A problem for Abelian groups

Gyula O.H. Katona*
Rényi Institute
Budapest, Hungary
ohkatona@renyi.hu

Leonid Makar-Limanov†
Dept. Math., Wayne State University
Detroit, MI 48202, USA
lml@math.wayne.edu

AMS subject index: 20K01, 94B99, 05D05 Keywords: Abelian group, constant weight codes, families of subsets

Abstract

1 The problem

Let A be a finite Abelian group of order n. Introduce the notation: $h = \left\lfloor \frac{n}{2} \right\rfloor$ and define the family

$$\mathcal{F}_a = \{\{x_1, \ldots, x_h\} : \text{ distinct elements of } A,\ x_1 + \ldots + x_h = a\}.$$

What can we say about the sizes of the families $\mathcal{F}_a$? It is obvious that

$$\sum_a |\mathcal{F}_a| = \binom{n}{h}$$

*The work of the first author was supported by the Hungarian National Foundation for Scientific Research, grant number NK062321.

†The work of the second author was supported by an NSA grant and by grant FAPESP, processo 06/59114-1.

holds, therefore there is an $a \in A$ such that

$$\frac{1}{n}\binom{n}{h} \leq |\mathcal{F}_a|. \tag{1}$$

These families have an interesting property.

Lemma 1.1 *If $F_1, F_2 \in \mathcal{F}_a$ are distinct members then $|F_1 \cap F_2| < h - 1$ holds.*

Proof. Suppose that $|F_1 \cap F_2| = h - 1$ holds for two members. Then

$$x_1 + \ldots + x_{h-1} + x_h = a, \qquad x_1 + \ldots + x_{k-1} + x'_h = a$$

implies $x_h = x'_h$, we have the same set. $\square$

All $(h-1)$-element subsets of members of $\mathcal{F}_a$ are distinct. By this property

$$|\mathcal{F}_a| h \leq \binom{n}{h-1}$$

and

$$|\mathcal{F}_a| \leq \frac{1}{h}\binom{n}{h-1} = \frac{2}{n}\binom{n}{h}(1 + o(1)) \tag{2}$$

holds for every $a \in A$.

Let $M(A)$ and $m(A)$ denote the size of the largest and smallest class $\mathcal{F}_a$ for a given Abelian group A:

$$M(A) = \max_{a \in A} |\mathcal{F}_a|, \quad m(A) = \min_{a \in A} |\mathcal{F}_a|.$$

Moreover, define

$$M(n) = \max_{A \text{ Abelian group}, |A| = n} M(A).$$

We have

$$\frac{1}{n}\binom{n}{h} \leq M(n) \leq \frac{2}{n}\binom{n}{h}(1 + o(1))$$

by (1) and (2).

Problem 1 *Determine*

$$\limsup \frac{M(n)}{\frac{1}{n}\binom{n}{h}}. \tag{3}$$

We will give some motivation for this problem from combinatorics/coding theory in Section 2. If (3) turns out to be more than 1 the result would be really useful for those applications. Unfortunately, in our example the ratio of the sizes of any two classes $\mathcal{F}_a$ tends to one.

Problem 2 *Is*

$$\lim_{|A|\to\infty} \frac{m(A)}{M(A)} = 1 \tag{4}$$

always true?

The least interesting version of our problem as far as the applications are concerned is the following one.

Problem 3 *How small can $m(A)$ be in asymptotical sense?*

2 The motivation

Let c_1 and c_2 be two 0,1 sequences of length n. Their *Hamming distance* is the number of different values in the n positions. A set of 0,1 sequences of length n is called a *code* of Hamming distance d if the Hamming distance of any two sequences (codewords) is at least d. Finally, a code is said to be of *fixed weight* h if the number of 1's in every codeword is exactly h.

An old problem of coding theory is to determine the maximum size of a code $C(n, h, 4)$ consisting of 0,1 sequences of length n, containing exactly h 1's where $h = \lfloor \frac{n}{2} \rfloor$, and having pairwise Hamming distance at least 4.

