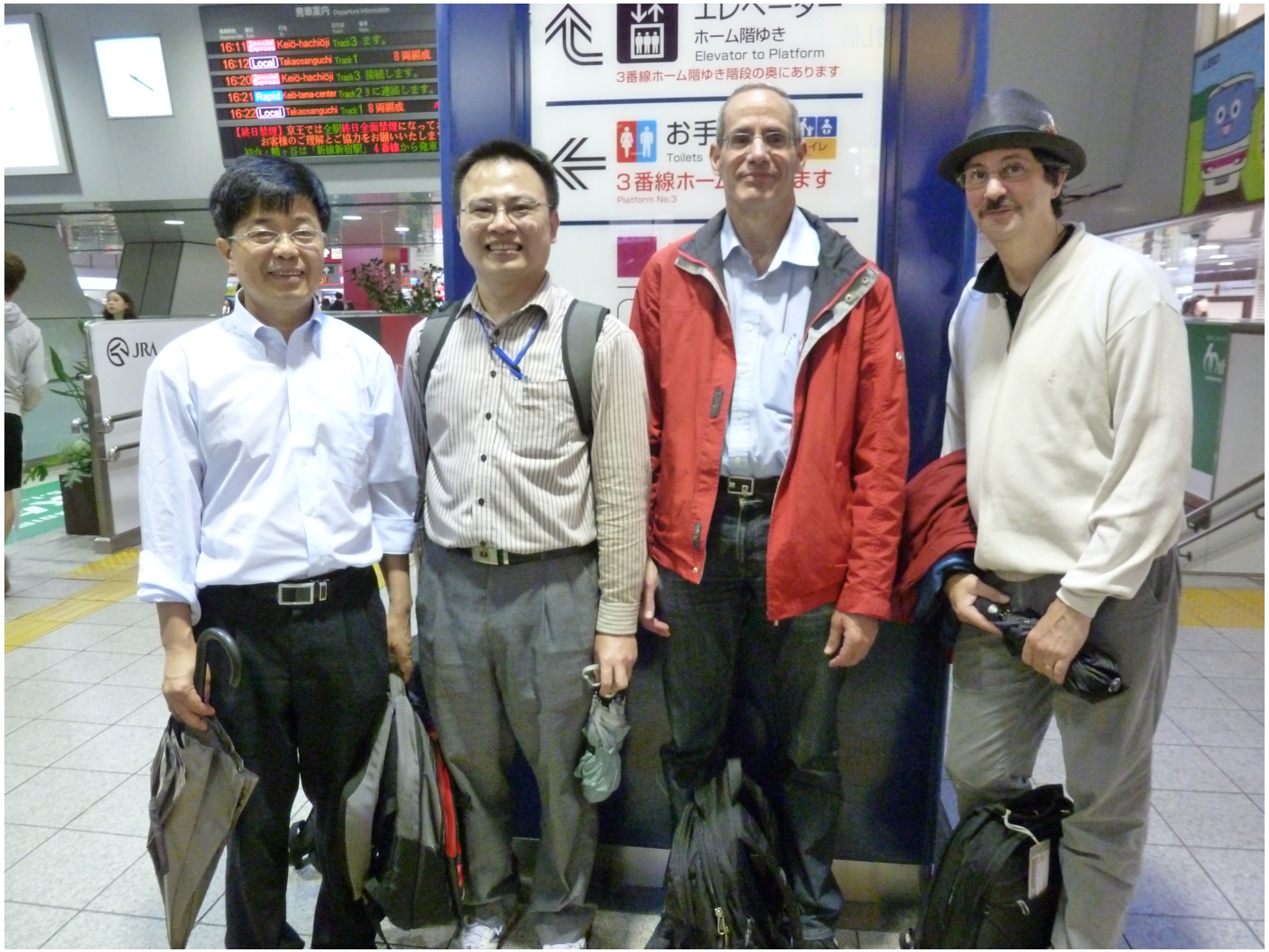
On affine-invariant strictly cyclic Steiner quadruple systems

Xiao-Nan Lu, Masakazu Jimbo
Nagoya University, Japan

"2014 Symposium for Young Combinatorialists"
National Taiwan Normal University, Taiwan, Aug 2, 2014.

The 2nd Japan-Taiwan Conference on Combinatorics and its Applications, Nagoya University. Nov 10-12, 2012.

JSPS-DST Asian Academic Seminar 2013 – Discrete Mathematics & its Applications, the University of Tokyo. Nov 3-10, 2013.



Japan Conference on Graph Theory and Combinatorics, Nihon University, May 17-21, 2014.

On affine-invariant strictly cyclic Steiner quadruple systems

Xiao-Nan Lu, Masakazu Jimbo
Nagoya University, Japan

"2014 Symposium for Young Combinatorialists"
National Taiwan Normal University, Taiwan, Aug 2, 2014.

Outline

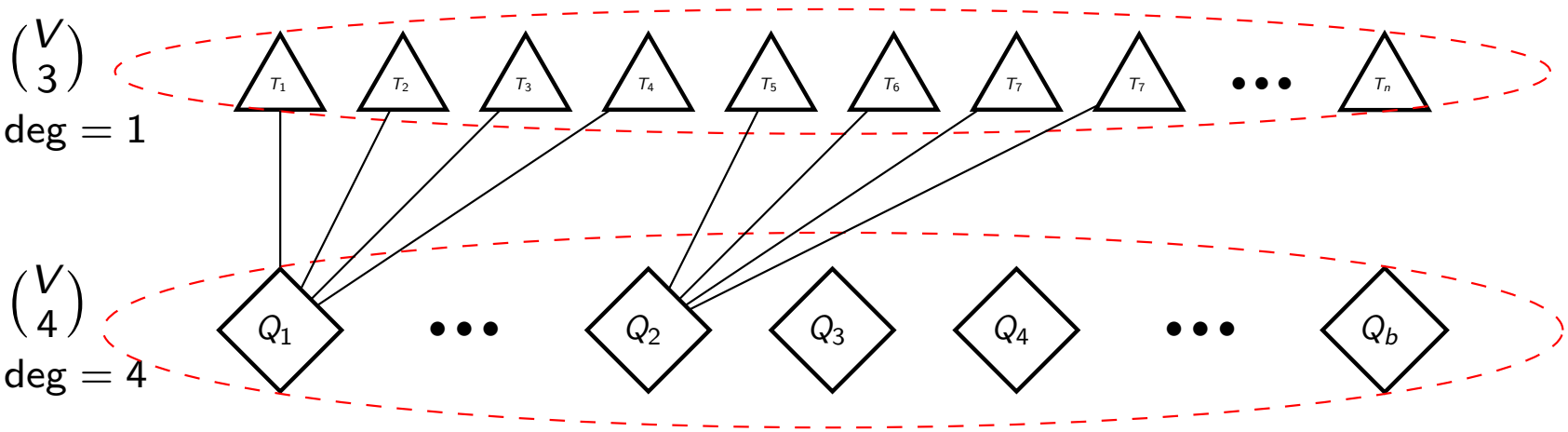
Steiner quadruple systems (SQS's)

Definition

A pair $(V, \mathcal{B})$ is called a Steiner quadruple systems, denoted by SQS(v), if

- V is a finite set of v elements (points).
- $\mathcal{B} \subseteq \binom{V}{4}$ is a collection of quadruples (4-subsets, blocks) of V.
- Each triple (3-subset) of V occurs in exactly one quadruple in $\mathcal{B}$.

Incidence structure $\mathcal{I}$



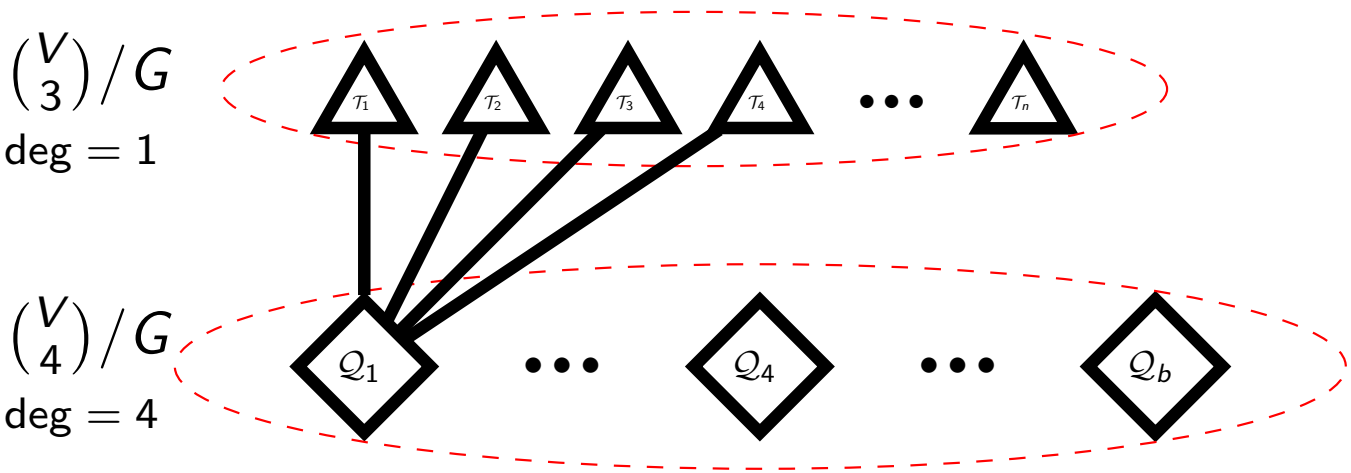
Steiner quadruple systems (SQS's)

Definition

A pair $(V, \mathcal{B})$ is called a Steiner quadruple systems, denoted by SQS(v), if

- V is a finite set of v elements (points).
- $\mathcal{B} \subseteq \binom{V}{4}$ is a collection of quadruples (4-subsets, blocks) of V.
- Each triple (3-subset) of V occurs in exactly one quadruple in $\mathcal{B}$.

