COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **20** (1) (2000) 71–85

SUPERPOLYNOMIAL SIZE SET-SYSTEMS WITH RESTRICTED INTERSECTIONS MOD 6 AND EXPLICIT RAMSEY GRAPHS

VINCE GROLMUSZ*

Received January 15, 1996
Revised August 2, 1999

Dedicated to the memory of Paul Erdős

We construct a system $\mathcal{H}$ of $\exp(c\log^2 n/\log\log n)$ subsets of a set of n elements such that the size of each set is divisible by 6 but their pairwise intersections are not divisible by 6. The result generalizes to all non-prime-power moduli m in place of $m=6$. This result is in sharp contrast with results of *Frankl* and *Wilson* (1981) for prime power moduli and gives strong negative answers to questions by *Frankl* and *Wilson* (1981) and *Babai* and *Frankl* (1992). We use our set-system $\mathcal{H}$ to give an explicit Ramsey-graph construction, reproducing the logarithmic order of magnitude of the best previously known construction due to *Frankl* and *Wilson* (1981). Our construction uses certain mod m polynomials, discovered by *Barrington*, *Beigel* and *Rudich* (1994).

1. Introduction

Generalizing the *Ray-Chaudhuri–Wilson* theorem [11], *Frankl* and *Wilson* [9] proved the following intersection theorem, one of the most important results in extremal set theory:

Theorem 1.1 (Frankl–Wilson). *Let $\mathcal{F}$ be a set-system over a universe of n elements. Suppose $\mu_0, \mu_1, \ldots, \mu_s$ are distinct residues modulo a prime p,*

* Part of this research was done while the author was visiting the Department of Computer Science at The University of Chicago.

Mathematics Subject Classification (1991): 05D05, 05D10, 68Q25

such that for all $F \in \mathcal{F}$,

$$|F| = k \equiv \mu_0 \pmod{p},$$

where $k+s \le n$, *and for any two distinct* $F, G \in \mathcal{F}$:

$$|F \cap G| \equiv \mu_i \pmod{p} \text{ for some } i,\ 1 \le i \le s.$$

Then

$$|\mathcal{F}| \le \binom{n}{s}. \tag{1}$$ ∎

This theorem has numerous applications in combinatorics and in geometry (e.g., the disproof of *Borsuk's conjecture* by *Kahn* and *Kalai* [10] (cf. [2], Sec. 5.6.), an explicit construction of Ramsey graphs, and geometric applications related to the Hadwiger-problem [9].)

Frankl and *Wilson* [9] asked whether inequality (1) remains true when the modulus p is replaced by a composite number m, or at least in the subcase $s = m-1$.

Frankl [8] answered the first of these questions (arbitrary $s \le m$) in the negative: he constructed faster growing set-systems for $m=6$, as well as for $m=p^2$, p prime. For $m=6$, *Frankl's* set-systems satisfy $s=3$ and $|\mathcal{F}| \approx cn^4$.

On the other hand, *Frankl* and *Wilson* [9] proved that inequality (1) remains in force when $s=m-1$ and m is a prime power.

In this paper we consider non-prime-power moduli m. For any such modulus, we give a very strong negative answer to both versions of the Frankl–Wilson question: we prove that for $s=m-1$, no upper bound of the form $n^{f(m)}$ exists. More precisely, we prove the following.

Theorem 1.2. *Let* m *be a positive integer, and suppose that* m *has* $r>1$ *different prime divisors:* $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. *Then there exists* $c = c(m) > 0$, *such that for every integer* $h > 0$, *there exists an explicitly constructible uniform set-system* $\mathcal{H}$ *over a universe of* h *elements, such that*

(a) $|\mathcal{H}| \ge \exp\left(c \frac{(\log h)^r}{(\log\log h)^{r-1}}\right)$,
(b) $\forall H \in \mathcal{H}\colon |H| \equiv 0 \pmod{m}$,
(c) $\forall G, H \in \mathcal{H}, G \ne H\colon |G \cap H| \not\equiv 0 \pmod{m}$.

Remark 1.1. The value of c is roughly p_r^{-r}, where p_r is the largest prime divisor of m. The size of the sets in the set-system we construct is

$$h^{\frac{r-1}{2r-1}+o(1)}. \tag{2}$$

We note that for fixed m (m is not a prime power), the size of $\mathcal{H}$ grows faster than any polynomial of n. This is quite surprising, since previously it was believed that the failure of the attempts to prove a polynomial upper bound was due to the lack of techniques to handle non-prime-power composite moduli.

