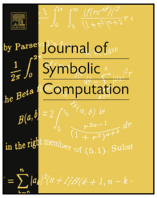
Journal of Symbolic Computation 60 (2014) 47–61

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc



Self-dual skew codes and factorization of skew polynomials

Delphine Boucher, Felix Ulmer

IRMAR, CNRS, UMR 6625, Université de Rennes 1, Université européenne de Bretagne, Campus de Beaulieu, F-35042 Rennes, France

ARTICLE INFO

Article history:
Received 8 May 2013
Accepted 25 September 2013
Available online 15 October 2013

Keywords:
Error-correcting codes
Finite fields
Skew polynomial rings

ABSTRACT

The construction of cyclic codes can be generalized to so-called “module θ-codes” using noncommutative polynomials. The product of the generator polynomial g of a self-dual “module θ-code” and its “skew reciprocal polynomial” is known to be a noncommutative polynomial of the form $X^n - a$, reducing the problem of the computation of all such codes to the resolution of a polynomial system where the unknowns are the coefficients of g. We show that a must be ± 1 and that over $\mathbb{F}_4$ for $n = 2^s$ the factorization of the generator g of a self-dual θ-cyclic code has some rigidity properties which explains the small number of self-dual θ-cyclic codes with length $n = 2^s$. In the case θ of order two, we present a construction of self-dual codes, based on the least common multiples of noncommutative polynomials, that allows to reduce the computation to polynomial systems of smaller sizes than the original one. We use this approach to construct a $[78, 39, 19]_4$ self-dual code and a $[52, 26, 17]_9$ self-dual code which improve the best previously known minimal distances for these lengths.

1. Introduction

For a finite field $\mathbb{F}_q$ and θ an automorphism of $\mathbb{F}_q$ we consider the ring $R = \mathbb{F}_q[X; \theta] = \{a_n X^n + \cdots + a_1 X + a_0 \mid a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}$ where addition is defined to be the usual addition of polynomials and where multiplication is defined by the basic rule $X \cdot a = \theta(a)X$ ($a \in \mathbb{F}_q$), extended to all elements of R by associativity and distributivity. The noncommutative ring R is called a *skew polynomial ring* or Ore ring (cf. Ore, 1933b) and its elements are *skew polynomials*. It is a left and right Euclidean ring whose left and right ideals are principal. Left and right gcds and lcms exist in R and can be computed

E-mail addresses: delphine.boucher@univ-rennes1.fr (D. Boucher), felix.ulmer@univ-rennes1.fr (F. Ulmer).

http://dx.doi.org/10.1016/j.jsc.2013.10.003

using the left and right Euclidean algorithm. Over finite fields skew polynomial rings are also known as linearized polynomials (cf. Ore, 1933a; Lidl and Niederreiter, 1983). Following Boucher and Ulmer (2009a) we define module θ-codes using the skew polynomial ring R.

Definition 1. A *module θ-code* (or module skew code) $\mathcal{C}$ is a left R-submodule $Rg/Rf \subset R/Rf$ in the basis $1, X, \ldots, X^{n-1}$ where $g \in R = \mathbb{F}_q[X;\theta]$ and f is a left multiple of g in R of degree n. We denote this code $\mathcal{C} = (g)_n^\theta$. If there exists an $a \in \mathbb{F}_q \setminus \{0\}$ such that g divides $X^n - a$ on the right, then the code $(g)_n^\theta$ is *θ-constacyclic*. We will denote it $(g)_n^{\theta,a}$. If $a = 1$, the code is *θ-cyclic* and if $a = -1$, it is *θ-negacyclic*.

The length of the code is n and its dimension is $k = n - \deg(g)$, we say that the code $\mathcal{C}$ is of type $[n,k]_q$. If the minimal distance of the code is d, then we say that the code $\mathcal{C}$ is of type $[n,k,d]_q$. As in the commutative case we identify a codeword in the $\mathbb{F}_q$-vector space R/Rf of dimension n with the list of coefficients of a skew polynomial of degree $< n$ which is a left multiple of g. The code $\mathcal{C} = Rg/Rf \subset R/Rf$ is the set of left multiples of g of degree $< n$ and therefore depends only on g and n. For $g = \sum_{i=0}^{n-k} g_i X^i$, the generator matrix of the module θ-code $(g)_n^\theta$ is given by

$$G_{g,n}^{\theta} = \begin{pmatrix} g_0 & \ldots & g_{n-k-1} & g_{n-k} & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \ldots & \theta(g_{n-k-1}) & \theta(g_{n-k}) & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \ldots & 0 & \theta^{k-1}(g_0) & \ldots & \theta^{k-1}(g_{n-k-1}) & \theta^{k-1}(g_{n-k}) \end{pmatrix} \qquad (1)$$

showing that distinct generator polynomials correspond to distinct generator matrices. On the other hand, a skew polynomial f, that can be used to define $\mathcal{C}$ as Rg/Rf, gives informations on the properties of the code. For example, for a θ-constacyclic code $(g)_n^{\theta,a}$, where one can choose $f = X^n - a$, we have

$$(c_0, \ldots, c_{n-1}) \in (g)_n^{\theta,a} \quad \Rightarrow \quad \bigl(a\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})\bigr) \in (g)_n^{\theta,a}.$$

Since $\mathbb{F}_q[X;\theta]$ is not a unique factorization ring, we obtain much more codes that are θ-constacyclic, using the noncommutative approach, than constacyclic codes in the commutative case. Module θ-codes are a generalization of Gabidulin codes (cf. Gabidulin, 1985) based on linearized polynomials.

Example 2. For $\mathbb{F}_4 = \mathbb{F}_2(a)$ where $a^2 + a + 1 = 0$ and θ the Frobenius automorphism $\alpha \mapsto \alpha^2$ the skew polynomial $X^2 + 1$ admits three distinct decompositions as products of irreducible polynomials in $\mathbb{F}_4[X;\theta]$

$$X^2 + 1 = \bigl(X + a^2\bigr)(X + a) = (X + a)\bigl(X + a^2\bigr) = (X + 1)(X + 1). \qquad (2)$$

The polynomials $X^4 + 1$, $X^6 + 1$ and $X^8 + 1$ admit respectively 15, 90 and 543 distinct decompositions as products of irreducible polynomials in $\mathbb{F}_4[X;\theta]$ (counting the number of factorizations is considered in von zur Gathen et al., 2010).

In previous work many self-dual module θ-codes with good minimum distances were obtained, sometimes even improving the previously best known minimal distances. However, as in the case of cyclic codes (Jia et al., 2011), there is a phenomena for the module θ-codes whose lengths are a power of 2. For the lengths 4, 8, 16, 32 and 64 there are only three self-dual module θ-codes over $\mathbb{F}_4$, while otherwise there is a large number of self-dual codes which increases with the length. The authors conjectured that for any s there are only three self-dual module θ-codes of length 2^s over $\mathbb{F}_4$ (Boucher and Ulmer 2009a, 2011). The aim of this paper is to use the factorization properties of skew polynomials to count self-dual module θ-codes of length 2^s over $\mathbb{F}_4$ and to construct self-dual module θ-codes when θ is of order two. The material is organized as follows: