Regular Automorphism Subgroups of Classical Divisible Designs

Huang Yiwei, Bernhard Schmidt

Maths Division, SPMS, Nanyang Technological University

27 May 2011

A Classical Affine Plane

- Denote the finite field of q elements by $\mathbb{F}_q$, and 2-dimensional vector space over $\mathbb{F}_q$ by V.

A Classical Affine Plane

- Denote the finite field of q elements by $\mathbb{F}_q$, and 2-dimensional vector space over $\mathbb{F}_q$ by V.
- Let the point set $\mathcal{P}$ consist of all the vectors in V, and the line set $\mathcal{L}$ consist of all the cosets of 1-dimensional subspaces of V.

A Classical Affine Plane

- Denote the finite field of q elements by $\mathbb{F}_q$, and 2-dimensional vector space over $\mathbb{F}_q$ by V.
- Let the point set $\mathcal{P}$ consist of all the vectors in V, and the line set $\mathcal{L}$ consist of all the cosets of 1-dimensional subspaces of V.
- The design $(\mathcal{P}, \mathcal{L})$ is the classical affine plane, denoted by $AG(2, q)$.

A Classical Affine Plane

- Denote the finite field of q elements by $\mathbb{F}_q$, and 2-dimensional vector space over $\mathbb{F}_q$ by V.
- Let the point set $\mathcal{P}$ consist of all the vectors in V, and the line set $\mathcal{L}$ consist of all the cosets of 1-dimensional subspaces of V.
- The design $(\mathcal{P}, \mathcal{L})$ is the classical affine plane, denoted by $AG(2, q)$.
- This design has the property that every two points are in exactly one line.

Induced Divisible Design from the Affine Plane

- Delete all the cosets of one 1-dimensional subspace from $AG(2, q)$, what will happen?

Induced Divisible Design from the Affine Plane

- Delete all the cosets of one 1-dimensional subspace from $AG(2, q)$, what will happen?
- Easy to see that any two points in the same coset of the subspace will not be contained in any line, and two points from different cosets are still contained in exactly one line.

Induced Divisible Design from the Affine Plane

- Delete all the cosets of one 1-dimensional subspace from $AG(2, q)$, what will happen?
- Easy to see that any two points in the same coset of the subspace will not be contained in any line, and two points from different cosets are still contained in exactly one line.
- This is a $(q, q, q, 1)$-**divisible design**. It is an induced divisible design from classical affine plane $AG(2, q)$, so we call it the **classical divisible design**.

- Let the point set be $\mathcal{P} = \{(x, y) : x, y \in \mathbb{F}_q\}$. Let the block set be $\mathcal{B} = \{(v, 1)^{\perp} + w : v, w \in \mathbb{F}_q\}$.

Automorphims of the Classical Divisible Design

- Let the point set be $\mathcal{P} = \left\{(x, y) : x, y \in \mathbb{F}_q\right\}$. Let the block set be $\mathcal{B} = \left\{(v, 1)^{\perp} + w : v, w \in \mathbb{F}_q\right\}$.
- An **automorphism** σ of the divisible design $(\mathcal{P}, \mathcal{B})$ is a bijective mapping from $\mathcal{P} \to \mathcal{P}$ and $\mathcal{B} \to \mathcal{B}$ such that if a point p belongs to a block B, then $\sigma(p)$ belongs to $\sigma(B)$.

Automorphims of the Classical Divisible Design

- Let the point set be $\mathcal{P} = \{(x, y) : x, y \in \mathbb{F}_q\}$. Let the block set be $\mathcal{B} = \{(v, 1)^\perp + w : v, w \in \mathbb{F}_q\}$.
- An **automorphism** σ of the divisible design $(\mathcal{P}, \mathcal{B})$ is a bijective mapping from $\mathcal{P} \to \mathcal{P}$ and $\mathcal{B} \to \mathcal{B}$ such that if a point p belongs to a block B, then $\sigma(p)$ belongs to $\sigma(B)$.
- Automorphisms can be composited, and the composition of automorphisms is still an automorphism. The group os all the automorphisms are the **automorphism group** of the design. A subgroup of automorphisms is called an **automorphism subgroup** of the design.

