Some Remarks on Optimal Codes

Anton Betten

Department of Mathematics
Colorado State University

August 3, 2007
Abstract

When is a code useful? Certainly, the information rate should be high, and the error correction capabilities should be good. But the complexity of encoding and decoding plays a role as well. Optimal linear codes maximize the minimum distance given the length and dimension and the size of the defining field (and have been studied for quite some time).

In this talk, we discuss two families of optimal linear codes which have the additional property that they are invariant under large automorphism groups (which may be used do devise efficient decoding algorithms).

The two types of codes are obtained by tensor twisting an oval in the plane with respect to a quadratic subfield, and by tensor twisting the projective line with respect to a cubic subfield (respectively). Relations to other, previously known codes are discussed as well.
When is a code useful?

1. High information rate,
2. High error correction rate,
3. Easy to encode and decode.

Linear codes are very easy to encode:

$$x \mapsto x \cdot G$$

$x$ is row vector of length $k$, $G$ is a $k \times n$ matrix over $\mathbb{F}_q$.

We say, the code is an $[n, k, d]_q$ code if in addition the minimum distance is $d$. 
Goals for linear codes:

1. Information rate $k/n$ should be large
2. Error correction rate $d/n$ should be large
3. Automorphism group should be big

Optimizing $k/n$ and $d/n$ at the same time are contradicting aims. This is the packing problem of combinatorics:
The Packing Problem

Here, big and small stands for high or low minimum distance, resp. Many and few stand for high and low information rate, resp.
Optimal Linear Codes

An \([n, k, d]_q\)-code \(C\) is \textit{optimal} if there is no \([n, k, D]_q\) code with \(D > d\).

An \([n, k, d]_q\)-code \(C\) is \textit{best known} if no \([n, k, D]_q\) code with \(D > d\) is known.

Use database http://www.codetables.de to look up the best known codes (Markus Grassl, Andries Brouwer)

These tables do not classify codes up to isometry
Isometry and Automorphism

We consider 3 types of isometries. They give rise to three types of automorphism groups.

- $\text{PAut} = \text{permutational automorphisms (coordinate permutations, } \text{Sym}_n \text{ action)}$
- $\text{MAut} = \text{PAut} + \text{multiplication of coordinates by non-zero field elements (monomial group } M_n(q) \text{ action)}$
- $\Gamma \text{ Aut} = \text{MAut} + \text{field automorphisms (simultaneously for all coordinates)}$

$$\text{PAut}(C) \leq \text{MAut}(C) \leq \Gamma \text{Aut}(C)$$
Frobenius, Trace and Norm maps

In the following, \( q \) will always denote a prime power.

- The Frobenius automorphism of \( \mathbb{F}_{q^r} \) over \( \mathbb{F}_q \):
  \[
  \phi_r : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}, \ x \mapsto x^q
  \]

- The Trace map from \( \mathbb{F}_{q^r} \) to \( \mathbb{F}_q \):
  \[
  T_r : \mathbb{F}_{q^r} \to \mathbb{F}_q, \ x \mapsto \sum_{i=0}^{r-1} \phi_r^i(x)
  \]

- The Norm map from \( \mathbb{F}_{q^r} \) to \( \mathbb{F}_q \):
  \[
  N_r : \mathbb{F}_{q^r} \to \mathbb{F}_q, \ x \mapsto \prod_{i=0}^{r-1} \phi_r^i(x)
  \]
Cyclic and constacyclic codes

Let $\sigma_n = (1, 2, \ldots, n)$ be an $n$-cycle in $\text{Sym}_n$.

A code $C$ is cyclic if it is permutational equivalent to a code $D = C^\pi$ with $\sigma_n \in \text{PAut}(C)$.

