t-SUM GENERATORS OF FINITE ABELIAN GROUPS

RON M. ROTH AND ABRAHAM LEMPEL

Department of Computer Science

Technion, Israel Institute of Technology

Haifa 32000 - Israel

ABSTRACT

Given a finite Abelian group A and an integer $t, 1 \le t \le |A|-1$, a subset S of A is called a t-sum generator of A if every element of A can be written as the sum of exactly t distinct elements of S. In this paper we investigate the minimal integer $M(t, A)$ such that every set $S \subseteq A$ of size $|S| > M(t, A)$ is a t-sum generator of A. The value of $M(t, A)$ is completely determined for groups of even order.

I. INTRODUCTION

Let A be a finite (additive) Abelian group. Let S be a subset of A and let t be an integer in the range $1 \le t \le |S|$. We define the *t-span* of S, denoted by $L(S, t)$, as the set of all elements of A which can be obtained as a sum of exactly t distinct elements of S. A subset S of A is called a *t-sum generator* of A if $L(S, t) = A$. Let $M(t, A)$ denote the smallest integer such that every subset of A of size *greater* than $M(t, A)$ is a t-sum generator of A; when A has no t-sum generator, $M(t, A) = |A|$. In this work we find the exact values of $M(t, A)$ for even-order groups. In particular, we show that for all even-order groups and for all $4 \le t \le \frac{|A|-3}{2}$, $M(t, A) = \frac{|A|}{2}$ (Theorem 3.1). Some of the bounds obtained apply also to odd-size groups, for which, to the best knowledge of the authors, the problem of determining $M(t, A)$ remains open. For related work see, for instance [1][4][5].

The values of $M(t, A)$ can be applied to construct certain sub-classes of *maximum-distance-separable* (in short, MDS) codes [8, Ch. 11]. The relationship between $M(t, A)$ and these constructions is better described in terms of the following counterpart of a t-sum generator: given an element $\delta \in A$, a set $S \subseteq A$ of size m is called an (m, t, δ)-*set* in A if $\delta \notin L(S, t)$. Hence, given t, the largest (m, t, δ)-set in A will have $M(t, A)$ elements. In [9], the authors present a construction of special MDS codes of length $m+2$ and dimension $t+1$ over a finite field $GF(q)$, employing (m, t, δ)-sets in the additive group of $GF(q)$. The distinction of these codes is that they are not of the generalized Reed-Solomon type, the prevailing type of MDS codes. In [6], (m, t, δ)-sets in certain Abelian groups are used to construct MDS codes of length m and dimension $m - t$ on an elliptic curve having $|A|$ rational points.

II. BASIC RESULTS

We begin with several results valid for all finite Abelian groups. We consider nontrivial groups of order greater than one.

First, we recall some basic facts. For any integer $n \geq 2$, denote by Z_n the ring modulo n. Every finite Abelian group A is isomorphic to $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_h}$, where the h values n_i are unique, up to permutation, powers of primes and $|A| = n_1 n_2 \cdots n_h$ [7, p. 354]. The n_i are called *elementary divisors* of A. It follows that there exists a one-to-one correspondence between all elements $\alpha \in A$ and the h-tuples $[a_1\ a_2 \cdots a_h]$, $a_i \in Z_{n_i}$, with component-wise addition modulo n_i. In a similar manner, we associate every subset S of A with an $h \times |S|$ matrix $H_S \triangleq [a_{ij}]$, with $a_{ij} \in Z_{n_i}$, $1 \leq i \leq h$, $1 \leq j \leq |S|$, where the columns of H_S correspond to the elements of S. We shall use the short-hand notation Z_n^k for $\underbrace{Z_n \times Z_n \times \cdots \times Z_n}_{\leftarrow\ k \text{ times } \rightarrow}$.

In the sequel we shall consider in particular groups of the form Z_p^h where p is a prime. Every element in such a group is associated with an h-dimensional vector over Z_p and every subset $S \subseteq Z_p^h$ corresponds to an $h \times |S|$ matrix H_S over Z_p. Denote by $M(t, A, \delta)$ the maximal size m of any (m, t, δ)-set in A. It is easy to show that $M(t, Z_p^h, \delta)$ is constant for all nonzero $\delta \in Z_p^h$. To see this, let $\mathbf{u}_1$ and $\mathbf{u}_2$ be the h-vector representations of two nonzero elements $\delta_1, \delta_2 \in Z_p^h$, respectively, and let B be an $h \times h$ nonsingular matrix over Z_p such that $\mathbf{u}_2 = B\mathbf{u}_1$. Given an (m, t, δ_1)-set S, $\delta_1 \neq 0$, we can form an (m, t, δ_2)-set by taking the columns of $B \cdot H_S$. On the other hand, $M(t, Z_p^h, 0)$ may differ from $M(t, Z_p^h, \delta)$, $\delta \neq 0$.

The following lemma presents a case in which $M(t, A, \delta)$ is constant for all $\delta \in A$, including $\delta = 0$.

Lemma 2.1. *If* $gcd(t, |A|) = 1$, *then* $M(t, A, \delta) = M(t, A)$ *for all* $\delta \in A$.

