CODES CORRECTING RESTRICTED ERRORS

IGOR E. SHPARLINSKI AND ARNE WINTERHOF

Abstract. We study the largest possible length B of $(B-1)$-dimensional linear codes over $\mathbb{F}_q$ which can correct up to t errors taken from a restricted set $\mathcal{A} \subseteq \mathbb{F}_q^*$. Such codes can be applied to multilevel flash memories.

Moreover, in the case that $q = p$ is a prime and the errors are limited by a constant we show that often the primitive ℓth roots of unity, where ℓ is a prime divisor of $p-1$, define good such codes.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, $\mathcal{A}$ be a nonempty subset of $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ and t be a positive integer. We call a subset $\mathcal{B} \neq \emptyset$ of $\mathbb{F}_q^*$ of size $B = \#\mathcal{B}$ a $(t, \mathcal{A}, q)$-*packing set* if for any $x \in \mathbb{F}_q$ there is at most one solution

$$\mathbf{a} = (a_b)_{b\in\mathcal{B}} \in (\mathcal{A} \cup \{0\})^B$$

to the equation in $\mathbb{F}_q$

$$\sum_{b\in\mathcal{B}} a_b b = x$$

with Hamming-weight $w(\mathbf{a}) \leq t$, that is, $\mathbf{a}$ has at most t nonzero coordinates.

We can use the elements of $\mathcal{B}$ to define a $(B-1)$-dimensional linear code $\mathcal{C}$ of length B with the one line parity check matrix $H = (b)_{b\in\mathcal{B}}$:

$$\mathcal{C} = \left\{ (c_b)_{b\in\mathcal{B}} \in \mathbb{F}_q^B : \sum_{b\in\mathcal{B}} c_b b = 0 \right\}.$$

Using nearest neighbor decoding without further knowledge about the errors such a code of minimum weight at most 2 (by the Singleton bound) cannot correct any error, see for example [5, 16–18]. However, if we assume that all occurring errors a are elements of $\mathcal{A}$, we can correct up to t errors. More precisely, the syndromes

$$S_{\mathcal{B}}(\mathbf{a}) = \sum_{b\in\mathcal{B}} a_b b$$

2010 *Mathematics Subject Classification.* 68P30, 94B05, 94B65.

Key words and phrases. Restricted errors, packing sets.

of any error $\mathbf{a} = (a_b)_{b\in\mathcal{B}} \in (\mathcal{A}\cup\{0\})^B$ of Hamming weight at most t are all distinct and we can determine the unique error $\mathbf{a}$ from a syndrome table since $S_\mathcal{B}(\mathbf{c}+\mathbf{a}) = S_\mathcal{B}(\mathbf{a})$ for every code word $\mathbf{c} \in \mathcal{C}$ uniquely determines $\mathbf{a}$. Note that the information rate $(B-1)/B$ of these codes improves with the size B of $\mathcal{B}$ and we are interested in $(t,\mathcal{A},q)$-packing sets of large size.

A particularly interesting case is

$$\mathcal{A} = \{1,2,\ldots,\lambda\} \quad \text{and} \quad q = p \text{ is a prime,} \tag{1.1}$$

that is, we can correct all errors of limited magnitude λ, where λ is a positive integer. Such codes have been first proposed in [2] which in turn is based on [20]. They are used for multilevel flash memories, see [8, 15, 21].

In Section 2 we present an upper bound on the size of any $(t,\mathcal{A},q)$-packing set $\mathcal{B}$ with any nonempty set $\mathcal{A} \subseteq \mathbb{F}_q^*$, which is a simple generalization of the upper bound of [15] for the special case (1.1). We also provide examples of sets $\mathcal{A}$ for which this bound is tight.

In Section 3 we prove a lower bound on the size of any *maximal* $(t,\mathcal{A},q)$-packing set $\mathcal{B}$, that is, for all $u \in \mathbb{F}_q^* \setminus \mathcal{B}$ the set $\mathcal{B}\cup\{u\}$ is not a $(t,\mathcal{A},q)$-packing set. Note that this does not imply that there is no $(t,\mathcal{A},q)$-packing set of larger size than B (but such larger sets cannot contain $\mathcal{B}$).

In Section 4 we consider the case (1.1) again and give a probabilistic construction for a dense sequence of reasonably large $(t,\mathcal{A},q)$-packing sets. This construction is based on some properties of cyclotomic polynomials and resultants.

