Discrete Mathematics 44 (1983) 31–43
North-Holland Publishing Company

SOME APPLICATIONS OF GRAPH THEORY TO FINITE GROUPS

Edward A. BERTRAM

Department of Mathematics, University of Hawaii at Manoa, Honolulu, HI 96822, USA

Received 31 March 1981
Revised 10 March 1982

Results on vertex coloring and the vertex independence number of a finite graph are used to prove:

Theorem. Let G be a finite group with conjugacy classes indexed by cardinality: $1 = |[x_1]| \leq |[x_2]| \leq \cdots$, and let $C_G(x)$ denote the centralizer of x. If m is the smallest integer i such that $|[x_1]| + |[x_2]| + \cdots + |[x_i]| \geq |C(x_i)|$, then each abelian subgroup A of G has cardinality $|A| \leq |[x_1]| + |[x_2]| + \cdots + |[x_m]|$.

Theorem. Let G be a finite group with a proper subgroup M, such that $x \in M - \{1\} \Rightarrow C_G(x) \subseteq M$. Then G contains at least $[|G|^{1/3}]$ pairwise non-commuting elements, and hence G cannot be covered by the union of fewer than $[|G|^{1/3}]$ abelian subgroups.

Theorem. Let S be a locally maximal sum-free subset of the abelian group G. Then $|S-S| + |S \cup -S| - 3 \leq |G|\,(1 - |S-S|^{-1})$, with equality if and only if $S-S$ is a subgroup H of G, $[G:H] = 3$, and S is a coset of H.

Some open problems are also stated.

1. Introduction

In this paper graph theoretic results concerning the degree sequence, vertex coloring, and the vertex independence number are used to derive theorems about finite groups. First, two elements x, y of the group G are connected by an edge whenever they commute: $xy = yx$. A well-known fact about coloring the vertices of a finite graph is shown to yield an upper bound to the order of the largest abelian subgroup(s) of G, in terms of the cardinalities of the conjugacy classes of G. The same graph, and a lower bound to the vertex independence number in terms of the degree sequence, yields a sufficient condition on a non-abelian group G in order that G contain at least $[|G|^{\frac{1}{3}}]$ pairwise non-commuting elements, and hence cannot be covered by the union of fewer than $[|G|^{\frac{1}{3}}]$ abelian subgroups. Such groups are, for example, permutation groups of prime degree, Frobenius groups, the simple groups PSL$(2, p)$, and the sporadic simple groups.

Finally, turning to finite abelian groups G and an entirely different graph association, we use the vertex independence number to prove an extremal result concerning the cardinalities of the (disjoint) sets $S \cup -S$ and $S-S$ when S is a locally-maximal sum-free subset of G. Along the way we find a lower bound for all such $S \subset G$, of the form $|S| \geq \text{constant} \cdot |G|^{\frac{1}{2}}$. We also show that whenever

$|S+S| \leqslant c\,|S|$ the lower bound can be improved to $|S| \geqslant |G|/f(c)$ where $f(c)$ is a quadratic function of c.

2.

Let $\mathscr{G}$ be an undirected graph, with no loops or multiple edges, whose vertices are $\{x_1, x_2, \ldots, x_n\}$. The *degree* $d(x)$ of a vertex is the number of edges incident with x. We say that the vertices of $\mathscr{G}$ can be *c-colored* whenever there exists a partition of $\{x_1, x_2, \ldots, x_n\}$ into c subsets, with no two vertices in the same subset joined by an edge of $\mathscr{G}$. A *complete* subgraph of $\mathscr{G}$ is a subset of the vertices, every pair of which is connected by an edge of $\mathscr{G}$. A maximal complete subgraph of $\mathscr{G}$ is called a *clique*. Thus if $\mathscr{G}$ can be c-colored, each clique has cardinality $\leqslant c$.

Lemma 1 [Berge, p. 325, Corollary 1]. *If, for some integer $q \geqslant 1$, the number of vertices of degree $\geqslant q$ is $\leqslant q$, then $\mathscr{G}$ can be q-colored.*

Let G be a finite group. The *conjugacy class* $[x]$ containing $x \in G$ is defined by $[x] = \{y^{-1}xy \mid y \in G\}$. The *centralizer* of x in G is given by $C(x) = \{y \in G \mid y^{-1}xy = x\}$, and the *center* Z of G is given by $Z(G) = \bigcap_{x \in G} C(x)$. We will use the basic fact that $|[x]| \cdot |C(x)| = |G|$, the order of G.

Theorem 1. *Let G be a finite group. Index the conjugacy classes of G according to cardinality: $1 \leqslant |[x_1]| \leqslant |[x_2]| \leqslant \cdots$. Let m be the smallest integer i such that $|[x_1]| + |[x_2]| + \cdots + |[x_i]| \geqslant |C(x_i)|$. Then each abelian subgroup $A \leqslant G$ has order $|A| \leqslant |[x_1]| + |[x_2]| + \cdots + |[x_m]|$.*

Proof. The theorem is clearly true if G is abelian, so assume that G is non-abelian and a largest centralizer ($\neq G$) is $C(x_l)$. Thus $|[x_1]| = |[x_2]| = \cdots = |[x_{l-1}]| = 1$, $|[x_l]| \geqslant 2$, and $|C(x_l)| \geqslant |C(x_{l+1})| \geqslant |C(x_{l+2})| \geqslant \cdots$. If $A < G$ is maximal among abelian subgroups of G, then clearly $Z(G) \leqslant A \cap C(x_l)$. Furthermore $|A| \leqslant |C(x_l)|$. To see this suppose there is an element $a \in A$, $a \notin C(x_l)$. Since $A \leqslant C(a)$ and $a \notin Z(G)$, we have $|A| \leqslant |C(a)| \leqslant |C(x_l)|$. Since the conjugacy classes partition G, which is non-abelian, the integer m (in the statement of the theorem) must be $\geqslant l$. If $m = l$ then $|A| \leqslant |C(x_l)| \leqslant |[x_1]| + |[x_2]| + \cdots + |[x_m]|$ and we are finished. So assume $m \geqslant l+1$. We now consider the graph $\mathscr{G}_G$ on the elements of G, with $x, y \in G$ connected by an edge just in case $xy = yx$. $\mathscr{G}_{G-Z}$ is the subgraph with $Z(G)$ and connecting edges deleted, and we claim that $\mathscr{G}_{G-Z}$ can be $\sum_{i=l}^{m} |[x_i]|$-colored. For this we show that the number of vertices of degree $\geqslant \sum_{i=l}^{m} |[x_i]|$, is $< \sum_{i=l}^{m} |[x_i]|$. Clearly each vertex $y \in G-Z$ has degree $|C(y)| - |Z| - 1$ in $\mathscr{G}_{G-Z}$. If $|C(y)| - |Z| - 1 \geqslant \sum_{i=l}^{m} |[x_i]|$, then