Let $\gamma \in \mathbb{F}_q^\times$ Let $f_\gamma : \{1, \ldots, n\} \rightarrow \mathbb{F}_q^\times$ with

$$f_\gamma(i) = \begin{cases} 
\gamma & \text{if } i = n, \\
1 & \text{otherwise}.
\end{cases}$$

A code $C$ is constacyclic if it is permutational equivalent to a code $D = C^\pi$ with $(\sigma_n, f_\gamma) \in \text{MAut}(C)$ for some $\gamma \in \mathbb{F}_q^\times$. 
The Automorphism group comes together with a representation in $GL(k, q)$

Let $C$ have generator matrix $G$ over $\mathbb{F}_{q^r}$

Let $M \in \text{MAut}(C) \leq M_n(q)$ be a monomial automorphism of $C$

Since $M$ takes the vector space $C$ to itself (as a whole), we can find $A = A(M) \in GL(k, q)$ such that

$$A \cdot G \cdot M = G.$$

The map $M \rightarrow A(M)$ is a homomorphism.

A similar result holds for $\Gamma\text{Aut}(C)$ (with $\Gamma L$ instead of $GL$)
Example: the Hexacode

Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ where $\omega^2 = \omega + 1$.

For sake of simplicity, we write $2\hat{=}\omega$ and $3\hat{=}\omega^2$.

Consider the $[6, 3, 4]_4$ code generated by

$$
G = \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 \\
3 & 2 & 1 & 0 & 1 & 0 \\
2 & 3 & 1 & 0 & 0 & 1
\end{pmatrix}
$$
Example: the Hexacode

The automorphism group has order 168 and is generated by

<table>
<thead>
<tr>
<th>$f$</th>
<th>$A(f)$</th>
<th>$f$</th>
<th>$A(f)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1,4,3,2,6)$</td>
<td>$\begin{pmatrix} 1 &amp; 2 &amp; 3 \ 0 &amp; 0 &amp; 1 \ 2 &amp; 2 &amp; 2 \end{pmatrix}$</td>
<td>$(3,4,5,6), \phi_2$</td>
<td>$\begin{pmatrix} 3 &amp; 0 &amp; 0 \ 0 &amp; 2 &amp; 0 \ 3 &amp; 2 &amp; 1 \end{pmatrix}$</td>
</tr>
<tr>
<td>$(1,3,5)$</td>
<td>$\begin{pmatrix} 1 &amp; 3 &amp; 2 \ 0 &amp; 1 &amp; 0 \ 3 &amp; 0 &amp; 0 \end{pmatrix}$</td>
<td>$(4,5), \phi_2$</td>
<td>$\begin{pmatrix} 2 &amp; 0 &amp; 0 \ 0 &amp; 3 &amp; 0 \ 0 &amp; 0 &amp; 1 \end{pmatrix}$</td>
</tr>
<tr>
<td>$(2,5,3)$</td>
<td>$\begin{pmatrix} 3 &amp; 0 &amp; 0 \ 0 &amp; 0 &amp; 2 \ 2 &amp; 1 &amp; 3 \end{pmatrix}$</td>
<td>$(5,6), \phi_2$</td>
<td>$\begin{pmatrix} 3 &amp; 0 &amp; 0 \ 0 &amp; 3 &amp; 0 \ 0 &amp; 0 &amp; 3 \end{pmatrix}$</td>
</tr>
</tbody>
</table>
Example: the Code $S_{18}$ of MacWilliams, Odlyzko, Sloane, Ward (JCT-A 1978)

Consider the $[18, 9, 8]_4$ code generated by

$$
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 3 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 3 & 1 & 1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
3 & 2 & 2 & 1 & 0 & 0 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
2 & 3 & 2 & 0 & 1 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
2 & 1 & 3 & 3 & 2 & 1 & 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 2 & 3 & 2 & 3 & 1 & 2 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 2 & 0 & 0 & 3 & 3 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$

The code is formally self-dual (b/c its dual is $\phi_2(C)$, its “complex conjugate”, and conjugation preserves weights).