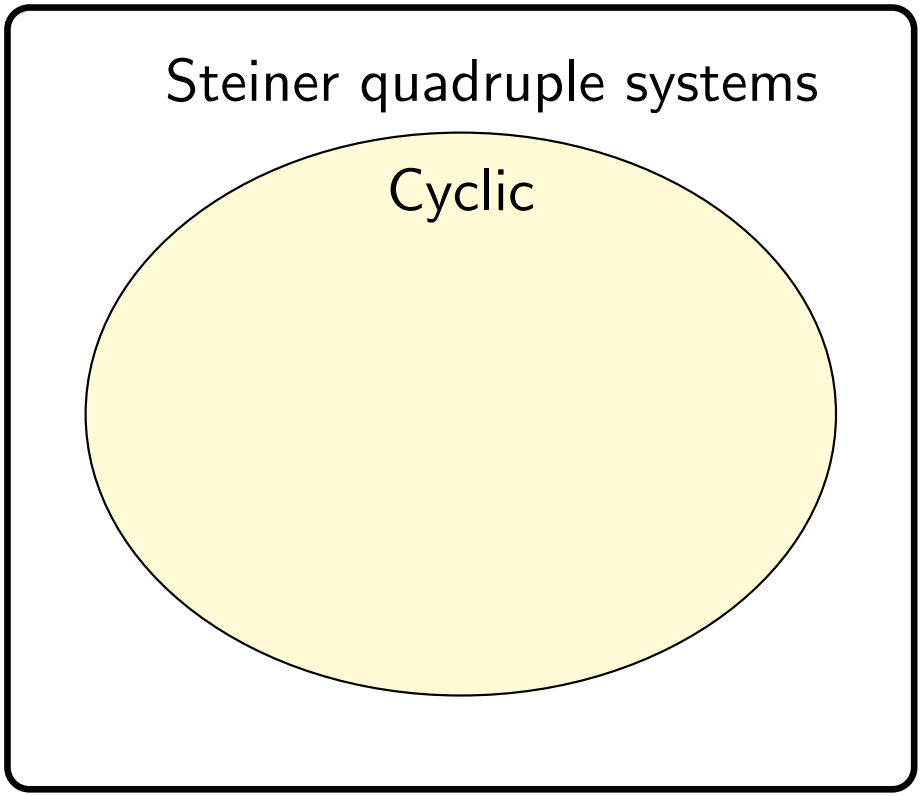
Quotient structure $\mathcal{I}/G$



G: (symmetries)

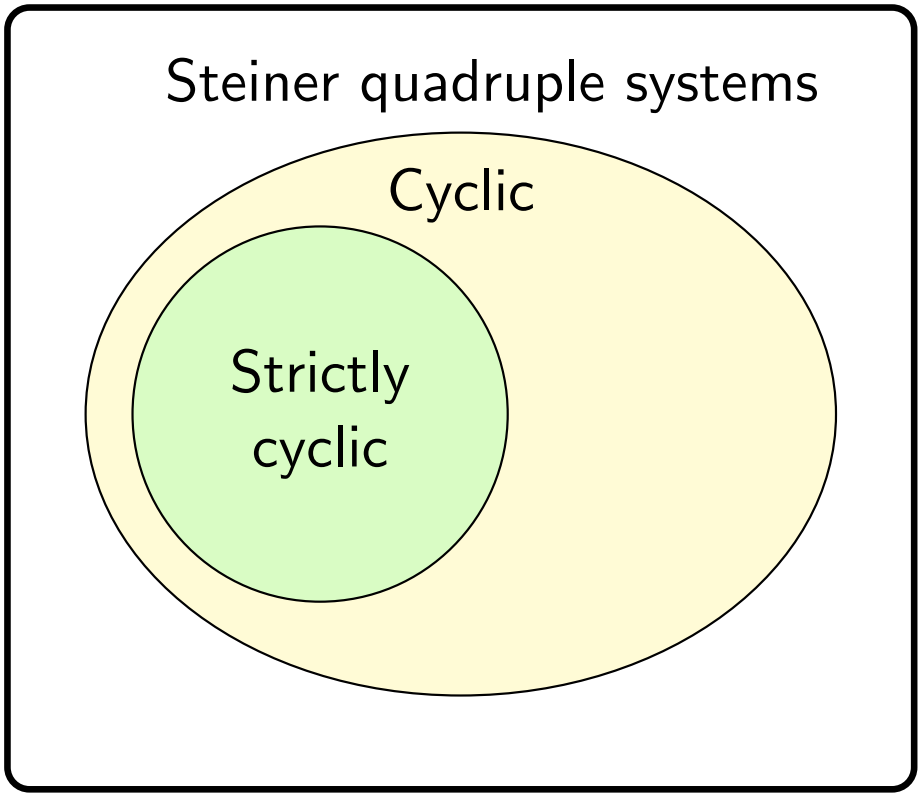
- Cyclic groups
- Dihedral groups
- Affine groups

A brief historical overview of studies on SQS's



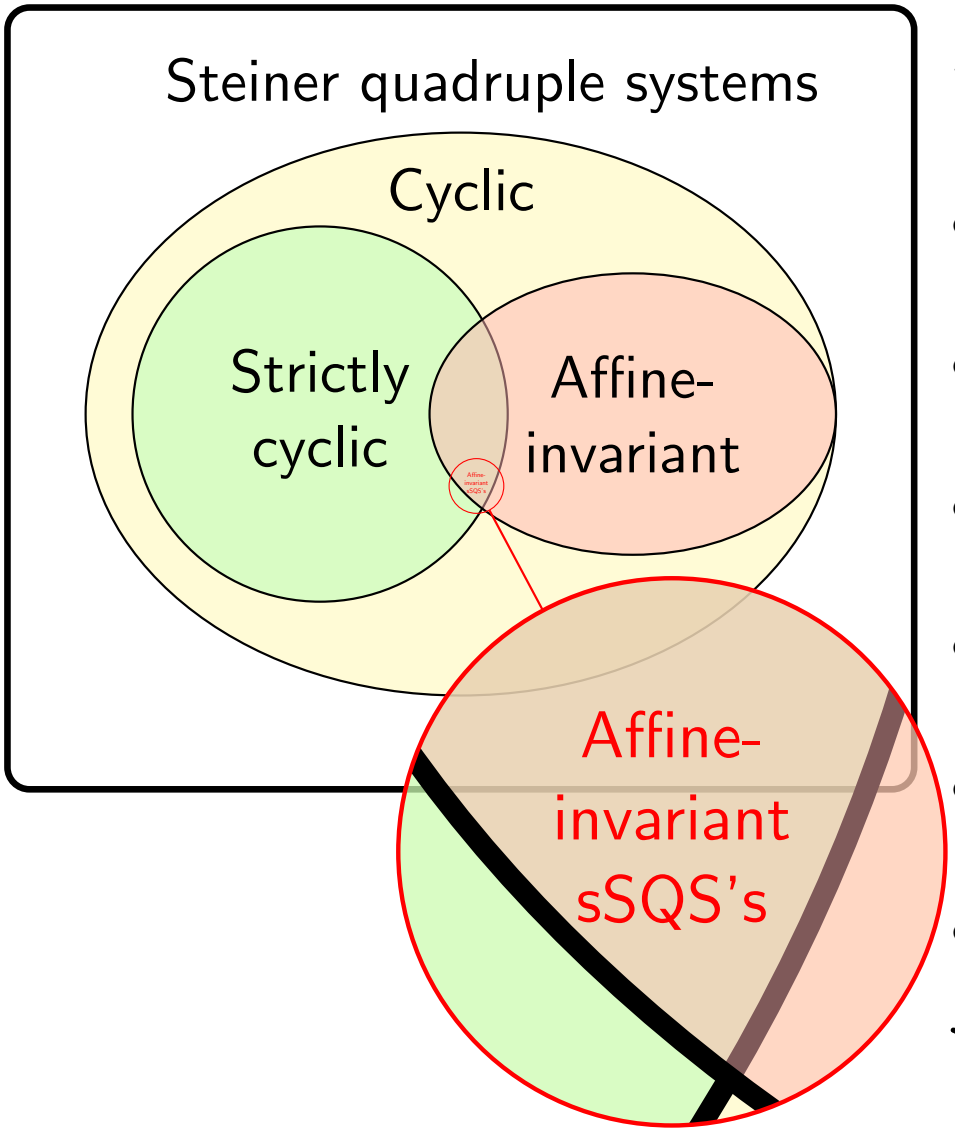
- 1847, Kirkman
  SQS(2^n) exists, for all $n > 0$.
- 1915, Fitting
  Cyclic SQS(v), $v \in \{26, 34\}$.
- 1960, Hanani
  SQS(v) exists, iff $v \equiv 2, 4 \pmod 6$.

A brief historical overview of studies on SQS's



- 1847, Kirkman
  SQS(2^n) exists, for all $n > 0$.
- 1915, Fitting
  Cyclic SQS(v), $v \in \{26, 34\}$.
- 1960, Hanani
  SQS(v) exists, iff $v \equiv 2, 4 \pmod 6$.
- 1979, Köhler
  Strictly cyclic SQS's (sSQS's).
- 1985, Piotrowski
  sSQS($2p$) admitting D_{2p}.
- 1987-1998, Siemon
  Köhler graphs and number theory.

A brief historical overview of studies on SQS's



- 1847, Kirkman
  SQS(2^n) exists, for all $n > 0$.
- 1915, Fitting
  Cyclic SQS(v), $v \in \{26, 34\}$.
- 1960, Hanani
  SQS(v) exists, iff $v \equiv 2, 4 \pmod 6$.
- 1979, Köhler
  Strictly cyclic SQS's (sSQS's).
- 1985, Piotrowski
  sSQS($2p$) admitting D_{2p}.
- 1987-1998, Siemon
  Köhler graphs and number theory.
- Now,
  Affine-invariant sSQS's.

