

# A Family of Constacyclic Ternary Quasi-Perfect Codes with Covering Radius 3

Danyo Danev<sup>\*1</sup>, Stefan Dodunekov<sup>\*2</sup> and Diana Radkova<sup>\*3</sup>

<sup>1</sup> Department of Electrical Engineering, Linköping University, SE-581 83 Linköping, Sweden. E-mail: danyo@isy.liu.se

<sup>2</sup> Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 8 G. Bontchev Street, 1113 Sofia, Bulgaria. E-mail: stedo@moi.math.bas.bg

<sup>3</sup> Sofia University "St. Kl. Ohridski", Faculty of Mathematics and Informatics, Department of Algebra, 5 James Bourchier Blvd., 1164 Sofia, Bulgaria. E-mail: dradkova@fmi.uni-sofia.bg

**Abstract.** In this paper a family of constacyclic ternary quasi-perfect linear block codes is presented. This family extends the result presented in a previous work by the first two authors, where the existence of codes with the presented parameters was stated as an open question. The codes have a minimum distance 5 and covering radius 3.

## 1 Introduction

In the beginning we give a brief reminder of some definitions from the field of coding theory. The Galois field of  $q$  elements, where  $q$  is a prime power, is denoted by  $GF(q)$ . The linear space of all  $n$ -tuples of elements from  $GF(q)$  is denoted by  $H(n, q)$  and is known as the Hamming space. The elements of this space will be referred to as words or vectors. The Hamming space becomes a metric space if define the metric function  $d_H(\mathbf{x}, \mathbf{y})$ , which equals the number of positions where  $\mathbf{x}$  and  $\mathbf{y}$  differ. This is known as Hamming distance. To keep the notations concise we omit the subscript of the distance function. A sphere and ball of radius  $r$  around a vector  $\mathbf{x}$  is defined as the set of all vectors at Hamming distance exactly and at most  $r$  from  $\mathbf{x}$ , respectively. A  $q$ -ary error-correcting code, or just a code, is an arbitrary subset  $C$  of  $H(n, q)$ . The parameter  $n$  is called the length of the code. The addition and multiplication by scalar, which define  $H(n, q)$  as a vector space over the field  $GF(q)$ , are performed component-wise as in  $GF(q)$ . A linear subspace of  $H(n, q)$  is referred to as a linear code. The minimum distance for a code  $C$  is defined by

$$d(C) \triangleq \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

The notation  $(n, M, d)_q$  for a general code of length  $n$ , cardinality  $M$  and minimum distance  $d(C) = d$  is commonly used. In the case when the code is linear subspace of dimension  $k$  it is denoted by  $[n, k, d]_q$ .

---

\* This work has been partially supported by the CENIIT foundation and the Bulgarian NSF under contract MM 1405.

For the remainder of this section we present the notions of perfect and quasi-perfect codes and account for some known facts about them. The minimum distance of a code is closely connected to the error-correcting properties when the code is used for communication over additive-white-Gaussian-noise (AWGN) communication channels. It is known that up to

$$t(C) = \left\lfloor \frac{d(C) - 1}{2} \right\rfloor$$

errors, caused by the transmission over the channel, can be successfully corrected by the aid of decoding. This quantity is known as the packing radius of the code  $C$ . Apparently this coincides with the largest integer such that the spheres of this radius around the codewords are disjoint. On the other hand the least possible integer number such that the balls of this radius around the codewords cover the whole space  $H(n, q)$  is called the covering radius of the code. It can be expressed as

$$\rho(C) \triangleq \max_{\mathbf{x} \in H(n, q)} \min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}).$$

It is clear that for each code the packing radius should be at most the covering radius. Codes that achieve this equality, i.e.  $t(C) = \rho(C)$ , are called perfect. A complete classification of the parameters for which perfect codes over Galois fields exist have been completed in the early 1970's [13–15]. This classification shows that the possible sets of parameters  $(n, M, d)_q$  for a perfect code are

- $(n, q^n, 1)_q$  - the whole space  $H(n, q)$ , where  $n$  is a positive integer and  $q$  is a prime power;
- $(2l - 1, 2, 2l - 1)_2$  - the binary repetition codes, where  $l$  is a positive integer;
- $((q^s - 1)/(q - 1), q^{(q^s - 1)/(q - 1) - s - 1}, 3)_q$  - the Hamming codes, where  $s$  is a positive integer and  $q$  is a prime power;
- $(23, 2048, 7)_2$  - the binary Golay code;
- $(11, 729, 5)_3$  - the ternary Golay code.

