*Combinatorics, Probability and Computing* (2002) 11, 475–486. © 2002 Cambridge University Press
DOI: 10.1017/S0963548302005242 Printed in the United Kingdom

# Constructing Large Set Systems with Given Intersection Sizes Modulo Composite Numbers

SAMUEL KUTIN

Center for Communications Research,
805 Bunn Drive, Princeton, NJ 08540, USA
(e-mail: kutin@idaccr.org)

*Received 17 September 2001; revised 15 January 2002*

We consider $k$-uniform set systems over a universe of size $n$ such that the size of each pairwise intersection of sets lies in one of $s$ residue classes mod $q$, but $k$ does not lie in any of these $s$ classes. A celebrated theorem of Frankl and Wilson [8] states that any such set system has size at most $\binom{n}{s}$ when $q$ is prime. In a remarkable recent paper, Grolmusz [9] constructed set systems of superpolynomial size $\Omega(\exp(c \log^2 n / \log\log n))$ when $q = 6$. We give a new, simpler construction achieving a slightly improved bound. Our construction combines a technique of Frankl [6] of 'applying polynomials to set systems' with Grolmusz's idea of employing polynomials introduced by Barrington, Beigel and Rudich [5]. We also extend Frankl's original argument to arbitrary prime-power moduli: for any $\epsilon > 0$, we construct systems of size $n^{s+g(s)}$, where $g(s) = \Omega(s^{1-\epsilon})$. Our work overlaps with a very recent technical report by Grolmusz [10].

## 1. Introduction

We consider extremal set systems with restricted intersection sizes modulo composite numbers.

We first introduce some notation, following [4]. Let $q$ be a positive integer. For $L \subset \mathbb{Z}$, we say that '$r \in L \pmod q$' if $r \equiv \ell \pmod q$ for some $\ell \in L$. We say '$r \notin L \pmod q$' if $r \not\equiv \ell \pmod q$ for every $\ell \in L$.

Let $X$ be a universe, $|X| = n$. A *set system* $\mathscr{F}$ over $X$ is a set of subsets of $X$. We let $\binom{X}{k}$ denote the set system containing all subsets of $X$ of size $k$.

**Definition 1.** The set system $\mathscr{F}$ is *$L$-avoiding* mod $q$ if, for all $E \in \mathscr{F}$, $|E| \notin L \pmod q$.

**Definition 2.** The set system $\mathscr{F}$ is *$L$-intersecting* mod $q$ if, for all $E, F \in \mathscr{F}$, $E \neq F$, $|E \cap F| \in L \pmod q$.

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

**Definition 3.** Let $m(n, s, q)$ denote the maximal size of a set system over a universe of size $n$ which is $L$-avoiding mod $q$ and $L$-intersecting mod $q$ for some $L$ with $|L| = s$.

Following the seminal paper by Frankl and Wilson [8], it was shown by Alon, Babai and Suzuki [2] that $m(n, s, q) = O(n^s)$ if $q$ is prime. This has subsequently been extended [4]: if $q$ is a prime power, then $m(n, s, q) \leqslant n^{f(s)}$, where $f(s) = 2^{s-1}$.

This contrasts with Grolmusz's remarkable result [9]. He showed that, if $q$ is not a prime power, then there is no $f(s)$ for which $m(n, s, q) < n^{f(s)}$.

**Theorem 1.1. (Grolmusz)** *Let $q$ be a composite number with at least $r$ distinct prime factors, $r \geqslant 2$. Then, for infinitely many values of $n$,*

$$m(n, 2^r - 1, q) \geqslant \exp(c_q (\log n)^r / (\log \log n)^{r-1}),$$

*where $c_q$ is a constant depending on $q$.*

Grolmusz observed a connection with polynomials introduced by Barrington, Beigel and Rudich [5]. He used these polynomials to construct certain sets of matrices, which yield large $L$-avoiding and $L$-intersecting set systems.

Our main result is a simpler proof of Theorem 1.1 with an improved constant (see Theorem 1.2). The proof uses a technique of Frankl [6] for applying polynomials to set systems (see Section 2). We observe that Frankl's technique gives a natural context for using the Barrington–Beigel–Rudich (BBR) polynomials. We discuss the BBR polynomials in Section 3, and our proof of Theorem 1.1 appears in Section 4.

**Remark 1.** After Grolmusz published his original proof, but before our work presented in this note, Grolmusz [10, Section 3.3] independently found the same simplified argument. We were unaware of Grolmusz's technical report when this note was originally written. We note that, amusingly, Grolmusz himself seemed unaware of Frankl's 1981 paper, which developed the notion of applying polynomials to set systems [6]. Grolmusz reproduced this concept [10, Section 2.2].

