数理解析研究所講究録
第 1926 巻 2014 年 78-87

22 次 Mathieu 群の dual hyperoval を通じた簡明な構成について

$$m(x,y) = x \otimes y + \Delta(\iota(x \times y))$$

吉荒 聡
東京女子大学 現代教養学部 数理科学科
Satoshi Yoshiara
Department of Mathematics,
Tokyo Woman's Christian University

This is based on the slides for my talk given on March 5, 2014, at RIMS. Further details are found in my manuscript with title "A simple description of the Mathieu dual hyperoval and its splitness", which was submitted for publication.

1 Contents and some history

1.1 DHO

We first recall the notion of dimensional dual hyperovals. Let n be an integer with $n \geq 2$ and let U be a finite vector space over $\mathbb{F}_q$ of dimension at least $2n-1$.

Definition 1 *A collection $\mathcal{S}$ of n-dimensional subspaces of U is called a* **dual hyperoval** *over $\mathbb{F}_q$ of* **rank** *n (abbreviated to n-***DHO** *in the sequel), if it satisfies the following conditions (i),(ii) and (iii):*

(i) $\dim(X \cap Y) = 1$ *for distinct* $X, Y \in \mathcal{S}$,

(ii) $X \cap Y \cap Z = \{0\}$ *for mutually distinct* $X, Y, Z \in \mathcal{S}$,

(iii) $|\mathcal{S}| = 1 + \{(q^n - 1)/(q-1)\}$.

1.2 Contents of my talk

In this talk, I will first give

a simple construction of a 3-DHO $\mathcal{M}$ over $\mathbb{F}_4$ (so that $|\mathcal{M}| = 22$),

which is given inside the symmetric tensor product $S^2(\mathbb{F}_4^3)$ as a deformation of the Veronesean DHO. Based on this construction, then I will present

a self-contained introduction to M_{22}.

More precisely I will discuss

- how to see $\mathrm{Aut}(\mathcal{M}) \cong 3.M.2$ with M a simple group of order $2^7.3^2.5.7.11$, and
- how to find explicit unitary matrices in $SU_6(\mathbb{F}_4)$ generating $L(\mathcal{M}) \cong 3.M$.

1.3 Known models of $\mathcal{M}$

As far as I know, the 3-DHO $\mathcal{M}$ over $\mathbb{F}_4$ associated with the simple Mathieu group M_{22} was first mentioned in paper [1] below. It is given in terms of the Leech lattice. Then it appears in [2] as a table in terms of MOG arrangement. The paper [3] characterizes $\mathcal{M}$ as a 3-DHO $\mathcal{M}$ over $\mathbb{F}_4$ of unitary polar type, in the sense that every member of the DHO is totally isotropic with respect to a nondegenerate hermitian form on the ambient space. It also recovers the seemingly miracle table given in [2] as explicit descriptions of all members.

1 W. Jónsson and J. McKay, "More about the Mathieu group M_{22}", Can.J.Math. 28 (1976), 929–937.

2 J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, W.A.Wilson, p.39 in "Atlas of Finite Groups", 1985.

3 N.Nakagawa, "On 2-dimensional dual hyperovals of polar type", Utilitas Mathematica 76 (2008), 101–114.

Below I repeat Nakagawa's descriptions of members of $\mathcal{M}$, where $\mathbf{e}_i$ $(i = 0, \dots, 5)$ are basis for a 6-dimensional vector space U over $\mathbb{F}_4$ equipped with a nondegenerate hermitian form $(\ ,\ )$ with $(\mathbf{e}_i, \mathbf{e}_j) = \delta_{i+j,5}$ $(0 \leq i, j \leq 5)$. The letters α and θ denote nonzero elements in $\mathbb{F}_4$ with $\beta = \alpha + \theta$, and $\overline{x} = x^2$ for $x \in \mathbb{F}_4$.