Proof. Assume $gcd(t, |A|) = 1$. Let δ_1 and δ_2 be two distinct elements of A and let $S_1 \subseteq A$ with $m = |S_1|$. Consider the set

$$S_2 \triangleq \{\ \alpha + t^{-1}(\delta_2 - \delta_1)\ \ |\ \ \alpha \in S_1\ \},$$

where t^{-1} stands for the multiplicative inverse of t modulo $|A|$ and $t^{-1}\delta$ stands for $\sum_{i=1}^{t^{-1}} \delta$. By the Lagrange theorem we have $t \cdot t^{-1}(\delta_2 - \delta_1) = \delta_2 - \delta_1$ and, therefore, S_2 is an (m, t, δ_2)-set if and

only if S_1 is an (m, t, δ_1)-set. Thus, the value of $M(t, A, \delta)$ is independent of δ. □

For a set $S \subseteq A$, denote by $\sigma(S)$ the sum of elements of S. Note that every (m, t, δ)-set S, $t < m$, is also an $(m, m-t, \sigma(S)-\delta)$-set. This can be summarized as follows.

Lemma 2.2. *For a finite Abelian group A, let l and m be two positive integers such that $l \le |A|-1$ and $l < m \le M(l, A)$. Then,*

$$m \le M(m-l, A) .$$

Clearly, $M(1, A) = |A|-1$ for every group A, since $L(A-\{\delta\}, 1) = A-\{\delta\}$. Also, $M(|A|-1, A) \le |A|-1$, or else we have a contradiction by setting $l = |A|-1$ and $m = |A|$ in Lemma 2.2. The equality $M(|A|-1, A) = |A|-1$ follows now from $|L(A-\{\alpha\}, |A|-1)| = 1$ for all $\alpha \in A$.

Lemma 2.3. *Let A be a finite Abelian group and let h_2 be the number of even elementary divisors of A. Then,*

$$M(2, A) = \frac{|A| + 2^{h_2}}{2} .$$

Proof. Given a prime power n and an element $a \in Z_n$, the number of distinct solutions in Z_n of the equation $2x = a$ is one when n is odd; two if both n and a are even; and there are no solutions if n is even and a is odd.

Now let S be a $(|S|, 2, \delta)$-set in A and let $\delta = [a_1\ a_2 \cdots a_h]$ be the representation of δ. Suppose the first h_2 coordinates of δ correspond to the even elementary divisors, with s of the h_2 values a_i being odd. If $s > 0$, the equation $2x = \delta$ has no solutions in A and, therefore, for every $\alpha \in A$, the set $\{\alpha, \delta-\alpha\}$ contains two distinct elements, implying $|S| \le \frac{|A|}{2}$.

Assume now that $s = 0$. In this case, the set $X = \{\ x \mid x \in A \text{ and } 2x = \delta\ \}$ is of size 2^{h_2}. Here S may contain any element of X and, in addition, one element from each pair

$\{\alpha, \delta - \alpha\}_{\alpha \in A-X}$, implying

$$|S| \le \frac{|A| - 2^{h_2}}{2} + 2^{h_2} = \frac{|A| + 2^{h_2}}{2}.$$

This bound can be attained by choosing δ so that $s = 0$ (say, $\delta = 0$). □

In particular, when $A = Z_2^h$ we have $M(2, Z_2^h) = M(2, Z_2^h, 0) = 2^h$, whereas $M(2, Z_2^h, \delta) = 2^{h-1}$ for every $\delta \neq 0$.

Lemma 2.4. *Let A be a finite Abelian group. Then, for every $2 \le t \le |A| - 1$,*

$$M(t, A) \le M(t-1, A) + 1.$$

Proof. Let α be an element of an (m, t, δ)-set S. Then $S - \{\alpha\}$ is an $(m-1, t-1, \delta - \alpha)$-set. □

Lemma 2.5. *Let A be a finite Abelian group. Then,*

$$M(3, A) \le \lfloor \frac{|A| + 3}{2} \rfloor.$$

Proof. When $|A|$ is odd, the lemma is a direct corollary of Lemmas 2.3 and 2.4. Assume now that the first elementary divisor of A is even and suppose S is an $(m, 3, \delta)$-set in A with $m = |S| \ge \frac{|A|}{2} + 1$. Since $|S| > \frac{|A|}{2}$, there exists $\alpha \in S$ such that $\delta - \alpha$ has an odd leading component. As no two distinct elements in $S - \{\alpha\}$ sum to $\delta - \alpha$, it follows, as in the proof of Lemma 2.3, that $|S| - 1 \le \frac{|A|}{2}$. □

Lemma 2.6. *Let A be a finite Abelian group and, for a given integer s, $1 \le s \le |A| - 2$, let t be an integer in the range $M(s+1, A) - s \le t \le M(s, A) - s$. Then,*

$$M(t, A) = t + s.$$

Proof. Suppose $M(t, A) \ge t + s + 1$. By Lemma 2.2 we must have $M(s+1, A) \ge t + s + 1$, contradicting our assumption on t. The inequality in the other direction follows from Lemma 2.2

and the fact that $M(s, A) \geq t + s > s$. □

Theorem 2.1. *For any finite Abelian group A,* $|A| \geq 3$,

$$M(t, A) = \begin{cases} t+2 & \text{if } \left\lfloor \frac{|A|-1}{2} \right\rfloor \leq t \leq \frac{|A|+2^{h_2}}{2} - 2 \\ t+1 & \text{if } \frac{|A|+2^{h_2}}{2} - 1 \leq t \leq |A| - 2 \end{cases},$$

where h_2 *is the number of even elementary divisors of A.*

Proof. This is a direct corollary of Lemma 2.3 and Lemma 2.5, obtained by substituting $s = 1$ and $s = 2$ in Lemma 2.6. □

In particular, we have $M(|A|-2, A) = |A|-1$ for all finite Abelian groups A except when $A = Z_2^h$, in which case $M(2^h - 2, Z_2^h) = 2^h$. Also, when $|A|$ is odd, $M(t, A) = t+1$ for all $\frac{|A|-1}{2} \leq t \leq |A|-2$.

