On explicit Ramsey graphs and estimates of the number of sums and products

(preliminary version)

Pavel Pudlák*

April 4, 2005

1 Introduction

In finite combinatorics there are many proofs of the existence of certain combinatorial structures which do not provide us with any explicit example of such structures. To give an explicit construction is not only a mathematical challenge, but often it is the only way to determine the extremal structures for a particular question.

One of such problems is to give an explicit construction of a two-coloring of the complete bipartite graph $K_{N,N}$ such that no subgraph $K_{r,r}$ is monochromatic for some small r. It is well-known that there exist such colorings for $r = (2 + o(1)) \log_2 N$, but until recently explicit constructions were only known for $r \approx \sqrt{N}$. In 2004 Barak, Kindler, Shaltiel, Sudakov and Wigderson [1] found a polynomial construction of two-colorings of $K_{N,N}$ which leave no $K_{r,r}$ monochromatic for $r = N^{\varepsilon}$, where ε can be chosen arbitrarily small. Their result was a breakthrough not only in the field of Ramsey graphs, but they also succeeded in constructing extractors and other gadgets needed in derandomization with much better parameters.

However, their construction is very complicated and uses derandomization. Thus it seems reasonable to look for more explicit constructions even if they have worse parameters. In this paper we give a very explicit construction of a three-coloring of $K_{N,N}$ in which no $K_{r,r}$ is monochromatic for

*Supported by grnats IAA1019401 and 1M002162080

$r = N^{1/2-\varepsilon}$, and some constant $\varepsilon > 0$. We present some evidence why a similar construction should give a two-coloring with r of the same form. Our result is an application of the recently proved bounds on the number of sums and products in finite fields of Bourgain, Katz and Tao [2]. That result is also used in the main building block of the construction of Barak et al., but it is used in a different way.

Our construction possess a symmetry property which implies a slightly stronger result than stated above. We construct a three-coloring of K_N such that for some $\varepsilon > 0$ independent of N the coloring has the following property. There are no two subsets of vertices X and Y of size at least $N^{1/2-\varepsilon}$ (disjoint or not disjoint) such that all edges between X and Y have the same color.

2 The result

Let F be a field. Let $S \subseteq F^n$. We define a coloring γ of the complete bipartite graph $S' \times S''$, where $S' = \{1\} \times S$ and $S'' = \{2\} \times S$ by the formula

$$\gamma((1,u),(2,v)) = \langle u, v \rangle,$$

where $\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i$ is the scalar product in F. Thus if $N = |S|$ and $c = |F|$, γ is a coloring of $K_{N,N}$ by c colors. In [5] we proved the following simple proposition only for the two-element field, but the proof is completely general.

Proposition 1 *Suppose every vector space $V \subseteq F^n$ of dimension $\lfloor (n+1)/2 \rfloor$ intersects S in less than r elements, then no complete bipartite subgraph $K_{r,r}$ is monochromatic with respect to γ, ie., for no two subsets $A \subseteq S_1$, $B \subseteq S_2$, $|A| = |B| = r$ the value of $\gamma(a,b)$ is the same for all $a \in A$ and $b \in B$.*

We shall consider the following construction of S. Let $p > 2$ be a prime and $n = 2q$. Put

$$S_{p,q} = \{(x, x^2);\ x \in \mathbb{F}_{p^q}\}.$$

In order to define the coloring $\gamma_{p,q}$, think of $\mathbb{F}_{p^q}$ as a q-dimensional vector space over $\mathbb{F}_p$. Thus $S_{p,q} \subseteq \mathbb{F}_p^n$ and we can define $\gamma_{p,q}$ using the scalar product in F_p. Thus $\gamma_{p,q}$ is a coloring of $K_{N,N}$, $N = p^q$, by p colors.

Our main result is the following theorem.

Theorem 2 *For every prime $p > 2$ there exists $\varepsilon > 0$ such that for every sufficiently large prime q, the coloring $\gamma_{p,q}$ of $K_{N,N}$ has no monochromatic subgraph $K_{r,r}$ for $r > N^{1/2-\varepsilon}$.*

Let the field $\mathbb{F}_p$ be fixed for the proof of this theorem. The following is a finite field version of Theorem 1 of Elekes, Nathanson and Ruzsa [3] originally proved for the real numbers and every strictly convex function in place of x^2.