$$
\begin{aligned}
A &:= \langle \mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2 \rangle, \\
A[\mathbf{e}_0] &:= \langle \mathbf{e}_0, \mathbf{e}_3, \mathbf{e}_4 \rangle, \\
A[\mathbf{e}_1] &:= \langle \mathbf{e}_1, \mathbf{e}_3, \mathbf{e}_5 \rangle, \\
A[\mathbf{e}_2] &:= \langle \mathbf{e}_2, \mathbf{e}_4, \mathbf{e}_5 \rangle, \\
A[\alpha\mathbf{e}_0 + \mathbf{e}_1] &:= \langle \mathbf{e}_0 + \alpha\mathbf{e}_3, \mathbf{e}_1 + \overline{\alpha}\mathbf{e}_3, \mathbf{e}_2 + \alpha\mathbf{e}_4 + \overline{\alpha}\mathbf{e}_5 \rangle, \\
A[\alpha\mathbf{e}_0 + \mathbf{e}_2] &:= \langle \mathbf{e}_0 + \alpha\mathbf{e}_4, \mathbf{e}_2 + \overline{\alpha}\mathbf{e}_4, \mathbf{e}_1 + \alpha\mathbf{e}_3 + \overline{\alpha}\mathbf{e}_5 \rangle, \\
A[\alpha\mathbf{e}_1 + \mathbf{e}_2] &:= \langle \mathbf{e}_1 + \alpha\mathbf{e}_5, \mathbf{e}_2 + \overline{\alpha}\mathbf{e}_5, \mathbf{e}_0 + \alpha\mathbf{e}_3 + \overline{\alpha}\mathbf{e}_4 \rangle, \\
\begin{matrix} A[\alpha\theta\mathbf{e}_0 + \\ \alpha\mathbf{e}_1 + \mathbf{e}_2] \end{matrix} &:= \langle \theta\mathbf{e}_0 + \mathbf{e}_1 + \overline{\alpha}\mathbf{e}_2, \overline{\beta}\mathbf{e}_0 + \mathbf{e}_3 + \alpha\mathbf{e}_4, \beta\mathbf{e}_2 + \overline{\theta}\mathbf{e}_4 + \mathbf{e}_5 \rangle.
\end{aligned}
$$

1.4 Motivation to find another description

All descriptions obtained in papers [1], [2] and [3] are just tables. Thus in analogy with coding theory, they are just "generator matrices". This gives difficulties in finding the intersectrion of two members, specifically between $A[\alpha\theta\mathbf{e}_0 + \alpha\mathbf{e}_1 + \mathbf{e}_2]$'s in the description by Nakagawa. Consequently, it is not straightforward to find automorphisms based only on these tables.

Thus we need more concise description of members of $\mathcal{M}$, which corresponds "parity-check conditions" in analogy with coding theory.

2 A construction of $\mathcal{M}$

2.1 Reviews on $\mathbb{F}_4^3$ and $S^2(\mathbb{F}_4^3)$

2.1.1 Notation

We use the letter V to denote a 3-dimensional vector space over $\mathbb{F}_4$ with a specified basis e_i $(i = 0, 1, 2)$. Consider the symmetric square tensor product $S^2(V)$ of V. (which is obtained as $(V \otimes V)/W$ with W the subspace of $V \otimes V$ spanned by $x \otimes y + y \otimes x$ for all $x, y \in V$. We denote the image of $x \otimes y$ in this factor space by the same symbol $x \otimes y$, so that we have $x \otimes y = y \otimes x$ for all $x, y \in V$.) The vector space $S^2(V)$ is a 6-dimensional vector space over $\mathbb{F}_4$ with a basis Δ_i, ∇_i $(i = 0, 1, 2)$, where

$$\begin{aligned} &\Delta_i := e_i \otimes e_i \ (i = 0, 1, 2), \\ &\nabla_i := e_j \otimes e_k \ (\{i, j, k\} = \{0, 1, 2\}). \end{aligned}$$

Explicitly, $\nabla_0 = e_1 \otimes e_2$, $\nabla_1 = e_2 \otimes e_0$, $\nabla_2 = e_0 \otimes e_1$.

