A NOTE ON A SUMSET IN $\mathbb{Z}_{2^k}$

OCTAVIO ALBERTO AGUSTÍN-AQUINO

Abstract. Let $A$ and $B$ be additive sets of $\mathbb{Z}_{2^k}$, where $A$ has cardinality $k$ and $B = v.\mathcal{C}A$ with $v \in \mathbb{Z}_{2^k}$. In this note some bounds for the cardinality of $A + B$ are obtained, using four different approaches.

1. Introduction

Let $U$ and $V$ be additive subsets of $\mathbb{Z}_{2^k}$ with cardinality $k$, and

$U + V = \{u + v : u \in U, v \in V\},$

$x.U = \{xa : x \in \mathbb{Z}_{2^k}, a \in U\}.$

I stumbled upon the problem of proving that, if $k$ is large enough and under certain hypothesis regarding the structure of $U$, we have

$|U + V| = 2k$

where $U$ is a set closely related to $V$. A very interesting case (at least from the mathematical counterpoint theory viewpoint) is when

$V = v.\mathcal{C}U, \quad v \in \mathbb{Z}_{2^k} \setminus \{-1\}$

and, additionally, $\mathcal{C}U = U + k$. In order to explain why, let $\overrightarrow{GL}(\mathbb{Z}_{2^k})$ be the set of bijective functions

$e^u.v : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_{2^k},$

$x \rightarrow vx + u,$

where $v \in \mathbb{Z}_{2^k}$ and $u \in \mathbb{Z}_{2^k}$. If $A \subseteq \mathbb{Z}_{2^k}$ is such that $g(A) \neq A$ for every $g \in \overrightarrow{GL}(\mathbb{Z}_{2^k})$ except the identity, and $A \cup p(A) = \mathbb{Z}_{2^k}$ for a unique $p \in \overrightarrow{GL}(\mathbb{Z}_{2^k})$, then it is called a counterpoint dichotomy and $p$ is its polarity.

Example 1. One of my favorite examples is $A = \{0, 2, 3\} \subseteq \mathbb{Z}_6$, whose polarity is $e^1 \cdot -1$. Another important specimen is

$K = \{0, 3, 4, 7, 8, 9\} \subseteq \mathbb{Z}_{12},$

Date: February 9, 2014.

2010 Mathematics Subject Classification. 11B13, 11L07.
with polarity $e^{2.5}$, for $K$ is the set of consonances in Renaissance counterpoint modulo octave, when the intervals in 12-tone equally tempered scale are interpreted as $\mathbb{Z}_{12}$. The interested reader may consult [6, Part VII] and references therein for further details.

Throughout this paper, we will attack (with varying degrees of generality) the following question.

**Question 1.** Given a subset $A \subseteq \mathbb{Z}_{2k}$ of cardinality $k$, is it true that

\begin{equation}
A + v, \mathcal{C}A = \begin{cases}
\mathbb{Z}_{2k}, & v \in \mathbb{Z}_{2k}^\times \setminus \{-1\}, \\
\mathbb{Z}_{2k} \setminus \{0\}, & v = -1?
\end{cases}
\end{equation}

If this question can be answered in the affirmative then, for any $e^u, (-v)$ except the identity, there exists $x \in A$ and $y \in \mathcal{C}A$ such that

$$x + (-v)y = u \quad \text{or} \quad vy + u = x \quad \text{or} \quad e^u.(-v)(y) \in A$$

which means that no element of $\overrightarrow{GL}(\mathbb{Z}_{2k})$ but the identity leaves the set $A$ invariant. If also there exists $p \in \overrightarrow{GL}(\mathbb{Z}_{2k})$ such that $p(A) = \mathcal{C}A$, then $A$ is a counterpoint dichotomy.

A set that I have been trying to prove it is a counterpoint dichotomy for a long time (for reasons I would state in some other place) via answering Question 1 is

\begin{equation}
A = \{0, 1\} \cup \{3, 4, \ldots, k - 1\} \cup \{k + 2\}.
\end{equation}

It is not difficult to verify that $e^k.1(A) = \mathcal{C}A$ and to see that

$$A + A = \mathbb{Z}_{2k} \quad \text{and} \quad A - A \supseteq \mathbb{Z}_{2k} \setminus \{k\},$$

since $2 = 1 + 1$, $2k - 1 = (k + 2) + (k - 3)$ and $k + 1 = (k - 2) + 3$. The other one is consequence of $3 - 1 = 2$ and $1 - 3 = -2$.

