Pure Mathematics 理论数学, 2021, 11(10), 1685-1690
Published Online October 2021 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2021.1110188

Hans汉斯

单纯3-设计与群$\mathrm{PSL}(2,q)$，$q\equiv 1(\mathrm{mod}4)$

韦萌萌，李伟霞*

青岛大学数学与统计学院，山东 青岛

收稿日期：2021年9月5日；录用日期：2021年10月6日；发布日期：2021年10月13日

摘 要

在本文中，我们以特殊射影线性群$\mathrm{PSL}(2,q)$为自同构群，考虑了$\mathrm{PSL}(2,q)$在射影直线$X=GF(q)\cup\{\infty\}$上的作用，其中q是一个素数幂且$q\equiv 1(\mathrm{mod}4)$。通过取$\mathrm{PSL}(2,q)$作用下的轨道的并，我们构建了一些单纯3-设计。

关键词

3-齐次的，自同构群，3-设计

Simple 3-Designs and Group $\mathrm{PSL}(2,q)$, $q\equiv 1(\mathrm{mod}4)$

Mengmeng Wei, Weixia Li*

School of Mathematics and Statistics, Qingdao University, Qingdao Shandong

Received: Sep. 5th, 2021; accepted: Oct. 6th, 2021; published: Oct. 13th, 2021

Abstract

In this paper, we consider the action of $\mathrm{PSL}(2,q)$ acting as a group of automorphisms on the projective line $X=GF(q)\cup\{\infty\}$, where q is a prime power and congruent to 1 modulo 4. We construct some simple 3-designs by taking a union of orbits under the action of $\mathrm{PSL}(2,q)$.

*通讯作者。

文章引用: 韦萌萌, 李伟霞. 单纯 3-设计与群 $\mathrm{PSL}(2,q)$, $q\equiv 1(\mathrm{mod}4)$ [J]. 理论数学, 2021, 11(10): 1685-1690.
DOI: 10.12677/pm.2021.1110188

Keywords

3-Homogeneous, Automorphism Group, 3-Design

1. 引言

设 t,v,k 和 λ 是整数，其中 $0<t\le k<v$，$\lambda>0$。令 X 是一个 v-集合，$\mathcal{B}$ 是 X 的一组 k-子集，若 X 的任意给定的 t-子集都恰好出现在 $\mathcal{B}$ 的 λ 个成员之中，则称有序对 $(X,\mathcal{B})$ 是一个 t-(v,k,λ) 设计，其中 X 的元素称为点，$\mathcal{B}$ 中的成员称为区组。若 $\mathcal{B}$ 中的任意两个区组都不相同，则称这个设计为单纯的。在本文中，我们只考虑单纯 t-设计。

设 $G\le sym(X)$，对于任意 $g\in G$，$S\subseteq X$，令 $g(S)=\{g(x)\mid x\in S\}$。$G(S)=\{g(S)\mid g\in G\}$ 和 $G_S=\{g\in G\mid g(S)=S\}$ 分别称为 S 的轨道和稳定子群，且 $|G|=|G(S)||G_S|$ [1]。长度为 $|G|$ 的轨道 $G(S)$ 称为正则轨道，即 $|G(S)|=|G|$，其它的轨道称为非正则轨道。对于任意的 $x,y\in X$，若存在 $g\in G$ 使 $g(x)=y$，则称 G 在 X 上的作用是传递的。若 G 在集合 $P_k(X)$ 上的作用是传递的，其中 $P_k(X)$ 是 X 的所有 k-子集的集合，则称 G 是 k-齐次的。

在本文中，设 $q=p^n$，其中 $q\equiv 1(\bmod 4)$ 且 p 为素数，$X=GF(q)\cup\{\infty\}$ 为射影直线。对于任意的 $a,b,c,d\in GF(q)$，定义映射 f：

$$x\mapsto\frac{ax+b}{cx+d}=f(x),$$

其中 $ad-bc$ 是 $GF(q)$ 中的一个非零平方元。所有形如 f 的映射的集合构成一个群，称为射影特殊线性群 $\mathrm{PSL}(2,q)$。以下总是用 G 表示 $\mathrm{PSL}(2,q)$。