The following lemma will be used in the next section to determine the exact value of $M(3, A)$ for even-order groups A.

Lemma 2.7. *Let S be a subset of a finite Abelian group A and let* $m \triangleq |S|$.

(a) If m is an odd integer greater than 1, *then* $|L(S, 2)| \geq m$.

(b) If m is an even integer greater than 2 *and the number of elements* $\alpha \in A$ *satisfying* $(m/2)\alpha = 0$ *does not exceed* $m-2$, *then* $|L(S, 2)| \geq m$.

Proof. (a) Let $l \triangleq |L(S, 2)|$. No element of $L(S, 2)$ can be obtained in more than $\lfloor m/2 \rfloor$ ways as the sum of two distinct elements of S. Enumerating over all $\binom{m}{2}$ possible pairs in S, we obtain at most $l \cdot \lfloor m/2 \rfloor$ values (not necessarily distinct), implying

$$\binom{m}{2} \leq l \cdot \lfloor m/2 \rfloor = l \cdot (m-1)/2$$

or, since $m > 1$,

$$l \geq m .$$

(b) No element of $L(S,2)$ is the sum of more than $m/2$ pairs in S. Furthermore, according to our assumption, there exist at most $m-2$ elements $\beta \in L(S,2)$ which are the sums of *exactly* $m/2$ pairs in S; these elements satisfy $(m/2)\beta = \sigma(S)$. We thus have,

$$\binom{m}{2} \leq (m-2)\cdot(m/2) + [l-(m-2)]\cdot[(m/2)-1]$$

or, since $m > 2$,

$$l \geq \left\lceil \frac{m(m-1)/2 - m(m-2)/2}{m/2-1} + (m-2) \right\rceil = \left\lceil \frac{1}{m/2-1} \right\rceil + m - 1 = m . \qquad \square$$

In particular, when $|S| > 2$ and $gcd(|S|, |A|) = 1$, we have $|L(S,2)| \geq |S|$.

III. ABELIAN GROUPS OF EVEN ORDER

In this section we prove the following theorem:

Theorem 3.1. *Let A be a finite Abelian group of even order ≥ 12. Then, for $3 \leq t \leq \frac{|A|}{2} - 2$,*

$$M(t, A) = \frac{|A|}{2} ,$$

except when $A \in \{Z_2^h, Z_4 \times Z_2^{h-1}\}$ and $t \in \{3, \frac{|A|}{2} - 2\}$, in which case $M(t, A) = \frac{|A|}{2} + 1$.

Remark 3.1. We have excluded the case $A = Z_{10}$ and $t = 3$, where we have $M(3, Z_{10}) = 6$; $S(3, Z_{10}, 0) = \{2, 3, 4, 6, 7, 8\}$.

Throughout this section we assume A to be an even-order Abelian group and, without loss of generality, we may assume that A is isomorphic to $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_h}$ where n_1 is even. For each such group we define the *binary partition* $A = A_0 \cup A_1$ by

$$A_b \triangleq \{\, [a_1\ a_2 \cdots a_h] \mid a_i \in Z_{n_i} \text{ and } a_1 \equiv b \pmod 2 \,\}, \quad b \in Z_2 .$$

Clearly, $|A_0| = |A_1| = \frac{|A|}{2}$.

The following lemma establishes the desired lower bound on $M(t, A)$ for even-order groups.

Lemma 3.1. *Let A be a finite Abelian group of even order. Then, for $3 \le t \le \frac{|A|}{2} - 2$,*

$$M(t, A) \ge \frac{|A|}{2},$$

except when $A \in \{Z_2^h,\ Z_4 \times Z_2^{h-1}\}$ and $t \in \{3,\ \frac{|A|}{2} - 2\}$, in which case $M(t, A) \ge \frac{|A|}{2} + 1$.

Proof. For odd t, A_1 is a $(\frac{|A|}{2}, t, \delta)$-set for every $\delta \in A_0$ and, for even t, A_1 is a $(\frac{|A|}{2}, t, \delta)$-set for every $\delta \in A_1$. When $A = Z_2^h$ we can adjoin the zero element to A_1 to obtain a $(\frac{|A|}{2} + 1, 3, 0)$-set, and when $A = Z_4 \times Z_2^{h-1}$ we obtain a $(\frac{|A|}{2} + 1, 3, 0)$-set by adjoining the element $[2\ 0\ 0 \cdots 0]$ to A_1. The results for $t = \frac{|A|}{2} - 2$ in these last two cases are direct corollaries of Lemma 2.2. □

Lemmas 2.5 and 3.1 establish the exception cases of Theorem 3.1. The upper bound on $M(t, A)$ for the main case will be obtained via the following steps:

(i) First, we show that $M(3, A) \le \frac{|A|}{2}$ for all Abelian groups of order $2r$ where r is an odd integer ≥ 7.

(ii) Using (i), we show that Theorem 3.1 holds for all Abelian groups of order $2r$, where r is an odd integer ≥ 7.

(iii) We prove the upper bound on $M(3, A)$ for all Abelian groups by induction on the power of 2 in the prime factorization of $|A|$, using (i) as the induction base.

(iv) Finally, we complete the proof of Theorem 3.1 using (ii) as the induction base.

