Twisted Tensor Product Codes

Anton Betten

Colorado State University, U.S.A.

July 2011

Abstract

We present two families of constacyclic codes with large automorphism groups.

The codes are obtained from the twisted tensor product construction.

The talk is based on the paper "Twisted Tensor Product Codes", Designs, Codes, Cryptography 47 (2008), 191-219.

Experimental Data

Data from a computer search, as published in

A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann: Error-Correcting Linear Codes, Classification by Isometry and Applications, 2006.

There exists a $[18, 9, 8]$ code over $\mathbb{F}_4$:

Experimental Data

the 1 isometry classes of irreducible [18,9,8]_4 codes are:

code no 1:

==========

1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
3 2 2 2 1 1 1 0 0 0 1 0 0 0 0 0 0 0
2 3 2 1 2 1 0 1 0 0 0 1 0 0 0 0 0 0
2 2 3 1 1 2 0 0 1 0 0 0 1 0 0 0 0 0
3 2 2 1 0 0 2 1 1 0 0 0 0 1 0 0 0 0
2 3 2 0 1 0 1 2 1 0 0 0 0 0 1 0 0 0
2 1 3 3 2 1 3 2 1 0 0 0 0 0 0 1 0 0
1 2 3 2 3 1 2 3 1 0 0 0 0 0 0 0 1 0
1 1 2 0 0 3 3 3 1 0 0 0 0 0 0 0 0 1

the automorphism group has order 16320

orbits: { 1, 12, 18, 15, 8, 17, 14, 2, 4, 13, 6, 7, 5, 11, 16, 3, 9 }, { 10 }

Experimental Data

Observe that 16320 is the order of $\mathrm{P\Gamma L}(2, 16)$, since

$$|\mathrm{P\Gamma L}(2, q)| = \frac{(q^2 - 1)(q^2 - q)h}{q - 1}$$

($q = p^h$, p prime), which, for $q = 16$, evaluates to

$$\frac{255 \cdot 16 \cdot 15 \cdot 4}{15} = 16320$$

Question: Is there a connection?

Experimental Data

Remark: That same code was also mentioned (briefly) in:

MacWilliams, Odlyzko, Sloane, and Ward, 1978:

$n = 17$, $[18, 9, 8] = S_{18}$ with weight enumerator η_{18}, cyclotomic cosets are $\{1, 4, 16, 13\}$, $\{2, 8, 15, 9\}$, $\{3, 12, 14, 5\}$, $\{6, 7, 11, 10\}$, and

$$E(x) = 1 + \alpha\left(\sum_{i \in C_1^{(4)}} x^i + \sum_{i \in C_3^{(4)}} x^i\right) + \beta\left(\sum_{i \in C_2^{(4)}} x^i + \sum_{i C \in_6^{(4)}} x^i\right),$$

The Brouwer/Grassl tables contain a reference to this paper.

Results

THEOREM 1

A) There exist constacyclic $[q^2+1, q^2-8, \geq 6]_q$ for any $q \geq 3$. They are cyclic if and only if q is even.

B) There exist $[q^2+2, q^2-7, \geq 6]_q$ codes for any $q \geq 4$ even.

In both cases, the codes are invariant under $\mathrm{P\Gamma L}(2, q^2)$.

THEOREM 2

There exist constacyclic $[q^3+1, q^3-7, \geq 5]_q$ for any $q \geq 3$. The codes are invariant under $\mathrm{P\Gamma L}(2, q^3)$.

$q = p^h$, p prime.

$$\mathbb{F}_q = \{\alpha^i \mid i = 0, \ldots, q-2\} \cup \{0\}.$$

α a primitive element over $\mathbb{F}_p$.

$\Phi : t \mapsto t^p$ the Frobenius automorphism.

$\mathrm{PG}(n,q)$ the n-dimensional projective space over $\mathbb{F}_q$.

$$\mathrm{PG}(1,q) = \{\underbrace{(t,1)}_{t} \mid t \in \mathbb{F}_q\} \cup \{\underbrace{(1,0)}_{\infty}\}$$

Automorphism group:

$$\mathrm{P\Gamma L}(2,q) = \{\begin{pmatrix} a & c \\ b & d \end{pmatrix}_e \mid a,b,c,d \in \mathbb{F}_q,\ ad-bc \neq 0,\ e \in \mathbb{Z}_h\}$$

acting by semilinear right multiplication:

$$(u,v)\cdot\begin{pmatrix} a & c \\ b & d \end{pmatrix}_h = (ua+vn, uc+vd)^{\Phi^h} = ((ua+vn)^{\Phi^h}, (uc+vd)^{\Phi^h}).$$

The conic $Y^2 = XZ$:

$$\{\underbrace{(t^2,t,1)}_{H_t} \mid t \in \mathbb{F}_q\} \cup \{\underbrace{(1,0,0)}_{H_\infty}\}$$

Same automorphism group, different action.

- The Frobenius automorphism of $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$

$$\phi_s : x \mapsto x^q$$

  of order s leaving $\mathbb{F}_q$ fixed.
- The relative trace from $\mathbb{F}_{q^s}$ to $\mathbb{F}_q$

$$\mathrm{T}_s : x \mapsto x + \phi_s(x) + \cdots + \phi_s^{s-1}(x)$$

- The relative norm from $\mathbb{F}_{q^s}$ to $\mathbb{F}_q$

$$\mathrm{N}_s : x \mapsto x \cdot \phi_s(x) \cdots \phi_s^{s-1}(x)$$

We write ϕ for ϕ_h (if $q = p^h$ with p prime)

Vector Spaces over Finite Fields

$\mathbb{F}_{q^s}^k$ the k-dimensional vector space over $\mathbb{F}_{q^s}$.

