Twisted Tensor Product Codes

Anton Betten

Department of Mathematics
Colorado State University

October, 2007

Abstract

Two families of constacyclic codes with large automorphism groups will be presented.

They are obtained from the twisted tensor product construction.

Coincidentally, the smallest nontrivial member of the first family is the quaternary self-orthogonal code S18 discussed by MacWilliams, Odlyzko, Sloane, and Ward in 1978.

References

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

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.

THEOREM 1

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

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

In both case, $\Gamma\mathrm{Aut} = \mathrm{P\Gamma L}(2, q^2)$, and $\mathrm{P\Gamma_2 L}(2, q^2) \leq \mathrm{MAut}$

(throughout, q denotes a prime power)

$\mathrm{PAut} \leq \mathrm{MAut} \leq \Gamma\mathrm{Aut}$ (as in Pless / Huffman)

Example

B) for $q = 4$ gives the $[18, 9, 8]_4$ code S_{18} of MacWilliams, Odlyzko, Sloane, Ward (JCT-A 1978).

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

Here, 2 and 3 denote ω and ω^2 in $\mathbb{F}_4$, respectively. ϕ_2 is the Frobenius Automorphism of $\mathbb{F}_4$ over $\mathbb{F}_2$.

The code is formally self-dual (b/c its dual is $\phi_2(S_{18})$, its “complex conjugate”, and conjugation preserves weights).

The Automorphism group of S_{18}

Its automorphism group is $\mathrm{P\Gamma L}(2, 16)$

orbit structure: $17 + 1$

Q: How can $\mathrm{P\Gamma L}(2, 16)$ act on a code defined over $\mathbb{F}_4$?
A: the twisted tensor product action (see below)

THEOREM 2

$\exists$ constacyclic $[q^3+1, q^3-7, \geq 5]_q$ any $q \geq 3$

$\Gamma\mathrm{Aut} = \mathrm{P\Gamma L}(2, q^3)$,

$\mathrm{P\Gamma_3 L}(2, q^3) \leq \mathrm{MAut}$

The codes are cyclic if and only if q is even.

The Construction

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

Consider
$\otimes_t V_n := V_n \otimes V_n \otimes \cdots \otimes V_n$ (t times)

Define a mapping

$$\begin{aligned} \iota_t : V_n &\rightarrow \otimes_t V_n, \\ x &\mapsto x \otimes \phi_t(x) \otimes \phi_t^2(x) \otimes \cdots \otimes \phi_t^{t-1}(x). \end{aligned}$$

This induces a mapping between the corresponding projective spaces:

$$\iota_t : \mathbf{P}(V_n) \rightarrow \mathbf{P}(\otimes_t V_n) : \ \mathbf{P}(x) \mapsto \mathbf{P}(\iota_t(x)).$$

Projective Codes

$$\left\{ \begin{array}{c} \text{isometry classes} \\ \text{of projective code} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{equivalence classes of} \\ n \text{ points in projective space} \end{array} \right\}$$

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

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

Conversely, n points in $\mathrm{PG}(k-1, q)$ 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 $\nu_t : \mathrm{PG}(1, q) \to \mathrm{PG}(t-1, q)$

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

$\iota_2 \circ \nu_3(\mathrm{PG}(1, q^2))$ gives a set of $n = q^2 + 1$ points in $\mathrm{PG}(8, q^2)$
Since it is a twisted tensor product image, it lies in a $\mathrm{PG}(8, q)$ subfield subspace.

This gives the codes of THEOREM 1 of length $n = q^2 + 1$.

For length $n = q^2 + 2$, add the nucleus to the image $\nu_3(\mathrm{PG}(1, q^2))$

$\iota_3(\mathrm{PG}(1, q^3))$ gives a set of $n = q^3 + 1$ points in $\mathrm{PG}(7, q^2)$

The Twisted Tensor Product Action

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

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.

Are they BCH codes ?

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

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

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 they BCH codes ?

Q: are the codes from THEOREM 1A BCH-codes?

Q: are the codes from THEOREM 1A cyclic?

A: no, except when q is even (see below).

Therefore, the codes of THEOREM 1A for q odd *are not BCH-codes*.

Are the codes of THEOREM 2 new?

Sloane's X-construction yields $[q^3+1, 8, q(q^2-q-1)]_q$ codes (when applied to a class of BCH-cdes).

These are the parameters of the dual of the codes of THEOREM 2.

The exact relationship between these classes of codes has yet to be determined.

The Automorphism Groups

The codes of THEOREM 1 and 2 have large automorphism groups.

