#A38 INTEGERS 18 (2018)

PACKING SETS OVER FINITE ABELIAN GROUPS

Oliver Roche-Newton
Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria
o.rochenewton@gmail.com

Ilya D. Shkredov
Division of Number Theory, Steklov Mathematical Institute, Moscow, Russia; IITP, Moscow, Russia; and *MIPT, Dolgoprudnii, Russia*
ilya.shkredov@gmail.com

Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria
arne.winterhof@oeaw.ac.at

Received: 6/29/17, Accepted: 4/13/18, Published: 4/20/18

Abstract

For a given subset $A \subseteq G$ of a finite abelian group $(G, \circ)$, we study the problem of finding a large packing set B for A, that is, a set $B \subseteq G$ such that $|A \circ B| = |A||B|$. Ruzsa's covering lemma and the trivial bound imply the existence of such a B of size $|G|/|A|^2 \leq |G|/|A \circ A^{-1}| \leq |B| \leq |G|/|A|$. We show that these bounds are in general optimal. More precisely, denote by $\nu(A)$ the maximal size of an A-packing set, then essentially any $\nu(A)$ in the interval $[|G|/|A|^2, |G|/|A|]$ can appear for some $|A|$. The case that G is the multiplicative group of the finite field $\mathbb{F}_p$ of prime order p and $A = \{1, 2, \dots, \lambda\}$ for some positive integer λ is particularly interesting in view of the construction of limited-magnitude error correcting codes. Here we construct a packing set B of size $|B| \gg p(\lambda \log p)^{-1}$ for any $\lambda \leq 0.9p^{1/2}$. This result is optimal up to the logarithmic factor.

1. Introduction

Given two subsets A and B of a finite abelian group $(G, \circ)$ with unit 1, the *product set* of A and B is defined as

$$A \circ B := \{a \circ b : a \in A, b \in B\}.$$

We consider the cardinality of this product set. A simple observation is that the trivial bound

$$|A \circ B| \leq \min\{|A||B|, |G|\}$$

holds for any $A, B \subseteq G$.

In this paper, we seek to answer the following question: given $\emptyset \neq A \subseteq G$, what is the size of the largest set $B \subseteq G$ such that $|A \circ B| = |A||B|$? We call any B with $|A \circ B| = |A||B|$ an A-*packing set* and denote by $\nu(A)$ the maximal size of an A-packing set:

$$\nu(A) := \max\{|B| : B \subseteq G, |A \circ B| = |A||B|\}.$$

Suppose that we have such a set B. Since $|A||B| = |A \circ B| \leq |G|$, it must be the case that $|B| \leq |G|/|A|$ and thus

$$\nu(A) \leq \left\lfloor \frac{|G|}{|A|} \right\rfloor.$$

For some interesting sets A, it can be easily established that $\nu(A)$ is close to $|G|/|A|$. For example, if $A \subseteq G$ is a subgroup with distinct cosets $x_1 \circ A, x_2 \circ A, \ldots, x_k \circ A$ where $k = |G|/|A|$, we can take

$$B = \{x_1, x_2, \ldots, x_k\} \tag{1}$$

and then $|A \circ B| = |A||B| = |G|$. Thus $\nu(A) = |B| = |G|/|A|$. Conversely, if $A = \{x_1, x_2, \ldots, x_k\}$ with elements in different cosets of a subgroup B of order $|G|/k$, B is an A-packing set.

The case that G is the multiplicative group $\mathbb{F}_p^*$ of the finite field $\mathbb{F}_p$ of p elements is particularly interesting in view of applications. More precisely, if p is prime and $A = \{1, 2, \ldots, \lambda\}$ for some positive integer λ, the authors in [9, 10, 11] used an A-packing set B to construct codes that correct single limited-magnitude errors. For more details see also [14, Section 6.2.2]. We denote

$$\nu(\lambda) = \nu(\{1, 2, \ldots, \lambda\}).$$

Ruzsa's Covering Lemma, see [20, Lemma 2.14] or [16], guarantees for any $A \subseteq G$ the existence of $B \subseteq G$ with $|A \circ B| = |A||B|$ and $G \subseteq A \circ A^{-1} \circ B$ and we get immediately

$$\nu(A) \geq \left\lceil \frac{|G|}{|A \circ A^{-1}|} \right\rceil \tag{2}$$

and, since $|A \circ A^{-1}| \leq |A|^2$,

$$\nu(A) \geq \left\lceil \frac{|G|}{|A|^2} \right\rceil. \tag{3}$$

For the convenience of the reader we will give a very short proof of (2) in Section 2. Equation (2) and its short proof have already known before by Buratti [4, Proposition 2.4].