Two types of subspaces:

- $\mathbb{F}_{q^s}^i$ for $i \leq k$ is called subspace
- $\mathbb{F}_{q^i}^k$ for $i \mid s$ is called subfield subspace

A basis is a set of linearly independent vectors that spans the subspace over

- $\mathbb{F}_{q^s}$
- $\mathbb{F}_{q^i}$

Linear Codes

Linear codes are subspaces of $\mathbb{F}_q^n$.

$[n, k]_q$ — a linear code C over $\mathbb{F}_q$ of length n, dimension k.

$\mathbf{c} = (c_0, \ldots, c_{n-1}) \in C$ a codeword (simply a vector over $\mathbb{F}_q$).

A generator matrix Γ is a $k \times n$ matrix whose rows form a basis for the code.

A check matrix Δ is a $(n - k) \times n$ matrix whose rows form a basis for the dual code $C^{\perp}$.

Thus, $\Gamma \cdot \Delta^{\top} = 0$.

The Minimum Distance (I)

For a code to be useful

- the minimum distance d should be large,
- the dimension k should be large,
- the length n should be small.

These are contradicting aims.

The Minimum Distance (II)

An $[n, k]_q$ code is distance optimal if has the largest value of d among all $[n, k]_q$ codes.

It is a challenge to find distance optimal codes.

$[n, k, d]_q$ — a linear code over $\mathbb{F}_q$ of length n, dimension k and minimum distance d.

$[n, k, \geq d]_q$ — a linear code over $\mathbb{F}_q$ of length n, dimension k and minimum distance $\geq d$.

Cyclic Codes

A code C is cyclic if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \iff (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Example: BCH codes, Reed-Solomon codes.

Remark:

- Cyclic codes are in 1 to 1 correspondence to the ideals in the ring $\mathbb{F}_q[X]/(X^n - 1)$ (provided $\gcd(n, q) = 1$).

Constacyclic Codes

A code C is constacyclic if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \iff (\kappa c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

for some $\kappa \in \mathbb{F}_q^\times$ (the same κ for every $\mathbf{c} \in C$).

A constacyclic code is cyclic if $\kappa = 1$.

Example: see below

Projective Codes

A code is called projective if

- No coordinate is always zero.
- No two coordinates are linearly dependent.

Let C be a projective code with $k \times n$ generator matrix Γ.

$$\mathbf{x}_0, \ldots, \mathbf{x}_{n-1} \text{ the columns of } \Gamma.$$

$$\Updownarrow$$

$$\mathbf{P}(\mathbf{x}_0), \ldots, \mathbf{P}(\mathbf{x}_{n-1}) \text{ a set of points in } \mathrm{PG}(k-1, q).$$

Why do we Need Projective Codes?

THEOREM (well known)

Let C be a linear code over $\mathbb{F}_q$ with check matrix Δ. The following are equivalent:

- C has minimum distance d
- In Δ, any $d-1$ columns are linearly independent and there exist d columns that are linearly dependent.

That is, quite often the dual code is projective.

Projective Codes

A code is called projective if

- No coordinate is always zero.
- No two coordinates are linearly dependent.

Let C be a projective code with $k \times n$ generator matrix Γ.

$$\mathbf{x}_0, \ldots, \mathbf{x}_{n-1} \text{ the columns of } \Gamma.$$

$$\Updownarrow$$

$$\mathbf{P}(\mathbf{x}_0), \ldots, \mathbf{P}(\mathbf{x}_{n-1}) \text{ a set of points in } \mathrm{PG}(k-1, q).$$

Why do we Need Projective Codes?

THEOREM

Let C be a linear code over $\mathbb{F}_q$ with check matrix Δ. The following are equivalent:

- C has minimum distance d
- In Δ, any $d-1$ columns are linearly independent and there exist d columns that are linearly dependent.

That is, quite often the dual code is projective.

Recipe for Finding Good Codes

In order to find $[n, k, \geq d]_q$ codes, we have to find n points in $\mathrm{PG}(n-k-1, q)$ with the property that

Any $d-1$ are independent.

In order to reduce excess searching, we need to talk about Code Isomorphism.

Permutational, Monomial and Semilinear Isometry

Isometric Codes: Different codes may behave the same way with respect to the Hamming metric.

There are three types of code isometries:

- Permutational isometries (permuting the coordinates),
- Monomial isometries (permuting the coordinates and multiplying non-zero constants),
- Semilinear isometries (all of the above plus field automorphisms).

When we say 'Code', we often mean the *equivalence class of isometric codes*.

In this sense, a code can be cyclic / constacyclic in many different ways, according to different arrangements of the coordinates.

Permutational, Monomial and Semilinear Automorphism Groups

An automorphism is a isometry (of the Hamming space) that maps the code to itself.

There are three types of automorphism groups:

- Permutational automorphism group PAut,
- Monomial automorphism group MAut,
- Semilinear automorphism group $\Gamma\mathrm{Aut}$.

$$\mathrm{PAut} \leq \mathrm{MAut} \leq \Gamma\mathrm{Aut}.$$

Automorphisms of Projective Space

We need to understand the automorphisms of projective space.

An automorphism of projective space is an

incidence preserving isomorphism

(also called collineation).

Two sets A and B in $\mathrm{PG}(n, q)$ are projectively equivalent if there is an automorphism α of $\mathrm{PG}(n, q)$ with $\alpha(A) = B$.

Automorphisms of Projective Space

There are two types of automorphisms of projective space:

- Linear: $\mathrm{GL}(n+1,q)$ acts on $\mathrm{PG}(n,q)$ as follows:

$$A \cdot \mathbf{P}(x) = \mathbf{P}(Ax).$$

- Semilinear: ϕ acts on $\mathrm{PG}(n,q)$ as follows:

$$\phi(\mathbf{P}(\mathbf{x})) = \phi(\mathbf{P}(x_0,\ldots,x_n)) = \mathbf{P}(\phi(x_0),\ldots,\phi(x_n)).$$

The induced maps of the first type are called projectivities. Let $\mathrm{PGL}(n+1,q)$ be the group generated by them.

The Fundamental Theorem of Projective Geometry

Together they generate the semilinear group

$$\mathrm{P\Gamma L}(n+1,q) = \mathrm{PGL}(n+1,q) \ltimes \langle \phi \rangle.$$

THEOREM (well known)

For $n \geq 2$, the automorphism group of $\mathrm{PG}(n,q)$ is $\mathrm{P\Gamma L}(n+1,q)$.

Some One-to-One Correspondences

There is a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{isometry classes} \\ \text{of projective} \\ [n,k]_q\text{-codes} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{projective equivalence} \\ \text{classes of } n\text{-point-sets} \\ \text{in } \mathrm{PG}(n-k-1,q) \end{array} \right\}$$

There is a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{isometry classes} \\ \text{of projective} \\ [n,k,\geq d]_q\text{-codes} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{projective equivalence} \\ \text{classes of } n\text{-point-sets} \\ \text{in } \mathrm{PG}(n-k-1,q) \\ \text{any } d-1 \text{ independent} \end{array} \right\}$$

The Construction (I)

Let $V_n = \mathbb{F}_{q^s}^n$ be an n-dimensional vector space over $\mathbb{F}_{q^s}$.

Consider

$$\otimes_s V_n := V_n \otimes V_n \otimes \cdots \otimes V_n \quad (s \text{ times})$$

Define a mapping

$$\iota_s : V_n \to \otimes_s V_n,$$

$$x \mapsto x \otimes \phi_s(x) \otimes \phi_s^2(x) \otimes \cdots \otimes \phi_s^{s-1}(x).$$

This induces a mapping between the corresponding projective spaces:

$$\iota_s : \mathbf{P}(V_n) \to \mathbf{P}(\otimes_s V_n)$$

The Construction (II)

The points of $\mathrm{PG}(1,q)$ are often identified as follows:

$$\mathbf{P}(1,t) \leftrightarrow t, \quad \mathbf{P}(0,1) \leftrightarrow \infty$$

The Veronese map

$$\nu_k : \mathrm{PG}(1,q) \to \mathrm{PG}(k-1,q), \quad \mathbf{P}(a,b) \mapsto \mathbf{P}(a^k, a^{k-1}b, \ldots, b^k)$$

$\nu_2(\mathrm{PG}(1,q))$ is the conic

$$\{\mathbf{P}(1,t,t^2), \quad t \in \mathbb{F}_{q^2}\} \cup \{\mathbf{P}(0,0,1)\}.$$

The Construction (III)

Consider

- $\iota_2 \circ \nu_3(\mathrm{PG}(1, q^2)) \Rightarrow n = q^2 + 1$ points in $\mathrm{PG}(8, q^2)$
- $\iota_3(\mathrm{PG}(1, q^3)) \Rightarrow n = q^3 + 1$ points in $\mathrm{PG}(7, q^3)$

The image lies in an $\mathbb{F}_q$-subfield subspace.

- $\mathrm{PG}(8, q)$
- $\mathrm{PG}(7, q)$

The codes are projective codes whose point sets are the subspace bases. For Theorem 1 B, add the nucleus to the conic $\nu_2(\mathrm{PG}(1, q))$ (recall that $2 \mid q$ in this case).

Example: Theorem 1

Using $t = 0, 1, \ldots, \infty$ for the points of the projective line, the ν_2 image of $\mathrm{PG}(1, q^2)$ is the conic

$$\{\mathbf{P}(1, t, t^2), \quad t \in \mathbb{F}_{q^2}\} \cup \{\mathbf{P}(0, 0, 1)\}.$$

The ι_2-image of this set is

$$\{\mathbf{P}\underbrace{(1, t^{q+1}, t^{2q+2}, t^q, t, t^{2q}, t^2, t^{2q+1}, t^{q+2})}_{=:\mathbf{y}_t}, \quad t \in \mathbb{F}_{q^2}\}$$

together with $\mathbf{P}\underbrace{(0, 0, 1, 0, 0, 0, 0, 0, 0)}_{\mathbf{y}_\infty}$.

