PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 10, October 1995

A REDUCTION THEOREM ON PURELY SINGULAR SPLITTINGS OF CYCLIC GROUPS

ANDREW J. WOLDAR

(Communicated by Ronald Solomon)

ABSTRACT. A set M of nonzero integers is said to split a finite abelian group G if there is a subset S of G for which $M \cdot S = G\backslash\{0\}$. If, moreover, each prime divisor of $|G|$ divides an element of M, we call the splitting purely singular. It is conjectured that the only finite abelian groups which can be split by $\{1, \ldots, k\}$ in a purely singular manner are the cyclic groups of order 1, $k+1$ and $2k+1$. We show that a proof of this conjecture can be reduced to a verification of the case $\gcd(|G|, 6) = 1$.

1. INTRODUCTION

A set M of nonzero integers is said to *split* a finite abelian group G (written additively) if there is a subset S of G such that every nonzero element of G can be uniquely expressed in the form $m \cdot s$, $m \in M$, $s \in S$, while 0 has no such representation. In this case we write $M \cdot S = G\backslash\{0\}$ and refer to S as a *splitting set* for G. Splittings arise very naturally in the context of certain geometric tiling problems, especially that of lattice tiling Z^n by certain clusters of cubes called "crosses" (corresponding to $M = \{\pm 1, \pm 2, \ldots, \pm k\}$) and "semicrosses" (corresponding to $M = \{1, 2, \ldots, k\}$). The sets $\{1, 2, \ldots, k\}$ and $\{\pm 1, \pm 2, \ldots, \pm k\}$ are usually denoted by $S(k)$ and $F(k)$, respectively ("S" for semicross and "F" for full cross). For details and extensive bibliographies the reader is referred to [4], [5], [6], [7].

A splitting $M \cdot S = G\backslash\{0\}$ is called *nonsingular* if every element of M is relatively prime to $|G|$, and *purely singular* if every prime divisor of $|G|$ divides some element of M. As shown in [3], the study of splittings can be reduced to the study of nonsingular and purely singular splittings.

In this note we restrict our attention to splittings of the form $S(k) \cdot S = G\backslash\{0\}$. As the nonsingular case is fairly well understood [2], we concentrate here on singular splittings, which, by the following result of Hickerson, directs us to the case $G = C(m)$, the cyclic group of order m, $m \geq 1$.

[3, Theorem 2.1.0]. *If $S(k)$ or $F(k)$ splits the finite abelian group G purely singularly, then G is cyclic.*

Received by the editors March 5, 1994.
1991 *Mathematics Subject Classification.* Primary 20K01, 05A18.
This research was supported by NSF grant DMS 9304580 and was completed during the author's stay at the Institute for Advanced Study, Princeton, NJ 08540.

By taking as splitting set $S = \varnothing$, $S = \{1\}$, and $S = \{1, -1\}$, respectively, one sees that $S(k)$ splits $C(1)$, $C(k+1)$, and $C(2k+1)$ for every k; moreover, the splitting is purely singular precisely when the group has nonprime order. It is conjectured that every purely singular splitting is of one of these three types.

Conjecture. If $S(k)$ splits the finite abelian group G purely singularly, then G is one of $C(1)$, $C(k+1)$, or $C(2k+1)$.

Remark. The conjecture has been verified by Hickerson for all $k \leq 3000$.

In this note we show that the conjecture would be confirmed if one could show that it holds for cyclic groups whose order is odd and not a multiple of three.

2. Some preliminary lemmas

Lemma 1. *Let $S(k)$ split $C(m)$, and suppose there exist an integer $a > 0$ and p prime such that* (i) $p \mid m$, (ii) $p \mid ak+1$, *and* (iii) $a \mid p-1$. *Then $ak+1 \mid m$.*

Proof. Let $S = \{s_1, \ldots, s_n\}$ be a splitting set for the assumed splitting, and suppose the elements of S are arranged so that $p \mid s_i$ for $1 \leq i \leq t$ and $p \nmid s_i$ for $t+1 \leq i \leq n$. We claim that for $t+1 \leq i \leq n$, $|\{j: p \mid js_i\}| = \frac{ak-(p-1)}{ap}$. This amounts to showing that $\alpha = \frac{ak-(p-1)}{a}$ is the largest integer less than or equal to k which is divisible by p. That α is an integer follows from (iii). Rewriting the numerator as $ak+1-p$, we see that $p \mid \alpha$ by (ii) (and the fact that $\gcd(a, p) = 1$ from (iii)). Finally, $\alpha < k$ and the next largest integer divisible by p is $\alpha + p > k$. From this it is obvious that $\langle p \rangle = \{0\} \cup \{js_i : 1 \leq j \leq k,\ 1 \leq i \leq t\} \cup \{(hp)s_i : 1 \leq h \leq \frac{ak+1-p}{ap},\ t+1 \leq i \leq n\}$, which gives

$$\frac{nk+1}{p} = |\langle p \rangle| = 1 + kt + \left(\frac{ak+1-p}{ap}\right)(n-t).$$

