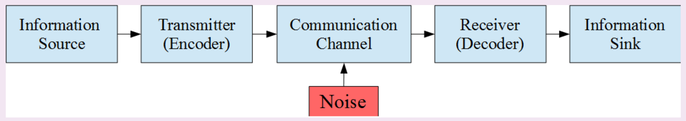
# Constructing Linear Codes with Record Breaking Parameters


## Prof. Nuh Aydin and Nicholas Connolly

Department of Mathematics, Kenyon College, Gambier OH


## What is Coding Theory?

Coding theory is the branch of mathematics interested in the reliable transfer of information (it is different from cryptography). Codes are used everywhere electronic information is transferred. When information is sent, it is **encoded** by a transmitter, sent through a communication channel, and then **decoded** by a receiver. Within the communication channel, external sources of **noise** can change the information being sent.




Certain codes can **detect** when an error occurs, depending on their mathematical structure, and some codes are even capable of **correcting** these errors.

## 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** which obey 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** $d$
   The smallest number of differences between the positions of any two 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 **distance** between any two codewords is the number of positions by which they differ. The distance between the two codewords below is 2:

$$0001010110$$

$$1011010010$$

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


In this project, we attempt to construct new linear codes with larger minimum distances than the previously best known codes by exploiting the algebraic structures of constacyclic and quasi-twisted codes. For a given length and finite field, we used the computer algebra system Magma to exhaustively construct all constacyclic codes and record those codes with the highest minimum distance for a given length and dimension. We then use those best constacyclic codes to construct 1-generator quasi-twisted codes. Finally, we compare the minimum distance of these quasi-twisted codes against the best known linear codes with the goal of discovering new linear codes with better parameters. We have been able to find 96 new codes with this method which have been added to the online database of best known linear codes.


## 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.

**Theorem:**

1. Constacyclic codes are **ideals** in $\frac{\mathbb{F}_q[x]}{\langle x^n - a \rangle}$.
2. $\frac{\mathbb{F}_q}{\langle x^n - a \rangle}$ is a principal ideal ring.
3. Each $C \in \frac{\mathbb{F}_q}{\langle x^n - a \rangle}$ is generated by some $g(x) \in \mathbb{F}_q[x]$
4. If $\langle g(x) \rangle = C$, then $g(x)$ is a divisor of $x^n - a$
5. There is a **one-to-one correspondence** between the divisors of $x^n - a$ and $[n, k]_q$ constacyclic codes.

We may exhaustively generate every constancylic 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 $a \in \mathbb{F}_q$. For some values of $a$ and $n$, the generated code will be **equivalent** to a cyclic code. Thus, we only need to consider certain combinations of $a$ and $n$ to exhaustively generate all constacyclic codes over a certain finite field. The table below shows which values we used

| $q$ | $a \neq 0, 1$ | $n$ | Maximum $n$ |
|---|---|---|---|
| 3 | 2 | All $n \ni 2\|n$ | 243 |
| 4 | Any constant in field | All $n \ni 3\|n$ | 256 |
| 5 | 2 | All $n \ni 2\|n$ | 130 |
| | 4 | All $n \ni 4\|n$ | |
| 7 | 2 | All $n \ni 3\|n$ | 100 |
| | 3 | All $n \ni 2\|n$ or $n \ni 3\|n$ | |
| | 6 | All $n \ni 2\|n$ | |
| 8 | Any constant in field | All $n \ni 7\|n$ | 130 |
| 9 | $\alpha$ | All $n \ni 2\|n$ | 130 |
| | $\alpha^2$ | All $n \ni 4\|n$ | |
| | $\alpha^4$ | All $n \ni 8\|n$ | |

Note that we only considered finite fields of sizes 2, 4, 5, 7, 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 $k < n$

## Quasi-Twisted Codes

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

**Quasi-twisted** codes are a generalization of **constacyclic** codes. Many record breaking codes are quasi-twisted, which makes them promising candidates. It turns out that QT codes can be constructed by combining the generator polynomials constacyclic codes. More specifically, the generator polynomial of an $[m, k, d]_q$ constacyclic code with shift constant $a$ can be used to construct and $\ell$-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 quasi-twisted codes.

## Our Results

We were able to discover explicit constructions for 31 record breaking quasi-twisted codes. In addition to these, we were also able to construct an additional 65 record breaking codes using the standard constructions of extending, puncturing, or shortening a given code. While we constructed constacyclic codes over the six finite fields listed earlier, we only constructed quasi-twisted codes over $\mathbb{F}_7$. We chose to start with $\mathbb{F}_7$ because it had the largest number of gaps in the online database [3], but it is very likely that we would have discovered even more codes had we extended our search into QT codes over other finite fields.

The table lists the 31 record breaking quasi-twisted codes, as well as the coefficients of the polynomials we used to construct them. They're pretty awesome, so they extend past the page.

| $[\mathbf{n}, \mathbf{k}, \mathbf{d}]_\mathbf{q}$ | $\ell$ | $a$ | **Polynomials** |
|---|---|---|---|
| $[28, 10, 14]_7$ | 2 | 3 | $g = [20101]$<br>$f_2 = [4631415664]$ |
| $[40, 14, 19]_7$ | 2 | 3 | $g = [1110601]$<br>$f_2 = [6653546334161]$ |
| $[56, 10, 35]_7$ | 4 | 3 | $g = [20101]$<br>$f_2 = [1116114504]$<br>$f_3 = [0116022034]$<br>$f_4 = [0046621621]$ |
| $[60, 16, 31]_7$ | 3 | 3 | $g = [26311]$<br>$f_2 = [4306630625334312]$<br>$f_3 = [2100611365244222]$ |
| $[63, 13, 36]_7$ | 3 | 1 | $g = [120426231]$<br>$f_2 = [0266451653142]$<br>$f_3 = [1426041266324]$ |
| $[63, 14, 35]_7$ | 3 | 1 | $g = [56520201]$<br>$f_2 = [53456465314443]$<br>$f_3 = [45602511055454]$ |
| $[68, 18, 34]$ | 2 | 3 | $g = [45334361535421311]$<br>$f_2 = [356141002520132461]$ |
| $[72, 12, 44]_7$ | 3 | 1 | $g = [3160552536401]$<br>$f_2 = [102131140204]$<br>$f_3 = [16645415666]$ |
| $[72, 13, 43]_7$ | 3 | 1 | $g = [635054304101]$<br>$f_2 = [040145443601]$<br>$f_3 = [1300222053634]$ |
| $[72, 16, 39]_7$ | 4 | 6 | $g = [101]$<br>$f_2 = [1565260064566031]$<br>$f_3 = [3444016656241334]$<br>$f_4 = [4142552425143116]$ |
| | | | $f_3 = [5504522513464]$ |
| $[78, 15, 45]_7$ | 2 | 2 | $g = [4165036146215620542545531]$<br>$f_2 = [06126622226123]$ |

## References


**[1.]** N. Aydin, and John M. 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, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Wall. Coding Theory and Cryptography: The Essentials. 2nd ed. New York: M. Dekker, 2000. Print.

**[3.]** Grassl, Markus. "Tables of Linear Codes and Quantum Codes." Tables of Linear Codes and Quantum Codes. N.p., n.d. Web. 30 July 2014.

**[4.]** Ackerman, Ryan, and Nuh Aydin. "New Quinary Linear Codes from Quasi-twisted Codes and Their Duals." Applied Mathematics Letters 24.4 (2011): 512-15. Web.

**[5.]** Aydin, Nuh, Irfan 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. Web.

**[6.]** Aydin, Nuh and Asamov, Tsvetan. "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,