Affine-invariant sSQS($2p$)

EXAMPLE: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

$$
\begin{array}{lll}
\{0,1,5,9\}, & \{0,2,5,8\}, & \{0,1,3,4\}, \\
\{1,2,6,0\}, & \{1,3,6,9\}, & \{1,2,4,5\}, \\
\{2,3,7,1\}, & \{2,4,7,0\}, & \{2,3,5,6\}, \\
\{3,4,8,2\}, & \{3,5,8,1\}, & \{3,4,6,7\}, \\
\{4,5,9,3\}, & \{4,6,9,2\}, & \{4,5,7,8\}, \\
\{5,6,0,4\}, & \{5,7,0,3\}, & \{5,6,8,9\}, \\
\{6,7,1,5\}, & \{6,8,1,4\}, & \{6,7,9,0\}, \\
\{7,8,2,6\}, & \{7,9,2,5\}, & \{7,8,0,1\}, \\
\{8,9,3,7\}, & \{8,0,3,6\}, & \{8,9,1,2\}, \\
\{9,0,4,8\}, & \{9,1,4,7\}, & \{9,0,2,3\}.
\end{array}
$$

Affine-invariant sSQS($2p$)

EXAMPLE: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

$+5$

$\{0,1,5,9\}$,	$\{0,2,5,8\}$,	$\{0,1,3,4\}$,
$\{1,2,6,0\}$,	$\{1,3,6,9\}$,	$\{1,2,4,5\}$,
$\{2,3,7,1\}$,	$\{2,4,7,0\}$,	$\{2,3,5,6\}$,
$\{3,4,8,2\}$,	$\{3,5,8,1\}$,	$\{3,4,6,7\}$,
$\{4,5,9,3\}$,	$\{4,6,9,2\}$,	$\{4,5,7,8\}$,
$\{5,6,0,4\}$,	$\{5,7,0,3\}$,	$\{5,6,8,9\}$,
$\{6,7,1,5\}$,	$\{6,8,1,4\}$,	$\{6,7,9,0\}$,
$\{7,8,2,6\}$,	$\{7,9,2,5\}$,	$\{7,8,0,1\}$,
$\{8,9,3,7\}$,	$\{8,0,3,6\}$,	$\{8,9,1,2\}$,
$\{9,0,4,8\}$,	$\{9,1,4,7\}$,	$\{9,0,2,3\}$.

A strictly cyclic SQS (sSQS)

Cyclic orbits $B + c \in \mathcal{O}_{\text{cyclic}}$

Affine-invariant sSQS($2p$)

EXAMPLE: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

$+5$

$\{0,1,5,9\}$,	$\{0,2,5,8\}$,	$\{0,1,3,4\}$,
$\{1,2,6,0\}$,	$\{1,3,6,9\}$,	$\{1,2,4,5\}$,
$\{2,3,7,1\}$,	$\{2,4,7,0\}$,	$\{2,3,5,6\}$,
$\{3,4,8,2\}$,	$\{3,5,8,1\}$,	$\{3,4,6,7\}$,
$\{4,5,9,3\}$,	$\{4,6,9,2\}$,	$\{4,5,7,8\}$,
$\{5,6,0,4\}$,	$\{5,7,0,3\}$,	$\{5,6,8,9\}$,
$\{6,7,1,5\}$,	$\{6,8,1,4\}$,	$\{6,7,9,0\}$,
$\{7,8,2,6\}$,	$\{7,9,2,5\}$,	$\{7,8,0,1\}$,
$\{8,9,3,7\}$,	$\{8,0,3,6\}$,	$\{8,9,1,2\}$,
$\{9,0,4,8\}$,	$\{9,1,4,7\}$,	$\{9,0,2,3\}$.

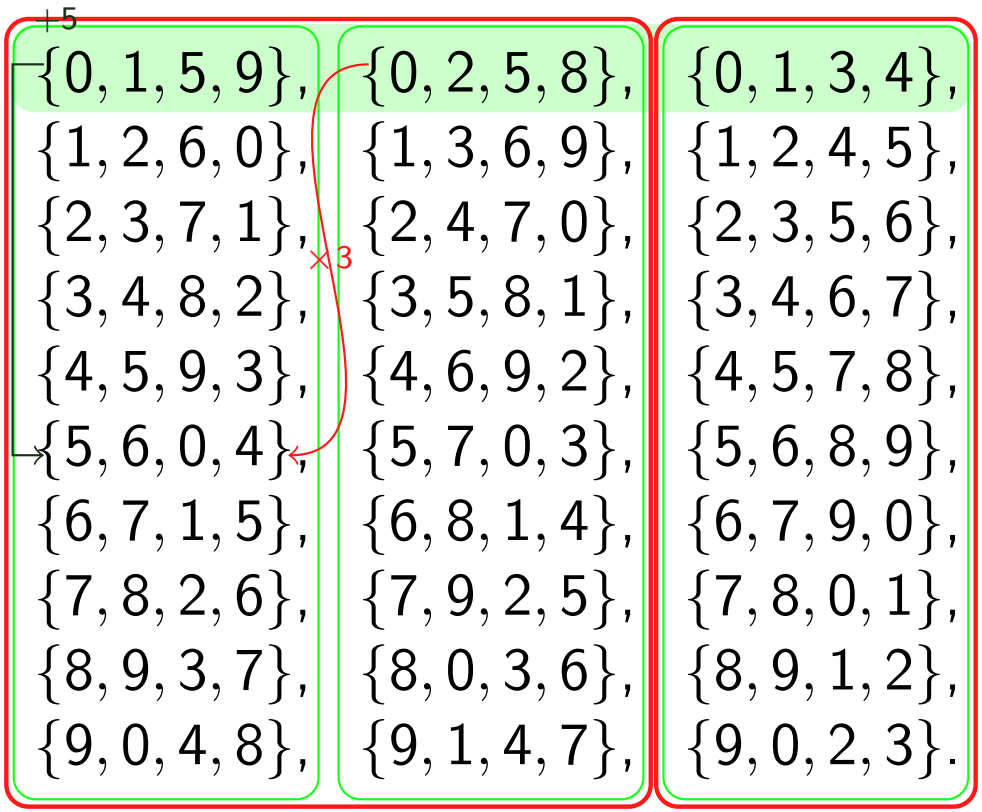
A strictly cyclic SQS (sSQS)

Cyclic orbits $B + c \in \mathcal{O}_{\text{cyclic}}$

Base blocks of cyclic orbits

Affine-invariant sSQS($2p$)

EXAMPLE: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.



A strictly cyclic SQS (sSQS)

Cyclic orbits $B + c \in \mathcal{O}_{\text{cyclic}}$

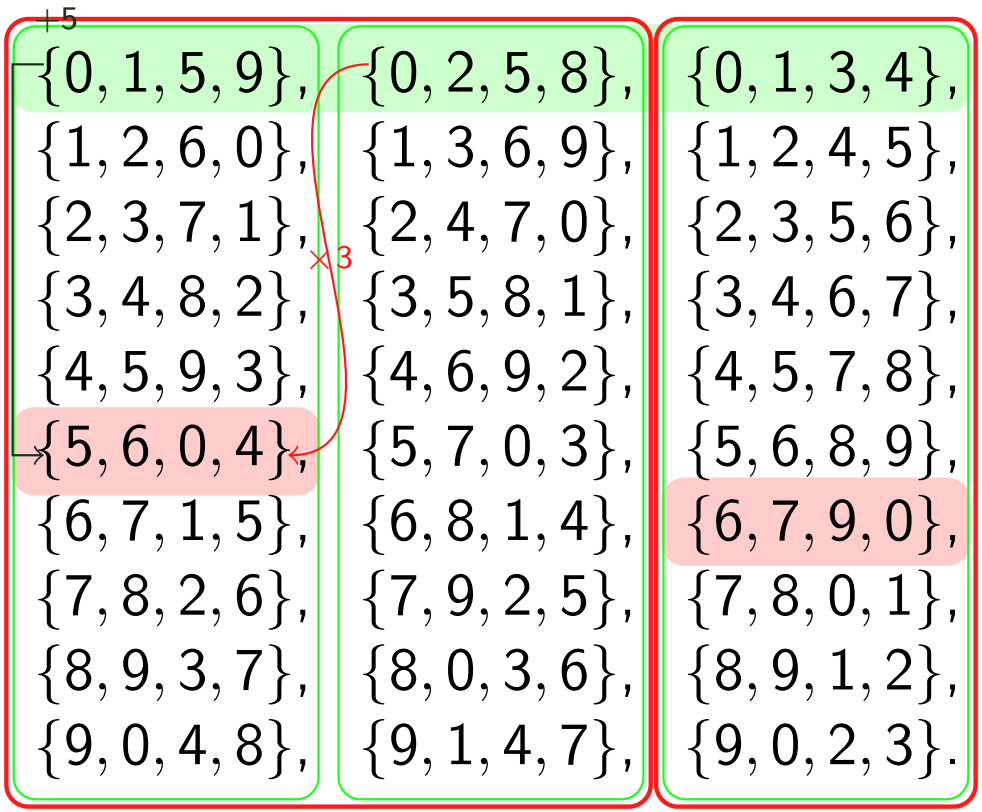
Base blocks of cyclic orbits

An affine-invariant sSQS

Affine orbits $aB + c \in \mathcal{O}_{\text{affine}}$

Affine-invariant sSQS($2p$)

EXAMPLE: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.



$\{0,1,5,9\}$,	$\{0,2,5,8\}$,	$\{0,1,3,4\}$,
$\{1,2,6,0\}$,	$\{1,3,6,9\}$,	$\{1,2,4,5\}$,
$\{2,3,7,1\}$,	$\{2,4,7,0\}$,	$\{2,3,5,6\}$,
$\{3,4,8,2\}$,	$\{3,5,8,1\}$,	$\{3,4,6,7\}$,
$\{4,5,9,3\}$,	$\{4,6,9,2\}$,	$\{4,5,7,8\}$,
$\{5,6,0,4\}$,	$\{5,7,0,3\}$,	$\{5,6,8,9\}$,
$\{6,7,1,5\}$,	$\{6,8,1,4\}$,	$\{6,7,9,0\}$,
$\{7,8,2,6\}$,	$\{7,9,2,5\}$,	$\{7,8,0,1\}$,
$\{8,9,3,7\}$,	$\{8,0,3,6\}$,	$\{8,9,1,2\}$,
$\{9,0,4,8\}$,	$\{9,1,4,7\}$,	$\{9,0,2,3\}$.

A strictly cyclic SQS (sSQS)

Cyclic orbits $B + c \in \mathcal{O}_{\text{cyclic}}$

Base blocks of cyclic orbits

An affine-invariant sSQS

Affine orbits $aB + c \in \mathcal{O}_{\text{affine}}$

Base blocks of affine orbits

Our aim: find base blocks $B_i = \{0, p+1, x, y\}$, s.t. $\mathcal{B} = \bigcup_i \mathcal{O}_{\text{affine}}(B_i)$.