Our result gives a strong negative answer to a conjecture of *Babai* and *Frankl* ([2], Section 7.3, Conjecture C(r)). *Babai* and *Frankl* conjectured that conditions (b) and (c) of Theorem 1.2 imply

$$|\mathcal{H}| \le \binom{h}{m-1};$$

whereas our result shows that no bound of the form $h^{f(m)}$ exists for composite, non-prime power moduli m.

We can even strengthen statement (c) of Theorem 1.2 as follows:

Theorem 1.3. *Theorem 1.2 remains valid if we add the following condition:*

(d) $\forall G, H \in \mathcal{H}$, $G \neq H$ *and* $\forall i \in \{1,2,\ldots,r\}$, *we have* $|G \cap H| \equiv 0 \pmod{p_i^{\alpha_i}}$ *or* $|G \cap H| \equiv 1 \pmod{p_i^{\alpha_i}}$.

Remark 1.2. *Theorem 1.3 implies that there exist super-polynomial size set-systems $\mathcal{H}$ such that the size of each set in $\mathcal{H}$ is divisible by m and the sizes of the pairwise intersections of the sets in $\mathcal{H}$ occupy at most $2^r - 1$ residue classes mod m out of the possible $m-1$ nonzero residue classes.*

In fact, this result can be further strengthened: 3 residue classes of intersection size suffice! This answers a question of Peter Frankl (private communication).

Corollary 1.1. *Let m be a positive integer, and suppose that m has $r > 1$ different prime divisors: $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Then there exists $c = c(m) > 0$, such that for every integer $h > 0$, there exists an explicitly constructible uniform set-system $\mathcal{H}$ over a universe of h elements such that*

(a) $|\mathcal{H}| \ge \exp\left(c \frac{(\log h)^2}{\log\log h}\right)$,

(b) $\forall H \in \mathcal{H}$: $|H| \equiv 0 \pmod{m}$,

(c) *the sizes of the pairwise intersections $|G \cap H|$ $(G, H \in \mathcal{H}, G \neq H)$ occupy only 3 residue classes mod m, none of which is 0.*

One of the striking applications of the Frankl–Wilson theorem for prime moduli was an explicit construction of graphs of size $\exp(c \log^2 n / \log\log n)$ without homogeneous subsets (cliques or anti-cliques) of size n. These are the

largest explicit Ramsey-graphs known to-date. As an application of our Theorem 1.2, we give an alternative construction of explicit Ramsey graphs of the same logarithmic order of magnitude, *i.e.,* of size $\exp(c' \log^2 n / \log\log n)$. (But our c' is less than their c).

A key ingredient of our construction is a low-degree polynomial constructed by *Barrington*, *Beigel* and *Rudich* [5], to represent the Boolean "OR" function mod m. Any reduction of the degree of such polynomials would yield improved explicit Ramsey graphs.

2. Preliminaries

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function and let m be a positive integer. *Barrington*, *Beigel* and *Rudich* [5] gave the following definition:

Definition 2.1. The polynomial P with integer coefficients *weakly represents* the Boolean function f modulo m if there exists an $S \subset \{0,1,2,\ldots,m-1\}$ such that for all $x \in \{0,1\}^n$,

$$f(x) = 0 \iff (P(x) \bmod m) \in S.$$

Here $(a \bmod m)$ denotes the smallest non-negative $b \equiv a \bmod m$.

We are interested in the smallest degree of polynomials representing f modulo m. Without loss of generality we may assume P is multilinear (since $x_i^2 = x_i$ over $\{0,1\}^n$).
Let $\mathrm{OR}_n : \{0,1\}^n \to \{0,1\}$ denote the n-variable OR-function:

$$\mathrm{OR}_n(x_1, x_2, \ldots, x_n) = \begin{cases} 0, & \text{if } x_1 = x_2 = \cdots = x_n = 0 \\ 1 & \text{otherwise.} \end{cases}$$

Suppose that the polynomial P weakly represents OR_n modulo a prime p. Without loss of the generality we may assume that for $x \in \{0,1\}^n$,

$$P(x) \equiv 0 \bmod p \iff x = (0,0,\ldots,0).$$

Then

$$1 - P^{p-1}(1 - x_1, 1 - x_2, \ldots, 1 - x_n)$$

is exactly the n-variable AND function, which can uniquely be written as a multilinear monomial

$$x_1 x_2 x_3 \ldots x_n.$$

Consequently, if the polynomial P weakly represents OR_n over $GF(p)$, then its degree is at least

$$\left\lceil \frac{n}{p-1} \right\rceil.$$

Tardos and *Barrington* [12] proved that the same conclusion holds if p is a prime power.