Its automorphism group is $\text{PGL}(2, 16)$.
Example: the Automorphism group of $S_{18}$

generated by
\[(4, 7)(5, 8)(6, 9)(11, 14)(12, 15)(13, 18),\]
\[(4, 14, 7, 11)(5, 15, 8, 12)(6, 18, 9, 13)(16, 17),\]
\[(3, 6, 9, 13)(4, 5)(7, 17, 12, 14)(8, 16, 11, 15),\]
\[(3, 17, 16)(4, 13, 5, 7, 18, 8)(6, 14, 12, 9, 11, 15),\]
\[(2, 12, 7, 14)(3, 4, 15, 6)(5, 13, 16, 8)(9, 11),\]
\[(2, 4, 5)(3, 14, 8)(6, 16, 7)(9, 17, 11)(12, 13, 15),\]
\[(1, 8, 4, 12)(2, 7, 5, 11)(3, 9, 6, 13)(14, 15),\]
\[(1, 17, 14, 15, 9, 6, 16, 2, 12, 11, 13, 18)(3, 7)(4, 8, 5)\]

orbits on the columns:

\[\{1, 12, 18, 15, 8, 17, 14, 2, 4, 13, 6, 7, 5, 11, 16, 3, 9\}, \{10\}\]
Example: the Automorphism group of $S_{18}$

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}, \ldots, \\
\begin{bmatrix}
3 & 3 & 2 & 0 & 0 & 1 & 1 & 1 & 3 \\
2 & 3 & 1 & 1 & 2 & 3 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\
3 & 2 & 3 & 0 & 1 & 0 & 1 & 3 & 1 \\
\end{bmatrix}.
\]

Q: How can $\mathrm{PGL}(2, 16)$ act on a code defined over $\mathbb{F}_4$ ?
A: the twisted tensor product action
THEOREM 1:
A) $\exists$ constacyclic $[q^2 + 1, q^2 - 8, \geq 6]_q$ any $q \geq 3$
B) $\exists [q^2 + 2, q^2 - 7, \geq 6]_q$ codes any $q \geq 4$ even

In both case, $\Gamma \text{Aut} = P\Gamma L(2, q^2)$, and $P\Gamma L_2(2, q^2) \leq M\text{Aut}$

Only the codes of length $q^2 + 1$ for $q$ even are cyclic.

REMARK:
B) for $q = 4$ gives the $[18, 9, 8]_4$ code $S_{18}$ from above
2 Families of Codes

THEOREM 2:
\[ \exists \text{ constacyclic } [q^3 + 1, q^3 - 7, \geq 5]_q \text{ any } q \geq 3 \]
\[ \Gamma \text{Aut} = \text{PGL}(2, q^3), \]
\[ \text{PGL}_3(2, q^3) \leq \text{MAut} \]
The codes are cyclic if and only if \( q \) is even.

REMARK:
The codes from THM 1-2 are often optimal or best known.
The Construction

Let \( V_n = \mathbb{F}^n_{q^t} \) be an \( n \)-dimensional vector space over \( \mathbb{F}_{q^t} \).

Consider
\[
\otimes_t V_n := V_n \otimes V_n \otimes \cdots \otimes V_n \text{ (} t \text{ times)}
\]

Define a mapping
\[
\iota_t : V_n \rightarrow \otimes_t V_n, \quad x \mapsto x \otimes \phi_t(x) \otimes \phi_t^2(x) \otimes \cdots \otimes \phi_t^{t-1}(x).
\]

This induces a mapping between the corresponding projective spaces:
\[
\iota_t : \mathbb{P}(V_n) \rightarrow \mathbb{P}(\otimes_t V_n) : \mathbb{P}(x) \leftrightarrow \mathbb{P}(\iota_t(x)).
\]
Projective Codes

\[ \left\{ \text{isometry classes of projective code} \right\} \leftrightarrow \left\{ \text{equivalence classes of } n \text{ points in projective space} \right\} \]

Often, a \([n, k]_q\) code can be identified with a set of \(n\) points in \(\text{PG}(k - 1, q)\).

The columns of the generator matrix are the homogeneous coordinates of the \(n\) points.

Conversely, \(n\) points in \(\text{PG}(k - 1, q)\) may be considered as generating a code.

