Can. J. Math., Vol. XXXVI, No. 3, 1984, pp. 529-536

A GENERALIZATION OF AN ADDITION THEOREM FOR SOLVABLE GROUPS

THOMAS YUSTER AND BRUCE PETERSON

The "sets" in this paper are actually multi-sets. That is, we allow an element to occur several times in a set and distinguish between the number of elements in a set and the number of distinct elements in the set. On the few occasions when we need to avoid repetition we will use the term "ordinary set."

Definition. Let G be a group and let S a set of elements of G. An *r-sum* in S is an ordered subset of S of cardinality r; the *result* of that r-sum is the product of its elements in the designated order.

Definition. If S is a set, $r(x, S)$ denotes the number of times x appears in S and $[x, S]$ is a set consisting of $r(x, S)$ copies of x. An *n-set* or *n-subset* is a set consisting of n elements. Hence $[x, S]$ is an $r(x, S)$-subset of S.

The following result due to Cauchy [**1**] will be used throughout the paper.

PROPOSITION 1. *Let A and B be ordinary subsets of $\mathbf{Z}_n$ (the integers* mod *n) with $|A| = a$ and $|B| = b$. If n is prime then either*

$$A + B = Z_n \text{ or } |A + B| \geqq (a + b - 1).$$

In this paper, we will generalize the following result. It was originally proved for abelian groups by Erdös, Ginsburg and Ziv [**2**] and was later generalized to solvable groups. It is a direct consequence of Proposition 1.

PROPOSITION 2. *Let G be a solvable group of order n and let S be a $(2n - 1)$-subset of G. Then S contains an n-sum of result* 1.

This result does not hold if $2n - 1$ is replaced by $2n - 2$ since a subset of $\mathbf{Z}_n$ consisting of $n - 1$ 0's and $n - 1$ 1's contains no n-sum of result 1. Our main theorem is the following generalization of Proposition 2.

THEOREM 1. *Let G be a solvable group of order n and S a $(2n - 2)$-subset of G which contains no n-sum of result* 1. *Then*:

1. *There are exactly two distinct elements x and y in S,*
2. *$r(x, S) = r(y, S) = n - 1$, and*
3. *G is cyclic.*

Received February 28, 1983 and in revised form September 15, 1983.

LEMMA 1. *Let G be a counter-example to Theorem* 1 *with $|G|$ minimal, and let $K \lhd G$ with $1 < |K| < |G|$. Let $|G| = ab$ and $|K| = b$, and let $S\mathcal{I}$ be the image of S in G/K. Then*:

1. *Any set of c a-sums of S with results in K can be extended to a set of $2b - 2$ a-sums of S with results in K.*
2. *Any set of $2b - 2$ a-sums of S with results in K contains exactly two distinct results, with each result occurring exactly $b - 1$ times. There is no set of $2b - 1$ a-sums of S with results in K.*
3. *Both K and G/K are cyclic.*
4. *There are exactly two distinct elements x and y in $S\mathcal{I}$, and*

$$r(x, S\mathcal{I}) \equiv r(y, S\mathcal{I}) \equiv -1 \pmod{a}.$$

Proof. 1. We have $|G/K| = a$, so if T is an r-subset of G with $r \geqq 2a - 1$, and $T\mathcal{I}$ is its image in G/K, $T\mathcal{I}$ contains an a-sum of result 1 and thus T contains an a-sum with result in K. Thus if we have c a-sums in S with results in K, there are

$$(2ab - 2) - ca = (2b - c)a - 2$$

other elements in S. If $c < 2b - 2$, then

$$(2b - c)a - 2 > 2a - 2,$$

so we can obtain another a-sum with result in K.

2. Suppose that S contains $2b - 1$ a-sums with results in K. Let T be the set of these results. Then Proposition 2 implies that there is a b-sum in T of result 1. Hence there is an n-sum in S of result 1. Thus we may assume that there are at most $2b - 2$ a-sums in S with results in K. Now suppose that S contains $2b - 2$ a-sums with results in K. Let T be the set of these results. Since $K < G$, minimality assures that there is a b-sum of result 1 in T unless there are exactly two elements in T and each appears exactly $b - 1$ times.

3. Suppose that K is not cyclic. By part 1, we can find $2b - 2$ a-sums of S with results in K. Let T be the set of these results. Since $K < G$ and K is not cyclic, T contains a b-sum of result 1, and S contains an n-sum of result 1. Thus K is cyclic.

