Finite Fields and Their Applications 50 (2018) 84–112

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# Hartmann–Tzeng bound and skew cyclic codes of designed Hamming distance ☆

José Gómez-Torrecillas [a,*], F.J. Lobillo [a], Gabriel Navarro [b], Alessando Neri [c]

[a] *CITIC and Department of Algebra, University of Granada, Spain*
[b] *CITIC and Department of Computer Sciences and AI, University of Granada, Spain*
[c] *Institut für Mathematik, University of Zürich, Switzerland*

ARTICLE INFO

*Article history:*
Received 25 April 2017
Received in revised form 9 September 2017
Accepted 6 November 2017
Available online xxxx
Communicated by W. Cary Huffman

*MSC:*
94B10
94B15
94B65
94B35
94B05

*Keywords:*
Linear codes
Convolutional codes
Cyclic codes
Skew cyclic codes

ABSTRACT

The use of skew polynomial rings allows to endow linear codes with cyclic structures which are not cyclic in the classical (commutative) sense. Whenever these skew cyclic structures are carefully chosen, some control over the Hamming distance is gained, and it is possible to design efficient decoding algorithms. In this paper, we give a version of the Hartmann–Tzeng bound that works for a wide class of skew cyclic codes. We also provide a practical method for constructing them with designed distance. For skew BCH codes, which are covered by our constructions, we discuss decoding algorithms. Detailed examples illustrate both the theory as the constructive methods it supports.



☆ Research partially supported by grants MTM2013-41992-P and TIN2013-41990-R from Ministerio de Economía y Competitividad of the Spanish Government and from FEDER, by grant MTM2016-78364-P from Agencia Estatal de Investigación and from FEDER, and by grant number 169510 from the Swiss National Science Foundation.

* Corresponding author.
*E-mail address:* gomezj@ugr.es (J. Gómez-Torrecillas).

https://doi.org/10.1016/j.ffa.2017.11.001
1071-5797/

Hartmann–Tzeng bound
BCH skew code

## 1. Introduction

The availability of additional algebraic structure in error correcting linear codes has helped their construction in two ways. On one hand, a better knowledge of the main parameters of the code can be obtained. For instance the pioneer works [3,20] use cyclic structures in linear block codes to design them with a prescribed distance. Those ideas were generalized by Hartmann and Tzeng in [19]. In these papers, the behavior of the roots of the cyclic generator in a suitable field extension of the alphabet (a finite field), provides lower bounds of the Hamming distance of the code. On the other hand, the presence of higher algebraic structures also allows the design of fast decoding algorithms. This is the case for instance of the Peterson–Gorenstein–Zierler algorithm, see [30,18], where linear algebra techniques are used, in conjunction with the aforementioned behavior of the roots of cyclic codes, to design decoding procedures.

Let $\mathbb{F}$ be a finite field. Classically, a cyclic block code over the alphabet $\mathbb{F}$ is an ideal of $\mathbb{F}[x]/\langle f\rangle \cong \mathbb{F}^n$, where $f$ is a polynomial of degree $n$. In this way, only a few codes of length $n$ enjoy a cyclic structure modeled by $f$ (in fact they are in one to one correspondence with the monic divisors of $f$) and most of the codes are not cyclic. However, by replacing $\mathbb{F}[x]/\langle f\rangle$ by some $n$-dimensional non-commutative $\mathbb{F}$-algebra, new cyclic structures on some non cyclic codes arise. One of the most successful ways to follow this philosophy consists in twisting the multiplication of the polynomial ring. Concretely, skew cyclic block codes are left ideals of factor algebras of skew polynomial rings $\mathbb{F}[x;\sigma]$ by a two-sided ideal, where $\sigma$ is an automorphism of the finite field $\mathbb{F}$. Such an ideal is generated by a normal polynomial $f \in \mathbb{F}[x;\sigma]$, so that skew cyclic codes will be in correspondence with right divisors of $f$. It is well known that this number of divisors is much larger than in the commutative case, due essentially to the lack of uniqueness, in the usual sense, of factorizations in $\mathbb{F}[x;\sigma]$ (see [29]). Of course we want to get some control on the parameters of the skew cyclic code, and also to take advantage of this cyclic structure to design efficient decoding algorithms. To this end, both $\sigma$ and $f$ have to be carefully chosen. These skew block codes were introduced, for $f = x^n - 1$, in [5], and, in the general case, independently in [6,12]. The notion can be traced back to [11], where the author used the arithmetics of linearized polynomials to introduce and investigate the nowadays known as Gabidulin codes.

In [5] bounds of the Hamming distance and a Sugiyama like decoding algorithm are provided for skew cyclic codes when the alphabet is $\mathbb{F}_{2^n}$, the automorphism is the Frobenius automorphism, $\sigma(a) = a^2$, and $f = x^n - 1$. One advantage of this choice of parameters is that $f$ fully decomposes as a least common left multiple of $n$ linear polynomials. For a more general $f$ a way to find a decomposition of this type is needed. In [9] Picard–Vessiot fields of $\sigma$-difference equations associated to skew codes are used to