Automorphims of the Classical Divisible Design

- Let the point set be $\mathcal{P} = \{(x, y) : x, y \in \mathbb{F}_q\}$. Let the block set be $\mathcal{B} = \{(v, 1)^{\perp} + w : v, w \in \mathbb{F}_q\}$.
- An **automorphism** σ of the divisible design $(\mathcal{P}, \mathcal{B})$ is a bijective mapping from $\mathcal{P} \to \mathcal{P}$ and $\mathcal{B} \to \mathcal{B}$ such that if a point p belongs to a block B, then $\sigma(p)$ belongs to $\sigma(B)$.
- Automorphisms can be composited, and the composition of automorphisms is still an automorphism. The group os all the automorphisms are the **automorphism group** of the design. A subgroup of automorphisms is called an **automorphism subgroup** of the design.
- If an automorphism subgroup acts regularly both on the point set and the block set, then it is called a **regular** automorphism subgroup.

Divisible Designs and Relative Difference Sets

- It is well known that a regular automorphism subgroup G of a divisible design corresponds to a relative difference set in G.

Divisible Designs and Relative Difference Sets

- It is well known that a regular automorphism subgroup G of a divisible design corresponds to a relative difference set in G.
- An **relative difference set** (in short, we say RDS) R in a group G relative to a normal subgroup N of G, is a subset of G such that the multi-set $\left\{r_1 r_2^{-1} : r_1, r_2 \in R\right\}$ covers every element in $G \backslash N$ with exactly λ times, while nonidentity elements in N is not covered at all, we call N the **forbidden subgroup**.

Divisible Designs and Relative Difference Sets

- It is well known that a regular automorphism subgroup G of a divisible design corresponds to a relative difference set in G.
- An **relative difference set** (in short, we say RDS) R in a group G relative to a normal subgroup N of G, is a subset of G such that the multi-set $\left\{r_1 r_2^{-1} : r_1, r_2 \in R\right\}$ covers every element in $G \backslash N$ with exactly λ times, while nonidentity elements in N is not covered at all, we call N the **forbidden subgroup**.
- The RDS is defined by $R = \{\sigma : \sigma \in G\ ,\ \sigma(p) \in B\}$ for an arbitrary point p and a block B.

Divisible Designs and Relative Difference Sets

- It is well known that a regular automorphism subgroup G of a divisible design corresponds to a relative difference set in G.
- An **relative difference set** (in short, we say RDS) R in a group G relative to a normal subgroup N of G, is a subset of G such that the multi-set $\left\{r_1 r_2^{-1} : r_1, r_2 \in R\right\}$ covers every element in $G \backslash N$ with exactly λ times, while nonidentity elements in N is not covered at all, we call N the **forbidden subgroup**.
- The RDS is defined by $R = \{\sigma : \sigma \in G \ , \ \sigma(p) \in B\}$ for an arbitrary point p and a block B.
- Conversely, if take all the elements of G as points, the translates of R, $(Rg, g \in G)$ as the blocks, then it forms a divisible design which has an regular automorphism group isomorphic to G.

An Example of Regular Automorphism Group

- Recall the classical divisible design, an induced divisible design from $AG(2, q)$:

$$Point\ set\ \mathcal{P} = \{(x, y) : x, y \in \mathbb{F}_q\},$$

and

$$Block\ set\ \mathcal{B} = \left\{(v, 1)^{\perp} + w : v, w \in \mathbb{F}_q\right\}.$$

.

An Example of Regular Automorphism Group

- Recall the classical divisible design, an induced divisible design from $AG(2, q)$:

$$Point\ set\ \mathcal{P} = \{(x, y) : x, y \in \mathbb{F}_q\},$$

and

$$Block\ set\ \mathcal{B} = \left\{(v, 1)^{\perp} + w : v, w \in \mathbb{F}_q\right\}.$$

.