Lemma 3 *For every $\alpha > 0$ there exist $\varepsilon_0, \varepsilon_1 > 0$ such that for every sufficiently large prime q, every subset $S \subseteq S_{p,q}$ and every set $T \subseteq \mathbb{F}_p^{2q}$, if $p^{\alpha q} \leq |T| \leq p^{(2-\alpha)q}$ then*

$$|S + T| \geq \varepsilon_0 |S| \cdot |T|^{1/2+\varepsilon_1}.$$

We shall first prove the theorem using this lemma. Let V be a vector subspace of $\mathbb{F}_p^{2q}$ of dimension $q+1$. Put $S = S_{p,q} \cap V$ and $T = S + S$. Then $|T| \geq \binom{|S|+1}{2}$, since the pair $(x+y, x^2+y^2)$ uniquely determines the set $\{x, y\}$. We can apply the previous lemma to T, since $T \subseteq V$, hence $|T| \leq p^{q+1}$. According to the lemma we thus have

$$|S + S + S| \geq |S| \cdot \binom{|S|+1}{2}^{1/2+\varepsilon_1} \geq |S|^{2+\varepsilon_1}/2.$$

Hence the dimension of the vector space spanned by S is at least $\log_p(|S|^{2+\varepsilon_1}/2)$. This must be at most the dimension of V, hence

$$\log_p(|S|^{2+\varepsilon_1}/2) \leq q + 1,$$

from which we get

$$|S| \leq \left(2p^{q+1}\right)^{\frac{1}{2+\varepsilon_1}} \leq p^{(\frac{1}{2}-\varepsilon)q}$$

for some $\varepsilon > 0$. ∎

To prove Lemma 3 we shall use the following an estimate on the number of incidences of points and lines in a finite plane proved by Bourgain, Katz and Tao in [2] as Theorem 6.2.

Theorem 4 *Let $0 < \alpha < 2$, $0 < \beta < \alpha/2$. Then there exist constants $\varepsilon_2 > 0$ and C such that for every finite field F, set of points P and set of lines L in*

the projective plane over F, if $|P|, |L| \leq N = |F|^{\alpha}$ and F does not contain a subfield of size bigger than $|F|^{\beta}$, then

$$I_{P,L} \leq CN^{3/2-\varepsilon_2},$$

where $I_{P,L} = |\{(p,l) \in P \times L;\ p \in l\}|$ denotes the number of incidences.

In [2] the theorem is proven only for prime fields and a stronger statement which implies the theorem above is stated without a proof. However it is easy to verify the stronger statement by inspecting the proof in [2].

We shall need an estimate for the case when the number of lines and the number of points is different.

Corollary 5 *Let F, P, L be as above and $2\beta < \alpha' < \alpha$. If $|F|^{\alpha'} < |L| \leq |P|$, then*

$$I_{P,L} \leq C'|P| \cdot |L|^{\frac{1}{2}-\varepsilon_3},$$

where $\varepsilon_3 > 0$ and C' depend only on α, α' and β.

Proof. Let $P' \subseteq P$ be a random subset of P of size $|L|$. Then the expected value of the number of incidences $I_{P',L}$ is $I_{P,L}|L|/|P|$. Thus there exists P' such that $I_{P',L} \geq I_{P,L}|P'|/|P| = I_{P,L}|L|/|P|$. Applying the theorem to P' and L, we get

$$I_{P,L}|L|/|P| \leq I_{P',L} \leq C'|L|^{3/2-\varepsilon_3},$$

for some $\varepsilon_3 > 0$ and C', whence we get the statement of the corollary. ∎

Now we shall prove Lemma 3. Let $S \subseteq S_{p,q}$ and $T \subseteq \mathbb{F}_p^{2q}$ be given. Put $Q = \{S_{p,q} + t;\ t \in T\}$. We think of $S_{p,q}$ as a parabola in the afine plane and Q as the set of all shifts of this parabola by vectors $t \in T$. Put $P = S + T$. So P is a set of points on parabolas Q. We want to use the estimate on the number of incidences in Corollary 5. The corollary speaks only about sets of lines, but we can show that a suitable one-to-one transformation maps our parabolas on lines. This mapping is defined by $(u, v) \mapsto (u, v - u^2)$, and it maps the parabola $S_{p,q} + (a, b)$ onto the line

$$\{(x + a, 2ax - a^2 + b);\ x \in \mathbb{F}_{p^q}\}.$$

The number of incidences is $|S| \cdot |T|$, since we have $|T|$ parabolas in Q, and on each parabola $Q + t$ we have $|S|$ points, namely the points $S + t$. Thus by Corollary 5, we have

$$|S| \cdot |T| = I_{P,Q} \leq C'|P| \cdot |Q|^{\frac{1}{2}-\varepsilon_3} = C'|S + T| \cdot |T|^{\frac{1}{2}-\varepsilon_3},$$

whence Lemma 3 follows. ∎

Proposition 6 *For $p > 2$ prime and q arbitrary positive integer, $K_{N,N}$ colored by $\gamma_{p,q}$ contains a monochromatic subgraph $K_{r,r}$ for $r = \varepsilon_4 N^{1/4}$, for some $\varepsilon_4 > 0$.*

Proof. Represent the elements of $\mathbb{F}_{p^q}$ as polynomials modulo an irreducible polynomial of degree q over $\mathbb{F}_p$. Let A be the set of all polynomials of degree less than $q/4$ and let B be the set of all polynomials that have nonzero coefficients only at terms of degree n for $q/4 \leq n < q/2$. Then the polynomials that represent the squares of elements of A are the polynomials of degree less than $q/2$ and the polynomials that represent the squares of elements of B are the polynomials that have nonzero coefficients at terms of degree n for $q/2 \leq n < q$. Hence the scalar product of every pair $a \in A$ and $b \in B$ is zero. ∎

We do not know other monochromatic subgraphs $K_{r,r}$.

