BULL. AUSTRAL. MATH. SOC. MOS 05B10

VOL. 4 (1971), 407-418. (20D99, 20K99)

Maximal sum-free sets in cyclic groups of prime-power order

Anne Penfold Street

A subset S of an additive group G is called a maximal sum-free set in G if $(S+S) \cap S = \emptyset$ and $|S| \geq |T|$ for every sum-free set T in G. In this paper, the maximal sum-free sets in cyclic p-groups are characterized to within automorphism.

Given an additive group G and non-empty subsets S, T of G, let $S + T$ denote the set $\{s+t;\ s \in S,\ t \in T\}$, $\bar{S}$ the complement of S in G and $|S|$ the cardinality of S. We call S a *sum-free set* in G if $(S+S) \subseteq \bar{S}$. If, in addition, $|S| \geq |T|$ for every sum-free set T in G, then we call S a *maximal sum-free set* in G. We denote by $\lambda(G)$ the cardinality of a maximal sum-free set in G.

Exact values of $\lambda(G)$ were given by Diananda and Yap [*1*] for $|G|$ divisible by 3 or by at least one prime $q \equiv 2\ (3)$. When every prime divisor of $|G|$ is a prime $p \equiv 1\ (3)$ then, by [*1*], $|G|(m-1)/3m \leq \lambda(G) \leq (|G|-1)/3$, where m is the exponent of G, and it is conjectured that in fact

$$(1) \qquad |G|(m-1)/3m = \lambda(G) .$$

This conjecture was verified in [*1*] for Z_n, the cyclic group of order n, and by Rhemtulla and Street [*4*] for elementary abelian p-groups.

Maximal sum-free sets have been characterized (up to automorphism) for the following classes of abelian p-groups:

Received 18 December 1970.

(i) for Z_p , with $p \equiv 2\ (3)$ in [*1*] and [*6*], and with $p \equiv 1\ (3)$ in [*4*], (see also partial results in [*7*]);

(ii) for elementary abelian p-groups, with $p \equiv 2\ (3)$ in [*1*], and with $p \equiv 1\ (3)$ in [5];

(iii) for Z_{p^α} , with $p \equiv 2\ (3)$ in [*1*].

Here we extend the argument of [*4*] to characterize the maximal sum-free sets in Z_{p^α} with $p \equiv 1\ (3)$. More precisely, we prove the following:

THEOREM. *Let* $G = Z_{p^\alpha}$ *, where* $p = 3k + 1$ *is prime and* $p^\alpha = 3k_\alpha + 1$ *. Then any maximal sum-free set* S *may be mapped, under some automorphism of* G *, to one of the following:*

$$A_\alpha = \{k_\alpha,\ k_\alpha+2,\ \ldots,\ 2k_\alpha-1,\ 2k_\alpha+1\}\ ;$$

$$B_\alpha = \{k_\alpha,\ \ldots,\ 2k_\alpha-1\}\ ;$$

$$C_\alpha = \{k_\alpha+1,\ \ldots,\ 2k_\alpha\}\ .$$

DEFINITION. Let C be a subset and H a subgroup of an abelian group G .

(i) C is said to be in *arithmetic progression* if $C = \{g+id \mid i = 0, 1, \ldots, |C|-1\}$, for some $g, d \in G$, $d \neq 0$. If so, d is called a *difference* of C .

(ii) C is said to be *aperiodic* if $C + H = C$ implies $H = \{0\}$.

(iii) C is said to be *periodic* if $C + H = C$ for some $H \neq \{0\}$. If so, H is called a *period* of C .

(iv) C is said to be *quasiperiodic* if $C = C' \cup C''$, where $C' \cap C'' = \emptyset$, $C' + H = C'$ for some $H \neq \{0\}$ and C'' is contained in one coset of H . If so, H is called a *quasiperiod* of C .