Unfortunately there is no efficient decoding procedure for the codes based on packing sets. In the case of the sets (1.1) it may be possible to employ some geometry of numbers algorithms, for example for the shortest vector problem (in the L_∞-norm). However no precise results or algorithms seem to be known.

One can also consider generalisations with several sets $\mathcal{B}_1,\ldots,\mathcal{B}_k \subseteq \mathbb{F}_q$ of the same cardinality B, for which the vectors of syndromes

$$\left(S_{\mathcal{B}_1}(\mathbf{a}),\ldots,S_{\mathcal{B}_1}(\mathbf{a})\right), \qquad \mathbf{a} \in (\mathcal{A}\cup\{0\})^B,$$

are pairwise distinct. The counting arguments of Sections 2 and 3 extend to this case without any difficulties, however we do not see how to generalise the construction of Section 4.

2. An upper bound

Now we present an upper bound on the size of any $(t, \mathcal{A}, q)$-packing set which can be essentially found in [15]. We include its proof for the convenience of the reader.

Theorem 2.1. *Let $\mathcal{A}$ be a subset of $\mathbb{F}_q^*$ of cardinality $A \geq 1$ and let $\mathcal{B}$ be any $(t, \mathcal{A}, q)$-packing set of cardinality B. Then we have*

$$\sum_{j=0}^{t} \binom{B}{j} A^j \leq q.$$

Proof. Note that the number of possible errors $\mathbf{a} \in (\mathcal{A} \cup \{0\})^B$ of Hamming weight at most t is

$$M = \sum_{j=0}^{t} \binom{B}{j} A^j, \tag{2.1}$$

which equals the number

$$N = \# \left\{ S_{\mathcal{B}}(\mathbf{a}) \ : \ \mathbf{a} \in (\mathcal{A} \cup \{0\})^B \right\}$$

of corresponding syndromes $S_{\mathcal{B}}(\mathbf{a})$, which are pairwise distinct since $\mathcal{B}$ is a $(t, \mathcal{A}, q)$-packing set. Using the trivial bound $M = N \leq q$ we derive the desired bound. □

Remark 2.2. It is easy to see that

$$\sum_{j=0}^{t} \binom{B}{j} A^j \geq \binom{B}{t} A^t > \left(\frac{B-t}{t} \right)^t A^t.$$

Hence, Theorem 2.1 implies the bound

$$B < t \left(\frac{q^{1/t}}{A} + 1 \right). \tag{2.2}$$

Example 2.3. Take $\mathcal{A} = \mathbb{F}_p^*$, $q = p^B$ and choose $\mathcal{B}$ to be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then each element $x \in \mathbb{F}_q$ has a unique representation

$$x = \sum_{b \in \mathcal{B}} a_b b, \qquad a_b \in \mathcal{A} \cup \{0\}.$$

The number of such elements with at most t nonzero coefficients a_b, where $1 \leq t \leq B$, is given by M as in (2.1). Thus, since $\mathcal{B}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, for $t = B$ we have

$$\sum_{j=0}^{t} \binom{B}{j} A^j = \sum_{j=0}^{B} \binom{B}{j} A^j = (A+1)^B = q$$

and the bound of Theorem 2.1 is attained.

Example 2.4. Take $q = p$ a prime and $\mathcal{A} = \{1, 2, \dots, \lambda\}$. Set

$$L = \left\lfloor \frac{\log p}{\log(\lambda + 1)} \right\rfloor.$$

Then the set

$$\mathcal{B} = \{(\lambda + 1)^i : i = 0, \dots, L - 1\}$$

is a $(t, \mathcal{A}, p)$-packing set for any t with $2 \le t \le L$ since the $(\lambda + 1)$-adic representation of any integer is unique and the largest exponent i is chosen such that there is no modulo p reduction. For $t = L$ the bound (2.2) is attained up to a multiplicative constant. This is essentially mentioned in [15].

3. A lower bound

In this section we prove a lower bound on the size of any maximal $(t, \mathcal{A}, q)$-packing set.

Theorem 3.1. *Let $\mathcal{A}$ be a subset of $\mathbb{F}_q^*$ of size $A \ge 1$ and $\mathcal{B}$ be any maximal $(t, \mathcal{A}, q)$-packing set of size B. Then we have*

$$\sum_{h=0}^{t} \binom{B+1}{h} A^h \sum_{k=1}^{t} \binom{B}{k-1} A^k + B + 1 \ge q.$$

Proof. Assume $\mathcal{B}$ is a maximal $(t, \mathcal{A}, p)$-packing set and $u \notin \mathcal{B}$. Then for any $u \in \mathbb{F}_q^* \setminus \mathcal{B}$ the set $\mathcal{B} \cup \{u\}$ is not a $(t, \mathcal{A}, p)$-packing set and thus we have

$$\sum_{b \in \mathcal{B}} a_{1,b} b + a_{1,u} u = \sum_{b \in \mathcal{B}} a_{2,b} b + a_{2,u} u$$

for some

$$\mathbf{a}_\nu = (a_{\nu,b})_{b \in \mathcal{B} \cup \{u\}} \in (\mathcal{A} \cup \{0\})^{B+1}, \qquad \nu = 1, 2,$$

of Hamming weight at most t.

In particular, by the definition of a $(t, \mathcal{A}, q)$-packing set, we have $a_{1,u} \ne a_{2,u}$ and may assume $a_{2,u} \ne 0$. Therefore

$$u = (a_{1,u} - a_{2,u})^{-1} \sum_{b \in \mathcal{B}} (a_{1,b} - a_{2,b}) b.$$

We fix some h and k with $0 \le h \le t$ and $1 \le k \le t$. Further we assume

$$w(\mathbf{a}_1) = h \qquad \text{and} \qquad w(\mathbf{a}_2) = k.$$

There are

$$\binom{B+1}{h} A^h \qquad \text{and} \qquad \binom{B}{k-1} A^k$$

choices for $\mathbf{a}_1$ and $\mathbf{a}_2$, respectively. Hence the number $q-B-1$ of $u \in \mathbb{F}_q^* \setminus \mathcal{B}$ is bounded by

$$q-B-1 \le \sum_{h=0}^{t} \binom{B+1}{h} A^h \sum_{k=1}^{t} \binom{B}{k-1} A^k$$

and the result follows. □

Remark 3.2. For $t=1$ we get the more precise bound

$$B \ge \frac{q-1}{\#(\mathcal{A}/\mathcal{A})} \ge \frac{q-1}{A^2}, \tag{3.1}$$

where $\mathcal{A}/\mathcal{A} = \{ab^{-1} : a, b \in \mathcal{A}\}$ denotes the ratio set of $\mathcal{A}$, see [7, Proposition 2.4] or [19]. Furthermore, in [19], an example is given which attains this lower bound up to a multiplicative constant. We recall this construction for the convenience of the reader: Let $g \in \mathbb{F}_q^*$ be an element of order $k \ge 2$, put $d = \left\lceil \sqrt{k} \right\rceil \ge 2$ and choose

$$\mathcal{A} = \left\{ g, g^2, \ldots, g^d, g^{2d}, \ldots, g^{(d-1)d}, g^{d^2} \right\}.$$

Note that $\#\mathcal{A} \le 2d-1$ and $\mathcal{A}/\mathcal{A}$ is the subgroup of $\mathbb{F}_q^*$ of order k generated by g. Now suppose that $\mathcal{B}$ is any $(1, \mathcal{A}, q)$-packing set, that is,

$$\mathcal{A}/\mathcal{A} \cap \mathcal{B}/\mathcal{B} = \{1\}.$$

Then $\mathcal{B}$ cannot contain more than one element from each coset of $\mathcal{A}/\mathcal{A}$ and thus

$$B \le (q-1)/k = O\left(q/A^2\right).$$

Corollary 3.3. *Let $\mathcal{A}$ be a subset of $\mathbb{F}_q^*$ of size A and $\mathcal{B}$ be any maximal $(t, \mathcal{A}, q)$-packing set of size B. Then we have*

$$B > \frac{(q/(5A))^{1/(2t-1)}}{A} - 1.$$

Proof. By (3.1) we may assume that $t \ge 2$ and since otherwise the result is trivial we may assume $q \ge 11$ and thus by Theorem 3.1 we have $AB \ge 2$. Now, from Theorem 3.1 and the elementary inequalities

$$\begin{aligned}\sum_{h=0}^{t} \binom{B+1}{h} A^h &< \sum_{h=0}^{t} (A(B+1))^h \\ &= \frac{(A(B+1))^{t+1}-1}{A(B+1)-1} \le 2\left(A(B+1)\right)^t,\end{aligned}$$