Although the following three sections do not prove $A$ satisfies the rest of (2), they provide some evidence and results that may be interesting on their own.

2. Using the Ruzsa distance

Let $U$ and $V$ be subsets of an additive group $G$. A couple of weak bounds for $|U + V|$ can be obtained using Ruzsa’s useful notion of “distance” in additive combinatorics

$$d(U, V) = \log \frac{|U - V|}{\sqrt{|U||V|}},$$

which is a seminorm. In particular, it satisfies a triangle inequality

$$d(U, V) \leq d(U, W) + d(W, V).$$
Note now that, regarding the set \( A \), we have
\[
d(A, -A) = \log \frac{|A + A|}{|A|} = \log \frac{2k}{k} = \log 2;
\]
the number \( \delta(U) = \exp(d(U, -U)) \) is the \textit{doubling constant} of the set \( U \), and thus \( \delta(A) = 2 \).

From the Ruzsa triangle inequality we can deduce [9, p. 61]
\[
|U||V - V| \leq |U + V|^2
\]
which, for the case of \( V = A \) and \( U = B \), specializes to
\[
|A + B| \geq \sqrt{|B||A - A|} \geq \sqrt{k(2k - 1)} = \sqrt{2 - \frac{1}{k}}.
\]

On the other hand, again by the triangle inequality
\[
\log 2 = d(A, -A) \leq d(A, B) + d(B, -A)
\]
and a pigeon-hole argument, either
\[
d(A, B) \geq \frac{1}{2} \log 2
\]
or
\[
d(-A, B) = d(A, -B) \geq \frac{1}{2} \log 2.
\]

Equivalently, either
\[
|A - B| \geq \sqrt{2k}
\]
or
\[
|A + B| \geq \sqrt{2k}.
\]

We conclude that, for any subsets \( A \) and \( B \) of the cardinality \( k \) such that \( \delta(A) = 2 \), we have
\[
\max(|A + B|, |A - B|) \geq \sqrt{2k}.
\]

I have not been able to find pairs of subsets of \( \mathbb{Z}_{2k} \) such that \( A \) has doubling constant 2 and \( |A + B| \) or \( |A - B| \) get arbitrarily close to this bound.

### 3. Using additive energy and a theorem by Olson

Let
\[
[P] = \begin{cases} 
1, & P \text{ is true,} \\
0, & \text{otherwise,}
\end{cases}
\]
be the Iverson bracket [8, p. 24], and define the \textit{additive energy} of the subsets \( U \) and \( V \) of the additive group \( G \) by
\[
E(U, V) = \sum_{u_1, u_2 \in U, v_3, v_4 \in V} [u_1 + u_2 = v_3 + v_4].
\]
Another well-known inequality [9, p. 63] for the cardinality of $U + V$ is

$$|U \pm V| \geq \frac{(|U||V|)^2}{E(U, V)}.$$

From this we infer another strategy to improve the previous estimates for $|A + B|$, namely finding upper bounds for $E(A, B)$. A good start might be the Cauchy-Schwarz inequality

$$E(A, B) \leq \sqrt{E(A, A)E(B, B)}.$$

This seems promising when $B = v.\mathcal{C} A$ and $\mathcal{C} A = A + \{k\}$, since the invertibility of $v$ implies

$$E(v.\mathcal{C} A, v.\mathcal{C} A) = \sum_{a_1, a_2, a_3, a_4 \in A + \{k\}} [va_1 + va_2 = va_3 + va_4]$$

$$= \sum_{a_1, a_2, a_3, a_4 \in A} [v(a_1 + a_2) = v(a_3 + a_4)]$$

$$= \sum_{a_1, a_2, a_3, a_4 \in A} [a_1 + a_2 = a_3 + a_4] = E(A, A).$$

Thus $E(A, v.\mathcal{C} A) \leq E(A, A)$. Nevertheless, this straightforward approach loses some of its charm as soon as we calculate a few values of the energy and the corresponding bounds.