Delta-map We denote by Δ a map from V to $S^2(V)$ given by $\Delta(x) := x \otimes x$. Δ is a $\mathbb{F}_4$-semilinear injection, because for all $x, y \in V$ we have

$$\Delta(x + y) = \Delta(x) + \Delta(y), \quad \Delta(\alpha x) = \alpha^2 \Delta(x).$$

2.1.2 A quadratic map on $V = \mathbb{F}_4^3$

The map $\iota : V \to V$ sending $x = x_0 e_0 + x_1 e_1 + x_2 e_2 \in V$ to

$$\textstyle\sum_i x_j x_k e_i = x_1 x_2 e_0 + x_2 x_0 e_1 + x_0 x_1 e_2 \in V$$

is a quadratic map, in the sense that the associated map $(x, y) \mapsto \iota(x+y) + \iota(x) + \iota(y) + \iota(0)$ is a bilinear (in fact, alternating bilinear) map from $V \times V$ to V. The associated alternating map

$$\begin{aligned} & \iota(x + y) + \iota(x) + \iota(y) + \iota(0) \\ = \ & (x_1 y_2 + x_2 y_1) e_0 + (x_2 y_0 + x_0 y_2) e_1 + (x_0 y_1 + x_1 y_0) e_2 \end{aligned}$$

is the **exterior product** on $V = \mathbb{F}_4^3$, which I shall denote $x \times y$, following the common notation in colledge mathematics.

2.1.3 Basic equations

For all $x, y, z \in V = \mathbb{F}_4^3$, we have

$$\begin{aligned} x \times y &= \iota(x + y) + \iota(x) + \iota(y), \\ (x \times y) \cdot z &= \det(r(x, y, z)), \\ x \times (y \times z) &= (x \cdot z) y + (x \cdot y) z, \end{aligned}$$

where $x \cdot y := \sum_{i=0}^2 x_i y_i$ (**dot product**) and

$$r(x, y, z) = \begin{pmatrix} x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{pmatrix}.$$

2.2 Construction

2.2.1 Vector $m(x,y)$ in $S^2(\mathbb{F}_4^3)$

Definition 2 *For $x, y \in V = \mathbb{F}_4^3$, define a vector $m(x,y) \in S^2(V)$ by*

$$m(x,y) \ := \ x \otimes y + \Delta(\iota(x \times y)). \tag{1}$$

The expression of $m(x,y)$ as a linear combination of basis ∇_i, Δ_i $(i = 0,1,2)$ of $S^2(V)$ is given as follows for $x = \sum_{i=0}^{2} x_i e_i$ and $y = \sum_{i=0}^{2} y_i e_i$:

$$m(x,y) = \sum_{i=0}^{2} (x \times y)_i \nabla_i + \sum_{i=0}^{2} (x_i y_i + \overline{(x \times y)_j (x \times y)_k}) \Delta_i,$$

where $\{i,j,k\} = \{0,1,2\}$ and $\overline{\alpha} = \alpha^2$ $(\alpha \in \mathbb{F}_4)$.

Observe $m(x,y) = m(y,x)$, $m(x,x) = \Delta(x)$.

2.2.2 Subsets $A[v]$, A of $S^2(\mathbb{F}_4^3)$

Observe $m(\alpha x, y) = \alpha m(x,y)$ for $\alpha \in \mathbb{F}_4^\times$; because $\alpha^4 = \alpha$ (we are working with $\mathbb{F}_4$!). Thus a subset

$$A[v] := \{m(x,v) \mid x \in V\}$$

of $S^2(V)$ depends only on the projective point $[v]$ (1-space containing v).

We set

$$A := \{\Delta(x) \mid x \in V\},$$

which forms a subspace of $S^2(V)$ by the semilinearity of Δ.

In fact, $A[v]$ is a subspace of $S^2(V)$, as we shall see below.

2.2.3 Additive formula

Lemma 1 *For $a, b, v \in V$, the following equations hold with $\delta := \det(r(a,b,v))$:*

$$m(a,v) + m(b,v) \ = \ m(a+b,v) + \Delta(\delta v), \tag{2}$$
$$m(a,v) + m(b,v) \ = \ m(a+b+\overline{\delta}v, v). \tag{3}$$

Equation (3) follows from equation (2), because $\Delta(\delta v) = m(\delta v, \delta v) = \overline{\delta} m(v,v)$. Moreover, Equation (3) implies that $A[v]$ is a subspace of $S^2(V)$.