$$\sum_{k=1}^{t} \binom{B}{k-1} A^k < \frac{1}{B} \sum_{k=1}^{t} (AB)^k = A \frac{(AB)^t - 1}{AB-1} \le 2A^t B^{t-1},$$

we derive $q-B-1 < 4A^{2t}(B+1)^{2t-1}$ and the desired bound follows. $\square$

Remark 3.4. Note that if, for instance, $A < (q/6)^{1/(2t)}$, then the first term in the lower bound of Corollary 3.3 dominates and it becomes of order of magnitude $q^{1/(2t-1)}A^{-2t/(2t-1)}$.

4. A Probabilistic Construction

Now we consider the special case (1.1) and present a probabilistic construction, which for every λ, t and a sufficiently large positive Q, produces a prime $p \in [Q, 2Q]$ and a $(t, \mathcal{A}, p)$-packing set $\mathcal{B}$ of large cardinality.

We describe our construction first.

Algorithm 4.1. *Given arbitrary positive integers λ and sufficiently large positive integers $K < Q/2$:*

Step 1. *Choose a random integer $k \in [K+1, K+K/\log K]$ and test k for primality. Repeat this step until a prime $\ell = k$ is found.*

Step 2. *Choose a random factored integer $m \in [M, 2M]$, where $M = (Q-1)/\ell$, and test $m\ell+1$ for primality. Repeat this step until a prime $p = m\ell+1$ is found.*

Step 3. *Choose a random element $a \in \mathbb{F}_p^*$ and using the knowledge of the factorisation of $p-1$ test it for being a primitive root of $\mathbb{F}_p^*$. Repeat this step until a primitive root $g \in \mathbb{F}_p^*$ is found.*

Step 4. *Return $b_0 = g^{(p-1)/\ell}$.*

Theorem 4.2. *Assuming that*

$$\lambda^{2t}(4K)^{2t+2}\log(t\lambda) = o(Q), \tag{4.1}$$

Algorithm 4.1 runs in expected polynomial in $\log Q$ time and with probability $1+o(1)$ returns $b_0 \in \mathbb{F}_p^*$ for which the set $\mathcal{B}_0 = \{b_0, b_0^2, \ldots, b_0^{\ell-1}\} \subseteq \mathbb{F}_p^*$ with $\ell = (1+o(1))K$ is a $(t, \mathcal{A}, p)$-packing set, where $\mathcal{A}$ is as in (1.1).

Proof. We first analyse the complexity of Algorithm 4.1 and then show that it is correct with an overwhelming probability.

Running time. It follows easily from the classical prime number theorem that intervals of the form $[K+1, K+K/\log K]$ contain a set $\mathcal{L}$ of

$$L = (1+o(1))\frac{K}{(\log K)^2} \tag{4.2}$$

primes, see [13, Theorem 10.5] and the follow-up discussion, which is sufficient for our purpose. In fact the currently strongest result of Baker, Harman and Pintz [4] allows to use $k \in [K+1, K+K^{\alpha}]$ for any fixed $\alpha > 21/40 = 0.525$, but this does not affect our main result. Combining this with the deterministic polynomial time primality test of Agrawal, Kayal and Saxena [1] (or with any polynomial time probabilistic test, see [12]) we conclude that Step 1 returns a desired prime ℓ in polynomial time.

To generate factored integers in the interval $[M, 2M]$ uniformly at random, we use the polynomial time algorithm of Kalai [14] which simplified the previous algorithm of Bach [3]. After this we again apply one of the above primality tests to $m\ell + 1$. We now need to estimate the expected number of such choices before we find a prime

$$p = \ell m + 1.$$

Let, as usual, $\pi(x, k, a)$ denote the number of primes $p \le x$ in the arithmetic progression $p \equiv a \pmod{k}$.

We now recall that since $t \ge 1$ then by (4.1) we have $K = O(Q^{1/3})$. Thus by the celebrated Bombieri-Vinogradov theorem, see [13, Theorem 17.1], with the summation extended only over the primes from the set $\mathcal{L}$, we immediately derive the following bound

$$\pi(2Q, \ell, 1) - \pi(Q, \ell, 1) \ge \frac{Q}{2\ell \log Q} \tag{4.3}$$

for all but at most $O\left(L/\log Q\right)$ primes $\ell \in \mathcal{L}$.

