Transitive 1-perfect codes from quadratic functions

D. S. Krotov, V. N. Potapov

Sobolev Institute of Mathematics,

Novosibirsk State University

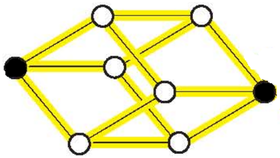
International Conference Mal'tsev Meeting

Novosibirsk, November 12–16, 2012

Let F be a finite field of order q; let F^n be the vector space of all n-words over the alphabet F.

Definition

A subset C of F^n is called a 1-perfect code if for every word v from F^n there is exactly one c in C agreeing with v in at least $n-1$ positions.



Definition

The automorphism group $\mathcal{AUT}(C)$ of a code $C \subset F^n$ is the set of permutations of F^n that preserve the neighborhood (two words are neighbors if they differ in exactly one position) and stabilize C.

Definition

The code C is transitive if for every two codewords a, b there exists $\varphi \in \mathcal{AUT}(C)$ such that sends a to b.

Vasil'ev — Schönheim construction

Let $H \subset F^n$ be a 1-perfect code and $\lambda : H \to F$ be an arbitrary function. Define the set

$$C(H, \lambda) = \{(v_0, \ldots, v_{q-1}, p) \, : \, v_i \in F^n, \; \sum_{i \in F} v_i = c \in H, p = \sum_{i \in F} i|v_i| + \lambda(c)\},$$

where $|v_i|$ is the sum of all n elements of v_i. Then $C(H, \lambda)$ is a 1-perfect code of length $qn + 1$, known as a Schonheim code (in the case $q = 2$, Vasil'ev code).

J. Schönheim. On linear and nonlinear single-error-correcting q-ary perfect codes // *Inform. Contr.*, 12(1):23–26, 1968.

Vasil'ev, Ju. L. On ungrouped, close-packed codes// *Problemy Kibernet.* No. 8 1962 337–339.(Russian)

Assume H is a subspace of F^n. A function $\lambda : H \to F$ is called *quadratic* if for every $c \in V$ there exist $\alpha_0^c, \alpha_1^c, \ldots, \alpha_n^c$ such that $\lambda(x+c) = \lambda(x) + \alpha_0^c + \alpha_1^c x_1 + \ldots + \alpha_n^c x_n$ for all $x = (x_1, \ldots, x_n) \in H$.

Theorem

If $H \subset F^n$ is a linear 1-perfect code and $\lambda : H \to F$ is a quadratic function, then $C(H, \lambda)$ is a transitive 1-perfect code.

The quadratic functions are exactly the functions whose polynomial representation has degree at most 2. The number of such functions has the form $q^{\frac{n^2}{2}(1+o(1))}$, and so, this expression gives a lower bound on the number of different transitive 1-perfect q-ary codes of length $qn+1$.

Corollary

The number of nonequivalent transitive 1-perfect q-ary codes of length $qn+1$ is not less than $q^{\frac{n^2}{2}(1+o(1))}$.

F. I. Solov'eva, "On Construction of Transitive Codes // *Problems of Information Transmission*, 2005, 41:3, 204–211.

V.N. Potapov. A lower bound for the number of transitive perfect codes // *Journal of Applied and Industrial Mathematics*, 2007, 1:3, 373–379

F. I. Solov'eva. On transitive partitions of an n-cube into codes// *Problems Inform. Transmission*, 45:1 (2009), 23–31.

J. Borges, J. Rifà, I. Yu. Mogilnykh, and F. I. Solov'eva. Structural properties of binary propelinear codes// *Advances in Mathematics of Communications.* 2012. V. 6, N 3, P. 329 - 346, 2012.

Lemma

Let $f'(x) = f(x) + \beta x_j$ for some $j \in [1..n]$, $\beta \in F$. Then $C(H, f') = \Pi_j^{\beta} C(H, f)$ where Π_j^{β} is the coordinate permutation that sends the $(\alpha+\beta, j)$th coordinate to the (α, j)th coordinate (the jth coordinate of the block v_α, $\alpha \in F$) for all $\alpha \in F$ and fix the other coordinates.

Proof. Let us consider the codeword $x = ((v_\alpha)_{\alpha \in F}, p)$ of $C(H, f)$. It satisfies $p = \sum_{\alpha \in F} \alpha |v_\alpha| + f(c)$. After the coordinate permutation Π_j^{β}, we obtain the word $y = \Pi_j^{\beta} x = ((u_\alpha)_{\alpha \in F}, p)$ 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 $v_{\alpha+\beta,j}$.

$p = \sum_{\alpha \in F} \alpha |v_\alpha| + f(c) = \sum_{\alpha \in F} \sum_{k \neq j} \alpha v_{\alpha,k} + \sum_{\alpha \in F} \alpha v_{\alpha,j} + f(c) =$
$= \sum_{\alpha \in F} \sum_{k \neq j} \alpha u_{\alpha,k} + \sum_{\alpha \in F} \alpha u_{\alpha-\beta,j} + f(c) =$
$= \sum_{\alpha \in F} \sum_{k \neq j} \alpha u_{\alpha,k} + \sum_{\alpha \in F} (\alpha+\beta) u_{\alpha,j} + f(c) =$
$= \sum_{\alpha \in F} \sum_{k=1}^{n} \alpha u_{\alpha,k} + \beta \sum_{\alpha \in F} u_{\alpha,j} + f(c) = \sum_{\alpha \in F} \alpha |u_\alpha| + f(c) + \beta c_j$,
$c = (c_1, \ldots, c_n) = \sum v_\alpha = \sum u_\alpha$ and $\Pi_j^{\beta}(x) \in C(H, f')$.

Proposition

For every codeword $w = ((w_\alpha)_{\alpha \in F}, p)$ of $C(H, f)$ the transform $\Phi_w(v) = \Pi^c(v) + w$, 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 $v = ((v_\alpha)_{\alpha \in F}, q)$ from $C(H, f)$. It satisfies $q = \sum_{\alpha \in F} \alpha |v_\alpha| + f(d)$, where $d = \sum_\alpha v_\alpha$. Applying the lemma with $j = 1..n$, we see that $\Pi^c(v) = ((u_\alpha)_{\alpha \in F}, q)$ satisfies $q = \sum_{\alpha \in F} \alpha |u_\alpha| + f(d) + \beta_1^c d_1 + \ldots + \beta_n^c d_n$, where $d = (d_1, \ldots, d_n) = \sum_\alpha u_\alpha$. Adding $w = ((w_\alpha)_{\alpha \in F}, p)$, we obtain $\Pi^c(v) + w = ((u_\alpha + w_\alpha), r)$, where

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

Since $f(0) = 0$, we have proved that $\Pi^c(v) + w$ belongs to $C(H, f)$.

Problem

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 example, for constructing transitive 1-perfect codes as above, we can take $V = H$ and $\mathcal{A} \subset \mathcal{AUT}(H)$.