Towards a Katona type proof for the 2-intersecting Erdős-Ko-Rado theorem

Ralph Howard*

Department of Mathematics, University of South Carolina
Columbia, SC 29208, USA
howard@math.sc.edu

Gyula Károlyi†

Department of Algebra and Number Theory, Eötvös University
1518 Budapest, Pf. 120, Hungary
karolyi@cs.elte.hu

László A. Székely‡

Department of Mathematics, University of South Carolina
Columbia, SC 29208, USA
szekely@math.sc.edu

Submitted: April 2, 2001; Accepted: October 9, 2001.
MR Subject Classifications: 05D05, 20B20, 11B25, 12L12

Abstract

We study the possibility of the existence of a Katona type proof for the Erdős-Ko-Rado theorem for 2- and 3-intersecting families of sets. An Erdős-Ko-Rado type theorem for 2-intersecting integer arithmetic progressions and a model theoretic argument show that such an approach works in the 2-intersecting case, at least for some values of n and k.

1 Introduction

One of the basic results in extremal set theory is the Erdős-Ko-Rado (EKR) theorem [8]: if $\mathcal{F}$ is an *intersecting* family of k-element subsets of an n-element set (i.e. every two

*The research of the first author was supported in part from ONR Grant N00014-90-J-1343 and ARPA-DEPSCoR Grant DAA04-96-1-0326.

†The research of the second author was supported in part by the Hungarian Scientific Research Grant contracts OTKA F030822 and T029759.

‡The research of the third author was supported in part by the Hungarian Scientific Research Grant contract T 016 358, and by the NSF contracts DMS 970 1211 and 007 2187.

members of $\mathcal{F}$ have at least one element in common) and $n \geq 2k$ then $|\mathcal{F}| \leq \binom{n-1}{k-1}$ and this bound is attained. A similar result holds for t-intersecting k-element subsets (Wilson, [11, 23]): if $n \geq (k-t+1)(t+1)$ and $\mathcal{F}$ is a t-intersecting family, then $|\mathcal{F}| \leq \binom{n-t}{k-t}$. The complete solution for other values of n, k, and t was discovered by Ahlswede and Khachatrian [1].

The simplest proof of the Erdős-Ko-Rado theorem is due to Katona [15]. This proof yields a stronger result, the Bollobás inequality, (Chapter 13 Theorem 2 in [4]), and pursuing such generalizations is the main motivation for the search of new Katona type proofs. We mention here a closely related result of Milner [20], which gives the maximum size of a t-intersecting Sperner system. Katona [17] and Scott [21] gave cycle permutation proofs to Milner's result for $t = 1$.

Péter Erdős, Faigle and Kern [9] came up with a general framework for group-theoretical proofs of Erdős-Ko-Rado type theorems and Bollobás type inequalities that generalizes the celebrated cyclic permutation proof of Katona for the classic Erdős-Ko-Rado theorem to a number of other structures. They explicitly asked for t-intersecting generalizations of their method. The present work was strongly motivated by their paper.

Katona type proofs are yet to be discovered for t-intersecting families of k-sets and for t-intersecting Sperner families, for which no Bollobás inequality is known. The present paper makes one step forward toward such extensions. We give a formal generalization of Katona's proof from the natural permutation group representation of the cyclic group to sharply t-transitive permutation groups. To make sure that the formal generalization actually works, an extra condition is needed. Then we study how this extra condition for the case $t = 2$, formulated for finite fields, can be stated for 2-intersecting integer arithmetic progressions, and then using the truth of the latter version, we show the existence of a Katona type proof for the case $t = 2$, for infinitely many pairs (n, k) by model theoretic arguments.

A permutation group acting on an n-element set is *t-transitive*, if any ordered t-set of vertices is mapped to any ordered t-set of vertices by a group element, and is *sharply t-transitive* if it can be done by a *unique* group element. Infinite families of sharply 2- and 3-transitive permutation groups exist, but only finitely many such groups exist for each $t \geq 4$. Moreover, only the symmetric and alternating groups have highly transitive $(t \geq 6)$ group actions. See [7] for details.

