An Improvement on Olson’s Constant for $\mathbb{Z}_p + \mathbb{Z}_p$
Gautami Bhowmik, Jan-Christoph Schlage-Puchta

To cite this version:
Gautami Bhowmik, Jan-Christoph Schlage-Puchta. An Improvement on Olson’s Constant for $\mathbb{Z}_p + \mathbb{Z}_p$. Acta Arithmetica, Instytut Matematyczny PAN, 2009. <hal-00279276>
AN IMPROVEMENT ON OLSON’S CONSTANT FOR $\mathbb{Z}_p \oplus \mathbb{Z}_p$

GAUTAMI BHOWMIK AND JAN-CHRISTOPH SCHLAGE-PUCHTA

Abstract. We prove that for a prime number $p$ greater than 6000, the Olson’s constant for the group $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is given by $\text{Ol}(\mathbb{Z}_p \oplus \mathbb{Z}_p) = p - 1 + \text{Ol}(\mathbb{Z}_p)$.

1. Introduction

Let $G$ be a finite additive abelian group of order $n$. A subset $A$ of $G$ is said to be a zero-sum set if the sum of all its elements is zero. and $\text{Ol}(G)$, the Olson’s constant of $G$, is defined to be the smallest integer $k$ such that every set of $k$ elements of $G$ contains a zero-sum subset.

The exact value of this constant is only known for a few cases. As far as bounds are concerned, Szemerédi[6] proved the Erdős-Heilbronn conjecture that $\text{Ol}(G) \leq c\sqrt{n}$, $c$ being an absolute constant. For cyclic groups, the conjectural value of $c$ (due to Erdős and Graham) $\sqrt{2}$, was recently attained by Nguyen, Szemerédi and Vu[3]. The conjecture was verified by Gao, Ruzsa and Thangadurai[4] for $\mathbb{Z}_p \oplus \mathbb{Z}_p$ for all $p > 4.67 \times 10^{34}$. They in fact proved that $\text{Ol}(\mathbb{Z}_p^2) = p - 1 + \text{Ol}(\mathbb{Z}_p)$ for such a $p$. Our aim is to improve the bound for $p$, and we prove that

Theorem 1. Let $p > 6000$ be a prime number. Then $\text{Ol}(\mathbb{Z}_p^2) = p - 1 + \text{Ol}(\mathbb{Z}_p)$.

Our proof falls into two parts, the first one being combinatorial and dealing with the case where the elements of $A$ are not well-distributed over $\mathbb{Z}_p$, the second one being analytical, using exponential sums. Unfortunately, our bound is still too large to allow for explicit computations. Though our method could be used to lower the bound for $p$ further, we would not be able to go below $p < 200$.

Many similar zero-sum problems have been studied, one among them being the Davenport’s constant where the objects are multi-sets rather than sets.

2. Proof

For a set $A$, we use $\Sigma(A)$ for the set of all its subset sums while $\Sigma_k(A)$ denotes the set of all sums of those subsets which have $k$ elements. We will use the fact that $\text{Ol}(\mathbb{Z}_p) \geq \lfloor \sqrt{2p} \rfloor$.[3]

The following result was proven by Olson [5, Theorem 2].

Lemma 1. Let $A \subseteq \mathbb{Z}_p$ be a set, $k$ an integer in the range $1 \leq k \leq |A|$. Then we have $|\Sigma_k(A)| \geq \min(p, k(|A| - k) + 1)$.

In particular, if $|A| \geq \ell := \lfloor \sqrt{4p - 1} \rfloor + 1$, and $k = \lfloor \ell / 2 \rfloor$, then $\Sigma_k(A) = \mathbb{Z}_p$.

Lemma 2. For $A, B \subseteq \mathbb{Z}_p$ we have $|A + B| \geq \min(p, |A| + |B| - 1)$.