The constant $c_q$ implicit in Grolmusz's paper [9] is $1/(2^r p^r r^{r-1})$, where $r$ is the number of prime divisors of $q$ and $p$ is the largest prime divisor of $q$. Grolmusz's later argument [10] reproduces the same constant.

We remove the dependence on the prime factors of $q$, as follows.

**Theorem 1.2.** *Let $q$ be a composite number with at least $r$ distinct prime factors, $r \geqslant 2$. Then, for any constant $c < r^{-r}$, for infinitely many values of $n$:*

$$m(n, 2^r - 1, q) \geqslant \exp(c (\log n)^r / (\log \log n)^{r-1}).$$

This improvement is due to a Diophantine approximation argument given in Lemma 4.1. The improved constant enables us to match the best-known explicit constructions of multicolour Ramsey graphs (Alon [1] and Grolmusz [9]: see Section 5). We note that

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

Grolmusz's original argument admits the same improvement, via Lemma 4.1, yielding the same constant as above.

In this note, we also apply Frankl's technique to the case of prime-power moduli.

**Definition 4.** Let $f(s)$ denote the smallest exponent such that $m(n,s,q) = O(n^{f(s)})$ for any prime power $q$. More precisely,

$$f(s) = \sup_q \limsup_{n\to\infty} \frac{\log m(n,s,q)}{\log n},$$

where $q$ ranges over all prime powers.

As noted above, it has been shown [4] that $f(s)$ is well defined, and that $f(s) \leqslant 2^{s-1}$.

Frankl and Wilson [8] showed that $|\mathscr{F}| \leqslant \binom{n}{s}$, for any prime power $q$, when $s = q-1$, assuming that $\mathscr{F}$ is uniform.

However, Frankl [6] showed that the $O(n^s)$ bound does not hold for prime power moduli: he gives a construction for $q = p^2$ showing that $f(s) > s + \sqrt{2s}$ for infinitely many values of $s$. Frankl starts with simple set systems, and then applies appropriately chosen polynomials to them to show the lower bound on $f(s)$. In Section 2, we discuss Frankl's technique.

In Section 6, we extend Frankl's argument to arbitrary prime-power moduli. We obtain the following slight improvement over Frankl's bound.

**Theorem 1.3.** *For any $\epsilon > 0$, for infinitely many values of $s$, $f(s) > s + \Omega(s^{1-\epsilon})$.*

In Section 7, we observe, as does Grolmusz [10], that Frankl's technique can be extended to multilinear polynomials. This technique may lead to improved explicit Ramsey bounds.

## 2. Frankl's technique: applying polynomials to set systems

Frankl's constructions of set systems [6] use the following theorem, which we will use in Sections 4 and 6. We give a short proof for completeness.

**Theorem 2.1. (Frankl)** *Let $g(x)$ be a polynomial of the form $g(x) = \sum_{i=0}^{d} b_i \binom{x}{i}$, where the $b_i$ are nonnegative integers. Choose $q \in \mathbb{Z}$, and $L \subset \mathbb{Z}$, and suppose $\mathscr{F}$ is a set system over $X$ which is $L$-intersecting mod $q$. Then there is a set system $\mathscr{G}$ on a universe of size $g(|X|)$, with $|\mathscr{G}| = |\mathscr{F}|$, which is $g(L)$-intersecting mod $q$. If we further have that, for all sets $E \in \mathscr{F}$, $g(|E|) \notin g(L) \pmod q$, then $\mathscr{G}$ is also $g(L)$-avoiding mod $q$.*

**Proof.** Our universe $Y$ is constructed as a disjoint union: $Y = \bigcup_{i=0}^{d} \bigcup_{j=1}^{b_i} \binom{X}{i}$. Clearly $|Y| = g(|X|)$. There is a natural map $\phi$ taking subsets of $X$ to subsets of $Y$:

$$\phi(E) = \bigcup_{i=0}^{d} \bigcup_{j=1}^{b_i} \binom{E}{i}.$$

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

So, let $\mathscr{G} := \{\phi(E) : E \in \mathscr{F}\}$. For any $E$, $|\phi(E)| = g(|E|)$, and, for any $E, F$, $\phi(E) \cap \phi(F) = \phi(E \cap F)$. It follows that $\mathscr{G}$ is $g(L)$-intersecting mod $q$. If $g(|E|) \notin g(L) \pmod q$ for every $E \in \mathscr{F}$, then $\mathscr{G}$ is also $g(L)$-avoiding mod $q$. □

For the case $q = 6$, Frankl [6] gave an example showing that $m(n, 3, 6) > cn^4$. Even this bound was surprising, which makes Grolmusz's result [9] that $m(n, 3, 6)$ is $\Omega(n^{c \log n / \log\log n})$ even more impressive.