Now suppose that G/K is not cyclic. Since $|G/K| < |G|$, if T is any subset of S with $|T| \geqq 2a - 2$, then T contains an a-sum with result in K. By part 1, we can find $2b - 2$ a-sums of S with results in K. There are

$$(2ab - 2) - (2b - 2)a = 2a - 2$$

other elements in S and thus another a-sum with result in K. This contradicts part 2, and hence G/K is cyclic.

4. It is clear that $S\mathcal{I}$ must contain at least two distinct elements, for otherwise any a-subset of S would be an a-sum with result in K, and there

would be $2b - 1$ a-sums of S with results in K, contradicting part 2. Suppose first that $S\mathcal{I}$ contains exactly two distinct elements x and y. After forming all the a-sums of result 1 we can from $[x, S\mathcal{I}]$, at most $a - 1$ elements remain. Doing the same thing in $[y, S\mathcal{I}]$, again at most $a - 1$ elements remain. If $r(x, S\mathcal{I})$ or $r(y, S\mathcal{I})$ is not congruent to $-1 (\text{mod } a)$, then there must be fewer than $2a - 2$ elements left over which means we must have used at least

$$(2ab - 2) - (2a - 3) = (2b - 2)a + 1$$

elements to form a-sums. Since the number of elements used must be divisible by a, we must have formed at least $2b - 1$ a-sums of result 1. Thus in S, there are at least $2b - 1$ a-sums with results in K. This contradicts part 2. Thus if there are exactly two distinct elements x and y in $S\mathcal{I}$, then

$$r(x, S\mathcal{I}) \equiv r(y, S\mathcal{I}) \equiv -1 (\text{mod } a).$$

Now suppose that $S\mathcal{I}$ contains at least three distinct elements x, y, and z. Then clearly $a > 2$. Let

$$T\mathcal{I} = S\mathcal{I} - \{x, y, z\}.$$

Then $|T\mathcal{I}| = 2ab - 5$. Suppose first that $a > 3$. If we have formed c a-sums in $T\mathcal{I}$ of result 1, there are

$$(2ab - 5) - ca = (2b - c)a - 5 \geqq (2b - c - 1)a - 1$$

elements left. Hence we can form $2b - 2$ a-sums in $T\mathcal{I}$ of result 1. There are $2a - 2$ elements of $S\mathcal{I}$ which have not been used, and at least three of these are distinct. Since $|G/H| < |G|$, we can form another a-sum of result 1. Hence there are $2b - 1$ a-sums of S with results in K. This contradicts part 2, so we may assume that $a = 3$.

Now part 1 implies that we can form $2b - 2$ 3-sums with result 1 in $S\mathcal{I}$. There is a set consisting of exactly 4 elements of $S\mathcal{I}$ which were not used to form these 3-sums. If one of x, y, or z appears 3 times in this set, or each element appears at least once, we can form another a-sum of result 1, since $|G/K| = 3$ and hence $x + y + z = 1$. Thus we may assume that the set of remaining elements is $T = \{x, x, y, y\}$. Since z is in $S\mathcal{I}$, we must have formed a 3-sum of the form $\{x, y, z\}$ or of the form $\{z, z, z\}$.

In the first case, we can combine the 3-sum with T and form $\{x, x, x\}$ and $\{y, y, y\}$, both of which have result 1. In the second case, we can combine the 3-sum with T and form two 3-sums of the form $\{x, y, z\}$, both of which have result 1. Thus in either case we have produced $2b - 1$ 3-sums of $S\mathcal{I}$ of result 1. This contradiction establishes part 4 and completes the proof.

LEMMA 2. *Let G be a group of order n and let S be a* $(2n - 2)$*-subset of G such that S contains no n-sum of result* 1. *Then S generates G.*

Proof. Suppose not. Let $H = <S>$. Then $|H| = a$ where $ab = n$ with $a < n$. In any $(2a - 1)$-subset of H there is an a-sum of result 1. Now

$$|S| = 2n - 2 = 2ab - 2 \geqq 2ab - b = b(2a - 1),$$

so we can find b a-sums of result 1 in S. But then S contains an n-sum of result 1.

