{F}) = \{|H_i \cap H_j|, H_i \neq H_j, H_i, H_j \in \mathcal{F}\} = \{l_1, l_2, \ldots, l_s\}.$$

Then we can construct in $O(\mathrm{L}_1(f)nm)$ time a hypergraph $f(\mathcal{F})$ of size m on the $\mathrm{L}_1(f)$-vertex universe, such that the sizes of the pairwise intersections of the sets of $f(\mathcal{F})$ is

$$f(l_1), f(l_2), \ldots, f(l_s).$$

Proof: The proof is immediate from Lemma 18 and Theorem 11. $\square$

We note, that if f contains $x_i's$ with a positive coefficient, then $f(\mathcal{F})$ is a set-system (see Lemma 9.)

The assumption on the non-negativity of the coefficients of f in Theorem 19 are very restrictive, it prohibits almost all interpolation polyniomials. The positivity assumption can be left out if the intersection-sizes are specified modulo r only. Moreover, we prove the following:

Theorem 20 *Let p be a prime, and let $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$ be a set-system on the n element universe. Suppose that*

$$\mathrm{L}(\mathcal{H}) \equiv \{l_1, l_2, \ldots, l_s\} \pmod p,$$

where $l_1, l_2, \ldots, l_s$ are pairwise distinct residue classes modulo p, and let $h_1, h_2, \ldots, h_s$, (not necessarily distinct) residue-classes modulo p. Then there exists a set-system with m sets $\mathcal{G} = \{G_1, G_2, \ldots, G_m\}$ on the $(p-1)\sum_{i=0}^{s-1}\binom{n}{i}$ element universe, which can be constructed in $O((p-1)n^{p+1}m)$ time, such that

$$\mathrm{L}(\mathcal{G}) \equiv \{h_1, h_2, \ldots, h_s\} \pmod p,$$

and, if

$$|H_i \cap H_j| \equiv l_k \pmod p, \text{then } |G_i \cap G_j| \equiv h_k \pmod p.$$

Moreover, if $\mathcal{H}$ was a uniform set-system, then $\mathcal{G}$ is also a uniform set-system.

Proof: Let g be the single-variable polinomial over the p element field, such that $g(l_i) = h_i, i = 1, 2, \ldots, s$. Let f be a multi-linear polynomial such that $f(x_1, x_2, \ldots, x_n) = g(x_1 + x_2 + \cdots + x_n)$, then the degree of f is at most $s-1$, and $\mathrm{L}_1(f) \leq (p-1)\sum_{i=0}^{s-1}\binom{n}{i} \leq (p-1)n^p$. Since f is symmetric, Theorem 11 applies for $\mathcal{G} = f(\mathcal{H})$, and Lemma 18 gives the time-bound. If $f(\mathcal{H})$ were not be a set system, then adding $p(x_1 + x_2 + \cdots + x_n)$ to f will produce one. $\square$

The following theorem shows that we can even drop the requirement of a primality of the modulus, and we can use non-symmetric polynomials for the construction, but then, the cardinality of the universe can be large:

Theorem 21 *Let $r \geq 2$ be an integer, and let $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$ be a set-system on the n element universe. Suppose that $\mathrm{I}(\mathcal{H}) = C = \{c_{ij}\}$. Let $D = \{d_{ij}\}$ be an $m \times m$ matrix, with entries from Z_r, satisfying the following property: If $c_{ij} = c_{kl}$, then $d_{ij} = d_{kl}$. Then there exists a set-system $\mathcal{G}$ of size m on the $O(2^n)$-element universe, such that*

$$\mathrm{IS}(\mathcal{G}) \equiv D \pmod{r},$$

and $\mathcal{G}$ is constructible in $O(2^n m)$ time.

