数理解析研究所講究録 1465 巻 2006 年 39-49

Translations of the Squares in a Finite Field and related Designs with Linear Fractional Groups

一橋大学・大学院経済学研究科　岩崎　史郎 (Shiro Iwasaki)

Graduate School of Econamics
Hitotsubashi University
Kunitachi,Tokyo 186-8601, Japan
E-mail:iwasaki@math.hit-u.ac.jp

Congratulations to Dr. Masaaki Harada for winning the Hall Medal
With respect for his constant noteworthy researches,
With love for his friendly warm personality,
With thanks for his sincere consideration for me

I would like to talk mainly about a survey of my papers

[1] An elementary and unified approach to the Mathieu-Witt systems, J. Math. Soc. Japan 40(1988) 393-414.

[2] Infinite families of 2- and 3-designs with parameters $v = p + 1, k = (p-1)/2^i + 1$, where p odd prime, $2^e \top (p-1), e \geq 2, 1 \leq i \leq e$, J.Combin.Designs 5(1997) 95-110.

[3] (with T.Meixner) A remark on the action of $PGL(2,q)$ and $PSL(2,q)$ on the projective line, Hokkaido Math.J.26(1997) 203-209.

[4] Translations of the squares in a finite field and an infinite family of 3-designs, Europ.J.Combin. 24(2003) 253-266.

1 Design construcion principle and some well-known examples

A well-known powerful method for constructing designs from groups:

“ t-homogeneous permutation group → t-design construction principle ”

G: a t-homogeneous permutation group on a finite set Ω (that is, $\forall$ two t-subsets T, T' of Ω, $\exists\, \sigma \in G$ such that $T^\sigma = T'$), $|\Omega| = v$ and

$B \subset \Omega, \quad |B| = k \geq t$

$\Downarrow$

The pair (Ω, B^G) : t-(v, k, λ) design with point set Ω and block set B^G, where

$B^G = \{B^\sigma | \sigma \in G\}$: set of the images of B under G,

$$\lambda = |B^G| \frac{\binom{k}{t}}{\binom{v}{t}} = \frac{|G|\binom{k}{t}}{|G_B|\binom{v}{t}}$$

$G_B = \{\sigma \in G \mid B^\sigma = B\}$: setwise stabilizer of B in G.

(B is called a **base block** for the design (Ω, B^G))

Though this is quite elementary and simple—in fact,this is immediately shown only by counting the number of $\{(T, C) \mid T \subset \Omega, |T| = t,\ T \subset C \in B^G\}$ in two ways—, by this principle we can construct various interesting designs if we take various appropriate (Ω, G) and B.

Some well-known examples :

	1	2	3
G	$PGL(n+1, q)$	$AGL(n, q)$	$PGL(2, q^n)$
Ω	$PG(n, q)$	$V(n, q) = AG(n, q)$	$\{\infty\} \cup GF(q^n)$
B	an i-dim.proj.subsp.	an i-dim.aff.subsp.	$\{\infty\} \cup GF(q)$
(Ω, B^G)	$PG_i(n, q)$	$AG_i(n, q)$	Witt's circle geometry

$\mathbf{V}$=$V(n, q) = K^n$: n-dim.vector space over the finite field $K = GF(q)$

For i, $1 \leq i < n$,

$\mathbf{V}_i = \mathbf{V}_i(n, q)$: set of all the i-dim. vector subspaces of $V(n, q)$,

$N_i(n, q) : = |\mathbf{V}_i| = \dfrac{(q^n - 1)(q^{n-1} - 1)\cdots(q^{n-i+1} - 1)}{(q^i - 1)(q^{i-1} - 1)\cdots(q - 1)}$,

$\mathbf{A}_i = \{U + v \mid U \in \mathbf{V}_i, v \in V(n, q)\}$: set of all the i-dim. affine subspaces of the affine space $\mathbf{A} = AG(n, q) = V(n, q)$. $|\mathbf{A}_i| = q^{n-i}N_i(n, q)$

Ex.1. The projective general linear group $PGL(n+1, q)$ acts 2-transitively on the projective space $\mathbf{P} = PG(n, q)$ and transitively on $\mathbf{P}_i$, the set of all the i-dim.proj.subspaces. By the principle we have

$PG_i(n, q) : = (\mathbf{P}, \mathbf{P}_i)$ is a 2-$((q^{n+1} - 1)/(q - 1), (q^{i+1} - 1)/(q - 1), N_{i-1}(n - 1, q))$ design.