当 $q\equiv 3(\bmod 4)$ 时，群 G 是 3-齐次的，即 G 作用在集合 $P_3(X)$ 上是传递的。因此，G 在 $P_k(X)$ 上作用的轨道可以构造出单纯 3-设计。文献[2] [3]给出了以 G 为自同构群，区组长度为 4，5 和 6 的单纯 3-设计的完整结果。目前，这种设计的最好结果在文献[4]中，给出了所有以 G 为自同构群，区组长度为 k 的所有单纯 3-设计，其中 $k\not\equiv 0,1(\bmod p)$。然而，当 $q\equiv 1(\bmod 4)$ 时，G 不是 3-齐次的。因此，G 在 $P_k(X)$ 上作用的轨道不一定能构造出单纯 3-设计。但在文献[5]中提供了一种方法，可以利用 G 在 $P_k(X)$ 上作用的轨道的并来构造单纯 3-设计。通过这种方法，文献[6] [7]找到了一些单纯 3-设计存在的例子。

本文在文献[6] [7]的基础上，借助上述方法给出了其它单纯 3-设计的一些例子。

2. 预备知识

下面的引理给出了 G 的所有子群。

引理 1 [8] G 的一个子群必为下列之一：

1) p^m 阶初等 Abel 群，其中 $m\le n$；

2) 循环群 C_d，$d\mid\dfrac{q\pm 1}{2}$；

3) $2d$ 阶二面体群， $d\left|\frac{q\pm 1}{2}\right.$；

4) A_4；

5) S_4，当 $q^2\equiv 1(\mathrm{mod}16)$ 时；

6) p^m 阶初等 Abel 群和 d 阶循环群的半直积，其中 $d\left|\frac{q-1}{2}\right.$ 且 $d\left|\left(p^m-1\right)\right.$；

7) A_5，当 $q^2\equiv 1(\mathrm{mod}5)$ 时；

8) $\mathrm{PSL}\left(2,p^m\right)$，其中 $m\mid n$；

9) $\mathrm{PGL}\left(2,p^m\right)$，其中 $2m\mid n$。

以下总假设 K 是群 G 的一个子群，N_l 表示 K 在 X 上作用的长度为l的轨道的条数。在文献[7] [9] [10]中都介绍了下面引理所列举的结果。

引理 2 设 K 是一个 d 阶循环群，则

1) 若 $d\left|\left(q+1\right)\right/2$，则 $N_d=\frac{q+1}{d}$；

2) 若 $d\left|\left(q-1\right)\right/2$，则 $N_1=2$，$N_d=\frac{q-1}{d}$；

3) 若 $d=p$，则 $N_1=1$，$N_d=\frac{q}{d}$。

引理 3 设 K 是一个 p^m 阶初等 Abel 群和一个 d 阶循环群的半直积，其中 $d\left|\frac{q-1}{2}\right.$ 且 $d\left|\left(p^m-1\right)\right.$，则 $N_1=1$，$N_{p^m}=1$ 且其他轨道是正则的。

引理 4 设 $K=\mathrm{PSL}\left(2,p^m\right)$，其中 $m\mid n$，则

1) 若 n/m 是奇数，则 $N_{p^m+1}=1$ 且其他轨道是正则的；

2) 若 n/m 是偶数，则 $N_{p^m+1}=1$，$N_{p^m\left(p^m-1\right)}=1$ 且其他轨道是正则的。

3. 主要结果

以下总假设 θ 是 $GF\left(q\right)$ 的一个本原元。下面的引理指出，我们可以通过 G 在 $P_k\left(X\right)$ 上作用轨道的并来构造一个 3-设计。设 $\mathcal{B}$ 是 X 的 k-子集的一个集合，Δ 是 X 的一个 t-子集，其中 $t<k$。令 $\lambda_{\mathcal{B}}\left(\Delta\right)$ 表示 $\mathcal{B}$ 中包含 Δ 的 k-子集的个数，即 $\lambda_{\mathcal{B}}\left(\Delta\right)=\left|\left\{B\mid B\in\mathcal{B},\Delta\subseteq B\right\}\right|$。

引理 5 [6]设 Γ 是 G 在 X 的 k-子集上作用的一个轨道，则

$$\lambda_{\Gamma}\left(\left\{0,1,\infty\right\}\right)=\lambda_{\theta\Gamma}\left(\left\{0,\theta,\infty\right\}\right),$$

$$\lambda_{\theta\Gamma}\left(\left\{0,1,\infty\right\}\right)=\lambda_{\Gamma}\left(\left\{0,\theta,\infty\right\}\right).$$