Proof: Suppose that for all $c_{ij} \in \{0,1\}^n$, $I_{ij} \subset \{1, 2, \ldots, n\}$ gives the indices of the 1's (all of the other indices correspond to 0 coordinates). Let

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} d_{ij} \prod_{k \in I_{ij}} x_k \prod_{k \notin I_{ij}} (1 - x_k).$$

By Theorem 11, $f(\mathcal{H})$ suffices. Set-systemity can be ensured by a possible addition of $r(x_1 + x_2 + \cdots + x_n)$ to f. □

3.2 Multiple intersections

Here we prove the multiple-intersection analogues of Theorems 20 and 21.

Theorem 22 *Let p be a prime, and let $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$ be a set-system on the n element universe. Suppose that for some $I_1, I_2, \ldots, I_s \subset \{1, 2, \ldots, m\}$:*

$$l_i = |\bigcap_{j \in I_i} H_j| \bmod p.$$

Let $h_1, h_2, \ldots, h_s$, (not necessarily distinct) residue-classes modulo p. Then there exists a set-system with m sets $\mathcal{G} = \{G_1, G_2, \ldots, G_m\}$ on the $(p-1)\sum_{i=0}^{s-1}\binom{n}{i}$ element universe, which can be constructed in $O((p-1)n^{p+1}m)$ time, such that

$$h_i \equiv |\bigcap_{j \in I_i} G_j| \pmod{p}.$$

Moreover, if $\mathcal{H}$ was a uniform set-system, then $\mathcal{G}$ is also a uniform set-system.

Proof: The proof is the same as the proof of Theorem 20. □

Theorem 23 *Let $r \geq 2$ be an integer, and let $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$ be a set-system on the n element universe. For $I \subset \{1, 2, \ldots, m\}$, let us define*

$$C_I = \bigcap_{i \in I} H_i.$$

For $I \subset \{1, 2, \ldots, m\}$, let numbers $d_I \in Z_r$ be given, satisfying the following property: If $C_I = C_J$, then $d_I = d_J$. Then there exists a set-system $\mathcal{G} = \{G_1, G_2, \ldots, G_m\}$ on the $O(2^n)$-element universe, such that for all $I \subset \{1, 2, \ldots, m\}$,

$$|\bigcap_{i \in I} G_i| \equiv d_I \pmod{r},$$

and $\mathcal{G}$ is constructible in $O(2^n m)$ time.

Proof: For set C_I, let $c_I \subset \{1, 2, \ldots, n\}$ give the indices of the 1's (all of the other indices correspond to 0 coordinates). Let

$$f(x_1, x_2, \ldots, x_n) = \sum_I d_I \prod_{k \in c_I} x_k \prod_{k \notin c_I} (1 - x_k).$$

By Theorem 11, $f(\mathcal{H})$ suffices. Set-systemity can be ensured by a possible addition of $r(x_1 + x_2 + \cdots + x_n)$ to f. $\square$

3.3 An application: restricted intersections modulo 6

It was conjectured, that if $\mathcal{H}$ is a set-system over an n element universe, satisfying that $\forall H \in \mathcal{H}$: $|H| \equiv 0 \pmod 6$, but $\forall G, H \in \mathcal{H},\ G \neq H :\ |G \cap H| \not\equiv 0 \pmod 6$ has size polynomial in n. The conjecture was motivated by theorems of Frankl and Wilson, showing polynomial upper bounds for prime or prime-power moduli [FW81]. We have shown in [Gro00b] that there exists an $\mathcal{H}$ with these properties and with super-polynomial size in n. (see the details in [Gro00b].)

Our machinery now permits us to describe this construction easily.

Let k be a positive integer, and let α be the smallest number such that $\sqrt{k} < 2^\alpha$, and let β be the smallest number such that $\sqrt{k} < 3^\beta$. By a result of Barrington, Beigel and Rudich [BBR94], there exists an explicitly constructible ℓ-variable, degree-O($\sqrt{k}$) polinomial f, satisfying over $x = (x_1, x_2, \ldots, x_\ell) \in \{0, 1\}^\ell$:

$$f(x) \equiv 0 \pmod 6 \iff \sum_{i=1}^{\ell} x_i \equiv 0 \pmod{2^\alpha 3^\beta}.$$

Let $\mathcal{G}$ denote the set-system of all $2^\alpha 3^\beta$-element subsets of the $\ell = 2(2^\alpha 3^\beta) - 1$-element universe.