One can describe the automorphism groups as representations of groups:

	THEOREM 1	THEOREM 2
$\mathrm{MAut}:$	$\mathrm{P}\Gamma_2\mathrm{L}(2, q^2) \rightarrow \mathrm{PGL}(8, q)$	$\mathrm{P}\Gamma_3\mathrm{L}(2, q^3) \rightarrow \mathrm{PGL}(9, q)$
$\Gamma\mathrm{Aut}:$	$\mathrm{P}\Gamma\mathrm{L}(2, q^2) \rightarrow \mathrm{P}\Gamma\mathrm{L}(8, q)$	$\mathrm{P}\Gamma\mathrm{L}(2, q^3) \rightarrow \mathrm{P}\Gamma\mathrm{L}(8, q)$

NOTATION

$$\varphi_{a,b,c,d} : x \mapsto \frac{ax+c}{bx+d} \quad ad - bc \neq 0$$

an element in $\mathrm{PGL}(2, q^t)$

$$\mathrm{P\Gamma}_e\mathrm{L}(k, q^e) = \mathrm{PGL}(k, q^e) \rtimes \langle \phi_e \rangle$$

with $\phi_e : x \mapsto x^q$ (of order e)

Cyclic Collineations

Consider the columns of the generator matrix as the homogeneous coordinates of a set of points in $\mathrm{PG}(k-1, q)$.

A code automorphism is a stabilizer of this set.

A constacyclic code automorphism permutes this set cyclically.

A cyclic code automorphism permutes this set cyclically and maps the first vector to itself (i.e., no scalar multiplication allowed) after n applications.

Cyclic Collineations

That is, we have to study the equations

$$T^n v = v, \quad \text{and} \quad T^i v \notin \langle v \rangle \quad i = 1, \dots, n-1$$

(for cyclic codes) and

$$T^n v = cv, \quad \text{and} \quad T^i v \notin \langle v \rangle \quad i = 1, \dots, n-1, \quad c \neq 0$$

(for constacyclic codes).

Here T is the matrix associated to a collineation of $\mathrm{PG}(k-1, q)$.

The generator matrix is obtained by writing $T^i v$ ($i = 0, 1, \dots, n-1$) into the columns of a matrix.

Cyclic Collineations

Since “our” codes are obtained as images of the projective line, we are interested in cyclic (and constacyclic) automorphisms of $\mathrm{PG}(1, q^t)$.

More generally, we wish to determine the collineations which permute the $\theta_{d-1}(q) := \frac{q^d-1}{q-1}$ points of $\mathrm{PG}(d-1, q)$ in one cycle (a.k.a. Singer cycle)

Cyclic Collineations

LEMMA: (Hirschfeld 1973)

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

$= \#$ subprimitive polynomials of degree d over $\mathbb{F}_q$

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

Cyclic Collineations

NOTE:

If $m(x) = x^{n+1} + c_n x^n + \cdots + c_0 \in \mathbb{F}_q[x]$ with $c_0 \neq 0$ and $c = (c_1, \ldots, c_n)$ then

$$T_m := \left(\begin{array}{c|c} \mathbf{0}_n & -c_0 \\ \hline I_n & -c^\top \end{array} \right)$$

induces a collineation whose characteristic poynomial is $m(x)$.

Exponent and Subexponent

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

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

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

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

$m(x)$ is called subprimitive if $\mathrm{Subexp}(m) = \theta_{d-1}(q)$

Exponent and Subexponent

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

b/c if β 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 Code Automorphisms

For projective codes, the situation is as follows:

$$\left\{\begin{array}{r}\text{cyclic}\\ \text{collineation}\end{array}\right\} \leftrightarrow \left\{\begin{array}{l}\text{constacyclic}\\ \text{code}\end{array}\right\}$$

$$\left\{\begin{array}{r}\text{cyclic collineation}\\ \text{with integral elt } c = 1\end{array}\right\} \leftrightarrow \left\{\begin{array}{l}\text{cyclic}\\ \text{code}\end{array}\right\}$$

Counting Irreducible Polynomials by Integral Element

In order to count how many cyclic code automorphisms there are, we need to determine the *number of irreducible polynomials with integral element* 1.

More generally, we will now determine the *number of irreducible polynomials with integral element* $c \in \mathbb{F}_q^\times$.

Counting Irreducible Polynomials by Integral Element

Notation:

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

$R_c(d, q) = \#\mathcal{R}_c(d, q)$

$\theta_{d-1}(q) = \prod_{i=1}^{r} p_i^{e_i}$ factorization of $\theta_{d-1}(q)$ into prime powers

α a primitive element of $\mathbb{F}_q$.

