Constructing Ramsey Graphs from Boolean Function Representations

Parikshit Gopalan[*]
College of Computing,
Georgia Institute of Technology,
Atlanta, GA 30332, USA.
parik@cc.gatech.edu

May 1, 2006

Abstract

Explicit construction of Ramsey graphs or graphs with no large clique or independent set, has remained a challenging open problem for a long time. While Erdős' probabilistic argument shows the existence of graphs on 2^n vertices with no clique or independent set of size $2n$, the best explicit constructions achieve a far weaker bound. Constructing Ramsey graphs is closely related to polynomial representations of Boolean functions; a low degree representation for the OR function can be used to explicitly construct Ramsey graphs [17].

We generalize the above relation by proposing a new framework. We propose a new definition of OR representations: a pair of polynomials represent the OR function if the union of their zero sets contains all points in $\{0,1\}^n$ except the origin. We give a simple construction of a Ramsey graph using such polynomials. Furthermore, we show that all the known algebraic constructions, ones to due to Frankl-Wilson [12], Grolmusz [17] and Alon [2] are captured by this framework; they can all be derived from various OR representations of degree $O(\sqrt{n})$ based on symmetric polynomials.

Thus the barrier to better Ramsey constructions through such algebraic methods appears to be the construction of lower degree representations. Using new algebraic techniques, we show that better bounds cannot be obtained using symmetric polynomials.

[*]Supported by NSF grant CCR-3606B64

1 Introduction

This paper studies a problem at the intersection of combinatorics and computational complexity.

The combinatorial problem is that of explicitly constructing Ramsey graphs. Ramsey's theorem shows that every graph on 2^n vertices has either a clique or an independent set of size $n/2$. In his seminal 1947 paper introducing the probabilistic method, Erdős showed that there exist graphs with 2^n vertices where $\alpha(G), \omega(G) \leq (2 + o(1))n$ [11]. He posed the question of constructing such *Ramsey graphs* explicitly and offered a prize of \$100 for it. This is a central open problem in explicit combinatorial constructions; the best known constructions to date are far from the probabilistic bound. The first breakthrough on this problem was due to Frankl and Wilson in 1981 [12]; their construction gives $\alpha(G), \omega(G) \leq c^{\sqrt{n \log n}}$. For over two decades, there was no improvement on this bound despite much effort. However there were other constructions known due to Grolmusz and Alon [17, 2] that achieved exactly the same bound, and also extended to the problem of constructing multi-color Ramsey graphs, which is to t-color the edges of the complete graph so that there is not large monochromatic clique. At first sight, the construction of Grolmusz is quite different from that of Alon and Frankl-Wilson, yet it gives exactly the same bound. All three constructions use algebraic techniques, though in different ways. Very recently in 2006, the Frankl-Wilson bound was beaten by a new construction due to Barak, Rao, Shaltiel and Wigderson [8] which relies on machinery from pseudorandomness.

The complexity problem is to prove tight degree bounds for polynomials computing Boolean functions over $\mathbb{Z}_m$. A central open problem in circuit complexity is to show lower bounds for ACC, the class of circuits with And, Or and Mod gates. As a first step towards this goal, Barrington, Beigel and Rudich (BBR) studied polynomial representations of Boolean functions modulo composites [9]. They found surprisingly that such representations are much more powerful over $\mathbb{Z}_6$ than over $\mathbb{Z}_p$ when p is prime. They showed that the OR function can be represented by symmetric polynomials of degree $O(\sqrt{n})$ over $\mathbb{Z}_6$. In contrast an $\Omega(n)$ lower bound is known for the degree of such polynomials over $\mathbb{Z}_p$. BBR proved a matching $\Omega(\sqrt{n})$ lower bound for symmetric polynomials representing the OR function over $\mathbb{Z}_6$, and asked if better representations exist using asymmetric polynomials. Tardos and Barrington proved a lower bound of $\Omega(\log n)$ [22]. This is the best lower bound known for any function, despite much effort [16, 23, 15, 3, 10]. The main open question in this area is whether asymmetric polynomials can give lower degree representations of symmetric functions than symmetric polynomials.

A surprising connection between these two problems was discovered by Grolmusz, who used the OR polynomials of BBR to construct Ramsey graphs [17, 18]. As an intermediate step, he constructed a set system of size $n^{\omega(1)}$ on n elements where all set sizes are 0 mod 6 but all intersections are non-zero mod 6, settling an open problem in extremal set theory. He constructed Ramsey graphs from this set system and showed that lower degree OR representations mod 6 would give better Ramsey graphs.

1.1 Our Results

Our work generalizes and extends the connection between OR polynomials and Ramsey graphs. We propose a new definition of an OR representation: *a pair of polynomials represent the OR function on n variables if the union of their zero sets contains all points in $\{0,1\}^n$ except the origin.* We give a simple construction of a Ramsey graph from such representations. This viewpoint based on OR polynomials unifies the constructions of Frankl-Wilson, Alon and Grolmusz: they can all be derived from various OR representations of degree $O(\sqrt{n})$ based on symmetric polynomials. Thus the barrier to better Ramsey constructions through algebraic techniques appears to be the construction of lower degree representations. On one hand, since the best lower bound for any of these representations is only $\Omega(\log n)$ there is the possibility of better constructions. On the other hand, we show that further improvements cannot come from representations using symmetric polynomials; we prove an $\Omega(\sqrt{n})$ lower bound for such representations.

1.1.1 Ramsey Graphs from OR Representations:

Let $\mathbf{X} = (X_1, \cdots, X_n)$ denote a vector of variables and $\mathbf{x} = (x_1, \cdots, x_n)$ denote a Boolean vector. The following definition of Boolean function representation modulo m was introduced by BBR [9].

Definition 1 *Polynomial $P(\mathbf{X}) \in \mathbb{Z}_m[\mathbf{X}]$ weakly represents the function f mod m if for $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$, if $f(\mathbf{x}) \neq f(\mathbf{y})$ then $P(\mathbf{x}) \not\equiv P(\mathbf{y}) \bmod m$.*

We propose the following definition of an OR representation.

Definition 2 *Polynomials $P(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ and $Q(\mathbf{X}) \in \mathbb{Z}_q[\mathbf{X}]$ represent the OR function on n variables if*

$$P(0, \cdots, 0) \equiv 1 \bmod p \ \textit{ and } \ Q(0, \cdots, 0) \equiv 1 \bmod q$$

and for $\mathbf{x} \in \{0,1\}^n \setminus (0, \cdots, 0)$

$$P(\mathbf{x}) \equiv 0 \bmod p \ \textit{ or } \ Q(\mathbf{x}) \equiv 0 \bmod q$$

where p, q are primes. The degree of the representation is $d = \max(\deg(P), \deg(Q))$.

One can combine the two polynomials using the Chinese Remainder Theorem (CRT) to get a single polynomial that weakly represents OR mod pq. However the specific choice of values output by the weak representation is important for our application. The construction of BBR gives a degree $O(\sqrt{n})$ OR representation using polynomials over $\mathbb{Z}_2$ and $\mathbb{Z}_3$. A simple representation of degree $O(\sqrt{n})$ with $n = pq - 1$ using polynomials over $\mathbb{Z}_p$ and $\mathbb{Z}_q$ can be derived from Alon's construction. This highlights another difference about our definition and weak representations: for Ramsey constructions, we are not restricted to any fixed moduli p and q, we are free to choose them in any way, (possibly as functions of n) so that the degree is minimized as a function of n.

We give a simple Ramsey construction based on OR representations: the vertex set is $\{0,1\}^n$ and we add edge $(\mathbf{x}, \mathbf{y})$ to G if $\mathbf{x} \oplus \mathbf{y}$ is in the zero set of $P(\mathbf{X})$, where $\mathbf{x} \oplus \mathbf{y}$ denotes the symmetric difference of $\mathbf{x}$ and $\mathbf{y}$. In order to bound $\alpha(G)$ and $\omega(G)$, we use the notion of representations of graphs over spaces of polynomials introduced by Alon [2]. The idea is to assign polynomials to the vertices of G so that the polynomials assigned to vertices in a clique are linearly independent.

Definition 3 *Let $G(V, E)$ be a graph and $\mathcal{F}$ be a set polynomials in n variables over field $\mathbb{F}$. A polynomial representation of G over $\mathbb{F}$ is an assignment of a polynomial $P_v(\mathbf{X}) \in \mathcal{F}$ and a point $\mathbf{x}_v \in \mathbb{F}^n$ to $v \in V$ where:*
1) *For each $v \in V$, $P_v(\mathbf{x}_v) \neq 0$.*
2) *If $(u, v) \in E$ then $P_v(\mathbf{x}_u) = 0$.*

It is easy to see that $\omega(G) \leq dim(\mathcal{F})$ which is the dimension of the $\mathbb{F}$ vector space spanned by polynomials in $\mathcal{F}$. We use the polynomial $P(\mathbf{X})$ to construct a representation of G over $\mathbb{Z}_p$ and $Q(\mathbf{X})$ to construct a representation of $\overline{G}$ over $\mathbb{Z}_q$. The Frankl-Wilson construction can also be viewed in this framework, where we represent G over $\mathbb{Z}_p$ and $\overline{G}$ over $\mathbb{Q}$. However, quoting Alon *'It seems that this construction does not extend to the case of more than 2 colors'* [2]. We propose a definition of OR representation which leads to such an extension.

Definition 4 *Polynomials $P(\mathbf{X}) \in \mathbb{Z}_{p^a}[\mathbf{X}]$ and $Q(\mathbf{X}) \in \mathbb{Z}_{p^b}[\mathbf{X}]$ represent the OR function on n variables if*

$$P(0, \cdots, 0) \not\equiv 0 \bmod p^a \ \textit{ and } \ Q(0, \cdots, 0) \not\equiv 0 \bmod p^b$$

and for $\mathbf{x} \in \{0,1\}^n \setminus (0, \cdots, 0)$

$$P(\mathbf{x}) \equiv 0 \bmod p^a \ \textit{ or } \ Q(\mathbf{x}) \equiv 0 \bmod p^b$$

where p is prime and $a, b \geq 1$.The degree of the representation is $d = \max(\deg(P), \deg(Q))$.

To differentiate the representations of Definitions 2 and 4, we refer to them as prime representations and prime-power representations respectively. The Frankl-Wilson construction can be used to show that for $n = p^2 - 1$, there exist OR representations of degree $O(\sqrt{n})$. The interesting feature of this representation is that it does not use the Chinese Remainder Theorem (CRT). The construction of Ramsey graphs from prime-power representations stays the same; the difference is in the analysis. For this, we introduce polynomial representations of G over $\mathbb{Z}_{p^a}$.

Definition 5 *Let $G(V, E)$ be a graph and $\mathcal{F}$ a set of polynomials in n variables over $\mathbb{Z}$. A polynomial representation of G over $\mathbb{Z}_{p^a}$ is an assignment of a polynomial $P_v(\mathbf{X}) \in \mathcal{F}$ and a point $\mathbf{x}_v \in \mathbb{Z}^n$ to $v \in V$ s.t.:*
1) *For each $v \in V$, $P_v(\mathbf{x}_v) \not\equiv 0 \bmod p^a$.*
2) *If $(u, v) \in E$ then $P_v(\mathbf{x}_u) \equiv 0 \bmod p^a$.*

We show that the polynomials assigned to a clique are linearly independent over $\mathbb{Q}$ so $\omega(G)$ is bounded by the dimension of the $\mathbb{Q}$-vector space spanned by $\mathcal{F}$. Like polynomial representations of graphs over $\mathbb{Q}$, representations over $\mathbb{Z}_{p^a}$ assign linearly independent polynomials over $\mathbb{Q}$ to vertices in a clique. A crucial difference is that *representations over $\mathbb{Q}$ tensor, those over $\mathbb{Z}_{p^a}$ do not*. This means that if we have sets of polynomials $\mathcal{F}_1$ and $\mathcal{F}_2$ that represent G_1 and G_2 over $\mathbb{Q}$, then $\mathcal{F}_1 \otimes \mathcal{F}_2$ represents $G_1 \cdot G_2$ over $\mathbb{Q}$ for an appropriate definition of graph product (see [2] for definitions and proofs). This is important for the original application of these representations, which was to bound the Shannon capacity of the graph. However, this property implies that one cannot get low dimensional representations of both G and $\overline{G}$ over $\mathbb{Q}$, since $G \cdot \overline{G}$ always has a large clique. But since $\mathbb{Z}_{p^a}$ has zero divisors, we lose this tensor product property, so we can simultaneously get low dimensional representations of G and $\overline{G}$ over $\mathbb{Z}_{p^a}$.