Then consider $\mathcal{H} = f(\mathcal{G})$. By Corollary 17, part (iii), IS($f(\mathcal{G})$) contains 0's in the diagonal mod 6, and non-zeroes modulo 6 off-diagonal, as required. The size of $f(\mathcal{G})$ is the same as the size of $\mathcal{G}$:

$$\binom{\ell}{2^\alpha 3^\beta} > \binom{2k}{k} > \frac{1}{2k+1} 2^{2k},$$

and the size of the universe of $\mathcal{H} = f(\mathcal{G})$ is $n = \mathrm{L}_1(f) = k^{O(\sqrt{k})}$, so

$$|\mathcal{H}| = \exp\left(\frac{c(\log n)^2}{(\log\log n)^2}\right).$$

3.4 How to find initial set systems?

For the constructions of set-systems with restricted intersections, we need initial set-systems. The "quality" of our initial set-system is important for a good construction, however, words "quality" and "good" are not defined here, they always depend on our goals with the actual construction. Here we just give some examples which may lead to nice constructions.

Let p be a prime and α and ℓ be positive integers. Barrington, Beigel and Rudich [BBR94] showed, that there exists a degree-p^α polynomial f on ℓ variables, which is 0 modulo p if $\sum_{i=1}^{\ell} x_i$ is a multiple of p^α. If $\mathcal{H}$ denotes the power-set of the ℓ-element universe, then $f(\mathcal{H})$ is a set-system with 2^ℓ elements over a $O(\ell^{p^\alpha})$-element universe, $f[\mathrm{I}(\mathcal{H}]$ satisfying, that $f(A \cap B) \equiv 0 \pmod{p} \iff |A \cap B| \equiv 0 \pmod{p^\alpha}$. We note, that our construction in Subsection 3.3 can be got as a sum of two similar set systems, one for $p = 2$ and the other for $p = 3$.

Numerous constructions for block-designs and finite geometries may also give a good starting points for algorithmic constructions of new set systems.

One can also easily construct new set-systems using our addition and product operations (see Definition 5).

4 Constructive bounds on set systems

As an important by-product of our construction method, we can generalize some of the upper bounds to set systems with restricted intersections.

Theorem 24 *Let $\mathcal{F}$ be a set system of m sets over an n element universe. Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial with integer coefficients. Suppose, that*

$$f[\mathrm{I}(\mathcal{F})]$$

has full rank (that is, m), over a field. Then

$$m \leq w(f).$$

Proof: By Corollary 17 (iii) $f[\mathrm{I}(\mathcal{F})] = \mathrm{IS}(f(\mathcal{F}))$, so its rank is at most $w(f)$. On the other hand, the $m \times m$ matrix $f[\mathrm{I}(\mathcal{F})]$ is of full rank, so $m = r$. □

This theorem is a generalization of a theorem of Frankl and Wilson [FW81], who proved the theorem for symmetric f's modulo p.

Several theorems for bounding the size of set-systems is a consequence of this theorem. For example, the following theorem which is a non-uniform modular version of the Ray-Chaudhuri-Wilson Theorem [RCW75]) was proven by Deza, Frankl and Singhi [DFS83]. We give here a proof based on interpolating polynomials.