The property “minimum distance \(\geq d\)” corresponds to the geometric property “any \(d - 1\) points are independent”
The Construction

The Veronese map $\nu_t : \text{PG}(1, q) \rightarrow \text{PG}(t - 1, q)$

$$\mathbf{P}(a, b) \mapsto \mathbf{P}(a^t, a^{t-1}b, \ldots, b^t)$$

$\iota_2 \circ \nu_3(\text{PG}(1, q^2))$ gives a set of $n = q^2 + 1$ points in $\text{PG}(8, q^2)$
Since it is a twisted tensor product image, it lies in a $\text{PG}(8, q)$ subfield subspace.
This gives the codes of THM 1 of length $n = q^2 + 1$.
For length $n = q^2 + 2$, add the nucleus to the image $\nu_3(\text{PG}(1, q^2))$

$\nu_3(\text{PG}(1, q^3))$ gives a set of $n = q^3 + 1$ points in $\text{PG}(7, q^2)$
The Twisted Tensor Product Action

Let $G \leq \text{PGL}(n, q^t)$

$G$ acts on $V_n$.

$G$ also acts on $\otimes_t V_n$, namely

$$(v_1 \otimes \cdots \otimes v_t, g) \mapsto v_1 g \otimes \phi_t(v_2 g) \otimes \phi_t^2(v_3, g) \otimes \cdots \otimes \phi_t^{t-1}(v_t g)$$

Let $\rho(G)$ denote this action.
They are not BCH codes

There are BCH-codes with the same parameters as the codes of length $q^2 + 1$ and $q^3 + 1$

Q: are the codes from THM 1-2 BCH-codes?

A: No, since the codes from THM 1-2 are rarely cyclic whereas BCH-code are cyclic.
When are they cyclic?

There are BCH-codes with the same parameters as the codes of length $q^2 + 1$ and $q^3 + 1$

EXAMPLE:
For $n = q^2 + 1$, take the cyclotomic sets mod $q^2 + 1$ containing the consecutive set $-2, -1, 0, 1, 2$:
{0}
{1, $q$, $q^2$ $\equiv$ $-1$, $-q$, $-q^2$ $\equiv$ $1$}
{2, $2q$, $2q^2$ $\equiv$ $-2$, $-2q$, $-2q^2$ $\equiv$ $2$}
That is $1 + 4 + 4 = 9$ roots.
The dual code is a $[q^2 + 1, q^2 + 1 - 9, \geq 6]_q$ code.
(minimum distance $\geq 6$ b/c we have a consecutive set of size 5)
When are they cyclic?

Q: are the codes from THM 1-2 BCH-codes?

A: No, since the codes from THM 1-2 are rarely cyclic whereas BCH-code are cyclic.
Cyclic Collineations

\[ \varphi_{a, b, c, d} : x \mapsto \frac{ax + d}{bx + d} \in \text{PGL}(2, q) \iff ad - bc \neq 0. \]

More generally if \( m(x) = x^{n+1} + c_n x^n + \cdots + c_0 \in \mathbb{F}_q[x] \) and \( c = (c_1, \ldots, c_n) \) then

\[ T_m := \begin{pmatrix} 0_n & -c_0 \\ l_n & -c \end{pmatrix} \]

induces a collineation whose characteristic polynomial is \( m(x) \) iff \( c_0 \neq 0. \)

Q: When is such a collineation cyclic?
Exponent and Subexponent

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

$\text{Exp}(m) = \text{smallest positive integer } e \text{ such that } m(x) \text{ divides } x^e - 1$

$\text{Subexp}(m) = \text{smallest positive integer } s \text{ such that } m(x) \text{ divides } x^s - c \text{ for some } c \in \mathbb{F}_q \text{ (c is called integral element)}.$

$$\text{Subexp}(m) = \frac{\text{Exp}(m)}{\gcd(q - 1, \text{Exp}(m))}.$$ 

b/c if $\beta$ is a root of $m(x)$ in $\mathbb{F}_{q^d}$ then $s$ is the order of $\beta \mathbb{F}_q^\times$ in the factor group $\mathbb{F}_{q^d}^\times / \mathbb{F}_q^\times$. 
Cyclic Collineations