We could restate this argument from the viewpoint of OR representations. We cannot get low degree prime representations by taking $p = q$ since then $P(\mathbf{X})Q(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ is 0 at every point in $\{0, 1\}^n$ except the origin, and such a polynomial requires degree n. But this argument does not extend to prime-power representations because of zero-divisors.

All the OR representations above achieve a bound of $O(\sqrt{n})$ using symmetric polynomials. Plugging them into the simple construction above gives $\alpha(G), \omega(G) \leq c_1^{\sqrt{n} \log n}$ as opposed to the best bound of $c^{\sqrt{n \log n}}$. However, by massaging the polynomials and working with set intersections as opposed to distances, we can get exactly the constructions of Frankl-Wilson, Grolmusz and Alon. Here are some advantages of our unified view of these constructions:

- It places the constructions of Alon and Frankl-Wilson in the context of OR polynomials, and raises the possibility of getting better constructions from low degree representations. The notions of prime-power representations of graphs and Boolean functions arising from the Frankl-Wilson construction are of independent interest.

- It relates the construction of Grolmusz to those of Frankl-Wilson and Alon, which look very different at first. Our Ramsey graph construction from the OR polynomial of BBR is simple and direct. In fact it takes some work to show that we get the same graph as Grolmusz. Viewing this construction in terms of set intersections, we derive improved bounds for set systems with restricted intersections modulo prime powers.

- In this view, all the constructions naturally extend to multicolor Ramsey graphs. To construct t-color Ramsey graphs, we define OR representations involving t polynomials over $\mathbb{Z}_{q_1}, \cdots, \mathbb{Z}_{q_t}$ where $q_1 \cdots, q_t$ are prime powers. Taking powers of the same prime p extends the Frankl-Wilson construction.

1.1.2 Lower Bounds:

A natural question is to show tight degree bounds for OR representations. A better upper bound would lead to better Ramsey graphs. Lower bounds are interesting from the complexity-theory viewpoint of understanding polynomial representations over composites. For the OR function, we believe Definition 2 is the right one to use, since it seems to eliminate dependence of the degree on the modulus pq. Also it places the problem in the context of understanding the zero-sets of low degree polynomials over $\mathbb{Z}_p$. This question has been studied in various other contexts including low degree testing, zero-testing and derandomization (see Section 6). Prime-power representations are interesting since they do not rely on the CRT. Interestingly, the $\Omega(\log n)$ lower bound [22] also does not use the CRT, so it applies to prime-power representations too. It is possible that proving bounds for prime-power representations is easier than the prime case.

Degree lower bounds extend a line of work in combinatorics aimed at understanding why explicit Ramsey graphs are hard to construct, by showing limitations to various natural techniques. A conjecture of Babai states that one cannot construct good Ramsey graphs based on the sign of a set of real polynomials. There has been considerable progress towards proving this conjecture by Alon *et al.* [1, 4]. Degree lower bounds are weaker since they say the known technique for bounding $\alpha(G)$ and $\omega(G)$ does not yield good bounds, as opposed to showing either $\alpha(G)$ or $\omega(G)$ is large. But on the other hand, there are no good Ramsey constructions using signs of real polynomials, while OR representations are the best technique known for this problem. Further, the Ramsey graph constructions based on symmetric polynomials result in graphs where the vertex set is $\{0,1\}^n$ and where edges are added between vertices based on the Hamming distance between them. Such graphs possess a high degree of symmetry which is unlikely in a random graph. Our degree lower bound suggests that perhaps such Ramsey graph constructions cannot give better parameters (see Section 6).

We show a degree $\Omega(\sqrt{n})$ lower bound for OR representations by symmetric polynomials. Thus better representations if they exist must use asymmetric polynomials. A lower bound of $\Omega(\sqrt{n})$ is known for symmetric polynomials that weakly represent OR mod 6 [9]. Bhatnagar *et al.* [10] introduced the use of tools from communication complexity for proving degree lower bounds for symmetric polynomials. One might guess that similar arguments should work even for our definition of OR representations, but this is incorrect. In fact those arguments will not suffice even for prime representations. The precise bound they prove, and which holds for all weak representations is $\deg(P) \cdot \deg(Q) \geq n/(pq)$. This is good enough when p, q are small, but if $n < pq$ as in Alon's construction, this gives a bound of 1. One cannot hope for a stronger result since the polynomial $\sum_i X_i$ of degree 1 weakly represents OR on $n < pq$ variables over $\mathbb{Z}_{pq}$. Our definition restricts the values output by the weak representation, making it possible to show bounds independent of the modulus m. But exploiting this difference calls for new techniques, beyond the periodicity based arguments used for weak representations [9, 10].

1.1.3 Our Techniques:

While lower bounds for the prime and prime-power cases are very different, they have similar high-level structure: an *algebraic part* where we show that if the zero-set of the polynomial has certain structure, then the polynomial must have high degree, and a *combinatorial part* where we argue that there is no good partition of hypercube, that any partition results in one of the polynomials having high degree.

For the prime-power case, we translate the problem to one about univariate polynomials modulo $\mathbb{Z}_{p^a}$. However over $\mathbb{Z}_{p^a}$ it is no longer true that a degree d polynomial can have only d roots (take X^a for instance); so we need new tools for degree lower bounds. Building on an algorithm for interpolation over $\mathbb{Z}_{p^a}$ by the author [14], we define a *greedy sequence*, which roughly is a sequence that is distributed uniformly among various congruence classes modulo powers of p. We show that the longest greedy sequence in the zero-set lower-bounds the degree of a polynomial. Then a combinatorial argument shows that in any partition of integers $[1, \cdots, n]$ into A and B, one of them contains a long greedy sequence.

For the prime case, we view a symmetric polynomial P acting on a 0-1 vector $\mathbf{x}$ as a polynomial $\bar{P}$ acting on in the digits of the base p expansion of the weight $wt(\mathbf{x})$ following Bhatnagar *et al.*[10]. There it was shown that $\bar{P}$ can be used to bound $\deg(P)$ within a factor of p; we introduce a notion of weighted degree of $\bar{P}$ that exactly captures the degree of P. The combinatorial part of the proof uses a number theoretic lemma which seems of independent interest. It says that if p, q are primes, $n < pq$ and $A \subseteq \mathbb{Z}_p^*$ and $B \subseteq \mathbb{Z}_q^*$ are subsets so that every number in $[1, \cdots, n]$ lies in A mod p or in B mod q, then one of A or B has to be *large*.

We present our Ramsey constructions in Section 2. The lower bounds for prime-power representations are in Section 3. In Section 5, we give an alternate construction based on set intersections that results in exactly the constructions of Frankl-Wilson, Grolmusz and Alon. We also give improved bounds for set systems with restricted intersections modulo prime powers. We conclude with some open problems in Section 6.

A preliminary version of this paper appears in CCC'06 [13].

1.2 Preliminaries

Let $\mathbf{0} = (0, \cdots, 0)$. Given $\mathbf{x} \in \{0,1\}^n$ let $wt(\mathbf{x})$ denote its Hamming weight. Given $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$, $\mathbf{x} \oplus \mathbf{y}$ denotes symmetric difference, $\mathbf{x} \cap \mathbf{y}$ denotes the bitwise AND and $d(\mathbf{x}, \mathbf{y})$ denotes Hamming distance. Let $\binom{n}{\leq d} = \sum \binom{n}{i}$ for $i \leq d$. Let $S_k(\mathbf{X}) = \sum X_{i_1} \cdots X_{i_k}$ denote the k^{th} elementary symmetric polynomial. Every multilinear symmetric polynomial can be written as a linear combination of these polynomials. We will use Lucas' Theorem about binomial coefficients modulo p which states:

Fact 1 *Let*

$$w = \sum_{i \geq 0} w_i p^i, \ 0 \leq w_i < p$$

$$k = \sum_{i \geq 0} k_i p^i, \ 0 \leq k_i < p$$

$$\textit{Then} \quad \binom{w}{k} \equiv \prod_i \binom{w_i}{k_i} \bmod p.$$

For $x \in \mathbb{Z}$, let the valuation of x denoted $v_p[x]$ be the highest power of p that divides x. Let $v_p[0] = \infty$. We have the ultrametric inequality $v_p[x+y] \geq \min(v_p[x], v_p[y])$ and $v_p[xy] = v_p[x] + v_p[y]$.

We say a Ramsey graph $G(V, E)$ is explicit if there is a deterministic poly(|V|) time algorithm to compute the adjacency matrix and very explicit if there is a deterministic poly(log |V|) algorithm that computes the adjacency relation. We briefly describe the known explicit constructions of Ramsey graphs in chronological order.

− **Frankl-Wilson** [12]: Take p prime and $m = p^3$. The vertex set consists of all subsets of $[m]$ of size $p^2 - 1$. Two vertices S and T are adjacent if $|S \cap T| \not\equiv -1 \bmod p$. One can bound the size of $\alpha(G)$ and $\omega(G)$ using well-known results from extremal set theory [12, 5].

− **Grolmusz** [17, 18] : The main step is to construct a set system $\mathcal{F}$ on $[n]$ of size $n^{\omega(1)}$ so that $|S| \equiv 0 \bmod 6$ but $|S \cap T| \not\equiv 0 \bmod 6$. The vertices of the graph G are sets of $\mathcal{F}$ and S, T are adjacent if $|S \cap T|$ is odd. One can bound $\alpha(G)$ and $\omega(G)$ using results from extremal set theory.

− **Alon** [2]: Take $p < q$ to be nearly equal primes and $m = p^3$. The vertex set consists of all subsets of $[m]$ of size $pq - 1$. Two vertices S and T are adjacent if $|S \cap T| \not\equiv -1 \bmod p$. To bound $\alpha(G)$ and $\omega(G)$, we construct representations of G over $\mathbb{Z}_p$ and $\overline{G}$ over $\mathbb{Z}_q$.

− **Barak** [7]: Barak gives a product based construction (discovered independently by Pudlak and Rodl) where we first explicitly search for a good Ramsey graph in a small sample space and then use the Abbot product to get a larger graph. This gives $|V| = 2^n$ and $\alpha(G), \omega(G) \leq 2^{\epsilon\sqrt{n}\log n}$ for any $\epsilon > 0$. A similar product based construction, but with worse parameters is given by Naor [20].

− **Barak-Rao-Shaltiel-Wigderson** [8]: In a recent breakthrough, Barak et al. give a construction that achieves $\alpha(G), \omega(G) \leq 2^{n^{o(1)}}$. In fact they solve a more general problem, which is to construct bipartite Ramsey graphs. Their construction is rather intricate and makes significant use of machinery developed for extracting randomness from weak random sources.

The first three constructions above are very explicit, the last two are merely explicit.

2 OR Polynomials and Ramsey graphs

In this section, we prove the correctness of the construction described in the introduction. While the graphs obtained are not quite optimal, the construction is simple and best explains the close connections between OR representations and Ramsey graphs.

If graph G has a representation over a field $\mathbb{F}$ as in Definition 3, it is easy to show that $\omega(G) \leq dim(\mathcal{F})$ where $dim(\mathcal{F})$ is the dimension of the $\mathbb{F}$-vector space spanned by $\mathcal{F}$ [2]. For representations over $\mathbb{Z}_{p^a}$, we show that $\omega(G) \leq dim(\mathcal{F})$ where $dim(\mathcal{F})$ is the dimension of the $\mathbb{Q}$-vector space spanned by $\mathcal{F}$. The proof is by a valuation based argument similar to one used by Babai *et al.* [6].

Lemma 2 *If $G(V, E)$ has a polynomial representation over $\mathbb{Z}_{p^a}$, then $\omega(G) \leq dim(\mathcal{F})$.*

PROOF: Let $K \subseteq V$ be a clique. We claim that the polynomials $P_v(\mathbf{X})$ for $v \in K$ are linearly independent over $\mathbb{Q}$. Assume for contradiction that

$$\sum_{v \in K} \lambda_v P_v(\mathbf{X}) \;=\; 0$$

By clearing denominators, w.m.a that $\lambda_v \in \mathbb{Z}$, and by removing common factors w.m.a that p does not divide λ_u for some $u \in K$. Rearranging terms, we have

$$\lambda_u P_u(\mathbf{X}) \;=\; -\sum_{v \in K, v \neq u} \lambda_v P_v(\mathbf{X})$$

Substituting $\mathbf{X} = \mathbf{x}_u$,

$$\lambda_u P_u(\mathbf{x}_u) \;=\; -\sum_{v \in K, v \neq u} \lambda_v P_v(\mathbf{x}_u)$$

Since $P_u(\mathbf{x_u}) \not\equiv 0 \bmod p^a$ and $v_p[\lambda_u] = 0$, we have $v_p[\lambda_u P_u(\mathbf{x}_u)] \leq a - 1$. But $v \in K$ and $v \neq u$, then (v, u) is an edge, hence $P_v(\mathbf{x}_u) \equiv 0 \bmod p^a$. So the RHS is divisible by p^a, which is a contradiction. □

Construction 1 Graph $G(V, E)$ from OR polynomials.
− Let $V(G) = \{0, 1\}^n$.
− If $P(\mathbf{x} \oplus \mathbf{y}) \equiv 0$, add an edge $(\mathbf{x}, \mathbf{y})$.