LEMMA 3. *Let G be a group of order $n = ab$, and let T be a set of elements of G such that T contains no n-sum of result* 1. *Suppose that $T = T_1 \cup T_2 \cup \ldots \cup T_r$ and for each i with $1 \leqq i \leqq r$, every a-subset of T_i is an a-sum of result.* 1. *Then*

$$|T| \leqq a(b - 1) + r(a - 1).$$

Proof. For each i, we form as many a-sums in T_i as possible. Suppose after running through all of the T_i's, we have formed c a-sums. All of these a-sums have result 1, so we can form an n-sum of result 1 unless $c \leqq b - 1$. If, after removing the elements to form these a-sums, there is a T_i with at least a elements remaining, we can form another a-sum of result 1. Thus no T_i has more than $a - 1$ elements remaining. We have used at most $a(b - 1)$ elements of T to form a-sums and there are at most $r(a - 1)$ elements remaining. Therefore

$$|T| \leqq a(b - 1) + r(a - 1).$$

Proof of Theorem 1. We will use additive notation here when we are working with abelian groups. Assume that G is a counter-example of minimal order and let S be a $(2n - 2)$-subset of G containing no n-sum of result 1. We observe that if G is abelian and x is an element of G, then $S + x$ is also a $(2n - 2)$-set containing no n-sum of result 0. Clearly then we may replace S by $S + x$ and assume that

$$r(0, S) \geqq r(y, S) \quad \text{for all } y \text{ in } S.$$

The proof proceeds in a series of steps.

Step 1. If G is abelian and S contains exactly 3 distinct elements x, y, and z, then it is not the case that $x = 0$ and $y = -z$.

Proof. If not, we may assume that

$$r(0, S) \geqq r(y, S) \geqq r(-y, S).$$

Choose T a subset of $[y, S]$ with $|T| = r(-y, S)$. Then in the set $T \cup [-y, S]$, there is a $2i$-sum of result 0 for $1 \leqq i \leqq |T|$. Since $r(0, S) > 0$, S contains an n-sum of result 0 unless

$$r(0, S) + 2r(-y, S) \leqq n - 1,$$

and since $r(y, S) \leqq n - 1$,

$$r(0, S) + r(y, S) + 2r(-y, S) \leqq 2n - 2.$$

But $r(-y, S) > 0$, so

$$|S| = r(0, S) + r(y, S) + r(-y, S) < 2n - 2.$$

This is a contradiction.

Step 2. If G is abelian, then n is not prime.

Proof. Suppose that n is prime. We observe that S must contain at least three distinct elements. We have that $r(0, S) \leqq n - 1$ and since we may assume that $r(0, S) \geqq r(x, S)$ for all x in $G - \{0\}$, it follows that $r(x, S) \leqq n - 2$ for all x in $G - \{0\}$. Choose g, a non-zero element of S. Step 1 implies that there is an element h in S which is not 0 or g or $-g$. Let $T_1 = \{0, g\}$ and $T_2 = \{0, h\}$. No element of $S - (T_1 \cup T_2)$ appears more than $n - 2$ times, so we can partition $S - (T_1 \cup T_2)$ into $n - 2$ non-empty ordinary subsets of G. Call these subsets $T_3, \ldots, T_n$, and let

$$A = T_1 + T_2 + \ldots + T_n.$$

Clearly $|T_1 + T_2| = 4$. Proposition 1 applied $n - 2$ times implies that $A = G$ which contradicts the non-existence of an n-sum of result 0.

Step 3. G is not isomorphic to $Z_a \times Z_b$ where $1 < a < b$.

Proof. Suppose that G is isomorphic to $Z_a \times Z_b$. Clearly $b \geqq 3$. By applying Lemma 1 to $Z_a \lhd G$ and $Z_b \lhd G$, we can assume there are exactly at most four distinct elements in S and, by replacing S by $S + u$ for the appropriate u and observing that S still must generate G, that these elements are $w = (0, 0)$, $x = (1, 0)$, $y = (0, 1)$, and $z = (1, 1)$. We may also assume that $r(w, S)$ is at least as large as each of $r(x, S)$, $r(y, S)$, and $r(z, S)$. Applying Lemma 3 to $[w, S] \cup [x, S]$ we conclude that

$$r(w, S) + r(x, S) \leqq a(b - 1) + 2(a - 1) = ab + a - 2,$$

and hence that

$$r(y, S) + r(z, S) \geqq (2n - 2) - (ab + a - 2) = a(b - 1) \geqq 2a.$$

If $r(y, S) > 0$, we can form an a-sum in $[y, S] \cup [z, S]$ of result $(0, a)$ and still have an element $y = (0, 1)$ left over. If $b = 3$ then $a = 2$ and $|S| = 10$, and thus