Frankl [6] also gave a construction with $q = p^2$, using the polynomial $(x + 2)^2$. He proved that

$$m(n, s, p^2) > c_p n^{s+\sqrt{2s}},$$

where $s = (p^2 - p)/2$ and $c_p$ is a constant depending only on $p$. This implies that $f(s) \geqslant s + \sqrt{2s}$, where $f(s)$ is the quantity in Definition 4. In Section 6, we extend Frankl's construction to prime-power moduli, proving Theorem 1.3: for any $\epsilon > 0$, $f(s) \geqslant s + \Omega(s^{1-\epsilon})$.

## 3. The Barrington–Beigel–Rudich polynomials

Before we present our construction, we define the BBR polynomials. The following theorem is due to Barrington, Beigel and Rudich [5].

**Theorem 3.1. (BBR)** *Let $p_1, \ldots, p_r$ be $r$ distinct primes, with $r \geqslant 1$. Let $t$ be an integer of the form $t = \prod_j p_j^{e_j}$, and let $q$ be a positive integer divisible by $\prod_j p_j$. Then there exists a polynomial $Q_{q,t}(x)$ such that:*

(1) $Q_{q,t}(x) = \sum b_i \binom{x}{i}$, *where* $0 \leqslant b_i < q$;
(2) $Q_{q,t}(x) \equiv 0 \pmod q$ *if and only if* $x \equiv 0 \pmod t$;
(3) $\deg Q_{q,t} \leqslant \max_j p_j^{e_j}$;
(4) $Q_{q,t}(x)$ *takes only* $2^r$ *values* $\pmod q$.

For completeness, we include a proof.

**Proof.** First, for any $k > 1$, define $g_k(x)$ by

$$g_k(x) = \sum_{i=1}^{k-1} (-1)^{i+1} \binom{x}{i}.$$

We make the following observations (proved in [5]):

- $g_k(0) = 0$;
- $g_k(\ell) = 1$ for any $0 < \ell < k$;
- for any prime $p$, if $p^e \geqslant k$, then, for all $x$,

$$g^k(x + p^e) \equiv g^k(x) \pmod p.$$

Let $P_j(x) = g_{p_j^{e_j}}(x)$. Then $P_j(x) \equiv 0$ or $1 \pmod{p_j}$, and $P_j(x) \equiv 0$ if and only if $p_j^{e_j} \mid x$. Note that $\deg P_j(x) < p_j^{e_j}$.

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

Now, write $P_j(x) = \sum_i a_{ji}\binom{x}{i}$, and let $z$ denote $\prod_j p_j$. Using the Chinese Remainder Theorem, we find coefficients $c_i$ such that, for all $j$, $c_i \equiv a_{ji} \pmod{p_j}$, and such that $0 \leqslant c_i < z$. Let $R(x) = \sum c_i\binom{x}{i}$. Then $R(x) \equiv 0 \pmod{z}$ if and only if $\prod p_i^{e_i} \mid x$. Since each $P_j(x)$ can take only two values mod $p_j$, $R(x)$ takes only $2^r$ values mod $z$. Note that $\deg R(x) < \max_j p_j^{e_j}$.

Finally, let $Q_{q,t}(x) = (q/z)R(x)$. Then $Q_{q,t}$ satisfies the desired conditions. □

**Remark 2.** Barrington, Beigel and Rudich [5] show that the BBR polynomials are the polynomials of lowest-possible degree satisfying conditions (1) and (2) of Theorem 3.1.

**Remark 3.** Barrington, Beigel and Rudich [5] actually construct symmetric multilinear polynomials in $n$ variables, $x_1, \ldots, x_n$, which represent the OR function (mod $q$). Since these polynomials are symmetric, they can be rewritten in terms of $x = \sum_i x_i$, yielding the polynomials of Theorem 3.1.

## 4. Non-prime-power moduli

We now restate our improved version of Grolmusz's Theorem 1.1 [9].

**Theorem 1.2.** *Let $q$ be a composite number with at least $r$ distinct prime factors, $r \geqslant 2$. Then, for any constant $c < r^{-r}$, for infinitely many values of $n$:*

$$m(n, 2^r - 1, q) \geqslant \exp(c(\log n)^r/(\log\log n)^{r-1}).$$

**Remark 4.** The bound above, with $c$ any constant less than $r^{-r}$, holds for infinitely many values of $n$. As Grolmusz showed [9, 10], there is a constant $C_q$ for which the inequality

$$m(n, 2^r - 1, q) \geqslant \exp(C_q(\log n)^r/(\log\log n)^{r-1})$$

holds for all $n$. The constant implicit in Grolmusz's work is $C_q = 1/(2^r p^{2r} r^{r-1})$, where $r$ is the number of prime divisors of $q$, and $p$ is the largest prime divisor of $q$. Our (simpler) proof reproduces that result as well.

