Families Intersecting on an Interval

Paul A. Russell[*†]

October 10, 2006

Abstract

We shall be interested in the following Erdős-Ko-Rado-type question. Fix some set $B \subset [n]$. How large a family $\mathcal{A} \subset \mathcal{P}[n]$ can we find such that the intersection of any two sets in $\mathcal{A}$ contains a cyclic translate (modulo n) of B? Chung, Graham, Frankl and Shearer have proved that, in the case where B is a block of length t, we can do no better than to take $\mathcal{A}$ to consist of all supersets of B. We give an alternative proof of this result, which is in a certain sense more 'direct'.

1 Introduction

Many questions in extremal combinatorics concern the pairwise intersections of families of subsets of a finite set. For example. how large a family $\mathcal{A} \subset [n]^{(r)} = \{A \subset [n] : |A| = r\}$ can we find with $A \cap B \neq \emptyset$ for all $A, B \in \mathcal{A}$? This question was answered in the seminal paper of Erdős, Ko and Rado [2]: for $r \leq n/2$, we can do no better than to take $\mathcal{A}$ to be the collection of all r-sets containing some fixed element of $[n]$. (We note in passing that the question is of no interest for $r > n/2$ as then the entire family $[n]^{(r)}$ is intersecting.)

Since the publication of [2], the field has rapidly expanded and is now rich in interesting problems, many of which remain unsolved. Several such problems arise when we endow the ground-set with some sort of structure. The question we shall be interested in here is the following. Fix some set $B \subset [n]$. How large a family $\mathcal{A} \subset \mathcal{P}[n]$ can we find such that the intersection of any two sets in $\mathcal{A}$ contains a cyclic translate (modulo n) of B? It is conjectured by Chung, Graham, Frankl and Shearer [1] that a kernel system is again best; they are able to establish their conjecture in the case where B is a block of length t:

Theorem 1 ([1]). *Let n and t be positive integers with $t \leq n$, and let $\mathcal{A}$ be a family of subsets of $[n]$ such that whenever we take A, $A' \in \mathcal{A}$ then $A \cap A'$ contains some cyclic translate (modulo n) of the set $[t]$. Then $|A| \leq 2^{n-t}$.*

The aim of this paper is to give an alternative proof of this theorem. As we remark below, it is sufficient to consider instead the problem of finding the largest possible family of subsets on $[n]$ with any two *agreeing* on some cyclic translate of the set $[t]$. The original proof of Theorem 1 in [1] proceeds in two

*Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, England.

†`P.A.Russell@dpmms.cam.ac.uk`

stages. First, the authors show that, for $t < n \leq 2t$, if $\mathcal{A}$ is a family of subsets of $[n]$ with any two agreeing on some cyclic translate of $[t]$ *either* modulo n *or* modulo $n-1$ then $|\mathcal{A}| \leq 2^{n-t}$. They then apply this result to prove the theorem in general, working in the Abelian group $(\mathcal{P}[n], \triangle)$ and applying a partitioning argument. Here, $\triangle$ denotes the symmetric difference operation on the power set $\mathcal{P}[n]$ of $[n]$, i.e. for A, $B \subset [n]$, we define

$$A \triangle B = \{x \in A : x \notin B\} \cup \{x \in B : x \notin A\}.$$

We again work in the group $(\mathcal{P}[n], \triangle)$. However, instead of going via a preliminary result, in our proof we show *directly* that $\mathcal{P}[n]$ can be partitioned into 2^{n-t} parts in such a way that no two distinct sets in the same part agree on any cyclic translate of $[t]$ modulo n.

2 Algebraic methods

In this section, we remind the reader of a certain general method for bringing algebraic methods to bear on this sort of problem. Our problem comes from the general class of problems of the following form:

> Suppose $\mathcal{B}$ is some fixed family of subsets of $[n] = \{1, 2, \ldots, n\}$. How large can we make a family $\mathcal{A}$ of subsets of $[n]$ subject to the condition that for all A, $A' \in \mathcal{A}$, there is some $B \in \mathcal{B}$ with $B \subset A \cap A'$?

We denote by $v(\mathcal{B})$ the maximal size of a family $\mathcal{A}$ with this property. Note that the above problems on graphs and arithmetic progressions also fall into this class.