- D. Jungnickel (1982) has introduced the $\mathcal{P} \to \mathcal{P}$ mappings σ_{ab} for all $a, b \in \mathbb{F}_q$, defined by

$$\sigma_{ab} : (x, y) \mapsto (x + a, y + ax + b).$$

Properties of the Mappings

- The mapping $\sigma_{ab} : (x, y) \mapsto (x + a, y + ax + b)$ is injective, thus **bijective** from $\mathcal{P}$ to $\mathcal{P}$.

Properties of the Mappings

- The mapping $\sigma_{ab} : (x, y) \mapsto (x + a, y + ax + b)$ is injective, thus **bijective** from $\mathcal{P}$ to $\mathcal{P}$.
- The points in a block, say $(v, 1)^{\perp} + w$, are mapped under α_{ab} to the points in block $(v - a, 1)^{\perp} + w + (a, b)$. Thus α_{ab} induced a mapping from $\mathcal{B}$ to $\mathcal{B}$. Furthermore, the induced mapping from $\mathcal{B}$ to $\mathcal{B}$ is also **bijective** (easy to verify).

Properties of the Mappings

- The mapping $\sigma_{ab} : (x, y) \mapsto (x + a, y + ax + b)$ is injective, thus **bijective** from $\mathcal{P}$ to $\mathcal{P}$.
- The points in a block, say $(v, 1)^{\perp} + w$, are mapped under α_{ab} to the points in block $(v - a, 1)^{\perp} + w + (a, b)$. Thus α_{ab} induced a mapping from $\mathcal{B}$ to $\mathcal{B}$. Furthermore, the induced mapping from $\mathcal{B}$ to $\mathcal{B}$ is also **bijective** (easy to verify).
- Hence σ_{ab} is an automorphism of the classical divisible design.

Properties of the Mappings

- The mapping $\sigma_{ab} : (x, y) \mapsto (x + a, y + ax + b)$ is injective, thus **bijective** from $\mathcal{P}$ to $\mathcal{P}$.
- The points in a block, say $(v, 1)^{\perp} + w$, are mapped under α_{ab} to the points in block $(v - a, 1)^{\perp} + w + (a, b)$. Thus α_{ab} induced a mapping from $\mathcal{B}$ to $\mathcal{B}$. Furthermore, the induced mapping from $\mathcal{B}$ to $\mathcal{B}$ is also **bijective** (easy to verify).
- Hence σ_{ab} is an automorphism of the classical divisible design.
- The set $G = \{\sigma_{ab} : a, b \in \mathbb{F}_q\}$ forms an automorphism group of size q^2.

Properties of the Mappings

- The mapping $\sigma_{ab} : (x, y) \mapsto (x + a, y + ax + b)$ is injective, thus **bijective** from $\mathcal{P}$ to $\mathcal{P}$.
- The points in a block, say $(v, 1)^{\perp} + w$, are mapped under α_{ab} to the points in block $(v - a, 1)^{\perp} + w + (a, b)$. Thus α_{ab} induced a mapping from $\mathcal{B}$ to $\mathcal{B}$. Furthermore, the induced mapping from $\mathcal{B}$ to $\mathcal{B}$ is also **bijective** (easy to verify).
- Hence σ_{ab} is an automorphism of the classical divisible design.
- The set $G = \{\sigma_{ab} : a, b \in \mathbb{F}_q\}$ forms an automorphism group of size q^2.
- It is a **regular** automorphism group of the design! (Acts regularly both on the point set and the block set)