若 $\mathcal{B}=\Gamma\cup\theta\Gamma$，则 $\lambda_{\mathcal{B}}\left(\left\{0,1,\infty\right\}\right)=\lambda_{\mathcal{B}}\left(\left\{0,\theta,\infty\right\}\right)$。因此，$\left(X,\mathcal{B}\right)$ 是一个 3-$\left(q+1,k,\lambda\right)$ 设计，其中 $\lambda=\frac{k\left(k-1\right)\left(k-2\right)}{\left|G_B\right|}$。

以下我们总假设 $H=\left\{1,\theta^2,\theta^4,\cdots,\theta^{q-3}\right\}$，$f\left(x\right)=\theta^2x$，$g\left(x\right)=\frac{1}{x}$，其中 $x\in X$，则 $f,g\in G$，易见 $f,g\in G_H$。因 $\left|f\right|=\frac{q-1}{2}$，$\left|g\right|=2$，$gf=f^{-1}g$，故 $\left\langle f,g\right\rangle\cong D_{q-1}$，易见 $\left\langle f,g\right\rangle\subseteq G_H$。

定理 1 设 $q\equiv 1(\mathrm{mod}\,8)$，$q>11$ 且 $k=\frac{q-1}{2}$，则存在一个单纯 3-$\left(q+1,k,\frac{(k-1)(k-2)}{2}\right)$ 设计。

证明取 $B=H$，令 $\mathcal{B}=\Gamma\cup\theta\Gamma$，其中 $\Gamma=G(B)=\{g(B)\mid g\in G\}$，由引理 5 知，$(X,\mathcal{B})$ 是一个 3-$(q+1,k,\lambda)$ 设计，其中

$$\lambda=\frac{k(k-1)(k-2)}{|G_B|}.$$

因 $\langle f,g\rangle\subseteq G_B$，故 $(2k)\mid|G_B|$，可得 $\lambda\mid\frac{(k-1)(k-2)}{2}$。又 $q\equiv 1(\mathrm{mod}\,8)$，故 $k\equiv 0(\mathrm{mod}\,4)$，从而 $\frac{(k-1)(k-2)}{2}$为奇数，可得 λ 为奇数。所以 $(X,\mathcal{B})$ 是一个单纯 3-设计。

因 $\langle f,g\rangle\subseteq G_B$，由引理 1 知，$G_B$ 不为循环群或初等 Abel 群。又 $|f|=k>5$，故 G_B 中含有阶数大于 5 的元素，从而 G_B 不为 A_4，S_4 或 A_5。又 $k=\frac{q-1}{2}$，故 $(k,p)=1$。若 G_B 是阶数为 p^md 的半直积，则 $(2k)\mid p^md$。又 p 是奇素数，故 $(2k,p^m)=1$，所以 $(2k)\mid d$，可得 $d>k$。由引理 2 知，这是不可能的。

若 $G_B=\mathrm{PSL}(2,p^m)$，其中 $m\mid n$，则 B 是由 $\mathrm{PSL}(2,p^m)$ 在 X 上作用的轨道的并构成。由引理 4 知，$|B|\geq p^m+1$。又 $f\in G_B$ 且 $|B|=k$，故 G_B 中元素的最大阶为 k。而 $\mathrm{PSL}(2,p^m)$ 中元素的最大阶为 $\frac{p^m+1}{2}$，故 $k=\frac{p^m+1}{2}$，即 $|B|=\frac{p^m+1}{2}$，与 $|B|\geq p^m+1$ 矛盾。

若 $G_B=\mathrm{PGL}(2,p^m)$，其中 $(2m)\mid n$，则 G_B 中元素的最大阶为 p^m+1。因此 $k=p^m+1$，即

$$p^m+1=\frac{q-1}{2}=\frac{p^n-1}{2},$$

可得 $p^m\mid 3$。所以 $p=3$，$m=1$，故 $k=4$，与 $k>5$ 矛盾。

综上所述，G_B 是阶数为 $2d$ 的二面体群，其中 $d\mid\frac{q\pm1}{2}$。因 $f\in G_B$，故 $d=\frac{q-1}{2}$，从而 $G_B=\langle f,g\rangle$，所以 $\lambda=\frac{(k-1)(k-2)}{2}$。

定理 2 设 $q\equiv 1(\mathrm{mod}\,8)$，$q>11$ 且 $k=\frac{q-1}{2}+2$，则存在一个单纯 3-$\left(q+1,k,\frac{k(k-1)}{2}\right)$ 设计。