Ex.2. The affine general linear group $AGL(n, q) \ : = \{x \mapsto xA + b \mid A \in GL(n, q),\ b \in V(n, q)\}$ acts 2-transitively on the affine space $\mathbf{A} = AG(n, q) = V(n, q)$ and transitively on $\mathbf{A}_i$, the set of all the i-dim. affine subspaces. By the principle we have

$AG_i(n, q) := (\mathbf{A}, \mathbf{A}_i)$ is a 2-$(q^n, q^i, N_{i-1}(n - 1, q))$ design. In particular,

$AG_1(n,q)$ is a 2-$(q^n, q, 1)$ design.
Also, for $n \geq 3$, $AGL(n,2)$ acts 3-transitively on $\mathbf{A}= V(n,q)$ and so
$AG_i(n,2)$ is a 3-$(2^n, 2^i, N_{i-2}(n-2,2))$ design, in particular,
$AG_2(n,2)$ is a 3-$(2^n, 4, 1)$ design.

Ex.3. $G = PGL(2,q^n)$ (res. $PGL(2,q)$) acts 3-transitively on the projective line $\Omega = \{\infty\} \cup GF(q^n)$ (res. $B = \{\infty\} \cup GF(q)$) and so by the principle we have
(Ω, B^G) is a 3-$(q^n+1, q+1, 1)$ design, which is called **Witt's circle geometry, spherical geometry** or **spherical design** and denoted by $CG(n,q)$ etc.
$CG(n,q)$ is an extension of $AG_1(n,q)$. $CG(2,q)$ is called **Miquelian** (**Moebius** or **inversive**) **plane**.

Another well-known examples :

	4	5
G	$ASL(1,q), q \equiv -1(\text{mod } 4)$	$PSL(2,11)$
Ω	$GF(q)$	$\{\infty\} \cup GF(11)$
B	$(GF(q) \setminus \{0\})^2$	$\{\infty\} \cup (GF(11) \setminus \{0\})^2$
(Ω, B^G)	Paley design	Mathieu-Witt design W_{12}

Ex.4. Let
$q = p^e$: odd prime p power with $q \equiv -1$ (mod 4), that is, $q-1 = 2 \cdot \text{odd}$.
$K = GF(q)$: finite field with q elements.
$Q = (K \setminus \{0\})^2 = \{x^2 \mid x \neq 0 \in K\}$: set of nonzero squares in K.
(i) The affine group $G = ASL(1,q) := \{x \mapsto ax+b \mid a \in Q, b \in K\}$ acts 2-homogeneously on K.
(ii) The pair (K, Q^G) is a symmetric 2-$(q, (q-1)/2, (q-3)/4)$ design, which is one of Hadamard 2-design called **Paley design**.
(iii) The block set : $Q^G = \{Q+i \mid i \in K\}$,
the setwise stabilizer of Q in G : $G_Q = \{x \mapsto ax \mid a \in Q\} \cong Q$.
(iv) For any $i \neq j \in K$,

$$|(Q+i) \cap (Q+j)| = |Q \cap (Q+1)| = (q-3)/4.$$

Ex.5. (see T.Beth, Some remarks on D.R.Hughes' construction of M_{12} and its associated design, in " Finite geometries and designs" London Math.Soc.Lect.Note 49, 1981)

2 A Motivation, a Main Problem and Notation

Constructing the design (Ω, B^G)(determining λ) by the Principle : " t-homo.per.gp.→ t-design" is reduced to determining the subgroup G_B. This may be not interesting as a group-theoretic problem when most or all the subgroups of G are known. However, suggested by above xamples, especially ex.3-5, we can expect to obtain new (sometimes interesting) designs (Ω, B^G) by choosing appropriate subsets B of Ω, even if a permutation group $(\Omega,\ G)$ is very simple and all the subgroups of G are known. We consider the following

Main Problem. What groups $(\Omega,\ G)$ and what subsets $B \subset \Omega$ yield interesting new designs (Ω, B^G) ? Particularly, in the case that G is the linear fractional group $PGL(2,q)$ or special linear fractional group $PSL(2,q)$ on the the projective line $\Omega = \{\infty\} \cup GF(q)$, what q and what $B \subset \Omega$ yield interesting new designs (Ω, B^G) ?

