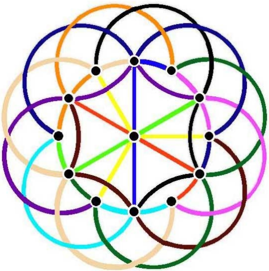
Construction of (p^a, p^b, p^a, p^{a-b}) Relative Difference Sets in Non-abelian Groups

Huang Yiwei(with Bernhard Schmidt)

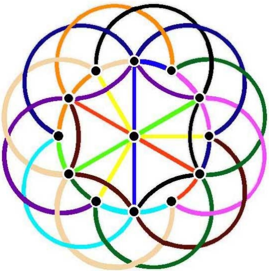
School of Physical and Mathmatical sciences, Nanyang Technological University, Singapore

A Very Nice Design!



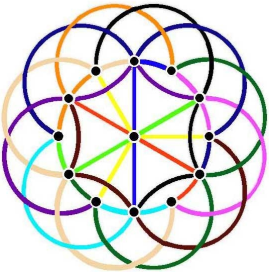
- A design consists of a set of points and blocks. The blocks are subsets of the point set.

A Very Nice Design!



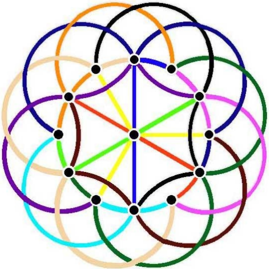
- A design consists of a set of points and blocks. The blocks are subsets of the point set.
- In the picture, there are 13 points and 13 blocks. Every two points(blocks) are incident with exactly one block(point).

A Very Nice Design!



- A design consists of a set of points and blocks. The blocks are subsets of the point set.
- In the picture, there are 13 points and 13 blocks. Every two points(blocks) are incident with exactly one block(point).
- It is a **projective plane** of order 3.

A Very Nice Design!



- A design consists of a set of points and blocks. The blocks are subsets of the point set.
- In the picture, there are 13 points and 13 blocks. Every two points(blocks) are incident with exactly one block(point).
- It is a **projective plane** of order 3.
- If 'design' is treated as an *art* of *selecting subsets from a point set*, then a projective plane is a perfect artwork!

Construction of Projective Plane by RDS

- Projective planes can be contructed by certain relatives difference sets.

Construction of Projective Plane by RDS

- Projective planes can be contructed by certain relatives difference sets.
- Given a projective plane, by deleting a block together with all points on it, we obtain an **affine plane**. Conversely, we can also construct a projective plane by an affine plane.

Construction of Projective Plane by RDS

- Projective planes can be contructed by certain relatives difference sets.
- Given a projective plane, by deleting a block together with all points on it, we obtain an **affine plane**. Conversely, we can also construct a projective plane by an affine plane.
- Let us represent the points by the elements in $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.

Construction of Projective Plane by RDS

- Projective planes can be contructed by certain relatives difference sets.
- Given a projective plane, by deleting a block together with all points on it, we obtain an **affine plane**. Conversely, we can also construct a projective plane by an affine plane.
- Let us represent the points by the elements in $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.
- Let the blocks be the elements in

$$\{Rg : g \in G\} \cup \{Ng : g \in G\}.$$

where $R = \{(0,0),(1,1),(2,1)\}, N = \{0\} \times \mathbb{Z}_3$.

Construction of Projective Plane by RDS

- Projective planes can be contructed by certain relatives difference sets.
- Given a projective plane, by deleting a block together with all points on it, we obtain an **affine plane**. Conversely, we can also construct a projective plane by an affine plane.
- Let us represent the points by the elements in $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.
- Let the blocks be the elements in

  $$\{Rg : g \in G\} \cup \{Ng : g \in G\}.$$

  where $R = \{(0,0),(1,1),(2,1)\}, N = \{0\} \times \mathbb{Z}_3$.
- It can be verified that it is an affine plane of order 3. Therefore, we also obtain a projective plane of order 3.

Construction of Projective Plane by RDS

- Projective planes can be contructed by certain relatives difference sets.
- Given a projective plane, by deleting a block together with all points on it, we obtain an **affine plane**. Conversely, we can also construct a projective plane by an affine plane.
- Let us represent the points by the elements in $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.
- Let the blocks be the elements in

$$\{Rg : g \in G\} \cup \{Ng : g \in G\}.$$

  where $R = \{(0,0),(1,1),(2,1)\}$, $N = \{0\} \times \mathbb{Z}_3$.
- It can be verified that it is an affine plane of order 3. Therefore, we also obtain a projective plane of order 3.
- The set R is called a $(3,3,3,1)-$**relative difference set(RDS)** in G relative to N.