Given an even-order Abelian group $A = Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_h}$, n_1 even, $|A| \geq 4$, we define the *truncation group* $\bar{A}$ by

$$\bar{A} = \begin{cases} Z_{n_2} \times \cdots \times Z_{n_h} & \text{if } n_1 = 2 \\ Z_{n_1/2} \times \cdots \times Z_{n_h} & \text{otherwise} \end{cases},$$

and the projection $\phi : A \rightarrow \bar{A}$ by

$$\phi([a_1\ a_2 \cdots a_h]) \triangleq \begin{cases} [a_2\ a_3 \cdots a_h] & \text{if } n_1 = 2 \\ [\lfloor a_1/2 \rfloor\ a_2 \cdots a_h] & \text{otherwise} \end{cases}.$$

Note that when $n_1 = 2$, ϕ is a homomorphism from A onto $\bar{A}$. For any $u \in \bar{A}$, $\phi^{-1}(u)$ stands for the set of two elements in A whose image under ϕ is u. Also, for any $T \subseteq A$, $\bar{T}$ stands for the set of (distinct) images of T under ϕ.

Given an even-order group $A = A_0 \cup A_1$, we extend the definition of a binary partition to any subset S of A: $S = S_0 \cup S_1$, where $S_b \triangleq S \cap A_b$, $b \in Z_2$.

Lemma 3.2. *Let A be a finite Abelian group of order $2r$, where r is an odd integer ≥ 7. Then,*

$$M(3, A) \leq r .$$

Proof. Let S be a subset of size $r+1$ in A. We will show that $L(S, 3) = A$. Assume, to the contrary, that S is an $(r+1, 3, \delta)$-set. Without loss of generality we may assume that $\delta \in A_0$ (or else, we can subtract any element $\beta \in A_1$ from each element of S, resulting in an $(r+1, 3, \delta' = \delta - 3\beta)$-set with $\delta' \in A_0$). Let $S_0 \cup S_1$ be the binary partition on S, with $m_b \triangleq |S_b|$. Since no three distinct elements of S_0 sum to δ, $\bar{S}_0$ is an $(m_0, 3, \bar{\delta})$-set in $\bar{A}$, implying, by Lemma 2.5, that $1 \leq m_0 \leq \frac{r+3}{2}$. Also, for every $\alpha \in S_0$, no two distinct elements of S_1 sum to $\delta - \alpha$ and, therefore, applying Lemma 2.3 to $\bar{S}_1$ as a subset of $\bar{A}$, yields $m_1 \leq \frac{r+1}{2}$. This leaves two pairs of

possible values: $m_0 = m_1 = \frac{r+1}{2}$, or $m_0 = \frac{r+3}{2}$ and $m_1 = \frac{r-1}{2}$; in either case we have $m_1 > 2$ and $gcd(m_1, r) = 1$. Applying Lemma 2.7 to $\bar{S}_1$, we obtain $|L(\bar{S}_1, 2)| \geq m_1$. On the other hand, no two distinct elements of S_1 may sum to any of the elements in $\{ \delta - \alpha \mid \alpha \in S_0 \}$, implying $|L(\bar{S}_1, 2)| \leq r - m_0$, or

$$|S| = m_0 + m_1 \leq m_0 + |L(\bar{S}_1, 2)| \leq m_0 + r - m_0 = r . \qquad \square$$

Lemma 3.3. *Let A be a finite Abelian group of order $2r$, where r is an odd integer ≥ 7. Then, for $3 \leq t \leq r-2$,*

$$M(t, A) \leq r .$$

Proof. By Lemmas 2.2 and 3.2, it suffices to cover only the range $4 \leq t \leq \frac{r+1}{2}$. Let S be a subset of A of size $r+1$ and let $S_0 \cup S_1$ be the binary partition of S. Since $|\bar{S}_0| + |\bar{S}_1| = r+1$, we have $|\bar{S}_0 \cap \bar{S}_1| \geq 1$. Now, choose any $\delta \in A$. We will show that for $4 \leq t \leq \frac{r+1}{2}$ we have $\delta \in L(S, t)$.

Case 1. $|\bar{S}_0 \cup \bar{S}_1| \geq \frac{r+5}{2}$. Let $u \in \bar{S}_0 \cap \bar{S}_1$ and let T_1 be a subset of $S - \phi^{-1}(u)$ such that $|T_1| = |\bar{T}_1| = \frac{r+3}{2}$. Since $4 \leq t \leq \frac{r+1}{2}$, we have $1 \leq t-3 \leq r+1-(\frac{r+3}{2}+2)$ and, therefore, we can find a subset $T_2 \subseteq S - \phi^{-1}(u) - T_1$ of size $t-3$. Applying Lemma 2.3 to $\bar{T}_1$ as a subset of $\bar{A}$, we conclude that T_1 must contain two distinct elements summing to $\delta - \sigma(T_2) - \alpha$ for some $\alpha \in \phi^{-1}(u)$. Hence, the set $T_1 \cup T_2 \cup \{\alpha\}$ contains a subset of size t which sums to the chosen δ.

Case 2. $|\bar{S}_0 \cup \bar{S}_1| = \frac{r+3}{2}$. Let T_1 be a subset of S of size $\frac{r+3}{2}$ such that $\bar{T}_1 = \bar{S}_0 \cup \bar{S}_1$. Since $4 \leq t \leq \frac{r+1}{2}$, we have $2 \leq t-2 < r+1-\frac{r+3}{2}$ and, therefore, we can find a subset T_2 of $S - T_1$ containing $t-2$ elements such that $2\sigma(\bar{T}_2) \neq \bar{\delta}$. Applying Lemma 2.3 to $\bar{T}_1$ as a subset of $\bar{A}$, there exists a pair P of distinct elements in T_1 satisfying $\sigma(P) + \sigma(T_2) = \gamma \in \phi^{-1}(\bar{\delta})$. Noting

that $\bar{T}_2 \subseteq \bar{T}_1$, with $|T_2| \geq 2$ and $\bar{P} \neq \bar{T}_2$, we can find two elements, $v_1 \in T_1 - P$ and $v_2 \in T_2$, such that $\bar{v}_1 = \bar{v}_2$. Thus, if $\gamma \neq \delta$, replacing $v_2 \in T_2$ with v_1 will result in $\sigma(P) + \sigma(T_2) = \delta$. Thus we obtain a set $P \cup T_2$ of t elements summing to δ.