Notation (We fix throughout this talk)
$q = p^e$: odd prime p power
(In many cases we assume that $q \equiv -1 \pmod 4$, that is, $q - 1 = 2 \cdot \text{odd}$.)
$K = GF(q)$: finite field with q elements
$F = K \setminus \{0\}$: nonzero elements in K
$Q = F^2 = \{x^2 \mid x \neq 0 \in K\}$: set of nonzero squares in K
$N = F \setminus Q$: set of nonsquares in K
(Note that $-1 \in N$ and $N = -Q$ when $q - 1 = 2 \cdot \text{odd}$.)
For $i \in K$,
$V_i = \{\infty\} \cup (Q + i)$, in particular $V_0 = \{\infty\} \cup Q$.
$\Omega = \{\infty\} \cup K$: projective line over K
$PGL(2,q) = \{x \mapsto (ax+b)/(cx+d) \mid a,b,c,d \in GF(q),\ ad - bc \neq 0\}$
: linear fractional group on Ω.
$PSL(2,q) = \{x \mapsto (ax+b)/(cx+d) \mid a,b,c,d \in GF(q),\ ad - bc \in Q\}$
: special linear fractional group on Ω.

For $B \subset \Omega$ with $|B| \geq 3$,
$\tilde{\mathbf{D}}(q,B) = (\Omega, B^{PGL(2,q)})$,
$\mathbf{D}(q,B) = (\Omega, B^{PSL(2,q)})$,

Note that

(1) $PGL(2,q)$ acts 3-transitively (so 3-homogeneouly) on Ω, and by the principle $\tilde{\mathbf{D}}(q,B)$ is a 3-design for any $B \subset \Omega$ with $|B| \geq 3$.

(2) $PSL(2,q)$ acts 2-transitively (so 2-homogeneouly) on Ω, and by the principle $\mathbf{D}(q,B)$ is a 2-design for any $B \subset \Omega$ with $|B| \geq 2$.

(3) If $q-1 = 2 \cdot$ odd, $PSL(2,q)$ acts 3-homogeneouly on Ω, and by the principle $\mathbf{D}(q,B)$ is a 3-design for any $B \subset \Omega$ with $|B| \geq 3$.

Main Problem. What q and what $B \subset \Omega$ yield interesting new designs $\mathbf{D}(q,B)$, $\tilde{\mathbf{D}}(q,B)$?

3 Obtained results etc.

Suggested by Ex.4 and 5, We have the following two theorems. (these may possibly have been already known explicitly or implicitly.)

Theorem 1 ([1] 1988)
Let $q-1 = 2 \cdot$ odd and $G = PSL(2,q)$.
(i) The setwise stabilizer of V_0 in G : $G_{V_0} = \{x \mapsto ax \mid a \in Q\} \cong Q$,
(ii) $\mathbf{D}(q,V_0) = (\Omega, V_0^G)$ is a 3-$(q+1, (q+1)/2, (q+1)(q-3)/8)$ design,
(iii) The block set is

$$V_0^G = \{V_i \mid i \in K\} \cup \{\overline{V_i} \mid i \in K\} \cup \{V_i \triangle V_j \mid i \neq j \in K\} \cup \{V_i \triangle \overline{V_j} \mid i \neq j \in K\},$$

where $\overline{V_i} = \Omega \setminus V_i$ and $\triangle$ denotes symmetric difference, namely
$X \triangle Y := (X \setminus Y) \cup (Y \setminus X)$ *for subsets X, Y of Ω.*
(iv) If $\mathbf{D}(q,V_0)$ is a 4-design, then $q = 11$ and it becomes a 5-$(12,6,1)$ design, namely the Mathieu-Witt design W_{12}.
($\mathbf{D}(11,V_0)$ is the very same as the design of Ex.5.)