Sharply 2-transitive permutation groups do act on q vertices, where q is prime power, and they have been classified by Zassenhaus [24], see also [7]. One of those groups is the *affine linear group over $GF(q)$*, that is, the group of linear functions $f = ax + b : GF(q) \rightarrow GF(q)$ under composition with $a \neq 0$. In this paper we consider *this* sharply 2-transitive permutation group only.

The non-constant fractional linear transformations $x \rightarrow \frac{ax+b}{cx+d}$ $(a, b, c, d \in GF(q))$ form a group under composition and permute $GF(q) \cup \{\infty\}$ under the usual arithmetic rules and act sharply 3-transitively. Group elements fixing ∞ are exactly the linear transformations. No sharply 3-transitive permutation groups act on underlying sets with cardinality different from $q + 1$.

In Katona's original proof the action of a cyclic permutation group is sharply 1-

transitive. Katona needed an additional fact, which is often called Katona's Lemma. As a reminder, we recall Katona's Lemma in an algebraic disguise (cf. [19, Ex. 13.28(a)]):

Lemma 1 *Consider the cyclic group Z_n with generator g. Assume $k \leq n/2$, and let $K = \{g, g^2, \ldots, g^k\}$. If for distinct group elements $g_1, g_2, \ldots, g_m \in Z_n$ the sets $g_i(K)$ are pairwise intersecting, then $m \leq k$.* ♠

The major difficulty that we face is how to find analogues of Katona's Lemma for sharply 2- and 3-transitive permutation group actions.

2 Katona's proof revisited

Theorem 1 *Let us be given a sharply t-transitive permutation group Γ acting on a set X with $|X| = n$. Assume that there exists a $Y \subseteq X$ with $|Y| = k$ such that*

$$\text{for distinct group elements } \phi_1, \phi_2, \ldots, \phi_m \in \Gamma,$$

$$\text{if, for all } i, j,\ |\phi_i(Y) \cap \phi_j(Y)| \geq t, \text{ then } m \leq \tfrac{k!}{(k-t)!}. \tag{1}$$

Then, for any t-intersecting family $\mathcal{F}$ of k-subsets of X, $|\mathcal{F}| \leq \binom{n-t}{k-t}$.

Proof. Let us denote by S_n the set of all permutations of X. For $g \in S_n$, let $\chi_{g(Y)}$ be 0 or 1 according to $g(Y) \notin \mathcal{F}$ or $g(Y) \in \mathcal{F}$. We are going to count

$$\sum_{g \in S_n} \chi_{g(Y)} = \sum_{\phi\Gamma} \sum_{g \in \phi\Gamma} \chi_{g(Y)} \tag{2}$$

in two different ways (the sum $\sum_{\phi\Gamma}$ is over all cosets of Γ in G). There are $|\mathcal{F}|$ elements of $\mathcal{F}$ and each can be obtained in the form of $g(Y)$ for $k!(n-k)!$ elements $g \in S_n$. Hence

$$|\mathcal{F}|k!(n-k)! = \sum_{g \in S_n} \chi_{g(Y)}.$$

On the other hand, we have

$$\sum_{g \in \phi\Gamma} \chi_{g(Y)} \leq k!/(k-t)!,$$

since if $g_i = \phi h_i$ has the property that $g_i(Y) \in \mathcal{F}$, then for all i we have $h_i(Y) \in \{\phi^{-1}(F) : F \in \mathcal{F}\}$, and hence $\{h_i(Y) : i = 1, 2, \ldots, m\}$ is t-intersecting and condition (1) applies to it. We have the same upper bound for the summation over any coset. To count the number of cosets note that a sharply t-transitive permutation group acting on n elements has $n!/(n-t)!$ elements. By Lagrange's Theorem the number of cosets is $\frac{n!}{n!/(n-t)!} = (n-t)!$. Combining these observations we have

$$|\mathcal{F}|k!(n-k)! \leq (n-t)!k!/(k-t)!$$

and the theorem follows. ♠

Note that a cyclic permutation group on n elements acts sharply 1-transitively, and condition (1) is the conclusion of Lemma 1 in the usual presentations of Katona's proof in texts.

