Liet. matem. rink, **45**, *spec. nr.*, 2005, 57–59

On degenerated cyclic codes

Gintaras SKERSYS (VU)
e-mail: gintaras.skersys@mif.vu.lt

Abstract. We characterize degenerate cyclic codes and study their properties.

Keywords: degenerate cyclic codes, hull.

Introduction

Recently an algorithm for computing the permutation and automorphism groups of an error-correcting block linear code, and for determining the equivalence and the permutation-equivalence of two such codes, based on the algorithms of J. Leon [2–4] and N. Sendrier [7], was presented [8–11]. This algorithm is limited by the size of the hull (the intersection of a code with its dual). That shows the necessity to study the size of the hull in various classes of linear codes. In [6], N. Sendrier studies the expected dimension of the hull of a random linear code. He shows that asymptotically it is a small positive constant. In [12], the author studies the expected dimension of the hull of a random cyclic code. He shows that either it is zero, or it grows at the same rate as the length of codes. It is thus important to find some classes of cyclic codes with a small hull. The present paper concerns a class of cyclic codes, called degenerate cyclic codes.

1. Preliminaries

See [5] for basic definitions of error-correcting codes.

In this paper q is a power of a prime p, $\mathbf{F}_q$ is the finite field of size q, n, m, n' are positive integers, $m > 1$, $n = mn'$.

Let $\mathbf{F}_q$ be any finite field. A *linear code C of length n over* $\mathbf{F}_q$ is a linear subspace of the vector space $\mathbf{F}_q^n$. The vectors of a code are called *codewords*. A linear code of length n and of dimension k will be denoted by $[n, k]$. The *dual code* $C^\perp$ of C is defined to be $C^\perp = \{\mathbf{u} \in \mathbf{F}_q^n \mid \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in C\}$, where $\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n$ is the *scalar product* of vectors $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$. The hull was introduced by Assmus and Key in [1]. The *hull* of a linear code C, denoted by $\mathcal{H}(C)$, is its intersection with its dual code: $\mathcal{H}(C) = C \cap C^\perp$.

A linear code C of length n is called *cyclic* if it verifies this condition: if $(c_0, \ldots, c_{n-2}, c_{n-1}) \in C$, then $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Usually cyclic codes are described by the means of polynomials. A vector $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbf{F}_q^n$ corresponds to the polynomial $c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in \mathbf{F}_q[X]/(X^n - 1)$. Then it can be shown that cyclic code of length n is an ideal in the ring $\mathbf{F}_q[X]/(X^n-1)$, generated by a monic factor $g_C(X)$ of X^n-1. Also, every monic divisor of X^n-1 generates a distinct ideal. The polynomial $g_C(X)$ is called the *generator polynomial* of C.

A linear code which consists of several repetitions of a linear code of smaller length is said to be *degenerate*. We will give a formal definition. Let u be a vector of length n'. Denote $\mathcal{R}_m(u) = (u|\cdots|u)$ (m times) — the concatenation of m vectors u. The vector $\mathcal{R}_m(u)$ is of length $n = mn'$. A linear code C of length n is said to be *degenerate* if there exist a divisor $m > 1$ of n and a linear code C' of length $n' = n/m$ such that $C = \mathcal{R}_m(C')$, where $\mathcal{R}_m(C') = \{\mathcal{R}_m(c') \mid c' \in C'\}$. We call the code C' the *inner* code of C. We see that the structure of degenerate codes is very special.

2. Degenerate cyclic codes

In the reminder of the paper we shall assume that $\gcd(n,q)=1$. We give a characterization of degenerate cyclic codes of length n over $\mathbf{F}_q$.

THEOREM 1. *Let* $\gcd(n,q)=1$. *These statements are equivalent.*

1. *A cyclic code C of length n over $\mathbf{F}_q$ is degenerate.*
2. *There exists integers r, $1<r<n$, and s, $1<s<n$, such that $n=rs$ and $1+X^s+\cdots+X^{(r-2)s}+X^{(r-1)s}$ divides $g_C(X)$.*
3. *There exists integers r, $1<r<n$, and s, $1<s<n$, such that $n=rs$ and $g_{C^\perp}(X)$ divides X^s-1.*

We get the following properties of degenerate cyclic codes.