The Corresponding RDSs

- Let $p = (0,0)$, and $B = (0,1)^{\perp}$. Then the corresponding RDS in group $G = \{\alpha_{ab} : a, b \in \mathbb{F}_q\}$ is

$$R = \{\alpha_{a0} : a \in \mathbb{F}_q\}.$$

The forbidden subgroup is

$$N = \{\alpha_{0b} : b \in \mathbb{F}_q\}.$$

The Corresponding RDSs

- Let $p = (0,0)$, and $B = (0,1)^{\perp}$. Then the corresponding RDS in group $G = \{\alpha_{ab} : a, b \in \mathbb{F}_q\}$ is
$$R = \{\alpha_{a0} : a \in \mathbb{F}_q\}.$$
The forbidden subgroup is
$$N = \{\alpha_{0b} : b \in \mathbb{F}_q\}.$$
- More conveniently, we define the elements in G by 2-tuples, then $G = \{\langle a, b\rangle : a, b \in \mathbb{F}_q\}$, with group operation defined by
$$\langle a, b\rangle * \langle c, d\rangle = \langle a + c, b + d + ac\rangle.$$
The RDS is
$$R = \{\langle a, 0\rangle : a \in \mathbb{F}_q\},$$
and N is
$$N = \{\langle 0, b\rangle : b \in \mathbb{F}_q\}.$$

The Corresponding RDSs

- Let $p = (0,0)$, and $B = (0,1)^{\perp}$. Then the corresponding RDS in group $G = \{\alpha_{ab} : a, b \in \mathbb{F}_q\}$ is
$$R = \{\alpha_{a0} : a \in \mathbb{F}_q\}.$$
The forbidden subgroup is
$$N = \{\alpha_{0b} : b \in \mathbb{F}_q\}.$$
- More conveniently, we define the elements in G by 2-tuples, then $G = \{\langle a, b\rangle : a, b \in \mathbb{F}_q\}$, with group operation defined by
$$\langle a, b\rangle * \langle c, d\rangle = \langle a + c, b + d + ac\rangle .$$
The RDS is
$$R = \{\langle a, 0\rangle : a \in \mathbb{F}_q\},$$
and N is
$$N = \{\langle 0, b\rangle : b \in \mathbb{F}_q\}.$$
- It is an RDS in an abelian group.

Can we obtain more?

- We noticed that the classical divisible design has many regular automorphism groups. Most of them are non-abelian.

Can we obtain more?

- We noticed that the classical divisible design has many regular automorphism groups. Most of them are non-abelian.
- The automorphisms can be represented by some elements from $AGL(2, q)$. They are matrices and translates.

Can we obtain more?

- We noticed that the classical divisible design has many regular automorphism groups. Most of them are non-abelian.
- The automorphisms can be represented by some elements from $AGL(2, q)$. They are matrices and translates.
- The above example is just one regular automorphism subgroup! Can we obtain some other regular subgroups in a simple form just like the example above?

More Automorphisms

- Consider the following mappings:

$$\sigma_{ab}^{f} : (x, y) \mapsto (x + f(a), y + ax + b) \text{ for } a, b \in \mathbb{F}_q,$$

where f is an arbitrary **additive permutation** function from $\mathbb{F}_q$ to $\mathbb{F}_q$.

More Automorphisms

- Consider the following mappings:

$$\sigma_{ab}^{f} : (x, y) \mapsto (x + f(a), y + ax + b) \text{ for } a, b \in \mathbb{F}_q,$$

  where f is an arbitrary **additive permutation** function from $\mathbb{F}_q$ to $\mathbb{F}_q$.

- A function f from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a **permutation** function if $f : x \longmapsto f(x)$ is bijective. The function f is **additive** if $f(x + y) = f(x) + f(y)$.

More Automorphisms

- Consider the following mappings:

$$\sigma_{ab}^{f} : (x, y) \mapsto (x + f(a), y + ax + b) \text{ for } a, b \in \mathbb{F}_q,$$

  where f is an arbitrary **additive permutation** function from $\mathbb{F}_q$ to $\mathbb{F}_q$.
- A function f from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a **permutation** function if $f : x \longmapsto f(x)$ is bijective. The function f is **additive** if $f(x + y) = f(x) + f(y)$.
- Similarly, we can verify that $\left\{\sigma_{ab}^{f} : a, b \in \mathbb{F}_q\right\}$ is a regular automorphism subgroup of the classical divisible design! If f is identity function, then it is just the mentioned example.