Theorem 25 (Deza, Frankl, Singhi 1983) *Let p be a prime, $L \subset \{0, 1, 2, \ldots, p-1\}$, $|L| = s$, and let $\mathcal{F}$ be a set-system over the n-element universe, such that all $F \in$ $|F| \bmod p \notin L$, but for all $F, G \in \mathcal{F}$, $|F \cap G| \bmod p \in L$. Then*

$$|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}.$$

Proof: Let $L = \{l_1, l_2, \ldots, l_s\}$, and let $g(y) = \prod_{i=1}^{s}(y - l_i)$. $g(y)$ modulo p is 0, if $y \in L$ and non-zero otherwise. Let us define multi-linear polynomial

$$f(x_1, x_2, \ldots, x_n) \equiv g(\sum_{j=1}^{n} x_j) \bmod p,$$

where the congruency holds for $x_i \in \{0, 1\}, i = 1, 2, \ldots, n$. Then by Theorem 24,

$$|\mathcal{F}| \le w(f) \le \sum_{i=0}^{s} \binom{n}{i}$$

and this proves the theorem.

Moreover, from Corollary 17, there exists a set-system $\mathcal{G}$ on the $\mathrm{L}_1(f)$ element universe, such that $|\mathcal{G}| = |\mathcal{F}|$, and the intersection matrix of $\mathcal{G}$ is a diagonal-matrix, with non-zero elements in the diagonal. □

The following theorem is also an easy corollary of Theorem 24, but for its proof we must use non-symmetric polynomials.

Theorem 26 *Let p be a prime, and let $\mathcal{H}$ be a set-system on the n-element universe S. Let $A \subset S, B \subset S$. Suppose, that the sets of $\mathcal{H}$ satisfy:*

(i) $\forall H \in \mathcal{H} : |A \cap H| \not\equiv |B \cap H| \pmod p$,

(ii) $\forall F, H \in \mathcal{H} : |A \cap F \cap H| \equiv |B \cap F \cap H| \pmod p$.

Then $|\mathcal{H}| \le |(A \cup B) - (A \cap B)|$.

Proof: Let $A = \{v_i \in S : i \in I\}, B = \{v_i \in S : i \in J\}$. Then let $f(x) = \sum_{i \in I} x_i - \sum_{j \in J} x_j$. Now, $f[I(\mathcal{H})]$ is a diagonal matrix of rank m, so Theorem 24 applies.

□

5 A structure theorem for polynomials on set-systems

We need the following definition from [Gro00a]:

Definition 27 ([Gro00a]) *Let R be a ring and let n be a positive integer. We say, that $n \times n$ matrix A over R has rank 0 if all of the elements of A are 0. Otherwise, the rank over the ring R of matrix A is the smallest r, such that A can be written as*

$$A = BC$$

over R, where B is an $n \times r$ and C is an $r \times n$ matrix. The rank of A over R is denoted by $\mathrm{rank}_R(A)$.

It is usually a very hard problem to give lower bounds for the degree (or weight or L_1-norm) for specific polynomials, mapping $\{0,1\}^n$ to R, for some ring R; (see [TB98], [BBR94], [Gro95]). Note, that all of the functions $f : \{0,1\}^n \to R$ can be given by such polynomials. The following theorem states, that "small" polynomials cannot make $\mathrm{rank}_R(f[\mathrm{I}(\mathcal{H})]$ large for a big enough set-system $\mathcal{H}$.

Especially, let $R = Z_6$, and if for an $0 \neq u \in Z_6$ and for any $G, H \in \mathcal{H}$, $f(H) = u$, but $f(G \cap H) = 0$, then $w(f) \geq |\mathcal{H}|$.

Moreover, we specify the "best" polynomial for this rôle.

We say, that a set-system $\mathcal{H}$ is a Sperner-system, if $U, V \in \mathcal{H}, U \neq V$ implies $U \not\subset V$. Note, that all uniform set-system is a Sperner-system.

Theorem 28 *Let R be a ring with a unit element, and let $\mathcal{H}$ be a Sperner-system with m members on the n element universe.*

(i) If f is an n-variable polynomial over R, and $\mathrm{rank}_R(f[\mathrm{I}(\mathcal{H})] \geq m$, then $w(f) \geq m$.

(ii) There exists an explicitly constructible polynomial f over R, such that $\mathrm{rank}_R(f[\mathrm{I}(\mathcal{H})] = m$, and $w(f) = \mathrm{L}_1(f) = m$.