Theorem 1 can be strengthened slightly. Call a permutation group *r-regularly t-transitive* if any ordered t-set is mapped to any ordered t-set by precisely r group elements. Thus, a permutation group is 1-regularly t-transitive if and only if it is sharply t-transitive. If Γ has r-regularly t-transitive action, the conclusion of the theorem remains true if we replace the right hand side of the inequality in condition (1) by $\frac{rk!}{(k-t)!}$.

3 2-intersecting arithmetic progressions

Given a field $\mathbb{F}$, let us denote by $\mathbf{1}$, $\mathbf{2}$,..., $\mathbf{k}$ the field elements that we obtain by adding the multiplicative unit to itself repeatedly.

In order to apply Theorem 1 for the case $t = 2$ using the affine linear group, we tried $Y = \{\mathbf{1}, \mathbf{2}, ..., \mathbf{k}\}$, and needed the corresponding condition (1). We failed to verify directly condition (1) but we were led to the following conjecture:

Conjecture 1 *If $A_1, A_2, \ldots, A_m$ are k-term increasing arithmetic progressions of rational numbers, and any two of them have at least two elements in common, then $m \le \binom{k}{2}$.*

It is easy to see that Conjecture 1 is equivalent for rational, real and for integer arithmetic progressions, and therefore we freely interchange these versions. This conjecture is the best possible, as it is easily shown by the following example: take two distinct numbers, $x < y$, and for all $1 \le i < j \le k$ take an arithmetic progression where x is the i^{th} term and y is the j^{th} term. This conjecture is the rational version of condition (1) for $t = 2$ with $Y = \{1, 2, \ldots, k\}$. Take the linear functions $\phi_i(x) = a_i x + b_i$. If $\phi_i(Y)$ $(i \in I)$ is 2-intersecting, then $|I| \le 2\binom{k}{2} = k(k-1)$, since any arithmetic progression can be obtained in exactly two ways as an image of Y.

There is a deep result in number theory, the *Graham Conjecture* (now a theorem), which is relevant for us: If $1 \le a_1 < \cdots < a_n$ are integers, then $\max_{i,j} \dfrac{a_i}{\gcd(a_i, a_j)} \ge n$. The Graham Conjecture was first proved for n sufficiently large by Szegedy [22], and recently cases of equality were characterized for all n by Balasubramanian and Soundararajan [2], e. g., the sequence $a_i = i$ $(i = 1, 2, ..., n)$ meets this bound.

How many distinct differences can a set of pairwise 2-intersecting integer arithmetic progressions of length k have? The Graham Conjecture immediately implies that the answer is at most $k - 1$ differences. Indeed, assume that the distinct differences are $d_1, d_2, \ldots, d_l$. Consider two arithmetic progressions of length k, the first with difference d_i, the second with difference d_j. The distance of two consecutive intersection points of these two arithmetic progressions is exactly $\mathrm{lcm}(d_i, d_j)$. This distance, however, is at most $(k-1)d_i$ and likewise is at most $(k-1)d_j$. From here simple calculation yields

$$l \le \max_{i,j} \frac{d_i}{\gcd(d_i, d_j)} = \max_{i,j} \frac{\mathrm{lcm}(d_i, d_j)}{d_j} \le k - 1.$$

It is obvious that at most $k-1$ pairwise 2-intersecting length k integer arithmetic progressions can have the same difference. (The usual argument to prove Lemma 1 also yields this.) Therefore, instead of the conjectured $\binom{k}{2}$, we managed to prove $(k-1)^2$.