Outline

A presentation of blocks over $\mathbb{Z}_p \times \mathbb{Z}_2$

Lemma (Köhler, 1979)

An sSQS(v) exists, only if $v \equiv 2, 10 \pmod{24}$. $v = 2p$, $p \equiv 1, 5 \pmod{12}$

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_p \times \mathbb{Z}_2 = \{(u, 0) \mid u \in \mathbb{Z}_p\} \cup \{(u, 1) \mid u \in \mathbb{Z}_p\}$$

For $B_i = \{0, p+1, x, y\}$, let $u \equiv x, w \equiv y \pmod{p}$.

$\{(0,0),(1,0),(u,1),(w,1)\} =: \{0,1;u,w\} \longrightarrow$ Type I

$\{(0,0),(1,0),(u,1),(w,0)\} =: \{0,1,w;u\}$

$\{(0,0),(1,0),(u,0),(w,1)\} =: \{0,1,u;w\}$ $\longrightarrow$ Type II

$\{(0,0),(1,0),(u,0),(w,0)\} =: \{0,1,u,w\} \longrightarrow$ Type III

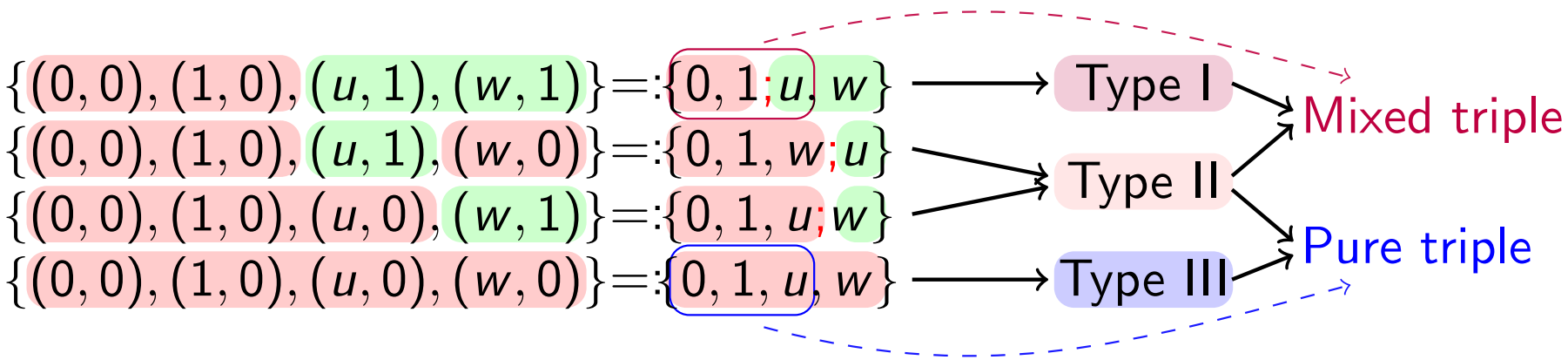
A presentation of blocks over $\mathbb{Z}_p \times \mathbb{Z}_2$

Lemma (Köhler, 1979)

An sSQS(v) exists, only if $v \equiv 2, 10 \pmod{24}$. $v = 2p$, $p \equiv 1, 5 \pmod{12}$

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_p \times \mathbb{Z}_2 = \{(u, 0) \mid u \in \mathbb{Z}_p\} \cup \{(u, 1) \mid u \in \mathbb{Z}_p\}$$

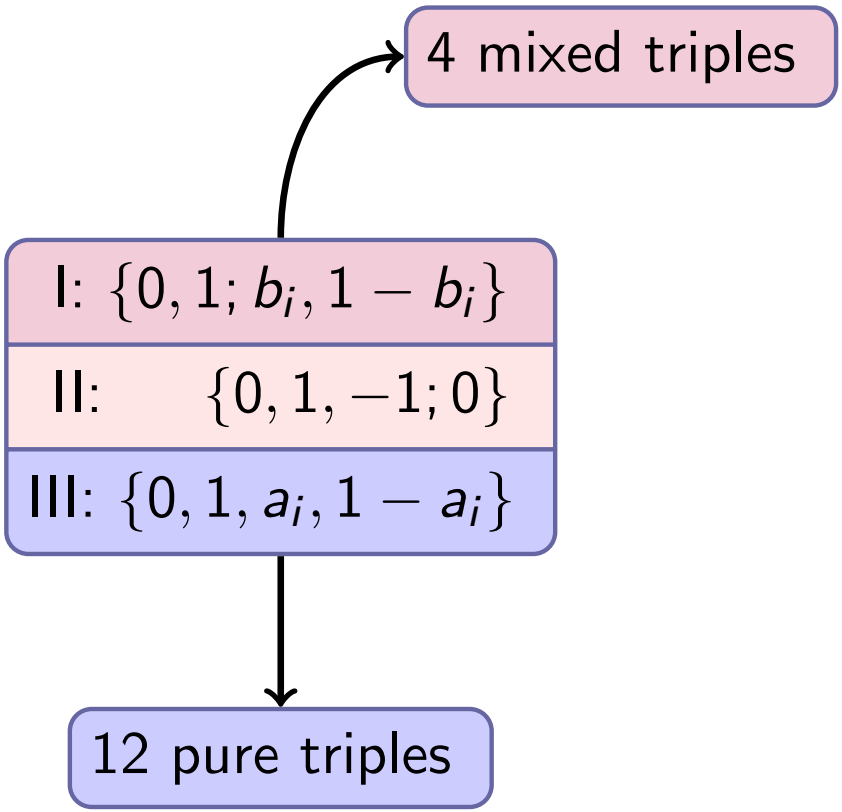
For $B_i = \{0, p+1, x, y\}$, let $u \equiv x, w \equiv y \pmod{p}$.



Base blocks of affine-invariant sSQS($2p$)

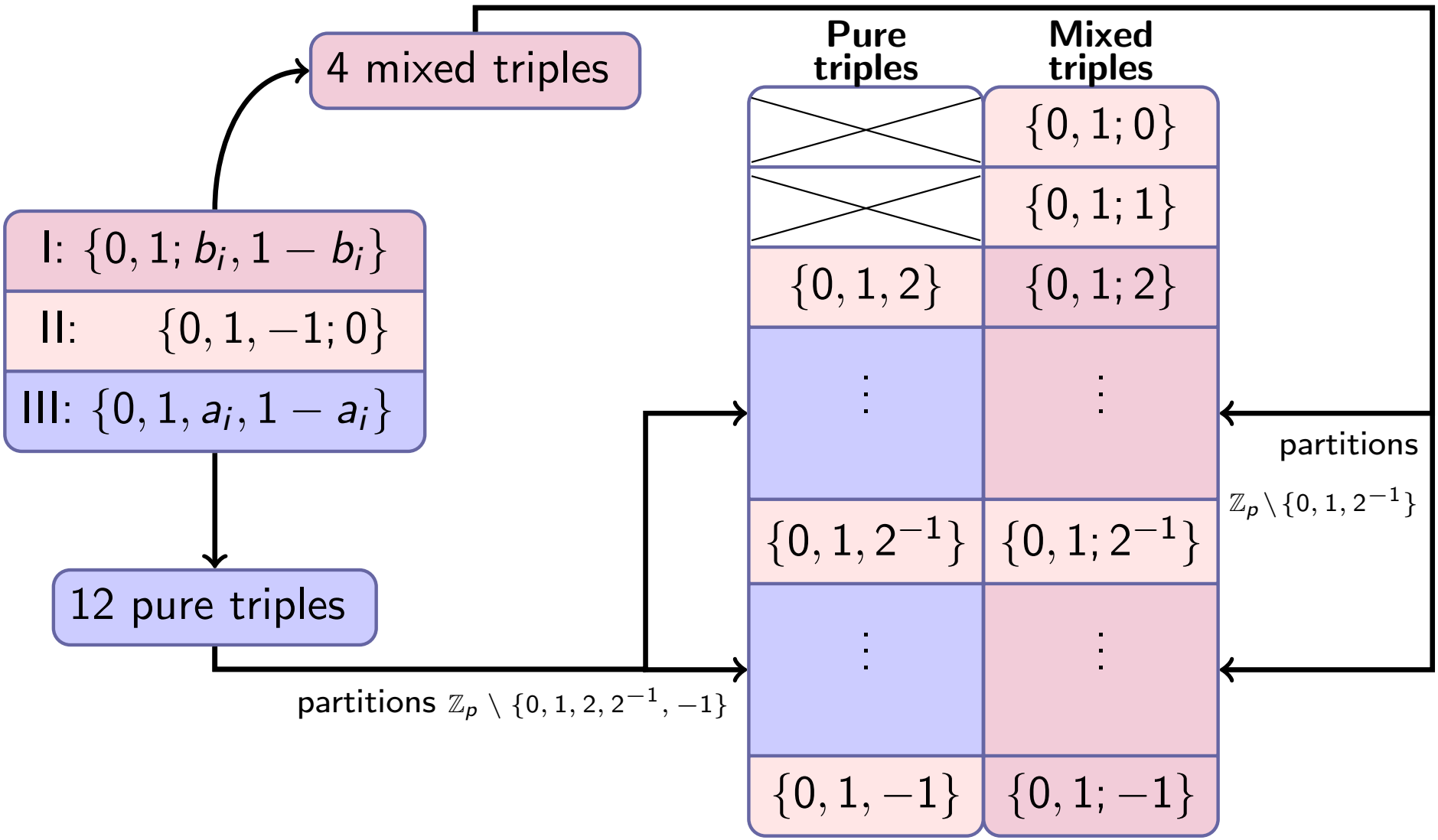
Pure triples	Mixed triples
~~$\{0,1,2\}$~~	$\{0,1;0\}$
~~$\{0,1,2^{-1}\}$~~	$\{0,1;1\}$
$\{0,1,2\}$	$\{0,1;2\}$
$\vdots$	$\vdots$
$\{0,1,2^{-1}\}$	$\{0,1;2^{-1}\}$
$\vdots$	$\vdots$
$\{0,1,-1\}$	$\{0,1;-1\}$

Base blocks of affine-invariant sSQS($2p$)



Pure triples	Mixed triples
	$\{0, 1; 0\}$
	$\{0, 1; 1\}$
$\{0, 1, 2\}$	$\{0, 1; 2\}$
⋮	⋮
$\{0, 1, 2^{-1}\}$	$\{0, 1; 2^{-1}\}$
⋮	⋮
$\{0, 1, -1\}$	$\{0, 1; -1\}$

Base blocks of affine-invariant sSQS(2p)



Projective lines and graphs $\mathrm{LG}(V_p)$

$\mathscr{P}(\mathbb{F}_p) := \mathbb{F}_p \cup \{\infty\}$: the projective line over the finite field $\mathbb{F}_p$.