Definition of RDS

- Let G be a group of order mn. Let N be a normal subgroup in G of order n.

Definition of RDS

- Let G be a group of order mn. Let N be a normal subgroup in G of order n.
- A $k-$subset R in G is called an $(m, n, k, \lambda)-$**relative difference set(RDS)** in G relative to N if each element in $G \setminus N$ can be representated in exactly λ ways in the form

$$r_1 r_2^{-1}, \ \ r_1, r_2 \in R,$$

and the non-identity elements in N cannot be represented in this way.

Definition of RDS

- Let G be a group of order mn. Let N be a normal subgroup in G of order n.
- A $k-$subset R in G is called an $(m, n, k, \lambda)-$**relative difference set(RDS)** in G relative to N if each element in $G \backslash N$ can be representated in exactly λ ways in the form

$$r_1 r_2^{-1}, \ \ r_1, r_2 \in R,$$

  and the non-identity elements in N cannot be represented in this way.
- The RDS is called **cyclic, abelian** or **non-abelian** when the group G is cyclic, abelian or non-abelian, repectively. We call N the **forbidden subgroup**.

Definition of RDS

- Let G be a group of order mn. Let N be a normal subgroup in G of order n.
- A $k-$subset R in G is called an $(m, n, k, \lambda)-$**relative difference set(RDS)** in G relative to N if each element in $G \backslash N$ can be representated in exactly λ ways in the form

$$r_1 r_2^{-1}, \;\; r_1, r_2 \in R,$$

  and the non-identity elements in N cannot be represented in this way.
- The RDS is called **cyclic, abelian** or **non-abelian** when the group G is cyclic, abelian or non-abelian, repectively. We call N the **forbidden subgroup**.
- When $n = 1$, the relative difference set(RDS) is just an ordinary difference set(DS). RDS is a generalization of DS.

Two Examples of RDS

- In the *cyclic* group $\mathbb{Z}_8$, the set $R = \{0, 1, 3\}$ is a $(4, 2, 3, 1)-$RDS relative to $N = \{0, 4\}$.

$$
\begin{aligned}
0 - 1 &\equiv 7 \pmod 8; 0 - 3 \equiv 5 \pmod 8; \\
1 - 0 &\equiv 1 \pmod 8; 1 - 3 \equiv 6 \pmod 8; \\
3 - 0 &\equiv 3 \pmod 8; 3 - 1 \equiv 2 \pmod 8.
\end{aligned}
$$

Two Examples of RDS

- In the *cyclic* group $\mathbb{Z}_8$, the set $R = \{0, 1, 3\}$ is a $(4, 2, 3, 1)-$RDS relative to $N = \{0, 4\}$.

$$\begin{aligned} 0 - 1 &\equiv 7 \pmod 8; 0 - 3 \equiv 5 \pmod 8; \\ 1 - 0 &\equiv 1 \pmod 8; 1 - 3 \equiv 6 \pmod 8; \\ 3 - 0 &\equiv 3 \pmod 8; 3 - 1 \equiv 2 \pmod 8. \end{aligned}$$

- Let $G =< a, t | a^4 = t^2 = 1, t^{-1}at = a^{-1} >$ be the dihedral group of order 8. Then $R = \{1, at, a^2t, a^3t\}$ is a $(4, 2, 4, 2)-$RDS in G relative to $< t >$. This is a *non-abelian* RDS.

Some Applications of RDS

- RDSs are equivalent to certain divisible designs with regular automorphism groups. In particular, certain types of RDSs correspond to projective planes.

Some Applications of RDS

- RDSs are equivalent to certain divisible designs with regular automorphism groups. In particular, certain types of RDSs correspond to projective planes.
- Construction of generalized Hadamard matrices.

Some Applications of RDS

- RDSs are equivalent to certain divisible designs with regular automorphism groups. In particular, certain types of RDSs correspond to projective planes.
- Construction of generalized Hadamard matrices.
- Construction of sequences with good autocorrelation properties.