The following result was proven by Olson [5, Theorem 2].
Lemma 3. Let $A \subseteq \mathbb{Z}_p$ be a set with all elements distinct and $|A| = s$. Suppose that for all $a \in A$, $-a \not\in A$; in particular, $0 \not\in A$. Then we have

$$|\Sigma(A)| \geq \min \left( \frac{p+3}{2}, \frac{s(s+1)}{2} + \delta \right),$$

where

$$\delta = \begin{cases} 1, & s \equiv 0 \pmod{2} \\ 0, & s \equiv 1 \pmod{2} \end{cases}.$$

In the sequel let $A \subseteq \mathbb{Z}_p^2$ be a zero-sum free set of size $p - 1 + \text{O}(\mathbb{Z}_p)$. Our aim is to show the following:

Theorem 2. Let $A \subseteq \mathbb{Z}_p^2$ be a zero-sum free set of size $p - 1 + \text{O}(\mathbb{Z}_p)$. Then there exists a subgroup $U \cong \mathbb{Z}_p$, such that $|A \cap U| = \text{O}(\mathbb{Z}_p)$, and all other elements of $A$ are contained in one coset of $U$.

Clearly, Theorem 2 implies Theorem 1. For an affine subspace $x + U$ and a set $B$ define $N(x, U, B) = |B \cap (x + U)|$. Set $M = M(A) = \max_{x, U} N(x, U, A)$.

Lemma 4. Suppose that $M \geq 2p/5$. Then Theorem 2 holds true for $A$.

Proof. This follows immediately from [1, Lemma 3.4] and [2, Lemma 3.5].

The following is the main technical result of the combinatorial part.

Lemma 5. Let $U$ be a non-trivial subgroup, and $B \subseteq A$ a set. Let $\pi : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ be a projection with kernel $U$, and let $x_1, \ldots, x_p$ be representatives of $\mathbb{Z}_p^2/U$. Suppose that the multi-set $\pi(B)$ represents each element of $\mathbb{Z}_p$ as a (possibly empty) subset sum, and that $\sum_i |N(x_i, U, A \setminus B)/2| [N(x_i, U, A \setminus B)/2] \geq p + 1$. Then $A$ contains a zero-sum.

Proof. Among each set $(A \setminus B) \cap (x_i + U)$ we choose all subsets of size $|N(x_i, U, A \setminus B)$ and add them up. By Lemma 1 we obtain in this way at least $[N(x_i, U, A \setminus B)/2] [N(x_i, U, A \setminus B)/2] = p + 1$. Then $A$ contains a zero-sum.

We shall repeatedly apply this Lemma to reduce the size of the numbers $N(x, U, A)$.

Lemma 6. Suppose that $p \geq 29$ and $2p/5 \geq M \geq \lceil \sqrt{4p-7} \rceil + 1$. Then $A$ contains a zero-sum.

Proof. Let $U$ be a subgroup such that there exist some $x$ with $N(x, U, A) = M$, and let $\pi$ be a projection with kernel $U$. We choose $\lceil \sqrt{4p-7} \rceil + 1$ elements in one coset, and let $B$ be the complement of this set. Consider the multi-set $\overline{B} = \pi(B)$. Then $|\overline{B}| \geq p - \sqrt{p}$. Moreover, $\overline{B}$ contains no element with multiplicity $\geq 2p/5$, hence, in $B$ we can find a system of $p/5 - \sqrt{p}$ disjoint subsets containing 3 different elements, that is, we find $p/5 - \sqrt{p}$ subsets containing two different elements, which are not inverse to each other. Hence, we have

$$p \geq |\Sigma(B)| \geq \min(p, 3(p/5 - \sqrt{p}) + (p - 2(p/5 - \sqrt{p})) = \min(p, 6/5p - \sqrt{p}) = p,$$

and we see that we can apply Lemma 5 to obtain our claim.

□
We now combine Lemma 3 with an estimate for exponential sums to obtain a
criterion for our theorem to hold which is numerically applicable.

Lemma 7. Let \( p > 800 \) be a prime number. Let \( A \subseteq \mathbb{Z}_p^2 \) be a subset with \( |A| = p + \text{OL}(\mathbb{Z}_p) \). For a subgroup \( U \cong \mathbb{Z}_p \) fix a complement \( V \), and define \( \lambda_i^j = N(j, U, A) \),
where \( j \) is viewed as an element of \( V \) via the isomorphism \( \mathbb{Z}_p \cong V \). Suppose that
one of the following two conditions holds true.