Unfortunately, the set $\mathcal{P}[n]$ does not seem to posess any useful algebraic structure under the intersection operation $\cap$. However, when endowed instead with the symmetric difference operation $\triangle$, the set $\mathcal{P}[n]$ becomes an Abelian group. This leads one to consider a modified version of the problem, where we insist only that any two sets in $\mathcal{A}$ *agree* on some set in $\mathcal{B}$:

> Suppose $\mathcal{B}$ is some fixed family of subsets of $[n] = \{1, 2, \ldots, n\}$. How large can we make a family $\mathcal{A}$ of subsets of $[n]$ subject to the condition that for all A, $A' \in \mathcal{A}$, there is some $B \in \mathcal{B}$ with $B \subset [n] - (A \triangle A')$?

We denote by $\bar{v}(\mathcal{B})$ the maximal size of a family $\mathcal{A}$ with this property.

It is clear that for any family $\mathcal{B}$ we have $v(\mathcal{B}) \leq \bar{v}(\mathcal{B})$. In particular, if a kernel family is best for the modified problem then the same must also be true for the original problem. Remarkably, it was proved by Chung, Graham, Frankl and Shearer that *equality* always holds. This is reassuring, as it means that we know it is always sufficient to attack the modified problem—a solution to this modified problem will instantly give a solution to the original problem.

Theorem 2 ([1]). *Let $\mathcal{B}$ be a family of subsets of $[n]$. Then $v(\mathcal{B}) = \overline{v}(\mathcal{B})$.*

Let us now explain the algebraic idea. As we have already mentioned, an important advantage of considering our problem in the modified form above is that, under the operation $\triangle$, $\mathcal{P}[n]$ forms an Abelian group, and the condition

$B \subset [n] - (A \triangle A')$ is equivalent to $(A \triangle A') \cap B = \emptyset$. Now, assume every set in $\mathcal{B}$ has size t. Then we know that $v(\mathcal{B}) \geq 2^{n-t}$ (by considering a kernel system). Suppose now that we manage to find some subgroup $G \leq \mathcal{P}[n]$ of order 2^t such that every non-zero set in G intersects every set in $\mathcal{B}$. Then, given $g \in \mathcal{P}[n]$ and h, $h' \in G$, we have the set $(g \triangle h) \triangle (g \triangle h') = h \triangle h'$ intersecting every set in $\mathcal{B}$ unless $h \triangle h' = \emptyset$, i.e. unless $h = h'$. So any family $\mathcal{A}$ satisfying the condition that for all A, $A' \in \mathcal{A}$ there is some $B \in \mathcal{B}$ with $B \subset [n] - (A \triangle A')$ can contain at most one element from each coset of G. We may then deduce immediately that $\bar{v}(\mathcal{B}) \leq 2^{n-t}$ and hence that $v(\mathcal{B}) = 2^{n-t}$.

This approach has been used for example by Griggs and Walker [4] to show that if $\mathcal{B}$ consists of all ordinary translates (rather than cyclic translates) of a fixed set of order t then $v(B) = 2^{n-t}$, and by Füredi, Griggs, Holzman and Kleitman [3] to show that if $\mathcal{B}$ consists of all *cyclic* translates of a fixed set of order 3 then $v(\mathcal{B}) = 2^{n-3}$.

In the following section, we apply the method to the case where $\mathcal{B}$ consists of all cyclic translates of a block of length t, hence producing a new proof of Theorem 1. The work comes in finding a suitable subgroup G, which in general seems far from obvious.

3 Cyclic translates of a block

We now proceed to our proof of Theorem 1. In view of the preceding section, it is enough to find a subgroup G of $(\mathcal{P}[n], \triangle)$ of order 2^t with every non-zero element of G intersecting every block of order t. We shall define the group G by giving a list g_1, g_2, $\ldots$, g_t of t generators. For $1 \leq i, j \leq t$, we shall insist that $i \in g_j$ if and only if $i = j$. This ensures that all of the sums $\sum_{i \in I} g_i$ $(I \subset [t])$ are distinct, and hence that $|G| = 2^t$.

We begin by considering a number of special cases, beginning with cases where it is easy to construct the subgroup G and building up to progressively more complicated cases. We hope that this will give the reader some feel for the construction before we come to the (fairly complicated) construction of G in general.

The simplest case of all is where $t|n$. Then simply take

$$g_i = \{x \in [n] : x \equiv i \pmod{t}\}.$$

It is clear that each g_i intersects each block of length t. Moreover, the g_i are pairwise disjoint. Hence any non-zero element of G contains some g_i, and so intersects every block of length t.