Notation. Let $G = Z_{p^\alpha}$ and let $H \neq \{0\}$ be a subgroup of

G, $H = Z_{p^\beta}$. If S is a maximal sum-free set in G , then S_i denotes the subset of H such that $S_i + i = S \cap (H+i)$, where $H + 1$ generates G/H and $i = 0, 1, \ldots, p^{\alpha-\beta}-1$.

The proof of the theorem depends primarily on results of Kemperman [2], especially on Theorems 2.1 and 3.4 and Lemma 4.3. We also need Kneser's Theorem [3], the lemma of [4] and the following simple results.

LEMMA 1. *Let* $G = Z_{p^\alpha}$, $p = 3k + 1$, *and let* C *be a subset of* G *in arithmetic progression, with difference* d . *If* $|C| > p^\alpha/7$, *then* d *has order* p^α .

LEMMA 2. *Let* $G = Z_{p^\alpha}$ *where* $p = 3k + 1$ *and* $p^\alpha = 3k_\alpha + 1$. *Let* $H \neq \{0\}$ *be a subgroup of* G , $H = Z_{p^\beta}$, *and let* S *be a maximal sum-free set in* G .

(i) *Let* $I = \left\{i \mid i = 0, 1, \ldots, p^{\alpha-\beta}-1;\ |S_i| \geq \left(p^\beta+1\right)/2\right\}$. *Let* $L = \left\{l \mid l = 0, 1, \ldots, p^{\alpha-\beta}-1;\ S_l = \emptyset\right\}$. *Then* $I + I \subseteq L$.

(ii) *If* $S_0 \neq \emptyset$, *then* $S_i \neq H$ *for any* $i = 0, 1, \ldots, p^{\alpha-\beta}-1$.

(iii) $\lambda(G) > \lambda(G/H)|H|$.

(iv) *Suppose the theorem is true for* Z_{p^δ} , *for all* $\delta < \alpha$. *Then* $S_i = H$ *for fewer than* $k_{\alpha-\beta}$ *values of* i .

Proof. *(i)* Since S is sum-free,

$$(S_i+S_j) \cap S_{i+j} = \emptyset . \tag{2}$$

By Kneser's Theorem [3], there exists some subgroup $K < H$, $|K| = p^\gamma$, such that $S_i + S_j + K = S_i + S_j$ and $|S_i+S_j| \geq |S_i+K| + |S_j+K| - |K|$.

Since $|S_i| \geq \left(p^\beta+1\right)/2$, we must have $|S_i+K| \geq \left(p^\beta+p^\gamma\right)/2$ and

https://doi.org/10.1017/S000497270004675X Published online by Cambridge University Press

similarly for S_j . Hence $|S_i+S_j| \geq 2(p^\beta+p^\gamma)/2 - p^\gamma = p^\beta$ and $S_{i+j} = \emptyset$.

(ii) Apply (2) in the particular case $j = 0$.

(iii) $$\lambda(G) = k_\alpha = k(p^{\alpha-1} + \ldots + p+1) ,$$

$$\lambda(G/H)|H| = k_{\alpha-\beta}p^\beta = k(p^{\alpha-1} + \ldots + p^\beta) .$$

(iv) By *(i)*, if $S_i = H$ then $i \in I$ which is a sum-free set in $G/H = Z_{p^{\alpha-\beta}}$. Hence $S_i = H$ for at most $k_{\alpha-\beta}$ values of i .

Suppose $S_i = H$ for $k_{\alpha-\beta}$ values of i and let $T = \left\{i \in Z_{p^{\alpha-\beta}} \mid S_i = H\right\}$. Then T may be mapped (under automorphism of G/H) tc one of the sets $A_{\alpha-\beta}$, $B_{\alpha-\beta}$, $C_{\alpha-\beta}$.