Case 3. $|\bar{S}_0 \cup \bar{S}_1| = \frac{r+1}{2}$, i.e., $\bar{S}_0 = \bar{S}_1$ and $|\bar{S}_0| = \frac{r+1}{2} \triangleq m$. We show that for every $3 \leq t \leq \frac{r+1}{2}$ and for every $w \in \bar{A}$ there exists a multiset $V = V(w)$ of t elements of $\bar{S}_0$ satisfying the following three conditions: (a) every element in V appears twice at most; (b) there exists at least one element in V appearing exactly once; and (c) $\sigma(V) = w$. Having shown this, it will follow that for every $\delta \in A$ there exists a set T of t elements in S, the images of which under ϕ are the elements of V, and $\sigma(T) = \delta$.

Our proof is by induction on t, with Lemma 3.2 serving as the induction base for odd values of t. As our induction hypothesis does not assume condition (b), the case $t = 2$ can serve as the induction base for even values of t.

Assume now that for every $w \in \bar{A}$ there exists a multiset V of $t - 2 \geq 2$ elements of $\bar{S}_0$ satisfying conditions (a) and (c). Also suppose, to the contrary, that there exists an element $z \in \bar{A}$ for which there exists no multiset of size t satisfying (a), (b) and (c). Let U_0 be a subset of $t - 3$ (distinct) elements of $\bar{S}_0$ such that $2\sigma(U_0) \neq z$ (this condition is required to cover the case $t = 6$). Write $\bar{S}_0 = \{u_i\}_{i=1}^{m}$ and assume, without loss of generality, that $U_0 = \{u_i\}_{i=1}^{t-3}$. For $1 \leq i \leq m$, define the multisets $U_i \triangleq U_0 \cup \{u_i\}$. Clearly, $\sigma(U_i) \neq \sigma(U_j)$ for all $i \neq j$. For every $j, 1 \leq j \leq t - 3$, let P_j denote the pair $\{u_j, z - u_j - \sigma(U_j)\}$. Also, when $t = 4$, we denote by P_0 the pair forming one of the sets U_i (if any) satisfying the equality $2\sigma(P_0) = z$. Let P be a pair of distinct elements from $\bar{S}_0$, not belonging to $\pi = \{P_j\}_{j=0}^{t-3}$. It is easy to verify that for every such pair P, if the multiset $P \cup U_i$, $1 \leq i \leq m$, satisfies condition (c), it also satisfies conditions (a) and (b). Therefore, by our contrary assumption we must conclude that for every $P \notin \pi$ and every i, $\sigma(P) + \sigma(U_i) \neq z$. Hence, there exist at least $\binom{m}{2} - (t - 2)$ pairs P whose sums take no more than $r - m$ distinct values in $\bar{A}$. It follows that there exists at least one element $v \in \bar{A}$ which is

obtained as the sums of at least

$$\left\lceil \frac{m(m-1)/2-(t-2)}{r-m} \right\rceil$$

pairs in $\bar{S}_0$.

Now, by the induction hypothesis there exists a multiset, say V, of size $t-2$, satisfying (a) and (c) with respect to $z-v$. Write $t-2=2s+\tau$, where s is the number of distinct elements appearing twice in V. To negate the possibility of finding a pair of distinct elements $P \notin \pi$ such that $\sigma(P)=v$ and $V \cup P$ satisfy (a), (b) and (c) with respect to z, we must have

$$\left\lceil \frac{m(m-1)/2-(t-2)}{r-m} \right\rceil \leq s = \frac{t-2-\tau}{2}$$

when $\tau \neq 2$, or

$$\left\lceil \frac{m(m-1)/2-(t-2)}{r-m} \right\rceil \leq s+1 = \frac{t-\tau}{2}$$

when $\tau = 2$. In either case we obtain

$$\frac{(r+1)(r-1)/8-(t-2)}{(r-1)/2} \leq \frac{t}{2}-1,$$

or

$$t \geq \frac{r+1}{2}+\frac{4}{r+3}$$

which, of course, is a contradiction. □

Remark 3.2. So far, we have completed steps (i) and (ii) of the outline of proof of the upper bound on $M(t, A)$. Writing $|A| = 2^k \cdot r$ where r is an odd integer, the remainder of the proof proceeds by induction on k, with Lemmas 3.2 and 3.3 serving as the induction base. Since the latter does not cover the cases of $r=1, 3, 5$, we need to verify that $M(t, A) = \frac{|A|}{2}$, $3 \leq t \leq \frac{|A|}{2}-2$, for the following groups: Z_{16}, $Z_2 \times Z_8$, $Z_4 \times Z_4$, Z_2^4 (only for $t=4, 5$), $Z_4 \times Z_2^2$ (only for $t=4, 5$), Z_{12}, $Z_2^2 \times Z_3$, Z_{20} and $Z_2^2 \times Z_5$. The verification of these cases is left to the

reader.

