Propelinear 1-Perfect Codes from Quadratic Functions

Denis S. Krotov and Vladimir N. Potapov

***Abstract*— Perfect codes obtained by the Vasil'ev–Schönheim construction from a linear base code and quadratic switching functions are transitive and, moreover, propelinear. This gives at least $\exp(cN^2)$ propelinear 1-perfect codes of length N over an arbitrary finite field, while an upper bound on the number of transitive codes is $\exp(C(N \ln N)^2)$.**

***Index Terms*— Perfect code, propelinear code, transitive code, automorphism group.**

I. Introduction

USUALLY, a group code is defined as a subgroup of the additive group of a finite vector space. There are alternative approaches [5]–[7], [9], [12], [13], [16] that allow to relate the codewords of a code with the elements of some group. Usually, the mapping from the group to the code is required to satisfy some metric properties, because the distance is what is very important for error-correcting codes. One of the approaches considers so-called propelinear codes, introduced in [16] for the binary space. The codewords of a propelinear code C are in one-to-one correspondence with a group G of isometries of the space that acts regularly on the code itself. In other words, given some fixed codeword $v \in C$ (say, the all-zero word), every other codeword can be uniquely written as $g(v)$, $g \in G$. Every propelinear code is transitive; that is, it is an orbit of a group of isometries of the space (for a transitive code in general, this group is not required to act regularly).

In the current paper, we will prove that the number of nonequivalent propelinear codes with the same parameters, namely, the parameters of 1-perfect codes over an arbitrary finite field, grows at least exponentially with respect to the square of the code length (Corollary 1). By the order of the logarithm, this number is comparable with the total number of propelinear codes (Theorem 2). In contrast, there is only one (up to equivalence) linear 1-perfect code for each admissible length, but the number of non-linear 1-perfect codes grows doubly-exponentially [17], [19].

For the case $q = 2$, an exponential lower bound (with respect to the square root of the code length, to be more accurate) on the number of transitive and the number of propelinear 1-perfect codes was firstly established in [15] and [2], respectively. Here, we will show how to improve the lower bound and generalize it to an arbitrary prime power q, using a rather simple construction. Some other constructions of transitive and propelinear perfect codes can be found in [1], [3], [8], and [18].

Section II contains definitions and auxiliary lemmas. In Section III, we formulate the main results of the paper. The main theorem is proven in Section IV. In Section V, we consider some remarks and examples concerning the structure of the group related to a propelinear code, survey the transitive (propelinear) Vasil'ev codes of length 15, and discuss a problem about functions that can result in transitive codes.

Manuscript received October 19, 2013; revised January 22, 2014; accepted January 25, 2014. Date of publication February 20, 2014; date of current version March 13, 2014. This work was supported in part by the RFBR under Project 13-01-00463, in part by the Ministry of Education and Science of Russian Federation under Project 8227, and in part by the Target Program of SB RAS for 2012-2014 Integration under Project 14. This paper was presented at the 2012 Mal'tsev Meeting.

The authors are with the Sobolev Institute of Mathematics, Novosibirsk 630090, Russia, and also with Novosibirsk State University, Novosibirsk 630090, Russia (e-mail: krotov@math.nsc.ru; vpotapov@math.nsc.ru).

Communicated by N. Kashyap, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2014.2303158

II. Preliminaries

Let F be a finite field of order q, where q is a power of prime; let F^n be the vector space of all words of length n over the alphabet F. An arbitrary subset of F^n is referred to as a code. A code is linear if it is a vector subspace of F^n. A code $C \subset F^n$ is called 1-perfect if for every word v from F^n there is exactly one c in C agreeing with v in at least $n-1$ positions. It is well known that 1-perfect codes exist if and only if $n = (q^k - 1)/(q-1)$ for some integer k, see e.g. [10].