Theorem 3 *Given a degree d OR representation, graph G has 2^n vertices and $\alpha(G), \omega(G) \leq \binom{n}{\leq d}$.*

PROOF: Assume that we have a prime representation. We give a polynomial representation of G over $\mathbb{Z}_p$.

For each vertex $\mathbf{v} \in \{0, 1\}^n$, let

$$Y_i = \begin{cases} 1 - X_i & \text{if } \mathbf{v}_i = 1 \\ X_i & \text{if } \mathbf{v}_i = 0 \end{cases}$$

Define $P_{\mathbf{v}}(X_1, \cdots, X_n)$ to be the polynomial obtained by multi-linearizing $P(Y_1, \cdots, Y_n)$ (i.e setting $X_i^d = X_i$). Note that for $\mathbf{u} \in \{0,1\}^n$,

$$P_{\mathbf{v}}(\mathbf{u}) = P(\mathbf{v} \oplus \mathbf{u}).$$

Hence

$$P_{\mathbf{v}}(\mathbf{v}) = P(\mathbf{0}) \not\equiv 0 \bmod p.$$

On the other hand, from our construction, if $(\mathbf{u}, \mathbf{v}) \in E$ then $P(\mathbf{v} \oplus \mathbf{u}) \not\equiv 0 \bmod p$. Hence

$$P_{\mathbf{v}}(\mathbf{u}) = P(\mathbf{v} \oplus \mathbf{u}) \not\equiv 0 \bmod p.$$

Thus we get a polynomial representation of G over $\mathbb{Z}_p$. Since the $P_{\mathbf{v}}(\mathbf{X})$s are all multilinear polynomials of degree at most d in n variables, they lie in a vector space of dimension $\binom{n}{\le d}$. This shows that $\omega(G) \le \binom{n}{\le d}$. Similarly, if $(\mathbf{u}, \mathbf{v})$ is not an edge then $P(\mathbf{v} \oplus \mathbf{u}) \not\equiv 0 \bmod p$, hence $Q(\mathbf{v} \oplus \mathbf{u}) \equiv 0 \bmod q$. Using this we construct a representation of $\overline{G}$ over $\mathbb{Z}_q$ and bound $\alpha(G)$.

For prime-power representations of OR, we can represent G and $\overline{G}$ over $\mathbb{Z}_{p^a}$ by the same argument. □

One can construct explicit Ramsey graphs by plugging in various OR representations described below; all of which give $d = O(\sqrt{n})$ using symmetric polynomials. This gives a bound of $c_1^{\sqrt{n}\log n}$ for some constant c_1 on the clique size. In fact the constructions below are very explicit, since given vertices $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$, the color of the edge $(\mathbf{x}, \mathbf{y})$ can be computed in time $O(n)$.

1) **Alon** [2]: Let $p < q$ be primes and let $n = pq - 1$. Define $P(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ and $Q(\mathbf{X}) \in \mathbb{Z}_q[\mathbf{X}]$ as

$$\begin{aligned} P(\mathbf{X}) &= 1 - \left(\sum X_i\right)^{p-1} \\ Q(\mathbf{X}) &= 1 - \left(\sum X_i\right)^{q-1} \end{aligned} \tag{1}$$

For $\mathbf{x} \neq \mathbf{0}$, since $1 \le \sum_i wt(\mathbf{x}) \le pq - 1$, by the CRT $wt(\mathbf{x}) \not\equiv 0 \bmod p$ or $wt(\mathbf{x}) \not\equiv 0 \bmod q$. By Fermat's Theorem, in the former case $P(\mathbf{x}) \equiv 0 \bmod p$, in the latter $Q(\mathbf{x}) \equiv 0 \bmod q$. Taking p, q nearly equal gives degree $d = (1 + o(1))\sqrt{n}$.

2) **BBR** [9]: Let $n = 2^k 3^\ell - 1$. Define $P(\mathbf{X}) \in \mathbb{Z}_2[\mathbf{X}]$ and $Q(\mathbf{X}) \in \mathbb{Z}_3[\mathbf{X}]$ as

$$\begin{aligned} P(\mathbf{X}) &= \binom{\sum_i X_i + 2^k - 1}{2^k - 1}, \\ Q(\mathbf{X}) &= \binom{\sum_i X_i + 3^\ell - 1}{3^\ell - 1} \end{aligned} \tag{2}$$

Since $\binom{\sum_i x_i}{k} = S_k(\mathbf{x})$ for $\mathbf{x} \in \{0,1\}^n$, $P(\mathbf{X})$ and $Q(\mathbf{X})$ in fact have coefficients from $\mathbb{Z}_2$ and $\mathbb{Z}_3$. For $x \neq \mathbf{0}$, $1 \le \sum_i wt(\mathbf{x}) \le 2^k 3^\ell - 1$. Lucas' theorem implies that if $wt(\mathbf{x}) \not\equiv 0 \bmod 2^k$ then $P(\mathbf{x}) \equiv 0 \bmod 2$, and if $wt(\mathbf{x}) \not\equiv 0 \bmod 3^\ell$ then $Q(\mathbf{x}) \equiv 0 \bmod 3$. We can choose k, ℓ s.t. $d = (1 + \varepsilon)\sqrt{n}$ for any $\varepsilon > 0$ [19].

Both representations above are prime representations, we now construct prime power representations. For ease of exposition, we restate Definition 4 of prime-power representations in terms of rational polynomials; we omit the simple proof of equivalence.

Definition 6 *Polynomials $P(\mathbf{X}), Q(\mathbf{X}) \in \mathbb{Q}[\mathbf{X}]$ represent the OR function on $\{0,1\}^n$ if*

$$P(0, \cdots, 0) \equiv 1 \bmod p \;\; \textit{and} \;\; Q(0, \cdots, 0) \equiv 1 \bmod p$$

and for $\mathbf{x} \in \{0,1\}^n \setminus (0, \cdots, 0)$

$$P(\mathbf{x}) \equiv 0 \bmod p \;\; \textit{or} \;\; Q(\mathbf{x}) \equiv 0 \bmod p$$

for a prime p. The degree of the representation is $d = \max(\deg(P), \deg(Q))$.

Note that in general $P(\mathbf{x})$ could be rational. When we say $P(\mathbf{x}) \equiv 0/1 \bmod p$, we mean $P(\mathbf{x})$ is an integer satisfying the condition. However, if $\mathbf{x} \neq \mathbf{0}$ and $Q(\mathbf{x}) \equiv 0 \bmod p$, then $P(\mathbf{x})$ need not be an integer and vice versa.

3) **Frankl-Wilson** [12]: Take p prime and $n = p^2 - 1$. Define $P(\mathbf{X}), Q(\mathbf{X}) \in \mathbb{Q}[\mathbf{X}]$ as

$$\begin{aligned} P(\mathbf{X}) &= \prod_{j=1}^{p-1}\left(\sum_i X_i - j\right) \\ Q(\mathbf{X}) &= \prod_{j=1}^{p-1}\left(\frac{\sum_i X_i}{p} - j\right) \end{aligned} \tag{3}$$

For a non-zero vector $\mathbf{x} \in \{0,1\}^n$ we have $1 \leq wt(\mathbf{x}) \leq p^2 - 1$. If $wt(\mathbf{x}) \not\equiv \mathbf{0} \bmod \mathbf{p}$ then $P(\mathbf{x}) \equiv 0 \bmod p$. If $wt(\mathbf{x}) \equiv 0 \bmod p$, then $1 \leq \frac{wt(\mathbf{x})}{p} \leq p-1$ hence $Q(\mathbf{x}) \equiv 0 \bmod p$. The degree is $d = p - 1 < \sqrt{n}$.

4) We construct representations with the prime fixed and n varying, analogous to [9]. Let $n = 2^{2k} - 1$. Define $P(\mathbf{X}), Q(\mathbf{X}) \in \mathbb{Q}[\mathbf{X}]$ as

$$\begin{aligned} P(\mathbf{X}) &= \binom{\sum_i X_i + 2^k - 1}{2^k - 1} \\ Q(\mathbf{X}) &= \binom{\frac{\sum_i X_i}{2^k} + 2^k - 1}{2^k - 1} \end{aligned} \tag{4}$$

The proof of correctness is through Lucas' theorem. If $wt(\mathbf{x}) \not\equiv 0 \bmod 2^k$ then $P(\mathbf{x}) \equiv 0$. If $\mathbf{x} \neq 0$ but $wt(\mathbf{x}) \equiv 0 \bmod 2^k$ then $Q(\mathbf{x}) \equiv 0$.

Plugging any of these polynomials into construction 1 gives the following type of graph : Add $(\mathbf{x}, \mathbf{y})$ to E if $d(\mathbf{x}, \mathbf{y}) \not\equiv 0 \bmod \ell$ where ℓ is either a prime or a prime power close to $\sqrt{n}$.

For constructing t-color Ramsey graphs, we define OR representations with t polynomials $P_1(\mathbf{X}), \cdots, P_t(\mathbf{X})$ such that the union of their zero sets if $\{0,1\}^n \setminus \{\mathbf{0}\}$. We can extend constructions in Equations 1, 2 by taking t distinct primes. To extend the construction of Equation 3, let $n = p^t - 1$. For $1 \leq \ell \leq t$ define

$$P_\ell(\mathbf{X}) = \prod_{j=1}^{p-1}\left(\frac{\sum_i X_i}{p^\ell} - i\right) \tag{5}$$

We can similarly extend Equation 4, we omit the details.

3 Lower Bounds for Prime-power Representations

In this section we prove a lower bound for prime-power representations by symmetric polynomials.

Theorem 4 *Let $P(\mathbf{X}) \in \mathbb{Z}_{p^a}[\mathbf{X}]$ and $Q(\mathbf{X}) \in \mathbb{Z}_{p^b}[\mathbf{X}]$ be symmetric polynomials that represent the OR function on n variables. Then $(\deg(P) + 1) \cdot (\deg(Q) + 1) \geq \frac{n}{2}$.*

Since a symmetric polynomial on 0-1 inputs is essentially a polynomial in the weight of the input, we can restate Theorem 4 in terms of integer polynomials. The formal proof is easy and is omitted. While we could also work with polynomials in $\mathbb{Z}_{p^a}[X]$, the presence of zero divisors would make it messier to use valuations.

Proposition 5 *Let $P(X), Q(X) \in \mathbb{Z}[X]$ be univariate polynomials such that for $x \in \{1, \cdots, n\}$,*

$$v_p[P(0)] < v_p[P(x)] \quad \textit{or} \quad v_p[Q(0)] < v_p[Q(x)] \tag{6}$$

Then $(\deg(P) + 1) \cdot (\deg(Q) + 1) \geq \frac{n}{2}$.

The next two Lemmas (6 and 7) develop tools to show degree bounds for such polynomials.

Definition 7 *A sequence $S = (\alpha_1, \cdots, \alpha_d)$ of integers is called a greedy sequence if for all j,*

$$\sum_{i<j} v_p[\alpha_j - \alpha_i] \;\leq\; \sum_{i<j} v_p[\alpha_k - \alpha_i] \;\; \textit{for} \;\; k \neq j$$

Let us define $N_1(X) = 1$ and $N_j(X) = \prod_{i<j}(X - \alpha_i)$ for $j > 1$. The definition of a greedy sequence can be restated as $v_p[N_j(\alpha_j)] \;\leq\; v_p[N_j(\alpha_k)]$ for $k \neq j$. Given any set S, we can order it elements *greedily* as follows to get a greedy sequence: we choose α_1 arbitrarily; having chosen $(\alpha_1, \cdots, \alpha_{j-1})$ we choose $\alpha_j \in S$ to be the element that minimizes $v_p[N_j(\alpha_j)]$.