$$\begin{aligned} |C(y)| - 1 &\geqslant |Z| + \sum_{i=l}^{m} |[x_i]| \\ &= |[x_1]| + |[x_2]| + \cdots + |[x_m]| \geqslant |C(x_m)|. \end{aligned}$$

Thus $|C(y)|>|C(x_m)|$ which implies that $|[y]|<|[x_m]|$. Thus y has already been counted among $\bigcup_{i=l}^{m-1}[x_i]$, and we have shown that $\sum_{i=l}^{m-1}|[x_i]|$ is an upper bound to the number of vertices of degree $\geq\sum_{i=l}^{m}|[x_i]|$. By the lemma the vertices of $\mathscr{G}_{G-Z}$ can be $\sum_{i=l}^{m}|[x_i]|$-colored, and hence the vertices of $\mathscr{G}_G$ can be $(|Z|+\sum_{i=l}^{m}|[x_i]|)$-colored, that is $\sum_{i=1}^{m}|[x_i]|$-colored. Thus each clique in $\mathscr{G}_G$ has cardinality $\leq\sum_{i=1}^{m}|[x_i]|$ and the theorem is proved.

Remarks. Let M be an abelian group of odd order $2k-1$, $k\geq 2$. If x has order 2 and satisfies $xyx=y^{-1}$ for all $y\in M$, then $\langle x, M\rangle$, the group generated by x and M, is called a generalized dihedral group and has conjugacy class cardinalities:

$$1,\underbrace{2,2,2,\ldots,2}_{k-1\text{ times}},2k-1.$$

Here the integer m in the theorem is equal to k, and in fact we have $1+2+2+\cdots+2=2k-1=|M|$, i.e. equality can occur.

A check of the *solvable* groups with a small number (≤ 7) of conjugacy classes reveals that in each case, except $G=\mathrm{Sym}(4)$, the symmetric group on four symbols, the sum $\sum_{i=1}^{m}|[x_i]|$ is in fact *equal* to $|C(x_l)|$, the largest centralizer $\neq G$. Among these groups most (but not all) are Frobenius groups.

Problem. Find necessary and sufficient conditions on G in order that equality hold in Theorem 1, for some abelian $A<G$.

In Sym(4), and each of the non-solvable groups with ≤ 7 classes, $\sum_{i=1}^{m}|[x_i]|$ is *larger* than $|C(x_l)|$. However there are many examples of groups where this sum is *less* than $|C(x_l)|$; for example in Sym(n), $n\geq 7$, Alt(9) and other simple groups.

3.

For the remaining applications of graph-theoretic methods we need the notion of *vertex independence number*. An independent set in a graph $\mathscr{G}$ is a collection of vertices no two of which are connected by an edge in $\mathscr{G}$. For a finite graph $\mathscr{G}$, let $\alpha(\mathscr{G})$ (the independence number of $\mathscr{G}$) denote the largest cardinality of any independent set in $\mathscr{G}$. The following theorem relating $\alpha(\mathscr{G})$ and the degrees of the vertices of $\mathscr{G}$, was proved in 1980 in V.K. Wei's Ph.D. dissertation [11, pp. 104–106], by removing a vertex v_0 of *minimum* degree, all vertices connected to v_0, and all edges incident with any of these vertices. Here we give a different proof[1], based on deleting a vertex of *maximum* degree.

Theorem 2 [V.K. Wei]. *Let $d(v)$ denote the degree of the vertex v in $\mathscr{G}$. Then $\alpha(\mathscr{G})\geq\sum_{v\in\mathscr{G}}1/(d(v)+1)$, with equality if and only if $\mathscr{G}$ is a union of disjoint cliques.*

[1] My thanks to Jerry Griggs and Tom Ramsey for pointing out this proof of Theorem 2. It was also proved, independently, by Yair Caro, and others.

Proof. Let v_0 be a vertex of maximum degree: $d(v_0) \geq d(v)$ for all $v \in \mathscr{G}$. Let $\mathscr{G}^-$ be the deleted graph consisting of the vertices of $\mathscr{G} - \{v_0\}$ and all edges of $\mathscr{G}$ not incident with v_0. The inequality holds if $\mathscr{G}$ has no edges, or if $\mathscr{G}$ has only 2 vertices. Let $d^-(v)$ denote the degree of v in $\mathscr{G}^-$. For $v \in \mathscr{G}^-$, $d(v) = d^-(v)$ if (v, v_0) is not an edge of $\mathscr{G}$, while $d(v) = 1 + d^-(v)$ if (v, v_0) is an edge of $\mathscr{G}$. Clearly $\alpha(\mathscr{G}^-) \leq \alpha(\mathscr{G}) \leq \alpha(\mathscr{G}^-)+1$. In case $\alpha(\mathscr{G}) = \alpha(\mathscr{G}^-)+1$ it is easy to show, using induction on $\alpha(\mathscr{G}^-)$ and the fact that $1 > 1/(1+d(v_0))$, that $\alpha(\mathscr{G}) > \sum_{v \in \mathscr{G}} 1/(1+d(v))$. But to characterize the case of equality, we will need the fact that we *always* have

$$\sum_{v \in \mathscr{G}^-} \frac{1}{1+d^-(v)} \geq \sum_{v \in \mathscr{G}} \frac{1}{1+d(v)}.$$