A. Vasil'ev–Schönheim Construction

Let $H \subset F^n$, and let $f : H \to F$ be an arbitrary function. Define the set

$$C(H, f) = \Big\{((v_\alpha)_{\alpha \in F}, z) : v_\alpha \in F^n, \sum_{\alpha \in F} v_\alpha = c \in H, \quad z = \sum_{\alpha \in F} \alpha |v_\alpha| + f(c)\Big\}$$

where $(v_\alpha)_{\alpha \in F}$ is treated as the concatenation of the words v_α (which will be referred to as *blocks*) in some prefixed order, $|v_\alpha|$ is the sum of all n elements of v_α. If H is a 1-perfect code, then $C(H, f)$ is a 1-perfect code in F^{qn+1}, known as a Schönheim code [17] (in the case $q = 2$, as a Vasil'ev code [19]). Clearly, the set $C(H, f)$ essentially depends on the choice of the function f:

Lemma 1: For a fixed H, different functions f result in different $C(H, f)$.

Proof: The graph of the function f can be reconstructed from the set $C(H, f)$:

$$\{(x, f(x)) : x \in H\} = \Big\{\Big(\sum_{\alpha\in F} v_\alpha,\ z - \sum_{\alpha\in F} \alpha|v_\alpha|\Big) : ((v_\alpha)_{\alpha\in F}, z) \in C(H, f)\Big\}.$$

Hence, $C(H, f) = C(H, f')$ implies $f = f'$. ∎

B. Automorphisms, Equivalence, Transitivity and Propelinearity

The *Hamming graph* $G(F^n)$ is defined on the vertex set F^n; two words are connected by an edge if and only if they differ in exactly one position. It is known (see, e.g., [4, Theorem 9.2.1]) that every automorphism Π of $G(F^n)$ is composed from a coordinate permutation π and alphabet permutations ψ_i in each coordinate: $\Pi(x) = (\psi_1(x_{\pi^{-1}(1)}), \ldots, \psi_n(x_{\pi^{-1}(n)}))$. Two codes are said to be *equivalent* if there is an automorphism of $G(F^n)$ that maps one of the codes into the other. Note that the algebraic properties of the code, such as being a linear or affine subspace, are not invariant with respect to this combinatorial equivalence, in general. The *automorphism group* $\mathrm{Aut}(C)$ of a code C consists of all automorphisms of $G(F^n)$ that stabilize (fix set-wise) C. A code C containing the all-zero word $\bar{0}$ is *transitive* if for every codeword a there exists $\varphi_a \in \mathrm{Aut}(C)$ that sends $\bar{0}$ to a. If, additionally, the set $\{\varphi_a : a \in C\}$ is closed under composition (that is, for all a and b from C we have $\varphi_a\varphi_b = \varphi_c$, where $c = \varphi_a\varphi_b(\bar{0})$), then C is a *propelinear* code, see e.g. [2].

C. Quadratic Functions

Assume H is a subspace of F^n. A function $f : H \to F$ is called *quadratic* if it can be represented as a polynomial of degree at most 2.

We will use the following elementary property of the quadratic functions (actually, it is a characterizing property).

Lemma 2: Let H be a subspace of F^n. If $f : H \to F$ is a quadratic function, then for every $c \in H$ there exist $\beta_0^c, \beta_1^c, \ldots, \beta_n^c \in F$ such that

$$f(x + c) = f(x) + \beta_0^c + \beta_1^c x_1 + \ldots + \beta_n^c x_n \quad \text{for all } x = (x_1, \ldots, x_n) \in H. \tag{1}$$

Moreover, β_i^c, $i \in \{1, \ldots, n\}$, depends linearly on c:

$$\beta_i^{c+d} = \beta_i^c + \beta_i^d.$$

Proof: The difference of $(x_i + c_i)(x_j + c_j)$ and $x_i x_j$ has degree at most 1. Moreover, the coefficients at x_i and x_j in this difference depend linearly on c. Hence, the same is true for the difference of $P(x + c)$ and $P(x)$ for every polynomial P of degree at most 2. ∎

Lemma 3: Let H be an m-dimensional subspace of F^n. There are at least $q^{m^2/2}$ different quadratic functions from H to F.