Grolmusz proves Theorem 1.1 constructively. He starts with a BBR polynomial $Q(x)$, as discussed in Section 3. A matrix $A$ is constructed from $Q(x)$. We write $A = \sum B_i$, where the matrices $B_i$ correspond to the monomials which contribute to $Q(x)$, and each $B_i$ is a block-diagonal matrix. Grolmusz constructs the points of the universe from the blocks of these $B_i$ matrices, and the sets in the set system correspond to diagonal entries of $A$.

We give an alternate (and also constructive) proof of Grolmusz's theorem. We use the same BBR polynomials, but we use Frankl's technique (Theorem 2.1) for the construction. As we mentioned in the Introduction, this approach was also used by Grolmusz [10].

We need the following lemma, which allows us to choose a parameter $t$.

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

**Lemma 4.1.** *Let $p_1, \ldots, p_r$ be $r$ distinct primes, $r \geqslant 2$. Then, for any $\epsilon > 0$, there exist infinitely many integers $t$ such that:*

- $t = \prod_j p_j^{e_j}$ *for some* $e_1, \ldots, e_r$;
- *for all* $j$, $p_j^{e_j} \leqslant (1+\epsilon)t^{1/r}$.

**Proof.** Without loss of generality, we assume $p_r = \max_j p_j$. For $1 \leqslant j \leqslant r-1$, let $\alpha_j = \frac{\log p_r}{\log p_j}$. By Dirichlet's theorem, the system of inequalities

$$\left| \frac{e_j}{b} - \alpha_j \right| < b^{-(1+\frac{1}{r-1})}$$

for $1 \leqslant j \leqslant r-1$ has infinitely many solutions. (See, for example, [12, p. 170].)

For each $j < r$, we then have

$$|e_j \log p_j - b \log p_r| < b^{-\frac{1}{r-1}} \log p_j$$
$$\left| \log \frac{p_j^{e_j}}{p_r^b} \right| < b^{-\frac{1}{r-1}} \log p_r \tag{4.1}$$

Write $e_r = b$, and let $t = \prod_j p_j^{e_j}$. Then, summing (4.1) over all $j$ and dividing by $r$,

$$\left| \log \frac{t^{1/r}}{p_r^{e_r}} \right| < b^{-\frac{1}{r-1}} \log p_r.$$

So, for sufficiently large $b$, condition (2) of the lemma is satisfied for $j = r$, and, by (4.1), for $j < r$ as well. □

We are now ready to prove Theorem 1.2.

**Proof of Theorem 1.2.** Let $p_1, \ldots, p_r$ be $r$ distinct primes dividing $q$. We begin by fixing some $\epsilon > 0$, and then choosing a number $t$ satisfying the conditions of Lemma 4.1. Let $d = \deg Q_{q,t}$; note that $d \leqslant (1+\epsilon)t^{1/r}$.

Let $X$ be a universe of size $t^a$, where $a > 1$ is a constant to be chosen later. Let $\mathscr{F} = \binom{X}{t-1}$. Then $|\mathscr{F}| = \binom{t^a}{t-1} \geqslant (t^a/(t-1))^{t-1} \geqslant t^{(a-1)(t-1)}$. Note that $\mathscr{F}$ is $L$-avoiding and $L$-intersecting for $L = \{0, \ldots, t-2\}$.

We apply Theorem 2.1 with the polynomial $g(x) = Q_{q,t}(x+1)$. Then, by construction, $g(L) = Q_{q,t}(\{1, \ldots, t-1\})$ lies in $2^r - 1$ residue classes (mod $q$). Also, for all $E \in \mathscr{F}$,

$$g(|E|) = Q_{q,t}(t) \equiv 0 \pmod{q}.$$

Since $0 \notin g(L) \pmod{q}$, we have constructed a set system $\mathscr{G}$, with $|\mathscr{G}| = |\mathscr{F}|$, which is $g(L)$-intersecting and $g(L)$-avoiding (mod $q$). The system $\mathscr{G}$ is over a universe $Y$ of size

$$g(|X|) = Q_{q,t}(t^a+1) \leqslant (q-1)\sum_{i=0}^{d} \binom{t^a+1}{i} < (q-1)\left(\frac{\mathrm{e}(t^a+1)}{d}\right)^d.$$