$\otimes$	$\phi(1)$ 1	$\phi(t)$ t^q	$\phi(t^2)$ t^{2q}
1	1	t^q	t^{2q}
t	t	t^{q+1}	t^{2q+1}
t^2	t^2	t^{q+2}	t^{2q+2}

ordering of basis elts.

0	3	5
4	1	7
6	8	2

Example $q = 16$ (with $\alpha^4 = \alpha + 1$):

$$M = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^5 & \alpha^{10} & 1 & 0 & 1 \\
0 & 1 & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^{10} & \alpha^5 & 1 & 1 & 0 \\
0 & 1 & \alpha^4 & \alpha & \alpha^8 & \alpha^2 & \alpha^5 & \alpha^{10} & \alpha^{12} & \alpha^{11} & \alpha^6 & \alpha^{13} & \alpha^9 & \alpha^7 & \alpha^{14} & \alpha^3 & 0 & 0 \\
0 & 1 & \alpha & \alpha^4 & \alpha^2 & \alpha^8 & \alpha^5 & \alpha^{10} & \alpha^3 & \alpha^{14} & \alpha^9 & \alpha^7 & \alpha^6 & \alpha^{13} & \alpha^{11} & \alpha^{12} & 0 & 0 \\
0 & 1 & \alpha^8 & \alpha^2 & \alpha & \alpha^4 & \alpha^{10} & \alpha^5 & \alpha^9 & \alpha^7 & \alpha^{12} & \alpha^{11} & \alpha^3 & \alpha^{14} & \alpha^{13} & \alpha^6 & 0 & 0 \\
0 & 1 & \alpha^2 & \alpha^8 & \alpha^4 & \alpha & \alpha^{10} & \alpha^5 & \alpha^6 & \alpha^{13} & \alpha^3 & \alpha^{14} & \alpha^{12} & \alpha^{11} & \alpha^7 & \alpha^9 & 0 & 0 \\
0 & 1 & \alpha^9 & \alpha^6 & \alpha^3 & \alpha^{12} & 1 & 1 & \alpha^{12} & \alpha^6 & \alpha^6 & \alpha^3 & \alpha^9 & \alpha^{12} & \alpha^9 & \alpha^3 & 0 & 0 \\
0 & 1 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^3 & 1 & 1 & \alpha^3 & \alpha^9 & \alpha^9 & \alpha^{12} & \alpha^6 & \alpha^3 & \alpha^6 & \alpha^{12} & 0 & 0
\end{bmatrix}$$

This is a generator matrix of an $[18, 9, 8]$ code over $\mathbb{F}_{16}$ (with automorphism group $\mathrm{P\Gamma L}(2, 16)$).

Example: Theorem 1

The image lies in an $\mathbb{F}_q$-subfield subspace.

Need: Base change.

Observe that for $\mathbb{F}_q^2 = \mathbb{F}_q(\beta)$ we have

$$\begin{bmatrix} 1 & 1 \\ \beta & \beta^q \end{bmatrix} \cdot \begin{bmatrix} t \\ t^q \end{bmatrix} = \begin{bmatrix} t + t^q \\ \beta t + \beta^q t^q \end{bmatrix} = \begin{bmatrix} T_2(t) \\ T_2(\beta t) \end{bmatrix}$$

which is in the (quadratic) subfield $\mathbb{F}_q$.

Apply this trick in general:

Example: Theorem 1

$$S_\beta \mathbf{y}_t^\top = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & 1 & & & \\ & & & \beta^q & \beta & & & \\ & & & & & 1 & 1 & \\ & & & & & \beta^q & \beta & \\ & & & & & & & 1 \ 1 \\ & & & & & & & \beta^q \beta \end{pmatrix} \begin{pmatrix} 1 \\ t^{q+1} \\ t^{2q+2} \\ t^q \\ t \\ t^{2q} \\ t^2 \\ t^{2q+1} \\ t^{q+2} \end{pmatrix} = \begin{pmatrix} 1 \\ t^{q+1} \\ t^{2q+2} \\ t^q + t \\ \beta^q t^q + \beta t \\ t^{2q} + t^2 \\ \beta^q t^{2q} + \beta t^2 \\ t^{2q+1} + t^{q+2} \\ \beta^q t^{2q+1} + \beta t^{q+2} \end{pmatrix} = \begin{pmatrix} 1 \\ N_2(t) \\ N_2(t^2) \\ T_2(t) \\ T_2(\beta t) \\ T_2(t^2) \\ T_2(\beta t^2) \\ T_2(t^{q+2}) \\ T_2(\beta t^{q+2}) \end{pmatrix} = \mathbf{x}_t^\top$$

Let Δ be the check matrix whose columns are the $\mathbf{x}_t$, $t \in \mathbb{F}_{q^2}$ and $\mathbf{x}_\infty = \mathbf{y}_\infty$. This defines the code.

Example: Theorem 1

Here, the image lies in an $\mathbb{F}_4$ subspace.