As it is readily seen in Table 1, the quality of the bound is expected to decrease as $k$ increases, although it would remain as a mild improvement with respect the one obtained in the previous section. In fact, assuming $E(A, A)$ is a polynomial in $k$, from a simple interpolation we

| $k$ | $E(A, A)$ | $\frac{(|A||v.\mathcal{C} A|)^2}{E(A, A)} - \frac{k^4}{2E(A, A)}$ | $\frac{k^3}{2E(A, A)}$ |
|-----|-----------|---------------------------------|----------------|
| 8   | 296       | 13.84                           | 0.86           |
| 9   | 425       | 15.44                           | 0.86           |
| 10  | 590       | 16.95                           | 0.85           |
| 11  | 795       | 18.42                           | 0.84           |
| 12  | 1044      | 19.86                           | 0.83           |
| 100 | 665180    | 150.34                          | 0.751          |
| 1000| 666651080 | 1500.04                         | 0.750          |

Table 1. Additive energy $E(A, A)$ for small $k = |A|$, where $A$ is defined by (2), and the corresponding bounds for $|A + B|$ and the fraction of $\mathbb{Z}_{2k}$ that is guaranteed to be covered by $A + B$. 

Thus $E(A, v.\mathcal{C} A) \leq E(A, A)$. Nevertheless, this straightforward approach loses some of its charm as soon as we calculate a few values of the energy and the corresponding bounds.

As it is readily seen in Table 1, the quality of the bound is expected to decrease as $k$ increases, although it would remain as a mild improvement with respect the one obtained in the previous section. In fact, assuming $E(A, A)$ is a polynomial in $k$, from a simple interpolation we
find that
\[ E(A, A) = \frac{2}{3}k^3 - \frac{47}{3}k + 80. \]

This means that, for \( k \geq 6 \), we have \( E(A, A) \leq \frac{2}{3}k^3 \), and then
\[ |A \pm v, \mathcal{C}A| \geq \frac{3}{2}k. \]

This bound can be obtained from a theorem due to Olson, and actually it holds for any set \( B \) of cardinality \( k \). Before stating Olson’s theorem, observe that an additive subset \( U \) of \( G \) is contained in a coset of a unique smallest subgroup \( H \) of \( G \). Denote with \([U] \) such a coset.

**Theorem 1** (Olson, 1984, [7], [5].) Let \( U \) and \( V \) be additive subsets of \( G \). If \( U + V \neq G \) and \([U] = G\), then \(|U + V| \geq \frac{1}{2}|U| + |V|\).

Suppose \( G = \mathbb{Z}_{2k} \) and \( U = A \). Any coset containing \( A \) has cardinality at least \( k \). But it cannot have exactly \( k \) elements, for the cosets would be forced to be either the set of even elements of \( \mathbb{Z}_{2k} \) or its complement, but clearly \( A \) is contained in neither. Thus \([A] = \mathbb{Z}_{2k}\), so if \( A + B \) is not the whole group, it must consist in at least \( \frac{1}{2}k + k = \frac{3}{2}k \) elements.

4. **Using trigonometric sums**

Let \( r_{U+V}(t) \) the number of representations of \( t \) as a sum \( t = u + v \) for \( u \in U \) and \( v \in V \), where \( U, V \) are additive subsets of a group \( G \). The following is a standard technique using the so-called trigonometric sums in number theory (a readable and short introduction can be found in [2]). Note first that
\[ \frac{1}{m} \sum_{\xi=0}^{m-1} e^{2\pi i \xi x/m} = [x \equiv 0 \pmod{m}], \]
so we can write
\[ \frac{1}{2k} \sum_{\xi=0}^{2k-1} e^{2\pi i (u+v-\lambda)/(2k)} = [u + v \equiv \lambda \pmod{2k}]. \]

If we sum over \( U \) and \( V \) and exchange the order of summation,
\[ r_{U+V}(\lambda) = \sum_{u \in U} \sum_{v \in V} [u + v \equiv \lambda \pmod{2k}]. \]

\[
= \frac{1}{2k} \sum_{u \in U} \sum_{v \in V} \sum_{\xi=0}^{2k-1} e^{2\pi i (u+v-\lambda)/(2k)}
\]

