Pure Mathematics 理论数学, 2019, 9(4), 540-545
Published Online June 2019 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2019.94071

$PSL(2,2^n)$ and Simple 3-$(2^n + 1,2ld + 1,\lambda)$ Designs Where l Is Odd, $d|(2^n - 1)$ and $d \geq 3$

Lele Wei, Weixia Li*

School of Mathematics and Statistics, Qingdao University, Qingdao Shandong
Email: 1025910224@qq.com, *liweixia99@163.com

Received: Jun. 4th, 2019; accepted: Jun. 14th, 2019; published: Jun. 27th, 2019

Abstract

Let $X = GF(q) \cup \{\infty\}$ be the projective line. Let l be an odd integer. The integer d satisfies $d \mid (2^n - 1)$ and $d \geq 3$. In this paper, we determined the parameter set of simple 3-designs from $PSL(2,2^n)$ with block size $2ld + 1$ where the stabilizer of the initial block contains order d element of $PSL(2,2^n)$ and calculated the number of the orbits which form the simple 3-design with that parameter set. By using the orbits of $PSL(2,2^n)$ on the X, the results show that the number of the orbits is $\frac{1}{2l}\prod_{i=1}^{2l-1}\frac{2^n-1-id}{d}$ which forms the simple $3\text{-}\left(2^n+1, 2ld+1, 2l(2ld-1)(2ld+1)\right)$ design.

Keywords

Simple *t*-Designs, Projective Special Linear Group, Automorphism Group

$PSL(2,2^n)$与单纯3-$(2^n + 1,2ld + 1,\lambda)$设计($l$为奇数，$d|(2^n - 1)$且$d \geq 3$)

魏乐乐，李伟霞*

青岛大学数学与统计学院，山东 青岛
Email: 1025910224@qq.com, *liweixia99@163.com

收稿日期：2019年6月4日；录用日期：2019年6月14日；发布日期：2019年6月27日

*通讯作者。

文章引用: 魏乐乐, 李伟霞. $PSL(2,2^n)$与单纯 3-$(2^n + 1,2ld + 1,\lambda)$设计($l$ 为奇数，$d|(2^n - 1)$且 $d \geq 3$) [J]. 理论数学, 2019, 9(4): 540-545. DOI: 10.12677/pm.2019.94071

摘　要

令 $X = GF(q)\cup\{\infty\}$ 是射影直线。设l为奇数，d为满足 $d\mid(2^n-1)$ 且$d\geq 3$的正整数。本文确定了以$PSL(2,2^n)$为自同构群，区组长度为$2ld+1$，初始区组的稳定子群中含有d阶元的单纯3-设计的参数，并计算了构成这一参数的轨道的条数。利用$PSL(2,2^n)$在X上作用的轨道，得到如下结论：这类单纯3-设计的参数为 $3\text{-}\left(2^n+1,2ld+1,2l(2ld-1)(2ld+1)\right)$，构成这一设计的轨道的条数为 $\frac{1}{2l}\prod_{i=1}^{2l-1}\frac{2^n-1-id}{d}$。

关键词

单纯t-设计，射影特殊线性群，自同构群

1. 引言

1.1. 研究背景

参数为t-(v,k,λ)的一个设计，简称t-设计，定义为符合以下条件的一对符号$(X,\mathfrak{B})$：

1) X是一个v-集合；

2) $\mathfrak{B}$是X的一组k-子集；

3) X的任意给定的t-子集都恰好含于$\mathfrak{B}$的λ个成员之中。

X的元素称为点，$\mathfrak{B}$的成员称为区组。若一个t-(v,k,λ)设计不包含重复的区组，则称这个设计为单纯的。在本文中我们只考虑单纯t-设计。

令$G\leq sym(X)$，则对于任意的$g\in G$，$S\subseteq X$，$S^g=\{x^g:x\in S\}$。$S^G=\{S^g:g\in G\}$称为S的轨道，$G_S=\{g\in G:S^g=S\}$称为S的稳定子群，且$|G|=|S^G||G_S|$。$(X,\mathfrak{B})$的一个自同构是指具有下述性质的X的置换g：如果$B\in\mathfrak{B}$，则$B^g\in\mathfrak{B}$。G是$(X,\mathfrak{B})$的自同构群当且仅当区组集$\mathfrak{B}$是G作用下X的k-子集的轨道的并。