Central Problem

Problem

How can we construct a relative difference set in a given group?

- By tools of group ring, character theory..., many constructions and non-existense results are known for abelian difference sets. However, most tools in abelian cases do not apply in non-abelian cases.

Central Problem

Problem

How can we construct a relative difference set in a given group?

- By tools of group ring, character theory..., many constructions and non-existense results are known for abelian difference sets. However, most tools in abelian cases do not apply in non-abelian cases.
- One of most interesting cases(said by A.Pott) of RDS is with parameter (p^a, p^b, p^a, p^{a-b}) where p is a prime number. In this talk, we construct RDSs with this parameter in non-abelian groups.

A Group in Form of 3-Tuple

- Consider the set K of 3-tuples

$$K = \left\{ < x, y; c >: x, y \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\}.$$

A Group in Form of 3-Tuple

- Consider the set K of 3-tuples

$$K = \left\{ < x, y; c >: x, y \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\}.$$

- Let $Tr : \mathbb{F}_{q^k} \to \mathbb{F}_q$. Then the operation between two elements in K is defined by

$$\begin{aligned} &< x_1, y_1; c_1 > * < x_2, y_2; c_2 > \\ =& < x_1 + x_2, y_1 + y_2; Tr(x_2 y_1) + c_1 + c_2 > . \end{aligned}$$

A Group in Form of 3-Tuple

- Consider the set K of 3-tuples

$$K = \left\{ < x, y; c >: x, y \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\}.$$

- Let $Tr : \mathbb{F}_{q^k} \to \mathbb{F}_q$. Then the operation between two elements in K is defined by

$$\begin{aligned} &< x_1, y_1; c_1 > * < x_2, y_2; c_2 > \\ &=< x_1 + x_2, y_1 + y_2; Tr(x_2 y_1) + c_1 + c_2 > . \end{aligned}$$

- Then K is a group of order q^{2k+1}.

A Subgroup in 3-Tuple

- A **permutation function** $f(x)$ from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$ is a mapping which permutes the elements of $\mathbb{F}_{q^k}$. We call $f(x)$ **additive** when $f(x_1 + x_2) = f(x_1) + f(x_2)$ for any x_1, x_2.

A Subgroup in 3-Tuple

- A **permutation function** $f(x)$ from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$ is a mapping which permutes the elements of $\mathbb{F}_{q^k}$. We call $f(x)$ **additive** when $f(x_1+x_2)=f(x_1)+f(x_2)$ for any x_1, x_2.
- Let
$$G=\left\{<x, f(x); c>: x\in\mathbb{F}_{q^k}, c\in\mathbb{F}_q\right\},$$
where $f(x)$ is an additive permutation function from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$.

A Subgroup in 3-Tuple

- A **permutation function** $f(x)$ from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$ is a mapping which permutes the elements of $\mathbb{F}_{q^k}$. We call $f(x)$ **additive** when $f(x_1 + x_2) = f(x_1) + f(x_2)$ for any x_1, x_2.
- Let
$$G = \left\{ < x, f(x); c >: x \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\},$$
where $f(x)$ is an additive permutation function from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$.
- Then G is a normal subgroup of order q^{k+1} in K.

Our Construction of RDSs

Theorem

Let the group

$$G = \left\{ < x, f(x); c >: x \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\},$$

Then the set

$$R = \left\{ < x, f(x); 0 >: x \in \mathbb{F}_{q^k} \right\}$$

is a $(q^k, q, q^k, q^{k-1})-$*RDS in* G *relative to*

$$N = \left\{ < 0, 0; c >: c \in \mathbb{F}_q \right\}.$$

Proof of the Main Theorem

Proof.

Check by definition. We consider the difference of two distinct elements in R.

$$\begin{aligned} &< x, f(x); 0 > * < y, f(y); 0 >^{-1} \\ = & < x-y, f(x-y); Tr\left(-y\left(f(x-y)\right)\right) > . \end{aligned} \quad (1)$$