The base change matrix is

$$S_\beta = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^8 & \alpha^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^8 & \alpha^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8 & \alpha^2 \end{bmatrix}$$

Example: Theorem 1

$$S_\beta \cdot M = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^5 & \alpha^{10} & 1 & 0 & 1 \\
0 & 1 & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & 1 & \alpha^{10} & 1 & \alpha^{10} & \alpha^5 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & 0 & 0 \\
0 & 1 & \alpha^{10} & \alpha^5 & 1 & 0 & \alpha^5 & \alpha^{10} & 0 & 1 & \alpha^{10} & \alpha^5 & 1 & 0 & \alpha^5 & \alpha^{10} & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^{10} & \alpha^5 & \alpha^5 & 0 & 0 \\
0 & 1 & 1 & 0 & \alpha^5 & \alpha^{10} & \alpha^{10} & \alpha^5 & 1 & 0 & 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^{10} & 0 & 0 \\
0 & 0 & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^{10} & 0 & 0 & \alpha^{10} & \alpha^5 & \alpha^5 & \alpha^{10} & \alpha^5 & \alpha^{10} & \alpha^5 & \alpha^{10} & 0 & 0 \\
0 & 1 & 1 & \alpha^{10} & \alpha^{10} & 0 & 1 & 1 & 0 & \alpha^{10} & \alpha^{10} & \alpha^{10} & 1 & 0 & 1 & \alpha^{10} & 0 & 0
\end{bmatrix}$$

Example: Theorem 1

Or, with $\omega = \alpha^5$ a primitive element for $\mathbb{F}_4$ with $\omega^2 = \omega + 1$.

$$\left[\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega & 1 & \omega^2 & 1 & \omega & 1 & \omega & \omega^2 & 1 & 0 & 1 \\
0 & 1 & \omega^2 & \omega^2 & \omega & \omega & \omega & \omega^2 & 1 & \omega & 1 & \omega^2 & 1 & \omega^2 & \omega & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \omega^2 & \omega^2 & \omega & \omega & \omega & \omega & \omega^2 & \omega^2 & 0 & 0 \\
0 & 1 & \omega^2 & \omega & 1 & 0 & \omega & \omega^2 & 0 & 1 & \omega^2 & \omega & 1 & 0 & \omega & \omega^2 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & 0 & 0 \\
0 & 1 & 1 & 0 & \omega & \omega^2 & \omega^2 & \omega & 1 & 0 & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & 0 & 0 \\
0 & 0 & \omega & \omega & \omega^2 & \omega^2 & 0 & 0 & \omega^2 & \omega & \omega & \omega^2 & \omega & \omega^2 & \omega & \omega^2 & 0 & 0 \\
0 & 1 & 1 & \omega^2 & \omega^2 & 0 & 1 & 1 & 0 & \omega^2 & \omega^2 & \omega^2 & 1 & 0 & 1 & \omega^2 & 0 & 0
\end{array}\right]$$

Or, in standard form...

Example: Theorem 1

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & \omega^2 & \omega \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & \omega & \omega^2 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & \omega & 0 & \omega^2 & 0 & \omega & 1 & \omega & \omega & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 & \omega & 1 & \omega & 1 & \omega^2 & \omega^2 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \omega^2 & 0 & \omega^2 & \omega & 0 & \omega^2 & 1 & \omega^2 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \omega & 0 & \omega & 0 & \omega^2 & 0 & \omega^2 & 1 & \omega \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & \omega & \omega \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \omega^2 & \omega^2 & \omega & \omega & \omega^2 & \omega^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2
\end{bmatrix}$$

Are The Codes New?

The following question arises:

QUESTION 1

Are the codes of Theorem 1 and 2 new?

Fact 1: There are BCH-codes with the same parameters as the codes in Theorem 1 A (see below).

Fact 2: There are codes with the same parameters as the duals of the codes in Theorem 2

Fact 1: A Class of BCH codes

For $n = q^2 + 1$, take the cyclotomic sets of $0, 1, 2$ mod $q^2 + 1$:

$\{0\}$
$\{1, q, q^2 \equiv -1, -q, -q^2 \equiv 1\}$
$\{2, 2q, 2q^2 \equiv -2, -2q, -2q^2 \equiv 2\}$

9 roots, in order:

$$-2q,\ -q,\ \underbrace{-2,\ -1,\ 0,\ 1,\ 2,}_{\text{consecutive set}}\ q,\ 2q,$$

This yields a $[q^2 + 1, q^2 - 8, \geq 6]_q$ BCH-code.

(minimum distance ≥ 6 b/c we have a consecutive set of size 5)

Are The Codes New?

Since BCH-codes are cyclic, we ask:

QUESTION 2

Are the codes of Theorem 1 and 2 cyclic?

If we can show that the codes of Theorem 1 A are not cyclic, then we have shown that they are not BCH-codes and hence (likely) new.

We ask:

QUESTION 3

Given a projective code, how can we tell if the code is cyclic?

When is a Projective Code Cyclic?

C is constacyclic $\iff$

There exists a code automorphism α with

$$\alpha(\mathbf{x}_0) = \mathbf{x}_1,\ \alpha(\mathbf{x}_1) = \mathbf{x}_2,\ \ldots \alpha(\mathbf{x}_{n-1}) = \kappa\mathbf{x}_0.$$

C is cyclic $\iff$ the above with $\kappa = 1$.

When is a Projective Code Cyclic?

The codes are images of $\mathrm{PG}(1, q)$. Thus we ask:

QUESTION 4

What are the cyclic collineations of $\mathrm{PG}(n, q)$?

Cyclic Collineations of Projective Space

LEMMA: (Hirschfeld 1973)

$\#$ conjugacy classes of cyclic projectivities of $\mathrm{PG}(d-1,q)$

$= \frac{1}{q-1} \cdot \#$ subprimitive polynomials of degree d over $\mathbb{F}_q$

$= \frac{\Phi(\theta_{d-1}(q))}{d}$ (with Φ Euler's totient function)

This answers the question for when a code is constacyclic. We still need the find the answer for cyclic.