令q为素数幂，$X=GF(q)\cup\{\infty\}$为射影直线。对任意的$a,b,c,d\in GF(q)$，定义$a/0=\infty$，$a/\infty=0$，$\infty+a=a+\infty=\infty$，$(a\infty+b)/(c\infty+d)=a/c$。所有行列式为非零平方元的线性分式的集合构成线性分式群$LF(2,q)$，它同构于$PSL(2,q)$。即

$$LF(2,q)=\left\{f\,\middle|\,f:X\to X,x^f=\frac{ax+b}{cx+d},ad-bc\text{为非零平方元}\right\}.$$

设$q=p^n$，其中p为素数。利用$PSL(2,q)$为设计的自同构群来研究t-设计是一个可行的方法。特别的，文献[1]已完整解决了以$PSL(2,q)$为自同构群，区组长度为k的3-设计的存在性问题，其中$k\neq 0,1(\mathrm{mod}\ p)$。文献[2] [3] [4] [5]完整讨论了以$PSL(2,2^n)$为自同构群，区组长度为$k$($4\leq k\leq 8$)的单纯3-设计的存在性问题。文献[6] [7]介绍了以$PSL(2,2^n)$为自同构群，区组长度为d和$d+1$的单纯3-设计的有关结果，这里$d\mid(2^n-1)$。文献[8]-[13]找到了一些$t\geq 4$时的t-设计存在的例子。

注意到当 $q=2^n$ 时，对于任意的区组长度 k 总满足 $k\equiv 0,1(\bmod 2)$。又 $PSL(2,2^n)=PGL(2,2^n)$ 在 X 上的作用是精确 3 重传递的，故任意不相交的 k-子集的轨道的并可构成单纯 $3-(2^n+1,k,\lambda)$ 设计，其中 λ 为正整数。

本文只考虑 $q=2^n$ 的情形。用 $\mathcal{G}$ 表示 $PSL(2,2^n)$，用 $X=GF(2^n)\cup\{\infty\}$ 表示射影直线。总假设 l 为奇数，d 为满足 $d\mid(2^n-1)$ 且 $d\geq 3$ 的整数。利用 $PSL(2,2^n)$ 在 X 上作用的轨道，确定了以 $PSL(2,2^n)$ 为自同构群，区组长度为 $2ld+1$，初始区组的稳定子群中含有 d 阶元的单纯 3-设计的参数，并计算了满足这一参数的轨道的条数。得到了如下结果：

定理： 令 B 为 $\mathcal{G}$ 中一个 d 阶元的 $2l$ 个 d 圈及其一个不动点所构成的 X 的 $2ld+1$-子集，则 $(X,B^{\mathcal{G}})$ 构成一个 3-$(2^n+1,2ld+1,2l(2ld-1)(2ld+1))$ 设计。构成这一设计的轨道的条数为 $\dfrac{1}{2l}\prod_{i=1}^{2l-1}\dfrac{2^n-1-id}{d}$。

1.2. 预备知识

引理 1 [14]： 设 $g\in\mathcal{G}$，g 的阶为 h 且 $h>1$，则 g 有 a 个不动点和 $b=(2^n+1-a)/h$ 个 h 圈。其中当 $h=2$ 时，$a=1$；当 $h\mid(2^n-1)$ 时，$a=2$；当 $h\mid(2^n+1)$ 时，$a=0$。

注： 由引理 1 易知若 B 为 X 的一个 k-子集，$g\in\mathcal{G}_B$ 当且仅当 B 由 g 的 q 个 h 圈和 r 个不动点构成，其中 $k=hq+r$，$0\leq r<h$。

引理 2 [14]： $\mathcal{G}$ 的一个非平凡子群必为下列之一：

1) 2^h 阶初等 $Abel$ 群，其中 $h\leq n$；
2) d 阶循环群，其中 $d\mid(2^n\mp 1)$；
3) 二面体群 D_{2d}，其中 $d\mid(2^n\mp 1)$；
4) 2^h 阶的初等 $Abel$ 群和 d 阶循环群的半直积，其中 $d\mid(2^n-1)$；
5) $PSL(2,2^k)$，其中 $k\mid n$；
6) 交错群 A_4。