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

Putting all this together, we have

$$\log|\mathscr{G}| \geqslant (a-1)(t-1)\log t \sim (a-1)t\log t, \tag{4.2}$$

$$\log|Y| \leqslant (1+\epsilon)t^{1/r}\left(\log(t^a+1)+\log\frac{\mathrm{e}}{1+\epsilon}-\log t^{1/r}\right)+\log(q-1)$$

$$\sim (1+\epsilon)(ar-1)t^{1/r}\log t^{1/r}. \tag{4.3}$$

Solving (4.3) for $t^{1/r}$, we get that

$$t^{1/r} \gtrsim \frac{\log|Y|}{(ar-1)(1+\epsilon)\log\log|Y|}$$

and hence, by (4.2),

$$\log|\mathscr{G}| \gtrsim c_r\frac{(\log|Y|)^r}{(\log\log|Y|)^{r-1}},$$

for the constant $c_r = r(a-1)((ar-1)(1+\epsilon))^{-r}$.

The function $\frac{a-1}{(ar-1)^r}$ is maximized when $a = 1+1/r$. This gives $c_r = r^{-r}(1+\epsilon)^{-r}$, proving the theorem. □

## 5. Explicit Ramsey graphs

Alon [1, Proposition 4.2] and Grolmusz [9, Theorem 6.7] have each shown the following.

**Theorem 5.1. (Alon, Grolmusz)** *For any $r \geqslant 2$ and $c < r^{-r}$, and for infinitely many values of $n$, there exists an explicitly constructible $r$-colouring of the edges of the complete graph of size $N$ that contains no monochromatic cliques of size $n$, where*

$$N = \exp\left(c\frac{(\log n)^r}{(\log\log n)^{r-1}}\right).$$ □

Grolmusz [9, Section 4] uses Theorem 1.1 to give an explicit construction of multicolour Ramsey graphs as in Theorem 5.1. However, the constant $c$ obtained from this construction is only $1/(2^r p_r^r r^{r-1})$, where $p_r$ is the $r$th prime. We observe that Theorem 1.2, together with Grolmusz's earlier work, gives a new construction achieving the bound in Theorem 5.1. This is currently the best-known construction of multicolour Ramsey graphs.

## 6. Prime-power moduli

We now extend Frankl's construction to $q = p^k$, $k \geqslant 2$.

**Theorem 6.1.** *For any odd prime $p$, and any $k \geqslant 2$,*

$$m(n, s, p^k) > n^{s+\Omega(s^{1-1/k})}$$

*for $s = (p^k - p^{k-1})/2 + p^{k-2}$.*

In terms of $f(s)$ from Definition 4, we get the following corollary, stated as Theorem 1.3.

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

**Corollary 6.2.** *For any $\epsilon > 0$, and for infinitely many values of $s$,*

$$f(s) > s + \Omega(s^{1-\epsilon}).$$ □

**Proof of Theorem 6.1.** Fix some $n$, some odd prime $p$, and some $q = p^k$. Let $X$ be a universe of $n$ points, and let $\mathscr{F} = \binom{X}{q-3}$. Then $\mathscr{F}$ is $L$-avoiding mod $q$ and $L$-intersecting mod $q$ for $L = \{0, \ldots, q-4\}$. Following Frankl [6], let $g(x) = (x+2)^2 = 4 + 5x + 2\binom{x}{2}$. We construct $\mathscr{G}$ as in Theorem 2.1. By the theorem, $\mathscr{G}$ is $g(L)$-intersecting. We also note that, for any $E \in \mathscr{F}$, $g(|E|) = (p^k - 1)^2 \equiv 1 \pmod q$, and that $1 \notin g(L) \pmod q$. Hence, $\mathscr{G}$ is also $g(L)$-avoiding mod $q$. It remains to compute the size of a minimum set $K$ such that $\ell \in g(L) \pmod q$ if and only if $\ell \in K \pmod q$; equivalently, we want to compute how many congruence classes mod $q$ are represented in $g(L)$.