Partition the set $S = \{(x, y) : x, y \in \mathbb{F}_{q^k}, x \neq y\}$ into q^k subsets of size q^k : $S_a = \left\{(a+d, d) : d \in \mathbb{F}_{q^k}\right\}, a \in \mathbb{F}_{q^k} \backslash \{0\}$. For each subset S_a, the value in (1) will become

$$< a, f(a); Tr(-df(a)) >, d \in \mathbb{F}_{q^k}. \quad (2)$$

Since $f(a) \neq 0$, then $\mathbb{F}_{q^k} = \left\{-df(a) : d \in \mathbb{F}_{q^k}\right\}$, and for $Tr : \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_q$ is a surjective $\mathbb{F}_q-$linear function, we have (2) cover q^{k-1} times of the elements in

$$\{< a, f(a); c >: c \in \mathbb{F}_q\}.$$

□

Divsible Design and RDS

- The existence of an $(m, n, k, \lambda)-$RDS in G is equivalent to the existence of an $(m, n, k, \lambda)-$divisible design with a Singer group G.

Divsible Design and RDS

- The existence of an $(m, n, k, \lambda)-$RDS in G is equivalent to the existence of an $(m, n, k, \lambda)-$divisible design with a Singer group G.
- It tells us two things.

Divsible Design and RDS

- The existence of an $(m, n, k, \lambda)-$RDS in G is equivalent to the existence of an $(m, n, k, \lambda)-$divisible design with a Singer group G.
- It tells us two things.

1. The construction of a divisible design with a Singer group G can be reduced to the construction of RDS in G.

Divsible Design and RDS

- The existence of an $(m, n, k, \lambda)-$RDS in G is equivalent to the existence of an $(m, n, k, \lambda)-$divisible design with a Singer group G.
- It tells us two things.

1. The construction of a divisible design with a Singer group G can be reduced to the construction of RDS in G.
2. Since a divisible design can have many non-isomorphic Singer groups, we can obtian RDSs in many different groups. Our idea of construction is from the investigation of the automorphisms(represeted by elements in $AGL(n, q)$) of the classical $(q^k, q, q^k, q^{k-1})-$divisible design.

Remarks

- Let R be a $(q^k, q, q^k, q^{k-1})-$RDS in G relative to N. Let U be a subgroup of N of order u. By dividing out U, there exists an $(q^k, q/u, q^k, q^{k-1}u)-$RDS in G/U relative to N/U. Hence it is a contruction of any $(p^a, p^b, p^a, p^{a-b})-$RDS.

Remarks

- Let R be a $(q^k, q, q^k, q^{k-1})-$RDS in G relative to N. Let U be a subgroup of N of order u. By dividing out U, there exists an $(q^k, q/u, q^k, q^{k-1}u)-$RDS in G/U relative to N/U. Hence it is a contruction of any $(p^a, p^b, p^a, p^{a-b})-$RDS.
- The groups G that admitting a RDS are mostly non-abelian. We will describe the structures of all the groups in the construction in generators and relations.

Remarks

- Let R be a $(q^k, q, q^k, q^{k-1})-$RDS in G relative to N. Let U be a subgroup of N of order u. By dividing out U, there exists an $(q^k, q/u, q^k, q^{k-1}u)-$RDS in G/U relative to N/U. Hence it is a contruction of any $(p^a, p^b, p^a, p^{a-b})-$RDS.
- The groups G that admitting a RDS are mostly non-abelian. We will describe the structures of all the groups in the construction in generators and relations.
- One major construction of RDSs which belong to parameter (p^a, p^b, p^a, p^{a-b}) is from Davis(1992), it is shown the existence of $(p^{2n}, p^k, p^{2n}, p^{2n-k})-$RDS in the groups whose center contains a large elementary abelian subgroup. Most non-abelian groups do not have such large center. A lot of non-abelian cases from our contruction are without that restriction.

Group Structures

- Recall that in our construction, the group G that admitting an RDS is

$$G = \left\{ < x, f(x); c >: x \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\}.$$

where $f(x)$ is an additive permutation function from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$.

Group Structures

- Recall that in our construction, the group G that admitting an RDS is

$$G = \left\{ < x, f(x); c >: x \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\}.$$

where $f(x)$ is an additive permutation function from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$.

- The structures of G depend on the choices of $f(x)$.

Group Structures

- Recall that in our construction, the group G that admitting an RDS is

$$G = \left\{ < x, f(x); c >: x \in \mathbb{F}_{q^k}, c \in \mathbb{F}_q \right\}.$$

  where $f(x)$ is an additive permutation function from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{q^k}$.
- The structures of G depend on the choices of $f(x)$.
- We can choose the permutative $p - polynomials$ over $\mathbb{F}_{q^k}$ for the choices of $f(x)$, and there are a lot of such polynomails.