Lemma 3.4. *Let A be a finite Abelian group of even order ≥ 12 other than Z_2^h, $Z_4 \times Z_2^{h-1}$. Then,*

$$M(3, A) \leq \frac{|A|}{2}.$$

Proof. As indicated above, the proof is carried out by induction on k in $|A| = 2^k \cdot r$, with Lemma 3.2 and Remark 3.2 serving as the induction base. The reduction in k when applying the induction hypothesis may lead to different optional groups, depending on the elementary divisors of A. Some of these options may correspond to an exception case, but there is always an option satisfying the induction hypothesis.

Assume that $k \geq 2$ and suppose, to the contrary, that there exists a $(\frac{|A|}{2}+1, t, \delta)$-set S in A. Let S_0 and S_1 be the subsets of the binary partition of S, of sizes m_0 and m_1, respectively. As in Lemma 3.2, without loss of generality, we can assume $\delta \in A_0$.

Case 1. $m_0 \geq \frac{|A|}{4}+1$. No three distinct elements in S_0 sum to δ, implying that $\bar{S}_0$ is an $(m_0, 3, \bar{\delta})$-set in $\bar{A}$. This contradicts the induction hypothesis.

Case 2. $m_0 \leq \frac{|A|}{4}$. Here we derive a contradiction by showing that there exists an element $\alpha \in S_0$ such that $\delta - \alpha \in L(S_1, 2)$. Since $|S_1| = m_1 > \frac{|A|}{4}$, it suffices to show that for every $u \in \bar{A}$, there exists an element $v \in \bar{S}_0$ such that $u - v$ is not an "even" element in $\bar{A}$; that is, there is no solution in $\bar{A}$ to the equation $2x = u - v$.

Let l be the number of even elementary divisors of $\bar{A}$. Since our contrary assumption implies $L(\bar{S}_1, 2) \neq \bar{A}$, it follows from Lemma 2.3 that

$$m_1 \le \frac{|\bar{A}| + 2^l}{2}$$

and

$$m_0 \ge 1 + \frac{|\bar{A}| - 2^l}{2}.$$

Now, the number of "even" elements in $\bar{A}$ is $|\bar{A}|/(2^l)$, and it is easy to check that

$$1 + \frac{|\bar{A}| - 2^l}{2} > \frac{|\bar{A}|}{2^l}$$

whenever $2 < 2^l < |\bar{A}|$. Since $\bar{A} \neq Z_2^l$, we have $2^l < |\bar{A}|$. Therefore, when $l > 1$, for every $u \in \bar{A}$ there exists at least one element $v \in \bar{S}_0$ such that $u - v$ is "odd" in $\bar{A}$.

Finally, if $l = 1$, it remains to check only the case $m_0 = \frac{|A|}{4}$ and $m_1 = \frac{|A|}{4} + 1$. It is easy to verify that the conditions of Lemma 2.7 hold in this case for $\bar{S}_1$ as a subset of $\bar{A}$ and, therefore, $L(\bar{S}_1, 2) \ge m_1 = \frac{|A|}{4} + 1$. On the other hand, by our contrary assumption, no two distinct elements in S_1 may sum to any of the elements in $\{\delta - \alpha \mid \alpha \in S_0\}$, implying $L(\bar{S}_1, 2) \le |\bar{A}| - m_0 = \frac{|A|}{4}$. □

Lemma 3.5. *(a) Every* $(2^{h-1}+1, 3, \delta)$*-set* S *in* Z_2^h, $h \ge 3$, *satisfies* $\sigma(S) = \delta$. *(b) Every* $(2^{h-1}+1, 2^{h-1}-2, \delta)$*-set in* Z_2^h, $h \ge 3$, *satisfies* $\delta = 0$.

Proof. (a) Let S be a $(2^{h-1}+1, 3, \delta)$-set. First, we show that $\delta \in S$. If $\alpha \in S$ and $\alpha \neq \delta$, then $S - \{\alpha\}$ contains exactly one element of every pair of Z_2^h whose sum is $\delta - \alpha$. In particular, $S - \{\alpha\}$ contains the element δ of the pair $\{\alpha, \delta\}$.

Now let H_S be an $h \times (2^{h-1}+1)$ matrix representing a $(2^{h-1}+1, 3, \delta)$-set S in Z_2^h, $h \ge 3$. Without loss of generality we can assume that $\delta = 0$ and, in this case, H_S must contain the zero column. As the number of (distinct) columns in H_S exceeds 2^{h-1}, $\text{rank}(H_S) = h$, and since every nonsingular linear operation on the rows of H_S results in a $(2^{h-1}+1, 3, 0)$-set, we can assume that

H_S contains the $h \times h$ identity matrix. Hence, we can write

$$H_S = \begin{bmatrix} \mathbf{0} & H_0 & \mathbf{0} & H_1 \\ 0 & 0\,0\cdots 0 & 1 & 1\,1\cdots 1 \end{bmatrix}. \tag{3.1}$$

It is easy to verify that all the columns of $[H_0\ H_1]$ must be nonzero; they also must be distinct, or else, we would have three columns in H_S which sum to $\mathbf{0}$. It follows that every row of H_S, including the last one, must have Hamming weight 2^{h-2} (implying that H_0 contains 2^{h-2} columns and that $[\mathbf{0}\ H_0]$ is, in fact, a $(2^{h-2}+1, 3, 0)$-set in Z_2^{h-1}). Thus the sum of elements of a $(2^{h-1}+1, 3, 0)$-set S must be zero.