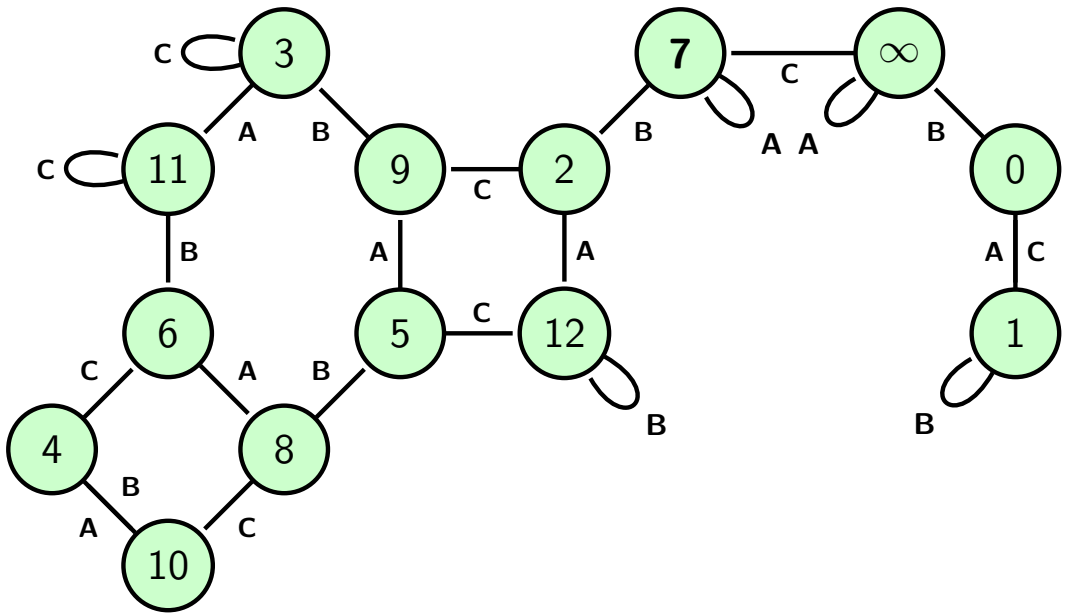
Let $\mathrm{LG}(V_p)$ be a graph whose vertex set is $V_p \subseteq \mathscr{P}(\mathbb{F}_p)$ and edge set is $\{\{x, y\} \mid x = y^\sigma, \sigma \in \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}\}$.

Let

$$\sigma_{\boldsymbol{A}} : x \mapsto 1 - x,$$
$$\sigma_{\boldsymbol{B}} : x \mapsto \frac{1}{x},$$
$$\sigma_{\boldsymbol{C}} : x \mapsto \frac{x-1}{2x-1}$$

be mappings on $\mathscr{P}(\mathbb{F}_p)$.
For $p \equiv 1 \pmod 4$,
$\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}} \rangle = \mathrm{PSL}(2, p)$.

Example: $\mathrm{LG}(\mathscr{P}(\mathbb{F}_{13}))$



Projective lines and graphs $\mathrm{LG}(V_p)$

$\mathscr{P}(\mathbb{F}_p) := \mathbb{F}_p \cup \{\infty\}$: the projective line over the finite field $\mathbb{F}_p$.

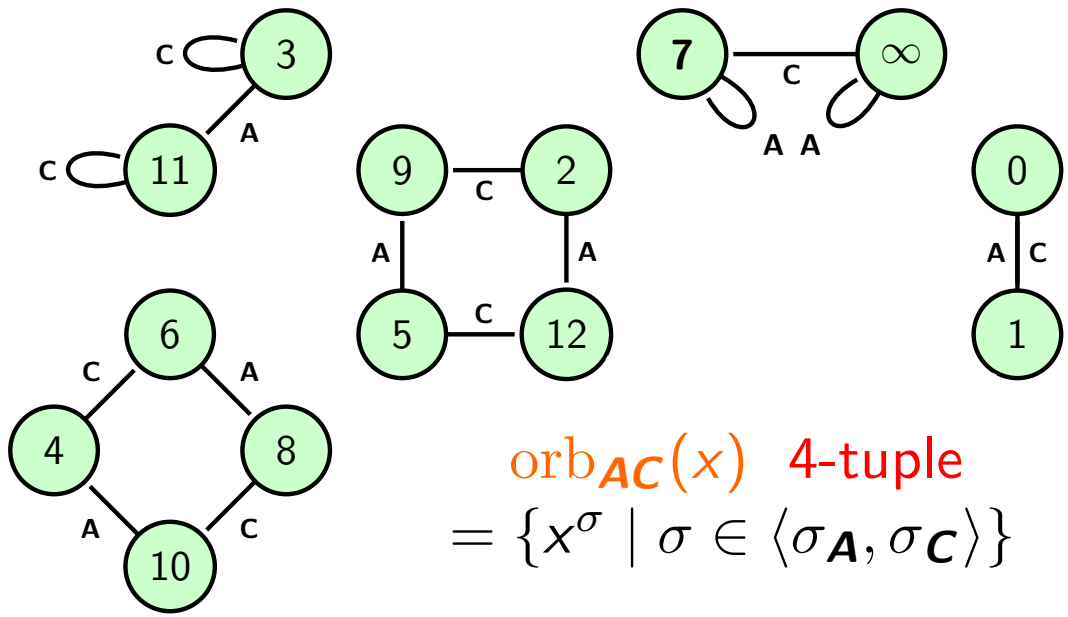
Let $\mathrm{LG}(V_p)$ be a graph whose vertex set is $V_p \subseteq \mathscr{P}(\mathbb{F}_p)$ and edge set is $\{\{x, y\} \mid x = y^\sigma, \sigma \in \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}\}$.

Let

$$\sigma_{\boldsymbol{A}} : x \mapsto 1 - x,$$
$$\sigma_{\boldsymbol{B}} : x \mapsto \frac{1}{x},$$
$$\sigma_{\boldsymbol{C}} : x \mapsto \frac{x-1}{2x-1}$$

be mappings on $\mathscr{P}(\mathbb{F}_p)$.
For $p \equiv 1 \pmod 4$,
$\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}} \rangle = \mathrm{PSL}(2, p)$.

EXAMPLE: $\mathrm{LG}(\mathscr{P}(\mathbb{F}_{13}))$



$\mathrm{orb}_{\boldsymbol{AC}}(x)$ 4-tuple
$= \{x^\sigma \mid \sigma \in \langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{C}} \rangle\}$

Projective lines and graphs $\mathrm{LG}(V_p)$

$\mathscr{P}(\mathbb{F}_p) := \mathbb{F}_p \cup \{\infty\}$: the projective line over the finite field $\mathbb{F}_p$.

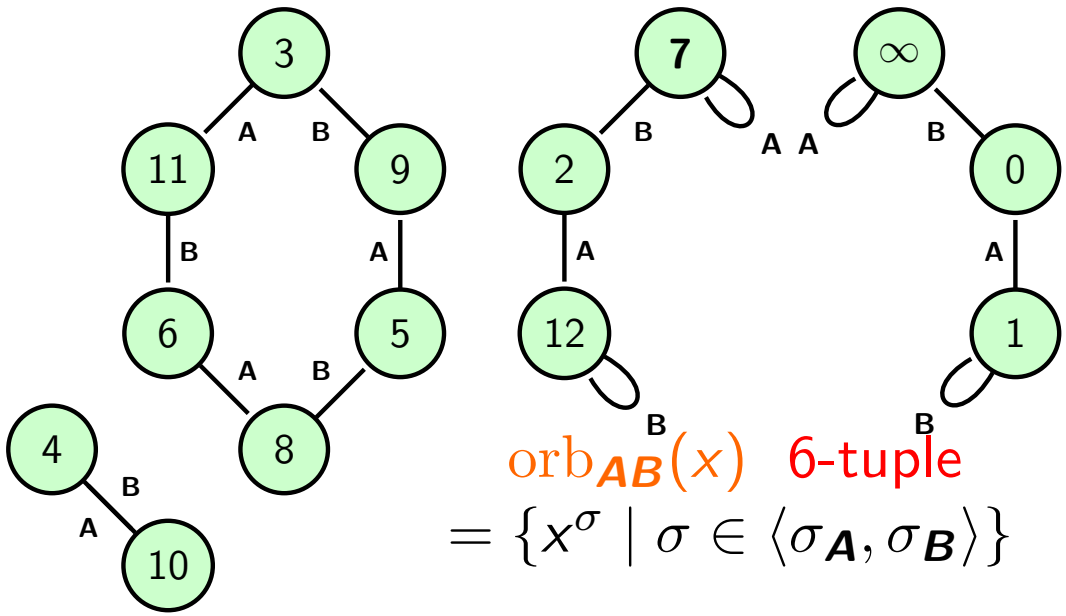
Let $\mathrm{LG}(V_p)$ be a graph whose vertex set is $V_p \subseteq \mathscr{P}(\mathbb{F}_p)$ and edge set is $\{\{x, y\} \mid x = y^\sigma, \sigma \in \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}\}$.

Let

$$\sigma_{\boldsymbol{A}} : x \mapsto 1 - x,$$
$$\sigma_{\boldsymbol{B}} : x \mapsto \frac{1}{x},$$
$$\sigma_{\boldsymbol{C}} : x \mapsto \frac{x-1}{2x-1}$$

be mappings on $\mathscr{P}(\mathbb{F}_p)$.
For $p \equiv 1 \pmod 4$,
$\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}} \rangle = \mathrm{PSL}(2, p)$.