Suppose instead $n \equiv 1 \pmod{t}$, say $n = qt + 1$. Then we can take

$$g_i = \{x \in [n] : x \equiv i \pmod{t} \text{ or } x = n\}.$$

By the same reasoning as above, every non-zero $g \in G$ intersects every block of length t which is contained entirely within $[n-1]$. Can some g fail to intersect some block B of length t with $n \in B$? If so then $n \notin g$, and so $g = \sum_{i \in I} g_i$ for some non-empty $I \subset [t]$ of *even* order. In particular, $|I| \geq 2$. Let $i = \min I$ and $j = \max I$. Then B must contain at least one of i and $(q-1)t + j$ (as $(n+i) - ((q-1)t + j) = t + 1 + i - j \leq t$), and both of these points are in g, a contradiction.

More generally, if $n \equiv r \pmod t$ for some $r|t$, say $n = qt + r$, then we may take

$$g_i = \{x \in [n] : x \equiv i \pmod t \text{ or } (x > n - r \text{ and } x \equiv i \pmod r)\}.$$

The proof that each non-zero g intersects each block of length t is very similar to the previous case. The only time when things could conceivably go wrong is if $g = \sum_{i \in I} g_i$ for some $I \subset [t]$ containing distinct a and b with $a \equiv b \pmod r$. But then letting i and j be the least and greatest elements of I congruent to a modulo t, we have i, $(q-1)t + j \in g$ and $(n+i) - ((q-1)t + j) = t + r + i - j \leq t$ and we are done.

The final special case we consider is where $n \equiv r \pmod t$ for some $r \nmid t$, say $n = qt + r$, but with $t \equiv r' \pmod r$ for some $r'|r$. For $i \leq t - r'$ we set

$$g_i = \{x \in [n] : x \equiv i \pmod t \text{ or } (x > qt \text{ and } x - qt \equiv i \pmod r)\}$$

while for $i > t - r'$ we set

$$\{x \in [n] : x \equiv i \pmod t \text{ or } (x > qt \text{ and } x - qt \equiv i \pmod{r'})\}.$$

Again, the $g_i \cap [n - r]$ for $i \in [t]$ are pairwise disjoint, and things can only go wrong if $g = \sum_{i \in I} g_i$ for some $I \subset [t]$ containing distinct i, j with $g_i \cap g_j \neq \emptyset$. There are two ways that this can happen. The first is if I contains $i \neq j$ with $i \equiv j \pmod r$, but we can deal with this case as in the previous paragraph. The other possibility is if I contains $i \leq t - r' < j$ with $i \equiv j \pmod{r'}$. Let l be the least positive residue of i modulo r, and assume that i is chosen so as to minimize l. We may assume $l > r'$, as otherwise we would have $i \equiv j \pmod r$ which was dealt with in our first case. So g contains each of the points i and $qt + l - r'$, and $n + i - (qt + l - r') = (i - l) + r + r' \leq (t - r - r') + r + r' = t$ so we are done.

We now proceed to define the group G for general n and t. The construction can be thought of as an iteration of ideas similar to those used above.

Let n, t be positive integers with $t \leq n$. We apply Euclid's algorithm to n and t, thus obtaining

$$\begin{aligned} n &= q_1 t + r_1 \\ t &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{i-2} &= q_i r_{i-1} + r_i \\ &\vdots \\ r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} &= q_k r_{k-1}, \end{aligned}$$

where $t > r_1 > r_2 > \cdots > r_{k-1} > 0$.

Observe that for k odd we have

$$\begin{aligned} n &= q_1 t + q_3 r_2 + q_5 r_4 + \cdots + q_k r_{k-1} \\ t &= q_2 r_1 + q_4 r_3 + q_6 r_5 + \cdots + q_{k-1} r_{k-2} + r_{k-1} \end{aligned}$$

while for k even we have

$$\begin{aligned} n &= q_1 t + q_3 r_2 + q_5 r_4 + \cdots + q_{k-1} r_{k-2} + r_{k-1} \\ t &= q_2 r_1 + q_4 r_3 + q_6 r_5 + \cdots + q_k r_{k-1}. \end{aligned}$$

We define the *partial sums* of n by

$$n_m = q_1 t + q_3 r_2 + \cdots + q_{2m-1} r_{2m-2}$$

and of t by

$$t_m = q_2 r_1 + q_4 r_3 + \cdots + q_{2m} r_{2m-1},$$

where in each case we allow m to take any value for which the above expressions make sense. We interpret $n_0 = t_0 = 0$ and $n_1 = q_1 t$. It will sometimes be convenient to write $r_0 = t$ and $r_k = 0$. Observe that we have $n = n_m + r_{2m-1}$ and $t = t_m + r_{2m}$ for each m.

