Discrete Mathematics 339 (2016) 1624–1627

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

Long module skew codes are good

Adel Alahmadi [a], André Leroy [b], Patrick Solé [c,a,*]

[a] Math Department, King Abdulaziz University, Jeddah, Saudi Arabia
[b] Dép. de Mathématique, Université d'Artois, Lens, France
[c] Telecom ParisTech, 46 rue Barrault, 75634 Paris Cedex 13, France

ARTICLE INFO

Article history:
Received 13 May 2014
Received in revised form 8 January 2016
Accepted 12 January 2016
Available online 9 February 2016

Keywords:
Skew cyclic codes

ABSTRACT

Module skew codes are one sided modules for (a quotient of) a skew polynomial ring where multiplication is twisted by an automorphism of the Galois group of the alphabet field. We prove that long module skew codes over a fixed finite field are asymptotically good by using a non-constructive counting argument. We show that for fixed alphabet size, and automorphism order and large length their asymptotic rate and relative distance satisfy a modified Varshamov–Gilbert bound.

1. Introduction

Cyclic codes form an important family of linear codes [11], studied since the fifties for their favorable encoding and decoding properties. In spite of a long attention span and of recent results [1] it is still an open problem to know if long cyclic codes are good [11, p. 270]. The folklore conjecture is that they are not.

Skew cyclic codes were introduced by Ulmer et al. in [2] as a non commutative generalization of cyclic codes. Because of the non unicity of factorization of the skew polynomial ring that enters their definition, the population of such codes even in short lengths outnumbers that of cyclic codes. It is thus natural to conjecture that they form a good class of codes in the asymptotic sense.

In this paper we shall prove that module skew codes, a generalization of skew cyclic codes [3,4], are asymptotically good, in the sense that the product of their rate by their relative distance is nonzero for the rate in some interval of $(0, 1)$ depending on the field size. To show this we will derive a modified Varshamov–Gilbert bound on the rate by a counting argument. The proof is inspired from the analogous result for the special case of $q = 2$ and $r = 1$ from [8, Appendix II]. That old result is saying that polycyclic codes are good. Polycyclic codes in the sense of [10] are ideals in some quotient ring of the form $F[x]/(f)$, where f is a polynomial of degree n that may not be $x^n - 1$. It is well-known and easy to prove that polycyclic codes (aka pseudo-cyclic codes) are exactly shortened cyclic codes [12, p. 241].

2. Definitions and notation

2.1. Skew cyclic codes

Let F denote a finite field of characteristic p and size $q = p^a$. Let σ denote an element of its Galois group, of order r, so that r divides a. If $a = rm$, then the fixed field of σ has order $Q = p^m$. Let us recall that the ring of skew polynomials

* Corresponding author at: Telecom ParisTech, 46 rue Barrault, 75634 Paris Cedex 13, France.
E-mail address: sole@enst.fr (P. Solé).

http://dx.doi.org/10.1016/j.disc.2016.01.008
0012-365X/

in X denoted $R = F[X; \sigma]$ is the ring whose elements are polynomials $\sum_{i=0}^{n} a_i X^i$ with coefficients $a_0, \ldots, a_n$ in F with the standard addition of polynomials but multiplication is based on the commutation rule $Xa = \sigma(a)X$, for all $a \in F$. By a **module skew code** of length n we shall mean a left submodule of the left R-module $R_f = R/Rf$ where $f \neq 0$ is arbitrary of degree n. Since R is left Euclidean it is easy to see that such a submodule is of the form Rg/Rf, where g right divides f.

2.2. Asymptotic bounds

Let C_n be a sequence of codes of length n, dimension k_n, and minimum distance d_n over F. The asymptotic rate ρ of the family is defined as

$$\rho = \limsup_{n\to\infty} \frac{k_n}{n}.$$

The asymptotic relative distance δ is defined as

$$\delta = \limsup_{n\to\infty} \frac{d_n}{n}.$$

A family of codes is said to be **good** if $\rho\delta > 0$. Define the symmetric q-ary **entropy function** as

$$H_q(x) = -x \log_q(x) - (1-x)\log_q(1-x) + x\log_q(q-1). \tag{1}$$

The volume $V(n, q, t)$ of the Hamming ball of radius t about the origin is given by

$$V(n, q, t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

By [5, Lemma 2.10.3] we know that when $t \sim \tau n$, for some $\tau \in (0, 1)$, we have

$$\lim_{n\to\infty} \left(\frac{\log_q(V(n, q, t))}{n} \right) = H_q(\tau).$$

The **asymptotic Varshamov–Gilbert** bound says (cf. Theorem 30, p. 557 in [11]) that there are families of codes such that

$$\rho \geq 1 - H_q(\delta).$$

3. Counting codes

We consider a polynomial $f \in R = F[X; \sigma]$, where F is a finite field of order $q = p^a$ and σ is an automorphism of order r. We denote the number of fixed elements by Q. It is well known that factorization in $R = F[X; \sigma]$ has the following property (cf. P.M. Cohn [6]): If $f_1 \ldots f_l = g_1 \ldots g_r$ are two factorizations where the polynomials $f_1 \ldots, f_l, g_1, \ldots, g_r$ are all irreducible, then $l = r$ and there exists a permutation $\tau \in S_n$ such that for every $1 \leq i \leq l$ we have an isomorphism of left R-modules $R/Rf_i \cong R/Rg_{\tau(i)}$.

In his thesis J. Le Borgne introduced a map ψ from R to its center. The next lemma can be found in [9], Corollary 4.5 and Proposition 5.2.

Lemma 1. (a) *Two monic polynomials f and g are similar if and only if $\psi(f) = \psi(g)$.*
(b) *For a polynomial $f \in R = F[x; \sigma]$ of degree t, the number of $g \in R$ with $\psi(g) = \psi(f)$ is*

$$\frac{q^t - 1}{Q^t - 1}.$$

We use this result to compute the number of irreducible factors. For a polynomial $P \in R$; we will say that $\psi(P)$ is the norm of P.

Lemma 2. *The number of irreducible polynomials of degree t that divide a polynomial f of degree n is at most $\frac{n}{t}\frac{q^t-1}{Q^t-1}$.*

Proof. The number of similarity classes of irreducible factors of f of degree t that appears in a factorization of f is bounded by n/t. The similarity class of such a degree t factor of f has a number of elements given by the part (b) of Lemma 1. This gives the required bound. □

Let $\phi(q, r; t)$ denote the number of irreducible polynomials of degree t in $R = F[X; \sigma]$.

Proposition 1. *If*

$$\left\lfloor \frac{n}{t}\frac{q^t - 1}{Q^t - 1} \right\rfloor \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < \phi(q, r; t),$$

then there is a module skew code of length n codimension t and minimum distance $\geq d$.