EXAMPLE: $\mathrm{LG}(\mathscr{P}(\mathbb{F}_{13}))$

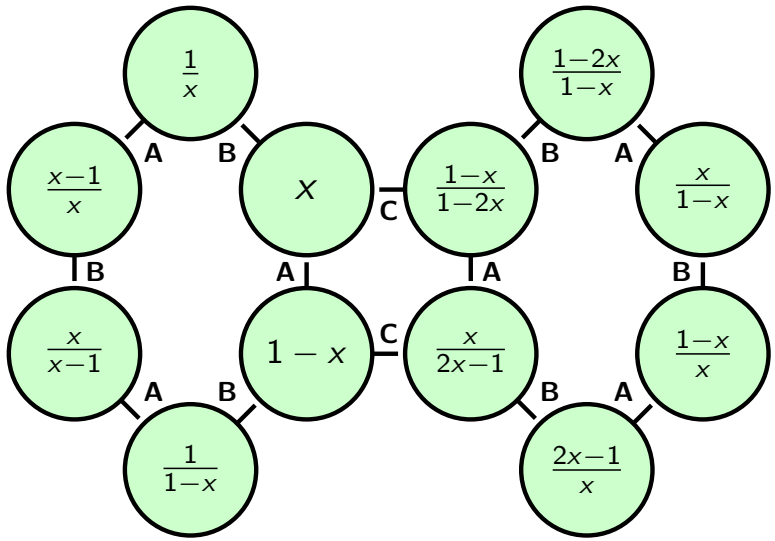


$\mathrm{orb}_{\boldsymbol{AB}}(x)$ 6-tuple
$= \{x^\sigma \mid \sigma \in \langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}} \rangle\}$

Cross-ratio classes and and graphs $\mathrm{CG}(V_p)$

- $\mathrm{orb}_{\boldsymbol{AB}}(x) = \{x, \frac{1}{x}, \frac{x-1}{x}, \frac{x}{x-1}, \frac{1}{1-x}, 1-x\}$ $=: C(x)$, a cross-ratio class.
- $|C(x)| = \begin{cases} 3 & \text{if } x \in C(0) \cup C(2) \\ 2 & \text{if } x \in C(\xi_p) \\ 6 & \text{otherwise} \end{cases}$,

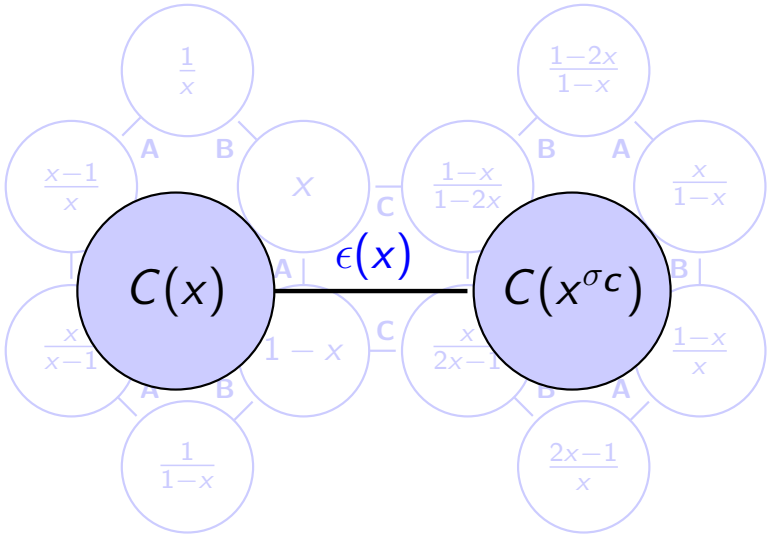
  where ξ_p is a root of $x^2 - x + 1 = 0$.



Cross-ratio classes and and graphs $\mathrm{CG}(V_p)$

- $\mathrm{orb}_{\boldsymbol{AB}}(x) = \{x, \frac{1}{x}, \frac{x-1}{x}, \frac{x}{x-1}, \frac{1}{1-x}, 1-x\}$ $=: C(x)$, a cross-ratio class.
- $|C(x)| = \begin{cases} 3 & \text{if } x \in C(0) \cup C(2) \\ 2 & \text{if } x \in C(\xi_p) \\ 6 & \text{otherwise} \end{cases}$,

  where ξ_p is a root of $x^2 - x + 1 = 0$.



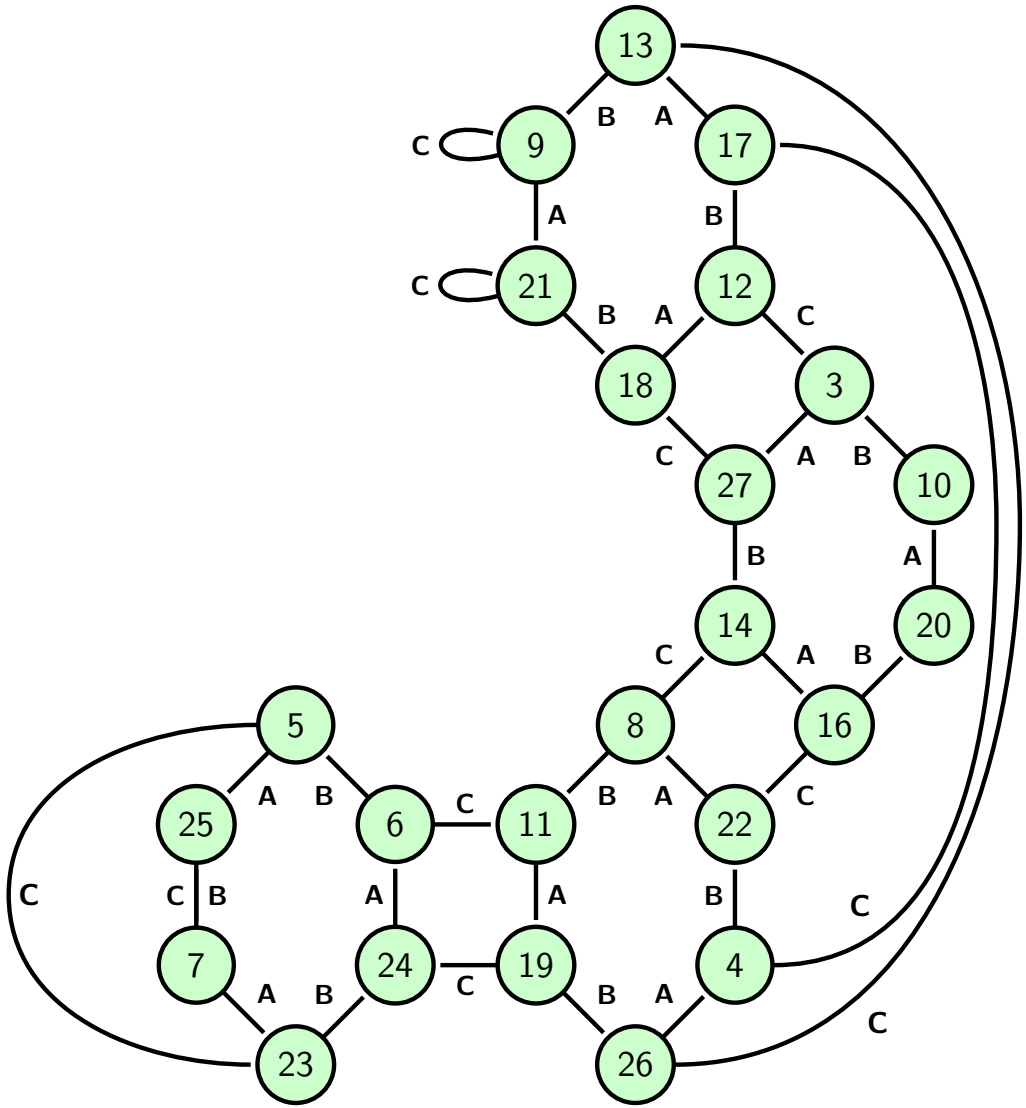
Let $\mathrm{CG}(V_p)$ be a graph with vertex set consisting of cross-ratio classes $\{C(x) \mid x \in V_p \subseteq \mathscr{P}(\mathbb{F}_p)\}$. Each pair of $\boldsymbol{C}$-edges in $\mathrm{LG}(V_p)$ corresponds to an edge in $\mathrm{CG}(V_p)$.

- Our main interest: 1-factors (perfect matchings) of $\mathrm{CG}(\Omega_p)$, where $\Omega_p = \mathscr{P}(\mathbb{F}_p) \setminus (C(0) \cup C(2)) = \mathbb{F}_p \setminus \{0, 1, -1, 2, 2^{-1}\}$.