证明取 $B=H\cup\{0,\infty\}$，易知 $f,g\in G_B$ 且 $\langle f,g\rangle\subseteq G_B$。令 $\mathcal{B}=\Gamma\cup\theta\Gamma$，其中 $\Gamma=G(B)=\{g(B)\mid g\in G\}$，由引理 5 知，$(X,\mathcal{B})$ 是一个 3-$(q+1,k,\lambda)$ 设计，其中

$$\lambda=\frac{k(k-1)(k-2)}{|G_B|}.$$

因 $\langle f,g\rangle\subseteq G_B$，故 $(2k-4)\mid|G_B|$，从而 $\lambda\mid\frac{k(k-1)}{2}$。又 $q\equiv 1(\mathrm{mod}\,8)$，故 $k\equiv 2(\mathrm{mod}\,4)$，从而 $\frac{k(k-1)}{2}$为奇数，可得λ为奇数。所以，$(X,\mathcal{B})$ 是一个单纯 3-设计。

因 $\langle f,g\rangle\subseteq G_B$，由引理 1 知，$G_B$ 不为循环群或初等 Abel 群。又 $k>7$，则 $|f|=k-2>5$，从而 G_B 中含有阶数大于 5 的元素，所以 G_B 不为 A_4，S_4 或 A_5。又 $k=\frac{q-1}{2}+2$，故 $(k-2,p)=1$。若 G_B 是阶数为 p^md

的半直积，则$(2k-4)\mid p^m d$。又p是奇素数，故$(2,p)=1$，从而$(2(k-2),p)=1$，所以$(2k-4)\mid d$，可得$d>k$。由引理2知，这是不可能的。

若$G_B=\mathrm{PSL}(2,p^m)$，其中$m\mid n$，则G_B中元素的最大阶为$\frac{p^m+1}{2}$，而G_B中含有阶数为$k-2$的元素，故$k-2\le\frac{p^m+1}{2}$，即$q\le p^m+2$。所以$m=n$，即$G_B=\mathrm{PSL}(2,q)$，从而G_B中含有$\frac{q+1}{2}$阶元h_1，而h_1无不动点，与$k=\frac{q+1}{2}+1$矛盾。

若$G_B=\mathrm{PGL}(2,p^m)$，其中$(2m)\mid n$，设h_2是G_B中阶数为p^m+1的元素，则$k-2\le|h_2|\le k$，而h_2无不动点，故

$$p^m+1=k=\frac{q-1}{2}+2=\frac{p^n+3}{2},$$

可得$p^m\mid 1$。所以$p=1$，从而$q=1$，与$q>11$矛盾。

综上所述，G_B是阶数为$2d$的二面体群，其中$d\mid\frac{q\pm1}{2}$。因$f\in G_B$，故$d=\frac{q-1}{2}$，从而$G_B=\langle f,g\rangle$，所以$\lambda=\frac{k(k-1)}{2}$。

定理3 设$q\equiv1(\mathrm{mod}\,4)$，$q>11$且$k=\frac{q-1}{2}+1$，则存在一个单纯3-$(q+1,k,k(k-2))$设计。

证明取$B=H\cup\{0\}$，易知$f\in G_B$，从而$\langle f\rangle\subseteq G_B$。令$\mathcal{B}=\Gamma\cup\theta\Gamma$，其中$\Gamma=G(B)=\{g(B)\mid g\in G\}$，由引理5知，$(X,\mathcal{B})$是一个3-$(q+1,k,\lambda)$设计，其中

$$\lambda=\frac{k(k-1)(k-2)}{|G_B|}.$$

因$f\in G_B$，故$(k-1)\mid|G_B|$，从而$\lambda\mid k(k-2)$。又$q\equiv1(\mathrm{mod}\,4)$，故$k$为奇数，从而$k(k-2)$为奇数，可得$\lambda$为奇数。所以，$(X,\mathcal{B})$是一个单纯3-设计。

因$\langle f\rangle\subseteq G_B$，由引理1知，$G_B$不为初等Abel群。又$k>6$，则$|f|=k-1>5$，从而$G_B$中含有阶数大于5的元素，所以$G_B$不为$A_4$，$S_4$或$A_5$。若$G_B=D_{2d}$，则$(k-1)\mid d$，即$\frac{q-1}{2}\mid d$，从而$d=\frac{q-1}{2}=k-1$，而$|G_B|=(2k-2)\mid k(k-1)(k-2)$，故$2\mid k(k-2)$，与$k(k-2)$为奇数矛盾。所以$G_B$不为二面体群。又$k=\frac{q-1}{2}+1$，故$(k-1,p)=1$，从而$(k-1,p^m)=1$。若$G_B$是阶数为$p^m d$的半直积，则$(k-1)\mid p^m d$，即$\frac{q-1}{2}\mid p^m d$，从而$\frac{q-1}{2}\mid d$，可得$d=\frac{q-1}{2}$。因$d\mid(p^m-1)$，故$\frac{q-1}{2}\mid(p^m-1)$，所以$m=n$，即$|G_B|=\frac{q(q-1)}{2}$。因$B$是由$G_B$在$X$上作用的轨道的并构成，由引理3知，$|B|\ge q$，而$|B|=k=\frac{q+1}{2}$，与$q>\frac{q+1}{2}$矛盾。