On the other hand, *Barrington, Beigel* and *Rudich* [5] proved that the conclusion fails for composite moduli with at least two distinct prime divisors:

Theorem 2.4 (Barrington, Beigel, Rudich). *Given $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ where the p_i are distinct primes, there exists an explicitly constructible polynomial P of degree $O(n^{1/r})$ which weakly represents OR_n modulo m.*

For completeness, we reproduce here a short proof of this theorem.

Proof. Let $S_k(x)$ denote the k^{th} elementary symmetric polynomial, *i.e.* the sum of all multilinear monomials of degree k, formed from variables $x_1, x_2, \ldots, x_n$. For $x \in \{0,1\}^n$, the *weight* of x is defined as $\mathrm{wt}(x) = \sum_{i=1}^{n} x_i$. If $\mathrm{wt}(x) = \ell$, then

$$s_k(x) = \binom{\ell}{k}.$$

Since the value of $s_k(x)$ depends only on $\mathrm{wt}(x)$, with some abuse of the notation we shall write $s_k(x)$ as $s_k(j)$ where $j = \mathrm{wt}(x)$. Using this notation, one can formulate the following observation made in [5]:

Lemma 2.1. *[5] Let k be a positive integer, p be a prime and let e be the smallest integer satisfying $k < p^e$. Then $s_k(j) \equiv s_k(j + p^e) \pmod{p}$.*

Proof. We need to prove

$$\binom{j + p^e}{k} \equiv \binom{j}{k} \pmod{p}.$$

This is immediate from the identity

$$\binom{u+v}{t} = \sum_{w=0}^{t} \binom{u}{w} \binom{v}{t-w},$$

and the elementary fact that for any $1 \le \ell < p^e$, p is a divisor of $\binom{p^e}{\ell}$. ∎

Now, for $i = 1, 2, \ldots, r$, let e_i be the smallest integer that satisfies

$$p_i^{e_i} > \lceil n^{1/r} \rceil.$$

We define, for $i = 1, 2, \ldots, r$, the symmetric polynomial $G_i(x)$ by

$$G_i(x) = \sum_{j=1}^{p_i^{e_i} - 1} (-1)^{j+1} s_j(x).$$

One can easily prove (using the binomial expansion of $(1-1)^{p_i^{e_i}-1}$), that G_i correctly computes over the integers the OR function for inputs of weight at most $p_i^{e_i}-1$. Consequently, G_i correctly computes modulo p_i the OR function for inputs of weight at most $n^{1/r}$, and, additionally, $G_i \bmod p_i$ is periodic with period $p_i^{e_i}$.

And now, by the Chinese Remainder Theorem, there exists a polynomial P which satisfies

$$P \equiv G_i \pmod{p_i}$$

for $i = 1,2,\ldots,r$, and the degree of P is the maximum of the degrees of polynomials G_i, $O(n^{1/r})$.

It is obvious that for $x \in \{0,1\}^n$, if $\mathrm{wt}(x) \neq 0$ then there exists an i, $1 \leq i \leq r$, such that $\mathrm{wt}(x) \not\equiv 0 \bmod p_i^{e_i}$, so $P(x) \not\equiv 0 \bmod p_1 p_2 \ldots p_r$. In addition, $P(0,0,\ldots,0) = 0$. Consequently, P weakly represents the OR function for all inputs in $\{0,1\}^n$ modulo $p_1 p_2 \ldots p_r$. Since $p_1 p_2 \ldots p_r$ is a divisor of m, if $P(x)$ is not 0 modulo $p_1 p_2 \ldots p_r$ then it is not 0 modulo m. Consequently, P weakly represents the OR function for all inputs in $\{0,1\}^n$ modulo m. ∎

Example. Let $m = 6$, and let

$$G_1(x) = \sum_{j=1}^{2^3-1} (-1)^{j+1} s_j(x),$$

and

$$G_2(x) = \sum_{j=1}^{3^2-1} (-1)^{j+1} s_j(x).$$

Then

$$P(x) = 3G_1(x) + 4G_2(x)$$

weakly represents OR_{71} modulo 6 (or modulo 6ℓ for any integer ℓ), and its degree is only 8.

Corollary 2.2. *Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Then there exists an explicitly constructible polynomial P' with n variables and of degree $O(n^{1/r})$ which is equal to 0 on $x = (0,0,\ldots,0) \in \{0,1\}^n$, it is nonzero mod m for all other $x \in \{0,1\}^n$, and for all $x \in \{0,1\}^n$ and for all $i \in \{1,\ldots,r\}$, $P(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ or $P(x) \equiv 1 \pmod{p_i^{\alpha_i}}$.*

Proof. Let us consider first the easy case, when $\alpha_1 = \alpha_2 = \cdots = \alpha_r = 1$. Then the statement is immediate from Lemma 2.1 and from the fact that polynomials G_i not only represent, but compute the OR function for inputs of weight less than $p_i^{e_i}$.