In the above result, $A \circ A^{-1}$ denotes the set $\{a \circ b^{-1} : a, b \in A\}$, which we call the *ratio set of* A. Note that the bound (2) is tight, up to multiplicative constants[1], in the case when the ratio set satisfies the bound $|A \circ A^{-1}| \ll |A|$. This generalizes the result given by the simple construction (1) when A is a multiplicative subgroup to the broader class of sets A with small ratio set.

In fact, the weaker bound (3) is also optimal up to multiplicative constants in general, as the construction described in Section 2 shows. This construction can be modified to see that essentially any integer value $\nu(A)$ in the interval $[|G|/|A|^2, |G|/|A|]$ can be attained.

Section 3 deals with the special case when $G = \mathbb{F}_p^*$ with a prime p and $A = \{1, 2, \ldots, \lambda\}$. In this case we use the standard notation AB for the product set, rather than $A \circ B$ as above. Since $|AA^{-1}| \gg \min\{\lambda^2, p\}$, (2) is only of limited power in this case. However, we give a simple construction which proves that[2]

$$\nu(\lambda) \gg \frac{p}{\lambda \log p}$$

under the condition that $\lambda \leq 0.9p^{1/2}$.

Section 4 contains a result on the group of symmetries $\mathrm{Sym}(B) = \{x \in G : x \circ B = B\}$ of any A-packing set B of maximal size.

Finally in Section 5, we briefly discuss the related problem of finding a small A-*covering set* B, that is, a set $B \subseteq G$ such that $A \circ B = G$.

2. Proof of (2) and Proof of the Optimality of (3)

Proof of (2). Let $B \subseteq G$ be any set with $\nu(A) = |B|$. Then, by the maximality of B, for each $x \in G$ we have $(A \circ x) \cap (A \circ B) \neq \emptyset$, that is, $G \subseteq A^{-1} \circ A \circ B$ and hence $|G| \leq |A^{-1} \circ A \circ B| \leq |A \circ A^{-1}||B|$. Thus $|B| \geq |G|/|A \circ A^{-1}|$. □

The following construction shows that (3) is (up to a multiplicative constant) optimal.

Let $H = \{g, g^2, \ldots, g^k\} \subseteq G$ be any cyclic subgroup of G with $|H| = k \geq 2$. Let $d = \lceil \sqrt{k} \rceil \geq 2$ and define

$$A_1 = \{g, g^2, \ldots, g^d\}, \quad A_2 = \{g^d, g^{2d}, \ldots, g^{(d-1)d}, g^{d^2}\}.$$

Define $A = A_1 \cup A_2$. Note that $|A| < 2d$ and that $A \circ A^{-1} = H$.

Now suppose that $|A \circ B| = |A||B|$ for some $B \subseteq G$. This is true if and only if there are no non-trivial solutions to the equation

$$a_1 \circ b_1 = a_2 \circ b_2, \quad (a_1, a_2, b_1, b_2) \in A \times A \times B \times B,$$

[1]Here and throughout the paper, the notation $X \ll Y$ and $Y \gg X$ indicates that there exists an absolute constant $c > 0$ such that $X \leq cY$. If both $X \ll Y$ and $Y \ll X$, we write $X \approx Y$.

[2]We denote by log the natural logarithm.

which happens if and only if

$$(A \circ A^{-1}) \cap (B \circ B^{-1}) = \{1\}.$$

We want to show that B cannot be too large. Since $A \circ A^{-1} = H$, it must be the case that $(B \circ B^{-1}) \cap H = \{1\}$. But then B cannot contain more than one element from each coset of H. Indeed, if $b_1, b_2 \in B$ with $b_1 = x \circ h_1$ and $b_2 = x \circ h_2$ and with $h_1, h_2 \in H$ distinct, it follows that

$$b_1 \circ b_2^{-1} = h_1 \circ h_2^{-1} \in H \setminus \{1\} = A \circ A^{-1} \setminus \{1\}.$$

Therefore

$$|B| \leq \frac{|G|}{k} < \frac{|G|}{(d-1)^2} \leq \frac{16|G|}{|A|^2}.$$

This shows that $\nu(A) \ll |G|/|A|^2$. Furthermore, one can modify this construction by adding more elements from H to the set A in order to obtain, for any $0 \leq \alpha \leq 1$, a set A' with $|A' \circ A'^{-1}| \approx |A'|^{1+\alpha}$ and with $\nu(A') \ll |G|/|A' \circ A'^{-1}|$. This gives a broader class of sets for which the bound (2) is tight up to multiplicative constants.