Lemma 6 *Let $S = (\alpha_1, \cdots, \alpha_d)$ be a greedy sequence. Let $P(X) \in \mathbb{Z}[X]$ be such that*

$$v_p[P(\alpha_d)] \;\;<\;\; v_p[P(\alpha_i)] \quad \textit{for } i \leq d-1$$

Then $\deg(P) \geq d - 1$.

PROOF: The proof is by induction on d. We will show the converse, namely that if $\deg(P) \leq d - 2$.

$$v_p[P(\alpha_d)] \;\geq\; \min_{i \leq d-1} v_p[P(\alpha_i)]$$

The base case $d = 2$ is trivial, in this case P is constant so it is clear that $v_p[P(\alpha_2)] = v_p[P(\alpha_1)]$. Assume the property holds for greedy sequences of length $d - 1$. Given a polynomial $P(X)$ of degree $d - 2$, since $N_{d-1}(X)$ is a monic polynomial of degree $d - 2$, we write $P(X) = Q(X) + c_{d-1}N_{d-1}(X)$, where $Q(X)$ is a polynomial of degree $d - 3$. Substituting $X = \alpha_d$,

$$P(\alpha_d) \;=\; Q(\alpha_d) + c_{d-1}N_{d-1}(\alpha_d)$$

hence by the ultrametric inequality

$$v_p[P(\alpha_d)] \;\geq\; \min\{v_p[Q(\alpha_d)], v_p[c_{d-1}N_{d-1}(\alpha_d)]\} \tag{7}$$

To lower bound $v_p[Q(\alpha_d)]$, note that the sequence $(\alpha_1, \cdots, \alpha_{d-2}, \alpha_d)$ of length $d - 1$ obtained by deleting α_{d-1} is also greedy. Hence applying the inductive hypothesis to $Q(\alpha_d)$, we get

$$v_p[Q(\alpha_d)] \;\geq\; \min_{i \leq d-2} v_p[Q(\alpha_i)] \;=\; \min_{i \leq d-2} v_p[P(\alpha_i)] \tag{8}$$

The last equality follows since $N_{d-1}(\alpha_i) = 0$ for $i \leq d - 2$, hence $Q(\alpha_i) = P(\alpha_i)$. We now lower bound $v_p[c_{d-1}N_{d-1}(\alpha_d)]$. Using the greedy property of the sequence $(\alpha_1, \cdots, \alpha_d)$,

$$v_p[c_{d-1}N_{d-1}(\alpha_d)] \;\geq\; v_p[c_{d-1}N_{d-1}(\alpha_{d-1})]$$

$$c_{d-1}N_{d-1}(\alpha_{d-1}) \;=\; P(\alpha_{d-1}) - Q(\alpha_{d-1})$$

Hence we have

$$v_p[c_{d-1}N_{d-1}(\alpha_{d-1})] \;\geq\; \min\{v_p[P(\alpha_{d-1})], v_p[Q(\alpha_{d-1})]\} \tag{9}$$

Since $(\alpha_1, \cdots, \alpha_{d-1})$ is a greedy sequence and Q has degree $d - 3$, we get by induction that

$$v_p[Q(\alpha_{d-1})] \;\geq\; \min_{i \leq d-2} v_p[Q(\alpha_i)] \;=\; \min_{i \leq d-2} v_p[P(\alpha_i)] \tag{10}$$

Combining Equations 7, 8, 9, 10 gives the desired result. □

An example of a greedy sequence is when $(\alpha_1, \cdots, \alpha_d)$ are consecutive integers. Thus while a degree d polynomial over $\mathbb{Z}_{p^a}$ can have several zeroes, the lemma implies that it can have at most d consecutive zeroes. The intuition for this Lemma is from an algorithm for polynomial interpolation over $\mathbb{Z}_{p^a}$ by the author [14]. Given a set S, and values $f(x)$ for $x \in S$ of some polynomial in $\mathbb{Z}_{p^a}[X]$, the algorithm will output the smallest degree polynomial $P(X)$ that fits the data, provided it sees the elements of S in the above greedy order. If the polynomial is 0 on every element but the last, the algorithm is forced to output a polynomial of degree $d-1$.

Next we define the notion of a greedy array which we use to construct long greedy sequences. Given a t-dimensional matrix A of dimension $d_0 \times \cdots \times d_{t-1}$, we use $A[\mathbf{i}]$ to denote $A[i_0, \cdots, i_{t-1}]$.

Definition 8 *A t-dimensional matrix of distinct integers A is called a greedy array if*

$$v_p[A[\mathbf{i}] - A[\mathbf{j}]\,] = \min\{a | i_a \neq j_a\} \tag{11}$$

We define an ordering of the array indices, which is essentially the reverse lexicographic (revlex) ordering.

Definition 9 *Given a t-dimensional integer vectors* $\mathbf{i}$ *and* $\mathbf{j}$, *let* $\ell = \max\{a | i_a \neq j_a\}$. *Then* $\mathbf{i} < \mathbf{j}$ *if* $i_\ell < j_\ell$.

Note that for a greedy array, the valuation should equal the smallest index where $\mathbf{i}$ and $\mathbf{j}$ differ. However to order elements, we look at the largest index where they differ. For example, consider the $p \times \cdots \times p$ array where $A[i_0, \cdots, i_{t-1}] = i_0 + i_1 p \cdots i_{t-1} p^{t-1}$ and $0 \leq i_j \leq p-1$. Thus the array contains $i \in \{0, \cdots, p^t - 1\}$ with numbers indexed by their base-p expansion. Since $v_p[i-j]$ depends on the smallest digit where i and j, this is a greedy array. The ordering defined above is the usual ordering of integers, it depends on the largest digit where the expansions differ.

Lemma 7 *Ordering elements of a greedy array gives a greedy sequence.*

PROOF: We want to show that for $\mathbf{k} \neq \mathbf{j}$

$$\sum_{\mathbf{i}<\mathbf{j}} v_p[A[\mathbf{j}] - A[\mathbf{i}]\,] \;\leq\; \sum_{\mathbf{i}<\mathbf{j}} v_p[A[\mathbf{k}] - A[\mathbf{i}]\,] \tag{12}$$

For $0 \leq a \leq t-1$, we define the set

$$S_a = \{\mathbf{i} | i_a < j_a,\ i_{a+1} = j_{a+1}, \cdots,\ i_{t-1} = j_{t-1}\}$$

The indices $i_0, \cdots, i_{a-1}$ are unrestricted. Note that the S_as are disjoint and they partition the set $\{\mathbf{i} | \mathbf{i} < \mathbf{j}\}$. We show that for every a, and for $\mathbf{k} \neq \mathbf{j}$

$$\sum_{\mathbf{i}\in S_a} v_p[A[\mathbf{j}] - A[\mathbf{i}]\,] \;\leq\; \sum_{\mathbf{i}\in S_a} v_p[A[\mathbf{k}] - A[\mathbf{i}]\,] \tag{13}$$

Equation 12 will follow by summing over all a. Hence consider a fixed a. Note that if $\mathbf{i} \in S_a$ then $0 \leq v_p[A[\mathbf{j}] - A[\mathbf{i}]\,] \leq a$. Accordingly we partition S_a into $J(0), \cdots, J(a)$ as follows: for $0 \leq \ell \leq a-1$,

$$\begin{aligned} J(\ell) &= \{\mathbf{i} \in S_a | i_0 = j_0, \cdots, i_{\ell-1} = j_{\ell-1}, i_\ell \neq j_\ell\} \\ &= \{\mathbf{i} \in S_a | v_p[A[\mathbf{j}] - A[\mathbf{i}]\,] = \ell\} \\ J(a) &= \{\mathbf{i} \in S_a | i_0 = j_0, \cdots, i_{a-1} = j_{a-1}\} \end{aligned}$$

For $\mathbf{i} \in J(a)$ we have $v_p[A[\mathbf{j}] - A[\mathbf{i}]\ ] = a$ since for all $\mathbf{i} \in S_a$, $i_a < j_a$ so $i_a \neq j_a$. Now given $\mathbf{k} \neq \mathbf{i}$ let us define the sets $K(0), \cdots, K(a)$ as follows. For $0 \leq \ell \leq a-1$,

$$\begin{aligned} K(\ell) &= \{\mathbf{i} \in S_a | i_0 = k_0, \cdots, i_{\ell-1} = k_{\ell-1}, i_\ell \neq k_\ell\} \\ &= \{\mathbf{i} \in S_a | v_p[A[\mathbf{k}] - A[\mathbf{i}]\ ] = \ell\} \\ K(a) &= \{\mathbf{i} \in S_a | i_0 = k_0, \cdots, i_{a-1} = k_{a-1}\} \end{aligned}$$

Unlike for $J(a)$, for $i \in K(a)$ it could be that $i_a = k_a$, so we have $v_p[A[\mathbf{k}] - A[\mathbf{i}]\ ] \geq a$. Since the indices $i_0, \cdots, i_{a-1}$ are unrestricted in S_a, we have $|J(\ell)| = |K(\ell)|$ for $0 \leq \ell \leq a$. We now prove Equation 13.

$$\begin{aligned} \sum_{\mathbf{i} \in S_a} v_p[A[\mathbf{j}] - A[\mathbf{i}]\ ] &= \sum_{0 \leq \ell \leq a} \sum_{\mathbf{i} \in J(\ell)} v_p[A[\mathbf{j}] - A[\mathbf{i}]\ ] \\ &= \sum_{0 \leq \ell \leq a} \ell \cdot |J(\ell)| \\ \sum_{\mathbf{i} \in S_a} v_p[A[\mathbf{k}] - A[\mathbf{i}]\ ] &= \sum_{0 \leq \ell \leq a} \sum_{\mathbf{i} \in K(\ell)} v_p[A[\mathbf{k}] - A[\mathbf{i}]\ ] \\ &\geq \sum_{0 \leq \ell \leq a} \ell \cdot |K(\ell)| \\ &\geq \sum_{0 \leq \ell \leq a} \ell \cdot |J(\ell)| \end{aligned}$$

Hence the claim follows. □

A two-dimensional greedy array is a matrix G of integers such that elements in the same row are congruent $\bmod\, p$, while elements in distinct rows are not congruent $\bmod\, p$. Lemma 7 says that ordering the elements of G column-wise gives a greedy sequence.

This concludes the algebraic step of the proof. Let us sketch the rest of the proof when $n = p^2 - 1$, which corresponds to the Frankl-Wilson construction (see Figure 1). Define the sets

$$A = \{0\} \cup \{x \in \{1, \cdots, p^2 - 1\} \mid v_p[P(0)] < v_p[P(x)]\}$$

$$B = \{0\} \cup \{x \in \{1, \cdots, p^2 - 1\} \mid v_p[P(0)] \geq v_p[P(x)]\}$$

Note that $v_p[Q(0)] < v_p[Q(x)]$ for every $x \neq 0$ in B. Further A and B partition the set $\{1, \cdots, p^2 - 1\}$ and they intersect only at 0. We will show that A and B contain *large* greedy arrays.

1. Arrange $\{0, \cdots p^2 - 1\}$ in $p \times p$ grid, each row corresponding to a congruence class $\bmod\, p$.

2. Within each row, place elements lying in A before those in B. Since 0 lies in $A \cap B$, place all other elements in A which are $0 \bmod p$ before 0.

3. Sort the rows according to how many elements from A they contain.

This reordering is illustrated in Figure 1, the dark line separates A and B. It is clear that A and B contain greedy arrays G of size $k_0 \times k_1$ and H of size $\ell_0 \times \ell_1$ respectively (indicated by shaded regions) so that $k_0 + \ell_0 = k_1 + \ell_1 = p + 1$. From this it follows that $|G||H| \geq p^2$. Also, we can ensure that 0 is the last element of these arrays in the column-wise ordering. So $v_p[P(x)]$ is minimized at the last element in G, hence by Lemma 7 $\deg(P) \geq |G| - 1$. Similarly $\deg(Q) \geq |H| - 1$, which proves the desired bound. Also, $|G||H|$

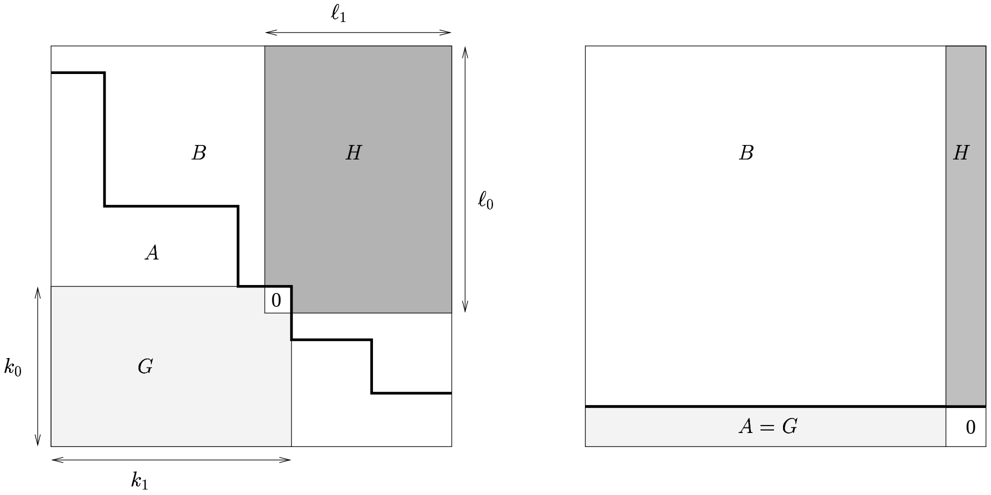

Figure 1: Lower bound for $p^2 - 1$ and the Frankl-Wilson construction

is minimized when $A = \{x | x \equiv 0 \bmod p\}$, and $B = 0 \cup \{x | x \not\equiv 0 \bmod p\}$ (or vice versa), the corresponding polynomials give exactly the Frankl-Wilson construction.