Proof: Obviously, a linear transformation of the space does not affect to the property of a function to be quadratic. Hence, we can assume without loss of generality that H consists of the words of length n with zeroes in the last $n - m$ positions. Then, the number of different quadratic functions is the number of polynomials of degree at most 2 in the first m variables, i.e., $q^{m(m-1)/2+m+m+1}$ for $q > 2$ and $q^{m(m-1)/2+m+1}$ for $q = 2$ (when $x_i^2 \equiv x_i \pmod 2$). ∎

III. Main Result

A. Lower Bound

In the Section IV, we will prove the following theorem.

Theorem 1: If $H \subset F^n$ is a linear q-ary code and $f : H \to F$ is a quadratic function, $f(\bar{0}) = 0$, then $C(H, f)$ is a propelinear code of length $N = qn + 1$.

Corollary 1: The number of nonequivalent propelinear 1-perfect q-ary codes of length $N = (q^k - 1)/(q - 1)$ obtained by the Vasil'ev–Schönheim construction is at least $q^{\frac{N^2}{2q^2}+O(N\ln N)}$.

Proof: As follows from Theorem 1, Lemma 1, and Lemma 3, the number of different propelinear 1-perfect codes of type $C(H, f)$ is at least $q^{\frac{m^2}{2}}$, where $m = n - \log_q(nq - n + 1)$ and n is the length of H. Since $N = qn + 1$, we see that $q^{\frac{m^2}{2}} = q^{\frac{N^2}{2q^2}+O(N\ln N)}$. To evaluate the number of nonequivalent codes, we divide this number by the number $N!(q!)^N = q^{O(N\ln N)}$ of all automorphisms of F^N and find that this does not affect on the essential part of the formula. ∎

B. Upper Bound

To evaluate how far our lower bound on the number of transitive (propelinear) 1-perfect codes can be from the real value, we derive an upper bound:

Theorem 2: (a) The number of different transitive codes in F^N does not exceed $2^{(N\log_2 N)^2(1+o(1))}$. (b) The number of different propelinear codes in F^N does not exceed $q^{N^2\log_2 N(1+o(1))}$.

Proof: Since every subgroup of $\mathrm{Aut}(F^N)$ is generated by at most $\log_2|\mathrm{Aut}(F^N)|$ elements, the number of subgroups is less than $|\mathrm{Aut}(F^N)|^{\log_2|\mathrm{Aut}(F^N)|} = 2^{(N\log_2 N)^2(1+o(1))}$ (recall that $|\mathrm{Aut}(F^N)| = (q!)^N N! = N^{N(1+o(1))}$). Since every transitive code C containing $\bar{0}$ is uniquely determined by its automorphism group (indeed, C is the orbit of $\bar{0}$ under $\mathrm{Aut}(F^N)$), statement (a) follows.

The automorphisms assigned to the codewords of a propelinear code C form a group of order $|C| \le q^N$. It is generated by at most $\log_2 q^N = N\log_2 q$ elements; each of them can be chosen in less than $|\mathrm{Aut}(F^N)| = N^{N(1+o(1))}$ ways; (b) follows. ∎

IV. Proof of Theorem 1

Let $H \subset F^n$ be a linear code and let $f : H \to F$ be a quadratic function. The key point in the proof is the following simple statement.

Lemma 4: Let $f'(x) = f(x) + \beta x_j$ for some $j \in \{1, \ldots, n\}$, $\beta \in F$. Then $C(H, f') = \Pi_j^\beta C(H, f)$ where Π_j^β is the coordinate permutation that sends the j'th coordinate of

the block $v_{\alpha+\beta}$ to the j'th coordinate of the block v_α for all $\alpha \in F$ and fixes the other coordinates.