2.2.4 Proof of additive formula

As $m(x,y) = x \otimes y + \Delta(\iota(x \times y))$ and Δ is $\mathbb{F}_2$-linear, in order to prove equation (2) it suffices to show

$$\iota((a+b) \times v) + \iota(a \times v) + \iota(b \times v) \ = \ \delta v. \tag{4}$$

As ι is quadratic with the associated form $\times$ (that is, $\iota(v+w) + \iota(v) + \iota(w) = v \times w$), the left hand side of equation (4) is $(a \times v) \times (b \times v)$, which equals
$\{(a \times v) \cdot b\} v + \{(a \times v) \cdot v\} b = \det(r(a,b,v)) v$.

2.2.5 DHO $\mathcal{M}$

We shall now define a DHO $\mathcal{M}$. We denote by $\mathbf{PG}(V)$ the set of projective points in V.

Proposition 1 *(i) The collection* $\mathcal{M} := \{A[v] \mid [v] \in \mathbf{PG}(V)\} \cup \{A\}$ *is a DHO of rank* 3 *over* $\mathbb{F}_4$.

(ii) For $[v] \in \mathbf{PG}(V)$, $A \cap A[v]$ *is a* 1*-subspace spanned by* $\Delta(v)$.

(iii) For distinct $[v]$, $[w]$ *in* $\mathbf{PG}(V)$, $A[v] \cap A[w]$ *is a* 1*-subspace spanned by* $m(w, v) = m(v, w)$.

2.2.6 Proof of (iii)

Assume $0 \neq c := m(x, v) = m(y, w) \in A[v] \cap A[w]$. Comparing the coefficients of ∇_i in the expressions of $m(x, v)$ and $m(y, w)$, this implies that $(x \times v)_i = (y \times w)_i$ $(i \in \{0, 1, 2\})$ and thus $x \times v = y \times w$ $(=: a)$.

It's easy to show $a \neq 0$.

Then $a^{\perp} := \{z \in V \mid z \cdot a = 0\}$ is a hyperplane of V, which is spanned by v and w, as $[v] \neq [w]$. Thus $a^{\perp} \ni x = \alpha v + \beta w$, $y = \gamma v + \delta w$ for some α, β, γ, δ in $\mathbb{F}_4$.

Then the additive formula implies

$$\begin{aligned} m(x, v) &= m(\alpha v + \beta w, v) \\ &= m(\alpha v, v) + m(\beta w, v) + \Delta(\det(r(\alpha v, \beta w, v))v) \\ &= \alpha\Delta(v) + \beta m(w, v). \end{aligned}$$

Similarly, we have $m(y, w) = \gamma m(v, w) + \delta\Delta(w)$. As $m(x, v) = m(y, w)$, these expressions imply

$$(\beta + \gamma)m(v, w) = \Delta(\overline{\alpha} v + \overline{\delta} w).$$

This holds iff $\beta + \gamma = 0 = \overline{\alpha} v + \overline{\delta} w$, or equivalently $\beta = \gamma$ and $\alpha = \delta = 0$. Thus $c = m(x, v) = m(y, w) = \beta m(v, w)$.

3 Automorphisms

3.1 Basic idea

3.1.1 Automorphisms

Definition 3 $\mathrm{Aut}(\mathcal{M})$ *and* $L(\mathcal{M})$ *respectively denote the groups of* $\mathbb{F}_4$*-semilnear and linear bijections on* $S^2(V)$ *permuting the members of* $\mathcal{M}$.

It is not difficult to establish the following facts:

- $\mathrm{Aut}(\mathcal{M})$ contains $L(\mathcal{M})$ with index two: a field automorphism lies in $\mathrm{Aut}(\mathcal{M}) \setminus L(\mathcal{M})$.
- The kernel of the action of $L(\mathcal{M})$ on $S^2(V)$ is $Z := \langle \omega I_6 \rangle$, a central subgroup of order 3 of $SL_6(4)$, where ω denotes a primitive cubic root of unity in $\mathbb{F}_4$.
- The stabilizer of A in $L(\mathcal{M})/Z$ is a subgroup of $GL(V) \cong GL_3(4)$.

3.1.2 A method to find an automorphism of a DHO

Assume $\lambda \in L(\mathcal{M})$ stabilizes $A = \{\Delta(x) \mid x \in V\}$. We shall explain a basic idea to find the action of λ on $m(x,y)$. It is easy to see that there is a linear bijection g on V such that $\Delta(x)^\lambda = \Delta(x^g)$ for all $x \in V$.