From this equation it follows that $a + akt + t - n = p(a + akt + t - n)$, hence $n - t = a(1+kt)$. Replacing $n-t$ by $a(1+kt)$ in the displayed equation yields $m = nk + 1 = (ak+1)(tk+1)$. □

Remark. Observe that the constant t introduced in the proof of Lemma 1 does not depend on the choice of prime p satisfying the conditions of the lemma.

Lemma 2. *$S(k)$ does not split $C(m)$ in a purely singular manner for $m = (k+1)(2k+1)$.*

Proof (due to D. R. Hickerson). Assume that $S(k)$ splits $C(m)$ with splitting set S, i.e., $C(m)\backslash\{0\} = S(k) \cdot S$. By Theorem 1.2.1 of [3], the splitting induces splittings of the subgroups $\langle 2k+1 \rangle \cong C(k+1)$ and $\langle k+1 \rangle \cong C(2k+1)$ of $C(m)$, that is, there exist $s_1, s_2, s_3 \in S$ such that

$$S(k) \cdot \{s_1\} = \langle 2k+1 \rangle \backslash \{0\}, \qquad S(k) \cdot \{s_2, s_3\} = \langle k+1 \rangle \backslash \{0\}.$$

Set $\overline{S} = S\backslash\{s_1, s_2, s_3\}$. Then $S(k) \cdot \overline{S} = C(m)\backslash(\langle 2k+1 \rangle \cup \langle k+1 \rangle)$. Observe that $\gcd(s, k+1) = 1$ for all $s \in \overline{S}$. Indeed, if $\gcd(s, k+1) = d > 1$, then $\frac{k+1}{d} \cdot s = (k+1)\frac{s}{d} \in \langle k+1 \rangle$, a contradiction as $\frac{k+1}{d} \cdot s \in S(k) \cdot \overline{S}$. One similarly shows that $\gcd(s, 2k+1) = 1$; thus every $s \in \overline{S}$ is co-prime to each of $k+1$ and $2k+1$. Now let a and b be maximal proper divisors

of $k+1$ and $2k+1$, respectively. Then it is immediate that $k+1 \nmid ab$ and $2k+1 \nmid ab$. Thus $ab \in C\backslash(\langle 2k+1\rangle \cup \langle k+1\rangle)$, so $ab = j \cdot s$ for some $j \in S(k)$, $s \in \overline{S}$. This means that $m \mid js - ab$, whence $ab \mid js$. (Here js denotes the ordinary integer product, in contrast to $j \cdot s$ which denotes the group sum of j copies of s.) As ab is co-prime to s we now have $ab \mid j$; in particular, $ab \leq j \leq k$. But, since the splitting is purely singular, $k+1$ and $2k+1$ are each composite, hence $a \geq \sqrt{k+1}$ and $b \geq \sqrt{2k+1}$. Thus $ab \geq \sqrt{(k+1)(2k+1)}$, a contradiction. □

The following lemma generalizes a result of Szabó (see Theorem 2.4 of [8]).

Lemma 3. *$S(k)$ does not split $C(m)$ in a purely singular manner, where $m = (2k+1)^2$.*

Proof. If $2k+1 = p^r$ for some prime p, the result follows from Theorem 3.2 of [9]. Assuming otherwise, we write $2k+1 = ab$, where $a > b$ and $\gcd(a, b) = 1$. In particular, this implies $2k+1 < a^2 < (2k+1)^2$. Now suppose $S(k)$ splits $C(m)$ with splitting set S. As in the proof of Lemma 2, this splitting of $C(m)$ induces one on its subgroup $\langle 2k+1\rangle \cong C(2k+1)$, so there exist $s_1, s_2 \in S$ such that $S(k)\cdot\{s_1, s_2\} = \langle 2k+1\rangle\backslash\{0\}$. Set $\overline{S} = S\backslash\{s_1, s_2\}$. Clearly $a^2 \notin \langle 2k+1\rangle$, hence $a^2 = j\cdot s$ for some $j \in S(k)$, $s \in \overline{S}$. Proceeding as in the proof of Lemma 2, we obtain $a^2 \mid j$, and so the contradiction $2k+1 < a^2 \leq j \leq k$. □

The following lemma is a special case of Theorem 1.2.1 of [3].