Proof: Let us consider the codeword $x = ((v_\alpha)_{\alpha\in F}, z)$ of $C(H, f)$. It satisfies $z = \sum_{\alpha\in F} \alpha|v_\alpha| + f(c)$. After the coordinate permutation Π_j^β, we obtain the word $y = \Pi_j^\beta x = ((u_\alpha)_{\alpha\in F}, z)$ where for all α the word u_α coincides with v_α in all positions except the jth, $u_{\alpha,j}$ which is equal to $v_{\alpha+\beta,j}$. Now we have

$$\begin{aligned} z &= \sum_{\alpha\in F} \alpha|v_\alpha| + f(c) \\ &= \sum_{\alpha\in F}\sum_{k\neq j} \alpha v_{\alpha,k} + \sum_{\alpha\in F} \alpha v_{\alpha,j} + f(c) \\ &= \sum_{\alpha\in F}\sum_{k\neq j} \alpha u_{\alpha,k} + \sum_{\alpha\in F} \alpha u_{\alpha-\beta,j} + f(c) \\ &= \sum_{\alpha\in F}\sum_{k\neq j} \alpha u_{\alpha,k} + \sum_{\alpha\in F} (\alpha+\beta) u_{\alpha,j} + f(c) \\ &= \sum_{\alpha\in F}\sum_{k=1}^{n} \alpha u_{\alpha,k} + \beta \sum_{\alpha\in F} u_{\alpha,j} + f(c) \\ &= \sum_{\alpha\in F} \alpha|u_\alpha| + f(c) + \beta c_j, \end{aligned}$$

(we used that $c = (c_1, \ldots, c_n) = \sum v_\alpha = \sum u_\alpha$) which proves that $\Pi_j^\beta(x) \in C(H, f')$. ∎

Now denoting $\Pi^c = \Pi_1^{\beta_1^c}\Pi_2^{\beta_2^c}\ldots\Pi_n^{\beta_n^c}$, where the coefficients β_j^c are from (1), we get the following fact, which immediately proves the transitivity of the code:

Lemma 5: For every codeword $w = ((w_\alpha)_{\alpha\in F}, z)$ of $C(H, f)$, the transform $\Phi_w(v) = w + \Pi^c(v)$, where $c = \sum_{\alpha\in F} w_\alpha$, is an automorphism of $C(H, f)$, which sends the all-zero word to w.

Proof: Consider $v = ((v_\alpha)_{\alpha\in F}, s)$ from $C(H, f)$. It satisfies $s = \sum_{\alpha\in F} \alpha|v_\alpha| + f(d)$, where $d = \sum_\alpha v_\alpha$. Applying Lemma 4 with $j = 1, \ldots, n$, we see that $\Pi^c(v) = ((u_\alpha)_{\alpha\in F}, s)$ satisfies $s = \sum_{\alpha\in F} \alpha|u_\alpha| + f(d) + \beta_1^c d_1 + \ldots + \beta_n^c d_n$, where $d = (d_1, \ldots, d_n) = \sum_\alpha u_\alpha$. Adding $w = ((w_\alpha)_{\alpha\in F}, z)$, we obtain $w + \Pi^c(v) = ((w_\alpha + u_\alpha), r)$, where

$$\begin{aligned} r &= \sum_{\alpha\in F} \alpha|u_\alpha| + f(d) + \beta_1^c d_1 + \ldots + \beta_n^c d_n \\ &\quad + \sum_{\alpha\in F} \alpha|w_\alpha| + f(c) \\ &= \sum_{\alpha\in F} \alpha|u_\alpha + w_\alpha| + f(d+c) - \beta_0^c + f(c). \end{aligned}$$

But $f(c) = f(\bar{0}) + \beta_0^c$, as we see from (1). Since $f(\bar{0}) = 0$, we have proved that $w + \Pi^c(v)$ belongs to $C(H, f)$. ∎

So, we get the transitivity. It remains to prove that the set of Φ_w, $w \in C(H, f)$ is closed under composition.

Lemma 6: For every $c, d \in H$ the composition $\Pi^c\Pi^d$ equals Π^{c+d}.