1. There exists a subgroup \( U \), such that the following holds true. Denote by
   \( J \) the set of indices \( j \) such that \( \lambda_i \) is odd. Suppose there exists a set of
   integers \( I \subseteq \mathbb{Z}_p \), such that \( \lambda_i \geq 1 \) for all \( i \in I \), \( \Sigma(I \cup J) = \mathbb{Z}_p \), and
   \( \sum_{j} [\lambda_i^j/2][\lambda_i^j/2] \geq p - 1 \), where
   \[
   \lambda_i^j = \begin{cases} 
   \lambda_i - 1, & i \in I, \\
   \lambda_i, & \text{otherwise}.
   \end{cases}
   \]

2. For all subgroups \( U \) and all isomorphisms \( \mathbb{Z}_p \cong V \) we have the bound
   \[
   \prod_{i=0}^{p-1} |\cos \frac{j\pi}{p}|^{|\lambda_i|} \leq \frac{1}{p^2}.
   \]

Then every subset \( A \subseteq \mathbb{Z}_p^2 \) with \( |A| = p + \text{OL}(\mathbb{Z}_p) \) contains a zero-sum.

Proof. Let \( A \) be a subset of \( \mathbb{Z}_p^2 \) with \( |A| = p + \text{OL}(\mathbb{Z}_p) \).

Suppose that there exists a subgroup \( U \), such that for the partition \( \lambda_i = N(U, i, A) \)
the first condition holds true. Set \( x = \sum_{i} i[\lambda_i^j/2] \). By assumption we can choose
a subset of \( I \cup J \) adding up to \(-x\), let \( I', J' \) be the intersection of this set with
\( I \) and \( J \), respectively. Then we choose elements \( x_j \) in \( A \cap (j, 0) + (0, 1)\mathbb{Z}_p \) for
all \( j \in I' \cup J' \), these elements sum up to an element \( s \) with first coordinate \(-x\).
Hence, if we choose a set \( A_j \) consisting of \( \lambda_i^j/2 \) elements in \( (j, 0) + (0, 1)\mathbb{Z}_p \),
then \( \sum_{j} \sum_{a \in A_j} a + \sum_{j \in I' \cup J'} x_j \) has first coordinate 0. To prove that \( A \) contains a
zero-sum, it suffices to show that by choosing the sets \( A_j \) in all possible ways, all elements in \( (0, 1)\mathbb{Z}_p \) can be reached, and from Lemma 3 and 4 we see that this is the case if \( \sum_{j} [\lambda_i^j/2][\lambda_i^j/2] \geq p - 1 \), thus, the first condition is sufficient.

Hence, we may assume that for each subgroup \( U \) the partition \( N(i, U, A) \) satisfies
the second condition. Write \( e(x) = e^{2\pi i x/p} \); we view this as a function \( e : \mathbb{Z}_p \to \mathbb{C} \).
Then using orthogonality we see that the number of subsets of \( A \) adding up to 0 equals
\[
\frac{1}{p^2} \sum_{\alpha \in \mathbb{Z}_p^2} \prod_{a \in A} 1 + e((a, \alpha)).
\]

Clearly, the summand \( \alpha = 0 \) contributes \( \frac{2|A|}{p^2} \). We have
\[
\prod_{a \in A} |1 + e((a, (0, 1)))| = \prod_{j \in \mathbb{Z}_p} |1 + e(j)|^{N(j, (0, 1), A)}
\]
\[
= 2^{|A|} \prod_{j \in \mathbb{Z}_p} |\cos(\pi j/p)|^{N(j, (0, 1), A)} \leq 2^{|A|} \frac{p^2}{p^2},
\]
where in the last step we used the second condition. Hence, the number of zero-sums
is bounded from below by

\[
\frac{2^{|A|}}{p^2} \frac{p^2 - 1}{p^2} \frac{2^{|A|}}{p^4} \geq 2,
\]

provided that \( p \geq 11 \), that is, there exists a non-empty subset with sum 0. \( \square \)

Note that the two conditions in the lemma work in different directions: While
the first condition says that most of the \( \lambda_j \) are small, the second condition says
that most of the weight of the partition lies on indices \( i \) which are close to 0 or to
\( p \), from this difference we shall obtain our result.