Rough sketch of Theorem 1.
(i) is proved by standard permutaion group arguments and by using the well-known list of the subgroups of $G = PSL(2,q)$.
(iii) Note that $G = G_\infty \cup G_\infty \tau G_\infty$, where $\tau : x \mapsto -1/x$, and examine the actions of G_∞ and τ to V_i.

Remark for (ii), (iii). Note that the design $\mathbf{D}(q,V_0)$ =(Ω, V_0^G) is different from the design (Ω, B) with block set B =$\{V_i \mid i \in K\} \cup \{\overline{V_i} \mid i \in K\}$, which is an extension of the Paley design (K, Q^{G_∞}), i.e. $\Omega \setminus \{\infty\} = K$ and $\{B \setminus \{\infty\} \mid \infty \in B \in \mathsf{B}\} = Q^{G_\infty}$.

Ex. $\mathbf{D}(23,V_0)$ is a 3-(24, 12, 60) design. $\mathbf{D}(3^3,V_0)$ is a 3-(28, 14, 84) design.

It seems that these designs are not found in the design table known till then.

Theorem 2. ([1] 1988) *If* $q = 23, G = PSL(2,23)$ *and*
$B = V_0 \triangle V_1 \triangle V_4 = \{\infty, 1, 13, 14, 18, 19, 20, 22\}$,
then $\mathrm{D}(23, B)$ *is a* 5-(24, 8, 1) *design, namely the Mathieu-Witt design* W_{24}.

Remark. We can take another B as a basis block. For example,
$B = V_0 \triangle V_1 \triangle V_6, \quad V_0 \triangle V_1 \triangle V_{15}, \quad V_0 \triangle V_1 \triangle \overline{V_{-4}}$.
Question : Which B is the most natural ?

The above theorems lead us to two approaches :

Approach I. Under the condition "$(q-1) = 2 \cdot \text{odd}$" and keeping the notation for G, Q, V_i etc., take symmetric differences of *three* V_i's as a base block B and consider designs $\mathbf{D}(q, B)$ somewhat systematically. Note that determining the value of $|V_i \triangle V_j \triangle V_k|$ is reduced to determining the value of $|(Q+i) \cap (Q+j) \cap (Q+k)|$ or $|Q \cap (Q+1) \cap (Q+i)|$.

Approach II. Remove the condition :" $q - 1 = 2 \cdot \text{odd}$ ".

As for Approach I, we consider

Problem 1. Determine the value of $|Q \cap (Q+1) \cap (Q+i)|$ for $i \neq 0, 1 \in K$ (as precisely as possible).

Problem 2. Set $B = V_0 \triangle V_1 \triangle V_i$ ($i \neq 0, 1 \in K$) and determine (the order of) the stabilizer G_B and the parameters of the 3-design $\mathbf{D}(q, B)$ (as precisely as possible).

We have obtained a few results in the case $i = -1$.

In the following (Theorem 3 – Theorem 4),
Suppose that $q - 1 = 2\cdot$ odd and set
$V = V_0 \triangle V_1 \triangle V_{-1}$, where $V_i = \{\infty\} \cup (Q+i)$.
$\overline{V} = \Omega \setminus V$
$G = PSL(2, q)$
$H = G_V = G_{\overline{V}}$: setwise stabilizer of V or $\overline{V}$ in G
$\overline{V}^G = \{\overline{V}^\sigma \mid \sigma \in G\}$: set of the images of $\overline{V}$ under all $\sigma \in G$

Theorem 3 ([4] 2003) *For any $i \neq 0 \in K$,*

$$| Q \cap (Q+i) \cap (Q-i) | = \begin{cases} (q-7)/8 & if\ 2 \in Q, \\ (q-3)/8 & if\ 2 \in N. \end{cases}$$

Corollary 1 *For any $i \neq 0 \in K$, we have the following values.*
(1) *The case $2 \in Q$.*
$| Q \cap (Q+i) \cap (Q-i) | = | N \cap (N+i) \cap (N-i) | = (q-7)/8.$
$| N \cap (Q+i) \cap (Q-i) | = | Q \cap (N+i) \cap (N-i) | = (q+1)/8.$

$$| Q \cap (Q+i) \cap (N-i) | = | N \cap (Q+i) \cap (N-i) | = \begin{cases} (q+1)/8 & if\ i \in Q, \\ (q-7)/8 & if\ i \in N. \end{cases}$$

$$| Q \cap (Q-i) \cap (N+i) | = | N \cap (Q-i) \cap (N+i) | = \begin{cases} (q-7)/8 & if\ i \in Q, \\ (q+1)/8 & if\ i \in N. \end{cases}$$

(2) *The case $2 \in N$.*
All the values are equal to $(q-3)/8$.