One can easily see that this problem is equivalent to the determination of the largest family $\mathcal{F}$ consisting of h-element subsets of an n-element set satisfying the condition $|F_1 \cap F_2| < h - 1$ for every pair of distinct members of $\mathcal{F}$. Therefore the upper bound (2) holds for this coding problem, too. The lower bound was given in [2] with the method shown in Section 1, using the Abelian group $\mathbb{Z}_n$. Hence we have

$$\frac{1}{n}\binom{n}{h} \le \max|C(n, h, 4)| \le \frac{2}{n}\binom{n}{h}(1 + o(1)).$$

There is no progress since [2]. The aim of our note is to attract more attention to the coding problem mentioned above with the algebraic problem suggested.

If the answer to Problem 1 is more than 1, it would give an improvement in the lower bound. If however, the answer is 1, no novelty for coding theory is obtained. Even so, we think it would be an interesting algebraic result.

The limit in Problem 2 has not been determined yet even for $\mathbb{Z}_n$. However the following conjecture is widely believed to be true.

Conjecture 1 (folklore)

$$\lim_{n\to\infty} \frac{m(\mathbb{Z}_n)}{M(\mathbb{Z}_n)} = 1.$$

For some applications of this coding problem to combinatorics, see [4], [1] and the survey [3].

3 Another trial

In this section the group $A = (\mathbb{Z}_2)^r$ is considered. Using the notation of Section 1, $n = 2^r$. In the case of this group all the sizes $|\mathcal{F}_a|$ can be exactly determined. Let $\mathcal{F}_a(k)$ denote the family of k-element subsets $\{x_1, \ldots, x_k\}$ of distinct elements of A satisfying

$$x_1 + \ldots + x_k = a.$$

The size $|\mathcal{F}_a(k)|$ will be denoted by $f_a(k)$.

Lemma 3.1 *If $a \neq 0, b \neq 0$ then*

$$f_a(k) = f_b(k)$$

holds.

Proof. A can be considered as the additive group of the Galois field $\mathrm{GF}(2^r)$. Then a multiplication is defined among the elements of A. The family $\mathcal{F}_1(k)$ is defined by

$$x_1 + \ldots + x_k = 1. \tag{5}$$

Its multiplication by a non-zero a gives

$$ax_1 + \ldots + ax_k = a.$$

The mapping from $\{x_1, \ldots, x_k\}$ to $\{ax_1, \ldots, ax_k\}$ is obviously a bijection between $\mathcal{F}_1(k)$ and $\mathcal{F}_a(k)$. So $f_a(k) = f_1(k)$ and the statement is proved. □

Lemma 3.2 *If k is odd then $f_1(k) = f_0(k)$.*

Proof. Since (5) implies $(x_1 + 1) + \ldots + (x_k + 1) = 0$, the mapping from $\{x_1, \ldots, x_k\}$ to $\{(x_1+1), \ldots, (x_k+1)\}$ is a bijection between $\mathcal{F}_1(k)$ and $\mathcal{F}_0(k)$. Hence $f_1(k) = f_0(k)$. □

Therefore the numbers $f_a(k)(a \in A)$ are all equal when k is odd and

$$f_a(k) = \frac{1}{2^r}\binom{2^r}{k}$$

holds in this case. We need, however, the case $k = h = 2^{r-1}$ where k is even.