We wish to determine the collineations which permute the
\[ \theta_d(q) := \frac{q^d - 1}{q - 1} \]
points of \( \text{PG}(d - 1, q) \) in one cycle (a.k.a. Singer cycle)

\[ m(x) \] is called primitive if \( \exp(m) = q^d - 1 \)

\[ m(x) \] is called subprimitive if \( \text{Subexp}(m) = \theta_{d-1}(q) \)

**LEMMA:** (Hirschfeld 1973)

\# cyclic projectivities of \( \text{PG}(n, q) \)

\[ = \# \text{ subprimitive polynomials of degree } d \text{ over } \mathbb{F}_q \]

\[ = (q - 1) \frac{\Phi(\theta_d(q))}{d} \] (with \( \Phi \) Euler’s totient function)
Cyclic Code Automorphisms

For projective codes, the situation is as follows:

\[
\begin{align*}
\{ \text{cyclic collineation} \} & \iff \{ \text{constacyclic code} \} \\
\{ \text{cyclic collineation} \} & \iff \{ \text{cyclic code} \}
\end{align*}
\]

Let \( \mathcal{R}_c(d, q) \) be the set of monic irreducible polynomials of degree \( d \) over \( \mathbb{F}_q \) with integral element \( c \in \mathbb{F}_q \).

Let \( R_c(d, q) = \# \mathcal{R}_c(d, q) \).
**LEMMA:**
Let $c = \alpha^i$ with $\alpha$ a primitive element of $\mathbb{F}_q$. Let

$$\theta_{d-1}(q) = \prod_{i=1}^{r} p_i^{e_i}$$

be the factorization of $\theta_{d-1}(q)$ into powers of distinct primes. Then $R_{\alpha^i}(d, q) =

\begin{align*}
\begin{cases}
\frac{1}{d} \left( \prod_{j=1}^{r} p_j^{e_j} \right) \cdot \Phi \left( \prod_{j=1}^{r} p_j^{e_j} \right) & \text{if } \gcd(i, q - 1, \theta_{d-1}(q)) = 1, \\
0 & \text{otherwise}.
\end{cases}
\end{align*}

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 $i$. 
Counting Irreducible Polynomials by Integral Element

COROLLARY:

\[
R_c(2, q) = \begin{cases} 
  \frac{1}{2} \Phi(q + 1) & \text{for all } c \text{ if } q \text{ is even}, \\
  \frac{2}{\Phi(q + 1)} & \text{if } q \text{ is odd and } c \text{ is a nonsquare in } \mathbb{F}_q, \\
  0 & \text{if } q \text{ is odd and } c \text{ is a nonzero square in } \mathbb{F}_q.
\end{cases}
\]

COROLLARY:

\[
R_1(2, q) = \begin{cases} 
  \frac{1}{2} \Phi(q + 1) & \text{if } q \text{ is even}, \\
  0 & \text{if } q \text{ is odd}.
\end{cases}
\]
COROLLARY:
The codes of length $q^2 + 1$ or $q^3 + 1$ are cyclic iff $q$ is even

COROLLARY:
The codes of length $q^2 + 1$ or $q^3 + 1$ for odd $q$ are not BCH-codes

NOTE:
If the codes are cyclic, then they are cyclic in $R_1(2, q)$ many ways.
The Representation Associated with Theorem 1

\[ \varphi_{a,b,c,d} \mapsto U(a, b, c, d, \beta) = (U_1 \mid U_2 \mid U_3) \]