引理 3 [6]： 类型(4)的子群不可能是 $2d$ 阶的。

引理 4 [14]： 所有二面体群 D_{2d} 在 $\mathcal{G}$ 中共轭。

以下总假设 $d\mid(2^n-1)$ 且 $d\geq 3$，α 为 $GF^*(2^n)$ 中的一个 d 阶元，$x^{f_1}=\alpha x$，$x^{f_2}=\dfrac{1}{x}$，$G=\langle f_1,f_2\rangle$，m 为任意正整数，l 为任意奇数。

引理 5 [6]： $G=\langle f_1,f_2\rangle$ 为一个二面体群 D_{2d}。

引理 6 [7]： 若 S 为一个 $d+1$-子集，则无二面体群 D_{2d} 包含在 $\mathcal{G}_S$ 中。

由引理 6 易得下面的推论。

推论 1： 若 S 为一个 $md+1$-子集，则无二面体群 D_{2d} 包含在 $\mathcal{G}_S$ 中。

证明： 若存在一个二面体群 $D_{2d}\subseteq\mathcal{G}_S$，由引理 4 及引理 5 知存在 $g\in\mathcal{G}$，使得 $g^{-1}D_{2d}g=G\subseteq\mathcal{G}_{S^g}$。由引理 1 知 S^g 由 f_1 的 m 个 d 圈和 1 个不动点构成，则 S^g 中恰包含 0 和 ∞ 中的一个元素。又因为 $f_2\in G\subseteq\mathcal{G}_{S^g}$，由此推得若 $0\in S^g$ 必有 $\infty\in S^g$，产生矛盾。证毕。

引理 7 [6]： 若 S 为 X 的 k-子集，则 $(X,S^{\mathcal{G}})$ 是一个单纯 3-$(2^n+1,k,\lambda)$ 设计，其中 $\lambda=\dfrac{k(k-1)(k-2)}{|\mathcal{G}_S|}$。

2 定理的证明

引理 8： 令 B 为 $\mathcal{G}$ 中一个 d 阶元的 $2l$ 个 d 圈及其一个不动点所构成的 X 的 $2ld+1$-子集，则 $(X,B^{\mathcal{G}})$

构成一个 3-$\left(2^n+1,2ld+1,2l\left(2ld-1\right)\left(2ld+1\right)\right)$ 设计。

证明： 由于 $\mathcal{G}_B$ 中有 d 阶元，由引理 2 知 $\mathcal{G}_B$ 不为类型(1)。由推论 1 知 $\mathcal{G}_B$ 不为类型(3)。进一步的 $\mathcal{G}_B$ 不为类型(5)，否则存在一个二面体群 D_{2d} 包含在 $\mathcal{G}_B$ 中，与推论 1 矛盾。又类型(6)是类型(4)的一种情形，综上述 $\mathcal{G}_B$ 只能为类型(2)或类型(4)的子群。可设 $\left|\mathcal{G}_B\right|=2^h d$，其中 h 为非负整数。由引理 7 知 $\lambda=\dfrac{\left(2ld+1\right)2ld\left(2ld-1\right)}{2^h d}$ 为整数，又 l 是奇数，故 $h=0$ 或 1。再由引理 3 知 $h=0$。故 $\left(X,B^{\mathcal{G}}\right)$ 构成一个 3-$\left(2^n+1,2ld+1,2l\left(2ld-1\right)\left(2ld+1\right)\right)$ 设计。

推论 2： 令 S 为 X 的 $2ld+1$-子集，若 $\mathcal{G}_S$ 中有 d 阶元，则 $\mathcal{G}_S$ 为 d 阶循环群。

引理 9： 设 S 是 X 的 $md+1$-子集，若 $\mathcal{G}_S$ 中有 d 阶元，则轨道 $S^{\mathcal{G}}$ 中包含形如 $\left\{1,\alpha,\cdots,\alpha^{d-1},\beta_1,\beta_1\alpha,\cdots,\beta_1\alpha^{d-1},\cdots,\beta_{m-1},\beta_{m-1}\alpha,\cdots,\beta_{m-1}\alpha^{d-1},\infty\right\}$ 的区组。其中 α 为 $GF^*\left(2^n\right)$ 中的一个 d 阶元，$\beta_i\in GF^*\left(2^n\right)$（$i=1,2,\cdots,m-1$）。