When is a Projective Code Cyclic?

C is constacyclic $\iff$

There exists a code automorphism α with matrix T s.t.

$$T^n \mathbf{x}_0 = \kappa \mathbf{x}_0, \quad \kappa \neq 0, \quad \text{and} \quad T^i \mathbf{x}_0 \notin \langle \mathbf{x}_0 \rangle \quad i = 1, \ldots, n-1$$

C is cyclic $\iff$ the above with $\kappa = 1$.

The Exponent of a Polynomial

Let $m(x) \in \mathbb{F}_q[x]$ be monic, irreducible of degree $d > 1$.

The Exponent e

The Exponent of m, denoted $\mathrm{Exp}(m)$, is the smallest positive integer e such that

$$m(x) \quad \text{divides} \quad x^e - 1$$

If β denotes a root of $m(x)$ in $\mathbb{F}_{q^d}$ then e is the order of β in $\mathbb{F}_{q^d}^{\times}$.

The Subexponent of a Polynomial

The Subxponent s

The Subexponent of m, denoted $\mathrm{Subexp}(m)$, is the smallest positive integer s such that

$$m(x) \quad \text{divides} \quad x^s - \kappa$$

for some $\kappa \in \mathbb{F}_q^\times$ (κ is called integral element).

If β denotes a root of $m(x)$, then s is the order of β in the factor group $\mathbb{F}_{q^d}^\times / \mathbb{F}_q^\times$. Therefore,

$$s = \frac{e}{\gcd(q-1, e)}.$$

Primitive and Subprimitive Polynomials

$m(x)$ is called primitive if

$$e = q^d - 1$$

$m(x)$ is called subprimitive if

$$s = \theta_{d-1}(q) = \frac{q^d - 1}{q - 1} = |\mathrm{PG}(d-1, q)|$$

Remarks:

- If $m(x)$ is primitive, multiplication by β is a cyclic collineation of the affine space $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$.
- If $m(x)$ is subprimitive, multiplication by β is a cyclic collineation of the projective space $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$.

Generalizing Hirschfeld's Result

In

$$T^n \mathbf{x}_0 = \kappa \mathbf{x}_0,$$

we need $\kappa = 1$. Thus we need to count subprimitive polynomials with integral element $\kappa = 1$.

Actually, we'll compute the more general counting function

$R_\kappa(d, q) =$ *# of subprimitive polynomials of degree d over* $\mathbb{F}_q$ *with integral element* $\kappa \in \mathbb{F}_q$.

Write $\kappa = \alpha^i$ where α is a primitive element of $\mathbb{F}_q$.

Generalizing Hirschfeld's Result

LEMMA

$$R_\kappa(d,q) = R_{\alpha^i}(d,q) = \begin{cases} \dfrac{g}{\Phi(g)} \cdot \dfrac{\Phi(\theta_{d-1}(q))}{d} & \text{if } \gcd(i,g) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

where $g = \gcd(q-1, \theta_{d-1}(q))$

Remarks:

- The function $R_{\alpha^i}(d,q)$ is periodic in i with period $\gcd(q-1, \theta_{d-1}(q))$.
- The non-zero function values depend only on d and q, but not on i.
- The factor $q-1$ in Hirschfeld's formula is replaced by $\frac{g}{\Phi(g)}$.

Counting Subprimitive Polynomials by Integral Element (IV)

COROLLARY

$$R_\kappa(2,q) = \begin{cases} \frac{1}{2}\Phi(q+1) & \text{for all } \kappa \text{ if } 2 \mid q, \\ \Phi(q+1) & \text{if } 2 \nmid q \text{ and } \kappa \text{ is a nonsquare in } \mathbb{F}_q^\times, \\ 0 & \text{if } 2 \nmid q \text{ and } \kappa \text{ is a square in } \mathbb{F}_q^\times. \end{cases}$$

COROLLARY

$$R_1(2,q) = \begin{cases} \frac{1}{2}\Phi(q+1) & \text{if } 2 \mid q, \\ 0 & \text{if } 2 \nmid q. \end{cases}$$

Cyclic Code Automorphisms

COROLLARY

The codes of length $q^2 + 1$ or $q^3 + 1$ are cyclic iff $2 \mid q$

COROLLARY

The codes of length $q^2 + 1$ for $2 \nmid q$ are not BCH-codes

Remark:
If the codes are cyclic, then they are cyclic in $R_1(2, q)$ many ways.

The Twisted Tensor Product Representation

Let $G \leq \mathrm{P\Gamma L}(n, q^s)$

G acts on $V_n = \mathbb{F}_{q^s}^n$.

G also acts on $\otimes_s V_n$, namely

$$(v_1 \otimes \cdots \otimes v_s, g) \mapsto$$
$$v_1 g \otimes \phi_s(v_2 g) \otimes \phi_s^2(v_3 g) \otimes \cdots \otimes \phi_s^{s-1}(v_s g)$$

This representation can be written over the smaller field $\mathbb{F}_q$

Let ρ denote this representation.

