Finding putative automorphism groups of a parallelism of PG(3,q) by GAP *

SVETLANA TOPALOVA, STELA ZHELEZOVA

INSTITUTE OF MATHEMATICS AND INFORMATICS, BAS, BULGARIA

*The research of the first author is supported by the Bulgarian National Science Fund under Contract No KP-06-N32/2-2019 , and of the second author by the Bulgarian National Science Fund under Contract No DH 02/2, 13.12.2016.

Outline

- Definitions and notations
- State-of-the-art
- PΓL(4,q) and its Sylow subgroups
- Cyclic automorphism subgroups
- Noncyclic automorphism subgroups

Parallelisms – relations and applications

Johnson, Combinatorics of Spreads and Parallelisms, CRC Press (2010)

- translation planes
- network coding
- error-correcting codes
- cryptography

Definitions and notations

- Spread in PG(n,q) - a partition of the point set by lines.
- Isomorphic spreads - if there is an automorphism of PG(n,q) which takes one spread to the other.
- Parallelism in PG(n,q) – a partition of the set of all lines by spreads

Definitions and notations

- Isomorphic parallelisms - if there is an automorphism of PG(n,q) which maps each spread of one parallelism to a spread of the other.

- Automorphism of a parallelism – an automorphism of PG(n,q) which preserves the parallelism, i.e. maps each spread of the parallelism to a spread of the same parallelism.

BNSF Contract No DH 02/2, 13.12.2016

State - of - the - art

General constructions of parallelisms:

- in PG(n,2), Zaicev, Zinoviev, Semakov, 1973; Baker, 1976.
- in PG(2^n-1,q), Beutelspacher, 1974.
- a pair of orthogonal parallelisms in PG(3,q) – Fuji-Hara,1986.
- two infinite families of regular cyclic parallelisms, PG(3,q), q ≡ 2 (mod 3), Penttila and Williams, 1998.

State - of - the - art

Parallelisms in PG(3,q):

- PG(3,2) – all (2) are classified, regular;
- PG(3,3)
  - aut(5) – Prince, 1997;
  - all (73 343) – Betten, 2016;
- PG(3,4)
  - odd prime order – Topalova, Zhelezova, 2013, 2015, 2017;
  - Baer involution – Betten, Topalova, Zhelezova, 2018;
  - cyclic groups of order 4 – Betten, Topalova, Zhelezova, 2019

BNSF Contract No DH 02/2, 13.12.2016

The number of known parallelisms of PG(3,4) with nontrivial automorphisms

Aut	2	3	4	5	6	7	8	10	12	15	16	17	20	24	30	32	48	60	64	96	960
#	≥ 286 340	8 115 559	≥ 25 1836	31 830	4 488	482	≥ 596	76	52	40	≥ 170	0	52	14	38	≥ 14	12	8	≥ 4	2	4

$G \cong P\Gamma L(4,4)$ $|G| = 2^{13} . 3^4 . 5^2 . 7 . 17$

State - of - the - art

Parallelisms in PG(3,5):

- automorphism of order 31 – Prince, 1998;
- regular – Topalova, Zhelezova, 2016;
- automorphism of order 13 – Topalova, Zhelezova, 2019;
- cyclic automorphism group of order 8 which fixes 2 points and for which some additional restrictions hold, ACCT 2020.

PG(3,q) construction

- lexicographic order on the points → lines → parallelisms
- points - $v = q^n + q^{n-1} + q + 1$;
- lines - $(q^2+1)(q^2+q+1)$;
- lines in a spread - q^2+1;
- spreads in a parallelism - q^2+q+1;

parameters	PG(3,4)	PG(3,5)
Aut group	PΓL(4,4)	PΓL(4,5)
points	85	156
lines	357	806
lines per spread	17	26
spreads per parallelisms	21	31

- generators of PΓL(4,q) – permutations of the points.

PΓL (4,q)

$|P\Gamma L(4,q)| = r(q^4 - 1)(q^4 - q)(q^4 - q^2)(q^4 - q^3) / (q-1)$,

p is a prime number and $p^r = q$;

> Let G be a finite group and p be a prime. A subgroup of G whose order is the highest power of p dividing |G| is called a p-Sylow subgroup of G.

$|P\Gamma L(4,q)| = a^m . b^n . c^w \ldots$, a, b, c, … – prime numbers

a-Sylow subgroup of order a^m, b-Sylow subgroup of order b^n, ...

$|P\Gamma L(4,4)| = 2^{13} . 3^4 . 5^2 . 7 . 17$; $|P\Gamma L(4,5)| = 2^9 . 3^2 . 5^6 . 13 . 31$

A subgroup of PΓL (4,q)

https://www.gap-system.org/

$|G| = a^m. b^n. c^w \dots$, a, b, c, … – prime numbers;

G:=Group([a generator list]);

> Theorem (Sylow II). For each prime p, the p-Sylow subgroups of G are conjugate.