In the general case, let us observe that G_i is either 0 or 1 modulo p_i on $\{0,1\}^n$. Then we need the modulus-amplifying polynomials R_i of degree $2\alpha_i$ of *Beigel* and *Tarui* [6], with the following properties:

$$N \equiv 0 \pmod{p_i} \Longrightarrow R_i(N) \equiv 0 \pmod{p_i^{\alpha_i}}$$

and

$$N \equiv 1 \pmod{p_i} \Longrightarrow R_i(N) \equiv 1 \pmod{p_i^{\alpha_i}}.$$

Now, set $G_i' = R_i \circ G_i$ and construct P' by applying the Chinese Remainder Theorem to the G_i'. ∎

3. The Lower Bound

Proof of Theorem 1.2

Let $P(z_1, z_2, \ldots, z_n)$ be a polynomial of degree d which satisfies that $P(0,0,0,\ldots,0) = 0$, and for every $(z_1, z_2, \ldots, z_n) \in \{0,1\}^n$

$$P(z_1, z_2, \ldots, z_n) \equiv 0 \pmod{m} \Longleftrightarrow z_1 = z_2 = \ldots = z_n = 0.$$

An explicit construction of such P of degree $d = O(n^{1/r})$ was given in Theorem 2.4.
Let $Q(z_1, z_2, \ldots, z_n) = P(1 - z_1, 1 - z_2, \ldots, 1 - z_n)$. Then $Q(1,1,1,\ldots,1) = 0$, and for all $z \in \{0,1\}^n$ we have

$$Q(z) \equiv 0 \pmod{m} \Longleftrightarrow z_1 = z_2 = \ldots = z_n = 1. \tag{3}$$

Using the polynomial Q we state our main Lemma:

Lemma 3.2. *For every integer $n > 0$, there exists a uniform set-system $\mathcal{H}$ over a universe of $2(m-1)n^{2d}/d!$ elements which is explicitly constructible from the polynomial Q and satisfies*

(a) $|\mathcal{H}| = n^n$,
(b) $\forall H \in \mathcal{H}\colon |H| \equiv 0 \pmod{m}$,
(c) $\forall G, H \in \mathcal{H}, G \neq H\colon |G \cap H| \not\equiv 0 \pmod{m}$.

Lemma 3.2 easily yields Theorem 1.2 setting $d = \Theta(n^{1/r})$ and using elementary estimations for the binomial coefficients.

Proof of Lemma 3.2. Q can be written as

$$Q(z_1, z_2, \ldots, z_n) = \sum_{i_1, i_2, \ldots, i_\ell} a_{i_1, i_2, \ldots, i_\ell} z_{i_1} z_{i_2} \ldots z_{i_\ell},$$

where $0 \le \ell \le d$, and $a_{i_1,i_2,\ldots,i_\ell}$ is integer, $1 \le i_1 < i_2 < \cdots < i_\ell \le n$. Let us define

$$\tilde{Q}(z_1, z_2, \ldots, z_n) = \sum_{i_1,i_2,\ldots,i_\ell} \tilde{a}_{i_1,i_2,\ldots,i_\ell} z_{i_1} z_{i_2} \ldots z_{i_\ell}, \tag{4}$$

where $\tilde{a}_{i_1,i_2,\ldots,i_\ell} = (a_{i_1,i_2,\ldots,i_\ell} \bmod m)$ is the smallest, positive integer, congruent to $a_{i_1,i_2,\ldots,i_\ell}$ modulo m, for $1 \le i_1 < i_2 < \cdots < i_\ell \le n$.

We note, that (3) is satisfied for $\tilde{Q}$, but $\tilde{Q}(1,1,1,\ldots,1)$ is not necessarily 0.

Let the function $\delta : \{0,1,\ldots,n-1\} \times \{0,1,\ldots,n-1\} \to \{0,1\}$ be defined as

$$\delta(u,v) = \begin{cases} 1, & \text{if } u = v, \\ 0 & \text{otherwise.} \end{cases}$$

Let $A = (a_{xy})$ be an $n^n \times n^n$ matrix $(x, y \in \{0,1,2,\ldots,n-1\}^n)$.

We define the entry a_{xy} as follows:

$$a_{xy} = \tilde{Q}(\delta(x_1,y_1), \delta(x_2,y_2), \ldots, \delta(x_n,y_n)) \bmod m. \tag{5}$$

We note that $a_{xx} = \tilde{Q}(1,1,\ldots,1) \equiv 0 \pmod m$. Conversely, if $a_{xy} \equiv 0 \pmod m$ then $x = y$.