引理 10： 若 $\left(X,\Gamma\right)$ 是一个 3-$\left(2^n+1,md+1,m\left(md-1\right)\left(md+1\right)\right)$ 设计，则轨道 Γ 中包含 m 个形如 $\left\{1,\alpha,\cdots,\alpha^{d-1},\beta_1,\beta_1\alpha,\cdots,\beta_1\alpha^{d-1},\cdots,\beta_{m-1},\beta_{m-1}\alpha,\cdots,\beta_{m-1}\alpha^{d-1},\infty\right\}$ 的区组。其中 α 为 $GF^*\left(2^n\right)$ 中的一个 d 阶元，$\beta_i\in GF^*\left(2^n\right)\left(i=1,2,\cdots,m-1\right)$。

证明： 设 S 为轨道 Γ 中的一个区组。由引理 7 得 $\left|\mathcal{G}_S\right|=d$，即 d 阶循环群。由引理 9 可设

$$S=\left\{1,\alpha,\cdots,\alpha^{d-1},\beta_1,\beta_1\alpha,\cdots,\beta_1\alpha^{d-1},\cdots,\beta_{m-1},\beta_{m-1}\alpha,\cdots,\beta_{m-1}\alpha^{d-1},\infty\right\}.$$

若

$$S'=\left\{1,\alpha,\cdots,\alpha^{d-1},\beta_1',\beta_1'\alpha,\cdots,\beta_1'\alpha^{d-1},\cdots,\beta_{m-1}',\beta_{m-1}'\alpha,\cdots,\beta_{m-1}'\alpha^{d-1},\infty\right\}$$

与 S 位于同一条轨道，则存在 $\mathcal{G}$ 中的一个线性分式 f'，使得 $S^{f'}=S'$。设 $x^{f'}=\dfrac{ax+b}{cx+d}$，$x^{f_1}=\alpha x$。由于 $\left|\mathcal{G}_S\right|=\left|\mathcal{G}_{S'}\right|=d$ 且 $f_1\in\mathcal{G}_{S'}\cap\mathcal{G}_S$，从而 $\mathcal{G}_S=\mathcal{G}_{S'}=\left\langle f_1\right\rangle$。又 $\mathcal{G}_{S'}=f'^{-1}\mathcal{G}_S f'$，由此可得 $f'\mathcal{G}_S=\mathcal{G}_S f'$。即 $\left\{f',f'f_1,\cdots,f'f_1^{d-1}\right\}=\left\{f',f_1f',\cdots,f_1^{d-1}f'\right\}$。对于 $1\le i\le d-1$，若 $f'f_1=f_1^i f'$，则对任意的 $x\in X$，有 $x^{f'f_1}=x^{f_1^i f'}$。即

$$\frac{a\alpha x+b\alpha}{cx+d}=\frac{a\alpha^i x+b}{c\alpha^i x+d}.$$

由上述等式知存在 $u\in GF^*\left(2^n\right)$，使得

$$\begin{bmatrix}a\alpha & b\alpha\\ c & d\end{bmatrix}=u\begin{bmatrix}a\alpha^i & b\\ c\alpha^i & d\end{bmatrix}.$$

故只能 $u=1$，$b=c=0$ 且 $i=1$。即 $f'f_1=f_1f'$。可令 $x^{f'}=rx$，其中 $r=\dfrac{a}{d}$。因此

$$S'=S^{f'}=\left\{r,r\alpha,\cdots,r\alpha^{d-1},r\beta_1,r\beta_1\alpha,\cdots,r\beta_1\alpha^{d-1},\cdots,r\beta_{m-1},r\beta_{m-1}\alpha,\cdots,r\beta_{m-1}\alpha^{d-1},\infty\right\}.$$

又 $S'=\left\{1,\alpha,\cdots,\alpha^{d-1},\beta_1',\beta_1'\alpha,\cdots,\beta_1'\alpha^{d-1},\cdots,\beta_{m-1}',\beta_{m-1}'\alpha,\cdots,\beta_{m-1}'\alpha^{d-1},\infty\right\}$，令 $H=\left\langle\alpha\right\rangle$，从而 $r\in H$ 或 $r\in\beta_j'H$，其中 $1\le j\le m-1$。下分两种情况讨论：