Proof: (i) is a corollary of Theorem 24. For proving (ii), let

$$f(x_1, x_2, \ldots, x_n) = \sum_{H \in \mathcal{H}} \prod_{i : v_i \in H} x_i.$$

Clearly, $f[\mathrm{I}(\mathcal{H})]$ is the $m \times m$ identity matrix. □

Let $\mathcal{G}$ denote the uniform set-system, of size $m = \exp\left(c\frac{\log^2 n}{\log\log n}\right)$, constructed on the n element universe in [Gro00b], with the following properties: $\mathrm{IS}(\mathcal{G})$ has 0 elements mod 6 in its diagonal and non-zero element mod 6 elsewhere.

Corollary 29 *For any n variable polynomial over ring Z_6, which is non-zero modulo 6 on the characteristic vectors of the sets of $\mathcal{G}$ and 0 modulo 6 on the characteristic vectors of the intersections of any two elements of $\mathcal{G}$, satisfies*

$$w(f) \geq \exp\left(c\frac{\log^2 n}{\log\log n}\right),$$

for a positive $c > 0$.

Acknowledgments.

The author thanks Zoltán Füredi, Gyula O.H. Katona, Vera T. Sós for discussions on this topic. Part of this research was done while visiting the DIMACS Center in Piscataway, NJ. The author also acknowledges the partial support of János Bolyai Fellowship, of Farkas Bolyai Fellowship, and research grants FKFP 0607/1999, and OTKA T030059.

References

[BBR94] David A. Mix Barrington, Richard Beigel, and Steven Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Comput. Complexity*, 4:367–382, 1994. Appeared also in *Proc. 24th Ann. ACM Symp. Theor. Comput.*, 1992.

[BF92] László Babai and Péter Frankl. *Linear algebra methods in combinatorics*. Department of Computer Science, The University of Chicago, September 1992. preliminary version.

[BMRV00] H. Buhrman, P.B. Miltersen, J. Radhakrishnan, and S. Venkatesh. Are bitvectors optimal? In *Proc. 32nd Ann. ACM Symp. Theor. Comput.*, pages 449–458, 2000.

[DFS83] M. Deza, P. Frankl, and N. M. Singhi. On functions of strength t. *Combinatorica*, 3:331–339, 1983.

[FF86] P. Frankl and Z. Füredi. Finite projective spaces and intersecting hypergraphs. *Combinatorica*, 6(4):335–354, 1986.

[Für91] Zoltán Füredi. Turán type problems. In *Surveys in combinatorics, 1991 (Guildford, 1991)*, pages 253–300. Cambridge Univ. Press, Cambridge, 1991.

[FW81] Péter Frankl and R. M. Wilson. Intersection theorems with geometric consequences. *Combinatorica*, 1(4):357–368, 1981.

[Gro95] Vince Grolmusz. On the weak mod m representation of Boolean functions. *Chicago Journal of Theoretical Computer Science*, 1995(2), July 1995.

[Gro00a] Vince Grolmusz. Low-rank co-diagonal matrices and Ramsey graphs. *The Electronic Journal of Combinatorics*, 7:R15, 2000. www.combinatorics.org.

[Gro00b] Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20:73–88, 2000.

[HBc95] Handbook of combinatorics. Elsevier-MIT Press, 1995.

[KK93] Jeff Kahn and Gil Kalai. A counterexample to Borsuk's conjecture. *Bull. Amer. Math. Soc. (N.S.)*, 29(1):60–62, 1993.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs. randomness. *J. Comput. System Sci.*, 49:149–167, 1994.

[RCW75] D. K. Ray-Chaudhuri and R. M. Wilson. On t-designs. *Osaka J. Math.*, 12:735–744, 1975.

[TB98] Gábor Tardos and David A. Mix Barrington. A lower bound on the MOD 6 degree of the OR function. *Comput. Complex.*, 7:99–108, 1998.