By equation (4), the polynomial $\tilde{Q}(z)$ is a sum of the monomials of the form $z_{i_1} z_{i_2} \ldots z_{i_\ell}$ $(\ell \le d)$. We wish to keep all coeffcients equal to 1; therefore we shall say that the monomial $z_{i_1} z_{i_2} \ldots z_{i_\ell}$ $(\ell \le d)$ occurs with *multiplicity* $\tilde{a}_{i_1,i_2,\ldots,i_\ell}$ in this sum. Note that each multiplicity is a nonnegative integer $\le m-1$.

Consequently, the matrix A is a sum of the matrices $B_{i_1,i_2,\ldots,i_\ell} = (b_{x,y}^{i_1,i_2,\ldots,i_\ell})$, corresponding to the monomial $z_{i_1} z_{i_2} \ldots z_{i_\ell}$ in the following way:

$$b_{x,y}^{i_1,i_2,\ldots,i_\ell} = \delta(x_{i_1}, y_{i_1}) \delta(x_{i_2}, y_{i_2}) \ldots \delta(x_{i_\ell}, y_{i_\ell}).$$

This matrix occurs in the sum with multiplicity $\tilde{a}_{i_1,i_2,\ldots,i_\ell}$.

It is easy to verify that $B_{i_1,i_2,\ldots,i_\ell}$ is permutationally equivalent to the matrix

$$\begin{pmatrix} J_1 & & & 0 \\ & \ddots & & \\ 0 & & & \\ & & & J_{n^\ell} \end{pmatrix} \tag{6}$$

where the diagonal blocks J_i are all-ones matrices of size $n^{n-\ell} \times n^{n-\ell}$, and there are exactly n^ℓ pairwise disjoint all-ones blocks in $B_{i_1,i_2,\ldots,i_\ell}$. "Permutationally equivalent" means that there exists a permutation such that if it

is applied both to the rows and to the columns of the matrix, the result is equal to (6). Let us refer to these all-ones blocks of $B_{i_1,i_2,\ldots,i_\ell}$ as *B-blocks*. We shall say that each B-block of $B_{i_1,i_2,\ldots,i_\ell}$ occurs with multiplicity $\tilde{a}_{i_1,i_2,\ldots,i_\ell}$.

By equation (4), A can be written in the following form:

$$A = \sum_{i_1,i_2,\ldots,i_\ell} \tilde{a}_{i_1,i_2,\ldots,i_\ell} B_{i_1,i_2,\ldots,i_\ell}. \tag{7}$$

Lemma 3.3. *Taking multiplicities into account,*

(a) *every cell of the main diagonal of A is covered by the same number of B-blocks, and this number is divisible by m;*
(b) *for any pair of cells of the main diagonal of A, the number of those B-blocks which cover both members of the pair, is not divisible by m.*

Proof. We note that the number of B-blocks covering cell (x,y) is a_{xy}. Now statement (a) follows by equation (3), observing that for all x,

$$a_{xx} = \tilde{Q}(1,1,\ldots,1) \equiv 0 \pmod{m}.$$

For part (b), we note that the B-blocks are square submatrices, symmetric to the diagonal; therefore a B-block covers the cells (x,x) and (y,y) exactly if it covers the cell (x,y). The number of B-blocks covering both (x,x) and (y,y) is therefore $a_{xy} \not\equiv 0 \pmod{m}$, again by equation (3). ∎

Corollary 3.3. *There exists an explicitly constructible hypergraph $\mathcal{G}$ with n^n vertices and fewer than $2(m-1)n^{2d}/d!$ edges, such that every vertex is contained in the same number of edges, and this number is divisible by m; while for any two vertices, the number of edges, containing both of the vertices, is not divisible by m. (We allow multiple edges and take multiplicities into account.)*

Proof. From Lemma 3.3, choose the cells of the diagonal of A for the vertices and the intersections of the B-blocks with the diagonal for edges (with the corresponding multiplicity).

The number of edges is

$$h := \tilde{Q}(n,n,\ldots,n) = \sum_{\ell \le d} \sum \tilde{a}_{i_1,i_2,\ldots,i_\ell} n^\ell \le (m-1) \sum_{\ell \le d} \binom{n}{\ell} n^\ell$$

$$< (m-1) \sum_{\ell \le d} n^{2\ell}/\ell! < 2(m-1)n^{2d}/d!,$$

assuming, as we may, that $n \ge 2d$. ∎

We note that the number of edges containing each vertex is

$$\tilde{Q}(1,1,\ldots,1) \leq (m-1)\left(\binom{n}{d}+\binom{n}{d-1}+\ldots\binom{n}{0}\right) < 2(m-1)\binom{n}{d}.$$

Now we are ready to complete the proof of Lemma 3.2.