In the case when the covering radius exceeds the packing radius by one, i.e.  $\rho(C) = t(C) + 1$ , the code  $C$  is called quasi-perfect. The corresponding classification task for the sets of possible parameters for quasi-perfect codes is much more complicated. Efforts towards solution have been done by many researchers in the past decades. Among those a survey of the known results for the binary case by Etzion and Mounits [8] is worth mentioning. Similarly to the case of perfect codes, it appears that the existence of quasi-perfect codes is limited to the ones with small covering radii. There is a great variety of such codes of covering radius up to 3. For greater covering radii only few non-trivial examples of binary quasi-perfect codes exist (see e.g. [2, Table 1]).

Non-binary quasi-perfect codes are known in rare cases. The known infinite families are due to Gashkov and Sidel'nikov [9] for the parameters  $[(3^s + 1)/2, (3^s + 1)/2 - 2s, 5]_3$ , Danev and Dodunekov [4] for  $[(3^s - 1)/2, (3^s - 1)/2 - 2s, 5]_3$ , where  $s$  is odd, Gevorkjan et. al. [10] for  $[(4^s - 1)/3, (4^s - 1)/3 - 2s, 5]_4$  and Dumer and Zinov'ev [7] for  $[(2^{2s+1} + 1)/3, (2^{2s+1} + 1)/3 - 2s - 1, 5]_4$ . The

quasi-perfectness, i.e. the fact that the covering radius is 3, of the latter two families has been shown by one of the authors in [5, 6].

In this paper we show that there exist ternary quasi-perfect codes with the parameters  $[(3^s - 1)/2, (3^s - 1)/2 - 2s, 5]_3$  for an arbitrary integer number  $s \geq 3$ . This extends the result in [4].

In Section 2 we present some basic facts about constacyclic codes and define the codes in the family. The minimum distance is determined as well. Section 3 is devoted to the proof of the fact that the covering radius is equal to 3. The paper is concluded in Section 4.

## 2 Presentation of the codes

Recall that a code over  $GF(q)$  is called constacyclic with respect to non-zero element  $0 \neq a \in GF(q)$  if every  $a$ -constacyclic shift of a codeword is also a codeword. Linear constacyclic codes can be regarded as invariant subspaces of  $H(n, q)$  with respect to a suitable linear operator. For an arbitrary non-zero element  $a$  of  $GF(q)$  let

$$\psi_a : \begin{cases} H(n, q) \rightarrow H(n, q) \\ (x_1, x_2, \dots, x_n) \mapsto (ax_n, x_1, \dots, x_{n-1}) \end{cases}$$

be the constacyclic linear mapping with respect to  $a$ . Then  $\psi_a \in \text{Hom}(H(n, q), H(n, q))$  and it has the following matrix

$$B_n(a) = B_n = \begin{pmatrix} 0 & 0 & 0 & \dots & a \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

with respect to the standard basis of  $H(n, q)$ . The characteristic polynomial of  $B_n$  is  $f_{B_n}(x) = (-1)^n(x^n - a)$ . We assume that  $n$  and  $q$  are relatively prime, i.e.  $(n, q) = 1$ . The polynomial  $f_{B_n}(x)$  has no multiple roots and splits into distinct irreducible monic factors  $f_{B_n}(x) = (-1)^n f_1(x) \dots f_t(x)$ . Let  $U_i = \text{Ker } f_i(\psi_a)$ ,  $i = 1, \dots, t$ . For the proof of the following theorem we refer to [12].