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

\[
U_1 = \begin{pmatrix}
N_2(d^2) & 4N_2(bd) & N_2(b^2) \\
N_2(cd) & N_2(ad) + N_2(bc) + T_2(a^q bcd^q) & N_2(ab) \\
N_2(c^2) & 4N_2(ac) & N_2(a^2) \\
T_2(cd^{2q+1}) & 2T_2(ab^q d^{q+1}) + 2T_2(b^{q+1} cd^q) & T_2(ab^{2q+1}) \\
T_2(cd^{2q+1} \beta) & 2T_2(ab^q d^{q+1} \beta) + 2T_2(b^{q+1} cd^q \beta) & T_2(ab^{2q+1} \beta) \\
T_2(c^2d^{2q}) & 4T_2(ab^q cd^q) & T_2(a^2 b^{2q}) \\
T_2(c^2d^{2q} \beta) & 4T_2(ab^q cd^q \beta) & T_2(a^2 b^{2q} \beta) \\
T_2(c^{q+2} d^q) & 2T_2(a^{q+1} cd^q) + 2T_2(ab^q c^{q+1}) & T_2(a^{q+2} b^q) \\
T_2(c^{q+2} d^q \beta) & 2T_2(a^{q+1} cd^q \beta) + 2T_2(ab^q c^{q+1} \beta) & T_2(a^{q+2} b^q \beta)
\end{pmatrix}
\]
The Representation Associated with Theorem 1

\[ U_2 = \begin{pmatrix}
2T_2(b^q d^{q+2} \gamma) & 2T_2(bd^{2q+1} \delta) & T_2(b^{2q} d^2 \gamma) \\
T_2(a^q cd^{q+1} \gamma) + T_2(b^q c^{q+1} d \gamma) & T_2(ac^{q+1} d^q \delta) + T_2(bc^{q+1} d^q \delta) & T_2(a^q b^q cd \gamma) \\
2T_2(a^q c^{q+2} \gamma) & T_2(ac^{q+1} \delta) + T_2(bc^{q+1} d^q \delta) & T_2(a^q c^2 \gamma) \\
2T_2(b^q cd^{q+1} \gamma) + T_2(a^q d^{q+2} \gamma) + T_2(b^q c^q d^2 \gamma) & 2T_2(bc^{q+2} d^q \delta) + T_2(acd^{2q} \delta) + T_2(b^q cd^2 \beta \gamma) & T_2(a^q b^q d^2 \beta \gamma) + T_2(b^q cd \beta \gamma) \\
2T_2(a^q c^q d^2 \beta \gamma) + 2T_2(b^q c^2 d^q \gamma) & 2T_2(b^2q d \delta) + 2T_2(acd^{2q} \delta) + T_2(b^2q c^2 \beta \gamma) & T_2(a^q d^2 \beta \gamma) + T_2(b^2q c^2 \beta \gamma) \\
2T_2(a^q c^q d^2 \beta \gamma) + 2T_2(b^q c^2 d^q \beta \gamma) & 2T_2(b^2q d \delta) + 2T_2(acd^{2q} \beta \delta) + T_2(b^2q c^2 \beta \gamma) & T_2(a^q d^2 \beta \gamma) + T_2(b^2q c^2 \beta \gamma) \\
2T_2(a^q c^{q+1} d \gamma) + T_2(a^q c^2 d^q \gamma) + T_2(b^q c^{q+2} \gamma) & 2T_2(ac^{q+1} d^q \delta) + T_2(acd^{2q} \delta) + T_2(bc^{q+1} d^q \delta) & T_2(a^q c d \gamma) + T_2(a^q b^q c \beta \gamma) \\
2T_2(a^q c^{q+1} d \beta \gamma) + T_2(a^q c^2 d^q \beta \gamma) + T_2(b^q c^{q+2} \beta \gamma) & 2T_2(ac^{q+1} d^q \beta \delta) + T_2(acd^{2q} \beta \delta) + T_2(bc^{q+1} \beta \delta) & T_2(a^q c d \beta \gamma) + T_2(a^q b^q c^2 \beta \gamma)
\end{pmatrix} \]
The Representation Associated with Theorem 1