Let us consider the dual of the hypergraph of Corollary 3.3, i. e., let the universe be the set of B-blocks, and if a B-block was present a times in the hypergraph $\mathcal{G}$, then it will correspond to a different points (or elements) in the universe. Consequently, our universe is a set (rather than a multiset). The size of the universe is $h<2(m-1)n^{2d}/d!$.

The diagonal cells of A correspond to the members of the set-system $\mathcal{H}$: the set corresponding to cell (x,x) consists of exactly those B-blocks which cover (x,x). Therefore $|\mathcal{H}|=n^n$.

Since every diagonal cell of A is covered by the same number of B-blocks, the resulting $\mathcal{H}$ is a uniform set system. As discussed previously, this number (the size of the members of $\mathcal{H}$) is $\tilde{Q}(1,1,\ldots,1)\leq(m-1)\sum_{\ell=0}^{d}\binom{n}{d}<2(m-1)\binom{n}{d}$.

From Corollary 3.3, statements (a), (b), (c) of Lemma 3.2 follow. ∎

Remark 3.3. *We note from the foregoing that the number of vertices of $\mathcal{H}$ is $h:=\tilde{Q}(n,n,\ldots,n)$, and the number of vertices of each member of $\mathcal{H}$ is $\tilde{Q}(1,1,\ldots,1)$. We note that $\tilde{Q}(n,n,\ldots,n)\leq n^d\tilde{Q}(1,1,\ldots,1)$.*

To prove the estimate on the size of the members of $\mathcal{H}$ in terms of h (the number of vertices of $\mathcal{H}$) given in Remark 1.1, we first add dummy vertices to increase h to its upper bound $h':=n^d\tilde{Q}(1,1,\ldots,1)$ stated above. Now, since this quantity is still $\leq 2(m-1)n^{2d}/d!$, we see, using the bound $d=O(n^{1/r})$ guaranteed by Theorem 2.4, that

$$n^d \geq (h')^{\frac{r}{2r-1}+o(1)}$$

and therefore the size of the members of $\mathcal{H}$ is

$$\tilde{Q}(1,1,\ldots,1) \leq (h')^{\frac{r-1}{2r-1}+o(1)},$$

as claimed in equation (2). ∎

Proof of Theorem 1.3. The statement is immediate if the polynomial P' of Corollary 2.2 is used for the construction of the set-system $\mathcal{H}$ in the proof of Theorem 1.2 in the place of the polynomial P. ∎

Proof of Corollary 1.1. Let $m' = p_1^{\alpha_1} p_2^{\alpha_2}$, and apply Theorem 1.3 for constructing a set-system $\mathcal{H}$ for h and this m'. The intersections occupy only 3 residue classes modulo m'. Now replace every point of the universe by m/m' new points; the new points will be the members of exactly the same sets of the set-system as the old point. The statement follows. ∎

4. An Application: Ramsey Graphs

The set-system $\mathcal{H}$ of Theorem 1.2 yields new families of explicit Ramsey-graphs.

Theorem 4.5 (Frankl–Wilson, 1981). *For $t \geq 3$, there exists an explicitly constructible graph on $\exp\left(c\frac{(\log t)^2}{(\log\log t)}\right)$ vertices which does not contain either a complete graph or an independent set of size t.*

The constant c given in [9] is $c = \frac{1}{4}$. Our construction yields $c = \frac{2}{81}$ only. In addition to giving a novel proof of Theorem 4.5, we extend it to the case of several colors:

Theorem 4.6. *For $r \geq 2$, $t \geq 3$, there exists an explicitly constructible r-coloring of the edges of the complete graph on $\exp\left(c_r \frac{(\log t)^r}{(\log\log t)^{r-1}}\right)$ vertices such that no color contains a complete graph on t vertices. Here $c_r = c/p_r^{2r} \sim c(r\ln r)^{-2r}$, where p_r is the r^{th} prime, and $c > 0$ is an absolute constant.*

The *existence* of graphs with $ct2^{t/2}$ vertices without a complete subgraph or an independent set of size t was proved in Erdős's celebrated 1947 paper [7]. Erdős's probabilistic proof can be easily adapted to yield the *existence* of an r-coloring of the edges of the complete graph on $c(r)tr^{t/2}$ vertices, without a monochromatic complete subgraph on t vertices. (The exact formula is $\lfloor (t/e)r^{(t-1)/2-1/t} \rfloor$ so we can take $c(r) = 1/(er)$.)