**Lemma 8.** Suppose that \( p > 1024 \) and that there exists a subgroup \( U \) such that
the image \( \pi(A) \) of the projection has less than \( p/5 \) elements. Then \( A \) contains a
zero-sum.

**Proof.** We choose a subset \( B \subset A \), such that all elements of \( \mathbb{Z}_p \) can be represented as
subset sums of \( B \), and \( |A \setminus B| \geq p \). Set \( f(\ell) = [\ell/2] \lfloor \ell/2 \rfloor \). If \( \sum_x f(N(x, U, A \setminus B)) \geq p \), we can apply Lemma 5. The function
\( f \) is convex, hence, we have

\[
\sum_x f(N(x, U, A \setminus B)) \geq f(5) \frac{6}{5} |A \setminus B| = \frac{6}{5} |A \setminus B|,
\]

and it suffices to show that we can choose \( B \) sufficiently small. Suppose first that the
projection of \( A \) onto \( U \) contains at least \( \sqrt{4p - 7} \) different elements. Then we take
arbitrary different elements and obtain our claim, provided that \( p/5 + O(\mathbb{Z}_p) \geq \sqrt{4p - 7} \), which is certainly the case for \( p > 100 \). If the projection of \( A \) onto \( U \)
contains less elements, there are \( p/2 \) elements in \( A \) contained in pre-images of \( \pi_U \)
of single points, which contain \( \sqrt{p}/4 \) elements. Let \( B \) be the complement of this
set. Again from convexity we see that \( \sum_x f(N(x, U, A \setminus B)) \geq p \), provided that
\( \sqrt{p}/4 \geq 8 \), which is the case for \( p > 1024 \). On the other hand, the remaining points
may be partitioned into sets containing \( p/2 \) elements altogether, and no \( 2\sqrt{p} \) have
the same image under \( \pi_U \), hence, we see that \( \Sigma(B) = \mathbb{Z}_p \) as well. \( \square \)

**Lemma 9.** Suppose that \( p > 6000 \). Then \( A \) contains a zero-sum.

**Proof.** For every subgroup we can select \( p/5 \) elements with different value under
\( \pi_U \). Since \( 4p/5 + O(\mathbb{Z}_p) > \sqrt{4p - 7} \), it suffices to show that the second condition
of Lemma 5 is satisfied for each set consisting of \( p/5 \) different elements. We have

\[
\log \prod_{j=-p/10}^{p/10} \cos(j\pi/p) < \int_{-p/10}^{p/10} \log(\cos(t\pi/p)) \, dt
\]

\[
= p \int_{-1/10}^{1/10} \log(\cos(t)) \, dt
\]

\[
< -0.00332296p,
\]

hence, our claim follows provided that \( p^2 < 1.003328p \), which is the case for \( p > 6000 \). \( \square \)

There are several obvious ways to improve the argument. First, \( p/5 \) in Lemma 5
can be improved, but not beyond \( p/4 \). Then, \( \frac{1}{p^2} \) in the second condition of Lemma 5
can be improved, since the exponential sum will have a smaller value most of the
time. However it will be difficult to ensure that for some subgroup there will
be no large term, that is, we do not expect to obtain anything better than $\frac{1}{p}$. Finally, one could consider the set of all partitions explicitly in the second part of Lemma 3, the improvement here is certainly smaller than the bound obtained by taking $p/4$ elements four times each. However, none of these improvements is completely straightforward and even if we suppose that the technical difficulties could be overcome, our method cannot reach $p = 200$, since the computational amount would increase dramatically – in particular for enumerating all partitions of $p$. Hence we do not attempt to push our method to its limits. Still we did formulate Lemma 3 in a more general way than we actually needed to help eventual improvements.

References