Fix i with $1 \le i \le t$. We define g_i in terms of its intersections with the intervals $(n_{j-1}, n_j]$. Take a maximal with $t_a < i$. Now, for $0 \le j \le a$, we set

$$g_i^{(j)} = \{x \in (n_j, n_{j+1}] : x - n_j \equiv i - t_j \pmod{r_{2j}}\}.$$

So in particular, we have

$$g_i^{(0)} = \{1 \le x \le n - r_1 : x \equiv i \pmod{t}\}.$$

Define also

$$g_i^{(a+1)} = \begin{cases} \{n_{a+1} + [i - t_a]_{r_{2a+1}}\} & \text{if } k \ne 2a+1 \\ \emptyset & \text{if } k = 2a+1 \end{cases},$$

where $[y]_z$ denotes the least strictly positive residue of y modulo z. Now, set $g_i = \bigcup_{j=0}^{a+1} g_i^{(j)}$. We define $G_{n,t}$ to be the subgroup of $\mathcal{P}[n]$ generated by g_1, g_2, …, g_t. Observe that in the cases $k = 1$, 2, 3, this reduces to our earlier definitions.

Lemma 3. *Let n and t be positive integers with $t \le n$, and define $G_{n,t}$ as above. Then*

(i) $|G_{n,t}| = 2^t$; and

(ii) every non-zero element of $G_{n,t}$ intersects every cyclic translate modulo n of $[t]$.

Proof. (i) is trivial—observe, for example, that if $1 \le s, u \le t$ then $u \in g_s$ if and only if $s = u$.

(ii) Let $0 \ne g \in G_{n,t}$. It is enough to show that we can find x_1, x_2, …, $x_m \in g$ with $x_1 < x_2 < \cdots < x_m$ satisfying $x_{i+1} - x_i \le t$ for $i = 1, 2, \ldots, m-1$ and $x_1 + n - x_m \le t$.

Suppose first that $g = g_i$ for some i with $1 \le i \le t$. Then g contains every $x \in [n]$ with $x \equiv i \pmod{t}$, so it is enough to show that if we take $x_1 = \min g$ and $x_m = \max g$ then $x_1 + n - x_m \le t$. Now, clearly $x_1 = i$. What is x_m?

Take a maximal with $t_a < i$. If $k \neq 2a+1$ then we must have $x_m = n_{a+1} + [i - t_a]_{r_{2a+1}}$. Now, $i - t_a \leq t_{a+1} - t_a = q_{2a+2} r_{2a+1}$ and so $(i - t_a) - [i - t_a]_{r_{2a+1}} \leq (q_{2a+2} - 1) r_{2a+1}$. Hence

$$\begin{aligned} x_1 + n - x_m &= i + n - (n_{a+1} + [i - t_a]_{r_{2a+1}}) \\ &= (i - [i - t_a]_{r_{2a+1}}) + (n - n_{a+1}) \\ &\leq ((q_{2a+2} - 1) r_{2a+1} + t_a) + r_{2a+1} \\ &= t_a + q_{2a+2} r_{2a+1} \\ &\leq t_a + r_{2a} = t. \end{aligned}$$

On the other hand, if $k = 2a+1$ then, since $i - t_a \leq t - t_a = r_{2a}$, we have $x_m = n_{a+1} - r_{2a} + i - t_a = n - r_{2a} + i - t_a$. Hence $x_1 + n - x_m = i + r_{2a} - i + t_a = t$.

Now, in general, we can write $g = \sum_{i \in I} g_i$ for some non-empty $I \subset [n]$. If the g_i $(i \in I)$ are pairwise disjoint, then pick some $i \in I$. We know that $g_i \subset g$ and that g_i intersects every block of length t. So g also intersects every block of length t.

So we may assume that there exist distinct $i, j \in I$ such that $g_i \cap g_j \neq \emptyset$. Pick $i, j \in I$ with $i < j$ such that $y \in g_i \cap g_j$, where y is the least positive integer which lies in at least two of the g_i $(i \in I)$. We take $x_1 = i$ and $x_2 < \cdots < x_m$ to be the elements of $g_j \cap [y-1]$. As g_j intersects every block of length t, it is enough to check that $n + i - x_m \leq t$.