Counting Irreducible Polynomials by Integral Element

LEMMA:

$R_{\alpha^i}(d,q) =$

$$\begin{cases} \frac{1}{d}\Big(\prod_{\substack{j=1 \\ p_j \mid q-1}}^{r} p_j^{e_j} \Big) \cdot \Phi\Big(\prod_{\substack{j=1 \\ p_j \nmid q-1}}^{r} p_j^{e_j} \Big) & \text{if } \gcd(i, q-1, \theta_{d-1}(q)) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

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:

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

COROLLARY:

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

Cyclic Code Automorphisms

COROLLARY:
The codes of length $q^2 + 1$ or $q^3 + 1$ are cyclic iff q is even

COROLLARY:
The codes of length $q^2 + 1$ 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 β a primitive elt of $\mathbb{F}_{q^2}$ and $\delta = 1/(\beta - \beta^q)$ and $\gamma = \beta\delta$)

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

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^2 d^{2q}\delta) & 2T_2(b^{2q+1} d\gamma) & 2T_2(b^{q+2} d^q\delta) \\ \hline
T_2(abc^q d^q\delta) & \begin{array}{c} T_2(a^{q+1} b^q d\gamma) \\ +T_2(a^q b^{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^2 c^{2q}\delta) & 2T_2(a^{2q+1} c\gamma) & 2T_2(a^{q+2} c^q\delta) \\ \hline
\begin{array}{c} T_2(b^2 c^q d^q\delta) \\ +T_2(abd^{2q}\delta) \end{array} & \begin{array}{c} 2T_2(a^q b^{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^q b^2 d^q\delta) \\ +T_2(b^{q+2} c^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(b^2 c^q d^q\beta^q\delta) \\ +T_2(abd^{2q}\beta\delta) \end{array} & \begin{array}{c} 2T_2(a^q b^{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^q b^2 d^q\beta^q\delta) \\ +T_2(b^{q+2} c^q\beta^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(a^2 d^{2q}\delta) \\ +T_2(b^2 c^{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^q b^2 c^q\delta) \\ +2T_2(a^2 b^q d^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(a^2 d^{2q}\beta\delta) \\ +T_2(b^2 c^{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^q b^2 c^q\beta^q\delta) \\ +2T_2(a^2 b^q d^q\beta\delta) \end{array} \\ \hline
\begin{array}{c} T_2(abc^{2q}\delta) \\ +T_2(a^2 c^q d^q\delta) \end{array} & \begin{array}{c} 2T_2(a^{q+1} b^q c\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^2 b^q c^q\delta) \end{array} \\ \hline
\begin{array}{c} T_2(abc^{2q}\beta^q\delta) \\ +T_2(a^2 c^q d^q\beta\delta) \end{array} & \begin{array}{c} 2T_2(a^{q+1} b^q c\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^2 b^q c^q\beta\delta) \end{array}
\end{array}\right)$$

The Representation Associated with Theorem 2

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

with U_i as follows (using β 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

$$U_2 = \begin{pmatrix} T_3(m_{dbd}\gamma_5) & T_3(m_{bbd}\gamma_6) & T_3(m_{bbd}\gamma_7) & T_3(m_{bbd}\gamma_8) \\ T_3(m_{cac}\gamma_5) & T_3(m_{aac}\gamma_6) & T_3(m_{aac}\gamma_7) & T_3(m_{aac}\gamma_8) \\ T_3(\eta_{1,1}\gamma_5) & T_3(\eta_{2,1}\gamma_6) & T_3(\eta_{2,1}\gamma_7) & T_3(\eta_{2,1}\gamma_8) \\ T_3(\eta_{1,2}\gamma_5) & T_3(\eta_{2,2}\gamma_6) & T_3(\eta_{2,2}\gamma_7) & T_3(\eta_{2,2}\gamma_8) \\ T_3(\eta_{1,3}\gamma_5) & T_3(\eta_{2,3}\gamma_6) & T_3(\eta_{2,3}\gamma_7) & T_3(\eta_{2,3}\gamma_8) \\ T_3(\zeta_{1,1}\gamma_5) & T_3(\zeta_{2,1}\gamma_6) & T_3(\zeta_{2,1}\gamma_7) & T_3(\zeta_{2,1}\gamma_8) \\ T_3(\zeta_{1,2}\gamma_5) & T_3(\zeta_{2,2}\gamma_6) & T_3(\zeta_{2,2}\gamma_7) & T_3(\zeta_{2,2}\gamma_8) \\ T_3(\zeta_{1,3}\gamma_5) & T_3(\zeta_{2,3}\gamma_6) & T_3(\zeta_{2,3}\gamma_7) & T_3(\zeta_{2,3}\gamma_8) \end{pmatrix},$$

The Representation Associated with Theorem 2

with

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

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

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

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

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

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

using the conventions that $m_{xyz} = x^{q^2} y^q z$, $\beta_{ijk} = \beta^{iq^2+jq+k}$, $\beta_{jk} = \beta_{0jk}$, and $\beta_k = \beta_{00k}$.