3. The Case When $G = \mathbb{F}_p^*$ and $A = \{1, 2, \ldots, \lambda\}$

In this Section, we consider the case of the multiplicative group $\mathbb{F}_p^*$ of a finite prime field and fix A to be the interval $A = \{1, 2, \ldots, \lambda\} \subseteq \mathbb{F}_p^*$. Recalling the notation from the introduction, we seek lower bounds for $\nu(\lambda)$. Inequality (2) does not immediately give a strong result because of the following proposition.

Proposition 1. *For $A = \{1, 2, \ldots, \lambda\} \subseteq \mathbb{F}_p^*$ we have $|AA^{-1}| \gg \min\{\lambda^2, p\}$.*

Proof. For the set $A_{\mathbb{Z}} = \{1, 2, \ldots, \lambda\}$ of integers we have

$$A_{\mathbb{Z}} A_{\mathbb{Z}}^{-1} = \left\{ ab^{-1} : a, b \in A_{\mathbb{Z}}, \gcd(a, b) = 1 \right\}$$

and thus

$$|A_{\mathbb{Z}} A_{\mathbb{Z}}^{-1}| = \varphi(1) + 2(\varphi(2) + \varphi(3) + \ldots + \varphi(\lambda)) = \frac{6}{\pi^2}\lambda^2 + O(\lambda \log \lambda)$$

by [8, Theorem 330], where φ is Euler's totient function. If $\lambda < p^{1/2}$ and $1 \leq a_1, b_1, a_2, b_2 \leq \lambda$, then the congruence $a_1 b_1^{-1} \equiv a_2 b_2^{-1} \bmod p$ is equivalent to the integer equation $a_1/b_1 = a_2/b_2$. Hence, the number of different elements of AA^{-1} is the same as of $A_{\mathbb{Z}}/A_{\mathbb{Z}}$. If $\lambda \geq p^{1/2}$, A contains the subset $A' = \{0, 1, \ldots, \lfloor p^{1/2} \rfloor\}$ and thus $|AA^{-1}| \geq |A'A'^{-1}| \gg p$. □

Remark. For $\lambda \geq p^{1/2} \log^{1+\varepsilon} p$ we have $|AA^{-1}| = (1 + o(1))p$, see [6]. This result was later extended to all λ with $p^{1/2} = o(\lambda)$, see [7, Theorem 1.7]. Also in [6], it is mentioned that $AA^{-1} = \mathbb{F}_p^*$ if and only if $\lambda \geq \frac{p+1}{2}$.

With Proposition 1 in mind, (2) implies that $\nu(\lambda) \gg p/\lambda^2$. An explicit construction of such a set B was given in [14, Section 6.2.2].

In fact, we can provide a simple construction of a set B which is almost as large as possible with the property that $|AB| = |A||B|$. Identify $\mathbb{F}_p$ with the set of integers $\{1, 2, \ldots, p\}$ in the obvious way and define

$$B := \left\{ x \in \mathbb{F}_p : \lambda < x \leq \frac{p}{\lambda}, x \text{ is prime} \right\}.$$

This set has the property that $|AB| = |A||B|$. Indeed, suppose for a contradiction that we have a non-trivial solution to the equation

$$ab = a'b', \quad (a, a', b, b') \in A \times A \times B \times B.$$

Since A and B are both contained in sufficiently small intervals, there are no wrap-around issues, and so we must have a non-trivial solution to the equation

$$ab = a'b', \quad (a, a', b, b') \in A_{\mathbb{Z}} \times A_{\mathbb{Z}} \times B_{\mathbb{Z}} \times B_{\mathbb{Z}}, \tag{4}$$

where

$$A_{\mathbb{Z}} = \{1, 2, \ldots, \lambda\} \subseteq \mathbb{Z}, \quad B_{\mathbb{Z}} = \{x \in \mathbb{Z} : \lambda < x \leq \frac{p}{\lambda}, x \text{ is prime}\}.$$

However, unique prime factorisation of the integers implies that the only solutions to (4) are trivial.