If $p \nmid \ell$, then $\ell^2$ is a quadratic residue mod $p$; thus $g(L)$ contains at most $(p^k - p^{k-1})/2$ classes relatively prime to $p$. If $p \mid \ell$, then $p^2 \mid \ell^2$, so $g(L)$ contains at most $p^{k-2}$ classes not relatively prime to $p$. We conclude that

$$s := |g(L)| \leqslant \frac{p^k - p^{k-1}}{2} + p^{k-2}.$$

Also,

$$|\mathscr{G}| = \binom{|X|}{q-3} = \Omega(|X|^{q-3}) = \Omega(|Y|^{(q-3)/2}).$$

Finally, we compute this exponent, $(q-3)/2$, in terms of $s$:

$$\frac{q-3}{2} \leqslant s + \frac{p^{k-1}}{2} - p^{k-2} - \frac{3}{2} = s + \frac{2s^{1-1/k}}{2} + o(s^{1-1/k}) = s + \Omega(s^{1-1/k}).$$ □

## 7. Multilinear polynomials

In Section 2, we discussed Frankl's technique of applying a polynomial to a set system. In this section, we state a natural extension of this approach to multilinear polynomials. This extension is also discussed in Grolmusz's technical report [10] (see Remark 1).

We first introduce some notation. Let $X$ be a universe of size $n$; we identify the points of $X$ with $\{1, \ldots, n\}$. If $g(x_1, \ldots, x_n)$ is a multilinear polynomial in $n$ variables, we write $g(x_1, \ldots, x_n) = \sum_S \alpha_S x_S$, where $S$ ranges over all subsets of $X$ and $x_S = \prod_{i \in S} x_i$. For any $E \subseteq X$, we can then write $g(E) = \sum_{S \subseteq E} \alpha_E x_E$. Alternatively, we can identify $E$ with the $n$-tuple $(y_1, \ldots, y_n)$, where $y_i = 1$ when $i \in E$ and $y_i = 0$ when $i \notin E$; then $g(E) = g(y_1, \ldots, y_n)$.

**Theorem 7.1.** *Let $g(x_1, \ldots, x_n)$ be a multilinear polynomial in $n$ variables with nonnegative integer coefficients. Let $X$ be a universe of size $n$, and let $\mathscr{F}$ be a set system over $X$. Let $K := \{g(E \cap F) : E, F \in \mathscr{F} \text{ and } E \neq F\}$. Then there is a set system $\mathscr{G}$ on a universe of size $g(X)$, with $|\mathscr{G}| = |\mathscr{F}|$, which is $K$-intersecting mod $q$. If we further have that, for all sets $E \in \mathscr{F}$, $g(E) \notin K \pmod q$, then $\mathscr{G}$ is also $K$-avoiding mod $q$.*

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

**Proof.** Our universe $Y$ is constructed as a disjoint union: $Y = \bigcup_{S \subseteq X} Z_S$, where $Z_S$ is a set of size $\alpha_S$. Clearly $|Y| = g(X)$. There is a natural map $\phi$ taking subsets of $X$ to subsets of $Y$:

$$\phi(E) = \bigcup_{S \subseteq E} Z_E.$$

So, let $\mathscr{G} := \{\phi(E) : E \in \mathscr{F}\}$. For any $E$, $|\phi(E)| = g(E)$, and, for any $E$, $F$, $\phi(E) \cap \phi(F) = \phi(E \cap F)$. The result follows. □

**Note.** If $g(x_1, \ldots, x_n)$ is a symmetric multilinear polynomial in $n$ variables, then we can write $g(x_1, \ldots, x_n) = \sum b_i s_i$, where $s_i$ is the degree-$i$ elementary symmetric polynomial. This is in turn equal to $h(x) = \sum b_i \binom{x}{i}$, where $x = \sum_j x_j$. So Theorem 2.1 can be viewed as a special case of Theorem 7.1 when $g$ is symmetric.

Barrington, Beigel and Rudich [5] prove that the polynomials they construct have minimal degree among symmetric polynomials that compute the OR function mod $q$. However, they observe that, in certain cases, nonsymmetric polynomials may have lower degree. (For example, G. Tardos and Barrington [16] observe that any symmetric polynomial computing the OR function mod 6 on 9 variables must have degree 3, but there is a nonsymmetric quadratic polynomial which computes OR mod 6 on 10 variables.)

Theorem 7.1 indicates that, if we could demonstrate the existence of nonsymmetric polynomials of lower degree which compute OR mod 6, we could use these polynomials to increase the lower bound on $m(n, 5, 6)$. Grolmusz [9] observed a striking connection between $L$-intersecting and $L$-avoiding set systems modulo non-prime-powers and Ramsey graphs (*cf.* Section 5). A construction of lower-degree polynomials computing OR mod 6 might thus improve the best-known Ramsey constructions (see Section 9). Grolmusz has also given explicit constructions of Ramsey hypergraphs using similar techniques [11].

The best-known lower bound on the degree of a polynomial in $n$ variables computing OR mod $q$, where $q$ has $r \geqslant 2$ prime divisors, is $\Omega((\log n)^{1/(r-1)})$. This is due to Tardos and Barrington [16].

