Finite Fields and Their Applications 45 (2017) 96–106

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A generalization of quasi-twisted codes: Multi-twisted codes

Nuh Aydin[a,*], Ajdin Halilović[b]

[a] Kenyon College, Department of Mathematics, Gambier, OH 43022, USA
[b] Lumina—The University of South-East Europe, Şos. Colentina 64b, 021187 Bucharest, Romania

A R T I C L E   I N F O

Article history:
Received 10 June 2016
Accepted 2 December 2016
Available online 4 January 2017
Communicated by Gary L. Mullen

MSC:
94B15
94B60
94B65

Keywords:
Constacyclic codes
Quasi-twisted codes
Best-known codes

A B S T R A C T

Cyclic codes and their various generalizations, such as quasi-twisted (QT) codes, have a special place in algebraic coding theory. Among other things, many of the best-known or optimal codes have been obtained from these classes. In this work we introduce a new generalization of QT codes that we call multi-twisted (MT) codes and study some of their basic properties. Presenting several methods of constructing codes in this class and obtaining bounds on the minimum distances, we show that there exist codes with good parameters in this class that cannot be obtained as QT or constacyclic codes. This suggests that considering this larger class in computer searches is promising for constructing codes with better parameters than currently best-known linear codes. Working with this new class of codes motivated us to consider a problem about binomials over finite fields and to discover a result that is interesting in its own right.

* Corresponding author.
E-mail address: aydinn@kenyon.edu (N. Aydin).

http://dx.doi.org/10.1016/j.ffa.2016.12.002
1071-5797/

1. Introduction and motivation

Every linear code over a finite field $\mathbb{F}_q$ has three basic parameters: the length (n), the dimension (k), and the minimum distance (d) that determine the quality of the code. One of the most important and challenging problems of coding theory is a discrete optimization problem: determine the optimal values of these parameters and construct codes whose parameters attain the optimal values. This optimization problem is very difficult. In general, it is only solved for the cases where either k or $n-k$ is small. There is a database of best known linear codes with upper bounds on minimum distances that is available online [1]. The database is updated as new codes are discovered and reported by researchers.

Computers are often used in searching for codes with best parameters but there is an inherent difficulty: computing the minimum distance of a linear code is computationally intractable (NP-hard) [11]. Since it is not possible to conduct exhaustive searches for linear codes if the dimension is large, researchers often focus on promising subclasses of linear codes with rich mathematical structures. A promising and fruitful approach has been to focus on the class of quasi-twisted (QT) codes which includes cyclic, constacyclic, and quasi-cyclic (QC) codes as special cases. This class of codes is known to contain many codes with good parameters. In the last few decades, a large number of record-breaking QC and QT codes have been constructed (e.g. [2–10]). The search algorithm introduced in [4] has been highly effective and used in several subsequent works ([5–10]).

In this work, we introduce a new generalization of QT codes that we call multi-twisted (MT) codes. It turns out that this class also generalizes more recently introduced classes of double cyclic codes ([2,3]), QCT codes ([15]), and GQC codes ([14]). After deriving some of their algebraic properties and obtaining a lower bound on the minimum distance, we show that from this class we can obtain linear codes with best-known or optimal parameters that cannot be obtained from the smaller classes of constacyclic or QT codes.

Before introducing this new class of codes, we recall some fundamental results about constacyclic and QT codes that will be needed later.

2. Constacyclic and quasi-twisted codes

Constacyclic codes are well-known in algebraic coding theory. Let $a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A linear code C over a finite field $\mathbb{F}_q$ is called constacyclic with shift constant a if it is closed under the constacyclic shift, i.e. for any $(c_0, c_1, \ldots, c_{n-1}) \in C$, $T_a(c_0, c_1, \ldots, c_{n-1}) := (ac_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. When $a = 1$, we obtain the very important special case of cyclic codes. Many well-known codes are instances of cyclic codes.

Under the usual isomorphism $\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - a\rangle$, where $\pi(u) = u_0 + u_1x + u_2x^2 + \ldots + u_{n-1}x^{n-1}$, for $u = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{F}_q^n$, it is well known that a constacyclic code is an ideal in the ring $\mathbb{F}_q[x]/\langle x^n - a\rangle$. Moreover, for every constacyclic code C there is a unique, monic polynomial of least degree in C that generates C, i.e. $C = \langle g(x)\rangle =$