Furthermore, by the Prime Number Theorem,

$$|B| \gg \frac{p/\lambda}{\log(p/\lambda)} - \frac{\lambda}{\log \lambda}.$$

In particular, if $\lambda \leq 0.9\sqrt{p}$, then we have $|B| \gg \frac{p}{\lambda \log p}$. We summarize this in the following statement:

Theorem 1. *Let $A = \{1, 2 \ldots, \lambda\} \subset \mathbb{F}_p^*$ with $\lambda \leq 0.9\sqrt{p}$. Then*

$$\nu(A) \gg \frac{p}{\lambda \log p}.$$

Remarks

1. Using explicit versions of the Prime Number Theorem, see [15],

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x} \quad \text{if } x \geq x_0$$

we can explicitly calculate the implied constant in Theorem 1.

2. The same approach applies to any residue class ring $\mathbb{Z}_n$ with composite n.

3. We may also take the larger packing set of *rough numbers*

$$B = \{x \in \mathbb{F}_p : \lambda < x \leq \frac{p}{\lambda}, x \text{ is not divisible by a prime} \leq \lambda\}.$$

We have[3]

$$|B| \sim \frac{p}{\lambda \log \lambda} \omega(u),$$

where ω is *Buchstab's function* and $u = \frac{\log(p/\lambda)}{\log \lambda}$, see [3] or [18, Paragraph IV.32]. In particular, if $p^{1/3} \leq \lambda \leq p^{1/2}$, we have $1 \leq u \leq 2$ and $\omega(u) = \frac{1}{u} = \frac{\log \lambda}{\log(p/\lambda)}$. However, for $u \to \infty$, the Buchstab function $\omega(u)$ converges to $e^{-\gamma}$, where γ is the *Euler-Mascheroni constant*, see [2]. In particular, if[4] $\lambda = e^{o(\log p)}$ is subexponential, we get $|B| \gg \frac{p}{\lambda \log \lambda}$ and so $\nu(\lambda) \gg \frac{p}{\lambda \log \lambda}$.

4. In some special cases one can get rid of the logarithmic factor. For example, take $\lambda = 2$ and $p \equiv \pm 3 \bmod 8$, that is, 2 is a quadratic non-residue modulo p. Then the quadratic residues modulo p are a packing set of maximal size. Similarly, if 1, 2 and 3 are in different cosets of the group B of cubic residues modulo p (take for example $p = 7$ or $p = 37$), then B is a packing set of maximal size. However, in general we do not know if the logarithmic factor can be completely removed.

4. Symmetries

Let $A \subseteq G$ be a set and B be an A-packing set. In this section we obtain a general result about symmetries of our set of translations B (this is in spirit of paper [17]). Surprisingly, the set of symmetries of this extremal set B does not grow after taking the ratio $B \circ B^{-1}$.

Consider an arbitrary set $T \subseteq G$. Denote by $\mathrm{Sym}(T)$ the group of symmetries of T that is

$$\mathrm{Sym}(T) = \{x \in G \ : \ x \circ T = T\}.$$

Notice that $1 \in \mathrm{Sym}(T)$, $\mathrm{Sym}(T) = \mathrm{Sym}^{-1}(T)$ and $\mathrm{Sym}(T) \subseteq T \circ T^{-1}$.

Proposition 2. *Let $A \subseteq G$ be a set and let B be an A-packing set of maximal size. Then*

$$\mathrm{Sym}(B) = \mathrm{Sym}(B \circ B^{-1}).$$

[3] We write $f(x) \sim g(x)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

[4] $f(x) = o(g(x))$ means $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Further

$$\big(\mathrm{Sym}(A\circ A^{-1})\big)\cap(A\circ A^{-1}) = (\mathrm{Sym}(A\circ A^{-1})\setminus\mathrm{Sym}(B))\bigsqcup\{1\}\,.$$[5]

Proof. The inclusion $\mathrm{Sym}(B)\subseteq\mathrm{Sym}(B\circ B^{-1})$ is trivial. Suppose that there is an element $x\in\mathrm{Sym}(B\circ B^{-1})$ but $x\notin\mathrm{Sym}(B)$. It follows that there is $b\in B$ such that $b\circ x\notin B$. As in the proof of (2) in Section 2, we get $B\circ A\circ A^{-1}\supseteq G$ and see that $b\circ x = b'\circ a_1\circ a_2^{-1}$ for some $a_1,a_2\in A$ and some $b'\in B$. Hence because $x\in\mathrm{Sym}(B\circ B^{-1})$, we get

$$\tilde{b}\circ(\tilde{b}')^{-1} = b\circ x\circ(b')^{-1} = a_1\circ a_2^{-1}$$

for some $\tilde{b},\tilde{b}'\in B$. But $|A\circ B| = |A||B|$ and thus $a_1=a_2$, $\tilde{b}=\tilde{b}'$. It gives us $b\circ x = b'\in B$ and this is a contradiction.