The Twisted Tensor Product Representation

The transformation in $\mathrm{PGL}(2, q^s)$ induced by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (with $ad - bc \neq 0$) becomes the map

$$\varphi_{a,b,c,d} : t \mapsto \frac{at + c}{bt + d}$$

Using the base change matrix S_β from above, we wish to write out the representation explicitly.

The Representation Associated with Theorem 1

$$\rho(\varphi_{a,b,c,d}) = U(a,b,c,d,\beta) = (U_1 \mid U_2 \mid U_3)$$

with U_i as follows (using β a primitive elt of $\mathbb{F}_{q^2}$ and $\delta = 1/(\beta - \beta^q)$ and $\gamma = \beta\delta$)

$$U_1 = \left(\begin{array}{c|c|c}
N_2(d^2) & 4N_2(bd) & N_2(b^2) \\ \hline
N_2(cd) & \begin{array}{c} N_2(ad) \\ +N_2(bc) \\ +T_2(a^q bcd^q) \end{array} & N_2(ab) \\ \hline
N_2(c^2) & 4N_2(ac) & N_2(a^2) \\ \hline
T_2(cd^{2q+1}) & \begin{array}{c} 2T_2(ab^q d^{q+1}) \\ +2T_2(b^{q+1} cd^q) \end{array} & T_2(ab^{2q+1}) \\ \hline
T_2(cd^{2q+1}\beta) & \begin{array}{c} 2T_2(ab^q d^{q+1}\beta) \\ +2T_2(b^{q+1} cd^q \beta) \end{array} & T_2(ab^{2q+1}\beta) \\ \hline
T_2(c^2 d^{2q}) & 4T_2(ab^q cd^q) & T_2(a^2 b^{2q}) \\ \hline
T_2(c^2 d^{2q}\beta) & 4T_2(ab^q cd^q \beta) & T_2(a^2 b^{2q}\beta) \\ \hline
T_2(c^{q+2} d^q) & \begin{array}{c} 2T_2(a^{q+1} cd^q) \\ +2T_2(ab^q c^{q+1}) \end{array} & T_2(a^{q+2} b^q) \\ \hline
T_2(c^{q+2} d^q \beta) & \begin{array}{c} 2T_2(a^{q+1} cd^q \beta) \\ +2T_2(ab^q c^{q+1} \beta) \end{array} & T_2(a^{q+2} b^q \beta)
\end{array}\right)$$

The Representation Associated with Theorem 1

$$U_2 = \left(\begin{array}{c|c|c}
2T_2(b^q d^{q+2}\gamma) & 2T_2(bd^{2q+1}\delta) & T_2(b^{2q}d^2\gamma) \\ \hline
\begin{array}{c} T_2(a^q cd^{q+1}\gamma) \\ +T_2(b^q c^{q+1}d\gamma) \end{array} & \begin{array}{c} T_2(ac^q d^{q+1}\delta) \\ +T_2(bc^{q+1}d^q\delta) \end{array} & T_2(a^q b^q cd\gamma) \\ \hline
2T_2(a^q c^{q+2}\gamma) & 2T_2(ac^{2q+1}\delta) & T_2(a^{2q}c^2\gamma) \\ \hline
\begin{array}{c} 2T_2(b^q cd^{q+1}\gamma) \\ +T_2(a^q d^{q+2}\gamma) \\ +T_2(b^q c^q d^2\gamma) \end{array} & \begin{array}{c} 2T_2(bc^q d^{q+1}\delta) \\ +T_2(ad^{2q+1}\delta) \\ +T_2(bcd^{2q}\delta) \end{array} & \begin{array}{c} T_2(a^q b^q d^2\gamma) \\ +T_2(b^{2q}cd\gamma) \end{array} \\ \hline
\begin{array}{c} 2T_2(b^q cd^{q+1}\beta\gamma) \\ +T_2(a^q d^{q+2}\beta^q\gamma) \\ +T_2(b^q c^q d^2\beta^q\gamma) \end{array} & \begin{array}{c} 2T_2(bc^q d^{q+1}\beta^q\delta) \\ +T_2(ad^{2q+1}\beta\delta) \\ +T_2(bcd^{2q}\beta\delta) \end{array} & \begin{array}{c} T_2(a^q b^q d^2\beta^q\gamma) \\ +T_2(b^{2q}cd\beta\gamma) \end{array} \\ \hline
\begin{array}{c} 2T_2(a^q c^q d^2\gamma) \\ +2T_2(b^q c^2 d^q\gamma) \end{array} & \begin{array}{c} 2T_2(bc^{2q}d\delta) \\ +2T_2(acd^{2q}\delta) \end{array} & \begin{array}{c} T_2(a^{2q}d^2\gamma) \\ +T_2(b^{2q}c^2\gamma) \end{array} \\ \hline
\begin{array}{c} 2T_2(a^q c^q d^2\beta^q\gamma) \\ +2T_2(b^q c^2 d^q\beta\gamma) \end{array} & \begin{array}{c} 2T_2(bc^{2q}d\beta^q\delta) \\ +2T_2(acd^{2q}\beta\delta) \end{array} & \begin{array}{c} T_2(a^{2q}d^2\beta^q\gamma) \\ +T_2(b^{2q}c^2\beta\gamma) \end{array} \\ \hline
\begin{array}{c} 2T_2(a^q c^{q+1}d\gamma) \\ +T_2(a^q c^2 d^q\gamma) \\ +T_2(b^q c^{q+2}\gamma) \end{array} & \begin{array}{c} 2T_2(ac^{q+1}d^q\delta) \\ +T_2(ac^{2q}d\delta) \\ +T_2(bc^{2q+1}\delta) \end{array} & \begin{array}{c} T_2(a^{2q}cd\gamma) \\ +T_2(a^q b^q c^2\gamma) \end{array} \\ \hline
\begin{array}{c} 2T_2(a^q c^{q+1}d\beta^q\gamma) \\ +T_2(a^q c^2 d^q\beta\gamma) \\ +T_2(b^q c^{q+2}\beta\gamma) \end{array} & \begin{array}{c} 2T_2(ac^{q+1}d^q\beta\delta) \\ +T_2(ac^{2q}d\beta^q\delta) \\ +T_2(bc^{2q+1}\beta^q\delta) \end{array} & \begin{array}{c} T_2(a^{2q}cd\beta^q\gamma) \\ +T_2(a^q b^q c^2\beta\gamma) \end{array}
\end{array}\right)$$