Base blocks of affine-invariant sSQS($2p$), for $p = 29$

Type II′

$$\{0, 1, 28; 0\},$$



Base blocks of affine-invariant sSQS($2p$), for $p = 29$

Type I′

$$\{0, 1; 9, 21\},$$

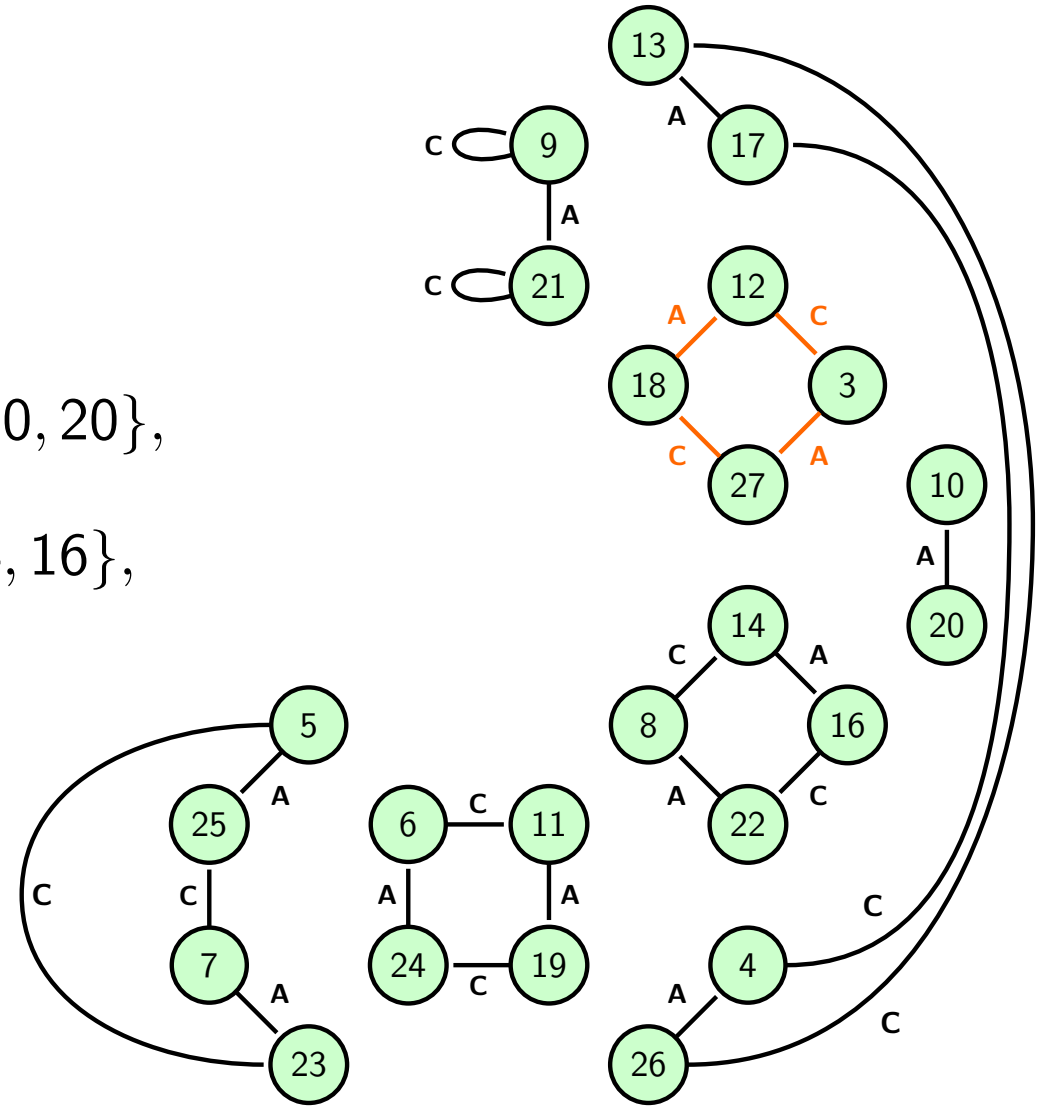
Type I

$$\{0, 1; 13, 17\}, \{0, 1; 12, 18\}, \{0, 1; 10, 20\},$$

$$\{0, 1; 7, 25\}, \{0, 1; 11, 19\}, \{0, 1; 14, 16\},$$

Type II′

$$\{0, 1, 28; 0\},$$



Base blocks of affine-invariant sSQS($2p$), for $p = 29$

Type I′

$$\{0, 1; 9, 21\},$$

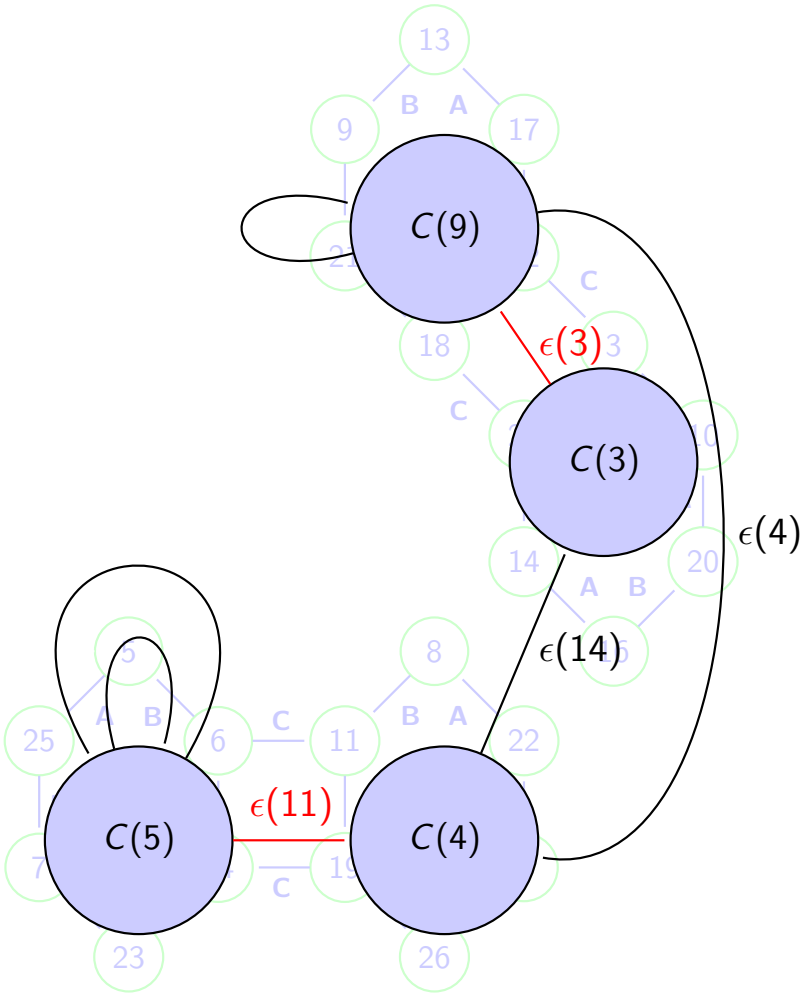
Type I

$$\{0, 1; 13, 17\}, \{0, 1; 12, 18\}, \{0, 1; 10, 20\},$$

$$\{0, 1; 7, 25\}, \{0, 1; 11, 19\}, \{0, 1; 14, 16\},$$

Type II′

$$\{0, 1, 28; 0\},$$



Base blocks of affine-invariant sSQS($2p$), for $p = 29$

Type I′

$\{0, 1; 9, 21\}$,

Type I

$\{0, 1; 13, 17\}$, $\{0, 1; 12, 18\}$, $\{0, 1; 10, 20\}$,

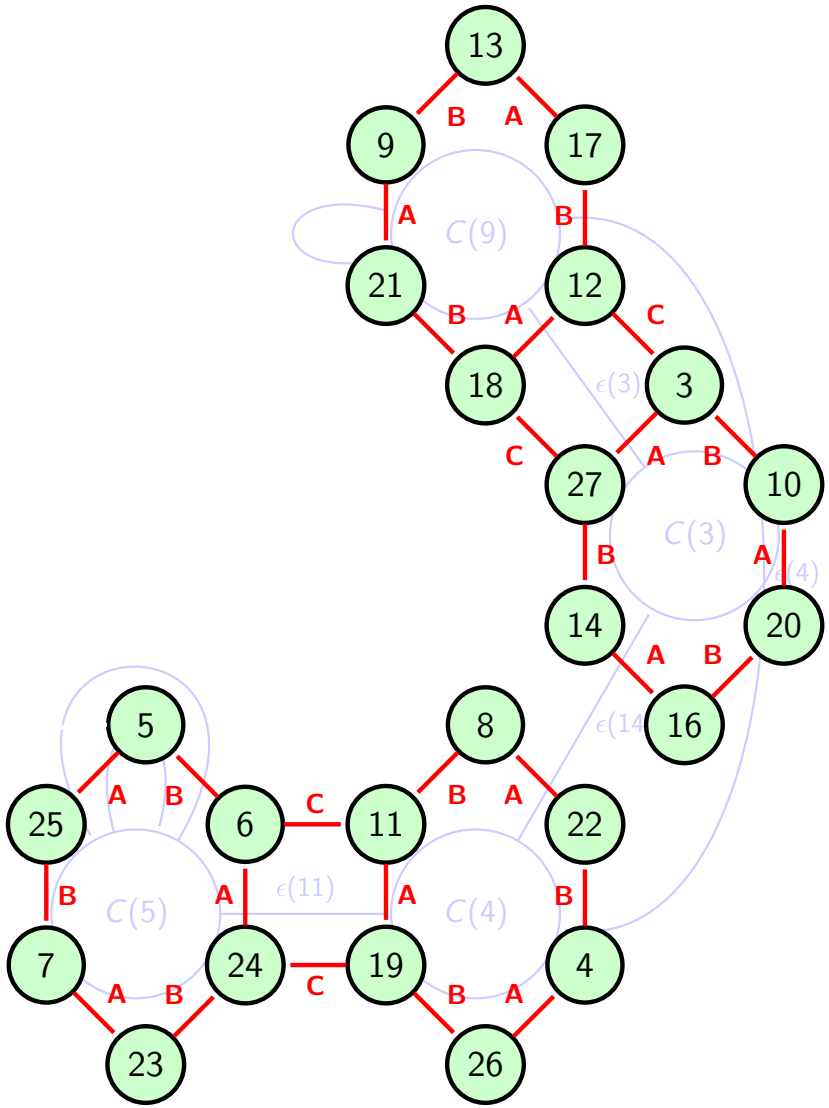
$\{0, 1; 7, 25\}$, $\{0, 1; 11, 19\}$, $\{0, 1; 14, 16\}$,