Now $A_{\alpha-\beta} + A_{\alpha-\beta} = \overline{A_{\alpha-\beta}}$, so if $T = A_{\alpha-\beta}$ then, by (2), $S_i = \emptyset$ for all $i \notin T$.

$$\left(B_{\alpha-\beta}+B_{\alpha-\beta}\right) \cup B_{\alpha-\beta} = \overline{\{k_\alpha-2, k_\alpha-1\}} .$$

Hence if $T = B_{\alpha-\beta}$ then, by (2), $S_i = \emptyset$ for all $i \notin T$ except possibly for $i = k_\alpha - 2$ or $k_\alpha - 1$. If $k_\alpha = 2$, then $S_{k_\alpha-2} = S_0 = \emptyset$ by *(ii)*; if $k_\alpha > 2$, then $2(k_\alpha-2) \in T$ so, by (2), $S_{k_\alpha-2} = \emptyset$. Also $2(k_\alpha-1) \in T$ so $S_{k_\alpha-1} = \emptyset$. Hence $S_i = \emptyset$ for all $i \notin T$.

A similar argument shows that if $T = C_{\alpha-\beta}$, then $S_i = \emptyset$ for all $i \notin T$.

Hence $\lambda(G) = \lambda(G/H)|H|$ which contradicts *(iii)*.

Proof of the Theorem. We proceed by induction on α . For $\alpha = 1$, the theorem reduces to Theorem 2 of [4].

By [1], for any α , $|S| = k_\alpha = (p^\alpha-1)/3$. Since S is sum-free, we must have $|S+S| \leq 2|S| + 1$ and $|S-S| \leq 2|S| + 1$.

Suppose that $|S+S| < 2|S| - 1$. By Kneser's Theorem [3], there exists a subgroup $H < G$, $H \neq \{0\}$, such that $S + S + H = S + S$ and $|S+S| \geq 2|S+H| - |H|$. By Lemma 1 of [1], $S + H = S$, which implies that $|H| \,\Big|\, |S|$. Since $|H| = p^{\beta}$, $1 \leq \beta < \alpha$, we have a contradiction. Hence $|S+S| \geq 2|S| - 1$ and a similar argument shows that $|S-S| \geq 2|S| - 1$.

Now $S - S = -(S-S)$ and $0 \in S - S$. Hence $|S-S|$ is odd and can take one of two values: $|S-S| = 2|S| \pm 1$.

I. If $|S-S| = 2|S| - 1$ then, by Theorem 2.1 of [2], either $S - S$ is in arithmetic progression or $S - S$ is quasiperiodic.

Suppose that $S - S$ is quasiperiodic. Now $|S-S| = 2k(p^{\alpha-1} + \ldots + p+1) - 1$. Hence there exists a subgroup $H < G$, $|H| = p^{\beta} \geq p$, such that $S - S$ consists of the union of $2k(p^{\alpha-\beta-1} + \ldots + p+1)$ complete cosets of H, together with $2k(p^{\beta-1} + \ldots + p+1) - 1$ elements, all contained in one other coset of H. Since $|G/H| = p^{\alpha-\beta}$ and since $S - S = -(S-S)$, these $2k(p^{\beta-1} + \ldots + p+1) - 1$ leftover elements must belong to H itself. Since $|(S-S) \cup S| = |G| - 2$, at least $k(p^{\beta-1} + \ldots + p+1)$ of the remaining elements of H must belong to S. But $k(p^{\beta-1} + \ldots + p+1) = k_{\beta} = \lambda(H)$, so $|S_0| = k_{\beta}$. So the remaining $k(p^{\alpha-\beta-1} + \ldots + p+1)$ cosets of H must be contained in S, contradicting Lemma 2 *(ii)*.

Hence $S - S$ is in arithmetic progression. Since $|S-S| = 2k_{\alpha} - 1$, Lemma 1 shows that the difference, d, of $S - S$ must be of order p^{α}. By Lemma 4.3 of [2], S (and $-S$) must also be in arithmetic progression with difference d. Hence S may be mapped (by some automorphism of G) to B_{α} or C_{α}.

II. If $|S-S| = 2|S| + 1$, then $S - S = \overline{S}$. Hence $S = -S$, $S + S = S - S$ and we may apply the Lemma of [4].