Taking $x\in\mathrm{Sym}(A\circ A^{-1})\setminus\mathrm{Sym}(B)$ and repeating the previous arguments, we obtain

$$b\circ(b')^{-1} = a_1\circ(x\circ a_2)^{-1} = \tilde{a}_1\circ(\tilde{a}_2)^{-1}$$

and hence, $b=b'$, $\tilde{a}_1=\tilde{a}_2$. Thus $x = a_1\circ a_2^{-1}\in A\circ A^{-1}$ and we get

$$\mathrm{Sym}(A\circ A^{-1})\setminus\mathrm{Sym}(B)\subseteq A\circ A^{-1}\,.$$

But $\mathrm{Sym}(B)\subseteq B\circ B^{-1}$ and $(B\circ B^{-1})\cap(A\circ A^{-1}) = \{1\}$ thus $\mathrm{Sym}(B)\cap(A\circ A^{-1}) = \{1\}$. This completes the proof. $\square$

If B is any A-packing set of maximal size, then the appearance of the set $\mathrm{Sym}(B)$ in our problem of computing $\nu(A)$ is natural in view of a trivial equality $\nu(A\circ\mathrm{Sym}(B)) = \nu(A) = |B|$.

5. Covering Sets

Given $A\subseteq G$, we say that $B\subseteq G$ is an A-*covering set* if $A\circ B = G$. The *covering number* of A, denoted $cov(A)$, is the size of the smallest A-covering set. There is a natural connection between covering and packing problems, and likewise with the problems of determining the values of $cov(A)$ and $\nu(A)$. In particular, it follows from Ruzsa's Covering Lemma that

$$cov(A\circ A^{-1})\le\nu(A).$$

The problem of determining $cov(A)$ in the case $G=\mathbb{F}_p^*$ was studied in [5, 12, 13], where $A=\{1,2,\ldots,\lambda\}$. A more general study of the problem can be found in

[5]We denote by $A\sqcup B$ the union of two disjoint sets.

[1]; see Section 3 therein for background on this problem in the finite setting. In particular, it is proved in [1, Corollary 3.2] that for any finite group G and $A \subset G$

$$\frac{|G|}{|A|} \leq cov(A) \leq \frac{|G|}{|A|}(\log |A| + 1). \tag{5}$$

By contrast with (5), we showed in Section 2 of this paper that $\nu(A)$ can essentially take any value in between $|G|/|A|^2$ and $|G|/|A|$. It is interesting to note that the size of $cov(A)$ is much more restricted than that of $\nu(A)$.

In the special case $G = \mathbb{F}_p^*$ and $A = \{1, 2, \ldots, \lambda\}$ we have the improvement $cov(A) < 2p/\lambda$ by [5, Theorem 2]. However, an interesting observation is that if we instead take A to be the middle third interval, then the log factor is needed and $cov(A) \approx \log |A|$. In particular, this gives us a constructive example (as opposed to random choice; see, say, [1]) of a set such that the upper bound in (5) is sharp.

Proposition 3. *For a prime $p > 3$ let*

$$A = \{x \in \mathbb{F}_p^* \ : \ x \in [p/3, 2p/3]\}.$$

Then we have

$$\frac{\log(p-1)}{\log(3)} \leq cov(A) < 3(\log(p) + 1).$$

Proof. Let $T = \{x \in \mathbb{F}_p^* \ : \ x \notin [p/3, 2p/3]\}$. For $\lambda \in \{1, \ldots, p-1\}$ let $\text{inv}(\lambda) \in \{1, \ldots, p-1\}$ be the unique integer with $\text{inv}(\lambda)\lambda \equiv 1 \bmod p$. By the simultaneous version of the Dirichlet Approximation Theorem, see [19], for any integer $1 \leq k < \log(p-1)/\log(3)$ and $\lambda_1, \ldots, \lambda_k \in \{1, \ldots, p-1\}$, there is an integer $1 \leq n < p$ and integers $a_1, \ldots, a_k$ such that

