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

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 $\geq d$.

Proof. We restrict our attention to skew cyclic codes with an irreducible generator polynomial $f \in R = F[X; \sigma]$ of degree n. The number of elements in the Hamming ball of radius $d-2$ is given by

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i.$$

These correspond to polynomials of degree at most n and, by Lemma 2, can be divided by at most $\lfloor \frac{n}{t} \frac{q^t-1}{Q^t-1} \rfloor$ irreducible generator polynomials. Therefore the hypothesis on the number of irreducible polynomial of degree t, shows that there exist enough generator polynomials for skew cyclic codes of length n with distance d to exist. □

We need an estimate on $\phi(q, r; t)$.

Lemma 3. *The number $\phi(q, r; t)$, for fixed q and large t is, up to sub exponential terms, of order q^t.*

Proof. An exact formula for $\phi(q, r; t)$, is given in [9, Cor. II.5.3], [7] by

$$\phi(q, r; t) = \frac{(q-1)}{t} \frac{q^t - 1}{Q^t - 1} \sum_{i|t} \mu\left(\frac{t}{i}\right) Q^i$$

where μ denotes the Moebius function. Note that $\mu(1) = 1$. For large t and q fixed (hence also Q fixed) we have

$$\phi(q, r; t) \sim \frac{(q-1)q^t}{t}.$$

The result follows. □

We are now ready for the main result, an asymptotic version of the proposition.

Theorem 1. *Given q and r there are skew cyclic codes for an automorphism of order r satisfying the modified Varshamov–Gilbert bound*

$$(1 - \rho) \leq rH_q(\delta).$$

Proof. Note first that $Q = q^{1/r}$. Also observe that the codimension of a skew cyclic code equals the degree of its generator polynomial, implying $t = n - k$ so that, for n large we have $\frac{t}{n} \to 1 - \rho$. Combine the proposition with the preceding lemma; observe that the sum that appears on the left hand side is of the same order as $V(n, q, d)$ for large n. We obtain, after taking logs, dividing by n and taking limits, the existence of families of codes with parameters

$$-\frac{1-\rho}{r} + H_q(\delta) \leq -\epsilon,$$

for all $\epsilon > 0$. Therefore letting $\epsilon \to 0$, we get

$$-\frac{1-\rho}{r} + H_q(\delta) = 0.$$

The result follows. □

4. Conclusion and open problems

In this note we have shown that module skew codes, a non commutative analogue of polycyclic codes are good. Indeed their asymptotic parameters satisfy a modified Varshamov–Gilbert bound. The main open problem would be to derive the same result for so-called σ-cyclic codes which are the special case where the polynomial f that defines R_f is $X^n - 1$. That subclass is the skew analogue of classical cyclic codes. This problem might be as difficult as for ordinary cyclic codes. Another open problem that emerges from the present study is the minimum distance of module skew codes with an irreducible generator polynomial. It might be interesting to look at codes of modest length in that family.

References

[1] L. Babai, A. Shpilka, D. Stefankovic, Locally testable cyclic codes, IEEE Trans. Inform. Theory 51 (8) (2005) 2849–2858.
[2] D. Boucher, W. Geiselmann, F. Ulmer, Skew cyclic codes, Appl. Algebra Engrg. Comm. Comput. 18 (2007) 379–389.
[3] D. Boucher, F. Ulmer, Codes as modules overs skew polynomial rings, in: Lecture Notes in Computer Science, vol. 5921, Springer, 2009, pp. 38–55.
[4] D. Boucher, F. Ulmer, A note on the dual codes of module skew codes, in: LNCS, vol. 7089, Springer, 2011, pp. 230–243.
[5] W. Cary Huffman, Vera Pless, Fundamentals of Error Correcting Codes, Cambridge University Press, 2003.
[6] P.M. Cohn, Free Ideal Rings and Localization in General Rings, in: New Mathematical Monographs, vol. 3, Cambridge University Press, Cambridge, 2006.
[7] R.S. Coulter, G. Havas, M. Anderson, On decomposition of sub-linearized polynomials, J. Aust. Math. Soc. 76 (2004) 317–328.
[8] T. Kasami, An upper bound on k/n for affine invariant codes with fixed d/n, IEEE Trans. Inform. Theory 15 (1969) 174–176.

[9] J. Le Borgne, Semi-characteristic polynomials, ϕ-modules, and skew polynomials (thesis), Université de Rennes, 2012, http://blogperso.univ-rennes1.fr/jeremy.le-borgne/index.php/post/2012/04/17/Math.
[10] S.R. Lopez-Permouth, B.R. Parra-Avila, S. Szabo, Dual generalizations of the concept of cyclicity of codes, Adv. Math. Commun. 3 (2009) 227–234.
[11] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[12] William Wesley Peterson, E.J. Weldon Jr., Error Correcting Codes, second ed., MIT Press, 1972.