(b) Every $(2^{h-1}+1, 2^{h-1}-2, \delta)$-set S is also a $(2^{h-1}+1, 3, \sigma(S)-\delta)$-set. By part (a), we have $\sigma(S) - \delta = \sigma(S)$, i.e., $\delta = 0$. □

Remark 3.3. Deleting the zero column from the matrix H_S in (3.1), we obtain an $h \times 2^{h-1}$ matrix H_S^*, in which every three columns are linearly independent over Z_2. Therefore, H_S^* serves as a parity-check matrix of a binary linear code of length 2^{h-1}, dimension $2^{h-1} - h$, and minimum distance ≥ 4 [8, Ch. 1]. It can be shown that such codes are *unique* up to linear operations on the rows of H_S^* or permutation of columns: they are all equivalent to the extended Hamming code. Hence, $(2^{h-1}+1, 3, \delta)$-sets in Z_2^h are completely classified.

Lemma 3.6. *Let A be a finite Abelian group of even order. Then,*

$$M(t, A) \le \frac{|A|}{2}, \quad 4 \le t \le \frac{|A|}{2} - 3.$$

Proof. Let $|A| = 2^k \cdot r$ where r is an odd integer. The proof proceeds by induction on k, with Lemma 3.3 and Remark 3.2 serving as the induction base. Unless otherwise stated, we assume n_1 to be the smallest even elementary divisor of A. Suppose now that $k \ge 2$. By Lemma 2.2, it suffices to consider only odd values of t, since every $(\frac{|A|}{2}+1, t, \delta)$-set, where t is even, also serves as a $(\frac{|A|}{2}+1, t', \delta')$-set, where $t' = \frac{|A|}{2}+1-t$ is odd. Note that having established

the case of odd t, we can apply Lemma 2.4 to obtain $M(\frac{|A|}{2}-2, A) \le \frac{|A|}{2}+1$ and, when A is not one of the exception cases, Z_2^k or $Z_4 \times Z_2^{k-2}$, applying Lemma 3.4 yields $M(\frac{|A|}{2}-2, A) \le \frac{|A|}{2}$.

Let t be an odd integer in the range $5 \le t \le \frac{|A|}{2}-3$ and suppose, to the contrary, that there exists a $(\frac{|A|}{2}+1, t, \delta)$-set S in A, with $S_0 \cup S_1$ being the binary partition of S and $m_b \triangleq |S_b|$, $b \in Z_2$. As before, without loss of generality, we assume $\delta \in A_0$.

We distinguish now between several cases.

Case 1. $m_1 \le \frac{|A|}{4}$ and $m_1 + 4 \le t \le \frac{|A|}{2}-3$. Let T be a subset of S_1, where

$$|T| = \begin{cases} m_1 & \text{if } m_1 \text{ is even} \\ m_1 - 1 & \text{if } m_1 \text{ is odd} \end{cases}.$$

Clearly, S_0 is an (m_0, t_0, γ)-set in A, where $t_0 \triangleq t - |T|$ and $\gamma \triangleq \delta - \sigma(T) \in A_0$. Therefore, $\bar{S}_0$ is an $(m_0, t_0, \bar{\gamma})$-set in $\bar{A}$, and we can apply the induction hypothesis to $\bar{A}$ and $\bar{S}_0$. We have,

$$4 \le t - m_1 \le t_0 \le t - m_1 + 1 \tag{3.2}$$

and, therefore,

$$m_0 - t_0 \ge \frac{|A|}{2} + 1 - m_1 - (t - m_1 + 1) = \frac{|A|}{2} - t \ge 3. \tag{3.3}$$

Thus, Theorem 2.1 implies $t_0 \le \frac{|A|}{4}-2$ and, since $m_0 \ge \frac{|A|}{4}+1$, the induction hypothesis implies either $t_0 = \frac{|A|}{4}-2$ or $t_0 \le 3$. As the latter case contradicts (3.2), it remains to check the case $t_0 = \frac{|A|}{4}-2$, which may be valid only when $\bar{A}$ is one of the exception cases. However, in such a case, $m_1 = \frac{|A|}{4}$ is even, $|T| = m_1$, and (3.3) can be replaced by $m_0 - t_0 \ge 4$, yielding the contradiction $m_0 \ge \frac{|A|}{4}+2$.

Case 2. $m_1 \le \frac{|A|}{4}$ and $5 \le t \le m_1 + 3$. Take any subset T of size $t-5$ in S_1. Then, no five elements of S_0 sum to $\gamma \triangleq \delta - \sigma(T)$, implying that $\bar{S}_0$ is an $(m_0, 5, \bar{\gamma})$-set in $\bar{A}$, contradicting the induction hypothesis for $|\bar{A}| > 12$. In case $|\bar{A}| = 12$, we change slightly the proof by taking T as a subset of S_1 of size $t-3$: there exist no $(m_0, 3, \bar{\gamma})$-sets in $\bar{A}$ in this case.

Case 3. $m_0 \le \frac{|A|}{4}$ and $m_0 + 4 \le t \le \frac{|A|}{2} - 3$. The proof in this case is similar to that of Case 1, except that here we take T as a subset of S_0, where

$$|T| = \begin{cases} m_0 - 1 & \text{if } m_0 \text{ is even} \\ m_0 & \text{if } m_0 \text{ is odd} \end{cases} .$$

It follows that $\bar{S}_1$ forms an $(m_1, t_1 \triangleq t - |T|, u)$-set for some $u \in \bar{A}$. Again, we have,

$$4 \le t - m_0 \le t_1 \le t - m_0 + 1 , \tag{3.4}$$

implying

$$m_1 - t_1 \ge \frac{|A|}{2} + 1 - m_0 - (t - m_0 + 1) = \frac{|A|}{2} - t \ge 3 . \tag{3.5}$$

