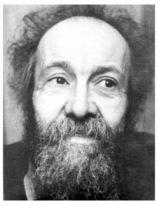

TRANSACTIONS OF THE CONFERENCE,
DEVOTED TO THE 90th ANNIVERSARY OF
ALEXEI A. LYAPUNOV
Novosibirsk, October 8–12, 2001

Perfect codes with big kernel dimensions *

Avgustinovich S.V.
Sobolev Institute of Mathematics, Novosibirsk

Heden O.
Royal Institute of Technology, Stockholm

Solov'eva F.I.
Sobolev Institute of Mathematics, Novosibirsk

Abstract

Perfect codes of all admissible lengths $n > 15$ with the rank $r < n$ and the kernel of dimension k for each $k \in \{(n-1)/2, \dots, U(n)\}$ are presented (here $U(n)$ is the dimension of maximal possible kernel of a full rank perfect code of length n). Full rank perfect codes of all admissible lengths $n > 2^{10} - 1$ with a kernel of dimension k for each $k \in \{(n-1)/2, \dots, U(n)\}$ are given. For length $31 \leq n \leq 2^{10} - 1$ the same result for each $k \in \{(n-1)/2, \dots, U(n) - 2\}$ is true.

A perfect binary code C of length n with code distance 3 (below a perfect code) is defined as a subset of the n-dimensional vector space E^n over $GF(2)$ such that for a vector $y \in E^n$ there exists a unique codeword $x \in C$ with $d(x, y) \leq 1$, where d is the Hamming distance. Perfect binary codes with distance 3 exist iff the length of the codewords is equal to $n = 2^m - 1, m > 1$. *The rank* $r = r(C)$ of a code C is the dimension of the subspace $< C >$ spanned by C. *The kernel* $Ker(C)$ of a code C is the set of all its *periods* (all codewords $x \in C$ such that $x + C = C$). The dimension of the kernel is denoted by $k = k(C)$.

First consider the short survey. Heden [2] constructed perfect codes of length 15 with kernels of dimension $1, 2, 3$. Etzion and Vardy [3] found perfect codes of length $n \geq 15$ of all admissible ranks. Phelps and LeVan [4] established the existence of a nonlinear perfect code of length $n \geq 15$ with a kernel of dimension k for each $k \in \{1, 2, \dots, n - m - 2\}$. Avgustinovich and Solov'eva [5] constructed full rank nonsystematic perfect codes of length $n > 127$ with trivial automorphism group (that means with trivial kernel of size 2). The same result for systematic perfect codes of length $n > 15$ was obtained by Malyugin [6]. Etzion and Vardy [7] proposed

*We are grateful to Swedish Institute for supporting this research. The work of S.V. Avgustinovich was also supported by NWO-047-008-006. The work of F.I. Solov'eva was also supported by the Russian Foundation for Basic Research under the grant 00-01-00822.

to describe all possible pairs of numbers (r, k) which are attainable as the rank r and kernel dimension k of a perfect code of length n. They proved [7] that for every $n \geq 2^m - 1, m > 3$, the upper bound of the dimension of the kernel of length n perfect codes is equal to $U(n) = n - m - \delta$, where δ is the smallest integer, such that $2^\delta - \delta - 1 \geq m$ and showed that the bound is tight for each $n \geq 2^{10} - 1$. Phelps and Villanueva [8] established the upper and lower bound of pairs (r, k) for a perfect code of length $n \geq 15$ and proved that all such pairs are attainable (with the exception of the upper bound of length 15th codes). They also constructed perfect codes of length n for each (r, k), where $k > n - 2m, r < n$. In [11] perfect codes of length $n > 15$ for all possible pairs (r, k), where $r < n$ are presented. In [10] the classification of perfect codes of ranks $n - m + 1$ and $n - m + 2$ is given. For $n = 15$ full rank perfect codes with dimension kernel $1 \leq k \leq 5$ are known, see [2, 1, 7]. For $r < 15$ perfect codes of length 15 for all possible pairs (r, k) are given in [9].