Clearly the latter, together with induction, yields the inequality for $\alpha(\mathscr{G})$. So we will show that

$$\sum_{v \in \mathscr{G}^-} \left(\frac{1}{1+d^-(v)} - \frac{1}{1+d(v)} \right) \geq \frac{1}{1+d(v_0)}.$$

Since $d^-(v) = d(v)$ if (v, v_0) is not an edge in $\mathscr{G}$, while $d^-(v) = d(v) - 1$ if (v, v_0) is an edge in $\mathscr{G}$, the latter inequality reduces to

$$\sum_{\substack{v \in \mathscr{G}^- \\ (v, v_0) \text{ edge}}} \frac{1}{d(v)(1+d(v))} \geq \frac{1}{1+d(v_0)}.$$

Since the left-hand side has $d(v_0)$ terms, each $\geq 1/(d(v_0)(1+d(v_0)))$, the inequality holds, and the first part of the theorem is proved.

Clearly, if $\mathscr{G}$ is a union of disjoint cliques, then $\alpha(\mathscr{G}) = \sum_{v \in \mathscr{G}} 1/(1+d(v))$. Now suppose the latter equality holds for a graph $\mathscr{G}$. Let v_0 and $\mathscr{G}^-$ be as before. Since we always have

$$\alpha(\mathscr{G}) \geq \alpha(\mathscr{G}^-) \geq \sum_{v \in \mathscr{G}^-} \frac{1}{1+d^-(v)} \geq \sum_{v \in \mathscr{G}} \frac{1}{1+d(v)},$$

equality between first and last implies that

$$\alpha(\mathscr{G}^-) = \sum_{v \in \mathscr{G}^-} \frac{1}{1+d^-(v)} = \sum_{v \in \mathscr{G}} \frac{1}{1+d(v)}.$$

By induction we may assume that $\mathscr{G}^-$ is a union of disjoint cliques, say $K_1, K_2, K_3, \ldots, K_r$ where $r = \alpha(\mathscr{G}^-) = \alpha(\mathscr{G})$. Thus v_0 must be adjacent to every vertex in some K_i, or else there is an independent set in $\mathscr{G}$ of cardinality $r+1$ (v_0 and one vertex from each K_i, $1 \leq i \leq r$). If v_0 is adjacent to every vertex in K_i and has no other adjacent vertices, then $\mathscr{G}$ is a disjoint union of cliques. If v_0 is adjacent to a vertex not in K_i, then $d(v_0) \geq |K_i| + 1$, and $d(v) = |K_i|$ for each $v \in K_i$. But now

$$\sum_{\substack{v \in \mathscr{G}^- \\ (v, v_0) \text{ edge}}} \frac{1}{d(v)(1+d(v))} > \frac{1}{1+d(v_0)},$$

contradicting the equality between $\sum_{v\in\mathcal{G}^-} 1/(1+d^-(v))$ and $\sum_{v\in\mathcal{G}} 1/(1+d(v))$; the proof is now complete.

Recall Tchebychef's inequality:

$$\sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i \geqslant n \sum_{i=1}^{n} a_i b_i$$

for $\{a_i\}_1^n$ and $\{b_i\}_1^n$ oppositely ordered sequences of real numbers, with equality if and only if either all a_i are equal or all b_i are equal. From this (or Cauchy's inequality) we obtain

$$\left(\sum_{v\in\mathcal{G}} \frac{1}{1+d(v)}\right)\left(\sum_{v\in\mathcal{G}} 1+d(v)\right) \geqslant |V(\mathcal{G})|^2,$$

or

$$\sum_{v\in\mathcal{G}} \frac{1}{1+d(v)} \geqslant \frac{|V(\mathcal{G})|^2}{|V(\mathcal{G})|+2|E(\mathcal{G})|},$$

where $V(\mathcal{G})$ is the vertex set of $\mathcal{G}$ and $E(\mathcal{G})$ the edge set of $\mathcal{G}$, with equality if and only if $\mathcal{G}$ is a regular graph. This, together with Wei's theorem, yields the following corollary, which is also a corollary of Turan's theorem characterizing graphs $\mathcal{G}$ with n vertices, $\alpha(\mathcal{G}) \leqslant b \leqslant n$, and $|E(\mathcal{G})|$ a minimum (see, e.g. [1, p. 269 ff.]).

Corollary 2.1. $\alpha(\mathcal{G}) \geqslant |V(\mathcal{G})|^2/(|V(\mathcal{G})|+2|E(\mathcal{G})|)$, *with equality if and only if* $\mathcal{G}$ *is a disjoint union of cliques of the same cardinality.*

4.

If the center $Z(G)$ of the group G is non-trivial, and $G = \dot{\bigcup}\, x_i Z$ is a coset decomposition of G, then $G = \bigcup \langle x_i Z\rangle$ is a covering of G by abelian subgroups. Responding to a question posed by P. Erdös and E.G. Straus [3], D.R. Mason has shown [7] that even when $|Z| = 1$ there are $\leqslant \frac{1}{2}|G|+1$ abelian subgroups which cover G.

With the 'commuting graph' $\mathcal{G}_G$ defined as in the proof of Theorem 1, $\alpha(\mathcal{G})$ (or $\alpha(\mathcal{G})$) denotes the maximum cardinality of any set of pairwise non-commuting elements of G.

Define $a(G)$ to be the minimum number of abelian subgroups in any such collection whose union equals G. The pigeon-hole principle and our previous discussion give $\alpha(G) \leqslant a(G) \leqslant [G:Z]$, and by Mason's result $a(G) \leqslant \frac{1}{2}|G|+1$. If $k(G)$ denotes the number of distinct conjugacy classes of G and A is any abelian subgroup of G, we also have:

Corollary 2.2. (a) $|G| \leq \alpha(G) \cdot k(G)$,

(b) $|A|^2 \leq k(G) \cdot |G|$,

(c) $|A|^2 \leq \alpha(G) \cdot k^2(G)$, *where in each case equality holds if and only if G is abelian, and $A = G$ in* (b) *and* (c).