The proof for general n is a high dimensional extension of this argument. The next lemma (Lemma 8) says that any disjoint partition of $\{0, \cdots, n-1\}$ into A, B will result in one of the partitions having a greedy array of size $\sqrt{n}$. In fact we prove something stronger, we can choose the dimensions of the array to be any solution to Equation 14. We also assume that n is of the form $n'p^{t-1}$ which makes it easier to use induction.

Lemma 8 *Let $1 \leq n' \leq p$. Let A, B be disjoint sets of integers such that $A \cup B = \{0, \cdots, n'p^{t-1} - 1\}$. Given any positive integers $k_0, \cdots, k_{t-1}, \ell_0, \cdots, \ell_{t-1}$ satisfying*

$$\begin{aligned} \textit{For } i \leq t-2 \qquad k_i + \ell_i &= p+1 \\ k_{t-1} + \ell_{t-1} &= n' + 1 \end{aligned} \tag{14}$$

either A contains a greedy array of size $k_0 \times \cdots \times k_{t-1}$ or B contains a greedy array of size $\ell_0 \times \cdots \times \ell_{t-1}$.

PROOF: The proof is by induction on t (the dimension of the greedy arrays).

When $t = 1$, we have disjoint sets A, B so that $A \cup B = \{0, \cdots, n' - 1\}$ hence $|A| + |B| = n'$. Since $n' - 1 < p$ any ordering of A and B gives greedy arrays of size $|A|$ and $|B|$ respectively. Given k_0, ℓ_0 such that $k_0 + \ell_0 = n' + 1$, if $|A| \leq k_0 - 1$, then $|B| \geq n' + 1 - k_0 = \ell_0$.

Assume that the claim is true up to $t - 1$. For $0 \leq i \leq p - 1$, we define the following sets

$$A(i) = \{x \in A | x \equiv i \bmod p\}$$
$$\hat{A}(i) = \{(x - i)/p \mid x \in A(i)\}$$

We define sets $B(i)$ and $\hat{B}(i)$ similarly. Note that for each i, $\hat{A}(i)$ and $\hat{B}(i)$ are disjoint, further $\hat{A}(i) \cup \hat{B}(i) = \{0, \cdots, n'p^{t-2} - 1\}$. So the induction hypothesis applied to $\hat{A}(i)$ and $\hat{B}(i)$ with $k_1, \cdots, k_{t-1}, \ell_1, \cdots, \ell_{t-1}$ implies that either A contains a greedy array of size $k_1 \times \cdots \times k_{t-1}$ or B contains a greedy array of size $\ell_1 \times \cdots \times \ell_{t-1}$. We define the following sets

$$S = \{i | \hat{A}(i) \text{ has a greedy array } \hat{G}_i \text{ of size } k_1 \times \cdots \times k_{t-1}\}$$
$$T = \{i | \hat{B}(i) \text{ has a greedy array } \hat{H}_i \text{ of size } \ell_1 \times \cdots \times \ell_{t-1}\}$$

Since S, T are disjoint and $|S| + |T| = p$ we have either $|S| \geq k_0$ or $|T| \geq \ell_0$. Assume $|S| \geq k_0$. We define a greedy array G of size $k_0 \times \cdots \times k_{t-1}$ as follows. Choose $S' \subset S$ of size k_0. For each $i \in S'$, the i^{th} row of G contains the pre-image G_i of $\hat{G}_i$ in $A(i)$ of dimension $k_1 \times \cdots \times k_{t-1}$.

We need to verify that G satisfies $v_p(G[\mathbf{i}] - G[\mathbf{j}]) = \min\{a | i_a \neq j_a\}$. Given $\mathbf{i}$ and $\mathbf{j}$, if $i_0 \neq j_0$, then $G[\mathbf{i}] \not\equiv G[\mathbf{j}] \bmod p$ so the condition holds. Now assume that $i_0 = j_0$, so that $\mathbf{i} = (i_0, \mathbf{i}'), \mathbf{j} = (i_0, \mathbf{j}')$. Since $G[\mathbf{i}]$ and $G[\mathbf{j}]$ are in the same row, $G[\mathbf{i}] \equiv G[\mathbf{j}] \equiv c \bmod p$ for $0 \leq c \leq p-1$. So

$$\begin{aligned} G[\mathbf{i}] - G[\mathbf{j}] &= G_c[\mathbf{i}'] - G_c[\mathbf{j}'] \\ &= (p\hat{G}_c[\mathbf{i}'] + c) - (p\hat{G}_c[\mathbf{j}'] + c) \\ &= p(\hat{G}_c[\mathbf{i}'] - \hat{G}_c[\mathbf{j}']) \\ \Rightarrow\ v_p[G[\mathbf{i}] - G[\mathbf{j}]\,] &= 1 + v_p[G_c[\mathbf{i}'] - G_c[\mathbf{j}']\,] \\ &= 1 + \min\{a | i'_a \neq j'_a\} \end{aligned}$$

Note that $\min\{a | i_a \neq i_a\} = 1 + \min\{a | i'_a \neq i'_a\}$. Hence G is a greedy array of the right dimension. □

The next Lemma is the key step in the combinatorial argument. Now we consider sets A and B which intersect only at 0, and we want to produce greedy arrays that end at 0 by our ordering. We show that such arrays exist whose dimensions satisfy Equation 14.

Lemma 9 Partition Lemma: *Let $1 \leq n' \leq p$. Let A, B be sets of integers such that*

$$A \cup B = \{0, \cdots, n'p^{t-1} - 1\}, \quad A \cap B = \{0\}$$

Then there exist positive integers $k_0, \cdots, k_{t-1}, \ell_0, \cdots, \ell_{t-1}$ satisfying Equation 14, so that A contains a greedy array G of size $k_0 \times \cdots \times k_{t-1}$ and B contains a greedy array H of size $\ell_0 \times \cdots \times \ell_{t-1}$, and both G and H contain 0 as the last element.

PROOF: The proof is by induction on t.

When $t = 1$, we have sets A, B so that $A \cup B = \{0, \cdots, n' - 1\}$ and $A \cap B = \{0\}$ so $|A| + |B| = n' + 1$. We take $k_0 = |A|, \ell_0 = |B|$. Define G to be an ordering of A where 0 comes last, similarly for H.

Assume that the claim holds up to $t - 1$. For $0 \leq i \leq p - 1$, we define the sets $A(i), \hat{A}(i), B(i), \hat{B}(i)$ as before. Note that

$$\begin{aligned} \hat{A}(0) \cup \hat{B}(0) = \{0, \cdots, n'p^{t-2} - 1\} \\ \hat{A}(0) \cap \hat{B}(0) = \{0\} \end{aligned}$$

By induction, there exist $k_1, \cdots, k_{t-1}$ and $\ell_1, \cdots, \ell_{t-1}$ as above so that $\hat{A}(0)$ contains a greedy array of size $k_1 \times \cdots \times k_{t-1}$ and $\hat{B}(0)$ contains a greedy array of size $\ell_1 \times \cdots \times \ell_{t-1}$. For $1 \leq i \leq p - 1$ we have

$$\begin{aligned} \hat{A}(i) \cup \hat{B}(i) &= \{0, \cdots, n'p^{t-2} - 1\} \\ \hat{A}(i) \cap \hat{B}(i) &= \phi \end{aligned}$$

Hence applying Lemma 8, either $\hat{A}(i)$ contains an array of size $k_1 \times \cdots \times k_{t-1}$ or $\hat{B}(0)$ contains a greedy array of size $\ell_1 \times \cdots \times \ell_{t-1}$. Again we define the sets

$$\begin{aligned} S = \{i | \hat{A}(i) \text{ has a greedy array } \hat{G}_i \text{ of size } k_1 \times \cdots \times k_{t-1}\} \\ T = \{i | \hat{B}(i) \text{ has a greedy array } \hat{H}_i \text{ of size } \ell_1 \times \cdots \times \ell_{t-1}\} \end{aligned}$$

Let $k_0 = |S|, \ell_0 = |T|$. Since $S \cap T = \{0\}$ and $S \cup T = \{0, \cdots, p-1\}$ we have $k_0 + \ell_0 = p + 1$. Order S and T so that 0 is the last element. We define a greedy array G of size $k_0 \times \cdots \times k_{t-1}$ as follows. For each $i \in S$, the i^{th} row of G contains the pre-image G_i of $\hat{G}_i$ in $A(i)$ of dimension $k_1 \times \cdots \times k_{t-1}$. Similarly we define H where the i^{th} row contains the pre-image H_i of $\hat{H}_i$ in $B(i)$. The proof that these are greedy arrays follows Lemma 8. They both contain 0 as the last element by induction. □

We now complete the proof of Theorem 4.

PROOF OF THEOREM 4:
Assume that $p^{t-1} \leq n < p^t$. We can choose n' so that $1 \leq n' \leq p$ and $n/2 \leq n'p^{t-1} - 1 \leq n$. Define the sets

$$A = \{0\} \cup \{x \mid 1 \leq x \leq n'p^{t-1} - 1,\ v_p[P(0)] < v_p[P(x)]\}$$
$$B = \{0\} \cup \{x \mid 1 \leq x \leq n'p^{t-1} - 1,\ v_p[P(0)] \geq v_p[P(x)]\}$$

Applying Lemma 9 implies that A and B contain greedy arrays G and H of size $k_0 \times \cdots \times k_{t-1}$ and $\ell_0 \times \cdots \times \ell_{t-1}$ respectively where k_i and ℓ_i satisfy Equation 14. Applying Lemma 7, by ordering G we get a greedy sequence $\{\alpha_1, \cdots, \alpha_{d-1}, 0\}$ in A of length $d = \prod_j k_j$. By the definition of set A, $v_p[P(0)] < v_p[P(\alpha_i)]$ for $i \leq d$. So by Lemma 6 $\deg(P) \geq \prod_j k_j - 1$.

Similarly we get a greedy sequence of length $\prod_j \ell_j$ in B ending in 0. Note that by Equation 6, $x \in B$ and $x \neq 0$ implies $v_p[Q(0)] < v_p[Q(x)]$. So by Lemma 6, $\deg(Q) \geq \prod_j \ell_j - 1$. By Equation 14, $k_j \ell_j \geq p$ for $j \leq t-2$ and $k_{t-1}\ell_{t-1} \geq n'$. Hence

$$\begin{aligned}(\deg(P)+1)(\deg(Q)+1) &\geq \prod_j k_j \ell_j \\ &\geq n'p^{t-1} > n/2.\end{aligned}$$

For the Frankl-Wilson construction where $n = p^2 - 1$, we get $(\deg(P)+1)(\deg(Q)+1) \geq p^2$ which is tight. □

4 Lower Bounds for Prime Representations

In this section we prove a lower bound for prime representations using symmetric polynomials.

Theorem 10 *Let $P(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ and $Q(\mathbf{X}) \in \mathbb{Z}_q[\mathbf{X}]$ be symmetric polynomials that represent the OR function on n variables. Then* $\deg(P).\deg(Q) \geq n/10$.

Note that this requires $\deg(P), \deg(Q) \geq 1$ but if $\deg(P) = 0$, then it is easy to show that $\deg(Q) = n$, so this case is not interesting. The hard case of this theorem is when p and q are fast-growing functions of n, as in Alon's construction. To handle this case, we prove a partition lemma (Lemma 11) which says that taking p and q large does not help.