**Theorem 1.** *Let  $C$  be a linear constacyclic code of length  $n$  over  $GF(q)$ . Then the following facts hold:*

- 1)  $C$  is a constacyclic code with respect to  $a$  iff  $C$  is a  $\psi_a$ -invariant subspace of  $H(n, q)$ .
- 2)  $C = U_{i_1} \oplus \dots \oplus U_{i_s}$  for some minimal  $\psi_a$ -invariant subspaces  $U_{i_r}$  of  $H(n, q)$  and  $k = \dim_{GF(q)} C = k_{i_1} + \dots + k_{i_s}$ , where  $k_{i_r}$  is the dimension of  $U_{i_r}$ .
- 3)  $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \dots f_{i_s}(x) = h(x)$ .
- 4)  $\mathbf{c} \in C$  iff  $h(B_n)\mathbf{c} = \mathbf{0}$ .
- 5) The polynomial  $h(x)$  has the smallest degree with respect to property 4).

6) The matrix  $H$ , the rows of which constitute an arbitrary set of  $n - k$  linearly independent rows of  $h(B_n)$ , is a parity check matrix of  $C$ .

Let us define  $\mu$  as a primitive  $2n$ -th root of unity in an extension field of  $GF(3)$ , where  $n = \frac{3^s - 1}{2}$ . Then  $\mu$  is a primitive element of the field  $GF(3^s)$  and  $\mu$  is a zero of the polynomial  $x^n + 1$ . In order to classify the zeros of  $x^n + 1$  with respect to the various irreducible polynomial divisors of  $x^n + 1$ , we first determine the cyclotomic cosets  $M_i = \{i, 3i, 3^2i, \dots\}$  of 3 modulo  $2n$ , consisting of odd integers only. The irreducible polynomials connected to the cyclotomic cosets  $M_1$  and  $M_{-1}$  are

$$g_1(x) = \prod_{i \in M_1} (x - \mu^i) \text{ and } g_{-1}(x) = \prod_{i \in M_{-1}} (x - \mu^i),$$

respectively. Note that  $\deg g_1(x) = \deg g_{-1}(x) = s$ . For every positive integer  $s$  let us define the code  $C_s$  to be the  $(-1)$ -constacyclic ternary code of length  $n = (3^s - 1)/2$  determined by the polynomial  $g(x) = \frac{f_{B_n}(x)}{f_{\psi_{-1}|C}(x)} = g_1(x)g_{-1}(x)$ .

Obviously the dimension of  $C_s$  is

$$k = n - \deg g(x) = \frac{3^s - 1}{2} - 2s.$$

To determine the minimum distance of the codes  $C_s$  we use the BCH bound for the minimum distance of a constacyclic code [12].

**Proposition 1.** *The constacyclic codes  $C_s$  defined above have minimum distance  $d(C_s) \geq 5$ .*

*Proof.* Indeed, we have that  $\mu^{-3}, \mu^{-1}, \mu, \mu^3$  are zeros of  $g(x)$ . Since  $\mu$  is a primitive  $2n$ -th root of unity, it follows that  $\alpha = \mu^2$  is a primitive  $n$ -th root of unity. In terms of  $\alpha_j = \mu\alpha^j, 1 \leq j \leq n$ , these zeros can be written as  $\alpha_{n-2}, \alpha_{n-1}, \alpha_n, \alpha_1$ . Hence,  $g(x)$  has a string of 4 consecutive zeros which means that the minimum distance of  $C_s$  is at least 5.

We shall see at the end of the next section that the minimum distance  $d(C_s)$  is actually exactly 5.

### 3 The Covering Radius

In order to show that the covering radius of the codes defined above is always 3 we use the idea from the proof of [4, Theorem 1]. For an arbitrary vector  $\mathbf{r} = (r_0, r_1, \dots, r_{n-1})$  in  $H(n, 3)$  we identify  $\mathbf{r}$  with the polynomial

$$r(x) = \sum_{i=0}^{n-1} r_i x^i \in GF(3)[x].$$

We have that  $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$  is a codeword in  $C_s$  if and only if its associated polynomial  $c(x)$  is divisible by the generator polynomial  $g(x)$ , i.e. all roots of  $g(x)$  are also roots of  $c(x)$ . In our specific case we have that  $\mathbf{c} \in C_s$  iff  $c(\mu) = c(\mu^{-1}) = 0$ .