Proof of Theorem 4.6. Let $m = p_1 p_2 \ldots p_r$, where p_i is the i^{th} prime. Let K be a complete graph on vertex-set $\mathcal{H}$, where $\mathcal{H}$ is a set-system with the properties stated in Theorem 1.2, with $h = \lfloor t^{1/p_r} \rfloor$. We define an r-coloring of the edges of K by colors $1, 2, \ldots, r$ as follows: edge UV, where $U, V \in \mathcal{H}$, has color i if

$$i = \min_{j \in \{1,2,\ldots,r\}} \{j : p_j \text{ does not divide } |U \cap V|\}.$$

Now suppose that K contains a monochromatic complete graph C_i of ℓ_i vertices in color i. Then the sets, corresponding to the vertices of C_i, give a family of ℓ_i sets, such that the size of each set is divisible with p_i, but the size of the intersection of any two elements of this set-system is not divisible by p_i. Consequently, by Theorem 1.1,

$$\ell_i \leq \binom{h}{p_i - 1} < t. \qquad \blacksquare$$

5. Open Problems

Problem 1. (*Barrington, Beigel* and *Rudich* [5]) Does there exist a polynomial P in n variables, with integer coefficients, of degree $d = o(\sqrt{n})$, which weakly represents the n-variable OR function modulo 6? (Recall, that this means that $P(0,0,\ldots,0) = 0$, and $P(x) \not\equiv 0 \bmod 6$ for any $x \in \{0,1\}^n, x \neq 0$.)

If the answer is yes for some $d = n^{\varepsilon}$ and the polynomials are explicitly constructed, then our method yields explicit Ramsey-graphs on

$$\exp\left(c\frac{(\log h)^{1/\varepsilon}}{(\log\log h)^{1/\varepsilon - 1}}\right)$$

vertices, with no complete subgraph and no independent set of size h.

For symmetric polynomials, *Barrington, Beigel* and *Rudich* [5] have shown that the degree is $\Omega(\sqrt{n})$.

Showing only the *existence* of polynomials, weakly representing the OR function with degree $o(\sqrt{n})$, would also have considerable theoretical interest, since this result would imply the existence of larger set-systems in Theorem 1.2. Here we should also mention that the best lower bound is due to *G. Tardos* and *Barrington* [12]. They proved that if the modulus m has $r > 1$ different prime divisors, then every polynomial, weakly representing the function OR_n modulo m, has degree at least

$$(\log n)^{1/(r-1)}.$$

Problem 2. Does there exist a quadratic polynomial P in n variables, with integer coefficients, which weakly represents the n-variable OR function modulo $2^{\alpha}3^{\beta}$, where both 2^{α} and 3^{β} are $o(\sqrt{n})$? If the answer is yes, then combining this P and the polynomial of *Barrington, Beigel* and *Rudich* [5], we would obtain a polynomial, satisfying the requirements of Problem 1.

Problem 3. It remains an open question whether, for a fixed positive integer m, a better than exponential ($\exp(o(n))$) upper bound holds for the size

of set-systems satisfying that the size of each set is divisible by m while the sizes of their pairwise intersections are not divisible by m.

This problem is open even for $m=6$. Our main result shows that if m is not a prime power then no polynomial upper bound ($O(n^c)$) holds. (If m is a prime power then a polynomial upper bound holds by Frankl–Wilson 1.1.)

Problem 4. If in Problem 3 we assume additionally that the sizes of the pairwise intersections occupy only two residue classes mod m then there may even be a polynomial upper bound (perhaps $O(n^2)$), yet we are not aware of any better-than-exponential upper bound even for this case. This, too, is open for $m=6$.

Acknowledgments. The author wishes to thank *Zoltán Király* and *David Mix Barrington* for fruitful discussions and to *Péter Frankl* for valuable comments and suggestions. The author is especially grateful to *Laci Babai* for numerous helpful remarks and suggestions. The author acknowledges the support of grants OTKA T030059, FKFP 0607/1999, AKP 97–56 2,1.

6. Added in Proof: Another multi-colored Ramsey graph construction

This section describes further developments regarding the multi-color Ramsey graph construction (Theorem 4.6).

While the present paper was being refereed, we found a much simpler proof of Theorem 4.6 (explicit multi-color Ramsey graphs). In addition to its simplicity, the new proof also yields a better constant in the exponent, matching the Frankl–Wilson bound in the case of 2 colors.

Originally we intended to publish this construction in a separate note. However, while the present paper was edited for printing, it was pointed out to us that Noga Alon's recent paper [1] includes a multi-colored Ramsey-graph construction. Alon's work and ours was independent, although our original submission, which included the proof of Theorem 4.6, predates Alon's.

Alon's construction as well as our two separate constructions share the idea of working modulo a product of consecutive primes within an interval $(p, p(1+\varepsilon))$. Alon's construction gives the same constant in the exponent as the one we give below. The two constructions are rather similar but not identical. Here we describe our version.