3 Conclusions

The most interesting open problem related to our result is whether we can get a two-coloring in such a way. If $p = 2$, then we cannot use $S_{p,q}$, because x^2 is a linear function in fields of characteristic 2, thus $S_{p,q}$ is a linear subspace and $\gamma_{2,q}$ is 0 for all edges. In [5] we proposed to use

$$\{(x, x^{-1});\ x \in \mathbb{F}_{2^q}\}, \quad \text{and} \quad \{(x, x^3);\ x \in \mathbb{F}_{2^q}\}.$$

We conjecture that the same statement as our Theorem 2 holds for $p = 2$ and the sets above. One could prove it in the same way if we had a generalization of the bound on the number of incidences of points and lines (Theorem 4) to hyperbolas and cubics. The corresponding result has been proven in the Euclidean plane for a much broader class of curves. Let us note that the graphs defined using the curve $y = x^3$ contain a monochromatic $K_{r,r}$ for $r = \varepsilon_5 N^{1/6}$, for some $\varepsilon_5 > 0$ (the proof is the same as in Proposition 6). For $y = x^{-1}$ we do not have any such result and we conjecture that they do not contain $K_{N^\varepsilon, N^\varepsilon}$ for any $\varepsilon > 0$.

The bound on the number of incidences in a finite plane is an application of the lower bound on the number of sums and products

$$|A+A|\cdot|A\cdot A|\geq\delta|A|^{2+\varepsilon}$$

for some constants $\delta,\varepsilon>0$, provided that A is not too small or too big in the finite field. (The first restriction has been removed in a paper of Konyagin [4] at least for prime fields.) This does not seem to be sufficient for proving the bound on the number of incidences with hyperbolas and cubics. For hyperbolas we rather need a bound

$$|A+A|\cdot|\{x^{-1}+y^{-1};\ x,y\in A\}|\geq\delta|A|^{2+\varepsilon},$$

and similarly for cubics.

We only note that for primes $p>2$ one can prove the corresponding statement for x^2.

Proposition 7 *Let $p>2$ be a prime, let $0<\beta<\alpha<1$. Then there exists an $\delta,\varepsilon>0$ such that for every sufficiently large prime q and every $A\subseteq\mathbb{F}_{p^q}$, if $p^{\beta q}\leq|A|\leq p^{\alpha q}$, then*

$$|A+A|\cdot|A^2+A^2|\geq\delta|A|^{2+\varepsilon}.$$

where $A^2+A^2=\{x^2+y^2;\ x,y\in A\}$.

Proof. We shall apply Corollary 3 in the same manner as we did in the proof of Theorem 2. Let $P=(A+A)\times(A^2+A^2)$ be a set of points. Let $Q=\{(x+a,x^2+b^2);\ a,b\in A\}$ be a set of parabolas. If $|P|$ is close to p^{2q}, then we are done. Otherwise we can apply Corollary 3. Notice that $\frac{1}{2}|A|^2\leq|Q|\leq|A|^2$, and the number of incidences between P and Q is $|A|\cdot|Q|$, since every parabola meets P in $|A|$ points. Thus

$$\frac{1}{2}|A|^3\leq I_{P,Q}\leq C'|P|\cdot|Q|^{1/2-\varepsilon_3}\leq C'|A+A|\cdot|A^2+A^2|\cdot(|A|^2)^{1/2-\varepsilon_3},$$

and we get the statement of the proposition. ∎

Acknowledgment. I would like to thank to Jiří Matoušek for explaining me a proof of Elekes and to Jiří Sgall for suggesting an idea for Proposition 6.

References

[1] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov and A. Wigderson, *Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors,* preprint, 2004.

[2] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications,* arXiv:math.NT/0304217 v1, 2003.

[3] G. Elekes, M. B. Nathanson and I. Z. Ruzsa, *Convexity and Sumsets.* J. of Number Theory **83**, (1999), 194-201.

[4] S. V. Konyagin, *A sum-product estimate in fields of prime order,* arXiv:math.CO/0301343 v2, 2003.

[5] P. Pudlák and V. Rödl, *Pseudorandom sets and explicit constructions of Ramsey graphs.* Quaderni di Matematica, Dipartimento di Matematica della SecondaUniversita di Napoli, 327-346.