Take b maximal such that $n_b < y$. Suppose first that $j \leq t_b$. Then, as $y \in g_j$, we must have $j > t_{b-1}$ and $y = n_b + [j - t_{b-1}]_{r_{2b-1}}$. Furthermore, $i < j \leq t_b$ and $y \in g_i$, so similarly we have $y = n_b + [i - t_{b-1}]_{r_{2b-1}}$. Hence $i \equiv j \pmod{r_{2b-1}}$, and, in particular, $i \leq j - r_{2b-1}$. Now, as $t_{b-1} < j \leq t_b$, we know that g_j contains no elements greater than n_b other than y, and that the elements of g_j in $(n_{b-1}, n_b]$ are precisely those $x \in (n_{b-1}, n_b]$ with $x - n_{b-1} \equiv j - t_{b-1} \pmod{r_{2b-2}}$. But $0 < j - t_{b-1} \leq t - t_{b-1} = r_{2b-2}$ and $r_{2b-2} | n_b - n_{b-1}$. Hence $x_m = n_b - r_{2b-2} + j - t_{b-1}$. So

$$\begin{aligned} i + n - x_m &= i + n - (n_b - r_{2b-2} + j - t_{b-1}) \\ &\leq (j - r_{2b-1}) + (n - n_b) + r_{2b-2} - j + t_{b-1} \\ &= (j - r_{2b-1}) + r_{2b-1} + r_{2b-2} - j + (t - r_{2b-2}) \\ &= t, \end{aligned}$$

as required.

Now, suppose instead that $j > t_b$. As $y \in g_j$, we must have $y - n_b \equiv j - t_b \pmod{r_{2b}}$. If we also suppose $i > t_b$ then, similarly, we have $y - n_b \equiv i - t_b \pmod{r_{2b}}$, and so $i \equiv j \mod r_{2b}$; but $t \geq i, j > t_b = t - r_{2b}$, giving a contradiction as $i \neq j$. So $i \leq t_b$ and $y = n_b + [i - t_{b-1}]_{r_{2b-1}}$. Now, $j - t_b \leq t - t_b = r_{2b}$ so $y \geq j - t_b + n_b$.

If in fact $y = j - t_b + n_b$, then $i - t_{b-1} \equiv j - t_b \pmod{r_{2b-1}}$. But $t_{b-1} \equiv t_b \pmod{r_{2b-1}}$, so $i \equiv j \pmod{r_{2b-1}}$ and so $i \leq j - r_{2b-1}$. Furthermore, $x_m = n_b - r_{2b-2} + j - t_{b-1}$, and so

$$\begin{aligned} i + n - x_m &\leq (j - r_{2b-1}) + n - (n_b - r_{2b-2} + j - t_{b-1}) \\ &= (j - r_{2b-1}) + (n - n_b) + r_{2b-2} - j + t_{b-1} \\ &= (j - r_{2b-1}) + r_{2b-1} + r_{2b-2} - j + (t - r_{2b-2}) \\ &= t, \end{aligned}$$

as required.

Otherwise, $y > j - t_b + n_b$. In this case, we have $x_m = y - r_{2b}$. Now, $i - t_{b-1} \leq t_b - t_{b-1} = q_{2b} r_{2b-1}$. So $(i - t_{b-1}) - [i - t_{b-1}]_{r_{2b-1}} \leq (q_{2b} - 1) r_{2b-1}$, and so

$$\begin{aligned} y &\geq n_b + (i - t_{b-1}) - (q_{2b} - 1) r_{2b-1} \\ &= (n_b + r_{2b-1}) + i - (t - r_{2b-2}) - q_{2b} r_{2b-1} \\ &= n + i - t + (r_{2b-2} - q_{2b} r_{2b-1}) \\ &= n + i - t + r_{2b}. \end{aligned}$$

Hence $i + n - x_m = i + n - (y - r_{2b}) \leq t$, as required. □

Theorem 1 now follows immediately, as explained earlier. While it is interesting to know that Theorem 1 can be proved by this direct algebraic argument, we cannot at present see any way to generalize this to deal with cyclic translates of a more general set; the proof seems to rely heavily on the points of $[t]$ being adjacent.

References

[1] Chung, F.R.K., Graham, R.L., Frankl, P., and Shearer, J.B., Some intersection theorems for ordered sets and graphs, *J. Combin. Theory Ser. A* **43** (1986), no. 1, 23–37.

[2] Erdős, P., Ko, C., and Rado, R., Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford Ser.(2)* **12** (1961), 313–320.

[3] Füredi, Z., Griggs, J.R., Holzman, R., and Kleitman, D.J., Representations of families of triples over $GF(2)$, *J. Combin. Theory Ser. A* **53** (1990), no. 2, 306–315.

[4] Griggs, J.R., and Walker, J.W., Anticlusters and intersecting families of subsets, *J. Combin. Theory Ser. A* **51** (1989), no. 1, 99–103.