Lemma 3.3 *If $\ell \geq 1$ then*

$$f_0(2\ell) = \frac{1}{2^r}\binom{2^r}{2\ell} + (-1)^\ell \left(1 - \frac{1}{2^r}\right)\binom{2^{r-1}}{\ell}. \tag{6}$$

Proof. Choose $k-1$ distinct elements $x_1, \ldots, x_{k-1} \in A$. We call such a set *good* if it can be extended to a member of $\mathcal{F}_0(k)$ by adding one element. The equation $x_1 + \ldots + x_k = 0$ always determines a unique x_k. However it might coincide with one of $x_1, \ldots, x_{k-1}$, not defining a member of $\mathcal{F}_0(k)$. If $x_k = x_u$ then $x_1 + \ldots + x_{u-1} + x_{u+1} + \ldots + x_{k-1} = 0$ gives a member of $\mathcal{F}_0(k-2)$. We see that the set $B = \{x_1, \ldots, x_{k-1}\}$ is good iff B does not contain a member of $\mathcal{F}_0(k-2)$.

A member of $\mathcal{F}_0(k-2)$ can be extended to a B in $2^r - (k-2)$ ways, therefore $(2^r - k + 2)f_0(k-2)$ of the $(k-1)$-element sets are not good. So

$$\binom{2^r}{k-1} - (2^r - k + 2)f_0(k-2)$$

$(k-1)$-element sets are good. Since every element of $\mathcal{F}_0(k)$ can be obtained from a B in exactly k ways we have the following recursion:

$$kf_0(k) = \binom{2^r}{k-1} - (2^r - k + 2)f_0(k-2). \tag{7}$$

Now the proof can be finished by induction on ℓ (with fixed r). The statement of the lemma is true for $\ell = 1$, since $f_0(2) = 0$. For the induction step we have to check that

$$\frac{1}{2\ell}\binom{2^r}{2\ell-1} - \frac{2^r - 2\ell + 2}{2\ell}\left[\frac{1}{2^r}\binom{2^r}{2\ell-2} + (-1)^{\ell-1}\left(1 - \frac{1}{2^r}\right)\binom{2^{r-1}}{\ell-1}\right]$$

is equal to (6). Fortunately the parts containing binomial coefficients of order 2^r and 2^{r-1} respectively are equal separately, making the verification easy. $\square$

If $r > 2$ then $\ell = 2^{r-2}$ in Lemma 3.3 gives

$$|\mathcal{F}_0| = f_0(2^{r-1}) = \frac{1}{2^r}\binom{2^r}{2^{r-1}} + \left(1 - \frac{1}{2^r}\right)\binom{2^{r-1}}{2^{r-2}}.$$

Using the fact that the sum of the sizes of all classes $\mathcal{F}_a$ is

$$\sum_{a\in(\mathbb{Z}_2)^r} |\mathcal{F}_a| = \binom{2^r}{2^{r-1}},$$

the formula

$$|\mathcal{F}_a| = \frac{1}{2^r}\left(\binom{2^r}{2^{r-1}} - \binom{2^{r-1}}{2^{r-2}}\right)$$

can be obtained for $a \neq 0$.

Summarizing, in this case $\mathcal{F}_a$ all have the same size, except for $\mathcal{F}_0$ which is somewhat larger. However, they are asymptotically equally sized.

So in this case we were able to prove that

Theorem 3.4 *For the family $(\mathbb{Z}_2)^r$ Problem 2 has a positive solution.*

References

[1] Annalisa De Bonis and Gyula O.H. Katona, Largest family without an r-fork, *Order* **24**(2007) 331-336.

[2] R.L. Graham and H.J.A. Sloane, Lower bounds for constant weight codes. *IEEE IT* **26**(1980) 37-43.

[3] Gyula O.H. Katona, Forbidden intersection patterns in the families of subsets (introducing a method), in *Horisons of Combinatorics*, eds. Ervin Győri, Gyula O.H. Katona, László Lovász, (Bolyai Society Mathematical Studies, **17**, Bolyai János Mathematical Society and Springer-Verlag, 2008) pp. 119-140.

[4] G.O.H. Katona and T.G. Tarján, Extremal problems with excluded subgraphs in the n-cube, in *Graph Theory, Lagów, 1981*, eds. M. Borowiecki, J.W. Kennedy, M.M. Sysło (Lecture Notes in Math. vol. **1018**, Springer-Verlag, 1983) pp. 84-93.