\[
= \frac{1}{2k} \sum_{\xi=0}^{2k-1} \left( \sum_{u \in U} e^{2\pi i u/(2k)} \sum_{v \in V} e^{2\pi i v/(2k)} \right) e^{-2\pi i \xi \lambda/(2k)},
\]
and then we extract the $\xi = 0$ term, we conclude
\[ r_{U\cap V}(\lambda) = \frac{k}{2} + E \]
where, by the triangle inequality,
\[ |E| \leq \frac{1}{2k} \sum_{\xi=1}^{2k-1} \left| \sum_{u \in U} e^{\pi i \xi u/k} \right| \left| \sum_{v \in V} e^{\pi i \xi v/k} \right| = 2k \sum_{\xi=1}^{2k-1} |\hat{1}_U(\xi)||\hat{1}_V(\xi)| \]
and
\[ \hat{f}(\xi) := \frac{1}{|G|} \sum_{x \in G} f(x)e^{2\pi i \xi x/|G|} \]
is the Fourier transform. Observe now that $|\hat{1}_{v \cdot cA}(\xi)| = |\hat{1}_{cA}(\xi)| \leq |\hat{1}_A(\xi)|$, so for $U = A$ and $V = v \cdot cA$, we have
\[ |E| \leq 2k \sum_{\xi=1}^{2k-1} |\hat{1}_A(\xi)|^2 \leq k, \]
which is not useful. On the other hand, since (see [10, p. 24])
\[ |\hat{1}_A(\xi)| \leq \frac{1}{2k \sin(\pi \xi/(2k))} + \frac{1}{k} \]
then
\[ \sum_{\xi=1}^{2k-1} |\hat{1}_A(\xi)|^2 \leq \sum_{\xi=1}^{2k-1} \left( \frac{1}{2k \sin(\pi \xi/(2k))} + \frac{1}{k} \right)^2 \]
\[ = 2 \sum_{\xi=1}^{k} \left( \frac{1}{2k \sin(\pi \xi/(2k))} + \frac{1}{k} \right)^2 - \frac{9}{4k^2}. \]
Now the sequence
\[ a_{k,\xi} = \begin{cases} \left( \frac{1}{2k \sin(\pi \xi/(2k))} + \frac{1}{k} \right)^2, & 1 \leq \xi \leq k, \\ 0, & \text{otherwise} \end{cases} \]
is such that $a_{k,\xi} \geq a_{k+1,\xi}$ and $\sum_{\xi=1}^{\infty} a_{1,\xi} = \frac{9}{4}$. By the monotone convergence theorem, we obtain
\[ \lim_{k \to \infty} \sum_{\xi=1}^{2k-1} |\hat{1}_A(\xi)|^2 = 2 \lim_{k \to \infty} \sum_{\xi=1}^{k-1} \frac{1}{\pi^2 \xi^2} = \frac{1}{3}, \]
which amounts to estimate $|E| \leq \frac{2}{3}k$ for large $k$, but that is not enough to ensure that $r_{A+v \cdot cA}(\lambda) \geq 0$ for any $\lambda$ and $v \neq -1$. Furthermore, it suggests that the most we can get this way is $|A + v \cdot cA| \geq \frac{5}{6}k$ (see [9, p. 210]).
In our last attempt we use the following generalization of the celebrated Cauchy-Davenport theorem.

**Theorem 2** (Mann, 1965, cf. [8]). *Let $S$ be a subset of an arbitrary abelian group $G$. Then one of the following holds:

1. For every subset $T$ such that $S + T \neq G$, we have $|S + T| \geq |S| + |T| - 1$.
2. There exists a proper subgroup $H$ of $G$ such that $|S + H| < |S| + |H| - 1$.

Thus one of these two alternatives holds:

1. It is true that $|A + v.\mathbb{C}A| \geq |A| + |v.\mathbb{C}A| + 1 = 2k - 1$.
2. There is proper subgroup $H$, such that $|A + H| < k + |H| + 1$.