The Corresponding RDSs

- Let the group $G = \{\langle a, b\rangle : a, b \in \mathbb{F}_q\}$ with operation

$$\langle a, b\rangle * \langle c, d\rangle = \langle a + c, b + d + af(c)\rangle .$$

The Corresponding RDSs

- Let the group $G = \{\langle a, b\rangle : a, b \in \mathbb{F}_q\}$ with operation

$$\langle a, b\rangle * \langle c, d\rangle = \langle a + c, b + d + af(c)\rangle .$$

- The RDS is

$$R = \{\langle a, 0\rangle : a \in \mathbb{F}_q\} .$$

The Corresponding RDSs

- Let the group $G = \{\langle a, b\rangle : a, b \in \mathbb{F}_q\}$ with operation

$$\langle a, b\rangle * \langle c, d\rangle = \langle a + c, b + d + af(c)\rangle .$$

- The RDS is

$$R = \{\langle a, 0\rangle : a \in \mathbb{F}_q\} .$$

- The forbidden subgroup is

$$N = \{\langle 0, b\rangle : b \in \mathbb{F}_q\} .$$

The Corresponding RDSs

- Let the group $G = \{\langle a, b\rangle : a, b \in \mathbb{F}_q\}$ with operation

$$\langle a, b\rangle * \langle c, d\rangle = \langle a + c, b + d + af(c)\rangle .$$

- The RDS is

$$R = \{\langle a, 0\rangle : a \in \mathbb{F}_q\} .$$

- The forbidden subgroup is

$$N = \{\langle 0, b\rangle : b \in \mathbb{F}_q\} .$$

- They are RDSs mostly in non-abelian groups.

Additive Permutation Function over Finite Fields

Theorem (K. Zhou 2008)

All additive permutation functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ can be written as

$$f(x) = \sum_{i=0}^{n-1} \left(\alpha_0 + \alpha^{p^i} \alpha_1 + \alpha^{2p^i} \alpha_2 + \cdots + \alpha^{(n-1)p^i} \alpha_{n-1} \right) x^{p^i},$$

where α is a fixed primitive element in $\mathbb{F}_{p^n}$, $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is any basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. There are exactly $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ different additive permutation functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$.

Horadam's Results

- K.J. Horadam (2002) has introduced a construction for many non-abelian central $(q, q, q, 1)$-RDSs, by using LP (linearized polynomial) cocycles.

Horadam's Results

- K.J. Horadam (2002) has introduced a construction for many non-abelian central $(q, q, q, 1)$-RDSs, by using LP (linearized polynomial) cocycles.
- The RDSs from Horadam's construction are essentially the same as the RDSs we introduced above.

Horadam's Results

- K.J. Horadam (2002) has introduced a construction for many non-abelian central $(q, q, q, 1)$-RDSs, by using LP (linearized polynomial) cocycles.
- The RDSs from Horadam's construction are essentially the same as the RDSs we introduced above.
- Though the author may not aware that these RDSs are from the classical divisible design.

How many Regular Automorphism Subgroups of Classical Divisible Designs?

- Note that the regular automorphism subgroups are

$$G^f = \left\{ \sigma^f_{ab} : a, b \in \mathbb{F}_q \right\},$$

which depends on the choice of the additive permutation function f.

How many Regular Automorphism Subgroups of Classical Divisible Designs?

- Note that the regular automorphism subgroups are

$$G^f = \left\{ \sigma^f_{ab} : a, b \in \mathbb{F}_q \right\},$$

  which depends on the choice of the additive permutation function f.
- If $q = p^n$, there are $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ distinct such functions. Does it mean that there are at least the same number of regular automorphism subgroups? Yes, but they are not all, in general.

How many Regular Automorphism Subgroups of Classical Divisible Designs?

- Note that the regular automorphism subgroups are

$$G^f = \left\{ \sigma^f_{ab} : a, b \in \mathbb{F}_q \right\},$$

  which depends on the choice of the additive permutation function f.
- If $q = p^n$, there are $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ distinct such functions. Does it mean that there are at least the same number of regular automorphism subgroups? Yes, but they are not all, in general.
- What are those automorphisms look like in the whole automorphism group?