1) 若 $r\in H$，从而 $S'=S$。

2) 若 $r\in\beta_j'H$，不失一般性，可令 $r\in\beta_1'H$，从而

$$S'=\left\{\beta_1',\beta_1'\alpha,\cdots,\beta_1'\alpha^{d-1},\beta_1'\beta_1,\beta_1'\beta_1\alpha,\cdots,\beta_1'\beta_1\alpha^{d-1},\cdots,\beta_1'\beta_{m-1},\beta_1'\beta_{m-1}\alpha,\cdots,\beta_1'\beta_{m-1}\alpha^{d-1},\infty\right\}.$$

故对于 $1\le k\le m-1$，必存在 $\beta_1'\beta_k\in H$。即

$$S'=\left\{\beta_k^{-1},\beta_k^{-1}\alpha\cdots\beta_k^{-1}\alpha^{d-1},\beta_k^{-1}\beta_1,\beta_k^{-1}\beta_1\alpha,\cdots,\beta_k^{-1}\beta_1\alpha^{d-1},\cdots,\beta_k^{-1}\beta_{m-1},\beta_k^{-1}\beta_{m-1}\alpha,\cdots,\beta_k^{-1}\beta_{m-1}\alpha^{d-1},\infty\right\}.$$

令 $x^{g_k}=\beta_k^{-1}x$ $(k=0,1,\cdots,m-1)$，其中 $\beta_0=1$，则上述 $S'=S^{g_k}$。综上述若 $S'\in S^{\mathcal{G}}$ 当且仅当 $S'=S^{g_k}$ $(k=0,1,\cdots,m-1)$。

下证 $S,S^{g_1},S^{g_2},\cdots,S^{g_{m-1}}$ 互不相同。由此说明 Γ 中包含 m 个形如 $\left\{1,\alpha,\cdots,\alpha^{d-1},\beta_1,\beta_1\alpha,\cdots,\beta_1\alpha^{d-1},\cdots,\beta_{m-1},\beta_{m-1}\alpha,\cdots,\beta_{m-1}\alpha^{d-1},\infty\right\}$ 的区组。对于任意的 $0\le s,t\le m-1$，若 $S^{g_s}=S^{g_t}$，则 $g_sg_t^{-1}\in\mathcal{G}_S=\langle f_1\rangle$，即 $\beta_s^{-1}\beta_t\in H$。从而 $\beta_s^{-1}\beta_t\left\{1,\alpha,\cdots,\alpha^{d-1}\right\}=\left\{1,\alpha,\cdots,\alpha^{d-1}\right\}$，即

$$\left\{\beta_t,\beta_t\alpha,\cdots,\beta_t\alpha^{d-1}\right\}=\left\{\beta_s,\beta_s\alpha,\cdots,\beta_s\alpha^{d-1}\right\}.$$

这是不可能的。

引理 11： 构成 3-$\left(2^n+1,2ld+1,2l(2ld-1)(2ld+1)\right)$ 设计的轨道的条数为 $\frac{1}{2l}\prod_{i=1}^{2l-1}\frac{2^n-1-id}{d}$。

证明： 设 l 为奇数，α 为 $GF^*\left(2^n\right)$ 中的一个 d 阶元，$\beta_i\in GF^*\left(2^n\right)$（$i=1,2,\cdots,2l-1$）。令 $\mathcal{B}=\left\{S\middle|S=\left\{1,\alpha,\cdots,\alpha^{d-1},\beta_1,\beta_1\alpha,\cdots,\beta_1\alpha^{d-1},\cdots,\beta_{2l-1},\beta_{2l-1}\alpha,\cdots,\beta_{2l-1}\alpha^{d-1},\infty\right\}\right\}$，易得 $\mathcal{B}$ 中元素的个数为 $\prod_{i=1}^{2l-1}\frac{2^n-1-id}{d}$。再由引理 10 可得构成 3-$\left(2^n+1,2ld+1,2l(2ld-1)(2ld+1)\right)$ 设计的轨道条数为 $\frac{1}{2l}\prod_{i=1}^{2l-1}\frac{2^n-1-id}{d}$。

