数理解析研究所講究録
第233巻 1975年 24-31

Automorphisms of Alltop's 4-designs

東大 理　　榎本 彦衛

永い間、自明でない4-designはMathieu群と関係したもの（有限個）しか知られておらず、新しい4-designが見つかれば新しい4重可移群が見つかるのではないかと期待されていました。Alltopにより初めて4-designの無限系列が構成された（J. Combinatorial Theory 6（1969）320-322）のですが、不思議なことにこのdesignの全自己同型群はすぐには決定されませんでした。今年になってようやく全自己同型群が決定できたのですが、残念ながら既に存在のわかっているもの以外には自己同型の存在しないことがわかり、新しい4重可移群の発見とはなりませんでした。

まず、このdesignの構成法の復習から始めることにします。$q = 2^n$とおき、

$$\Omega = GF(q) \cup \{\infty\}$$

をq個の元からなる有限体$GF(q)$上の射影直線とします。

$$
\begin{aligned}
\Omega_1 &= \Omega - \{\infty, 0, 1\} \\
&= GF(q) - GF(2) \\
&= \{\alpha \in GF(q) \mid \alpha^2 \neq \alpha\}
\end{aligned}
$$

とおき、$\alpha \in \Omega_1$ に対し

$$\Delta(\alpha) = \{\infty, 0, 1, \alpha, \alpha+1\}$$

と定義します。$PGL(2, q)$ が Ω の上に自然に働いているので、

$$\mathcal{D}(\alpha) = \{\Delta(\alpha)^g \mid g \in PGL(2, q)\},$$

$$\mathcal{D} = \bigcup_{\alpha \in \Omega_1} \mathcal{D}(\alpha)$$

と定義します。$PGL(2, q)$ の Ω 上の作用は3重可移なので、この *design* $(\Omega, \mathcal{D})$ が 3-*design* であることは明らかなのですが、実は 4-$(q+1, 5, 5)$ *design* になっていることが次の補題からわかります。

<u>補題 1</u> (*Alltop*). $\alpha \in \Omega_1$ に対し

$$\Gamma(\alpha) = \left\{\alpha+1, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha}, \alpha^2, \sqrt{\alpha}\right\}$$

とおく。n が3以上の奇数ならば、これらの5点は異なり、

$$\{\infty, 0, 1, \alpha, \beta\} \in \mathcal{D} \iff \beta \in \Gamma(\alpha)$$

が成り立つ。

（注） n が偶数の時にはこの補題は成り立た[redacted]ず、$(\Omega, \mathcal{D})$

も4-designにならない。

目標は次の定理を証明することです。

<u>定理</u>　nが5以上の奇数ならば、$P\Gamma L(2, q)$がこのdesignの全自己同型群になる。

（注）　$n = 3$の時には

$$\Gamma(\alpha) = \Omega - \{\infty, 0, 1, \alpha\}$$

となり、Ωの任意の5点部分集合がblockとなる。すなわちこれは自明なdesignであって、その全自己同型群は9次対称群となる。

$(\Omega, \mathcal{D})$の全自己同型群をGとおく。以下、nを5以上の奇数とし、$G = P\Gamma L(2, q)$を示すことが目標であるが、fを有限体$GF(q)$の自己同型とすると、

$$\begin{aligned}\Delta(\alpha)^f &= \{\infty^f, 0^f, 1^f, \alpha^f, (\alpha+1)^f\} \\ &= \{\infty, 0, 1, \alpha^f, \alpha^f+1\} \\ &= \Delta(\alpha^f)\end{aligned}$$

となり、これも$\mathcal{D}$に属するので、$P\Gamma L(2, q)$がGに含まれることはすぐにわかる。逆を証明するためには、3重可移に働いていることがわかっているので、3点を固定する部分群

についていえればよい。ところが、$P\Gamma L(2,8)$ の元で ∞, 0, 1 の3点を固定するものは有限体 $GF(8)$ の自己同型から引き起されるものである。故に

"$G_{\infty,0,1}$ に入る自己同型 x は、有限体 $GF(8)$ の自己同型として作用する"

ということを証明すればよい。

まず、$\Gamma(\alpha)$ の点 β に対し $\Gamma(\beta)$ を計算すると、

$$\Gamma(\alpha+1)=\left\{\alpha,\ \frac{\alpha+1}{\alpha},\ \frac{1}{\alpha+1},\ \alpha^2+1,\ \sqrt{\alpha}+1\right\},$$

$$\Gamma\left(\frac{\alpha}{\alpha+1}\right)=\left\{\frac{1}{\alpha+1},\ \alpha,\ \frac{\alpha+1}{\alpha},\ \frac{\alpha^2}{\alpha^2+1},\ \frac{\sqrt{\alpha}}{\sqrt{\alpha}+1}\right\},$$

$$\Gamma\left(\frac{1}{\alpha}\right)=\left\{\frac{\alpha+1}{\alpha},\ \frac{1}{\alpha+1},\ \alpha,\ \frac{1}{\alpha^2},\ \frac{1}{\sqrt{\alpha}}\right\},$$

$$\Gamma(\alpha^2)=\left\{\alpha^2+1,\ \frac{\alpha^2}{\alpha^2+1},\ \frac{1}{\alpha^2},\ \alpha^4,\ \alpha\right\}$$

$$\Gamma(\sqrt{\alpha})=\left\{\sqrt{\alpha}+1,\ \frac{\sqrt{\alpha}}{\sqrt{\alpha}+1},\ \frac{1}{\sqrt{\alpha}},\ \alpha,\ \sqrt[4]{\alpha}\right\}$$