The covering radius of the code  $C_s$  is three if and only if for an arbitrary polynomial  $r(x)$  of degree at most  $n - 1$ , there exist polynomials  $c(x)$  and  $e(x)$ , corresponding to vectors  $\mathbf{c}$  and  $\mathbf{e}$  from  $H(n, 3)$ , such that  $r(x) = c(x) + e(x)$ ,  $c(x) \in C_s$  and  $e(x)$  has at most 3 non-zero coefficients. We define the syndromes

$$S_i(r) = r(\mu^i) \in GF(3^s),$$

for  $i \in \{\pm 1\}$ . Since  $c(x)$  is a codeword and  $\mu^{\pm 1}$  are roots of the generator polynomial  $g(x)$ , we define

$$S_i = S_i(r) = r(\mu^i) = e(\mu^i) = S_i(e) \in GF(3^s),$$

for  $i \in \{\pm 1\}$ . Since every vector  $\mathbf{r} \in H((3^s - 1)/2, 3)$  is associated with a pair of syndromes  $(S_1, S_{-1}) \in (GF(3^s))^2$ , it is sufficient to show that for an arbitrary pair of elements  $(a, b) \in (GF(3^s))^2$  there exists a polynomial  $e(x)$  with at most 3 non-zero coefficients from  $GF(3^s)$ , such that

$$(S_1, S_{-1}) = (S_1(e), S_{-1}(e)) = (a, b). \quad (1)$$

The main result of the current section is stated below.

**Theorem 2.** *The ternary  $(-1)$ -constacyclic codes  $C_s$  defined in Section 2 have covering radius  $\rho(C_s) = 3$  and minimum distance  $d(C_s) = 5$  for every integer  $s \geq 3$ .*

*Proof.* We start the proof with the observation that for every non-zero element  $\mu^i$  of  $GF(3^s)$  there exists a unique monomial  $m(x) \in GF(3)[x]$  of degree at most  $(3^s - 3)/2$ , such that  $m(\mu) = \mu^i$ . This is due to the fact that  $\mu^{(3^s - 1)/2} = -1$ .

Every polynomial  $e(x) \in GF(3)[x]$  with  $l$  non-zero coefficients can be written as a sum of monomials in the following way

$$e(x) = \sum_{i=1}^l e_i x^{p_i} = \sum_{i=1}^l e_i(x).$$

Since the statement  $m(x^{-1}) = (m(x))^{-1}$  is valid for any monomial in  $e(x) \in GF(3)[x]$  we have that

$$e(x^{-1}) = \sum_{i=1}^l (e_i(x))^{-1}.$$

The existence of a polynomial  $e(x)$  that satisfies equation (1) is equivalent to the existence of a solution to the system of equations

$$\begin{cases} z_1 + z_2 + \dots + z_l = a \\ z_1^{-1} + z_2^{-1} + \dots + z_l^{-1} = b \end{cases} \quad (2)$$

over the field  $GF(3^s)$ . In the light of Proposition 1 the system (2) has no more than one solution (up to permutation) for  $l = 1$  and  $l = 2$ . Obviously when  $l = 1$  we have a solution if and only if  $ab = 1$ .

For an arbitrarily fixed pair  $(a, b) \in (GF(3^s))^2$ , such that  $(a, b) \neq (0, 0)$  and  $ab \neq 1$  we provide a solution to the system (2) in the case  $l = 3$ . We define the functions

$$\theta(x) = a^2b^2x^2 - ax^4 - b \text{ and } \nu(x) = a^2b^2x^2 - a\mu x^4 - b\mu^{-1}$$

on the field  $GF(3^s)$ . If for some  $x \in GF(3^s)$  the element  $\theta(x)$  is a perfect square in this field then the triple

$$(z_1, z_2, z_3) = \left( \frac{1 + ax^2}{b + x^2}, \frac{x(1 - ab) + \sqrt{\theta(x)}}{x(b + x^2)}, \frac{x(1 - ab) - \sqrt{\theta(x)}}{x(b + x^2)} \right),$$

constitutes a solution to (2) with  $l = 3$  if  $x^2 \notin \{0, -a^{-1}, -b\}$ . On the other hand if  $\nu(x)$  is a perfect square in this field then the triple

$$(z_1, z_2, z_3) = \left( \frac{1 + \mu ax^2}{b + \mu x^2}, \frac{x(1 - ab) + \sqrt{\nu(x)}}{x(b + \mu x^2)}, \frac{x(1 - ab) - \sqrt{\nu(x)}}{x(b + \mu x^2)} \right),$$

is a solution to (2) with  $l = 3$  if  $x^2 \notin \{0, -(\mu a)^{-1}, -b\mu^{-1}\}$ .