We claim that, for the set $A$, we have

$$|A + v.\mathbb{C}A| \geq 2k - 1$$

by discarding the second alternative. In order to do so, suppose $H = \langle d \rangle$ where $0 \leq d \leq k$ and

$$|H + A| < k + |H| + 1.$$

Being $H$ proper, we have $|H| \leq k$. Let us suppose that $d \geq 1$ (since the trivial case is covered by the first alternative), which implies that $|H| = \frac{2k}{d}$. Thus $A + H$ is the placement of copies of $A$ with spaces of $d$ elements, so it covers all the elements of $\mathbb{Z}_{2k}$ with at most $\frac{2k}{d}$ exceptions, thus

$$k + \frac{2k}{d} - 1 > |A + H| \geq 2k - \frac{2k}{d}.$$

This is possible if, and only if,

$$\frac{2k}{d} + k - 1 > 2k - \frac{2k}{d}$$

or, equivalently,

$$4 > \frac{4k}{k + 1} > d,$$

thereof $d = 2$ or $d = 3$. If $d = 2$, we are done, for $A$ has $\{0, 1\}$ as a subset, thus $A + H = \mathbb{Z}_{2k}$, a contradiction.

In the later case (which arises only when 3 divides $k$), it would be possible that each “slot” of $d$ elements determined by $H$ and covered by $A$ to have a gap, but the “antipodal” slot would fill the gap, covering it with the translate of $k + 2 \in A$. Moreover: we are certain that a copy of $A$ is placed in $k$ because 3 is one of its factors. So, $A + H$ would
leave no gap uncovered, for there are an even number of slots, each one paired with his antipode. Hence $H = \langle 3 \rangle$ is also an impossibility.

From the above proof we also obtain that $A$ is aperiodic, i.e., $A + H \neq A$ except for $H = \{0\}$. Invoking Kemperman structure theorem (as stated, for example, in [4]), we conclude that

$$A - C_A = \mathbb{Z}_{2^k} \setminus \{0\}$$

and, furthermore, if $A + v.C_A \neq \mathbb{Z}_{2^k}$, then there exists $u$ such that

$$v.C_A = u - C_A.$$

This equivalent to the following: for any $v \in \mathbb{Z}_{2^k}^* \setminus \{-1\}$, and any $u$ it is true that

$$-v.A + u \neq A,$$

which means exactly that $A$ is a counterpoint dichotomy. Thus, Kemperman’s theorem cannot lead us further in relation to the cardinality of $A + v.C_A$.

6. Some final remarks

The results distilled from Mann’s and Kemperman’s theorems takes us rather close to the goal of proving that (1) holds for the set $A$ defined by (2), but ultimately fail. Nevertheless, they make evident that there is a significant gap between $E(A, v.C_A)$ and $E(A, A)$. They also point out that, in order to succeed with the use of exponential sums, a very sharp estimate of (3) is required.

7. Acknowledgments

I sincerely thank my friends José Hernández Santiago at Centro de Ciencias Matemáticas (UNAM) and Marcelino Ramírez Ibáñez at Universidad del Papaloapan for their invaluable feedback regarding early drafts of this paper. I also thank an anonymous reviewer who brought an embarrassing blunder to my attention.

References

1. Thomas Boothby, Matt DeVos, and Amanda Montejano, A new proof of Kemperman’s theorem, arXiv:1301.0095 (2013).
2. Moubariz Z. Garaev, Sumas trigonométricas y congruencias aditivas, Gaceta de la Real Sociedad Matemática Española 12 (2009), no. 1, 129–143.
3. Ronald Graham, Donald Knuth, and Oren Patashnik, Concrete mathematics, 2nd ed., Addison-Wesley, 1994.
4. David J. Grynkiewicz, A step beyond Kemperman’s structure theorem, Mathematika 55 (2009), no. 1-2, 67–114.
5. Vsevolod F. Lev, Critical pairs in abelian groups and Kemperman’s structure theorem, International Journal of Number Theory 2 (2006), no. 03, 379–396.
6. Guerino Mazzola, *The topos of music: Geometric logic of concepts, theory, and performance*, Birkhäuser Verlag, 2002.
7. John E. Olson, *On the sum of two sets in a group*, Journal of Number Theory 18 (1984), no. 1, 110–120.
8. Oriol Serra and Gilles Zémor, *On a generalization of a theorem by Vosper*, INTEGERS 0 (2000), A10.
9. Terence Tao and Van Vu, *Additive combinatorics*, Cambridge studies in advanced mathematics, no. 105, Cambridge University Press, 2006.
10. Ivan M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Interscience Publishers, 1954.

Universidad de la Cañada, San Antonio Nanahuatipan Km 1.7 s/n. Paraje Titlacuautitla, Teotitlan de Flores Magón, Oaxaca, México, C.P. 68540.

E-mail address: octavioalberto@unca.edu.mx