Proof: As follows directly from the definitions of Π^c and Π_i^β,

$$\begin{aligned} \Pi^c\Pi^d &= \Pi_1^{\beta_1^c}\ldots\Pi_n^{\beta_n^c}\Pi_1^{\beta_1^d}\ldots\Pi_n^{\beta_n^d} \\ &= \Pi_1^{\beta_1^c}\Pi_1^{\beta_1^d}\Pi_2^{\beta_2^c}\Pi_2^{\beta_2^d}\ldots\Pi_n^{\beta_n^c}\Pi_n^{\beta_n^d}. \end{aligned}$$

By the definition of Π_i^β, we have $\Pi_i^{\beta_i^c}\Pi_i^{\beta_i^d} = \Pi_i^{\beta_i^c+\beta_i^d}$. But, by Lemma 2, $\beta_i^c + \beta_i^d = \beta_i^{c+d}$. Finally, we have $\Pi^c\Pi^d = \Pi_1^{\beta_1^{c+d}}\ldots\Pi_n^{\beta_n^{c+d}} = \Pi^{c+d}$. ∎

Now, consider $w = ((w_\alpha)_{\alpha\in F}, z)$ and $v = ((v_\alpha)_{\alpha\in F}, s)$ form $C(H, f)$. Denote $c = \sum_\alpha w_\alpha$ and $d = \sum_\alpha v_\alpha$; observe that the permutation Π^c will not change the value of the last sum. Then,

$$\begin{aligned} \Phi_w\Phi_v(\cdot) &= w + \Pi^c(v + \Pi^d(\cdot)) \\ &= w + \Pi^c(v) + \Pi^c(\Pi^d(\cdot)) = u + \Pi^e(\cdot), \end{aligned}$$

where $u = ((u_\alpha)_{\alpha\in F}, t) = w + \Pi^c(v)$, $e = \sum_\alpha u_\alpha = c + d$. This completes the proof of the theorem.

V. Remarks, Examples, and Further Research

A. On the Group Related to $C(H, f)$

As follows from the definition, to every codeword v of a propelinear code C there corresponds an automorphism Φ_v of C and the set $\{\Phi_v : v \in C\}$ forms a subgroup of the automorphism group of C. Although such a subgroup, a *propelinear structure*, is not unique in general (see [1] and also Remark 2 below), in the previous section we explicitly defined a variant of the choice of Φ_v for every $v \in C(H, f)$. Below, we provide two remarks with examples about the propelinear structure defined in the previous section.

Remark 1: For every $v \in C(H, f)$, the element Φ_v has order 1, p, or p^2, where p is the prime that divides q. Indeed, every permutation Π^c is of order 1 or p; hence, $(\Phi_v)^p$ corresponds to the identity permutation and has order 1 or p.

As an example, we consider the (non-perfect) code $C(H, f)$ constructed with the following parameters: $q = 2$, $n = 2$, $H = F^2$, $f(x_1, x_2) = x_1x_2$. From (1) we find $\beta_1^{01} = 1$, $\beta_2^{01} = 0$, $\beta_1^{10} = 0$, $\beta_2^{10} = 1$, $\beta_1^{11} = 1$, $\beta_2^{11} = 1$. The group of automorphisms related with the propelinear code $C(H, f)$ is generated by three elements Φ_u, Φ_v, Φ_w with $u = (11\,00\,1)$, $v = (10\,00\,0)$, $w = (10\,10\,1)$ and the corresponding coordinate permutations $\Pi^{11} = (13)(24)$, $\Pi^{10} = (24)$, $\Pi^{00} = \mathrm{Id}$. The first element Φ_u generates a cycle with the corresponding codewords $(00\,00\,0)$, $(11\,00\,1)$, $(11\,11\,0)$, $(00\,11\,1)$. The second generating element Φ_v adds four more codewords: $(10\,00\,0)$, $(00\,01\,1)$, $(01\,11\,0)$, $(11\,10\,1)$; the corresponding automorphisms are of order 2. The group generated by Φ_u and Φ_v is described by the orders of Φ_u, Φ_v and the identity $\Phi_v\Phi_u\Phi_v = (\Phi_u)^{-1}$, and it is isomorphic to the dihedral group D_4. The last generating element Φ_w commutes with all other elements and has order 2. It follows that the group of automorphisms related with $C(H, f)$ is isomorphic to the direct product $D_4 \times Z_2$, where Z_2 is the cyclic group of order 2.