(a) Suppose that, for some $g \in G$, $|(S+g) \cap S| = 1$. Then by the

https://doi.org/10.1017/S000497270004675X Published online by Cambridge University Press

lemma, $|(S+3g/2)\cap S| \geq k_\alpha - 3$.

If $p \nmid g$, map $3g/2$ to 1 so that $g = k_\alpha + 1$. The first part of the argument of Theorem 2 of [4] shows that S may be mapped, under automorphism of G , to A_α .

If $p^{\alpha-\beta} \mid g$, $p^{\alpha-\beta+1} \nmid g$, map $3g/2$ to $p^{\alpha-\beta}$ so that $g = \left(kp^{\beta-1} + kp^{\beta-2} + \ldots + kp + k+1\right)p^{\alpha-\beta} = \left(k_\beta+1\right)p^{\alpha-\beta}$. Now $\left|\left(S+p^{\alpha-\beta}\right)\cap S\right| \geq k_\alpha - 3$. Let $H = Z_{p^\beta} = \langle p^{\alpha-\beta}\rangle$. Then

$$S = \bigcup_{i=0}^{p^{\alpha-\beta}-1} \left(S_i+i\right) \quad \text{and} \quad \left|\left(S+p^{\alpha-\beta}\right)\cap S\right| = \sum_{i=0}^{p^{\alpha-\beta}-1} \left|\left(S_i+p^{\alpha-\beta}\right)\cap S_i\right| .$$

Note that $S_i + p^{\alpha-\beta} = S_i$ if and only if $S_i = \emptyset$ or $S_i = H$.

If $\left|\left(S+p^{\alpha-\beta}\right)\cap S\right| = k_\alpha$, then S consists of a union of complete cosets of H . Hence $|H| \,\Big|\, |S|$ which is a contradiction.

If $k_\alpha - 1 \geq \left|\left(S+p^{\alpha-\beta}\right)\cap S\right| \geq k_\alpha - 3$, we have to consider several possibilities for S :

(i) S consists of a union of $k\left(p^{\alpha-\beta-1} + \ldots + p+1\right) = k_{\alpha-\beta}$ complete cosets of H , together with $k\left(p^{\beta-1} + \ldots + p+1\right)$ other elements distributed between one, two or three other cosets of H . But this contradicts Lemma 2 *(iv)*.

(ii) S consists of a union of $k_{\alpha-\beta} - 1$ complete cosets of H , together with $p^\beta + k\left(p^{\beta-1} + \ldots + p+1\right)$ other elements distributed between two or three other cosets of H . But since $S = -S$, one of the complete cosets must be H itself, contradicting the sum-freeness of S .

(iii) S consists of a union of $k_{\alpha-\beta} - 2$ complete cosets of H , together with $2p^\beta + k\left(p^{\beta-1} + \ldots + p+1\right)$ other elements distributed

https://doi.org/10.1017/S000497270004675X Published online by Cambridge University Press

between three other cosets of H . Since $S = -S$, one of these three other cosets must be H itself. Since $\lambda(H) = k_\beta = k(p^{\beta-1} + \ldots + p+1)$, at most k_β of the remaining elements belong to H , and in fact $k_{\alpha-\beta}$ complete cosets of H are contained in S . This is impossible by (i).

(b) We are now left with the case where $|(S+g) \cap S| \neq 1$ for any $g \in G$.

(i) Suppose that by taking an automorphism of G , we may ensure that $|(S+1) \cap S| \geq |(S+g) \cap S|$ for all $g \in G$. We list the elements of S as follows:

(3) $$S = \{a_1, \ldots, a_1+l_1, a_2, \ldots, a_2+l_2, \ldots, a_h, \ldots, a_h+l_h\}$$

where $0 < a_1 \leq a_1+l_1 < a_2-1 < a_2+l_2 < \ldots < a_h-1 < a_h+l_h < p^\alpha$ and $a_i, \ldots, a_i+l_i$ denotes a string of (l_i+1) consecutive elements of S . Since $S = -S$,

(4) $$a_{h-i} + l_{h-i} = p^\alpha - a_{i+1} , \text{ for all } i = 0, 1, \ldots, h-1 ,$$

and $|(S+1) \cap S| = k_\alpha - h \geq |(S+g) \cap S|$ for all $g \in G$. Hence h is minimal in (3) and we show that $h = 2$.