\[
U_3 = 
\begin{pmatrix}
T_2(b^2 d^{2q}\beta) & 2T_2(b^{2q+1}d\gamma) & 2T_2(b^{q+2}d^q\delta) \\
T_2(a b c^q d^q\delta) & T_2(a^q b^q d\gamma) + T_2(a^q b^q c\gamma) & T_2(ab^{q+1}c^q\delta) + T_2(a^{q+1}b d^q\delta) \\
T_2(a^2 c^{2q}\delta) & 2T_2(a^{2q+1}c\gamma) & 2T_2(a^{q+2}c^q\delta) \\
T_2(b^2 c^q d^q\delta) + T_2(ab d^{2q}\delta) & 2T_2(a^q b^{q+1}d\gamma) + T_2(ab^{q+1}d\gamma) + T_2(a^q b^2 d^q\delta) + T_2(b^{q+2}c^q\delta) \\
T_2(a^2 d^{2q}\delta) + T_2(b^2 c^{2q}\delta) & 2T_2(a^2 b d\gamma) + 2T_2(ab^2 c\gamma) & 2T_2(a^q b^2 c^q\delta) + 2T_2(a^2 b^q d^q\delta) \\
T_2(a^2 d^{2q}\beta) + T_2(b^2 c^{2q}\beta) & 2T_2(a^q b d\beta) + 2T_2(ab^2 c\beta) & 2T_2(a^q b^2 c^q\beta) + 2T_2(a^2 b^q d^q\beta) \\
T_2(a b c^{2q}\delta) + T_2(a^2 c^q d^q\delta) & 2T_2(a^{q+1}b^q c\gamma) + T_2(a^{q+1}d\gamma) + T_2(a^{q+2}d^q\delta) + T_2(a^2 b^q c^q\delta) \\
T_2(a b c^{2q}\beta\delta) + T_2(a^2 c^q d^q\beta\delta) & 2T_2(a^{q+1}b^q c\beta\gamma) + T_2(a^{q+1}d\beta\gamma) + T_2(a^{q+2}d^q\beta\delta) + T_2(a^2 b^q c^q\beta\delta)
\end{pmatrix}
\]
The Representation Associated with Theorem 2

\[ \varphi_{a,b,c,d} \mapsto U(a, b, c, d, \beta) = (U_1 \mid U_2) \cdot \text{diag}(1, 1, \delta_1, \delta_1, \delta_1, \delta_2, \delta_2, \delta_2) \]

with \( U_i \) as follows (using \( \beta \) a primitive elt of \( \mathbb{F}_{q^3} \))

\[
U_1 = \begin{pmatrix}
N_3(d) & N_3(b) & T_3(m_{dbd} \gamma_3) & T_3(m_{dbd} \gamma_4) \\
N_3(c) & N_3(a) & T_3(m_{cac} \gamma_3) & T_3(m_{cac} \gamma_4) \\
T_3(m_{ddc}) & T_3(m_{bba}) & T_3(\eta_{1,1} \gamma_3) & T_3(\eta_{1,1} \gamma_4) \\
T_3(m_{ddc} \beta) & T_3(m_{bba} \beta) & T_3(\eta_{1,2} \gamma_3) & T_3(\eta_{1,2} \gamma_4) \\
T_3(m_{ddc} \beta^2) & T_3(m_{bba} \beta^2) & T_3(\eta_{1,3} \gamma_3) & T_3(\eta_{1,3} \gamma_4) \\
T_3(m_{dcc}) & T_3(m_{baa}) & T_3(\zeta_{1,1} \gamma_3) & T_3(\zeta_{1,1} \gamma_4) \\
T_3(m_{dcc} \beta_{11}) & T_3(m_{baa} \beta_{11}) & T_3(\zeta_{1,2} \gamma_3) & T_3(\zeta_{1,2} \gamma_4) \\
T_3(m_{dcc} \beta_{22}) & T_3(m_{baa} \beta_{22}) & T_3(\zeta_{1,3} \gamma_3) & T_3(\zeta_{1,3} \gamma_4)
\end{pmatrix}
\]
The Representation Associated with Theorem 2