Remark 2: If $H \neq F^n$, then there is more than one quadratic representations of every quadratic function on H. The coefficients β_i^c and, as follows, the subgroup $\{\Phi_v : v \in C\}$ of the automorphism group of the code depend on the representation; so, there are several propelinear structures corresponding to the same code $C(H, f)$. For example, the all-zero function over $H = \{000, 111\}$ ($q = 2$) can be

represented as $f(x_1, x_2, x_3) = 0$ or, e.g., as $f(x_1, x_2, x_3) = x_1x_2 + x_1x_3$. The resulting code is the same (a 1-perfect Hamming code of length 7); but in the first case, the group is isomorphic to Z_2^4, while the second representation leads to a group isomorphic to $Z_4 \times Z_2^2$. The general fact that several propelinear structures can correspond to the same (perfect) code was well demonstrated in [1].

B. Transitive Vasil'ev Codes of Length 15

There are 201 nonequivalent transitive 1-perfect codes of length 15 [14, Table III]. Five of these codes are Vasil'ev codes, including the linear one; their description can be found in [11] (the four nonlinear codes are denoted by $V4$, $V4^0$, $V4^1$, and $V22^02^1$). Let H be spanned by the words $u_1 = 1010101$, $u_2 = 0111100$, $u_4 = 0001111$, $u_0 = 1111111$. Define the functions f^{V4}, f^{V4^0}, f^{V4^1}, $f^{V22^02^1} : H \to \{0, 1\}$ by their sets of zeros $\{\bar{0}, u_0, u_1, u_0 + u_1\}$, $\{\bar{0}, u_1, u_2, u_1 + u_2\}$, $\{\bar{0}, u_0+u_1, u_0+u_2, u_1+u_2\}$, $\{\bar{0}, u_0, u_1, u_2, u_4, u_0+u_1+u_2+u_4\}$, respectively. Then the codes $C(H, f^{V4})$, $C(H, f^{V4^0})$, $C(H, f^{V4^1})$, $C(H, f^{V22^02^1})$ are representatives of the four equivalence classes of nonlinear transitive Vasil'ev codes of length 15. All these codes are propelinear [1]. Moreover, it can be directly checked that the functions are quadratic:

$$\begin{aligned} f^{V4}(x) &= x_2x_4 + x_2x_6 + x_4x_6 + x_2 + x_4 + x_6, \\ f^{V4^0}(x) &= x_1x_6 + x_2x_6 + x_3x_6 + x_1 + x_2 + x_3 + x_6, \\ f^{V4^1}(x) &= x_3x_5 + x_3 + x_5, \\ f^{V22^02^1}(x) &= x_3x_4 + x_3x_5 + x_3x_7 + x_4x_5 + x_4x_7 + x_5x_7 \\ &\quad + x_3 + x_4 + x_5 + x_7; \end{aligned}$$

so, the corresponding codes meet the hypothesis of Theorem 1. Therefore, all transitive Vasil'ev codes of length 15 belong to the class considered in the current paper.

C. Transitive Functions

For further development of the topic, it would be interesting to consider a wider class of functions resulting in transitive (propelinear) codes. Such functions should have properties similar to transitivity (propelinearity) of codes:

Problem 1: For a vector space V and a group $\mathcal{A}$ of linear permutations of V, find non-quadratic functions f such that for every c from V there exists $\mu \in \mathcal{A}$ meeting $f(\mu(x)+c) = f(x) + l(x)$ for some affine l. For instance, for constructing transitive (propelinear) 1-perfect codes as above, we can take $V = H$ and $\mathcal{A} \subset \mathrm{Aut}(H)$.

REFERENCES

[1] J. Borges, I. Y. Mogilnykh, J. Rifà, and F. I. Solov'eva, "Structural properties of binary propelinear codes," *Adv. Math. Commun.*, vol. 6, no. 3, pp. 329–346, 2012.