Proof. Clearly (c) follows immediately from (a) and (b). To prove (a) we use Corollary 2.1 and count the edges of $\mathcal{G}_G$. Hence $d(x) = |C(x)| - 1$, $x \in G$, so

$$2E(\mathcal{G}) = \sum_{x \in G} (|C(x)| - 1)$$

$$= \Bigl(\sum_{\substack{\text{distinct} \\ \text{classes}}} |[x]| \cdot |C(x)| \Bigr) - |G| = (k(G) - 1)\,|G|,$$

as $|C(x)| \cdot |[x]| = |G| = |V(\mathcal{G})|$ for all $x \in G$. Now (a) follows readily from Corollary 2.1, and we have equality in (a) if and only if $\mathcal{G}_G$ is a complete graph, i.e. G is abelian. To prove (b) we may assume A is a maximal abelian subgroup. Summing over the $k_G(A)$ distinct G-classes $[a]$, $a \in A$, we have

$$|A| = \sum |[a] \cap A| \leq \max_{a \in A} |[a]| \cdot k_G(A)$$

$$\leq \frac{|G| \cdot k(G)}{\min_{a \in A} |C_G(a)|} \leq \frac{|G| \cdot k(G)}{|A|}$$

since A is abelian; thus $|A|^2 \leq k(G) \cdot |G|$ follows. If G is abelian and $A = G$, we clearly have equality. Now assume we have equality. Then for each $a, b \in A$, $|[a]| = |[b]|$, hence $|[a]| = 1$. But then $A \subseteq Z$. Since A is a maximal abelian subgroup, A must be all of G, and the proof of (b) is complete.

Remarks. Using Corollary 2.2(a) we can produce a lower bound to $\alpha(G)$, and hence to $a(G)$, whenever we have an upper bound to $k(G)$. For example, when q is a prime power ≥ 4, it can be checked that each simple group $G \in \{\mathrm{PSL}(2, q)\}$ satisfies

$$c_1 |G|^{1/3} < k(G) \leq c_2 |G|^{1/3}$$

where $c_1 = (\frac{1}{4})^{1/3}$ and $c_2 = (\frac{25}{12})^{1/3}$. Thus, for each simple group $G \in \{\mathrm{PSL}(2, q)\}$ we know that $\alpha(G) \geq c|G|^{2/3}$ and hence that such G cannot be covered by the union of fewer than $c\,|G|^{2/3}$ abelian subgroups. It is also likely that $k(G) \leq c_2\,|G|^{1/3}$, and hence $a(G) \geq c\,|G|^{2/3}$ for all finite non-abelian simple groups. On the other hand, the author has shown [2] that for each fixed $\epsilon > 0$ almost all integers $n \leq x$, as $x \to \infty$, have the property that $k(G) > |G|^{1-\epsilon}$ for each group G of order n. In Theorem 3 we will show that if the group G contains a proper 'centralizer-closed' subgroup, then $\alpha(G) \geq [|G|^{1/3}]$ (greatest integer function).

Concerning Corollary 2.2(b), we note that the dihedral groups D_{2n} given by

$$D_{2n}=\langle x, y \mid x^2=y^n=e, x^{-1}yx=y^{-1}\rangle$$

have order $2n$, with $k(D_{2n})=\frac{1}{2}n+\frac{3}{2}$ (for n odd) and $k(D_{2n})=\frac{1}{2}n+3$ (for n even). In each case there is an abelian subgroup A of order n, and $k\cdot|G|/|A|^2\downarrow 1$ as $n\to\infty$.

Finally, the groups D_{2n} with n odd show that $\alpha(G)=a(G)=\frac{1}{2}|G|+1$ can occur. Here $\{x, y, xy, xy^2, \ldots, xy^{n-1}\}$ consists of $n+1$ non-commuting elements of D_{2n}. Other non-abelian groups G which satisfy $\alpha(G)=a(G)$ are those with $|G|=pq$, where $p<q$ are primes and $q\equiv 1 \pmod p$, and those with $|G|=pq^2$, where $q<p<q^2$. In fact any non-abelian group G in which all centralizers (except G) are abelian satisfies $\alpha(G)=a(G)$. For in such G, let $g_1, g_2, \ldots, g_\alpha$ be a largest collection of pairwise non-commuting elements. Then each $x\in G$ must commute with at least one of the g_i, so $G=\bigcup_{j=1}^{\alpha(G)} C(g_j)$. Since each centralizer is abelian $a(G)\leqslant\alpha(G)$. But always $\alpha(G)\leqslant a(G)$, and equality follows.

The condition that all centralizers be abelian is not necessary, however. In S_4, the symmetric group on the four symbols $\{1, 2, 3, 4\}$, the centralizer of the permutation $(1\,2)(3\,4)$ is non-abelian. Furthermore S_4 is covered by the 10 abelian subgroups: $\langle(1\,2\,3\,4)\rangle$, $\langle(1\,3\,2\,4)\rangle$, $\langle(1\,2\,4\,3)\rangle$, $\langle(1\,2\,3)\rangle$, $\langle(1\,2\,4)\rangle$, $\langle(1\,3\,4)\rangle$, $\langle(2\,3\,4)\rangle$, $\{(1\,2), (3\,4), (1\,2)(3\,4), e\}$, $\{(1\,3), (2\,4), (1\,3)(2\,4), e\}$, and $\{(1\,4), (2\,3), (1\,4)(2\,3), e\}$, which intersect pairwise only in the identity e. Finally, the first seven generators, together with $(1\,2)$, $(1\,3)$, and $(1\,4)$ form a collection of 10 pairwise non-commuting permutations. Thus $\alpha(S_4)=a(S_4)$.