Ford has proven most of Conjecture 1 [10]:

Theorem 2 *Conjecture 1 holds if k is prime or $k > e^{10100}$.*

This opened up the way to the following argument which starts with the following straightforward lemmas. Their proofs are left to the reader.

Lemma 2 *Given a natural number k, the following statement $\Upsilon(k)$ can be expressed in the first-order language of fields:*

> *"The characteristic of the field $\mathbb{F}$ is zero or at least k , and for all $\phi_1, \phi_2, \ldots, \phi_{k(k-1)+1} : \mathbb{F} \to \mathbb{F}$ linear functions if $|\phi_u(\{\mathbf{1},\ \mathbf{2},\ldots,\ \mathbf{k}\}) \cap \phi_v(\{\mathbf{1},\ \mathbf{2},\ldots,\ \mathbf{k}\})| \geq 2$ for all $1 \leq u < v \leq k(k-1)+1$, then the $k(k-1)+1$ linear functions are not all distinct."* ♠

Lemma 3 *Let $\mathbb{F}$ be a field and $Y = \{a+\mathbf{1}b, a+\mathbf{2}b, \ldots, a+\mathbf{k}b\} \subset \mathbb{F}$ an arithmetic progression with k distinct elements. If Y has two elements in common with some subfield $\mathbb{K}$ of $\mathbb{F}$ then $Y \subset \mathbb{K}$.* ♠

Recall that if $\mathbb{F}$ is a field then the *prime field*, $\mathbb{P}$, of $\mathbb{F}$ is the smallest nontrivial subfield of $\mathbb{F}$. When the characteristic of $\mathbb{F}$ is a prime $p > 0$ then the prime field of $\mathbb{F}$ is $\mathbb{P} = GF(p)$, the finite field of order p. When the characteristic of $\mathbb{F}$ is 0 then the prime field is $\mathbb{P} = \mathbb{Q}$, the field of rational numbers. Note that the theory of fields of characteristic 0 is not finitely axiomatizable.

Lemma 4 *The statement $\Upsilon(k)$ is true in some field $\mathbb{F}$ if and only if it is true in the prime field $\mathbb{P}$ of $\mathbb{F}$.*

Proof. As $\mathbb{P}$ is a subfield of $\mathbb{F}$ it is clear that if $\Upsilon(k)$ is true in $\mathbb{F}$ then it is true in $\mathbb{P}$. Now assume that $\Upsilon(k)$ is true in $\mathbb{P}$. Let $\phi_1, \phi_2, \ldots, \phi_{k(k-1)+1} : \mathbb{F} \to \mathbb{F}$ be linear functions such that for $Y_0 = \{\mathbf{1},\ \mathbf{2},\ldots,\ \mathbf{k}\}$, $\mathcal{F} = \{\phi_u(Y_0) : 1 \leq u \leq k(k-1)+1\}$ is a 2-intersecting family of sets. If $\phi_u^* := \phi_1^{-1}\phi_u$ for $u = 1, \ldots, k(k-1)+1$ then $\phi_1^* = \phi_1^{-1}\phi_1 = \mathrm{Id}$ is the identity map and $\mathcal{F}^* = \{\phi_u^*(Y_0) : 1 \leq u \leq k(k-1)+1\}$ is also a 2-intersecting family of sets. Also $\phi_1^*(Y_0) = \{\mathbf{1},\mathbf{2},\ldots,\mathbf{k}\} \subset \mathbb{P}$. As $\mathcal{F}^*$ is 2-intersecting each of the arithmetic progressions $\phi_u^*(Y_0)$ will have at least two elements in $\mathbb{P}$. Therefore by Lemma 3 $\phi_u^*(Y_0) \subset \mathbb{P}$. If $\phi_u^*(x) = a_u x + b_u$ then $\phi_u^*(Y_0) \subset \mathbb{P}$ implies $a_u, b_u \in \mathbb{P}$ and so $\phi_u^* : \mathbb{P} \to \mathbb{P}$. As $\Upsilon(k)$ is true in $\mathbb{P}$ this implies there are $u \neq v$ with $\phi_u^* = \phi_v^*$. But this implies $\phi_u = \phi_v$ and so $\Upsilon(k)$ is true in $\mathbb{F}$. This completes the proof. ♠

