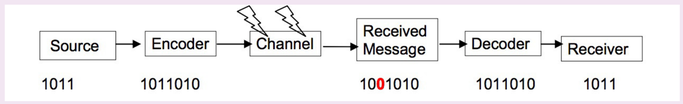
New Linear Codes over Non-Prime Fields

Jonathan Lambrinos 20' and Ghada Bakbouk 19', faculty advisor Prof. Nuh Aydin

Department of Mathematics and Statistics, Kenyon College, Gambier OH

What is Coding Theory?

Transferring information is one of the great advancements that make life as we know it possible. Whenever information is transferred, errors are prone to occur. Coding theory is a branch of mathematics that explores reliable and efficient transfer of information. Error correcting codes are used to detect and rectify the effects of undesirable disturbances, called *noise*, on the quality of the information received. They are used in all fields that require information transmission, such as texting and outer space missions.



The Structure of a Linear Code

A **linear code** is a **vector space** over a **finite field**. It can be thought of as a set of **codewords** (or **vectors**) with a certain mathematical structure.

A linear code C is defined by three parameters:

1. **Length** n
   The total number of "letters" in each codeword of C.
   (The total number of bits in a codeword.)
2. **Dimension** k $(\leq n)$
   The number of basis elements for C
   (The number of "information" bits in a codeword".)
3. **Minimum Distance** d
   $min\{d(u,v) : u, v \in C, u \neq v\}$
   The smallest number of differences (Hamming Distance) between the positions of any two distinct codewords in C.

These are known as $[n,k,d]_q$ codes, where q is the size of the finite field $\mathbb{F}_q$ over which C is a vector space.

Best Known Linear Codes (BKLC)

The **(Hamming) distance**, $d(u,v)$ for $u, v \in \mathbb{F}_q^n$, is the number of positions any given two distinct codewords (u and v) in the code differ. The distance between the two codewords below is 2:

$$1001010110$$

$$1011010010$$

The **minimum distance** d of a linear code is what determines that code's capacity for **error detection** and **error correction**.

Detectable Errors: $d-1$ Correctable Errors: $\lfloor \frac{d-1}{2} \rfloor$

For a given value of length n and dimension k, there exists an **upper bound** on the value of d. A known $[n,k]_q$ code with a minimum distance as close as possible to this upper bound is said to be a **best known linear code** (BKLC).

Abstract

One class of linear codes is quasi-twisted (QT) codes which contains cyclic and constacyclic codes as subclasses. We can also view constacyclic codes as building blocks of QT codes. Our goal is to find codes with better parameters than currently best known linear codes, by searching QT codes. There has been much research on the class of QT codes. Yet, we have been able to obtain more record-breaking codes over the non-prime fields $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_9$ by employing a comprehensive search strategy and an automated system including programs written in Magma and C++. Our strategy includes choosing the most promising constacyclic codes for each set of parameters. For each alphabet, only a subset of constants and lengths need to be examined. So far, we have been able to find 50+ record-breaking codes and our search continues. We also have plans to implement a more comprehensive method by considering only one code per equivalence class of constacyclic code given a fixed set of parameters.

Constacyclic Codes

Definition:
Let $a \in \mathbb{F}_q$ be nonzero. A linear code C of length n is said to be **constacyclic** if it is closed under the **constacyclic shift**.
If $(c_0, c_1, \cdots, c_{n-1}) \in C$, then $(ac_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in C$ too.

If the **shift constant** $a \in \mathbb{F}_q$ is taken to be 1, then C is a **cyclic code**.
We adopt the convention of representing the vectors in C as polynomials:

$$1001101 \quad \rightarrow \quad x^6 + x^3 + x^2 + 1$$

Polynomials are nice to work with algebraically! A constacyclic shift of a vector by a shift constant a corresponds to multiplying the corresponding polynomial by $x \mod x^n - a$. We may exploit the nice algebraic structure of constacyclic codes. We may exhaustively generate every constancyclic code within $\frac{\mathbb{F}_q[x]}{\langle x^n - a \rangle}$ by using the factors of $x^n - a$.

Boundaries of Our Search

Each divisor of $x^n - a$ will generate a constacyclic code with shift constant $a \in \mathbb{F}_q$. However, for a given code length n, we need not consider each $a \in \mathbb{F}_q$, since some values of a and n generated **equivalent** cyclic codes. Thus, we only need to consider certain combinations of a and n to exhaustively generate all constacyclic codes over a certain finite field. This result is shown in the following theorem:

Theorem:
If $\gcd(n,q) = 1$ and $a, b \in \mathbb{F}_q^*$ are such that $|a| = |b|$ then there exists a one-to-one correspondence between the set of constacyclic codes of length n with shift constant a and the set of constacyclic codes of length n with shift constant b such that corresponding codes in each set have the same parameters.