Perfect codes of length n with kernel dimension $k \geq (n-1)/2$ and different ranks are investigated in the paper using well known iterative Vasil'ev construction [12]. Let us remind Vasil'ev construction [12]. Let C' be a perfect code of length $(n-1)/2 = 2^{m-1} - 1, m \geq 2$, and λ be a function from C' to the set $\{0, 1\}$. The set $C = \{(u, u+v, |u| + \lambda(v)) : u \in E^{(n-1)/2}, v \in C'\}$ is the perfect code of length n, where $|u| = u_1 + \cdots + u_{(n-1)/2} \pmod 2$ for $u = (u_1, \ldots, u_{(n-1)/2})$.

Lemma. *Assume there exists a perfect code C' of length $(n-1)/2$ with maximal kernel and the rank $r(C') \leq n$. Then there exist perfect codes of length n with a kernel of dimension k for each $k \in \{(n-1)/2, \ldots, U(n)\}$ and the ranks $r = (n-1)/2 + r(C')$ and $r = (n+1)/2 + r(C')$.*

Taking into account the existence of perfect codes of length 15 with rank less than 15 and maximal kernel, a full rank perfect code of length $2^{10} - 1$ with maximal kernel and full rank perfect code of length 15 with kernel dimension 5 we have using the Lemma the following results respectively.

Theorem 1. *There exist perfect codes of length $n > 15$ with kernel dimension k for each $k \in \{(n-1)/2, ..., U(n)\}$ and the rank $r < n$.*

Theorem 2. *There exist full rank perfect codes of length $n > 2^{10} - 1$ with kernel dimension k for each $k \in \{(n-1)/2, ..., U(n)\}$.*

Theorem 3. *There exist full rank perfect codes of length n, $31 \leq n \leq 2^{10} - 1$, with kernel dimension k for each $k \in \{(n-1)/2, ..., U(n) - 2\}$.*

References

[1] *Näslund M.* Steiner triple systems and perfect codes, Master of Sci. thesis, 1993, Royal Institute of Technology, Stockholm, Sweden.

[2] *Heden O.* A binary perfect code of length 15 and codimension 0, Designs, Codes and Cryptography. 1994. V.4. P. 213–220.

[3] *Etzion T., Vardy A.,* Perfect binary codes: Constructions, properties and enumeration, IEEE Trans. Inform. Theory, 1994. V. 40. N. 3. P. 754-763.

[4] *Phelps K.T., LeVan M.J.,* Kernels of nonlinear Hamming codes, Designs, Codes and Cryptography, 1995. V. 6. P. 247-257.

[5] *Avgustinovich S. V., Solov'eva F. I.* Perfect binary codes with trivial automorphism group, Proc. of Int. Workshop on Information Theory, Killarney, Ireland. June. 1998. P. 114–115.

[6] *Malyugin S. A.* Perfect codes with trivial automorphism group, Proc. Second Int. Workshop on Optimal Codes and Related Topics. Sozopol, Bulgaria. June. 1998. P. 163–167.

[7] *Etzion T., Vardy A.,* On perfect codes and tilings: problems and solutions, SIAM J. Discrete Math., 1998. V. 11. N. 2. P. 205-223.

[8] *Phelps K.T., Villanueva M.*, On perfect codes: rank and kernel, Designs, Codes and Cryptography, to appear.

[9] *Phelps K. T.*, An enumeration of 1-perfect binary codes of length 15, Australasian Journal of Combinatorics, 2000. V. 21. P. 287-298.

[10] *Avgustinovich S. V., Heden O., Solov'eva F. I.* The classification of some perfect codes, submitted.

[11] *Avgustinovich S. V., Heden O., Solov'eva F. I.* On ranks and kernels of perfect codes, submitted.

[12] *Vasil'ev Y.L.,* On nongroup close-packed codes, Problems of Cybernetics 8 (1962) 375-378 (in Russian).