Corollary 2 (1) *If $2 \in Q$, then $| V | = | \bar{V} | = (q+1)/2$.*
(2) *If $2 \in N$, then $| V | = (q+5)/2$ and $| \bar{V} | = (q-3)/2$.*

Theorem 4 ([4] 2003) *Suppose $2 \in N$. Then the following hold.*
(1) (i) *The case $p \neq 3$.*
$H = \langle \tau, \rho \rangle$, the subgroup generated by τ and ρ, which is the 4-group.
(ii) *The case $p = 3$.*
$H = \langle \tau, \rho, \pi \rangle$, the subgroup generated by τ, ρ and π, which is isomorphic to A_4, the alternating group of degree 4.
Here $\tau : x \mapsto -1/x$, $\rho : x \mapsto (x+1)/(x-1)$ and $\pi : x \mapsto x+1$.

(2) *The design $\mathbf{D}(q, \bar{V}) = (\Omega, \bar{V}^G)$ with point set Ω and block set $\bar{V}^G$ is a 3-$(q+1, (q-3)/2, \lambda)$ design, where*

$$\lambda = \begin{cases} (q-3)(q-5)(q-7)/64 & for\ p \neq 3 \\ (q-3)(q-5)(q-7)/(3 \cdot 64) & for\ p = 3. \end{cases}$$

Remark. I do not know whether this design is interesting or not, but this is a new infinite family of 3-designs. If $\mathbf{D}(q, \bar{V})$ is a 4-design, then $q = 107$ and it may be a 4-(108, 52, $5 \cdot 7 \cdot 13 \cdot 17$) or a 5-(108, 52, $5 \cdot 6 \cdot 7 \cdot 17$) design. I do not know whether it is true or not. But, this design cannot be a 6-design.

Rough sketch of proof of Theorem 3.

Let ψ be the quadratic character of $K = GF(q)$ defined by

$$\psi(x) := \begin{cases} 1 & \text{for } x \in Q, \\ -1 & \text{for } x \in N, \\ 0 & \text{for } x = 0. \end{cases}$$

To seek the values of

$$\alpha_i := | (Q+1) \cap (Q+i) \cap Q |, \quad \beta_i := | (Q+1) \cap (Q+i) \cap N \mid \; for\, i \neq 0, 1 \in K$$

we consider

$$\Psi_i := \sum_{x \in K} \psi(x-1)\psi(x-i)\psi(-2x) = \psi(-2) \sum_{x \in K} \psi(x-1)\psi(x-i)\psi(x).$$

We have relations among α_i, β_i and Ψ_i, that is, we can express α_i and β_i by Ψ_i. For example, when $2 \in Q$, we have

$\alpha_i = (q-3-\Psi_i)/8, \quad \beta_i = (q-3+\Psi_i)/8 \quad \text{if } i \in (Q+1) \cap N$

$\alpha_i = (q-7-\Psi_i)/8, \quad \beta_i = (q+1+\Psi_i)/8 \quad \text{otherwise.}$

Though it seems difficult that determining the precise value of Ψ_i for general i, we can precisely evaluate Ψ_i, α_i and β_i for $i = -1$. That is, we can easily show $\Psi_{-1} = 0$ and the proof is done. (Theorem 4 is proved by using Theorem 3 and the well-known list of the subgroups of $G = PSL(2, q)$, etc. and through somewhat detailed arguments.)

Remark 1. $\Psi_{-1} = \sum_{x \in K} \psi(x-1)\psi(x+1)\psi(-2x)$ is not the Jacobi sum :

$$J_0(\psi, \psi, \psi) = \sum_{x_1+x_2+x_3=0} \psi(x_1)\psi(x_2)\psi(x_3).$$

(Ψ_{-1} is a subsum of $J_0(\psi, \psi, \psi)$.) It is known that $J_0(\psi, \psi, \psi) = 0$ [Lidl, Niederreiter, Finite Fields, p.206, 5.20.Theorem.]