$$r(w, S) \geqq 3 = 2a - 1.$$

If $b > 3$ then

$$|S| = 2n - 2 \geqq 8a - 2$$

so $r(w, S) \geqq 2a$. In either case, we can form an a-sum of result $(0, 1)$ and another of result $(0, 0)$ in $[w, S] \cup \{y\}$. This contradicts Lemma 1, and thus $r(y, S) = 0$. Therefore $r(z, S) \geqq 2a$. Thus if $r(x, S) > 0$, we can form two a-sums in $[z, S] \cup [x, S]$, one of result $(0, a)$ and one of result $(0, a - 1)$. But there is an a-sum of result $(0, 0)$ in $[w, S]$, which again contradicts Lemma 1. Hence $r(x, S) = 0$ and the assertion follows.

Step 4. G is not cyclic of prime power order.

Proof. Suppose that G is cyclic of order p^a, and let $H = \langle x \rangle$ be its unique subgroup of order p. We apply Lemma 1 to G/H. We conclude that S can be partitioned in two subsets S_1 and S_2 with S_1 contained in H and S_2 contained in the coset $H + g$. Lemma 2 implies that g is a generator of G and that

$$|S_1| \equiv |S_2| \equiv -1 (\text{mod } p^{a-1}).$$

We may assume that $|S_1| \geqq |S_2|$, and thus that $|S_1| \geqq p^a - 1$. Now any $(2p - 1)$-subset of S_1 contains a p-sum of result 0. Thus if

$$|S_1| \geqq p^a + p - 1$$

we can find a p^a-sum of result 0. We conclude that

$$|S_1| < p^a + p - 1$$

and hence

$$|S_1| = |S_2| = p^a - 1.$$

Every element of S_1 can be written in the form $u_i = c_i x$ and every element of S_2 can be written in the form $v_i = g + d_i x$ for $1 \leqq i \leqq p^a - 1$, where c_i and d_i are integers with $0 \leqq c_i, d_i \leqq p - 1$. Since S is not a counter-example if all the c_i's are identical and all the d_i's are identical, we may assume that not all of the c_i's are identical. Hence there is a (p^{a-1})-sum in S_1 of result other than 0. Since S_1 is contained in H, any $(2p - 1)$-subset of S_1 contains a p-sum of result 0. It follows that any $(p^{a-1} + p - 1)$-subset of S_1 contains a (p^{a-1})-sum of result 0. Thus, besides the (p^{a-1})-sum of result different from 0, we can find $p - 2$ other (p^{a-1})-sums in S_1, all of result 0.

Now look at $S_2 - g$. This set consists of elements of H, so, just as above, it must contain $p - 1$ (p^{a-1})-sums of result 0. Hence S_2 contains $p - 1$ (p^{a-1})-sums of result $p^{a-1} g$. Since Lemma 2 implies that g generates G, we know that $p^{a-1} g$ is an element of H but is not 0. We now have $2p - 2$ (p^{a-1})-sums in H but exactly $p - 2$ of these have result 0. This contradicts Lemma 1, even when $p = 2$.

Step 5. G is not elementary abelian of rank 2.

Proof. If G is elementary abelian of rank 2, then G is isomorphic to $Z_p \times Z_p$. By applying Lemma 1 to each factor in the product, we conclude that there are at most 4 distinct elements in S. We can take these elements to be $w = (0, 0)$, $x = (1, 0)$, $y = (0, 1)$, and $z = (1, 1)$. Any p-subset of $[z, S]$ is a p-sum of result $(0, 0)$, and the same is true for the sets $[w, S]$, $[x, S]$, and $[y, S]$. Thus Lemma 3 implies that

$$|S| \leqq p(p - 1) + 4(p - 1) = p^2 + 3p - 4.$$

But $|S| = 2p^2 - 2$ so $2p^2 - 2 \leqq p^2 + 3p - 4$ and hence $p(p - 3) + 2 \leqq 0$. Thus $p = 2$, $|G| = 4$ and $|S| = 6$. There cannot be two different 2-sums of result $(0, 0)$ in S, so at most one element in S can appear more than once. Since that element cannot appear as many as 4 times all of w, x, y and z must appear in S. This is impossible because

$$x + y + z + w = (0, 0).$$

Step 6. G is not abelian.