定理： 令 B 为 $\mathcal{G}$ 中一个 d 阶元的 $2l$ 个 d 圈及其一个不动点所构成的 X 的 $2ld+1$-子集，则 $\left(X,B^{\mathcal{G}}\right)$ 构成一个 3-$\left(2^n+1,2ld+1,2l(2ld-1)(2ld+1)\right)$ 设计。构成这一设计的轨道的条数为 $\frac{1}{2l}\prod_{i=1}^{2l-1}\frac{2^n-1-id}{d}$。

证明： 利用引理 8 和引理 11 可以得到定理。

推论 3： 令 B 为 $\mathcal{G}$ 中一个 d 阶元的 $2l$ 个 d 圈及其一个不动点所构成的 X 的 $2ld+1$-子集，则对于任意的正整数 t，其中 $1\le t\le\frac{1}{2l}\prod_{i=1}^{2l-1}\frac{2^n-1-id}{d}$，可构造出单纯 3-$\left(2^n+1,2ld+1,2l(2ld-1)(2ld+1)\right)$ 设计。

致　谢

衷心感谢导师李伟霞在本文写作过程中的悉心指导！

参考文献

[1] Cameron, P.J., Maimani, H.R., Omidi, G.R. and Tayfeh-Rezaie, B. (2006) 3-Designs from $PSL(2,q)$. *Discrete Mathematics*, **306**, 3063-3073. https://doi.org/10.1016/j.disc.2005.06.041

[2] Keranen, M.S. and Kreher, D.L. (2004) 3-Designs of $PSL\left(2,2^n\right)$ with Block Sizes 4 and 5. *Journal of Combinarorial Designs*, **12**, 103-111. https://doi.org/10.1002/jcd.10068

[3] Li, W. and Shen, H. (2008) Simple 3-Designs of $PSL\left(2,2^n\right)$ with Block Size 6. *Discrete Mathematics*, **308**, 3061-3072. https://doi.org/10.1016/j.disc.2007.08.030

[4] Li, W. and Shen, H. (2010) Simple 3-Designs of $PSL\left(2,2^n\right)$ with Block Size 7. *Journal of Combinarorial Designs*, **16**, 1-17. https://doi.org/10.1002/jcd.20141

[5] Gong, L.Z. and Fan, G.B. (2018) Simple 3-Designs of $PSL\left(2,2^n\right)$ with Block Size 8. *Utilitas Mathematica*, **106**, 3-9.

[6] 李伟霞. 区组长度为 2^n-1 因子的单纯 3-设计[J]. 上海交通大学学报, 2007, 41(5): 845-847.

[7] Li, W. and Shen, H. (2011) Simple 3-Designs with Block Sizes $d+1$ from $PSL\left(2,2^n\right)$ Where $d\mid\left(2^n-1\right)$. *Journal*

of Combinarorial Designs, **51**, 235-241.

[8] Bierbrauer, J. (1993) A Family of 4-Designs with Block Size 9. *Discrete Mathematics*, **138**, 113-117. https://doi.org/10.1016/0012-365X(94)00192-L

[9] 刘伟俊, 谭琼华, 龚罗中. 旗传递 5-$(v,k,2)$ 设计[J]. 江苏大学学报, 2010, 31(5): 612-615.

[10] 刘伟俊, 姚蹈, 陈静. 一般射影线性群 $PSL(2,q)$ 与 4-$(q+1,5,\lambda)$ 设计[J]. 数学理论与应用, 2010, 30(1): 123-128.

[11] 陈静, 陈暑波, 刘伟俊. 二维射影线性群与区传递 4-$(v,6,\lambda)$ 设计[J]. 中国科学, 2010, 40(11): 1045-1054.

[12] 唐剑雄, 陈静, 刘伟俊, 等. 二维射影线性群与区传递 4-$(q+1,5,\lambda)$ 设计[J]. 数学进展, 2012, 41(5): 547-553.

[13] 杨冠, 刘伟俊. 射影线性群区传递作用于 5-$(q+1,7,\lambda)$ 设计[J]. 浙江大学学报, 2013, 40(5): 489-491.

[14] Dickson, L.E. (1958) Linear Groups with an Introduction to the Galois Field Theory. Dover Publications, New York, 260-287.