Remark 2. As mentioned in 'sketch of proof of Theorem 3', determining the value of $\alpha_i = | Q \cap (Q+1) \cap (Q+i) |$ is reduced to determining the value of Ψ_i, and so we can say Problem 2 in the following form:

Problem 2′. Determine the value of Ψ_i for $i \neq 0, 1 \in K$ as precisely as possible. (We have seen that $\Psi_{-1} = 0$ and see that Ψ_i is divisible by 4 for any $i \neq 0, 1 \in K$.) For what i can we determine the precise value of Ψ_i ? What is the maximum or minimum of the values Ψ_i ? If we set $B_i = V_0 \triangle V_1 \triangle V_i$, what i yield interesting designs $(\Omega, {B_i}^G)$?

Remark 3. In [Berndt,Evans,Williams: Gauss and Jacobi sums, John Wiley Sons, 1998, Theorem 6.3.2] a result containing the case $q = p$ in Theorem 3 and Corollary 1 is proved, by making skillful use of basic facts about quadratic residues modulo p. We proved Theorem 3 with $q = p^e$, using the quadratic character ψ of K and Ψ_{-1}, a kind of variation of Jacobi sum. I owe partially the idea to Professor Tomio Kubota and I am deeply grateful to him.

Remark 4. By Theorems 3, 4 and their proofs, we see that there is a relation among
(i) finite fields (translations of the squares in a finite field) ,
(ii) number theory (multiplicative characters of finite fields),
(iii) (classical) permutaion groups, and
(iv) designs.
Such a relation seems interesting.

Remark 5. Theorem 4 does not deal with the case $2 \in Q$. This case seems to be somewhat difficult, and under investigation.

As for Approach II, we consider the following two problems.

Take $G = PSL(2, q)$ or $PGL(2, q)$.
Problem 3. Suppose that $q - 1 = 2^e \cdot$ odd, $e \geq 2$. For each $i, 1 \leq i \leq e$, set
$$B_i = \{\infty\} \cup F^{2^i}, \text{ where } F = GF(q) \setminus \{0\}$$
and determine the stabilizer G_{B_i} and construct designs $(\Omega, B_i^G) = \tilde{\mathbf{D}}(q, B_i)$ or $\mathbf{D}(q, B_i)$.

Problem 4. Let
p : any prime number, q : a power of p
m : a divisor of $q - 1$ with $1 < m < q - 1$.
U : a subgroup of order m of the cyclic group $F = GF(q) \setminus \{0\}$ and set
$$B = \{\infty\} \cup U.$$
Determine the stabilizer G_B and construct designs $(\Omega, B^G) = \tilde{\mathbf{D}}(q, B)$ or $\mathbf{D}(q, B)$.

[2] (1997) gave an answer to Problem 3 for $q = p$ prime.
[3] (with T.Meixner,1997) gave an answer to Problem 4.
(Their statements are slightly lengthy, and omitted here.)

These papers provided some new designs. For example, in the case
$q = p = 29, \quad q - 1 = 2^2 \cdot 7,$
$\tilde{\mathbf{D}}(29, B_1)$ is a 3-(30, 15, 15·13) design,

$\tilde{\mathbf{D}}(29, B_2)$ is a 3-(30, 8, 48) design,

$B = \{\infty\} \cup F^7, \tilde{\mathbf{D}}(29, B)$ is a 3-(30, 5, 15) design.

It seems that these designs are not found in the design table known till then (e.g. D.L.Kreher, *t*-Designs, $t \geq 3$, in : *CRC handbook of combinatorial designs* (eds. C.J.Colbourn and J.H.Dinitz), 47-66, CRC Press, 1996)

Problem 3 is contained in Problem 4, and so a result in [2] is a part of [3]. However, [2] dealt with the following problem, too :

Problem 5. Set $G = PSL(2, q)$ in Problem 3. Then G acts 2-homogeneously, but *not* 3-homogeneously on Ω. Hence, by the Principle, $\mathbf{D}(q, B_i)$ in Problem 3 is a 2-design for any i, but we do not see easily whether it is a 3-design or not.
When is $\mathbf{D}(q, B_i)$ a 3-design ?