Lemma 4. *If $S(k)$ splits each of $C(m)$ and $C(t)$ for t dividing m, then $S(k)$ splits $C(m/t)$.*

3. Main results

Theorem 5. *Suppose $S(k)$ splits $C(m)$ with $k+1$ composite. Then either*
(i) $\gcd(k+1, m) = 1$, *or*
(ii) $k+1$ *divides* m *and* $\gcd(k+1, \frac{m}{k+1}) = 1$.

Proof. Assume 'not (i)' so that $\gcd(k+1, m) > 1$. By Lemma 1 (with $a = 1$ and p any prime divisor of m), we see that $k+1$ divides m. As $S(k)$ splits each of $C(m)$ and $C(k+1)$, it splits $C(\frac{m}{k+1})$ by Lemma 4. Thus, if $\gcd(k+1, \frac{m}{k+1}) > 1$ we can repeat the above argument to conclude that $S(k)$ splits $C(\frac{m}{(k+1)^2})$. But then, again by Lemma 4, $S(k)$ splits $C((k+1)^2)$. This, however, contradicts Theorem 2.1 of [1], which states that such a splitting can occur only if $k+1$ is prime. □

Theorem 6. *Suppose $S(k)$ splits $C(m)$ with $2k+1$ composite. Then either*
(i) $\gcd(2k+1, m) = 1$, *or*
(ii) $2k+1$ *divides* m *and* $\gcd(2k+1, \frac{m}{2k+1}) = 1$.

Proof. Again, assume 'not (i)' so that $\gcd(2k+1, m) > 1$. By Lemma 1 (with $a = 2$ and p any odd prime divisor of m), we see that $2k+1$ divides m. As $S(k)$ splits each of $C(m)$ and $C(2k+1)$, it splits $C(\frac{m}{2k+1})$. Thus, if $\gcd(2k+1, \frac{m}{2k+1}) > 1$ we repeat the above argument to conclude that $S(k)$ splits $C(\frac{m}{(2k+1)^2})$, so it also splits $C((2k+1)^2)$. But this is in violation of Lemma 3. The result follows. □

Theorem 7. *Let $S(k)$ split $C(m)$ in a purely singular manner. Then either*
(i) $\gcd(k+1, m) = 1$, *or*
(ii) $\gcd(2k+1, m) = 1$.

Proof. If $\gcd(k+1, m) > 1$ and $\gcd(2k+1, m) > 1$, then, by Theorems 5 and 6, respectively, we have $k+1 \mid m$ and $2k+1 \mid m$. As $k+1 \mid m$, $S(k)$ splits $C(\frac{m}{k+1})$, and as $2k+1 \mid \frac{m}{k+1}$, $S(k)$ splits $C(\frac{m}{(k+1)(2k+1)})$. But then $S(k)$ splits $C((k+1)(2k+1))$, a contradiction to Lemma 2. □

Theorem 8. *Suppose it is proved for m odd and not a multiple of three (i.e., m congruent to ± 1 modulo 6) that $S(k)$ splits $C(m)$ in a purely singular manner only in the cases $m = 1$, $k+1$, and $2k+1$. Then, for any m, these are the only such splittings.*

Proof. Let m be minimal of the form $nk+1$, $n \geq 3$, such that $S(k)$ splits $C(m)$ in a purely singular manner. By assumption, either $2 \mid m$ or $3 \mid m$. If $2 \mid m$, then k is necessarily odd, and $\gcd(k+1, m) > 1$. By Lemma 4, $S(k)$ splits $C(\frac{m}{k+1})$, whence, by minimality of m, $\frac{m}{k+1} = k+1$ or $2k+1$. The former is ruled out by Theorem 5(ii), the latter by Theorem 7. If $3 \mid m$, then certainly $3 \nmid k$, so either $3 \mid k+1$ or $3 \mid 2k+1$. If $3 \mid k+1$, a contradiction is obtained as in the previous argument. If $3 \mid 2k+1$, then Lemma 4 and the minimality of m together force $\frac{m}{2k+1} = k+1$ or $2k+1$. The former is ruled out by Theorem 7, the latter by Theorem 6. □

We end with some examples which illustrate how our techniques can be applied to specific cases, namely $k = 11$, 13 and 17.