Definition 10 *Let $p < q$ be distinct primes, let $n < pq$. Let $A \subseteq \mathbb{Z}_p^*$ and $B \subseteq \mathbb{Z}_q^*$. We say that x is covered by A if $x \bmod p \in A$. We say A and B cover $[n]$ if every $x \in \{1, \cdots, n\}$ is covered by A or B.*

If $n < pq$, we can cover $[n]$ by taking $A = \mathbb{Z}_p^*$ and $B = \mathbb{Z}_q^*$. Given $A \subseteq \mathbb{Z}_p^*$ and $B \subseteq \mathbb{Z}_q^*$, the number of elements in $\{1, \cdots, pq\}$ that are covered by A or B is $|A|q + |B|p - |A||B|$ which can be much larger than $|A||B|$. The partition lemma states that to cover the first n integers however, $|A||B|$ needs to be $\Omega(n)$.

Lemma 11 **Partition Lemma:** *If $A \subseteq \mathbb{Z}_p^*$ and $B \subseteq \mathbb{Z}_q^*$ cover $[n]$, then $(|A|+1) \cdot (|B|+1) > \frac{n}{2}$.*

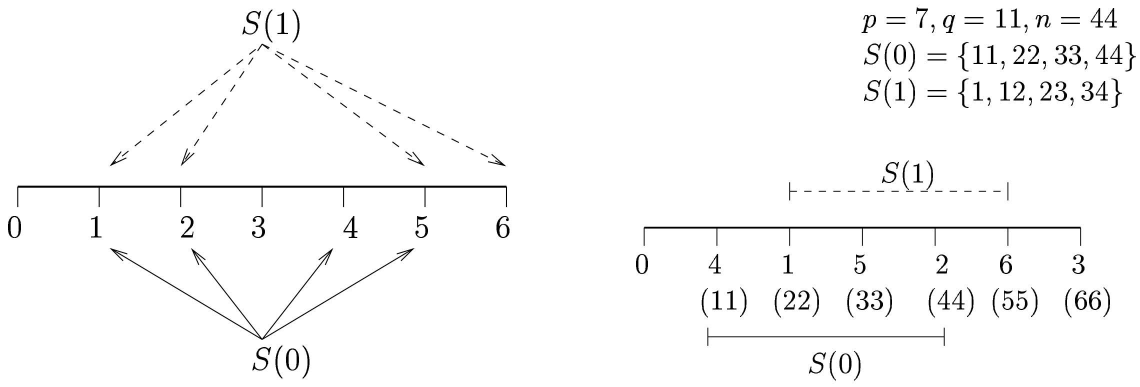

Figure 2: Proof of Prop 12

Using $|A| + 1$ rather than $|A|$ in the product lets us ignore the case when $|A| = 0$. Let us sketch the idea behind the proof of the Partition Lemma. Let $n = n_q q$. Assume that to begin with, we have $B = \mathbb{Z}_q^*$ and $A = \{q, 2q, \cdots, n_q q\}$. It is clear that A and B cover n, however $(|A| + 1)(|B| + 1) > n$. One could try and reduce $|B|$ by removing elements from it. We want to show that this results in an increase in $|A|$. Removing $i \in \mathbb{Z}_q^*$ from B results in the numbers $\{i, i + q, \cdots, i + (n_q - 1)q\}$ being uncovered. Call this set $S(i)$. The various elements of $S(i)$ are less than pq and they are congruent mod q, hence the CRT implies they cannot also be congruent mod p. But the problem is for $i \neq j$,there could be considerable overlap between the residues of $S(i)$ and $S(j)$ mod p. Hence it is not clear that removing many elements from B does actually cause $|A|$ to increase. However, by suitably reordering the elements of $\mathbb{Z}_p$, we show that every element removed from B causes the size of A to increase by at least 1. In fact Figure 2 shows that $|A|$ could increase by just 1. This is sufficient to prove the Partition Lemma.

Set $n_p = \left\lfloor \frac{n}{p} \right\rfloor$ and $n_q = \left\lfloor \frac{n}{q} \right\rfloor$. Given set S of integers, define $S \bmod p \subseteq \mathbb{Z}_p$ to be the set $\{x \bmod p | x \in S\}$.

Proposition 12 *Let $n \geq q$. If A and B cover $[n]$ and $|B| = q - \ell$ then $|A| \geq \left\lfloor \frac{n}{q} \right\rfloor + \ell - 1$.*

PROOF: Note that since $n \geq q$, $n_q \geq 1$. Let $\overline{B}$ denote the complement of B in $\mathbb{Z}_q$, so $0 \in \overline{B}$. For each $i \in \overline{B}$, take $S(i)$ to be the first n_q numbers in $\{1, \cdots, n\}$ congruent to i mod p. In other words, $S(0) = \{q, 2q \cdots, n_q q\}$ and for $i \neq 0, S(i) = \{i, i + q, \cdots, i + (n_q - 1)q\}$. Let

$$S = \bigcup_{i \in \overline{B}} S(i)$$

If $x \in S$, then x is not covered by B so it must be covered by A. We want to lower bound the size of $S \bmod p$.

Let us reorder the set $\mathbb{Z}_p$ as $\{0, q, 2q, \cdots, (p-1)q\}$ (this is a reordering since $(q, p) = 1$). It sends $j \bmod p$ to $c(j)q$ such that $c(j)q \equiv j \bmod p$. This map sends $S(0) \bmod p$ to $\{q, \cdots, n_q q\}$ and the set $S(i) \bmod p$ to the interval $\{c(i)q, (c(i) + 1)q, \cdots, (c(i) + n_q - 1)q\}$ of length n_q for $i \neq 0$. None of these intervals contain 0, since that would give $x \in \{1, \cdots, n\}$ such that $x \equiv i \bmod q$ and $x \equiv 0 \bmod p$. Such an x is not covered by A or B. Each interval $S(i) \bmod p$ begins at a distinct point $c(i)$. Sorting the intervals by their starting points, it follows that the union of ℓ such intervals of length n_q contains at least $n_q + \ell - 1$ elements of $\mathbb{Z}_p^*$. □

Figure 2 illustrates this argument for $p = 7, q = 11, n = 44$. Here $B = \mathbb{Z}_{11} \setminus \{0, 1\}$.

PROOF OF LEMMA 11:

We consider the cases $n < p$, $p < n \leq q$ and $q \leq n$ separately. The non-trivial case is when $q \leq n$.

1. Let $n \leq p < q$. Numbers $\{1, \cdots, n\}$ lie in distinct congruence classes mod p and q. Hence
$$|A| + |B| \geq n \;\; \Rightarrow \;\; (|A| + 1) \cdot (|B| + 1) > n$$

2. Let $p < n \leq q$. The numbers $\{1, \cdots, p\}$ lie in distinct congruence classes modulo p and q. Hence $|A| + |B| \geq p$ and $(|A| + 1) \cdot (|B| + 1) > p$. This proves the claim if $n \leq 2p$ so let $n > 2p$.

   Let $|A| = p - k$ for $1 \leq k < p$. There are n_p numbers $\leq n$ in each congruence class mod p. Thus $n_p k$ numbers are not covered by A and have to be covered by B. Since $n \leq q$, they lie in distinct congruence classes mod q. Hence $|B| \;\geq\; n_p k$. Using the fact that $n \geq 2p$ hence $pn_p \geq n/2$ we get
$$(|A| + 1) \cdot (|B| + 1) \;>\; (p - k + 1)kn_p \;\geq\; pn_p \;>\; n/2$$

3. Let $n > q$. By Prop. 12, if $|B| = q - \ell$, then $|A| \geq n_q + \ell - 1$. Since $|A| \leq p - 1$, we get $1 \leq \ell \leq p - n_q$. Hence for $1 \leq \ell \leq p - n_q$ we have
$$(|A| + 1)(|B| + 1) \;\geq\; (q - \ell + 1)\,(n_q + \ell)$$

   We will show that this is lower bounded by $n/2$. By differentiating, this bound is minimized at one of the extreme values of ℓ, so it suffices to check the bound is at least $\frac{n}{2}$ for those values. When $\ell = 1$,
$$(q - \ell + 1)\left(\left\lfloor \frac{n}{q} \right\rfloor + \ell\right) \;=\; q\left(\left\lfloor \frac{n}{q} \right\rfloor + 1\right) \;>\; n$$

   When $\ell = p - \left\lfloor \frac{n}{q} \right\rfloor$
$$\begin{aligned}(q - \ell + 1)\left(\left\lfloor \frac{n}{q} \right\rfloor + \ell\right) &= \left(q - p + \left\lfloor \frac{n}{q} \right\rfloor + 1\right)p \\ &\geq \left(q - p + \frac{n}{q}\right)p \\ &= (q - p)p + \frac{np}{q}\end{aligned}$$

   One of $(q - p)p$ and $(np)/q$ is at least $n/2$: If $q < 2p$, $(np)/q > n/2$. If $q > 2p$, then $(q - p)p \;>\; n/2$.

□

We now proceed to the algebraic step of the proof. Every symmetric polynomial $P(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ computes a symmetric function $w(\mathbf{X}) \to \mathbb{Z}_p$. Let $w(\mathbf{x}) = \sum_{i \leq \ell} w_i p^i$. Every polynomial $\bar{P}(w_0, \cdots, w_\ell)$ also computes a function $w(\mathbf{X}) \to \mathbb{Z}_p$. The following equivalence between the two kinds of polynomials is given by Theorem 2.4 of [10].

Proposition 13 *The functions that can be computed by symmetric polynomials $P(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ of degree less than p^{j+1} are the functions which can be computed by polynomials $\bar{P}(w_0, \cdots, w_j)$.*

For each variable w_j, let $\deg(w_j)$ denote the degree of w_j in $\bar{P}$. If j is the largest index so that $\deg(w_j) > 0$ then $p^j \;\leq\; \deg(P) \;<\; p^j$. This gives a bound with an error factor of p. By defining an appropriate weighted degree of $\bar{P}$, we can make the correspondence exact.

Definition 11 *Given $\bar{P}(w_0, \cdots, w_\ell) \in \mathbb{Z}_p[w_0, \cdots, w_\ell]$, the degree of a monomial $\prod_i w_i^{d_i}$ with $d_i \leq p-1$ is defined as* $\deg(\prod_i w_i^{d_i}) = \sum_i d_i p^i$*. The degree of $\bar{P}$ denoted* $\deg(\bar{P})$ *is the maximum degree over all monomials.*

Note that if j is the largest index such that $\deg(w_j) > 0$ then $\deg(\bar{P})/2 \leq \deg(w_j)p^j \leq \deg(\bar{P})$.

Lemma 14 *Given a symmetric polynomial $P(\mathbf{X}) \in \mathbb{Z}_p(\mathbf{X})$ there is a unique polynomial $\bar{P}(w_0, \cdots, w_\ell)$ that computes the same function $w(\mathbf{X}) \to \mathbb{Z}_p$ and vice versa. This correspondence preserves the degree.*

PROOF: Given a symmetric multilinear polynomial $P(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ of degree d, write it as $P(\mathbf{X}) = \sum_{k \leq d} c_k S_k(\mathbf{X})$. On at 0-1 input $\mathbf{x}$, $S_k(\mathbf{x}) = \binom{w(\mathbf{x})}{k}$. By Lucas' Theorem

$$\binom{w(\mathbf{x})}{k} \equiv \prod_{i \leq \ell} \binom{w_i}{k_i} \bmod p$$

Further the polynomial $\prod_{i \leq \ell} \binom{w_i}{k_i}$ has degree $\sum_i k_i p^i = k$. Thus $P(\mathbf{X})$ computes the same function as

$$\bar{P}(w_0, \cdots, w_\ell) = \sum_{k=0}^{d} c_k \prod_{i \leq \ell} \binom{w_i}{k_i} \bmod p$$

and they have the same degree.

