Propelinear codes from multiplicative group of $GF(2^m)$

Ivan Yu. Mogilnykh
Sobolev Institute of Mathematics SB RAS, Novosibirsk, Russia
ivmog@math.nsc.ru

This is joint work with Faina I. Solov'eva

All necessary definitions and notions can be found in [1]. It is well known that the *automorphism group* (the isometry group) $\mathrm{Aut}(GF(2^m))$ of the binary vector space $GF(2^m)$ with respect to the Hamming metric is the group of all transformations (x, π) fixing $GF(2^m)$ with respect to the composition $(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi \circ \pi')$. Given a binary code C the setwise stabilizer of C in $\mathrm{Aut}(GF(2^m))$ is called the *automorphism group* $\mathrm{Aut}(C)$ of C. The *symmetry group* $\mathrm{Sym}(C)$ of a code C is defined as $\mathrm{Sym}(C) = \{\pi \in S_n : \pi(C) = C\}$. A code C is called *transitive* if there is a subgroup H of $\mathrm{Aut}(C)$ acting transitively on the codewords of C. If we additionally require that for any $x, y \in C$, $x \neq y$ there is a unique element h of H such that $h(x) = y$, then H acting on C is called a *regular group* [2] and the code C is called *propelinear* (for the original definition see [3]). In this case the order of H is equal to the size of C. Each regular subgroup $H < \mathrm{Aut}(C)$ naturally induces a group operation on the codewords of C defined in the following way: $x * y := h_x(y)$, such that the codewords of C form a group with respect to the operation $*$, isomorphic to H: $(C, *) \cong H$, which is called *propelinear structure* on C. The notion of propelinearity is important from algebraic and combinatorial coding theory point of view since it provides a general view on linear and additive codes. It is obvious that any propelinear code is transitive but not vice versa. Many known good codes are propelinear, for example all Z_4-linear codes, see also [4] and list of references there.

Theorem 1. *Let $(D, *)$ and $(C, *)$ be propelinear structures such that $(D, *) < (C, *)$ and a group G be a subgroup of $\mathrm{Sym}(C) \cap \mathrm{Sym}(D)$ acting regularly on the right cosets from $(C/D) \setminus D$. Then $C \setminus D$ is propelinear.*

There are many good (uniformly packed and transitive) codes that have the multiplicative group of $GF(2^m)$ as a subgroup of their symmetry group. Taking this group as G we obtain the examples below. Denote by P the Preparata codes constructed in [6]. Denote by H the cyclic Hamming code with the generator polynomial $m_1(x)$ and a Goethals code by Γ. By H', P' and Γ' denote the known Z_4-linear perfect, Preparata and Goethals codes respectively. These codes form nested families: $H \supset P \supset \Gamma$, $H' \supset P' \supset \Gamma'$.

Theorem 2. *Let D be the cyclic code of length n, $n = 2^m$, $m \geq 3$, m is odd, with the generator polynomial $m_1(x)m_{\sigma+1}(x)$, where $((\sigma + 1), (2^m - 1)) = 1$. Then the code $H \setminus D$ is propelinear.*

Theorem 3. *Let n be $4^m, m \geq 2$. The codes $F_2^n \setminus H$, $H \setminus P$, $P \setminus \Gamma$, $H' \setminus P'$ and $P' \setminus \Gamma'$ of length n are propelinear.*

The work is supported by the Grant the Russian Scientific Fund 14-11-00555.

References

[1] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, *North Holland*, 1977.

[2] K. T. Phelps, J. Rifà, On binary 1-perfect additive codes: some structural properties *IEEE Trans. Inform. Theory* **48** (2002) 2587–2592.

[3] J. Rifà, J. M. Basart, L. Huguet, On completely regular propelinear codes *Proc. 6th Int. Conference, AAECC-6. LNCS* **357** (1989) 341–355.

[4] I. Yu. Mogilnykh, F. I. Solov'eva, Transitive nonpropelinear perfect codes *Discrete Math.* **338** (2015) 174–182.

[5] K. T. Phelps, J. Rifà, V. A. Zinoviev, On Z_4-linear Preparata-like and Kerdock-like codes *IEEE Trans. Inform. Theory* **49** (2003) 2834–2843.

[6] R. D. Baker, J. H. van Lint, R. M. Wilson, On the Preparata and Goethals codes *IEEE Trans. Inform. Theory* **29** (1983) 324–345.