Let $X = \{a_1, \ldots, a_h\}$ and let

$$Y = \{a_1+l_1+1, \ldots, a_h+l_h+1\} = \{1-a_1, \ldots, 1-a_h\} = 1 - X$$

by (4). A repetition of the argument of [4] shows that $|(S+a_i-1) \cap S| \geq h - 1$ and

(5) $$h \geq |(X+a_i) \cap Y| \geq h - 1 \text{ for all } i = 1, \ldots, h .$$

If $|X+X| \geq 2h - 1$, the argument of [4] shows that $h = 2$ and S maps under automorphism to A_α .

If $|X+X| \leq 2h - 2$, then by Kneser's Theorem [3], $X + X$ is periodic so that for some subgroup $H < G$, $H = Z_{p^\beta}$, we have $X + X + H = X + X$ and $|X+X| \geq 2|X+H| - |H|$. Using Theorem 3.4 of [2], we can construct all possible sets X . We choose a subset X^* of G/H such that $X^* + X^*$ is aperiodic in G/H and $|X^*+X^*| = 2|X^*| - 1$. If σ denotes the natural mapping of G to G/H , then X can be any subset of $\sigma^{-1}X^*$, such that $|\sigma^{-1}X^* \cap \overline{X}| \le (p^\beta-1)/2$. Hence any coset of H which contains the first element of a string of elements of S must contain the first elements of at least $(p^\beta+1)/2$ strings of S .

By (5), $X + X$ contains all of Y except possibly one element, say y . Since $X + X$ consists of a union of complete cosets of H , $(H+y) \cap Y = \{y\}$. Since $Y = 1 - X$, this implies that $|\sigma^{-1}X^* \cap \overline{X}| \ge p^\beta - 1$ which is impossible. Hence $Y \subseteq X + X$. We can now describe the distribution of the strings of S . Suppose

$$X^* = \{H+i_1, \ldots, H+i_l\} \text{ for some } i_1, \ldots, i_l \in \{0, 1, \ldots, p^{\alpha-\beta} - 1\} .$$

In each coset $H + i_j$, more than half of the elements of the coset are starting points of strings of S . Since $S = -S$, the strings finish in the cosets of $-X^*$. If a string finishes in $H - i_j$, then the next coset $H + (1-i_j) \in Y \subseteq X + X$. Hence no string can continue into this coset, and similarly no string could pass through $H + i_j - 1$.

Hence any coset which contains an element of S contains at least $(p^\beta+1)/2$ elements of S . By Lemma 2 *(i)*, the cosets containing elements of S must therefore form a sum-free set in G/H . Hence $|S| = \lambda(G) \le \lambda(G/H)|H|$, contradicting Lemma 2 *(iii)*.

(ii) Finally suppose that by taking an automorphism of G , we may ensure that $|(S+p^{\alpha-\beta}) \cap S| \ge |(S+g) \cap S|$ for all $g \in \overline{S}$ and that $|(S+p^{\alpha-\beta}) \cap S| > |(S+g) \cap S|$ for all $g \in \overline{S}$ such that $p^{\alpha-\beta} \nmid g$. Let $H = \langle p^{\alpha-\beta} \rangle = Z_{p^\beta}$ and let $q = p^{\alpha-\beta}$ for the remainder of this section.