## 8. An upper bound on $m(n, s, q)$

The trivial upper bound on $m(n, s, q)$ is $2^n$. This has been improved to roughly $2^{n/2}$ by Jiří Sgall [14] (see Corollary 8.2 below). We include his unpublished argument below, with permission.

The proof rests on the following theorem of Sgall [13], which holds for all moduli $q$.

**Theorem 8.1. (Sgall)** *Let $\mathscr{A}$, $\mathscr{B}$ be set systems over a universe $X$ of size $n$. Suppose that, for any $A \in \mathscr{A}$, $B \in \mathscr{B}$, $|A \cap B| \in L \pmod q$, where $|L| = s < q$. Then $|\mathscr{A}| \cdot |\mathscr{B}| \leqslant \binom{n}{s-1} 2^{n+s-1}$.* □

Sgall [14] observed that this theorem can be applied to the case of a single $L$-intersecting family modulo $q$.

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

**Corollary 8.2. (Sgall)** *For any $q$, $m(n,s,q) \leqslant c_s n^{(s-1)/2} 2^{n/2}$, where $c_s$ is a constant depending only on $s$.*

**Proof.** (From Sgall [14].) Let $\mathscr{F}$ be a set system over $X$ which is $L$-avoiding and $L$-intersecting mod $q$ for some set $L$ of size $s$. If we divide $\mathscr{F}$ into two equal parts $\mathscr{A}$ and $\mathscr{B}$, then these systems satisfy the requirements of Theorem 8.1. We conclude that $|\mathscr{F}|^2/4 \leqslant \binom{n}{s-1} 2^{n+s-1}$, proving the result. □

Sgall [14] also noted that the upper bound in Corollary 8.2 does not require the assumption that the set system be $L$-avoiding. There exist large $L$-intersecting set systems (for example, the system of sets $F$ where $2i \in F$ if and only if $2i-1 \in F$). So the bound cannot be substantially improved without using the $L$-avoiding property.

## 9. Open questions

There are several open questions regarding the quantities we have discussed.

### 9.1. Non-prime-power moduli

Recall (Definition 3) that $m(n,s,q)$ denotes the maximal size of a set system over a universe of size $n$ such that each pairwise intersection of sets lies in one of $s$ residue classes mod $q$, but the set sizes do not lie in any of these $s$ classes.

By Theorem 1.2, and by Theorem 8.1 (Sgall [14]), we have, for any $q$ with at least 2 prime divisors,

$$\exp(c \log^2 n / \log\log n) \leqslant m(n,3,q) \leqslant O(n 2^{n/2}), \tag{9.1}$$

where $c$ can be any constant less than $1/4$.

**Question 9.1.** *Can we narrow the gap in* (9.1)*? Can we prove an upper bound of the form $C(2-\epsilon)^{n/2}$ for some constant $C$ and some $\epsilon > 0$?*

**Question 9.2.** *Can we give a construction increasing the lower bound on $m(n,3,6)$ in* (9.1)*?*

Grolmusz [9] observed that there is a graph on $m(n,3,6)$ vertices which does not contain either a complete graph or an independent set of size $n$. The best-known explicit construction of such a Ramsey graph [8, 1, 9] has size $\exp\big(\big(\frac{1}{4} - o(1)\big)\log^2 n / \log\log n\big)$. So a construction of set systems larger than this would improve the best-known explicit constructions of Ramsey graphs.

**Question 9.3.** *Our construction in Section 4 uses the Barrington–Beigel–Rudich polynomials. Are there polynomials for which Frankl's technique yields larger set systems?*

**Question 9.4. ([5])** *Do there exist multilinear polynomials computing the OR function of $n$ variables modulo $q$ which have degree $o(n^{1/r})$, where $r$ is the number of prime divisors of $q$?*

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

Such polynomials would necessarily be nonsymmetric, by an argument of Barrington, Beigel and Rudich [5, Theorem 2.2].

As Grolmusz proved (*cf.* Section 7 of this paper), we could use such polynomials to improve the lower bound on $m(n, s, q)$. An explicit construction of such polynomials would yield an explicit construction of larger set systems. Such a construction would improve the best-known explicit constructions of Ramsey graphs (*cf.* Section 5 and Question 9.2).

### 9.2. Bounds on $m(n, 2, 6)$

It follows from Babai and Frankl [3] that, if $|L| = 1$, any $k$-uniform set system which is $L$-avoiding and $L$-intersecting mod $q$ has size at most $n$ when $0 \in L \pmod q$, and size at most $n + 1$ for any $L$. Frankl and Rosenberg [7] improve this bound to $n$ for any $L$.