Again, by Theorem 2.1, $t_1 \le \frac{|A|}{4} - 2$ and, since $m_1 \ge \frac{|A|}{4} + 1$, either $t_1 \le 3$, in contradiction to (3.4), or $t_1 = \frac{|A|}{4} - 2$. The latter option may hold only in one of the exception cases, where we must also have $m_0 = \frac{|A|}{4}$ and $m_1 = \frac{|A|}{4} + 1$ (these values correspond to $t = \frac{|A|}{2} - 3$). We combine the discussion of both cases Z_2^k and $Z_4 \times Z_2^{k-2}$ by assuming $n_1 = 4$ in the latter, thus having $\bar{A} = Z_2^{k-1}$. Refining our previous arguments, we note that $\bar{S}_1$ is an $(m_1 = \frac{|A|}{4} + 1, t_1 = \frac{|A|}{4} - 2, u)$-set in $\bar{A}$ for *every* subset $T \subseteq S_0$ of size $m_0 - 1 = \frac{|A|}{4} - 1$, with distinct u for each of the $\frac{|A|}{4}$ subsets T. However, by Lemma 3.5 we must have $u = 0$, implying $|A| = 4$.

Case 4. $m_0 \le \frac{|A|}{4}$ and $5 \le t \le m_0 + 3$. For any subset T of $t-4$ elements in S_0, no four distinct elements in S_1 sum to $\delta - \sigma(T)$, implying that $\bar{S}_1$ is an $(m_1, 4, u)$-set in $\bar{A}$ for some $u \in \bar{A}$. This contradicts our induction hypothesis. □

IV. REMARKS ON THE ODD ORDER CASE

The case of odd-order groups seems to be much more complicated than that of even-order groups. In this section we present some bounds on $M(t, Z_p^h)$, p an odd prime. Consider first the case when $A = Z_p$. Here we have

$$M(t, Z_p) \ge \lfloor \frac{p-2}{t} \rfloor + t \triangleq r \tag{4.1}$$

by, e.g., taking the set $S = \{ 0, 1, 2, \cdots, r-1 \}$. Note that the smallest sum over the *integers* of any t distinct elements in S is $t(t-1)/2$, whereas the largest attainable such sum is $t(r-(t+1)/2)$. Our assertion follows from the fact that the difference does not exceed $p-1$. We conjecture that the lower bound of (4.1) holds with equality. Alon [2] points out that results obtained in [1] imply the following upper bound

$$M(t, Z_p) \le \frac{p}{t} + O\left(\sqrt{t} \cdot \frac{p}{\log \log p}\right)$$

which, for any fixed t and $p \to \infty$, yields

$$M(t, Z_p) = \frac{p}{t} \cdot (1 + o(1)) . \tag{4.2}$$

For the more general case of $A = Z_p^h$, $h \ge 1$, we have $M(t, Z_p^h) \ge (\lfloor (p-2)/t \rfloor + 1) \cdot p^{h-1} + ((p-2) \bmod t)$ by taking the elements of Z_p^h whose leading component a is in the range $0 \le a \le \lfloor (p-2)/t \rfloor$, together with $(p-2) \bmod t$ elements with their leading component being $\lfloor (p-2)/t \rfloor + 1$.

Lemma 4.1. *Let t be relatively prime to p. Then,*

$$M(t, Z_p^h) \le \frac{p^h - 1}{p^{h-1} - 1} \cdot M(t, Z_p^{h-1}) .$$

Proof. First, note that $M(t, A) = M(t, A, 0)$. Let S be an $(m, t, 0)$-set in Z_p^h, $m = M(t, A)$, and let H_S be the $h \times m$ matrix over Z_p representing S. Clearly, every nonsingular linear operation on the rows of H_S results in a matrix H which is an $(m, t, 0)$-set in Z_p^h. In particular, there exists such a matrix H containing a nonzero row of Hamming weight d satisfying

$$d \le \frac{(p-1)p^{h-1}}{p^h - 1} \cdot m$$

(the Plotkin bound [3, p. 49]). Such a row contains at least $m - d$ zeros and, therefore, we have,

$$M(t, Z_p^{h-1}) \ge m - d \ge \frac{p^h - 1 - (p-1)p^{h-1}}{p^h - 1} \cdot m = \frac{p^{h-1} - 1}{p^h - 1} \cdot M(t, Z_p^h) . \qquad \square$$

For $t \le p - 1$ this lemma implies

$$M(t, Z_p^h) \le \frac{p^h - 1}{p - 1} \cdot M(t, Z_p)$$

and, therefore, by (4.2) we obtain:

Theorem 4.1. *For any fixed t and $p \to \infty$,*

$$M(t, Z_p^h) = \frac{p^h}{t} \cdot (1 + o(1)) .$$

REFERENCES

[1] N. Alon, Subset sums, J. Number Theory 27 (1987) 196-205.

[2] N. Alon, private communication.

[3] I.F. Blake, R.C. Mullin, The Mathematical Theory of Coding (Academic Press, New York, 1975).

[4] G. Cohen, G. Zemor, An application of combinatorial group theory to coding, Ars

Combinatoria 23A (1987) 81-89.

[5] G.T. Diderrich, H.B. Mann, Combinatorial problems in finite Abelian groups, in: J.N. Srivastava et al., ed., A Survey of Combinatorial Theory, (North-Holland, Amsterdam, 1973).

[6] C.M. Liu, P.V. Kumar, On the maximum length of MDS Goppa codes on elliptic curves, preprint.

[7] S. MacLane, G. Birkhoff, Algebra (Macmillan, New-York, 1967).

[8] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, (North-Holland, Amsterdam, 1977).

[9] R.M. Roth, A. Lempel, A construction of non-Reed-Solomon type MDS codes, IEEE Trans. Inform. Theory (to appear).