Problem. Find necessary and sufficient conditions on G in order that $\alpha(G)=a(G)$.

Lemma 2. *Let G be a finite non-abelian group such that $\alpha(G)\leqslant|G|^r-1$, $0<r<1$. then:*

(a) *For each $x\in G$, $|C(x)|\geqslant|G|^{(1-r)/2}$.*

(b) *There exists an element $g\in G-Z(G)$ with $|C(g)|>|G|^{1-r}$ and $|C(x)\cap C(g)|>|G|^{(1-3r)/2}$, for each element $x\in G$.*

(c) *Finally, in every finite group G, at least $k(G)-\alpha(G)$ of the distinct conjugacy classes in G satisfy $|[x]|<|G|^{1/2}$.*

Proof. (a) In the graph $\mathscr{G}_G$ we have the degree of a vertex $d(x)=|C(x)|-1$. From Theorem 2 it follows that $\sum_{x\in G} 1/|C(x)|\leqslant\alpha(G)$. Since $|C(x)|=|G|/|[x]|$ is a class invariant,

$$\frac{1}{|G|}\sum_{\substack{\text{distinct}\\ \text{classes}}}|[x]|^2=\sum_{\substack{\text{distinct}\\ \text{classes}}}\frac{|[x]|}{|C(x)|}\leqslant\alpha(G)<|G|^r.$$

Thus we obtain $\sum_{\text{classes}}|[x]|^2<|G|^{1+r}$, and each class satisfies $|[x]|<|G|^{(1+r)/2}$, i.e. $|C(x)|>|G|^{(1-r)/2}$.

To prove (b) we use

$$\sum_{x\in G-Z}\frac{1}{|C(x)|}+\frac{|Z|}{|G|}=\sum_{x\in G}\frac{1}{|C(x)|}\leq\alpha(G).$$

If $|C(x)|\leq|G|^{1-r}$ for each $x\in G-Z$, then our hypothesis on $\alpha(G)$ gives

$$\frac{|G|-|Z|}{|G|^{1-r}}\leq\alpha(G)-\frac{|Z|}{|G|}\leq|G|^r-1-\frac{|Z|}{|G|},$$

and rearranging the extremes gives

$$1\leq|Z|\left(\frac{1}{|G|^{1-r}}-\frac{1}{|G|}\right).$$

Since $|Z|\leq|C(x)|\leq|G|^{1-r}$, we are led to the contradiction $1\leq1-1/|G|^r$. Thus $|C(g)|>|G|^{1-r}$ for *some* $g\in G-Z$. For each $x\in G$ we know that

$$|C(g)\cap C(x)|\geq\frac{|C(g)|\,|C(x)|}{|G|},$$

since $C(g)$ and $C(x)$ are subgroups of G (see, e.g. [5, p. 45]). By (a) the right side of this inequality is $>|G|^{(1-3r)/2}$.

To prove (c), let $l(G)$ denote the number of distinct classes of G which satisfy $|[x]|^2<|G|$. Then $k(G)-l(G)$ of the classes satisfy $|[x]|^2\geq|G|$, so that

$$(k(G)-l(G))\,|G|\leq\sum_{\substack{\text{distinct}\\ \text{classes}}}|[x]|^2\leq|G|\cdot\alpha(G),$$

as in the proof of (a). Thus $l(G)\geq k(G)-\alpha(G)$.

From Lemma 2(b) we see that if $|[x]|\geq|G|^r$ for every non-central class $[x]$, then $\alpha(G)\geq[|G|^r]$, that is $\alpha(G)\geq\min_{x\in Z}|[x]|$. When $r=\frac{1}{2}$ above, Lemma 2(c) yields $\alpha(G)\geq k(G)-|Z|$. But in such groups $|G|^{1/2}\leq(|G|-|Z|)/(k-|Z|)$, so $k(G)-|Z|<|G|^{1/2}$. Thus Lemma 2(c) does not improve the lower bound for $\alpha(G)$ when $r=\frac{1}{2}$ above.

We turn now to those groups G which contain a proper 'centralizer-closed' subgroup M, that is for each $x\in M-\{1\}$, $C_G(x)\subseteq M$. Examples are: all Frobenius groups, all transitive permutation groups on p (a prime) symbols, all of the simple groups PSL(2, p), PSL(2, 2^m), and other PSL's, and all 26 of the sporadic simple groups.

Theorem 3. *Let G be a group containing a proper subgroup M such that whenever $x\in M-\{1\}$, $C_G(x)\subseteq M$. Then $\alpha(G)\geq[|G|^{1/3}]$, where $[r]=$ the greatest integer $\leq r$.*

Proof. Suppose $\alpha(G)<[|G|^{1/3}]$. Then $\alpha(G)\leq|G|^{1/3}-1$. In Lemma 2, put $r=\frac{1}{3}$. From part (b) of the lemma we know that there exists an element $g\in G-Z$, with the property that $|C(g)\cap C(x)|>1$ for *each* $x\in G$. However, this contradicts our hypothesis on the subgroup M. For suppose $g\in M-\{1\}$, and $x\notin M$. Then $y\in M-\{1\}$ implies that $y\notin C(x)$, and $y\in G-M$ implies that $y\notin C(g)$. In case $g\notin M$, let $x\in M-\{1\}$. Then $y\in G-M$ implies that $y\notin C(x)$, whereas $y\in M-\{1\}$ implies that $y\notin C(g)$.