\[ U_2 = \begin{pmatrix}
T_3(m_{dbh} \gamma 5) & T_3(m_{bbd} \gamma 6) & T_3(m_{bbd} \gamma 7) & T_3(m_{bbd} \gamma 8) \\
T_3(m_{cac} \gamma 5) & T_3(m_{aac} \gamma 6) & T_3(m_{aac} \gamma 7) & T_3(m_{aac} \gamma 8) \\
T_3(\eta_{1,1} \gamma 5) & T_3(\eta_{2,1} \gamma 6) & T_3(\eta_{2,1} \gamma 7) & T_3(\eta_{2,1} \gamma 8) \\
T_3(\eta_{1,2} \gamma 5) & T_3(\eta_{2,2} \gamma 6) & T_3(\eta_{2,2} \gamma 7) & T_3(\eta_{2,2} \gamma 8) \\
T_3(\eta_{1,3} \gamma 5) & T_3(\eta_{2,3} \gamma 6) & T_3(\eta_{2,3} \gamma 7) & T_3(\eta_{2,3} \gamma 8) \\
T_3(\zeta_{1,1} \gamma 5) & T_3(\zeta_{2,1} \gamma 6) & T_3(\zeta_{2,1} \gamma 7) & T_3(\zeta_{2,1} \gamma 8) \\
T_3(\zeta_{1,2} \gamma 5) & T_3(\zeta_{2,2} \gamma 6) & T_3(\zeta_{2,2} \gamma 7) & T_3(\zeta_{2,2} \gamma 8) \\
T_3(\zeta_{1,3} \gamma 5) & T_3(\zeta_{2,3} \gamma 6) & T_3(\zeta_{2,3} \gamma 7) & T_3(\zeta_{2,3} \gamma 8)
\end{pmatrix}, \]
The Representation Associated with Theorem 2

with

\[
\begin{pmatrix}
\eta_{1,1} & \eta_{1,2} & \eta_{1,3} \\
\eta_{2,1} & \eta_{2,2} & \eta_{2,3}
\end{pmatrix}
= 
\begin{pmatrix}
m_{dbc} & m_{dad} & m_{cbd} \\
m_{bbc} & m_{bad} & m_{abd}
\end{pmatrix}
\begin{pmatrix}
1 & \beta & \beta_2 \\
1 & \beta_{10} & \beta_{20} \\
1 & \beta_{100} & \beta_{200}
\end{pmatrix},
\]

\[
\begin{pmatrix}
\zeta_{1,1} & \zeta_{1,2} & \zeta_{1,3} \\
\zeta_{2,1} & \zeta_{2,2} & \zeta_{2,3}
\end{pmatrix}
= 
\begin{pmatrix}
m_{dac} & m_{cad} & m_{cbc} \\
m_{bac} & m_{aad} & m_{abc}
\end{pmatrix}
\begin{pmatrix}
1 & \beta_{11} & \beta_{22} \\
1 & \beta_{110} & \beta_{220} \\
1 & \beta_{101} & \beta_{202}
\end{pmatrix},
\]

\(\gamma_3 = \beta_{102} - \beta_{201}, \gamma_4 = \beta_{200} - \beta_2, \gamma_5 = \beta - \beta_{100},\)

\(\gamma_6 = \beta_{123} - \beta_{213}, \gamma_7 = \beta_{202} - \beta_{22}, \gamma_8 = \beta_{11} - \beta_{101},\)

\(\delta_1 = 1 / (T_3(\beta_{21} - \beta_{12})),\)

\(\delta_2 = 1 / (T_3(\beta_{123} - \beta_{132})),\)

using the conventions that \(m_{xyz} = x^{q^2} y^q z, \beta_{ijk} = \beta_i q^2 + jq + k,\)

\(\beta_{jk} = \beta_{0jk}, \text{ and } \beta_k = \beta_{00k}.\)
Further Reading

Anton Betten: Twisted Tensor Product Codes, to appear in Designs, Codes, Cryptography.