Theorem 3 *Let k be a fixed positive integer for which Conjecture 1 holds. For every power $n = p^l$ of any prime $p \geq p_0(k)$, condition (1) holds with $Y = \{\mathbf{1},\ \mathbf{2},\ldots,\ \mathbf{k}\}$ and $t = 2$ for the affine linear group over $GF(n)$. Therefore Theorem 1 gives for these values of n and k a Katona type proof for the 2-intersecting Erdős-Ko-Rado theorem. This is true in particular if k is a prime or $k > e^{10100}$.*

Proof. Observe first that for $t = 2$ with the choice of the affine linear group and $Y = \{\mathbf{1}, \mathbf{2}, \ldots, \mathbf{k}\}$, $\Upsilon(k)$ is exactly the condition (1) of Theorem 1. Also observe that the validity of Conjecture 1 for k is exactly the truth of $\Upsilon(k)$ for the field $\mathbb{Q}$. Now we are going to show, that for any fixed k, $\Upsilon(k)$ is true for all fields of characteristic p except for finitely many primes. Assume that there are infinitely many primes, which are characteristics of fields which provide counterexamples to $\Upsilon(k)$.

The proof uses the following well-known fact: If a first-order statement is true for fields of arbitrary large characteristic, then it is true for some field $\mathbb{F}$ of characteristic zero (cf. [Cor 2.1.10][5].)

By Lemma 4 this implies $\Upsilon(k)$ is false in the prime field of $\mathbb{F}$ which is the rational numbers $\mathbb{Q}$. This contradicts the assumption on k and thus completes the proof. ♠

4 Comments and open problems

It is not impossible to obtain an effective bound $p_0(k)$ in Theorem 3. Using a *rectification principle*, due to Bilu, Lev and Ruzsa [3], we obtained $p_0(k) = 2^{4(k-1)^3}$, which was improved by Gábor Tardos (personal communication) to $p_0(k) = 6k^3$.

Is the 3-intersection version of Conjecture 1 true? This would yield a Katona type proof for the Erdős-Ko-Rado theorem for $t = 3$.

Conjecture 2 *If $A_1, A_2, \ldots, A_m$ are images of the set $\{1, 2, \ldots, k\}$ under distinct non-constant fractional linear transformations with rational coefficients $x \to \frac{a_i x + b_i}{c_i x + d_i}$ ($i = 1, 2, \ldots, m$), such that $|A_i \cap A_j| \geq 3$ for all i, j, then $m \leq k(k-1)(k-2)$.*

This conjecture is the best possible, as it is easily shown by the following example: take any three distinct numbers, $x < y < z$, and for each ordered 3-set (i, j, k), $1 \leq i, j, l \leq k$, take the (unique) non-constant fractional linear transformation which maps i to x, j to y and l to z.

Others think about Katona's cyclic permutation method in a different way [18]. Their understanding is that a variant of the theorem can easily be shown in a special setting, and then a double counting argument transfers the special result to the theorem. We acknowledge that the proof of Theorem 1 can be written in this way, and one can avoid using groups.

One might ask: why is then the big fuss with groups? The answer is: we would hardly find our results presented here without using groups. Furthermore, in a forthcoming joint paper with Márió Szegedy we further justify the use of groups, showing that Katona type proofs in the group theoretic setting are more of a rule than an exception.

Acknowledgement. We are indebted to Dominique de Caen, Éva Czabarka, and Péter Erdős for conversations on the topic of this paper. We are also indebted to an anonymous referee for a careful reading of the manuscript and valuable comments.