Corollary. *Let p be any prime dividing the order of the non-abelian group G. If there exists an element $x\in G$ such that $|C(x)|=p$, then $\alpha(G)\geqslant[|G|^{1/3}]$.*

Remark. M. Isaacs [6] has shown that the corollary has a direct group-theoretic proof, as follows: Let $P=\langle x\rangle$, the cyclic subgroup of order p generated by x. Since $P=C_G(P)$, P is a Sylow p-subgroup of G, i.e. $p^2\nmid|G|$. Also $N_G(P)/C_G(P)$ is isomorphic to a subgroup of the automorphism group of P, a cyclic group of order $p-1$. Thus $|G|=p\cdot[G:N]\cdot[N:P]=p\cdot m\cdot e.$, where $m=[G:N]$ and $e\mid p-1$. Since any collection of m non-identity elements, chosen one from each of the m conjugates of P, are pairwise non-commuting we have $\alpha(G)\geqslant m$. If the theorem were false, then $\alpha^3(G)<|G|$, so $m^3<|G|, m^2<pe<p^2$ and $m<p$. By Sylow $m\equiv 1 \pmod p$ so $m=1$ and $p<pe=|G|<p^2$. Also, P is a normal subgroup of G with $G/P=N_G(P)/P$ a cyclic group.

Now let q be a prime, $q\mid e$, and suppose Q is a subgroup of G, with $|Q|=q$. If $x\in P$ and $x^{-1}Qx=Q$, then, for each $y\in Q$, $(x^{-1}y^{-1}x)y\in Q$ and $x^{-1}(y^{-1}xy)\in P$ since P is normal. Thus $x^{-1}y^{-1}xy\in P\cap Q=\{1\}$ or $y\in C(x)$, in contradiction to $C(P)=P$. Thus $p\nmid|N_G(Q)|$, so $p\mid[G:N_G(Q)]$ and Q has at least p conjugates, say $Q_1, Q_2, \ldots, Q_p$, with $Q_i=\langle x_i\rangle$. If no pair x_i, x_j commute, then $\alpha(G)\geqslant p>|G|^{\frac{1}{2}}$. If x_i and x_j commute, then $H=\langle x_i, x_j\rangle$ is abelian, but since $x_j\notin\langle x_i\rangle$, H is non-cyclic of order q^2. Since $H\cap P=\{1\}$, $H\cong HP/P\subseteq G/P$, which is cyclic, a contradiction.

In 1975 Erdös suggested the problem of finding an upper bound to $a(G)$ in terms of $\alpha(G)$, whenever the latter is finite, and Isaacs [6] found the following:

Theorem. [Isaacs]. *Define a function $f(n)$ inductively by $f(1)=1$ and $f(n)=n+\binom{n}{2}f(n-1)$. If $\alpha(G)<\infty$, then $a(G)\leqslant f(\alpha(G))$; in particular $a(G)<\infty$.*

Proof. Put $\alpha(G)=\alpha$. If $x, y\in G$ with $xy\neq yx$ and $c_1, c_2, \ldots, c_\alpha\in C(x)\cap C(y)$, then two of the elements $x, c_1y, c_2y, \ldots, c_\alpha y$ must commute. Since x commutes with none of the c_jy, two of the latter must commute and thus two of the c_j must commute. Hence $\alpha(C(x)\cap C(y))<\alpha(G)$, whenever $xy\neq yx$.

Now let $x_1, x_2, \ldots, x_\alpha$ be pairwise non-commuting and let $B_{jk}=C(x_j)\cap C(x_k)$ for $j\neq k$. Then $\alpha(B_{jk})<\alpha(G)$, so working by induction on α (and using the fact that f is monotone) we conclude that B_{jk} is the union of at most $f(\alpha-1)$ abelian subgroups. Now let $A_j = C(x_j) - \bigcup_{k \neq j} B_{jk}$. Since

$$G = \bigcup_{1 \leq j \leq \alpha} C(x_j) = \bigcup_{1 \leq j \leq \alpha} \langle A_j \rangle \cup \bigcup_{j,k} B_{jk},$$

once we show that each $\langle A_j \rangle$ is abelian, we have proved that

$$a(G) \leq \alpha + \binom{\alpha}{2} f(\alpha - 1) = f(\alpha(G)).$$

To show each $\langle A_j \rangle$ is abelian, let $u, v \in A_j$. Then $x_1, \ldots, x_{j-1}, u, x_{j+1}, \ldots, x_\alpha$ are α pairwise non-commuting elements, so v must commute with one of them. Then v commutes with u, and $\langle A_j \rangle$ is abelian.

Isaacs also finds that $\alpha(G) = 2n + 1$ for G extra-special of order 2^{2n+1}, and $a(G) \geq 2^n + 1$. Thus, whereas the above theorem shows that always $a(G) \leq f(\alpha(G)) < (\alpha(G)!)^2$, there exist G for which $a(G) > c^{\alpha(G)}$, with c a constant >1.

5.

In this section we assume G is a finite *abelian* group. A subset $S \subset G$ is called *sum-free* if whenever $x, y \in S$, $x + y \notin S$. If $S + S = \{x + y \mid x, y \in S\}$, and $S - S$ is defined analogously, we see that S is sum free if and only if

$$S \cap (S + S) = \emptyset = S \cap (S - S).$$

A sum-free set $S \subset G$ is called *locally maximal* (or non-extendable) if, whenever T is a sum-free subset of G and $S \subseteq T$, then $S = T$. Such a set S is called *maximal* if S also has the largest cardinality among all sum-free subsets of G. Considerable progress has been made on the general problem of characterizing all maximal sum-free sets in a given finite abelian group G; see e.g. [10, Ch. 7, pp. 205–242].

Locally maximal sum-free sets have been studied mainly because of their connection with the Ramsey number(s) $R_k(3, 2)$: the smallest positive integer n such that any k-coloring of the edges of the complete graph on n vertices results in at least one monochromatic triangle. In particular it is known [4] that if the set G^* of non-zero elements can be partitioned into k sum-free sets, then a triangle-free k-coloring of the complete graph on $|G|$ vertices is possible, and each sum-free set has cardinality $< R_{k-1}$. Further (see [9]) every sum-free partition of G^* can be 'embedded' in at least one covering of G^* by locally maximal sum-free sets, and again each of these has cardinality less than R_{k-1}.