We observe that if either  $a = 0$  or  $b = 0$  then the values of one of the functions  $\theta(x)$  or  $\nu(x)$  in all non-zero  $x \in GF(3^s)$  are all perfect squares. Thus we can assume that  $ab \neq 0$ . Let  $x_1$  and  $x_2$  be two non-zero elements of  $GF(3^s)$  for which  $x_1^2 + \mu x_2^2 = ab^2$  holds. It is straightforward to check that in this case we have

$$\theta(x_1) - \mu\nu(x_2) = 0. \quad (3)$$

Since  $\mu$  is not a square in  $GF(3^s)$  we have that either  $\theta(x_1)$  or  $\nu(x_2)$  is a square. To complete the proof we need to show that there are sufficiently many pairs  $(x_1, x_2)$  that satisfy the condition

$$x_1^2 + \mu x_2^2 = ab^2 \quad (4)$$

for an arbitrary choice of non-zero  $a$  and  $b$ . In fact, for any integer  $1 \leq k \leq 3^s/4$  and any non-zero element  $y \in GF(3^s)$ , there exist non-zero  $x_1$  and  $x_2$  in  $GF(3^s)$  such that  $x_1^2 + \mu x_2^2 = y$  and  $x_1/x_2 \in \{\mu^k, \mu^{1-k}\}$ . This is easily seen if we observe that

$$0 \neq (\mu^1)^2 + \mu(\mu^k)^2 = \mu((\mu^k)^2 + \mu(\mu^0)^2)$$

and

$$(\mu^{k+1})^2 + \mu(\mu^{0+1})^2 = \mu^2((\mu^k)^2 + \mu(\mu^0)^2).$$

We can now find at least  $\lfloor 3^s/4 \rfloor$  pairs  $(x_1, x_2)$  satisfying the desired condition (4) each with a different value of  $x_1/x_2$ . Two pairs  $(x_1, x_2)$  and  $(y_1, y_2)$  satisfying (4) for which  $x_1^2 = y_1^2$  must also fulfil  $x_2^2 = y_2^2$  and thus  $(x_1/x_2)^2 = (y_1/y_2)^2$ . Since  $-1 = \mu^{(3^s-1)/2}$  we can not have repeating values of  $x_1^2$  as well as  $x_2^2$  among

the constructed  $\lfloor 3^s/4 \rfloor$  pairs. The number of pairs that have “unsuitable” value of  $x_1^2$  or  $x_2^2$ , i.e. can not be used for a construction of a solution to (2), is at most 4. Since  $\lfloor 3^s/4 \rfloor > 4$  whenever  $s \geq 3$  we can always find a pair  $(x_1, x_2)$  satisfying (4) and thus a solution to (2). This completes the proof of the statement for the covering radius of the codes  $C_s$ .

It is well known that vectors with the same syndrome belong to the same coset defined by a code. Due to the fact that  $d(C_s) \geq 5$ , for fixed  $a$  and  $b$  such that  $ab \neq 1$ , it is not possible to have two different solutions of the system (2) with  $l = 2$ . We have shown that in the coset corresponding to the syndrome  $(a, b)$  for which  $ab \neq 1$ , there are at least  $\lfloor 3^s/4 \rfloor - 4$  vectors of Hamming weight at most 3. Since  $3(\lfloor 3^s/4 \rfloor - 4) - 1 > n = (3^s - 1)/2$  for all  $s \geq 4$ , we have two vectors of weight at most 3 in the coset which have a non-zero element in the same position. This means that we have a codeword in  $C_s$  of weight at most 5. The existence of a codeword of Hamming weight 5 in the case  $s = 3$  can be checked directly.

Theorem 2 establishes the fact that for odd  $s$  the codes  $C_s$  are quasi-perfect for any integer  $s \geq 3$ .

It can be mentioned that the codes  $C_s$  are reversible, i.e. a mirrored version of any codeword is also a codeword. Decoding procedure can be designed based on general decoding algorithms for reversible constacyclic codes. However, an algebraic decoding of the codes  $C_s$  similar to the one presented in [4, Section 4] can be defined based on the proof of Theorem 2. Here we omit the details.