若$G_B=\mathrm{PSL}(2,p^m)$，其中$m\mid n$，则B是由$\mathrm{PSL}(2,p^m)$在X上作用的轨道的并构成。由引理4知，$|B|\ge p^m+1$。又$f\in G_B$，故G_B中含有阶数为$k-1$的元素。而$\mathrm{PSL}(2,p^m)$中元素的最大阶为$\frac{p^m+1}{2}$，故$k-1\le\frac{p^m+1}{2}$，即$k\le\frac{p^m+1}{2}+1$，因此$p^m+1\le|B|\le\frac{p^m+1}{2}+1$。所以$p^m+1\le\frac{p^m+1}{2}+1$，即$p^m\le1$，可得$p=1$，从而$q=1$，与$q>11$矛盾。

若 $G_B = \mathrm{PGL}\left(2, p^m\right)$，其中 $\left(2m\right) | n$，设 h 是 G_B 中阶数为 p^m+1 的元素，则 $k-1 \le |h| \le k$，而 h 无不动点，故

$$p^m + 1 = k = \frac{q-1}{2} + 1 = \frac{p^n+1}{2},$$

可得 $p^m | 1$。所以 $p=1$，从而 $q=1$，与 $q>11$ 矛盾。

综上所述，G_B 是 d 阶循环群，其中 $d | \frac{q \pm 1}{2}$。因 $f \in G_B$，故 $d = \frac{q-1}{2}$。所以 $G_B = \langle f \rangle$，故 $\lambda = k\left(k-2\right)$。

致　谢

衷心感谢导师李伟霞在本文写作过程中的悉心指导。

基金项目

国家自然科学基金资助项目(11501315)。

参考文献

[1] Biggs, N.L. and White, A.T. (1979) Permutation Groups and Combinatorial Structures. Cambridge University Press, Cambridge, 1-27. https://doi.org/10.1017/CBO9780511600739

[2] Cusack, C.A., Graham, S.W. and Kreher, D.L. (1995) Large Sets of 3-Designs from $\mathrm{PSL}\left(2,q\right)$ with Block Sizes 4 and 5. *Journal of Combinatorial Designs*, **3**, 147-160. https://doi.org/10.1002/jcd.3180030207

[3] Omidi, G.R., Pournaki, M.R. and Tayfeh-Rezaie, B. (2007) 3-Designs with Block Size 6 from $\mathrm{PSL}\left(2,q\right)$ and Their Large Sets. *Discrete Mathematics*, **307**, 1580-1588. https://doi.org/10.1016/j.disc.2006.09.009

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

[5] Li, W.X. (2010) On the Existence of Simple 3-(30,7,15) and 3-(26,12,55) Designs. *Ars Combinatoria*, **95**, 531-536.

[6] Balachandran, N. and Ray-Chaudhuri, D. (2007) Simple 3-Designs and $\mathrm{PSL}\left(2,q\right)$ with $q \equiv 1 \left(\mathrm{mod}\, 4\right)$. *Designs Codes Crytography*, **44**, 263-274. https://doi.org/10.1007/s10623-007-9096-z

[7] Liu, W.J., Tang, J.X. and Wu, Y.X. (2012) Some New 3-Designs from $\mathrm{PSL}\left(2,q\right)$ with $q \equiv 1 \left(\mathrm{mod}\, 4\right)$. *Science China Mathematics*, **55**, 1901-1911. https://doi.org/10.1007/s11425-012-4454-3

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

[9] Huber, M. (2007) A Census of Highly Symmetric Combinatorial Designs. *Journal of Algebraic Combinatorics*, **26**, 453-476. https://doi.org/10.1007/s10801-007-0065-4

[10] Tang, J.X., Liu, W.J. and Wang, J.H. (2013) Groups $\mathrm{PSL}\left(n,q\right)$ and 3-$\left(v,k,1\right)$ Designs. *Ars Combinatoria*, **110**, 217-226.