From these statements, it is straightforward to show that $m(n, 1, q) \leqslant rn$, where $r$ is the number of distinct prime divisors of $q$. Szegedy [15] has shown that $m(n, 1, 6) \leqslant 2n - \log_2 n$.

From Theorem 1.1 by Grolmusz [9], we have

$$m(n, 3, 6) = \exp(\Omega(\log^2 n / \log\log n)).$$

The best-known upper and lower bounds on $m(n, 2, 6)$ are

$$\binom{n}{2} \leqslant m(n, 2, 6) \leqslant n^{1/2} 2^{(n+3)/2}$$

where the upper bound is due to Corollary 8.2 by Sgall [14].

**Question 9.5.** *What can we say about $m(n, 2, 6)$? Can we narrow the gap between the upper and lower bounds? Can we prove a polynomial upper bound, as we can for $m(n, 1, 6)$? Or can we prove a superpolynomial lower bound, as we can for $m(n, 3, 6)$?*

### 9.3. Prime-power moduli

Recall (Definition 4) that $f(s)$ denotes the smallest exponent such that $m(n, s, q) = O(n^{f(s)})$ for any prime power $q$. More precisely,

$$f(s) = \sup_q \limsup_{n\to\infty} \frac{\log m(n, s, q)}{\log n},$$

where $q$ ranges over all prime powers.

It has been shown [4] that $f(s) \leqslant 2^{s-1}$. Combining this statement with Corollary 6.2, we have

$$s + \Omega(s^{1-\epsilon}) \leqslant f(s) \leqslant 2^{s-1}.$$

**Question 9.6.** *Can we narrow the gap between the upper and lower bounds on $f(s)$? In particular, does there exist some $\epsilon > 0$ such that, for infinitely many values of $s$, $f(s) > (1 + \epsilon)s$?*

**Conjecture 9.7.** *For any prime power $q$, the limit*

$$\lim_{n\to\infty} \frac{\log m(n, s, q)}{\log n}$$

*exists.*

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press

**Acknowledgements**

I would like to thank László Babai for introducing me to this area and for many helpful comments on this paper. Thanks also to Vince Grolmusz, Jiří Sgall and Daniel Štefankovič for helpful discussions.

## References

[1] Alon, N. (1998) The Shannon capacity of a union. *Combinatorica* **18** 301–310.
[2] Alon, N., Babai, L. and Suzuki, H. (1991) Multilinear polynomials and Frankl–Ray–Chaudhuri–Wilson-type intersection theorems. *J. Combin. Theory Ser. A* **58** 165–180.
[3] Babai, L., and Frankl, P. (1980) On set intersections. *J. Combin. Theory Ser. A* **28** 103–105.
[4] Babai, L., Frankl, P., Kutin, S. and Štefankovič, D. (2001) Set systems with restricted intersections modulo prime powers. *J. Combin. Theory Ser. A* **95** 39–73.
[5] Barrington, D. A. M., Beigel, R. and Rudich, S. (1994) Representing boolean functions as polynomials modulo composite numbers. *Comput. Complexity* **4** 367–382.
[6] Frankl, P. (1983) Constructing finite sets with given intersections, in *Combinatorial Mathematics* (Marseille-Luminy, 1981), North-Holland, Amsterdam, pp. 289–291. *Ann. Disc. Math.* **17**.
[7] Frankl, P. and Rosenberg, I. G. (1981) A finite set intersection theorem. *Europ. J. Combin.* **2** 127–129.
[8] Frankl, P. and Wilson, R. M. (1981) Intersection theorems with geometric consequences. *Combinatorica* **1** 357–368.
[9] Grolmusz, V. (2000) Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica* **20** 71–86.
[10] Grolmusz, V. (2001) Constructing set-systems with prescribed intersection sizes. Technical report 2001-03, DIMACS.
[11] Grolmusz, V. (2001) Set-systems with restricted multiple intersections and explicit Ramsey hypergraphs. Technical report 2001-04, DIMACS.
[12] Hardy, G. H. and Wright, E. M. (1979) *An Introduction to the Theory of Numbers*, 5th edn, Oxford.
[13] Sgall, J. (1999) Bounds on pairs of families with restricted intersections. *Combinatorica* **19** 555–566.
[14] Sgall, J. (2000) Personal communication.
[15] Szegedy, M. Exercise 2.3.12 in [3].
[16] Tardos, G. and Barrington, D. A. M. (1998) A lower bound on the mod 6 degree of the OR function. *Comput. Complexity* **7** 99–108.

https://doi.org/10.1017/S0963548302005242 Published online by Cambridge University Press