Based on this theorem, we only need to consider the following:

q	$a \neq 0, 1$	n	Maximum n
4	Any constant in field	All $n \ni 3 \vert n$	256
8	Any constant in field	All $n \ni 7 \vert n$	130
9	α	All $n \ni 2 \vert n$	130
	α^2	All $n \ni 4 \vert n$	
	α^4	All $n \ni 8 \vert n$	

Note that we only considered non-prime finite fields of sizes 4, 8, and 9. For a given finite field, we used the upper bound of n for codes in the Online Database of Best Known Linear Codes [3] as the maximum length. We consider all values of $k < n$. However, it is important to note that sometimes, the upper bounds are not obtainable. Hence, finding a record-breaking code does not necessarily mean hitting the upper bound, but rather getting closer to it.

Quasi-Twisted and Quasi-Cyclic Codes

Definition:
A linear code is said to be ℓ**-quasi-twisted** (ℓ-QT) if it is closed under a constacylic shift of a field constant a by ℓ positions.

Quasi-twisted (QT) codes are a generalization of **constacyclic** codes. Many record breaking codes are QT, which makes them promising candidates. More specifically, the generator polynomial of an $[m,k,d]_q$ constacyclic code with shift constant a can be used to construct and ℓ-QT code of length $n = m\ell$. The first half of our project was devoted to constructing constacyclic codes with good parameters. We used the best codes from this search to then construct QT codes.

If the shift constant a of a QT code is 1, then it is a **Quasi-cyclic (QC)** code. QC codes are hence generalizations of cyclic codes.

Our Results

Using the methods described earlier, we were able to find ( ) new linear codes. These linear codes are from QT codes.

Note: the element α is the primitive element of the field F. This means that every non-zero element of F can be written as a power of α.

- $GF(4)$ Quasi-twisted:
- $GF(8)$ Quasi-twisted:
- $GF(9)$ Quasi-twisted:

Example: $[96, 10, 68]_9$ QT-Code ($\ell = 6$):

Factoring $x^{16} - 1$
$g = [1a^2a^2a^2a^7a^6a^5]$
$f_1 = [a^3002a^6a^3a^5a^3a^20]$
$f_2 = [a^521a^3a^32aa^2a^2a^2]$
$f_3 = [a^7a^22a2a^5a^3a^7a^2a^6]$
$f_4 = [a2a^2a^2aa^5a^21a^70]$
$f_5 = [1a^72a^30a^2aa^7a^2a^7]$

Moving forward, we are working on a new method that deals with equivalence classes of codes. This more comprehensive method will allow us to check more promising codes, while keeping the redundancy of the search minimal.

BKLC vs Best Known QT Codes

As explained before, every QT code is a linear code but not every linear code is a QT code. Our objective in this research was to find record-breaking linear codes. However, as a byproduct, we also ended up finding QT codes that are better than previously best known QT codes.

Example: $[52, 12, 30]_8$ QT-Code ($\ell = 4$):

Factoring $x^{13} - 1$
$g = [11]$
$f_1 = [a^2a^2a^6a^4a^50a^301aa^6a^3a]$
$f_2 = [a^4a^6a^50a^3a110a^3a^5a^5a^4]$
$f_3 = [0a^2aa^3a^6a1a^6a^6a01]$

The code above does not exceed the distance of the best linear code for the given set of parameters, but it is the best QT code for those parameters.

References

[1.] N. Aydin, and J. Murphree. "New Linear Codes from Constacyclic Codes." Journal of the Franklin Institute, Vol 351 (3),1691-1699, March 2014.

[2.] Hankerson, Darrel R., D. G. Hoffman, et. all. Coding Theory and Cryptography: The Essentials. 2nd ed. New York: M. Dekker, 2000.

[3.] M. Grassl. "Tables of Linear Codes and Quantum Codes." Tables of Linear Codes and Quantum Codes. N.p., n.d. Web. 2 August 2017.

[4.] N. Aydin, I. Siap, and Dijen K. Ray-Chaudhuri. "The Structure of 1-Generator Quasi-Twisted Codes and New Linear Codes." Designs, Codes and Cryptography 24 (2001): 313-26.

[5.] N. Aydin, and T. Asamov. Search for good linear codes in the class of quasi-cyclic and related codes Selected Topics in Information and Coding Theory, Edited Book, I. Woungang, S. Misra, S. Chandra Misra (Eds.), Series on Coding and Cryptology, World Scientific Publishing, March 2010.

[6.] N. Aydin, N. Connolly and M. Grassl. "Some Results on the Structure of Constacyclic Codes and New Linear Codes Over $GF(7)$ from Quasi-twisted Codes". Advances in Mathematics of Communications. Volume 11, No. 1, 2017, 245-258

[7.] R. Ackerman and N. Aydin, New quinary linear codes from quasi-twisted codes and their duals, Appl. Math.Lett., 24 (2011), 512-515.