THEOREM 2. *Let $m>1$. Let C' be a cyclic code of length n'. Let $C=\mathcal{R}_m(C')$ be a degenerate cyclic code. Then*

1. $g_C(X) = g_{C'}(X)(1+X^{n'}+X^{2n'}+\cdots+X^{n-n'})$.
2. $g_{C^\perp}(X) = g_{C'^\perp}(X)$.

By the inclusion-exclusion principle we get the following result on the number of degenerate cyclic codes.

THEOREM 3. *Let* $\gcd(n,q)=1$. *Let $n=p_1^{e_1}\cdots p_t^{e_t}$ be the prime decomposition of n, let $N(d)$ be the number of divisors of X^d-1 over $\mathbf{F}_q$. Then the number of degenerate cyclic codes of length n over $\mathbf{F}_q$ is*

$$\sum_{l=1}^{t}(-1)^{l+1}\sum_{\{i_1,\dots,i_l\}\subset\{1,\dots,t\}} N\Big(\frac{n}{p_{i_1}\cdots p_{i_l}}\Big).$$

In order that the algorithm mentioned in Introduction works, the dimension of the hull of a code must be small enough. As the following result shows, the dimension of the hull of a degenerate cyclic code is equal to that of its much smaller inner code.

THEOREM 4. *Let $m > 1$. Let $C = \mathcal{R}_m(C')$ be a degenerate cyclic code. Then* $\mathcal{H}(C) = \mathcal{R}_m(\mathcal{H}(C'))$.

COROLLARY 1. *Let $m > 1$. Let $C = \mathcal{R}_m(C')$ be a degenerate cyclic code. Then* $\dim \mathcal{H}(C) = \dim \mathcal{H}(C')$.

Conclusions

Let C' be a cyclic code. Then $\{\mathcal{R}_m(C')\}_{m>1}$ is a (infinite) family of degenerate cyclic codes. The dimension of the hull of any code in this family is constant and equal to the dimension of the hull of C'. So if the algorithm mentioned in Introduction runs for C', it will run for other codes in this family.

It remains to see what happens when $\gcd(n, q) \neq 1$. Moreover, it seems that it is possible to extend the results to linear codes.

References

1. E.F. Assmus, Jr., J.D. Key, Affine and projective planes, *Discr. Math.*, **83**, 161–187 (1990).
2. J. Leon, Computing automorphism groups of error-correcting codes, *IEEE Trans. Info. Theory*, **IT–28**(3), 496–511 (1982).
3. J. Leon, Permutation group algorithms based on partitions, I: Theory and algorithms, *J. Symbolic Computation*, **12**, 533–583 (1991).
4. J. Leon, Partitions, refinements, and permutation group computation, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, **28**, 123–158 (1997).
5. F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam (1978).
6. N. Sendrier, On the dimension of the hull, *SIAM Journal on Applied Mathematics*, **10**, 282–293 (1997).
7. N. Sendrier, Finding the permutation between equivalent codes: the support splitting algorithm, *IEEE Trans. Info. Theory*, **IT–46**(4), 1193–1203 (2000).
8. N. Sendrier, G. Skersys, Permutation groups of error-correcting codes, in: D. Augot and C. Carlet (Eds.), *Proceedings of Workshop on Coding and Cryptography*, INRIA, Paris (1999), pp. 33–41.
9. N. Sendrier, G. Skersys, On the computation of the automorphism group of a linear code, in: *Proceedings of IEEE ISIT'2001*, Washington, DC (2001).
10. G. Skersys, *Calcul du groupe d'automorphismes des codes. Détermination de l'équivalence des codes*, Ph.D. Thesis, Limoges University, Limoges (1999).
11. G. Skersys, Computing permutation groups of error-correcting codes, *Liet. matem. rink.*, **40**(spec. issue), 320–328 (2000).
12. G. Skersys, The average dimension of the hull of cyclic codes, *Discrete Applied Mathematics*, **128**(1), 275–292 (2003).

REZIUMĖ

G. Skersys. Apie išsigimusius ciklinius kodus

Šiame straipsnyje pateikiame kriterijus, leidžiančius nustatyti, ar duotas ciklinis kodas yra išsigimęs. Tiriame išsigimusių ciklinių kodų savybes.