We had a partial answer to this problem:

Theorem 5 ([2] 1997)

Suppose that p is a prime such that $p - 1 = 2^e \cdot m$, where $e \geq 2$ and m is odd. For each $i, 1 \leq i \leq e$, set

$$B_i = \{\infty\} \cup F^{2^i}.$$

(1) For any $i, 1 \leq i < e$, $\mathbf{D}(p, B_i)$ is not a 3-design.

(2) When $m = 3$, $\mathbf{D}(p, B_e)$ is not a 3-design.

(3) Suppose that $(F^{2^e} - 1) \cap Q \neq \emptyset$ and $(F^{2^e} - 1) \cap N \neq \emptyset$. Then

(i) When $m = 5$, $\mathbf{D}(p, B_e)$ is a 3-$(p + 1, 6, 12)$ design.

(ii) When $m = 7$, $\mathbf{D}(p, B_e)$ is a 3-$(p + 1, 8, 24)$ design.

(I do not know why, but we find magic numbers 6, 12 ; 8, 24 *here, too* !)

(iii) Any 3-design $\mathbf{D}(p, B_e)$ for $m = 5$ or 7, is not a 4-design.

(4) When $m = 5$, the following are equivalent.

(i) $(F^{2^e} - 1) \cap Q \neq \emptyset$ and $(F^{2^e} - 1) \cap N \neq \emptyset$

(ii) $5 \notin F^4$, that is, 5 is not a fourth power in $GF(p)$.

(iii) $5^{(p-1)/4} \neq 1$ in $GF(p)$.

Ex. (i) $p = 29, p - 1 = 2^2 \cdot 7$,

$\mathbf{D}(29, B_2)$ is a 3-(30, 8, 24) design.

(It seems that this is not found in the design table known till then.)

(ii) $p = 41, p - 1 = 2^3 \cdot 5$,

$\mathbf{D}(41, B_3)$ is a 3-(42, 6, 12) design.

As for (3),(4) in Theorem 5, we have the following question in general:

Problem 6. Let q be a prime p power such that $q-1 = 2^e \cdot m$, where $e \geq 2$ and m is odd, and set $F = GF(q) \setminus \{0\}, Q = F^2, N = F \setminus Q$. Then

(*) $\quad (F^{2^e} - 1) \cap Q \neq \emptyset$ and $(F^{2^e} - 1) \cap N \neq \emptyset \quad$?

(Does $F^{2^e} - 1$ contain both square and nonsquare elements in $GF(q)$ impartially ?)

(*) is equivalent to " Each of equations

$x^{2^e} - 1 = y^2$ and $x^{2^e} - 1 = \alpha y^2$, where α is a primitive element of F
has solutions $x \neq 0$ and $y \neq 0$ in $GF(q)$."

In what case is (*) true ?

(1) Professor T.Kubota kindly infomed me that (*) holds whenever $m > 2^e + 2$, giving his elegant proof which uses a Jacobi sum skillfully.

(2) By his comments we also see the following:

(i) 5 is a fourth power in $GF(p)$ if and only if p is of the form $p = x^2 + 100y^2$ (x, y integers). (see e.g. Hasse, Bericht ueber neuere Untersuchungen$\cdots$ Teil II,1930, 2nd ed. Physica-Verlag 1965, p.69)

(ii) In the case $p = 40961, \quad p - 1 = 2^{13} \cdot 5, \quad p = 31^2 + 100 \cdot 20^2$, and so 5 is a fourth power in $GF(p)$. Therefore (*) does not hold by Theorem 5 (4).

Here we can see an interesting connection among finite fields, number theory and designs, too.

4 Something like Summary

I have taken the **Principle** : " t-homo. perm. gp. → t-design construction" as a **Magic Formula** (or **Parrot-Cry, Baka no Hitotsu-oboe** ?), and we have investegated some problems on the basis of the Principle, and we see **an interesting Connection among**

(i) Finite Fields (translations of the squares in a finite field etc.)

(ii) Number Theory (characters, Jacobi sum, biquadratic residues etc.)

(iii) (Classical) Permutation Groups, and

(iv) Designs.

I hope that you are interested in such an approach and investigate it further from various or appropriate new points of view that get nearer to the essence.