Since the primes ℓ are generated uniformly at random we see that in expected polynomial time Step 2 outputs the desired prime p.

Since ℓ is prime and the prime number factorisation of m is known, one can test whether $a \in \mathbb{F}_p^*$ is a primitive root of $\mathbb{F}_p^*$ in deterministic polynomial time. Recall that the density of primitive roots in $\mathbb{F}_p^*$ is high enough, namely, it is

$$\frac{\varphi(p-1)}{p-1} \ge c\frac{1}{\log\log p}$$

for an absolute constant $c > 0$, which easily follows from Mertens' formula, see [13, Equation (2.16)]. We now immediately conclude that Step 3 outputs a primitive root of $\mathbb{F}_p^*$ in expected polynomial time.

The complexity analysis of Step 4 is trivial.

Correctness. Take $\mathcal{B}_0 = \{b_0, b_0^2, \ldots, b_0^{\ell-1}\} \subseteq \mathbb{F}_p^*$. If

$$\sum_{b \in \mathcal{B}_0} a_b b \ne 0 \tag{4.4}$$

for all $\mathbf{a} = (a_b)_{b \in \mathcal{B}_0} \in \{-\lambda, -\lambda+1, \ldots, \lambda\}^{\ell-1}$ with $1 \le w(\mathbf{a}) \le 2t$, then $\mathcal{B}_0$ is a $(t, \mathcal{A}, p)$-packing set.

Let $\Phi_\ell(X) \in \mathbb{Z}[X]$ be the ℓth cyclotomic polynomial which completely splits over $\mathbb{F}_p$, that is, $\mathcal{B}_0$ is exactly its set of zeros.

If (4.4) fails, then there is a nonzero polynomial with at most $2t$ nonzero coefficients $a_i \in \{-\lambda, \dots, \lambda\}$ of the form

$$f(X) = \sum_{i=0}^{\ell-2} a_i X^i \in \mathbb{F}_p[X] \tag{4.5}$$

of degree at most $\ell - 2$ which vanishes at some $b \in \mathcal{B}_0$. The resultant R_f of $f(X)$ and $\Phi_\ell(X)$ is

$$R_f = \prod_{\xi:\ \Phi_\ell(\xi)=0} f(\xi),$$

where the product is taken over all complex primitive ℓth roots of unity ξ, see, for example, [6, Theorem 1], and vanishes modulo p:

$$R_f \equiv 0 \pmod p. \tag{4.6}$$

Consider the set of

$$N = \sum_{i=1}^{2t} \binom{\ell-1}{i} (2\lambda)^i \le 2(2\ell\lambda)^{2t} \tag{4.7}$$

different polynomials of the form (4.5) with at most $2t$ nonzero coefficients $a_i \in \{-\lambda, \dots, \lambda\}$. Since $\Phi_\ell(X)$ is irreducible over $\mathbb{Q}$ and for any $f(X)$ of the form (4.5) we have $\deg(f) \le \ell - 2 < \deg(\Phi_\ell)$, the N resultants R_f do not vanish over $\mathbb{Q}$ and their size $|R_f|$ is bounded by

$$|R_f| = \prod_{\xi:\ \Phi_\ell(\xi)=0} |f(\xi)| \le (2t\lambda)^{\ell-1}.$$

So each R_f has at most

$$O\left(\log |R_f|\right) = O\left(\ell \log(t\lambda)\right) \tag{4.8}$$

prime divisors. Hence, from (4.7) and (4.8) we see that the set $\mathcal{S}$ of primes p that satisfy (4.6) for at least one of the resultants R_f is of cardinality

$$S = O\left(\lambda^{2t} (2\ell)^{2t+1} \log(t\lambda)\right). \tag{4.9}$$

On the other hand, we see from (4.2) and (4.3) that Algorithm 4.1 produces integers m uniformly at random from a set of cardinality

$$M + O(1) = Q/\ell + O(1). \tag{4.10}$$

Comparing (4.9) with (4.10) we see that under the condition (4.1) we have $S = o(M)$ which concludes the proof. $\square$

Remark 4.3. Note that a subgroup $\mathcal{B}$ of $\mathbb{F}_p^*$ of order ℓ is a $(1, \mathcal{A}, p)$-packing set whenever $\mathcal{A}$ contains at most one element from each coset of $\mathcal{B}$. For example, if $\ell = (p-1)/2$, that is, $\mathcal{B}$ is the subgroup of quadratic residues modulo p, then $\mathcal{B}$ is a $(1, \{1, 2\}, p)$-packing set whenever $p \equiv \pm 3 \bmod 8$, that is, whenever 2 is a quadratic nonresidue modulo p. Furthermore, for $t \geq 2$, recent advances towards the Waring problem in $\mathbb{F}_p$, see, for example, [9–11], imply rather severe restrictions on the order ℓ of a subgroup $\mathcal{B}$ of $\mathbb{F}_p^*$, for which $\mathcal{B}$ can be a $(t, \{1\}, p)$-packing set.