As $\langle \Delta(x) \rangle = A \cap A[x]$ for $x \neq 0$, $\langle \Delta(x)^\lambda \rangle = A^\lambda \cap A[x]^\lambda = A \cap A[x]^\lambda$. On the other hand, $\langle \Delta(x)^\lambda \rangle = \langle \Delta(x^g) \rangle = A \cap A[x^g]$. As $\mathcal{M}$ is a DHO, we have

$$A[x]^\lambda = A[x^g] \ (x \in V,\, x \neq 0).$$

Then for $x, y \in V$ with $[x] \neq [y]$ we have

$$\begin{aligned} \langle m(x,y)^\lambda \rangle &= (A[x] \cap A[y])^\lambda = A[x]^\lambda \cap A[y]^\lambda \\ &= A[x^g] \cap A[y^g] = \langle m(x^g, y^g) \rangle. \end{aligned}$$

Thus we have the following "Key Equation":

$$m(x,y)^\lambda \quad = \quad \gamma_{x,y} m(x^g, y^g) \ \text{ for some } \gamma_{x,y} \in \mathbb{F}_4^\times. \tag{5}$$

This restricts the shape of g, as $m(x,y)$ $(x, y \in V)$ span $S^2(V)$.

3.2 The stabilizer of A

3.2.1 Unitary form

Define a unitary form $(\ ,\ )$ on $S^2(V)$ by

$(\Delta_i, \Delta_j) := 0 =: (\nabla_i, \nabla_j)$ $(i, j \in \{0,1,2\})$,
$(\Delta_i, \nabla_j) := 1$ or 0 according as $i = j$ or not.

Lemma 2 *We can verify the following facts:*

(1) Every member of $\mathcal{M}$ is totaly isotropic.

(2) $L(\mathcal{M})$ preserves $(\ ,\ )$.

3.2.2 An important property of $m(x,y)$

For $x = \sum_{i=0}^2 x_i e_i$ and $y = \sum_{i=0}^2 y_i e_i$ in V, we already saw

$$m(x,y) = \sum_{i=0}^{2} (x \times y)_i \nabla_i + \sum_{i=0}^{2} (x_i y_i + \overline{(x \times y)_j (x \times y)_k}) \Delta_i.$$

Observe that $\nabla_i = e_j \otimes e_k = m(e_j, e_k)$, $\Delta_i = \Delta(e_i)$, $\det(r(e_0, e_1, e_2)) = 1$.

Lemma 3 *The same formula holds for another basis u_i $(i = 0,1,2)$ of V; namely, for $x = \sum_{i=0}^2 x_i u_i$, $y = \sum_{i=0}^2 y_i u_i$ in V with $\delta := \det(r(u_0, u_1, u_2))$, we have*

$$\begin{aligned} m(x,y) \quad &= \quad \sum_{i=0}^{2} (x \times y)_i m(u_j, u_k) \\ &\quad + \sum_{i=0}^{2} (x_i y_i + \overline{\delta (x \times y)_j (x \times y)_k}) \Delta(u_i). \end{aligned}$$

3.2.3 The stabilizer of A

We shall now state the main result and give its proof.

Proposition 2 *The stabilizer of A in $L(\mathcal{M})$ coincides with $\{\tilde{g} \mid g \in SL(V)\}$, where, if $g_i := e_i g = g_{i0}e_0 + g_{i1}e_1 + g_{i2}e_2$ $(i = 0, 1, 2)$, the action of $\tilde{g}$ is given as follows:*

$$\begin{aligned} \Delta_i \tilde{g} &= \overline{g_{i0}}\Delta_0 + \overline{g_{i1}}\Delta_1 + \overline{g_{i2}}\Delta_2, \\ \nabla_i \tilde{g} &= g_j \otimes g_k + \Delta(\iota(g_j \times g_k)), \end{aligned}$$

for $\{i, j, k\} = \{0, 1, 2\}$. Moreover $m(x, y)^{\tilde{g}} = m(x^g, y^g)$ and $A[x]^{\tilde{g}} = A[x^g]$ $(x, y \in V)$.