To prove the other direction, observe that the monomials $\prod_{i \leq \ell} \binom{w_i}{k_i}$ with $k_i \leq p-1$ form a basis for polynomials in $\mathbb{Z}_p[w_0, \cdots, w_\ell]$ with degree at most $p-1$ in each w_i. Further writing a polynomial in this basis does not change the degree as defined above. Let $k = \sum_i k_i p^i$ be the degree of the monomial $\prod_i \binom{w_i}{k_i}$. Hence given $\bar{P}(w_0, \cdots, w_\ell)$ with degree d, one can write

$$\bar{P}(w_0, \cdots, w_{\ell-1}) = \sum_{k=0}^{d} c_k \prod_{i < \ell} \binom{w_i}{k_i}$$

By Lucas' theorem, this computes the same function as the polynomial $P(\mathbf{X}) = \sum_{k \leq d} c_k S_k(\mathbf{X})$. □

For $w \in \{0, \cdots, n\}$, let $w = \sum_{i=0}^{\ell} u_i p^i = \sum_{j=0}^{k} v_j q^j$ denote the base p and base q expansions of w. For $\bar{P}(u_0, \cdots, u_\ell) \in \mathbb{Z}_p[u_0, \cdots, u_\ell]$ let $\bar{P}(w)$ denote the polynomial $\bar{P}$ applied to the base p expansion of w. As consequence of Lemma 14, to prove Theorem 10 it suffices to prove the following Proposition.

Proposition 15 *Let $\bar{P}(w) \in \mathbb{Z}_p[u_0, \cdots, u_\ell]$ and $\bar{Q}(w) \in \mathbb{Z}_q[v_0, \cdots, v_k]$ be polynomials such that*

$$\bar{P}(0) \equiv 1 \bmod p \text{ and } \bar{Q}(0) \equiv 1 \bmod q$$

For $1 \leq w \leq n$,

$$\bar{P}(w) \equiv 0 \bmod p \text{ or } \bar{Q}(w) \equiv 0 \bmod q$$

Further $\deg(\bar{P}) \cdot \deg(\bar{Q}) \geq \frac{n}{10}$.

PROOF: Let a denote the largest index such that $\deg(u_a) \geq 1$ in $\bar{P}$. This implies $\deg(\bar{P}) \geq p^a$ and $\bar{P}(w) = \bar{P}(u_0, \cdots, u_a)$. Similarly let b be the largest index so that $\deg(v_b) \geq 1$. Then $\deg(\bar{Q}) \geq q^b$ and $\bar{Q}(w) = \bar{Q}(v_0, \cdots, v_b)$. Hence $\deg(\bar{P}) \cdot \deg(\bar{Q}) \geq p^a q^b$. This proves the desired bound for $n < 10p^a q^b$. So we may assume that $n \geq 10p^a q^b$.

Also $n < p^{a+1}q^{b+1}$, since if $w = p^{a+1}q^{b+1} \leq n$, then $u_0, \cdots, u_a = 0$ and $v_0, \cdots, v_b = 0$ so

$$\bar{P}(p^{a+1}q^{b+1}) = \bar{P}(0, \cdots, 0) \equiv 1 \bmod p$$

$$\bar{Q}(p^{a+1}q^{b+1}) = \bar{Q}(0,\cdots,0) \equiv 1 \bmod p$$

which contradicts the hypothesis. Let $\hat{n} = \left\lfloor \frac{n}{p^a q^b} \right\rfloor < pq$.

Let us consider inputs of the form $w = yp^a q^b$ where $0 \leq y \leq \hat{n}$. Observe that this implies $u_0, \cdots, u_{a-1} = 0$ and $u_a \equiv yq^b \bmod p$. Similarly $v_0, \cdots, v_{b-1} = 0$ and $v_b \equiv yp^a \bmod q$. Define polynomials $R(Y) \in \mathbb{Z}_p[Y]$ as $R(Y) = \bar{P}(0,\cdots,0,Yq^b)$, and $S(Y) \in \mathbb{Z}_q[Y]$ as $S(Y) = \bar{Q}(0,\cdots,0,Yp^a)$. This implies $\deg(R) = \deg(u_a) \leq p-1$ and $\deg(S) = \deg(v_b) \leq q-1$. Note that

$$\begin{array}{lcll} R(0) \equiv 1 \bmod p & \text{and} & S(0) \equiv 1 \bmod q & \\ R(y) \equiv 0 \bmod p & \text{or} & S(y) \equiv 0 \bmod q & 1 \leq y \leq \hat{n} \end{array} \tag{15}$$

We define $A \subseteq \mathbb{Z}_p^*$ and $B \subseteq \mathbb{Z}_q^*$ to be the 0 sets of $R(Y)$ and $S(Y)$ respectively. By equation 15 A and B cover $[\hat{n}]$. So by Lemma 11,

$$(\deg(u_a)+1)(\deg(v_b)+1) \ \geq \ \hat{n}/2$$

Since $\deg(u_a), \deg(v_b) \geq 1$, this implies that $\deg(u_a) \cdot \deg(v_b) \ \geq \ \hat{n}/8$. Since $\deg(\bar{P}) \geq p^a \deg(u_a)$ and $\deg(\bar{Q}) \geq q^b \deg(v_b)$,

$$\deg(\bar{P}) \cdot \deg(\bar{Q}) \ \geq \ \frac{\hat{n}}{8} p^a q^b \ > \ \frac{1}{8}\frac{9n}{10} > \frac{n}{10}$$

The second inequality uses the fact that $n \geq 10p^a q^b$ hence $p^a q^b \left\lfloor \frac{n}{p^a q^b} \right\rfloor > \frac{9n}{10}$. □

5 Ramsey Graphs based on Set Intersections

The constructions of Frankl-Wilson, Alon and Grolmusz use a coloring scheme based on the size of set intersections. In this section we show that these can be constructed from certain polynomials that are closely related to OR polynomials. These polynomials are also used by Grolmusz [18] and Kutin [19] to give simple constructions of set systems with restricted intersections mod 6.

Definition 12 *The weight-n function W_n is a partial function defined on $\{0,1\}^m$ for $m \geq n$ as follows*

$$W_n(\mathbf{x}) = 0 \ \textit{ if } \ wt(\mathbf{x}) = n \qquad W_n(\mathbf{x}) = 1 \ \textit{ if } \ wt(\mathbf{x}) < n$$

The function is undefined for $wt(\mathbf{x}) \in [n+1,\cdots,m]$.

Note that W_n on n variables is simply the NAND function. We now define polynomial representations of W_m. We give an extension of Definition 2, a similar extension holds for Definition 4

Definition 13 *Polynomials $P(\mathbf{X}) \in \mathbb{Z}_p[\mathbf{X}]$ and $Q(\mathbf{X}) \in \mathbb{Z}_q[\mathbf{X}]$ represent the W_n function on m variables if*

$$\begin{array}{lcll} P(\mathbf{x}) \not\equiv 0 \bmod p & \textit{and} & Q(\mathbf{x}) \not\equiv 0 \bmod q & \textit{if } wt(\mathbf{x}) = n \\ P(\mathbf{x}) \equiv 0 \bmod p & \textit{or} & Q(\mathbf{x}) \equiv 0 \bmod q & \textit{if } wt(\mathbf{x}) < n \end{array}$$

The degree of the representation is $d = \max(\deg(P), \deg(Q))$.

Assume that $P(X_1,\cdots,X_m)$ and $Q(X_1,\cdots,X_m)$ represent W_n with degree d for some $m \geq n$. Define $\hat{P}(X_1,\cdots,X_n)$ and $\hat{Q}(X_1,\cdots,X_n)$ to be polynomial by substituting $1 - X_i$ for X_i when $i \leq n$ and setting $X_i = 0$ for $i \geq n$. It is easy to verify that $\hat{P}$ and $\hat{Q}$ represent OR on n variables with degree at most d. Further if P and Q were symmetric polynomials, then so are $\hat{P}$ and $\hat{Q}$. Thus lower bounds for OR representations imply lower bounds for W_n representations. In particular our lower bounds for OR representations rule out representations of W_n with symmetric polynomials of degree $o(\sqrt{n})$.

Conversely one can construct degree d representations of W_n from degree d symmetric polynomials representing OR on n variables. We do not know if a similar statement is true for asymmetric polynomials.

Lemma 16 *A degree d representation of OR on n variables using symmetric polynomials gives a degree d representation of W_n on n variables for all $m \geq n$,*

PROOF: Let $P(\mathbf{X}), Q(\mathbf{X})$ be symmetric polynomials of degree at most d on m variables that represent OR. Replace each X_i by $1 - X_i$ and multi-linearize. It is easy to show that the resulting polynomials $P'(\mathbf{X}), Q'(\mathbf{X})$ represent W_n on n variables. Further, they are symmetric multilinear polynomials of degree d, hence we can write them as

$$P'(X_1, \cdots, X_n) \;=\; \sum_{i \leq d} a_i S_i(X_1, \cdots, X_n) \qquad Q'(X_1, \cdots, X_n) \;=\; \sum_{i \leq d} b_i S_i(X_1, \cdots, X_n)$$

We obtain new polynomials P'' and Q'' by replacing $S_i(X_1, \cdots, X_n)$ by $S_i(X_1, \cdots, X_m)$.

$$P''(X_1, \cdots, X_m) \;=\; \sum_{i \leq d} a_i S_i(X_1, \cdots, X_m) \qquad Q''(X_1, \cdots, X_m) \;=\; \sum_{i \leq d} b_i S_i(X_1, \cdots, X_m)$$

Since the value of a symmetric function on a $0,1$-input depends only on the weight of the input, one can show that P'' and Q'' represent W_n on m variables. □

We can use the $O(\sqrt{n})$ OR representations to construct representations of W_n. We give a construction of explicit Ramsey graphs from representations of W_n.

```
Construction 2 Ramsey Graph $G(V,E)$ from representations of $W_n$.
– $V(G)$ consists of vectors $\mathbf{x} \in \{0,1\}^m$ of weight $n$.
– If $P(\mathbf{x} \cap \mathbf{y}) \equiv 0$, add $(\mathbf{x},\mathbf{y})$ to $E(G)$.
```

Theorem 17 *Given a degree d representation of the weight-n function on $\{0,1\}^m$, the graph G has $\binom{m}{n}$ vertices and $\alpha(G), \omega(G) \leq \binom{m}{\leq d}$.*

PROOF: Assume we have prime representation of W_n. We associate a polynomial $P_{\mathbf{v}}(\mathbf{X})$ with each vertex $\mathbf{v}$ so that $P_{\mathbf{v}}(\mathbf{u}) = P(\mathbf{v} \cap \mathbf{u})$. Given $\mathbf{v} = (v_1, \cdots, v_m)$, let $Y_i = 0$ if $v_i = 0$ and $Y_i = X_i$ if $v_i = 1$. Set $P_{\mathbf{v}}(\mathbf{X}) = P(Y_1, \cdots, Y_m)$ and multi-linearize. Using an argument like in Theorem 3, we can show that this gives a polynomial representation of G over $\mathbb{Z}_p$. Since the $P_{\mathbf{v}}(\mathbf{X})$s are multilinear polynomials of degree d, we get $\omega(G) \leq \binom{m}{\leq d}$. Similarly we bound $\alpha(G)$ by representing $\overline(G)$ over $\mathbb{Z}_q$.

For prime-power representations of OR, we can represent G and $\overline{G}$ over $\mathbb{Z}_{p^a}$ and get a similar bound. □

The OR representation of Equation 1 gives the following construction due to Alon [2]. Let $n = pq - 1, m = n^2$. The vertices are all subsets of $[m]$ of size n. Add $(\mathbf{x}, \mathbf{y})$ to $E(G)$ if $|\mathbf{x} \cap \mathbf{y}| \not\equiv -1 \bmod p$.

The OR representation of Equation 3 gives the Frankl-Wilson construction: Let $n = p^2 - 1, m = n^2$. The vertices are all subsets of $[m]$ of size n. Add edge $(\mathbf{x}, \mathbf{y})$ to $E(G)$ if $|\mathbf{x} \cap \mathbf{y}| \not\equiv -1 \bmod p$. This construction can be extended to $t \geq 2$ colors using the polynomials constructed in Equation 5.

Construction 3 Extending the Frankl-Wilson construction to t colors.
− Take $n = p^t - 1, m = p^{t+1}$. Vertices are all n subsets of m.
− Edges are colored $\{0, \cdots, t-1\}$. Edge $(\mathbf{x}, \mathbf{y})$ is given color $v_p(1 + |\mathbf{x} \cap \mathbf{y}|)$.