For each $i = 0, 1, \ldots, q-1$, we have $S_i = \emptyset$ or $S_i = H$ or

$$S_i = \{a_{1i}q, \ldots, (a_{1i}+l_{1i})q, a_{2i}q, \ldots, (a_{2i}+l_{2i})q, \ldots$$
$$\ldots, a_{\nu_i i}q, \ldots, (a_{\nu_i i}+l_{\nu_i i})q\}$$

where $0 < a_{1i} \le a_{1i}+l_{1i} < a_{2i}-1 < a_{2i}+l_{2i} < \ldots < a_{\nu_i i}-1 < a_{\nu_i i}+l_{\nu_i i} < p^\beta$ and $a_{ji}q, \ldots, (a_{ji}+l_{ji})q$ denotes the set of $(l_{ji}+1)$ consecutive multiples of q which we call an H-string in S.

Let $I = \{i \mid i = 0, 1, \ldots, q-1;\ 1 \le |S_i| \le p^\beta-1\}$. Since $S_i + q = S_i$ if and only if $i \notin I$, we have

(6) $$|(S+q)\cap S| = |S| - \sum_{i\in I} \nu_i > |(S+g)\cap S| \text{ for all } g \in G,\ q \nmid g .$$

Let $X = \{a_{ji}q+i \mid i = 0, 1, \ldots, q-1;\ j = 1, \ldots, \nu_i\}$. Since $S = -S$, we have $\nu_i = \nu_{q-i}$ and $(a_{ji}+l_{ji})q + i = p^\alpha - [a_{\nu_i-j+1,q-1}q+(q-i)]$, implying that

(7) $$(a_{ji}+l_{ji})q = p^\alpha - a_{\nu_i-j+1,q-i}q .$$

Let

$$Y = \{(a_{ji}+l_{ji}+1)q + i \mid i = 0, 1, \ldots, q-1;\ j = 1, \ldots, \nu_i\}$$
$$= q - X \text{ by (7).}$$

Now $(a_{ji}-1)q + i \in \overline{S}$ so, by (6) and the lemma of [4],

$$\left|[S + (a_{ji}-1)q + 1]\cap S\right| \ge \left(\sum_{i\in I} \nu_i\right) - 1 = |X| - 1 .$$

But for any $s_1, s_2 \in S$, $s_1 + (a_{ji}-1)q + i = s_2$ implies that $s_1 \in X$, $s_2 \in -X$ and $s_1 + a_{ji}q + i \in Y$. Hence

(8) $$|X| = \sum_{i\in I} \nu_i \ge |(X+a_{ji}q+i)\cap Y| \ge \left(\sum_{i\in I} \nu_i\right) - 1 = |X| - 1$$

for all j, i.

https://doi.org/10.1017/S000497270004675X Published online by Cambridge University Press

If $|X+X| \geq 2|X| - 1$, then $X + X$ contains at least $|X| - 1$ elements of $\overline{Y}$ but $X + a_{ji}q + i$ contains at most one element of $\overline{Y}$. Thus for at least $|X| - 2$ values of (j, i), we have $2(a_{ji}q+i) \notin Y$. But $2(a_{ji}q+1) \notin Y$ implies that $q(1-a_{ji}) - i \notin X + a_{ji}q + i$, since $Y = q - X$. Hence for at least $|X| - 2$ values of (j, i),

$$\begin{aligned}(X+a_{ji}q+i) \cap Y &= \{(a_{mn}+a_{ji})q + i + n \mid a_{mn}q + n \in X, (m, n) \neq (j, i)\} \\ &= \{q - (a_{mn}q+n) \mid a_{mn}q + n \in X, (m, n) \neq (j, i)\} .\end{aligned}$$

Hence, summing these two expressions for the elements of $(X+a_{ji}q+i) \cap Y$, we have

$$(|X|-3)(a_{ji}q+i) \equiv (|X|-1)q - 2 \sum_{n \in I} \sum_{m=1}^{\nu_n} (a_{mn}q+n) \pmod{p^\alpha} .$$

Hence $|X| \leq 3$ and S contains at most three H-strings, together with complete cosets of H.

If $|X| = 0$, S is a union of cosets of H. This implies $|H| \mid |S|$ which is a contradiction.