Proof. Suppose the contrary and let P be a Sylow-p subgroup of G with $|P| > 1$. Lemma 1 implies that G/P is cyclic. If Q is a Sylow-q subgroup of G with $q \neq p$ we conclude that Q is cyclic and, by applying Lemma 1 to G/Q, that P is cyclic. Thus either G is cyclic or G is a p-group. Steps 2, 3, and 4 imply that G is not cyclic, so G must be a non-cyclic abelian p-group. If H, the Frattini subgroup of G, is non-trivial, then G/H must be cyclic. But then G is cyclic, which is a contradiction. Therefore H is trivial and thus G is elementary abelian. Step 5 implies that the rank of G is at least 3. If K is any subgroup of G with $|K| = p$, then G/K is not cyclic. This is a contradiction.

Step 7. Final contradiction.

Proof. Step 6 implies that G is a solvable, non-abelian group. Choose $H \lhd G$ so that $|G/H|$ is prime. Observe that G/H is cyclic. Lemma 1 implies that H is cyclic. Let $|G/H| = a$ and $|H| = b$. If there are $ab + b - 1$ elements of S in H, we can form a b-sums of result 1 and hence an n-sum of result 1, so we may assume that there are at least

$$(2ab - 2) - (ab + a - 2) = a(b - 1)$$

elements in S but not in H. Let T be the set of those elements.

Now G is non-abelian, so $b > 2$, and thus $|T| \geqq 2a$. Now $|G/H| = a$, so it follows that T contains an a-sum with result in H. Using Lemma 1, we extend this a-sum to a set of $2b - 2$ a-sums of S with results in H. Let Z be the set of results of these a-sums. At least one of these a-sums consists entirely of elements of $G - H$. Let $U = \{u_1, \ldots, u_a\}$ be this a-sum. Since G/H is abelian, any rearrangement of the elements of U also has result in H. Rearrangement cannot change the result of U without contradicting Lemma 1. Thus the elements of U, indeed of any a-sum with result in H, may be rearranged without affecting the result. Let h be the result of U. We may assume that $h = xy = yx$ where x is an element of $G - H$. Clearly x commutes with h.

Lemma 1 implies that there are exactly two distinct elements of Z. Let $k \neq h$ be the other element that appears in Z. Lemma 1 implies that

$$r(h, Z) = r(k, Z) = b - 1,$$

and Lemma 2 implies that $\langle h, k \rangle = H$. Let

$$Y = Z - \{h, k\}.$$

The results of realizable $(b - 2)$-sums of Y are of the form

$$h^r k^{b-r-2} \quad \text{for } 0 \leqq r \leqq b - 2.$$

If these results are not all distinct, then it must be the case that $h^s = k^s$ for some s with $1 \leqq s \leqq b - 2$. Then $h^s k^{b-s} = 1$ is a realizable result of a b-sum in Z. We conclude that there are $b - 1$ distinct results of $(b - 2)$-sums in Y. If $(hk)^{-1}$ is one of these results then we can form a b-sum of result 1 in Z. Thus we conclude that all of the elements of H except $(hk)^{-1}$ are realizable as results of $(b - 2)$-sums in Y.

Now if we can rearrange the elements in an a-sum of result of h and an a-sum of result k to obtain a $2a$-sum with result in H different from hk, then this result will have an inverse which is realizable as a $(b - 2)$-sum in Y. Then we can combine these two sums and form an n-sum of result 1. Since this is impossible we may assume that no such rearrangement exists. But $h = xy$ and G/H is abelian, so xky is in H. Therefore

$$hk = kh = kxy = xky \quad \text{and} \quad xk = kx.$$

But $|G/H|$ is prime and $\langle h, k \rangle = H$, so $\langle x, h, k \rangle = G$. Now h and k commute, and it follows that G is abelian. This final contradiction establishes the theorem.

We remark that it is now easy to classify all solvable groups G of order n and $(2n - 2)$-subsets S of G such that S contains no n-sum of result 1.

COROLLARY. *Let G be a solvable group of order n and let S be a* $(2n - 2)$*-subset of G. Then S contains no n-sum of result* 1 *if and only if both of the following conditions hold*:

1. *G is cyclic, and*
2. *S can be written as $S = T + x$ (G is abelian) where x is an arbitrary element of G and T consists of* $n - 1$ 0's *and* $n - 1$ g's *with* $\langle g \rangle = G$.

REFERENCES

1. A. L. Cauchy, *Recherches sur les nombres*, Journal Ecole Polytechnique *9* (1813), 99-123.
2. Erdös, Ginsburg and Ziv, *Theorem in additive number theory*, Bull. Res. Coun. Israel *10* (1961), 41-43.

Middlebury College,
Middlebury, Vermont.