The OR representation of Equation 2 gives the following graph $G(V, E)$. Let $n = 2^k 3^\ell - 1, m = n^2$. The vertices are all subsets of $[m]$ of size n. Add $(\mathbf{x}, \mathbf{y})$ to $E(G)$ if $|\mathbf{x} \cap \mathbf{y}| \not\equiv -1 \bmod 2^k$. In fact the graph obtained is the same as Grolmusz. To show this, we first present his construction, following the simplified exposition of Grolmusz himself [18] and Kutin [19].
1) Let $n = 2^k 3^\ell - 1$. The BBR polynomials give the following representation of W_n.

$$P(\mathbf{X}) = \binom{\sum X_i}{2^k - 1}, \quad Q(\mathbf{X}) = \binom{\sum X_i}{3^\ell - 1}$$

Define $R(\mathbf{X}) \in \mathbb{Z}_6[\mathbf{X}]$ to be the polynomial obtained by combining these polynomials using the CRT. It follows that $R(\mathbf{x}) \equiv 1 \bmod 6$ when $wt(\mathbf{x}) = n$ and $R(\mathbf{x}$ is divisible by 2 or 3 when $wt(\mathbf{x}) < n$.
2) We can view $R(\mathbf{X})$ as an integer polynomial with coefficients in $\{0, \cdots, 5\}$. By repeating each monomial sufficiently many times, we can write

$$R(\mathbf{X}) = \sum_{\alpha} \prod_{i \in \alpha} X_i$$

The elements of the universe are the monomials. If α is repeated c times in $R(\mathbf{X})$, then there are c elements in the universe, one for each occurance of α. For each $\mathbf{x} \in \{0,1\}^m$ of weight n, the set $S(\mathbf{x})$ consists of monomials that evaluate to 1 on $\mathbf{x}$. One can verify that this system has restricted intersections mod 6 since $|S(\mathbf{x}) \cap S(\mathbf{y})| = R(\mathbf{x} \cap \mathbf{y})$.
3) The vertices of the graph H are the sets $S(\mathbf{x})$. We add edge $(S(\mathbf{x}), S(\mathbf{y}))$ if $|S(\mathbf{x}) \cap S(\mathbf{y})| \equiv 0 \bmod 2$.

We wish to show that this graph H is the same as the graph G constructed above. We identify $\mathbf{x} \in V(G)$ with $S(\mathbf{x}) \in V(H)$. In H, we add an edge between $S(\mathbf{x})$ and $S(\mathbf{y})$ if $R(\mathbf{x} \cap \mathbf{y}) \equiv 0 \bmod 2$. By the CRT, this implies that $P(\mathbf{x} \cap \mathbf{y}) \equiv 0 \bmod 2$. By Lucas' theorem, this happens if $wt(\mathbf{x} \cap \mathbf{y}) \not\equiv -1 \bmod 2^k$. But this is precisely when $(\mathbf{x}, \mathbf{y})$ is an edge of G.

This equivalence can also be seen from Kutin's construction [19]. While Grolmusz's set system construction is an important result, our approach seems to be simpler for the purpose of Ramsey graph construction. One can interpret the bounds on clique and independent set size as coming from an extension of the modular Ray-Chaudhuri-Wilson theorem to prime powers, which we prove below (Theorem 18).

5.1 Set Systems with restricted Intersections modulo Prime Powers

Definition 14 *A set system $\mathcal{F} = \{S_i\}$ on $[n]$ is said to have restricted intersections mod q if there exists $L \subset \mathbb{Z}_q$ so that $|S_i| \bmod q \notin L$ but $|S_i \cap S_j| \bmod q \in L$.*

For a fixed modulus q, we study the problem of how large $|\mathcal{F}|$ can be as a function of n. When $q = p$ is a prime, the non-uniform modular Ray-Chaudhuri Wilson theorem proved by Deza, Frankl and Singhi [5] gives a bound of

$$|\mathcal{F}| \le \binom{n}{\le |L|} \le \binom{n}{\le p - 1}$$

When q is not a prime power, Grolmusz shows a lower bound of $n^{\omega(1)}$ [17]. We give a near-tight bound of $\binom{n}{\le p^a - 1}$ for the prime power case. This improves the bound of $\binom{n}{\le 2^{|L| - 1}}$ due to Babai *et al.* [6]. Previously stronger bounds than ours were known for the special case when $|L| = p^a - 1$ i.e. when all set sizes are congruent to $k \mod p^a$ for some k (see theorems 5.30 and 7.18 in the book by Babai and Frankl [5]). To prove our result, we use the fact that every function from $\mathbb{Z}_{p^a}$ to $\mathbb{Z}_p$ can be written as a polynomial.

Theorem 18 *Let $\mathcal{F}$ be a set system with restricted intersections modulo p^a. Then $|\mathcal{F}| \leq \binom{n}{\leq p^a - 1}$.*

PROOF: We construct a univariate integer-valued polynomial $P(X) \in \mathbb{Q}[X]$ of degree $p^a - 1$ such that

$$P(x) \equiv \begin{cases} 1 \bmod p & x \bmod p^a \in L \\ 0 \bmod p & x \bmod p^a \notin L \end{cases}$$

By Lucas' theorem,

$$\begin{aligned} \binom{x}{p^a - 1} &\equiv \begin{cases} 1 \bmod p & x \equiv p^a - 1 \bmod p^a \\ 0 \bmod p & x \not\equiv p^a - 1 \bmod p^a \end{cases} \\ \Rightarrow \binom{x - \ell + p^a - 1}{p^a - 1} &\equiv \begin{cases} 1 \bmod p & x \equiv \ell \bmod p^a \\ 0 \bmod p & x \not\equiv \ell \bmod p^a \end{cases} \end{aligned}$$

$$\text{Set} \quad P(X) = \sum_{\ell \in L} \binom{X - \ell + p^a - 1}{p^a - 1}$$

By Lemma 3.1, of [6] this implies the desired bound. We sketch the argument below.

We will use $\mathbf{S_i}$ to denote the incidence vector of set S_i. Let $P_i(X_1, \cdots, X_n) = P(\sum_{j \in S_i} X_j)$ and multilinearize. It is easy to show that

$$P_i(\mathbf{S_j}) = P(|S_i \cap S_j|) \equiv \begin{cases} 1 \bmod p & i = j \\ 0 \bmod p & i \neq j \end{cases}$$

Using this one can show that the polynomials $P_i(\mathbf{X})$ are linearly independent over $\mathbb{Q}$. Since they are multilinear polynomials in n variables of degree $p^a - 1$, the bound follows. □

6 Discussion and Open Problems

Following the breakthrough of Barak *et al.* [8], the algebraic construction described here are no longer the best constructions known. However, the appeal of these constructions is their simplicity and elegance, together with the fact that they are very explicit. So we believe that it is important to resolve the question of whether this approach can beat the Frankl-Wilson bound. As we have seen, this problem is intimately linked to well-studied questions in complexity theory.

Lower Bounds for Asymmetric Polynomials:

The question of whether there are lower degree weak representations of the OR function mod 6 has been open for a while. This work raises the question of whether low degree OR representations exist for our definition. Better upper bounds would give better Ramsey graphs. Lower bounds for prime representations will imply lower bounds for weak representations mod 6. Prime-power representations are exciting from the lower bound viewpoint since they have not been studied previously and might turn out to be easier to work with. The $\Omega(\log n)$ lower bound of Barrington and Tardos citebar-tar applies to both kinds of representations.

Both our lower bounds for symmetric polynomials follow a similar scheme: we characterize the zero-sets of low-degree symmetric polynomials and then show that there is no good partition of the hypercube. A natural question is whether such a scheme could extend to the general case. The first step would be to give a of characterization of zero-sets of low degree polynomials. Motivated by this we pose the following problems:

1. Given $S \subseteq \{0,1\}^n \setminus \mathbf{0}$, let $\deg_p(S)$ denote the smallest degree of a polynomial in $\mathbb{Z}_p[\mathbf{X}]$ which is 0 at every point in S but not at the origin. Give a lower bound on $\deg_p(S)$.
2. Given $S \subset \{0,1\}^n$, let $\deg'_p(S)$ denote the smallest degree of a polynomial in $\mathbb{Z}_p[\mathbf{X}]$ which is 0 over S but not at every point in $\{0,1\}^n$. Give a lower bound on $\deg'_p(S)$.

Note that both these quantities are easy to compute, since they involve checking whether a system of equations is feasible. We are looking for a combinatorial lower bound, perhaps analogous to Lemma 6. The latter quantity $deg'_P(S)$ is closely related to the notion of *the degree of a subset* studied by Smolensky with a view towards proving circuit lower bounds [21]. The main difference is that he requires the zero-set to be exactly the set S.

Limitations to Constructions based on Distances:

We have shown that using symmetric polynomials in out construction, current techniques cannot give better bounds on $\alpha(G), \omega(G)$. Note that for the constructions of Alon, Frankl-Wilson and Grolmusz, this technique gives tight bounds.This raises the question: *do constructions based on symmetric polynomials contain either a large clique or independent set?*

Using a symmetric polynomial in our construction gives a graph where edges are added between vertices based on the Hamming distance between them. More formally, let $D \subset \{1, \cdots, n\}$. The graph $G(D)$ is defined as follows: The vertex set is $\{0,1\}^n$. We add $(\mathbf{x}, \mathbf{y})$ to E if $d(\mathbf{x}, \mathbf{y}) \in D$. Is it true that for every choice of D, $G(D)$ contains a large clique or independent set?

Similarly in Construction 2, symmetric polynomials give graphs where the vertices are sets and edges are added based on intersection sizes. Do such graphs always contain large cliques or independent sets?

Acknowledgments

I thank Dick Lipton for numerous interesting discussions on this subject. I thank Vince Grolmusz for comments on an early version. I also thank Boaz Barak, T.S. Jayram, Ravi Kumar, Anup Rao, Benny Sudakov, Prasad Tetali and Avi Wigderson for helpful comments.

References

[1] N. Alon, *Ramsey graphs cannot be defined by real polynomials*, Journal of Graph Theory 14, (1990), pp. 651–661.

[2] N. Alon, *The Shannon capacity of a union*, Combinatorica, 18(3) (1998), pp. 301–310.

[3] N. Alon and R. Beigel, *Lower bounds for approximations by low degree polynomials over $\mathbb{Z}_m$*, Proceedings of the 16^{th} IEEE Conference on Computational Complexity (CCC), (2001).

[4] N. Alon, J. Pach, R. Pinchasi, R. Rados, and M. Sharir, *Crossing patterns of semi-algebraic sets*, Journal of Combinatorial Theory Ser A 111, (2005), pp. 310–326.

[5] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics*, Preliminary version 2, 1992.

[6] L. Babai, P. Frankl, S. Kutin, and D. Stefankovic, *Set systems with restricted intersections modulo prime powers*, Journal of Combinatorial Theory, Ser. A, 95(1) (2001).

[7] B. Barak, *A simple explicit construction of an $n^{\tilde{o}(\log n)}$ Ramsey graph*, arXiv.org, math.CO/0601651, (2006).

[8] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson, *2-source dispersers for $n^{o(1)}$ entropy and Ramsey graphs beating the Frankl-Wilson construction*, in Proceedings of the 38^{th} Symposium on Theory of Computing (STOC), 2006.

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

[10] N. Bhatnagar, P. Gopalan, and R. J. Lipton, *Symmetric polynomials over $\mathbb{Z}_m$ and simultaneous communication protocols*, Proceedings of the 44^{th} Annual Symposium on the Foundations of Computer Science (FOCS), (2003).

[11] P. Erdős, *Some remarks on the theory of graphs*, Bulletin of the A. M. S., 53 (1947), pp. 292–294.

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

[13] P. Gopalan, *Constructing Ramsey graphs from Boolean function representations*, in Proceedings of the 21^{st} IEEE Conference on Computational Complexity (CCC), 2006.

[14] ———, *Query-efficient algorithms for polynomial interpolation over composites*, in Proceedings of the ACM-SIAM Symposium on Discrete algorithms (SODA), 2006.

[15] F. Green, *Complex Fourier technique for lower bounds on the mod-m degree*, Computational Complexity, 9 (2000), pp. 16–38.

[16] V. Grolmusz, *On the weak mod m representation of boolean functions*, Chicago Journal of Theoretical Computer Science, 2 (1995).

[17] ———, *Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs*, Combinatorica, 20 (2000), pp. 71–86.

[18] ———, *Constructing set systems with prescribed intersection sizes*, Journal of Algorithms, 44 (2002), pp. 321–337.

[19] S. Kutin, *Constructing large set systems with given intersection sizes modulo composite numbers*, Combinatorics, Probability and Computing, 11(5) (2002).

[20] M. Naor, *Constructing Ramsey graphs from small probability spaces*, Manuscript, available online, (1993).

[21] R. Smolensky, *On representations by low-degree polynomials*, in Proceedings of the 34^{th} Annual Symposium on Foundations of Computer Science (FOCS), 1993.

[22] G. Tardos and D. Barrington, *A lower bound on the mod 6 degree of the OR function*, Computational Complexity, 7 (1998), pp. 99–108.

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