If $|X| = 1$ or 3, then $S = -S$ implies $S_0 \neq \emptyset$. By Lemma 2 *(ii)*, $S_i \neq H$ for any i. Hence

$$|S| \leq \lambda(H) + 2(|H|-1) = 7(p^\beta-1)/3 = 7k_\beta < \lambda(G)$$

by Lemma 2 *(iii)*, since $p \geq 7$.

If $|X| = 2$, then $S = -S$ implies that either $\nu_0 = 2$ and $S_0 \neq \emptyset$ or $\nu_i = \nu_{q-i} = 1$ for some i.

By the previous argument, we must have $S_0 = \emptyset$. Hence S consists of a union of 2λ cosets of H together with two H-strings, each of length at most $p^\beta - 1$.

Thus

$$|S| = k_\alpha \leq 2\lambda p^\beta + 2(p^\beta-1) = 2(\lambda+1)p^\beta - 2 . \tag{9}$$

Since S is sum-free, $2\lambda \le k_{\alpha-\beta}$. If $2\lambda \le k_{\alpha-\beta} - 2$, then (9) becomes

$$k_\alpha \le k_{\alpha-\beta}p^\beta - 2$$

which is a contradiction by Lemma 2 *(iii)*. But if $2\lambda = k_{\alpha-\beta}$, we have a contradiction by Lemma 2 *(iv)*.

If $|X+X| \le 2|X| - 2$, then by Kneser's Theorem [3], $X + X$ is periodic and for some subgroup $K < G$, $K = Z_{p^\gamma}$, we have $X + X + K = X + X$ and $|X+X| \ge 2|X+K| - |K|$. We now apply the argument of (b) (i) to G/K, using (8) instead of (5). If $K \ge H$, then any coset of K is a union of cosets of H. By the previous argument, any coset of K which contains an element of X must contain at least $(p^\gamma+1)/2$ elements of X. Hence there exists a coset of H, more than half of whose elements are starting-points of H-strings in S. This is clearly impossible, so S must consist of a union of complete cosets of H. But this implies $|H| \,\big|\, |S|$ which is a contradiction.

If $K < H$, so that any coset of H is a union of cosets of K, then the argument of (b) (i) shows that any coset of K which contains any element of an H-string in S must contain at least $(p^\gamma+1)/2$ elements of H-strings in S. Hence for each coset, $K + i$, of K either $(K+i) \cap S = \emptyset$ or $|(K+i)\cap S| \ge (p^\gamma+1)/2$. But by Lemma 2 *(i)*, the cosets of K, more than half of whose elements belong to S, form a sum-free set in G/K. Hence $|S| = \lambda(G) \le \lambda(G/K)|K|$, contradicting Lemma 2 *(iii)*.

References

[1] Palahenedi Hewage Diananda and Hian Poh Yap, "Maximal sum-free sets of elements of finite groups", *Proc. Japan Acad.* 45 (1969), 1-5.

[2] J.H.B. Kemperman, "On small sumsets in an abelian group", *Acta Math.* 103 (1960), 63-88.

[3] Henry B. Mann, *Addition theorems: The addition theorems of group theory and number theory* (Interscience Tracts in Pure and Applied Mathematics, number 18; John Wiley, New York, London, Sydney, 1965).

[4] A.H. Rhemtulla and Anne Penfold Street, "Maximal sum-free sets in finite abelian groups", *Bull. Austral. Math. Soc.* 2 (1970), 289-297.

[5] A.H. Rhemtulla and Anne Penfold Street, "Maximal sum-free sets in elementary abelian p-groups", *Canad. Math. Bull.* (to appear).

[6] H.P. Yap, "The number of maximal sum-free sets in C_p", *Nanta Math.* 2 (1968), 68-71.

[7] H.P. Yap, "Structure of maximal sum-free sets in C_p", *Acta Arith.* 17 (1970), 29-35.

University of Queensland,
St Lucia,
Queensland.

https://doi.org/10.1017/S000497270004675X Published online by Cambridge University Press