Group Structures

- For the convenience to write down the structures, we divide into 4 cases according to value of q. The 4 cases are for: q is odd prime, even prime, odd prime power, even prime power.

Group Structures

- For the convenience to write down the structures, we divide into 4 cases according to value of q. The 4 cases are for: q is odd prime, even prime, odd prime power, even prime power.
- Case 1: Let q be an odd prime. Let $\mathbb{F}_{q^k}^* =<\alpha>$. Let $Tr : \mathbb{F}_{q^k} \to \mathbb{F}_q$, and $x_i =< \alpha^i, f(\alpha^i); 0 >$, $i = 0, \ldots, k-1$; $z =< 0, 0; 1 >$, then we have the structure of G as

$$G =< x_0, \ldots, x_{k-1}, z | x_i^q = z^q = 1, x_i z = z x_i,$$
$$x_i x_j = x_j x_i z^{Tr(\alpha^j f(\alpha^i) - \alpha^i f(\alpha^j))}, i, j = 0, \ldots, k-1 > .$$

Group Structures

Case 2: Let $q = 2$. Define Tr, x_i, z, α in the same way as case 1. Note that the order of generator x_i depends on whether $Tr(\alpha^i f(\alpha^i))$ is zero. Therefore, the group structure is:

$$< x_0, \dots, x_{k-1}, z | x_i^2 = z^{Tr(\alpha^i f(\alpha^i))}, z^2 = 1, x_i z = z x_i,$$
$$x_i x_j = x_j x_i z^{Tr(\alpha^j f(\alpha^i) - \alpha^i f(\alpha^j))}, i, j = 0, \dots, k-1 > .$$

Group Structures

- For the prime power cases, we introduce some notations in preparation. Let $q = p^n (n > 1)$, where p is a prime. Still, let $\mathbb{F}_{q^k}^* =< \alpha >$. Define $\beta = \alpha^{\frac{q^k-1}{q-1}}$, thus $\mathbb{F}_q^* =< \beta >$.

Group Structures

- For the prime power cases, we introduce some notations in preparation. Let $q = p^n (n > 1)$, where p is a prime. Still, let $\mathbb{F}_{q^k}^* =< \alpha >$. Define $\beta = \alpha^{\frac{q^k-1}{q-1}}$, thus $\mathbb{F}_q^* =< \beta >$.
- Let $Coef(x)$ where $x \in \mathbb{F}_q$ stands for a vector of coefficients of a polynomial of β over $\mathbb{F}_p$ by which we represent the element x. For example, if $x = a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1}$, then $Coef(x) = (a_0, \ldots, a_{n-1})$.

Group Structures

- For the prime power cases, we introduce some notations in preparation. Let $q = p^n (n > 1)$, where p is a prime. Still, let $\mathbb{F}_{q^k}^* =< \alpha >$. Define $\beta = \alpha^{\frac{q^k-1}{q-1}}$, thus $\mathbb{F}_q^* =< \beta >$.
- Let $Coef(x)$ where $x \in \mathbb{F}_q$ stands for a vector of coefficients of a polynomial of β over $\mathbb{F}_p$ by which we represent the element x. For example, if $x = a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1}$, then $Coef(x) = (a_0, \ldots, a_{n-1})$.
- Moreover, we define

$$(z_0, \ldots, z_{n-1})^{(a_0,\ldots,a_{n-1})} = z_0^{a_0} \ldots z_{n-1}^{a_{n-1}}.$$

Group Structures

Case 3: Let $q = p^n$, where p is an odd prime. Define the generators x_i $=< \alpha^i, f(\alpha^i); 0 >, i = 0, \ldots, kn-1$; $z_j =< 0, 0; \beta^j >, j = 0, \ldots n-1$. Then we have the structure of G as:

$$< x_0, \ldots, x_{kn-1}, z_0, \ldots, z_{n-1} \big| x_i^p = z_s^p = 1, x_i z_s = z_s x_i,$$
$$z_s z_m = z_m z_s, x_i x_j = x_j x_i (z_0, \ldots, z_{n-1})^{Coef(Tr(\alpha^j f(\alpha^i) - \alpha^i f(\alpha^j)))},$$
$$i, j = 0, \ldots, kn-1; s, m = 0, \ldots n-1 > .$$