Thus it is of interest to find the minimum cardinality of the locally maximal sum-free sets in a given G, as well as to characterize all locally maximal sum-free subsets. Our first results concern lower bounds for the cardinality of any locally-maximal sum-free set, in terms of $|G|$. Let $\frac{1}{2}S$ denote $\{x \in G \mid 2x \in S\}$. Clearly if S is sum-free, then $\frac{1}{2}S$ is sum-free, and if $|G|$ is odd, then $|\frac{1}{2}S| = |S|$. When $|G|$ is even, we see immediately that $|\frac{1}{2}S| \leq \frac{1}{2}|G|$, since every sum-free set in *any* finite group has cardinality $\leq \frac{1}{2}|G|$ (see e.g. [10, p. 205]). Also $|\frac{1}{2}S| = \frac{1}{2}|G|$ occurs e.g. when $S = \{2+4i\}_0^{n-1} \subset \mathbb{Z}_{4n}$.

Theorem 4. *Let S be a locally maximal sum-free set in G. Then*

(i) $G = S \cup (S+S) \cup (S-S) \cup \frac{1}{2}S$.

(ii) *If* $|G|$ *is odd, then* $|S| \geq \frac{1}{6}((24|G|-15)^{1/2}-3)$.

(iii) *If* $|G|$ *is even, then* $|S| \geq \frac{1}{6}((12|G|-23)^{1/2}-1)$.

(iv) *If* $|S+S| \leq c|S|$, *then* $|S| \geq |G|/(c^2+c+2)$ *for* $|G|$ *odd, and* $|S| \geq |G|/2(c^2+c+1)$, *for* $|G|$ *even.*

Proof. For (i), suppose $x \in G \setminus S \cup (S+S) \cup (S-S)$. Then $S \cup \{x\}$ is not sum-free. Thus either $2x \in S$, $x \in S+S$, or $(x+S) \cap S \neq \emptyset$. Since S is sum-free, the only possibility of the three is $2x \in S$, i.e. $x \in \frac{1}{2}S$. Thus

$$G = S \cup (S+S) \cup (S-S) \cup \tfrac{1}{2}S.$$

For (ii) and (iii) we use the fact that for every subset S,

$$|S+S| \leq \binom{|S|}{2} + |S| \quad \text{and} \quad |S-S| \leq 1 + 2\binom{|S|}{2}.$$

These estimates, together with (i) and our earlier remarks on $|\frac{1}{2}S|$, show that for $|G|$ odd: $|G| \leq \frac{3}{2}|S|^2 + \frac{3}{2}|S| + 1$, whereas for $|G|$ even we have $|G| \leq 3|S|^2 + |S| + 2$. To prove (iv), we use a result of I.Z. Ruzsa [8]: For an arbitrary set $A \subseteq G$, if $|A+A| \leq c|A|$, then $|A-A| \leq c^2|A|$. The lower bounds on $|S|$ follow in each case, as above.

Remarks. In our example: $S = \{2, 6, 10, 14, \ldots, 4n-2\} \subseteq \mathbb{Z}_{4n}$ the sum-free set $\frac{1}{2}S$ also satisfies $|\frac{1}{2}S| = 2|S|$. There is ample evidence that $|\frac{1}{2}S| \leq 2|S|$ is true whenever S is a *locally maximal* sum-free set. It does not hold for arbitrary sum-free sets, as the sum-free set $S = \{(2,0), (2,2), (2,3)\}$ in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ shows. Here $S \cup \{(2,1)\}$ is sum-free, and $|\frac{1}{2}S| = 8$. *If* $|\frac{1}{2}S| \leq 2|S|$ is true, we may modify our lower bound estimates, when $|G|$ is even, to $|S| \geq \frac{1}{6}((24|G|-11)^{1/2}-5)$ in part (iii) and $|S| \geq |G|/(c^2+c+3)$ in part (iv), of Theorem 4.

In [9, p. 226] it is pointed out that if $\frac{1}{5}(n+2) \leq h \leq \frac{1}{3}(n+2)$, then there exists a locally-maximal sum-free set in $\mathbb{Z}_n$ of cardinality h, namely $\{h, h+1, \ldots, 2h-1\}$. We add to this that in $\mathbb{Z}_{11k+2}$, k odd, the set $\{2k+1, 2k+2, \ldots, 3k, 4k+1, 6k+1\}$ is a locally maximal sum-free set of cardinality $<\frac{1}{11}|G|+2$.

Problems. (1) Does S locally maximal sum-free imply $|\frac{1}{2}S| \leq 2|S|$?

(2) Decide whether or not there exists a sequence of abelian groups G and locally maximal sum-free sets $S \subset G$ such that $|S+S|/|S| \to \infty$ as $|G| \to \infty$.

(3) Decide whether or not there exists a sequence of abelian groups G and locally maximal sum-free sets $S \subset G$ such that $|S| < c|G|^{1/2}$ c a constant, as $|G| \to \infty$.

As a prelude to our next use of the vertex independence number, consider an abelian group G of order divisible by 3, and H a subgroup of index 3 in G. Then $G = H \dot{\cup} (H+a) \dot{\cup} (H+2a)$, where a, $2a \notin H$, but $3a \in H$. Now $S = H+a$ is a locally maximal sum-free set in G, since $G = S \dot{\cup} (S+S) \dot{\cup} (S-S)$. Furthermore

$$|S-S| + |S \cup -S| - 3 = 3(|H|-1) = |G|\,(1 - |S-S|^{-1}).$$

Theorem 5. *Let S be a locally maximal sum-free set in the finite abelian group G. Then $|S-S| + |S \cup -S| - 3 \leq |G|\,(1-|S-S|^{-1})$, with equality if and only if $S-S$ is a subgroup of G, $[G:S-S]=3$, and S is a coset of $S-S$.*