References

[1] R. Ahlswede, L. Khachatrian, The Complete Intersection Theorem for systems of finite sets, Europ. J. Comb. 18 (1997), 125–136.

[2] B. Balasubramanian, K. Soundararajan, On a conjecture of R. L. Graham, Acta Arithm. LXXV (1996)(1), 1–38.

[3] Y. F. Bilu, V. F. Lev, and I. Z. Ruzsa, Rectification principles in additive number theory, Discrete Comput. Geom. 19 (1998), 343–353.

[4] B. Bollobás, Combinatorics: Set families, Hypergraphs, Families of vectors, and Combinatorial probability, Cambridge University Press, 1986.

[5] C. C. Chang, H. J. Keisler, Model Theory, North-Holland Publ. Co., Amsterdam–London, 1973.

[6] M. Deza, P. Frankl, Erdős-Ko-Rado theorem – 22 years later, SIAM J. Alg. Disc. Methods 4 (1983), 419–431.

[7] J. D. Dixon, B. Mortimer, Permutation Groups, Springer-Verlag, 1996.

[8] P. Erdős, C. Ko, R. Rado, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. 2 12 (1961), 313–318.

[9] P. L. Erdős, U. Faigle, W. Kern, A group-theoretic setting for some intersecting Sperner families, Combinatorics, Probability and Computing 1 (1992), 323–334.

[10] K. Ford, Maximal collections of intersecting arithmetic progressions, manuscript.

[11] P. Frankl, The EKR theorem is true for $n = ckt$, Coll. Soc. Math. Bolyai 18, 365–375, North-Holland, 1978.

[12] P. Frankl, On intersecting families of finite sets, J. Combin. Theory Ser. A 24 (1978), 146–161.

[13] P. Frankl, The shifting technique in extremal set theory, in: Combinatorial Surveys (C. Whitehead, ed.), Cambridge Univ. Press, London/New York, 1987, 81–110.

[14] Z. Füredi, Turán type problems, in: Surveys in Combinatorics (Proc. of the 13th British Combinatorial Conference, A. D. Keedwell, Ed.), Cambridge Univ. Press, London Math. Soc. Lecture Note Series 166 (1991), 253–300.

[15] G. O. H. Katona, A simple proof of the Erdős-Chao Ko-Rado theorem, J. Combinatorial Theory Ser. B 13 (1972), 183–184.

[16] G. O. H. Katona, Extremal problems for hypergraphs, in: Combinatorics (M. Hall Jr., J. H. van Lint, eds.), D. Reidel Publishing Co., Dordrecht–Boston, 1975, 215–244.

[17] G. O. H. Katona, A simple proof to a theorem of Milner, J. Comb. Theory A 83 (1998), 138–140.

[18] G. O. H. Katona, The cycle method and its limits, in: Numbers, Information and Complexity (I. Althöfer, N. Cai, G. Dueck, L. Khachatrian, M. S. Pinsker, A. Sárközy, I. Wegener, Z. Zhang, eds.), Kluwer Academic Publishers, 2000, 129–141.

[19] L. Lovász, Combinatorial problems and exercises, North-Holland Publishing Co., Amsterdam–New York 1979.

[20] E. C. Milner, A combinatorial theorem on systems of sets, J. London Math. Soc. 43 (1968), 204–206.

[21] A. D. Scott, Another simple proof to a theorem of Milner, J. Comb. Theory A 87 (1999), 379–380.

[22] M. Szegedy, The solution of Graham's greatest common divisor problem, Combinatorica 6 (1986), 67–71.

[23] R. M. Wilson: The exact bound in the Erdős-Ko-Rado theorem, Combinatorica 4 (1984), 247–257.

[24] H. Zassenhaus, Über endliche Fastkörper, Abh. Math. Sem. Univ. Hamburg 11 (1936), 187–220.