$$|\text{inv}(\lambda_i)n/p - a_i| \leq 1/(p-1)^{1/k} < 1/3$$

for $i = 1, \ldots, k$. In other words, for any $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_p^*$ with $1 \leq k < (p-1)/\log(3)$ there is $n \in \lambda_1 T \cap \cdots \cap \lambda_k T$. Letting $B = \{\lambda_1, \ldots, \lambda_k\}$, we see that $n \notin AB$ and hence $AB \neq \mathbb{F}_p^*$ for any B with $1 \leq |B| < \log(p-1)/\log(3)$. By the definition this means that $cov(A) \geq \log(p-1)/\log(3)$. The upper bound follows from (5). $\square$

Acknowledgements. The first and third authors are supported by the Austrian Science Fund FWF Projects F5509 and F5511-N26, respectively, which are part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications" as well as by FWF Project P 30405-N32. The second author was supported in part by the Program of the Presidium of the Russian Academy of Sciences 01 "Fundamental Mathematics and its Applications' under grant PRAS-18-01.

We are grateful to Antal Balog, Marco Buratti, Brandon Hanson, George Shakan and Igor Shparlinski for helpful conversations and insights.

References

[1] B. Bollobás, S. Janson, O. Riordan, On covering by translates of a set, *Random Structures Algorithms* **38** (2011), no. 1-2, 33–67.

[2] N. G. de Bruijn, On the number of uncancelled elements in the sieve of Eratosthenes, *Nederl. Akad. Wetensch. Proc.* **53** (1950), 803–812.

[3] A. A. Buchstab, Asymptotic estimates of a general number-theoretic function, (Russian.) *Mat. Sb. (N.S.)* **2 (44)** (1937), 1239–1246.

[4] M. Buratti, Packing the blocks of a regular structure, *Bull. Inst. Combin. Appl.* **21** (1997), 49–58.

[5] Z. Chen, I. E. Shparlinski and A. Winterhof, Covering sets for limited-magnitude errors, *IEEE Trans. Inform. Theory* **60** (2014), no. 9, 5315–5321.

[6] M. Z. Garaev, Character sums in short intervals and the multiplication table modulo a large prime, *Monatsh. Math.* **148** (2006), no. 2, 127–138.

[7] M. Z. Garaev and A. A. Karatsuba, The representation of residue classes by products of small integers, *Proc. Edinb. Math. Soc. (2)* **50** (2007), no. 2, 363–375.

[8] G. H. Hardy and E. M. Wright *An Introduction to the Theory of Numbers, Fifth Edition*, The Clarendon Press, Oxford University Press, New York, 1979.

[9] T. Kløve, B. Bose and N. Elarief, Systematic, single limited magnitude error correcting codes for flash memories, *IEEE Trans. Inform. Theory* **57** (2011), no. 7, 4477–4487.

[10] T. Kløve, J. Luo, I. Naydenova and S. Yari, Some codes correcting asymmetric errors of limited magnitude, *IEEE Trans. Inform. Theory* **57** (2011), no. 11, 7459–7472.

[11] T. Kløve, J. Luo and S. Yari, Codes correcting single errors of limited magnitude, *IEEE Trans. Inform. Theory* **58** (2012), no. 4, 2206–2219.

[12] T. Kløve and M. Schwartz, Linear covering codes and error-correcting codes for limited-magnitude errors, *Des. Codes Cryptogr.* **73** (2014), no. 2, 329–354.

[13] T. Kløve and M. Schwartz, Erratum to: Linear covering codes and error-correcting codes for limited-magnitude errors, *Des. Codes Cryptogr.* **73** (2014), no. 3, 1029.

[14] H. Niederreiter and A. Winterhof, *Applied Number Theory*, Springer, Cham, 2015.

[15] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[16] I. Z. Ruzsa, An analog of Freiman's theorem in groups, *Structure theory of set addition. Astérisque* **258** (1999), xv, 323–326.

[17] A. Samorodnitsky, I. Shkredov, and S. Yekhanin, Kolmogorov width of discrete linear spaces: an approach to matrix rigidity, *Computational Complexity* **25.2** (2016), 309–348.

[18] J. Sándor, D. S. Mitrinović, and B. Crstici, *Handbook of Number Theory. I*, second printing of the 1996 original, Springer, Dordrecht, 2006.

[19] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics, 785. Springer, Berlin, 1980.

[20] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006.