3.2.4 Proof of Proposition

Take $\lambda \in L(\mathcal{M})$ stabilizing A. Then there is $g \in GL(V)$ such that $\Delta(x)^\lambda = \Delta(x^g)$ $(x \in V)$. The vectors $g_i := e_i^g$ form a basis of V and $\Delta_i^\lambda = \Delta(g_i)$ $(i = 0, 1, 2)$.

By the previous argument given in Subsubsection 3.1.2, $A[e_i]^\lambda = A[e_i^g] = A[g_i]$ and

$$(e_i \otimes e_j)^\lambda = \gamma_{e_i,e_j} m(g_i, g_j) = \gamma_{e_i,e_j}\{g_i \otimes g_j + \Delta(\iota(g_i \times g_j))\}.$$

As λ preserves the unitary form $(\ ,\ )$, we can show that $\gamma_{e_i,e_j} = \overline{\det(g)}$.

Thus the action of λ on the basis Δ_i and ∇_i for $S^2(V)$ is determined as follows: for any $i \in \{0, 1, 2\} = \{i, j, k\}$,

$\Delta_i^\lambda = \Delta(g_i)$, $\nabla_i^\lambda = (e_j \otimes e_k)^\lambda = \overline{\det(g)} m(g_j, g_k)$.

Take any distinct $[x]$, $[y] \in \mathbf{PG}(V)$ with $x = \sum_{i=0}^2 x_i e_i$, $y = \sum_{i=0}^2 y_i e_i$. As we noticed above in equation (5),

$m(x, y)^\lambda = \gamma_{x,y} m(x^g, y^g)$ for some $\gamma_{x,y} \in \mathbb{F}_4^\times$.

The left hand side of equation (5) is calculated as

$$\begin{aligned} m(x, y)^\lambda &= \sum_{i=0}^{2} \overline{\det(g)}(x \times y)_i m(g_j, g_k) \\ &\quad + \sum_{i=0}^{2}\{x_i y_i + \overline{(x \times y)_j (x \times y)_k}\}\Delta(g_i), \end{aligned} \tag{6}$$

in view of the above action of λ on Δ_i, ∇_i applied to $m(x, y) = \sum_{i=0}^2 (x \times y)_i \nabla_i + \sum_{i=0}^2 \{x_i y_i + \overline{(x \times y)_j (x \times y)_k}\}\Delta_i$.

On the other hand, the right hand side of equation (5) is given by Lemma 3 applied to basis g_i for V $(\delta := \det(r(g_0, g_1, g_2)) = \det(g))$:

$$\begin{aligned} m(x^g, y^g) &= m(\sum_{i=0}^{2} x_i g_i, \sum_{i=0}^{2} y_i g_i) \\ &= \sum_{i=0}^{2}(x \times y)_i m(g_j, g_k) \\ &\quad + \sum_{i=0}^{2}\{x_i y_i + \overline{\delta}\ \overline{(x \times y)_j (x \times y)_k}\}\Delta(g_i). \end{aligned} \tag{7}$$

As $\Delta(g_i)$ and $m(g_j, g_k)$ ($i \in \{0,1,2\} = \{i,j,k\}$) form a basis for $S^2(V)$, "KeyEquation" (equation (5)) together with equations (6) and (7) implies

$$\begin{aligned} \overline{\det(g)}(x \times y)_i &= \gamma_{xy}(x \times y)_i, \text{ and} \\ x_i y_i + \overline{(x \times y)_j (x \times y)_k} &= \gamma_{xy}\{x_i y_i + \overline{\det(g)(x \times y)_j (x \times y)_k}\} \end{aligned}$$

for all $i \in \{0,1,2\}$. As $[x] \neq [y]$, there exists $i \in \{0,1,2\}$ with $(x \times y)_i \neq 0$. Thus we have $\gamma_{xy} = \overline{\det(g)}$ from the first equation above. Then the second equation above reads

$$(x_i y_i)(1 + \overline{\det(g)}) = (1 + \det(g))\overline{(x \times y)_j (x \times y)_k}$$

for all $i \in \{0,1,2\}$.

This conclusion holds for every distinct $[x], [y] \in \mathbf{PG}(V)$. Take $x = e_0 + e_1 + e_2$ and $y = e_0 + \omega e_1 + \overline{\omega} e_2$. Then the above conclusion for these x, y reads $1 + \overline{\det(g)} = 1 + \det(g)$, whence $\det(g) = \overline{\det(g)} = 1$.