## 4 Conclusions

We have presented a family of constacyclic ternary  $[(3^s - 1)/2, (3^s - 1)/2 - 2s, 5]_3$  codes previously unknown to be quasi-perfect. This family extends the set of parameters for which quasi-perfect codes exist and improves upon a previously published result in [4] by giving a positive answer to the open question stated there.

The results obtained in this paper raise some questions concerning the existence of quasi-perfect codes of certain types and parameters. Some of these questions are summarised below.

### Open questions

- 1) Are there any quasi-perfect codes over the finite field  $GF(q)$  for a prime power  $q \geq 5$ ?
- 2) Are there any quasi-perfect codes of minimum distance 5 over the finite field  $GF(q)$  for a prime power  $q \geq 5$ ?
- 3) Are there any quasi-perfect codes BCH codes over the finite field  $GF(q)$  for a prime power  $q \geq 5$ ?
- 4) Are there any quasi-perfect BCH codes of minimum distance at least 7?
- 5) Are there any quasi-perfect codes of minimum distance at least 9?
- 6) Is there an upper bound on the minimum distance of quasi-perfect codes?

We are aware that the stated questions are difficult to answer. However, we feel that answering them would be a good step towards better knowledge on the existence of quasi-perfect codes.

## References

1. Tsonka Baicheva, Stefan Dodunekov, and Ralf Koetter. On the performance of the ternary  $[13, 7, 5]$  quadratic-residue code. *IEEE Trans. Inform. Theory*, 48(2):562–564, 2002.
2. Tsonka Baicheva, Iliya Bouyukliev, Stefan Dodunekov, and Veerle Fack. Binary and Ternary Linear Quasi-Perfect Codes With Small Dimensions. *IEEE Trans. Inform. Theory*, 54(9):4335–4339, 2008.
3. R. E. Blahut. *The Theory and Practice of Error Control Codes*. Addison-Wesley, Reading, MA, USA, 1993.
4. Danyo Danev and Stefan Dodunekov. A family of ternary quasi-perfect BCH codes. *Des. Codes Cryptogr.*, 49(1-3):265–271, 2008.
5. S. M. Dodunekov. The optimal double-error correcting codes of Zetterberg and Dumer-Zinov'ev are quasiperfect. *C. R. Acad. Bulgare Sci.*, 38(9):1121–1123, 1985.
6. S. M. Dodunekov. Some quasiperfect double error correcting codes. *Problems Control Inform. Theory/Problemy Upravl. Teor. Inform.*, 15(5):367–375, 1986.
7. I. I. Dumer and V. A. Zinov'ev. Some new maximal codes over  $\text{GF}(4)$ . *Problemy Peredachi Informatsii*, 14(3):24–34.
8. T. Etzion and B. Mounits. Quasi-perfect codes with small distance. *IEEE Trans. Inform. Theory*, 51(11):3928–3946, 2005.
9. I. B. Gashkov and V. M. Sidel'nikov. Linear ternary quasiperfect codes that correct double errors. *Problemy Peredachi Informatsii*, 22(4):43–48, 1986.
10. D.N. Gevorkjan, A.M. Avetisjan, and G.A. Tigranjan. K voprosu o postroenii kodov s ispravleniem dvuh oshibok v metrike hemminga nad poljami galua. *Vichislitel'naja tehnika*, 3:19–21, 1975.
11. F. McWilliams and Neil J. Sloane. *The Theory of Error Correcting Codes*. Amsterdam: North-Holland, third edition, 1977.
12. D. Radkova and A.J. van Zanten. Constacyclic Codes as Invariant Subspaces. *Linear Algebra and its Applications*, 430:855–864, 2009.
13. Aimo Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, 24:88–96, 1973.
14. Aimo Tietäväinen. A short proof for the nonexistence of unknown perfect codes over  $\text{GF}(q)$ ,  $q > 2$ . *Ann. Acad. Sci. Fenn. Ser. A I*, (580):6, 1974.
15. V. A. Zinov'ev and V. K. Leont'ev. On non-existence of perfect codes over Galois fields. *Problems of Control and Information Theory/Problemy Upravljenija i Teorii Informacii*, 2(2):123–132, 1973.