Acknowledgements

This work was initiated during a visit of the authors to the Paris Lodron University of Salzburg. The authors are grateful for its support.

During the preparation of this work the first author was supported by the ARC Grants DP170100786 and DP180100201, and the second author was supported by the Austrian Science Fund FWF Project P 30405-N32.

The authors like to thank the anonymous referees for their valuable suggestions.

References

[1] M. Agrawal, N. Kayal and N. Saxena, 'PRIMES is in P', *Ann. of Math.*, **160** (2004), 781–793.

[2] R. Ahlswede, H. Aydinia and L. Khachatrian, 'Unidirectional error control codes and related combinatorial problems', *Proc. Eighth Int. Workshop Algebr. Combin. Coding Theory (ACCT-8)*, St. Petersburg, Russia, 2002, 6–9.

[3] E. Bach, 'How to generate factored random numbers', *SIAM J. Comp.*, **17** (1988), 179–193.

[4] R. C. Baker, G. Harman and J. Pintz, 'The difference between consecutive primes. II', *Proc. Lond. Math. Soc.*, **83** (2001), 532–562.

[5] E. Berlekamp, *Algebraic coding theory*. Revised ed., World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2015.

[6] Y. Bistritz and A. Lifshitz, 'Bounds for resultants of univariate and bivariate polynomials', *Linear Algebra Appl.*, **432** (2010), 1995–2005.

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

[8] Y. Cassuto, M. Schwartz, V. Bohossian and J. Bruck, 'Codes for asymmetric limited-magnitude errors with application to multilevel flash memories', *IEEE Trans. Inform. Theory*, **56** (2010), 1582–1595.

[9] J. Cipra, T. Cochrane and C. G. Pinner, 'Heilbronn's Conjecture on Waring's number mod p', *J. Number Theory*, **125** (2007), 289–297.

[10] T. Cochrane, D. Hart, C. Pinner and C. Spencer, 'Waring's number for large subgroups of $\mathbb{Z}_p$', *Acta Arith.*, **163** (2014), 309–325.

[11] T. Cochrane and C. Pinner, 'Sum-product estimates applied to Waring's problem mod p', *Integers*, **8** (2008), A46, 1–18.

[12] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, Springer-Verlag, New York, 2005.

[13] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[14] A. T. Kalai, 'Generating random factored numbers, easily', *J. Crypto.*, **16** (2003), 287–289.

[15] T. Kløve, J. Luo, I. Naydenova and S. Yari, 'Some codes correcting asymmetric errors of limited magnitude', *IEEE Trans. Inform. Theory*, **57** (2011), 7459–7472.

[16] S. Ling and C. Xing, *Coding theory. A first course*, Cambridge Univ. Press, Cambridge, 2004.

[17] J. H. van Lint, *Introduction to coding theory*, 3rd edition. Graduate Texts in Mathematics, vol.86. Springer-Verlag, Berlin, 1999.

[18] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes, Vol. II*, North-Holland Math. Library, vol. 16. North-Holland Publishing Co., Amsterdam – New York – Oxford, 1977.

[19] O. Roche-Newton, I. D. Shkredov and A. Winterhof, 'Packing sets over finite abelian groups', *Integers*, **18**, A38, 1–9.

[20] R. R. Varshamov, 'A class of codes for asymmetric channels and a problem from the additive theory of numbers', *IEEE Trans. Inform. Theory*, **19** (1973), 92–95.

[21] S. Yari, T. Kløve and B. Bose, 'Some codes correcting unbalanced errors of limited magnitude for flash memories', *IEEE Trans. Inform. Theory*, **59** (2013), 7278–7287.

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au

Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Str. 69, Linz, Austria

E-mail address: arne.winterhof@oeaw.ac.at