G_i – a subgroup of G, $i \in \{a, b, c, \dots\}$

G_i :=SylowSubgroup(G,i);

A p-Sylow subgroup of PΓL (4,q)

own C++ programs,
Q-extension [I.Bouyukliev]

```
G:=Group([a generator list]);
```

G_i – a subgroup of G, i ∈ {a, b, c, …}

G_i :=SylowSubgroup(G,i); → Print(G_i ,"\n"); → G_i := Group([...]);

Print(Elements(G_i),"\n"); ⇒

N_i := Normalizer(G, G_i); ⇒

Print(N,"\n");

a:=Order(N);

Print(a,"\n");

G_i and its normalizer **N_i** as point permutation – data for our own C++ programs

$N_G(G_i) = \{ \alpha \in G \mid \alpha G_i \alpha^{-1} = G_i \}$

$|P\Gamma L(4,4)| = 2^{13} . 3^4 . 5^2 . 7 . 17$; $|P\Gamma L(4,5)| = 2^9 . 3^2 . 5^6 .13 . 31$

The conjugacy classes

$|G| = a^m. b^n. c^w\ldots$, a, b, c – p numb;

G_i is i-Sylow subgroup of G

$|G_i| = i^k$, $1 \le j \le i^k - 1$, $k \in \{m, n, \ldots\}$

```
Print(Elements(G_i ),"\n");

c_j :=Group([ a point permutation of G_i ]);

Print(Order(c_j),"\n");
N_j:= Normalizer( G, c_j ); Print(Order(N_j),"\n");
```

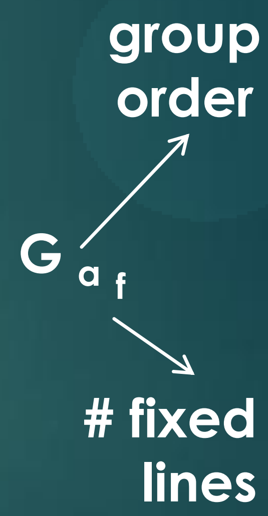
for each permutation of i-Sylow subgroup

```
Print(IsConjugate(G,c_t,c_v),"\n");
```

c_t,c_v are cyclic subgroups of G_i with equal orders and normalizer orders

PΓL(4,4) and its 2-Sylow subgroup ($|G_2|=2^{13}$)

element order	generated subgroup	normalizer order	subgroups
2	$G_{2_{21}}$	30720	-
2	$G_{2_{35}}$	40320	-
2	$G_{2_{37}}$	368640	-
4	G_{4_1}	256	$G_{2_{21}}$
4	G_{4_5}	3072	$G_{2_{37}}$
4	G_{4_7}	384	$G_{2_{21}}$
4	$G_{4_{11}}$	768	$G_{2_{37}}$
8	G_{8_1}	64	$G_{2_{21}}$, G_{4_1}
8	G_{8_3}	128	$G_{2_{37}}$, G_{4_5}



PG(3,4), $2^{13} = 8192$

Automorphism Groups by GAP

BNSF Contract No DH 02/2, 13.12.2016

PΓL(4,5) and its 2-Sylow subgroup ($|G_2|=2^9$)

class	1	2	3	4	5	6	7	8	9	10	11	12
element order	**2**	**2**	**2**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**8**	**8**
normalizer order	115200	187200	1488000	512	624	1152	1920	3840	115200	1488000	384	5760

PG(3,5), $2^9 = 512$

Automorphism Groups by GAP

Non cyclic automorphism groups of order 4

G_4 - subbgroup of G, $G_4 = \{e, c_1, c_2, c_3\}$

c_j – of order 2 => $c_j^{-1} = c_j$ $j = 1, 2, 3$

$c_i\, c_j\, c_i = c_k\, c_i = c_j$ => $c_i \in C(c_j)$, $j, k = 1, 2, 3;\ j \neq k$

$C(c_j) = \{ \beta \in G \mid \beta\, c_j\, \beta^{-1} = c_j \}$

$G_{2_{21}}$ - the subgroup of order 2

c_j is conjugate to c_k

Construction of the considered noncyclic automorphism groups:

- $c_1 \in G_2$;
- $c_2 \in C(c_1)$ and c_2 is conjugate to c_1
- $c_3 = c_1\, c_2$ and c_3 is conjugate to c_1

Non cyclic automorphism groups of order 4 in PΓL(4,4) - construction

G_4 - subbgroup of G, $G_4 = \{e, c_1, c_2, c_3\}$

$G_{2_{21}}$ - the subgroup of order 2, $c_1 \in G_{2_{21}}$

c_1;

c_2; …; c_420;

$c_2 \in C(c_1)$ and c_2 is conjugate to c_1
C(c_1) = { β ∈ G | β c1 β -1 = c1 }

```
d:=Group([c_1,c_i]);

Print(Order(d),"-");

Print(Elements(d),"\n");
```

for each c_2 to c_420 generate the group d, check its 3-rd element if it is conjugate to c_1 and c_i

```
N_i:= Normalizer(G,d); Print(Order(N_i,"\n");
```

partition in congugacy classes

BNSF Contract No DH 02/2, 13.12.2016

Conjugacy classes of non cyclic automorphism groups of order 4

generated subgroup	normalizer order
G_{4_1}	768
G_{4_2}	2560
G_{4_3}	92160
G_{4_4}	6144
G_{4_5}	9216

Thank you for the attention!