A *q-ary code of length n* is a subset of the set of q^n strings of length n over an alphabet of size q. We shall use the following extension of the

Frankl–Wilson theorem in the analysis of our construction. The result is due to *Babai, Snevily,* and *Wilson* [3].

Theorem 6.7 ([3, Theorem 4]). *Let C be a q-ary code of length n and let p be a prime. If the Hamming distances that occur between pairs of distinct codewords in C all belong to s residue classes mod p, no one of which is 0 mod p, then*

$$|C| \le \sum_{j=0}^{s} (q-1)^j \binom{n}{j}. \tag{8}$$

The construction. For a sufficiently large n, let $p_1, p_2, \ldots, p_r$ be distinct primes in the interval $n^{1/r} < p_i < (1+\varepsilon)n^{1/r}$ for $i = 1, 2, \ldots, r$.

The vertex set of our complete graph will be the set $V = \Sigma^n$, the set of strings of length n over the alphabet $\Sigma = \{0, 1, \ldots, q-2, q-1\}$. For $x, y \in V$ let $d(x, y)$ denote their Hamming-distance.

We define the r-coloring as follows: two strings $x, y \in V$ $(x \neq y)$ are joined by an edge of color i if $i = \min\{\ell : p_\ell \not| \, d(x, y)\}$. This is an r-coloring of the edges of the complete graph on vertex set V because $p_1 p_2 \cdots p_r > n$.

Analysis. Suppose that $V_i \subset V$ induces a monochromatic complete subgraph of color i. Then, by inequality (8),

$$|V_i| \le \sum_{j=0}^{p_i - 1} (q-1)^j \binom{n}{j}. \tag{9}$$

Set $q = \lceil n^{1/r} \rceil$. Then the right hand side of equation (9) is at most $\exp((1+\varepsilon)n^{1/r} \log n)$. Consequently,

$$|V| = q^n = \lceil n^{1/r} \rceil^n \ge \exp\left(\frac{c(\log |V_i|)^r}{(\log \log |V_i|)^{r-1}} \right),$$

where $c = ((1+\varepsilon)r)^{-r}$. ∎

Acknowledgment. The author wishes to thank *Laci Babai* for his advice regarding this proof and especially for pointing out reference [3].

We should also mention another relevant result. *Babai, Frankl, Kutin* and *Štefankovič* [4] recently filled the gap between the Frankl–Wilson Theorem (prime modulus, Theorem 1.1) and our main result (non-prime-power

modulus, Theorem 1.2) by showing that under the conditions of the Frankl–Wilson Theorem modulo a *prime power,* a bound of the form

$$|\mathcal{F}| \leq \sum_{k=0}^{f(s)} \binom{n}{k}$$

holds, where $f(s) \leq 2^{s-1}$. Note that for fixed s, the right hand side is polynomially bounded as a function of n (like in the Frankl–Wilson Theorem but unlike in our Theorem 1.2).

References

[1] N. Alon: The Shannon capacity of a union, *Combinatorica,* **18** (1998) 301–310.

[2] L. Babai and P. Frankl: *Linear algebra methods in combinatorics*, Department of Computer Science, The University of Chicago, September 1992 (preliminary version 2 of the monograph)

[3] L. Babai, H. Snevily, and R. M. Wilson: A new proof for several inequalities on codes and sets, *J. Combinatorial Theory Ser. A*, **71** (1995), 146–153.

[4] L. Babai, P. Frankl, S. Kutin, D. Štefankovič: Set systems with restricted intersections modulo prime powers, manuscript, 1999.

[5] D. A. M. Barrington, R. Beigel, and S. Rudich: Representing Boolean functions as polynomials modulo composite numbers, *Comput. Complexity,* **4** (1994), 367–382. Preliminary version appeared in *Proc. 24th Ann. ACM Symp. Theor. Comput.*, 1992, 455–461.

[6] R. Beigel and J. Tarui: On ACC, *Comput. Complexity*, **4** (1994), 350–366.

[7] P. Erdős: Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.,* **53** (1947), 292–294.

[8] P. Frankl: Constructing finite sets with given intersections, *Ann. Disc. Math.,* **17** (1983), 289–291.

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

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

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

[12] G. Tardos and D. A. M. Barrington: A lower bound on the MOD 6 degree of the OR function, *Comput. Complex.,* **7** (1998), 99–108. Preliminary version appeared in *Proceedings of the Third Israel Symosium on the Theory of Computing and Systems (ISTCS'95)*, 1995, 52–56.

Vince Grolmusz

Department of Computer Science,
Eötvös University, Budapest,
H-1088 Budapest, Hungary
grolmusz@cs.elte.hu