となるが、$\alpha^8\neq\alpha$ ならば右辺に出てくるものは形が違えば値も違うことがわかる。したがって

$$\Gamma_1(\alpha)=\left\{\alpha+1,\ \frac{\alpha}{\alpha+1},\ \frac{1}{\alpha}\right\},$$

$$\Gamma_2(\alpha)=\left\{\alpha^2,\ \sqrt{\alpha}\right\}$$

とおくと、

<u>補題2.</u> $\beta \in \Gamma_i(\alpha)$, $\gamma \in \Gamma_j(\alpha)$, $\beta \neq \gamma$ ならば

$$|\Gamma(\beta) \cap \Gamma(\gamma)| = \begin{cases} 4 & \alpha^8 = \alpha \\ 3 & \alpha^8 \neq \alpha, \quad i = j = 1 \\ 2 & \alpha^8 \neq \alpha, \quad i \neq j \\ 1 & \alpha^8 \neq \alpha, \quad i = j = 2 \end{cases}$$

となる。したがって

$$\begin{aligned} \Omega_2 &= GF(q) - GF(8) \\ &= \{\alpha \in GF(q) \mid \alpha^8 \neq \alpha\} \end{aligned}$$

とおくと、

$$\alpha \notin \Omega_2 \Longrightarrow \alpha^x \notin \Omega_2,$$

$$\alpha \in \Omega_2 \Longrightarrow \Gamma_i(\alpha)^x = \Gamma_i(\alpha^x) \qquad i = 1, 2$$

が成り立つ。

次に、α, β, γ を $GF(q)$ の異なる3点とすると、$\{\infty, \alpha, \beta, \gamma\}$ を含む block が5個存在するはずであるが、それを計算すると、

$$\{\infty, \alpha, \beta, \gamma, \delta\} \in \mathcal{D} \Longleftrightarrow \delta \in \Gamma(\alpha, \beta, \gamma)$$

となる。ただし

$$\Gamma(\alpha, \beta, \gamma) = \left\{ \alpha+\beta+\gamma, \frac{\alpha\beta+\gamma^2}{\alpha+\beta}, \frac{\beta\gamma+\alpha^2}{\beta+\gamma}, \frac{\gamma\alpha+\beta^2}{\gamma+\alpha}, \right.$$

$$\sqrt{\alpha\beta+\beta\gamma+\gamma\alpha}\}$$

とおく。

補題2と同じように、$\delta, \varepsilon \in \Gamma(\alpha, \beta, \gamma)$ に対し、

$$|\Gamma(\alpha, \beta, \delta) \cap \Gamma(\alpha, \beta, \varepsilon)|$$

を計算することにより、次の補題が得られる。

<u>補題3.</u> $\dfrac{\alpha+\gamma}{\alpha+\beta} \in \Omega_2$ ならば、

$$(\alpha+\beta+\gamma)^x = \alpha^x+\beta^x+\gamma^x,$$
$$\sqrt{\alpha\beta+\beta\gamma+\gamma\alpha}^{\,x} = \sqrt{\alpha^x\beta^x+\beta^x\gamma^x+\gamma^x\alpha^x}$$

が成り立つ。

変数に特殊な値を代入することにより、以下の補題が次々に得られる。

<u>補題4</u> $\dfrac{\beta}{\alpha} \in \Omega_2$ ならば

$$(\alpha+\beta)^x = \alpha^x+\beta^x$$
$$\sqrt{\alpha\beta}^{\,x} = \sqrt{\alpha^x\beta^x}$$

が成り立つ。

<u>補題5</u> $\alpha \in \Omega_2$ ならば

$$\sqrt{\alpha}^{\,x} = \sqrt{\alpha^x}$$

$$(\alpha^{-1})^x = (\alpha^x)^{-1}$$

が成り立つ。

補題 6　任意の $\alpha, \beta \in GF(q)$ に対し、

$$(\alpha+\beta)^x = \alpha^x + \beta^x$$

が成り立つ。

証明　$\frac{\beta+\gamma}{\alpha+\gamma}, \frac{\gamma}{\alpha}, \frac{\gamma}{\beta} \in \Omega_2$ ならば、

$$\begin{aligned}(\alpha+\beta)^x &= ((\alpha+\gamma)+(\gamma+\beta))^x \\ &= (\alpha+\gamma)^x + (\gamma+\beta)^x \\ &= (\alpha^x+\gamma^x)+(\gamma^x+\beta^x) \\ &= \alpha^x+\beta^x\end{aligned}$$

となる。ところが、$\frac{\beta+\gamma}{\alpha+\gamma}, \frac{\gamma}{\alpha}, \frac{\gamma}{\beta}$ のうち少なくとも1つが Ω_2 に入らないような γ は高々 $8\times 3 = 24$ 個しか存在しないので、上の条件を満たすような γ が存在する。

上と同様にして以下の補題が次々証明される。

補題 7　$\frac{\beta}{\alpha} \in \Omega_2$ ならば

$$(\alpha\beta)^x = \alpha^x\beta^x$$

が成り立つ。

<u>補題 8</u>　任意の $\alpha, \beta \in GF(q)$ に対し

$$\sqrt{\alpha\beta}^{\,x} = \sqrt{\alpha^x \beta^x}$$

が成り立つ。

<u>補題 9</u>　任意の $\alpha \in GF(q)$ に対し

$$\sqrt{\alpha}^{\,x} = \sqrt{\alpha^x}$$

が成り立つ。

<u>補題 10</u>　任意の $\alpha, \beta \in GF(q)$ に対し

$$(\alpha\beta)^x = \alpha^x \beta^x$$

が成り立つ。

補題 6 と補題 10 より x は $GF(q)$ 上に体の自己同型として作用していることがわかり、定理の証明が終った。