Group Structures

Case 4: Let $q = 2^n$, and x_i, z_j, α, β same as case 3. Then we have the group G as:

$$
\begin{aligned}
&< x_0, \ldots, x_{kn-1}, z_0, \ldots, z_{n-1} | z_s^2 = 1, \\
x_i^2 &= (z_0, \ldots, z_{n-1})^{Coef(Tr(\alpha^i f(\alpha^i)))}, x_i z_s = z_s x_i, z_s z_m = z_m z_s, \\
x_i x_j &= x_j x_i (z_0, \ldots, z_{n-1})^{Coef(Tr(\alpha^j f(\alpha^i) - \alpha^i f(\alpha^j)))}, \\
i, j &= 0, \ldots, kn-1; s, m = 0, \ldots n-1 > .
\end{aligned}
$$

RDSs represented in generators

- Given the group by generators and relations, we also can represent the RDS in generators.

RDSs represented in generators

- Given the group by generators and relations, we also can represent the RDS in generators.
- Let $1 \leq e_i \leq p$, and $0 \leq i \leq k-1$. The RDSs for case 1,2 are

$$\left\{ x_0^{e_0} x_1^{e_1} \cdots x_{k-1}^{e_{k-1}} z^{-\sum_{i=0}^{k-1} \frac{e_i(e_i-1)}{2} Tr(\alpha^i f(\alpha^i)))} \right\}.$$

RDSs represented in generators

- Given the group by generators and relations, we also can represent the RDS in generators.
- Let $1 \le e_i \le p$, and $0 \le i \le k-1$. The RDSs for case 1,2 are

$$\left\{ x_0^{e_0} x_1^{e_1} \cdots x_{k-1}^{e_{k-1}} z^{-\sum_{i=0}^{k-1} \frac{e_i(e_i-1)}{2} Tr(\alpha^i f(\alpha^i))} \right\}.$$

- Let $1 \le e_i \le p$, and $0 \le i \le kn-1$. The RDSs for case 3,4 are

$$\left\{ x_0^{e_0} x_1^{e_1} \cdots x_{kn-1}^{e_{kn-1}} (z_0, \ldots, z_{n-1})^{Coef(-\sum_{i=0}^{kn-1} \frac{e_i(e_i-1)}{2} Tr(\alpha^i f(\alpha^i)))} \right\}.$$

Computational Verifications

$(m, n, k, \lambda) - RDS$	$\mathbb{F}_{q^k}$	Group Type in Magma
$(8, 2, 8, 4)$	$\mathbb{F}_{2^3}$	10(abelian), 11, 12, 13
$(27, 3, 27, 9)$	$\mathbb{F}_{3^3}$	12, 15(abelian)
$(125, 5, 125, 25)$	$\mathbb{F}_{5^3}$	12, 15(abelian)
$(16, 2, 16, 8)$	$\mathbb{F}_{2^4}$	45, 46, 47, 48, 49, 50, 51(abelian)
$(81, 3, 81, 27)$	$\mathbb{F}_{3^4}$	62, 65, 67(abelian)
$(16, 4, 16, 4)$	$\mathbb{F}_{4^2}$	192(abelian), 193, 198, 199, 200, 202, 206, 207, 210, 214, 215, 217, 219, 223, 224, 230, 232, 237, 239, 242, 244, 245, 262, 264, 267(abelian)
$(81, 9, 81, 9)$	$\mathbb{F}_{9^2}$	425, 440, 453, 469, 498, 501, 504(abelian)

Some problems

- This construction provides many RDSs in isomorphic groups, but are they equivalent or not?

Some problems

- This construction provides many RDSs in isomorphic groups, but are they equivalent or not?
- The groups in the construction are sometimes isomorphic even with different representations. Is there any convenient method to judge whether two groups are isomorphic?

Some problems

- This construction provides many RDSs in isomorphic groups, but are they equivalent or not?
- The groups in the construction are sometimes isomorphic even with different representations. Is there any convenient method to judge whether two groups are isomorphic?
- This construction of RDS is an example of success by investigation of subgroups of $AGL(n, q)$. Can we achieve more in finding RDS in $AGL(n, q)$? Is it possible that the developments of the RDSs in subgroups of $AGL(n, q)$ generate new designs?

Thank you very much for your attention!