Thus we showed that if λ is a linear automorphism of $\mathcal{M}$ stabilizing A, then λ is of the form $\tilde{g}$ for some $g \in SL(V)$.

Conversely, we can show that $\tilde{g}$ for $g \in SL(V)$ in fact lies in $L(\mathcal{M})$.

3.2.5 Matrix form

For $g \in SL(V)$, we also use g to denote the matrix representing g with respect to e_i. Then the matrix representing $\tilde{g}$ in Proposition 2 with respect to Δ_i, ∇_i is given by

$$\begin{pmatrix} \overline{g} & 0 \\ L(g) & {}^t g^{-1} \end{pmatrix}, \quad L(g) = {}^t\iota({}^t g) + \iota(({}^t\overline{g})^{-1}),$$

where $\iota(h) = \begin{pmatrix} h_{01}h_{02} & h_{02}h_{00} & h_{00}h_{01} \\ h_{11}h_{12} & h_{12}h_{10} & h_{10}h_{11} \\ h_{21}h_{22} & h_{22}h_{20} & h_{20}h_{21} \end{pmatrix}$ for $h = (h_{ij})$. (The following property of ι may be of some interest: for matrices a, b of degree 3, we have $\iota(ab) = \overline{a}\iota(b) + \iota(a)({}^t b^{-1})$.)

For example, take the following matrices in $SL(V)$ generating $3_+^{1+2} : Q_8$, where we adopt the usual convention to denote monomial matrices t_1 and t_2.

$$t_1 := (e_0, e_1, e_2), \qquad t_2 := \mathrm{diag}(1, \omega, \overline{\omega});$$
$$q_1 := \begin{pmatrix} 1 & 1 & 1 \\ 1 & \overline{\omega} & \omega \\ 1 & \omega & \overline{\omega} \end{pmatrix}, \qquad q_2 := \begin{pmatrix} 1 & \overline{\omega} & \overline{\omega} \\ \omega & \omega & \overline{\omega} \\ \omega & \overline{\omega} & \omega \end{pmatrix}$$

The the corresponding matrices in the stabilizer of A in $L(\mathcal{M})$ can be obtained as follows:

$$\tilde{t}_1 = (\Delta_0, \Delta_1, \Delta_2)(\nabla_0, \nabla_1, \nabla_2), \qquad \tilde{t}_2 = \mathrm{diag}(1, \overline{\omega}, \omega, 1, \overline{\omega}, \omega);$$
$$\tilde{q}_1 = \begin{pmatrix} \overline{q_1} & 0 \\ 0 & \overline{q_1} \end{pmatrix}, \qquad \tilde{q}_2 = \begin{pmatrix} \overline{q_2} & 0 \\ \overline{q_2} & \overline{q_2} \end{pmatrix}.$$

3.3 Structure of $L(\mathcal{M})$

3.3.1 An involution moving A

The above arguments can also be applied to find a linear automorphism moving A. For example, consider the following involutive linear automorphism σ on $S^2(V)$ (represented with respect to basis Δ_i and ∇_i ($i = 0,1,2$).) Then σ sends A to $A[e_2]$.

$$\sigma = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Lemma 4 *Let σ be a linear bijection on $S^2(V)$ which fixes ∇_2 and Δ_2 and interchanges the pairs (∇_i, Δ_i) for $i = 0$ and 1. Then σ is an automorphism of $\mathcal{M}$. Moreover $\Delta(x)\sigma = m(e_2, \delta(x))$ and $m(x,y)\sigma = m(\delta(x), \delta(y))$, and hence $A\sigma = A[e_2]$, $A[e_2]\sigma = A$, $A[x]\sigma = A[\delta(x)]$ for every $x, y \in V \setminus [e_2]$, where $\delta(x)$ is given by:*

$$\delta(x) \quad := \quad \overline{x_1}e_0 + \overline{x_0}e_1 + (x_0x_1 + \overline{x_2})e_2.$$