Proof. The example immediately above shows that if S is a non-trivial coset of a subgroup of index 3 in G, we have equality. For the converse, let S be locally maximal sum-free in G. If $x_1, x_2, \ldots, x_r$ is any set of (distinct) elements of G with $x_i - x_j \notin S-S$, $i \neq j$, $1 \leq i$, $j \leq r$, then we first claim that

$$r \leq |G| - |S-S| - |S \cup -S| + 3.$$

For, consider the r-set: $y_1 = 0$, $y_2 = x_2 - x_1$, $y_3 = x_3 - x_1, \ldots, y_i = x_i - x_1, \ldots$. Since $i \neq j \Rightarrow y_i - y_j = x_i - x_j$, only y_1 belongs to $S-S$. Also at most one of the y_i, $i \geq 2$ belongs to S, and at most one of the y_i, $i \geq 2$ belongs to $-S$. Since S is sum free, $(S-S) \cap (S \cup -S) = \emptyset$, and thus

$$r + (|S-S|-1) + (|S \cup -S| - 2) \leq |G|.$$

Now let S be any subset of the abelian group G, $|G| = n$, $G = \{g_1, g_2, \ldots, g_n\}$. Define a graph $\mathcal{G}_S$ whose vertices are $g_1, \ldots, g_n$, with an edge $\{g_i, g_j\}$ between g_i and g_j if and only if $g_i - g_j \in S-S$. For each $g_i \in G$ there are $|S-S|-1$ elements $g_j \neq g_i$ such that $g_i - g_j \in (S-S) - \{0\}$. Thus $\mathcal{G}_S$ is a regular graph, each vertex of degree $|S-S|-1$, and $\mathcal{G}_S$ has $E = \frac{1}{2}n(|S-S|-1)$ edges. From Corollary (2.1) to Turan's or Wei's theorem we know that any independent set in $\mathcal{G}_S$ of maximum cardinality $\alpha(G)$ satisfies

$$\alpha(G) \geq \frac{|G|^2}{|G|+2E} = \frac{|G|}{|S-S|},$$

with equality if and only if $\mathcal{G}_S$ is a union of disjoint cliques, each of cardinality $|S-S|$ since $\mathcal{G}_S$ is regular.

An independent set in $\mathcal{G}_S$ is a set of distinct elements $g_1, g_2, \ldots, g_r$ which satisfy $g_i - g_j \notin S-S$ for $i \neq j$. When S is sum-free, we saw in the first paragraph that $r \leq |G| - |S-S| - |S \cup -S| + 3$. Thus

$$|G|/|S-S| \leq \alpha(G) \leq |G| - |S-S| - |S \cup -S| + 3$$

and the inequality has been proved. Furthermore the right-hand side is equal to the left-hand side if and only if $\mathcal{G}_S$ is the union of disjoint cliques, each of cardinality $|S-S|$.

When we have equality, the elements of $S-S$ themselves form a clique, since each element of $(S-S)-\{0\}$ is connected by an edge to 0. Thus $S-S$ is a subgroup of G, since the former is closed under differences. We claim that S is a clique in $\mathscr{G}_S$, whence $|S|=|S-S|$ and S is a (non-trivial) coset of $S-S$. For the proof, note that each pair of elements of S is connected by an edge in $\mathscr{G}_S$. Suppose $a\notin S$ and a is connected to each member of S, i.e. $(a-S)\cup(S-a)\subseteq S-S$. Then:

(i) $2a\notin S$; otherwise there exists an $s\in S$ such that $2a=s$ or $a=s-a\in S-S$, contradicting the fact that no element of $S-S$ is connected to any element not in $S-S$.

(ii) $a\notin S+S$; for otherwise there exist $s_1, s_2\in S$ such that $s_1=a-s_2\in S-S$, contradicting S is sum-free.

But $a\notin S-S \Leftrightarrow (a+S)\cap S=\emptyset$. This, together with (i) and (ii) imply that $S\cup\{a\}$ is also sum-free contradicting our assumption that S is locally maximal. Thus S is a clique in $\mathscr{G}_S$. Clearly S is a coset of $S-S$, since two elements of G are in the same coset modulo a subgroup if and only if their difference is in that subgroup. Finally, $-S$ is also a coset of $S-S$.

Thus either $S=-S$ or $S\cap -S=\emptyset$. If $S=-S$ and $|S-S|+|S\cup -S|-3=|G|(1-|S-S|^{-1})$, then $|S|=|S-S|$ yields $|S|(2|S|-3)=|G|(|S|-1)$. But $|S|-1$ is relatively prime to $|S|$ and $2|S|-3$, so $|S|=2=|G|$, a contradiction. So $S\cap -S=\emptyset$, and the equality gives

$$3|S|-3=\frac{|G|}{|S-S|}(|S|-1)$$

i.e. $S-S$ has index 3 in G.

References

[1] C. Berge, Graphes et Hypergraphes (Dunod, Paris, 1970).

[2] F A. Bertram, On large cyclic subgroups of finite groups, Proc. Amer. Math. Soc. 56 (1976) 63–66.

[3] P. Erdös and E.G. Straus, How abelian is a finite group? Linear and Multilinear Algebra 3 (1976) 307–312.

[4] R.E. Greemwood and A.M. Gleason, Combinatorial relations and chromatic graphs, Canad. J. Math. 7 (1955) 1–7.

[5] I.N. Herstein, Topics in Algebra, 2nd ed. (Wiley, New York, 1975).

[6] I.M. Isaacs, Personal communication.

[7] D.R. Mason, On coverings of finite groups by abelian subgroups, Math. Proc. Cambridge Philos. Soc. 83 (1978) 205–209.

[8] I.Z. Ruzsa, On the carinality of $A+A$ and $A-A$, in: A. Hajnal and V.T. Sós, eds., Combinatorics, Colloq. Math. Soc. János Bolyai 18 (North-Holland, Amsterdam, 1976) 933–938.

[9] A.P. Street and E.G. Whitehead, Jr., Group Ramsey theory, J. Combin. Theory 17 (1974) 219–226.

[10] W.D. Wallis, A.P. Street and J.S. Wallis, Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices, Lecture Notes in Math., Vol. 292 (Springer-Verlag, New York, 1972).

[11] V.K. Wei, Coding for a multiple access channel, Ph.D. dissertation, Dept. of Electrical Engineering, Univ. of Hawaii, August 1980.