The Whole Automorphism Group

- All the automorphisms of a classical $(q, q, q, 1)$-divisible design consist of the field Frobenius automorphism and elements from the affine general linear group $AGL(2, q)$ in the form

$$\left\langle \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} d \\ e \end{pmatrix} \right\rangle \textit{ for } a, b, c, d, e \in \mathbb{F}_q.$$

There are $2(q-1)(q^2-q)q^2$ many automorphisms.

The Whole Automorphism Group

- All the automorphisms of a classical $(q, q, q, 1)$-divisible design consist of the field Frobenius automorphism and elements from the affine general linear group $AGL(2, q)$ in the form

$$\left\langle \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} d \\ e \end{pmatrix} \right\rangle \textit{ for } a, b, c, d, e \in \mathbb{F}_q.$$

  There are $2(q-1)(q^2-q)q^2$ many automorphisms.

- The automorphisms we introduced are

$$\left\langle \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} f(a) \\ b \end{pmatrix} \right\rangle \textit{ for } a, b \in \mathbb{F}_q.$$

  There are at most q^3 such automorphisms.

The Whole Automorphism Group

- All the automorphisms of a classical $(q, q, q, 1)$-divisible design consist of the field Frobenius automorphism and elements from the affine general linear group $AGL(2, q)$ in the form

$$\left\langle \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} d \\ e \end{pmatrix} \right\rangle \textit{ for } a, b, c, d, e \in \mathbb{F}_q.$$

  There are $2(q-1)(q^2-q)q^2$ many automorphisms.
- The automorphisms we introduced are

$$\left\langle \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} f(a) \\ b \end{pmatrix} \right\rangle \textit{ for } a, b \in \mathbb{F}_q.$$

  There are at most q^3 such automorphisms.
- The conjugacy of the automorphism still have diagonal elements equal to 1. However, by computer search, there are regular subgroups whose automorphism's diagonal elements not equal to 1 for some parameters.

However... Let's see my yesterday-experiments!

- The algebra computing software "Magma" can list and identify all the regular automorphism subgroups of the classical $(q, q, q, 1)$-divisible design for relatively small q. We compare the number of non-isomorphic subgroups searched by computer, and that by the regular subgroups we introduced.

However... Let's see my yesterday-experiments!

- The algebra computing software "Magma" can list and identify all the regular automorphism subgroups of the classical $(q, q, q, 1)$-divisible design for relatively small q. We compare the number of non-isomorphic subgroups searched by computer, and that by the regular subgroups we introduced.
-

parameter q	p∈[2,19]	2^2	3^2	5^2	7^2	2^3	3^3	2^4
#RegularSubgroups	1	4	2	2	2	3	3	36
#R.S. by construction	1	2	2	2	2	3	3	?

My Questions?

1. It seems that the number of non-isomorphisc regular automorphism subgroups of the classical divisible design are equal to

$$\begin{cases} 1 & \textit{if } q \textit{ is a prime}; \\ 2 & \textit{if } q = p^2 \ (p \textit{ odd}) \\ 3 & \textit{if } q = p^3 \end{cases}$$

Is it true?

My Questions?

1. It seems that the number of non-isomorphisc regular automorphism subgroups of the classical divisible design are equal to

$$\begin{cases} 1 & \textit{if } q \textit{ is a prime}; \\ 2 & \textit{if } q = p^2 \ (p \textit{ odd}) \\ 3 & \textit{if } q = p^3 \end{cases}$$

   Is it true?

2. It seems that our construction of regular automorphism subgroups cover a large proportion of all the regular automorphism subgroups in most cases. Can we prove, for some infinite cases, they have covered all the non-isomorphic regular automorphism subgroups?

Many Thanks!

Thank you!

Danke sehr!

Merci Monsieur!

Blagodaryu!

Arigato!

Muito Obrigado!

Gracias a todos!

Xie Xie!