3.3.2 Structure of $\mathrm{Aut}(\mathcal{M})$

By Proposition 2, the stabilizer of A in $L(\mathcal{M})$ induces a permutation group isomorphic to $SL_3(4)/Z(SL_3(4)) \cong PSL_3(4)$ on the 21 memebers in $\mathcal{M} \setminus \{A\}$. This group is a non-abelian simple group and a doubly transitive on $\mathcal{M} \setminus \{A\}$, as this action is equivalent to the 2-transitive action of $PSL_3(4)$ on 21 points of $\mathbf{PG}(V)$. Then the existence of σ in $L(\mathcal{M})$ moving A to $A[e_2]$ implies that $L(\mathcal{M})/Z$ is a triply transitive permutation group on $\mathcal{M}$ with stabilizer $PSL_3(4)$. Hence $L(\mathcal{M})/Z$ is a simple group of order $22|PSL_3(4)| = 2^7 3^2.5.7.11$ acting 3-transitively on $\mathcal{M}$.

Summarizing, the structure of the automorphism group $\mathrm{Aut}(\mathcal{M})$ is determined as follows:

- $[\mathrm{Aut}(\mathcal{M}) : L(\mathcal{M})] = 2$ and $\mathrm{Aut}(\mathcal{M}) \setminus L(\mathcal{M})$ contains an involution (the filed automorphism).
- $L(\mathcal{M})$ is a subgroup of the special unitary group $SU_6(\mathbb{F}_4)$ containing the group Z of scalars (of order 3 inverted by the field automorphism).
- $L(\mathcal{M})/Z$ is a non-abelian group of order $2^7 3^2.5.7.11$ acting 3-transitively on $\mathcal{M}$. (As a Sylow 3-subgroup of $L(\mathcal{M})$ is 3_+^{1+2}, which is not split over its center Z, the extension $L(\mathcal{M})/Z$ does not split by a theorem of Gashütz.)

The explicit identification of the simple group $L(\mathcal{M})/Z$ with the Mathieu simple group M_{22} can also be given as follows. We first recall the fact that there is a unique block design with parameters $t = 3$, $v = 22$, $k = 6$ and $\lambda = 1$ and that the Mathieu group M_{22} is defined to be the automorphism group of such a block design. Thus it suffices to construct a block design with parameters $(t, v, k, \lambda) = (3, 22, 6, 1)$ on which $L(\mathcal{M})/Z$ acts faithfully. As the set of points, we take $\mathcal{M}$. We shall construct a block design on $\mathcal{M}$ by defining a block as follows: take three distinct members X_i ($i \in \{0,1,2\}$) of $\mathcal{M}$.

Then it can be uniquely extended to a 6-subset $B(X_0, X_1, X_2) := \{X_k \mid k \in \{0, \dots, 5\}\}$ of $\mathcal{M}$ with the following property: for any 3-subset $\{p, q, r\}$ of $\{0, \dots, 5\}$, the 2-subspace spanned by $X_p \cap X_q$ and $X_p \cap X_r$ contains $X_p \cap X_j$ for all $j \in \{0, \dots, 5\} \setminus \{p, q, r\}$. To verify this claim, we may assume that $X_0 = A$, $X_i = A[e_i]$ $(i = 1, 2)$ by the triply transitivity of $\mathrm{Aut}(\mathcal{M})$ on the members of $\mathcal{M}$. It can be verified that $B(X_0, X_1, X_2) = \{X_k \mid k \in \{0, \dots, 5\}\}$ with $X_{3+j} := A[e_1 + \omega^j e_2]$ $(j = 0, 1, 2)$. The above property implies that $B(X_0, X_1, X_2) = B(X_p, X_q, X_r)$ for every 3-subset $\{p, q, r\}$ of $\{0, \dots, 5\}$. We adopt as blocks all 6-subsets $B(X_0, X_1, X_2)$ determined by 3-subsets $\{X_0, X_1, X_2\}$ of $\mathcal{M}$. Then the 22-set $\mathcal{M}$ together with the set $\mathcal{B}$ of all blocks forms a design with parameters $t = 3$, $v = 22$, $k = 6$ and $\lambda = 1$. As $L(\mathcal{M})/Z$ acts faithfully on this block design $(\mathcal{M}, \mathcal{B})$, this establishes the claim $L(\mathcal{M}) \cong M_{22}$.