[2] J. Borges, I. Y. Mogilnykh, J. Rifà, and F. I. Solov'eva, "On the number of nonequivalent propelinear extended perfect codes," *Electron. J. Combinat.*, vol. 20, no. 2, pp. P37-1–P37-14, Mar. 2013.

[3] J. Borges and J. Rifà, "A characterization of 1-perfect additive codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1688–1697, May 1999.

[4] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*. Berlin, Germany: Springer-Verlag, 1989.

[5] C. Carlet, "Z_{2^k}-Linear codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1543–1547, Apr. 1998.

[6] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[7] T. Honold and A. A. Nechaev, "Fully weighted modules and representations of codes," *Probl. Inf. Transmiss.*, vol. 35, no. 3, pp. 205–223, 1999.

[8] D. S. Krotov, "Z_4-Linear perfect codes," *Diskretn. Anal. Issled. Oper.*, vol. 7, no. 4, pp. 78–90, 2000.

[9] D. S. Krotov, "Z_{2^k}-Dual binary codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1532–1537, Apr. 2007.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[11] S. A. Malyugin, "On the equivalence classes of perfect binary codes of length 15," preprint 138, Sobolev Inst. Math., Novosibirsk, Russia, Aug. 2004.

[12] A. A. Nechaev, "Trace-function in Galois ring and noise-stable codes," in *Proc. V All-Union Symp. Theory Rings, Algebras Modules*, Novosibirsk, Russia, 1982, p. 97.

[13] A. A. Nechaev, "Kerdock code in a cyclic form," *Discrete Math. Appl.*, vol. 1, no. 4, pp. 365–384, 1991.

[14] P. R. J. Östergård, O. Pottonen, and K. T. Phelps, "The perfect binary one-error-correcting codes of length 15: Part II—Properties," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2571–2582, Dec. 2010.

[15] V. N. Potapov, "A lower bound for the number of transitive perfect codes," *J. Appl. Ind. Math.*, vol. 1, no. 3, pp. 373–379, 2007.

[16] J. Rifà, J. M. Basart, and L. Huguet, "On completely regular propelinear codes," in *Proc. 6th Int. Conf. AAECC*, Rome, Italy, Jul. 1988, pp. 341–355.

[17] J. Schönheim, "On linear and nonlinear single-error-correcting q-ary perfect codes," *Inf. Control*, vol. 12, no. 1, pp. 23–26, 1968.

[18] F. I. Solov'eva, "On the construction of transitive codes," *Probl. Inf. Transmiss.*, vol. 41, no. 3, pp. 204–211, 2005.

[19] Y. L. Vasil'ev, "On nongroup close-packed codes," *Problems Cybern.*, vol. 8, pp. 337–339, Jan. 1962.

Denis S. Krotov was born in Novosibirsk, Russia, in 1974. He received the Bachelor's degree in mathematics in 1995 and the Master's degree in 1997, both from Novosibirsk State University, the Ph.D. and Dr.Sc. degrees in Discrete Mathematics and Theoretical Cybernetics from Sobolev Institute of Mathematics, Novosibirsk, in 2000 and 2011, respectively.

Since 1997, he has been with Theoretical Cybernetics Department, Sobolev Institute of Mathematics, where he is currently a Leading Researcher. In 2003, he was a Visiting Researcher with Pohang University of Science and Technology, Korea. His research interest includes subjects related to discrete mathematics, algebraic combinatorics, coding theory, and graph theory.

Vladimir N. Potapov was born in Novosibirsk, Russia, in 1971. He received the Bachelor's degree in mathematics from Novosibirsk State University in 1992, the Master's degree in 1994 from the same university, and the Ph.D. degree in Mathematical Analysis from Sobolev Institute of Mathematics, Novosibirsk, in 1997.

He has taught in Novosibirsk State University since 1995, where he is currently an Associated Professor. Since 1998, he has been a Senior Researcher at the Sobolev Institute of Mathematics. His research interests include combinatorics, source coding, coding theory, video processing, and cryptography.