Problem. *Determine all purely singular splittings by $S(11)$.*

Any purely singular splitting of $C(m)$ by $S(11)$ must satisfy $m = 2^a \cdot 3^b \cdot 5^c \cdot 7^d$ for certain nonnegative integers a, b, c and d. As $k+1 = 12$, Theorem 5 tells us that $2^a \cdot 3^b = 1$ or 12. If $c \geq 1$, we can apply Lemma 1 with $p = 5$ and $a = 4$. The result is that $45 \mid m$. But this contradicts $b \leq 1$; so $c = 0$. By Lemma 4, we now have that $S(11)$ splits $C(7^d)$. But, if $d \geq 1$, the group $C(7^d)$ has precisely $6 \cdot 7^{d-1}$ generators. As all generators are of the form $j \cdot s$ for $j \in S(11)$, $j \neq 7$, and $s \in S$, $7 \nmid s$, we see that 10 must divide $6 \cdot 7^{d-1}$, a contradiction. Thus the only groups split by $S(11)$ in a purely singular manner are $C(1)$ and $C(12)$.

Problem. *Determine all purely singular splittings by $S(13)$.*

Any purely singular splitting of $C(m)$ by $S(13)$ must satisfy $m = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 11^e$ for certain nonnegative integers a, b, c, d and e. As $k+1 = 14$, Theorem 5 asserts that $2^a \cdot 7^d = 1$ or 14. As $2k+1 = 27$, we have $3^b = 1$ or 27 by Theorem 6. If $e \geq 1$, apply Lemma 1 with $a = 5$ and $p = 11$. This gives $66 \mid m$, which contradicts Theorem 7; thus $e = 0$. By Theorem 7 we now have $m = 2 \cdot 5^c \cdot 7$ or $m = 3^3 \cdot 5^c$, so, in either case, $S(k)$ splits $C(5^c)$. But, if $c \geq 1$, the group $C(5^c)$ has $4 \cdot 5^{c-1}$ generators. As all generators are of the form $j \cdot s$ for $j \in S(13)$, $j \neq 5$, 10, and $s \in S$, $5 \nmid s$, we see that 11 must divide $4 \cdot 5^{c-1}$, a contradiction. Thus the only groups split by $S(13)$ in a purely singular manner are $C(1)$, $C(14)$ and $C(27)$.

Problem. *Determine all purely singular splittings by $S(17)$.*

Any purely singular splitting of $C(m)$ by $S(17)$ must satisfy $m = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 11^e \cdot 13^f$ for certain nonnegative integers a, b, c, d, e and f. As $k + 1 = 18$, Theorem 5 asserts that $2^a \cdot 3^b = 1$ or 18. As $2k + 1 = 35$, we have $5^c \cdot 7^d = 1$ or 35 by Theorem 6. If $f \geq 1$, apply Lemma 1 with $a = 3$ and $p = 13$; this gives $52 \mid m$, a contradiction as $a \leq 1$. Thus $f = 0$. We now see from Theorem 7 that $m = 2 \cdot 3^2 \cdot 11^e$ or $m = 5 \cdot 7 \cdot 11^e$. In either case $S(17)$ must split $C(11^e)$. If $e \geq 1$, then the group $C(11^e)$ has $10 \cdot 11^{e-1}$ generators. As argued above, this implies $16 \mid 10 \cdot 11^{e-1}$, a contradiction. Thus the only groups split by $S(17)$ in a purely singular manner are $C(1)$, $C(18)$ and $C(35)$.

Acknowledgments

This work was inspired by a talk delivered by Sherman K. Stein at the University of Delaware. I wish to thank Dean Hickerson for generously allowing me access to his unpublished manuscript *Splittings by $S(k)$, Report of work in progress*, which contains many interesting arguments and results.

References

1. S. Galovich and S. Stein, *Splittings of Abelian groups by integers*, Aequationes Math. **22** (1981), 249–267.
2. W. Hamaker and S. Stein, *Splitting groups by integers*, Proc. Amer. Math. Soc. **46** (1974), 322–324.
3. D. Hickerson, *Splittings of finite groups*, Pacific J. Math. **107** (1983), 141–171.
4. D. Hickerson and S. Stein, *Abelian groups and packing by semicrosses*, Pacific J. Math. **122** (1986), 95–109.
5. S. K. Stein, *Algebraic tiling*, Amer. Math. Monthly **81** (1974), 445–462.
6. ———, *Tiling, packing, and covering by clusters*, Rocky Mountain J. Math. **16** (1986), 277–321.
7. S. K. Stein and S. Szabó, *Algebra and tiling*, Carus Math. Monographs, vol. 25, Math. Assoc. America, Washington, DC, 1994.
8. S. Szabó, *Some problems on splittings of groups*, Aequationes Math. **30** (1986), 70–79.
9. ———, *Some problems on splittings of groups*. II, Proc. Amer. Math. Soc. **101** (1987), 585–591.

Department of Mathematical Sciences, Villanova University, Villanova, Pennsylvania 19085
E-mail address: woldar@vill.edu