The Representation Associated with Theorem 1

$$U_3 = \left(\begin{array}{c|c|c}
T_2(b^2d^{2q}\delta) & 2T_2(b^{2q+1}d\gamma) & 2T_2(b^{q+2}d^q\delta) \\ \hline
T_2(abc^qd^q\delta) & \begin{array}{c} T_2(a^{q+1}b^qd\gamma) \\ +T_2(a^qb^{q+1}c\gamma) \end{array} & \begin{array}{c} T_2(ab^{q+1}c^q\delta) \\ +T_2(a^{q+1}bd^q\delta) \end{array} \\ \hline
T_2(a^2c^{2q}\delta) & 2T_2(a^{2q+1}c\gamma) & 2T_2(a^{q+2}c^q\delta) \\ \hline
\begin{array}{c} T_2(b^2c^qd^q\delta) \\ +T_2(abd^{2q}\delta) \end{array} & \begin{array}{c} 2T_2(a^qb^{q+1}d\gamma) \\ +T_2(ab^{2q}d\gamma) \\ +T_2(b^{2q+1}c\gamma) \end{array} & \begin{array}{c} 2T_2(ab^{q+1}d^q\delta) \\ +T_2(a^qb^2d^q\delta) \\ +T_2(b^{q+2}c^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(b^2c^qd^q\beta^q\delta) \\ +T_2(abd^{2q}\beta\delta) \end{array} & \begin{array}{c} 2T_2(a^qb^{q+1}d\beta^q\gamma) \\ +T_2(ab^{2q}d\beta\gamma) \\ +T_2(b^{2q+1}c\beta\gamma) \end{array} & \begin{array}{c} 2T_2(ab^{q+1}d^q\beta\delta) \\ +T_2(a^qb^2d^q\beta^q\delta) \\ +T_2(b^{q+2}c^q\beta^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(a^2d^{2q}\delta) \\ +T_2(b^2c^{2q}\delta) \end{array} & \begin{array}{c} 2T_2(a^{2q}bd\gamma) \\ +2T_2(ab^{2q}c\gamma) \end{array} & \begin{array}{c} 2T_2(a^qb^2c^q\delta) \\ +2T_2(a^2b^qd^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(a^2d^{2q}\beta\delta) \\ +T_2(b^2c^{2q}\beta^q\delta) \end{array} & \begin{array}{c} 2T_2(a^{2q}bd\beta^q\gamma) \\ +2T_2(ab^{2q}c\beta\gamma) \end{array} & \begin{array}{c} 2T_2(a^qb^2c^q\beta^q\delta) \\ +2T_2(a^2b^qd^q\beta\delta) \end{array} \\ \hline
\begin{array}{c} T_2(abc^{2q}\delta) \\ +T_2(a^2c^qd^q\delta) \end{array} & \begin{array}{c} 2T_2(a^{q+1}b^qc\gamma) \\ +T_2(a^{2q+1}d\gamma) \\ +T_2(a^{2q}bc\gamma) \end{array} & \begin{array}{c} 2T_2(a^{q+1}bc^q\delta) \\ +T_2(a^{q+2}d^q\delta) \\ +T_2(a^2b^qc^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(abc^{2q}\beta^q\delta) \\ +T_2(a^2c^qd^q\beta\delta) \end{array} & \begin{array}{c} 2T_2(a^{q+1}b^qc\beta\gamma) \\ +T_2(a^{2q+1}d\beta^q\gamma) \\ +T_2(a^{2q}bc\beta^q\gamma) \end{array} & \begin{array}{c} 2T_2(a^{q+1}bc^q\beta^q\delta) \\ +T_2(a^{q+2}d^q\beta\delta) \\ +T_2(a^2b^qc^q\beta\delta) \end{array}
\end{array}\right)$$

The End

Thank you

for your attention

References

Anton Betten: Twisted Tensor Product Codes, Designs, Codes, Cryptography 47 (2008), 191-219.

A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann: Error-Correcting Linear Codes, Classification by Isometry and Applications, 2006.

V. Pless, C. Huffman. The yellow book.

Antonio Cossidente, Oliver King: Twisted Tensor product group embeddings and complete partial ovoids on quadrics in $\mathrm{PG}(2^t - 1, q)$. J. Algebra 273 (2004) 854-868.