Type II′

$\{0, 1, 28; 0\}$,

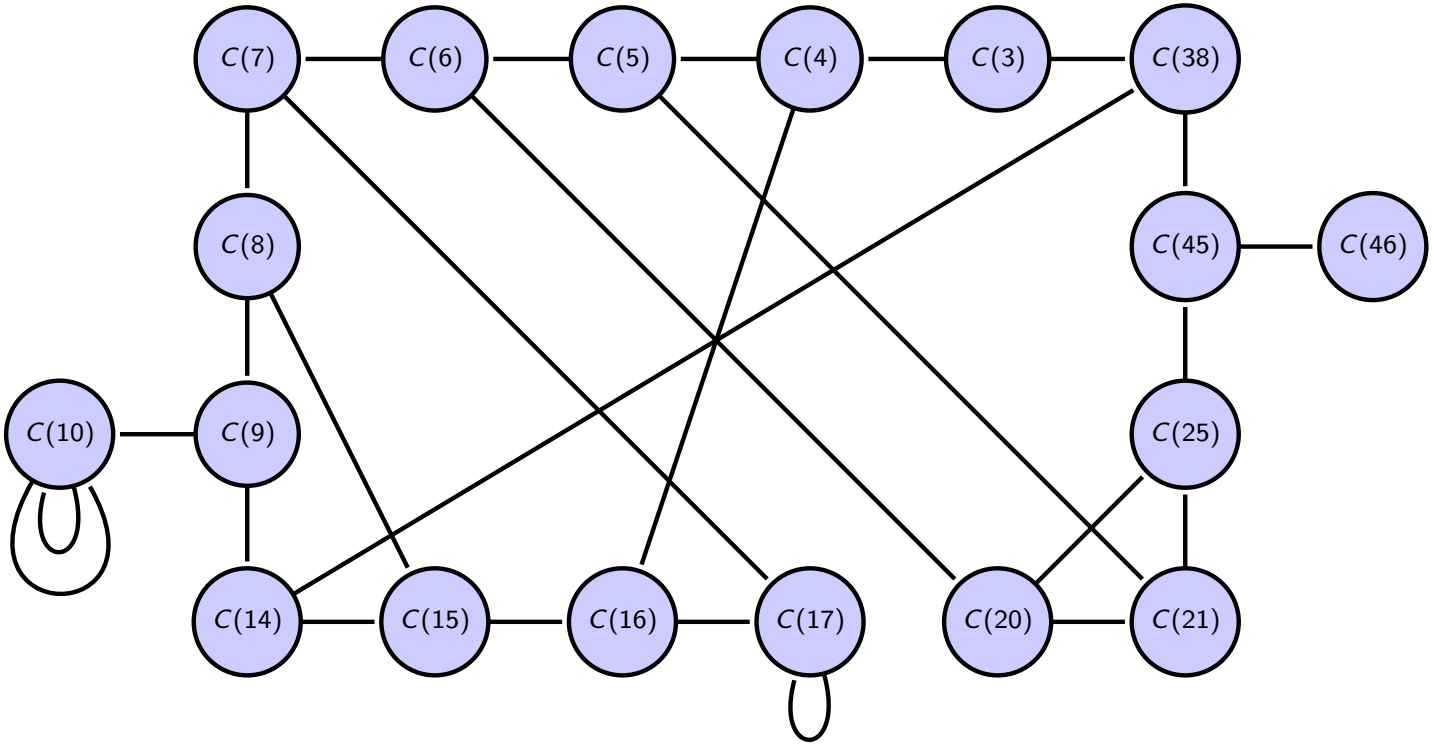
Type III

$\{0, 1, 3, 27\}$, $\{0, 1, 11, 19\}$



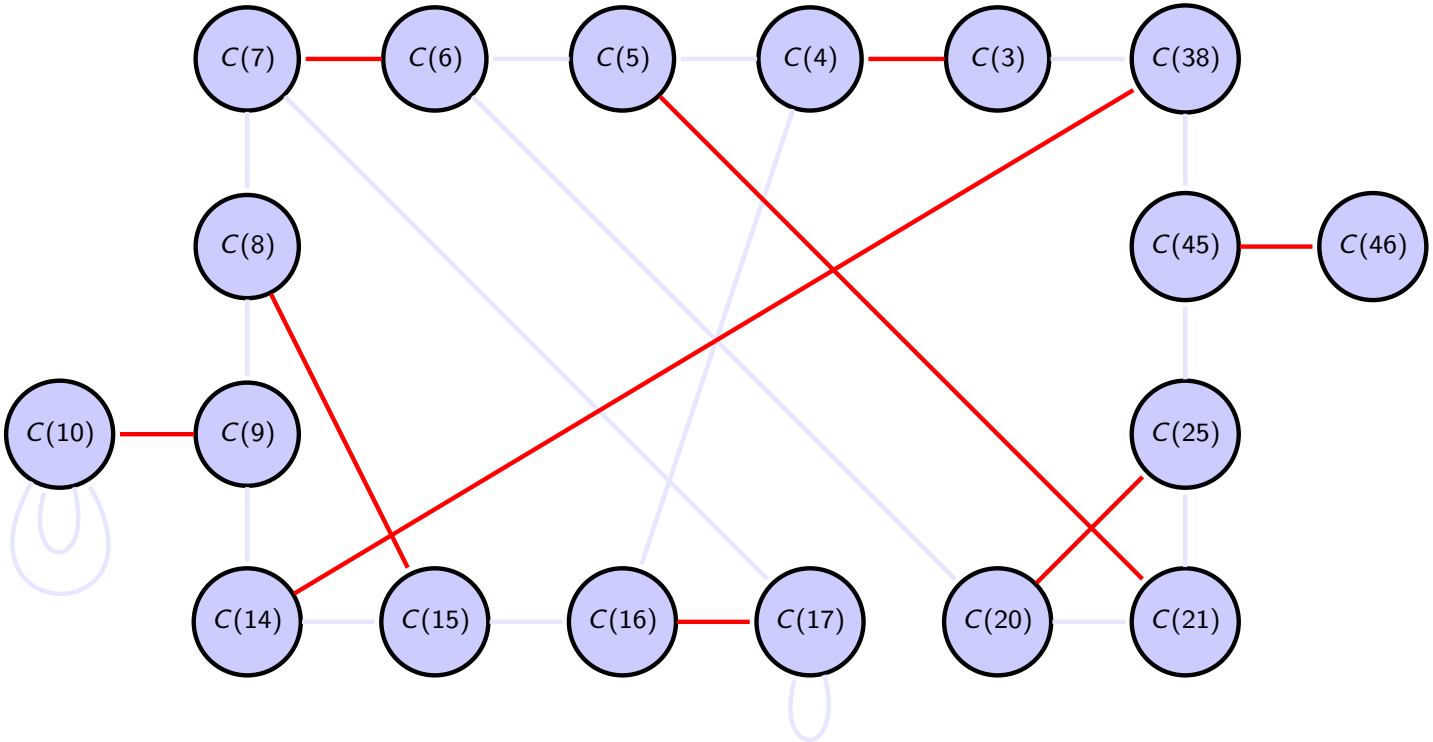
1-factors of $\mathrm{CG}(\Omega_p)$

EXAMPLE: $\mathrm{CG}(\Omega_{109})$



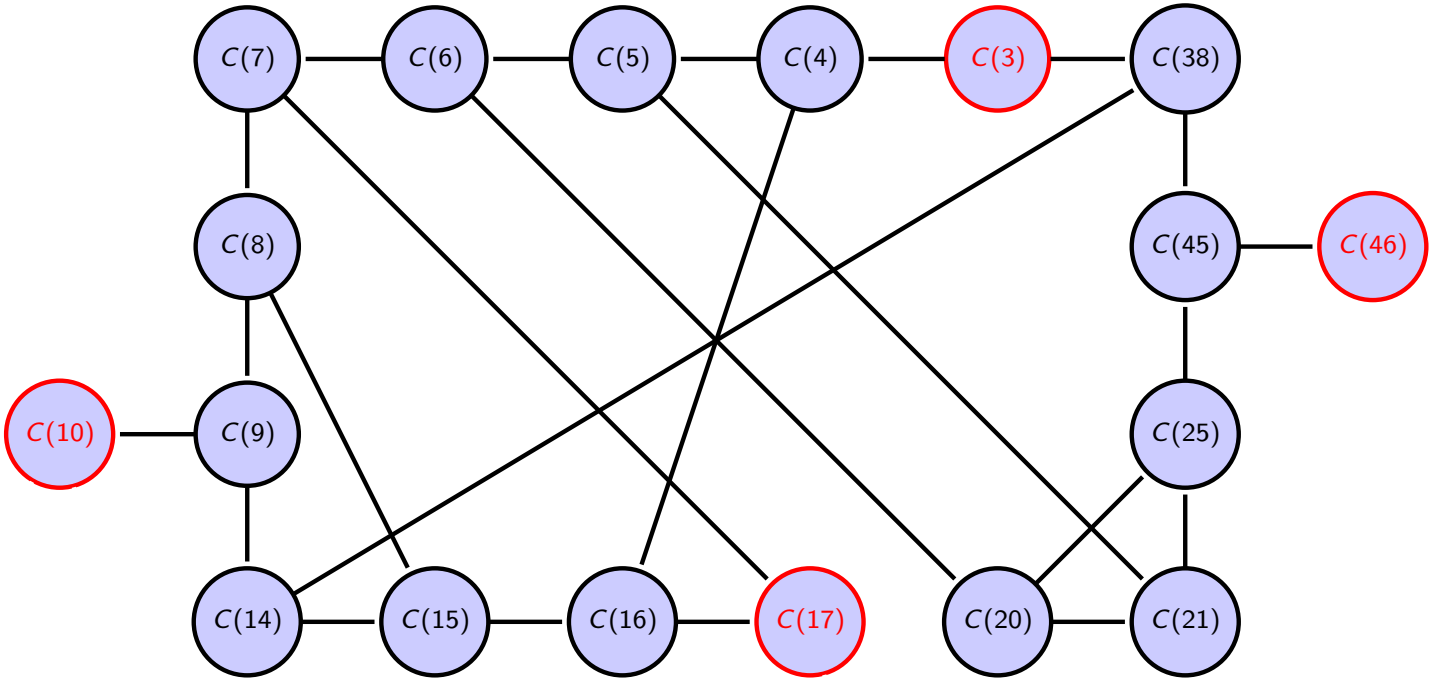
1-factors of $\mathrm{CG}(\Omega_p)$

EXAMPLE: $\mathrm{CG}(\Omega_{109})$

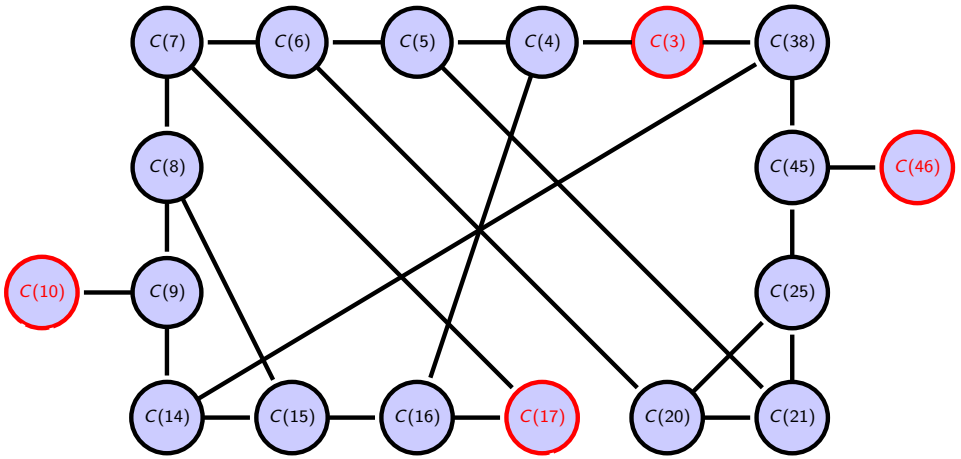


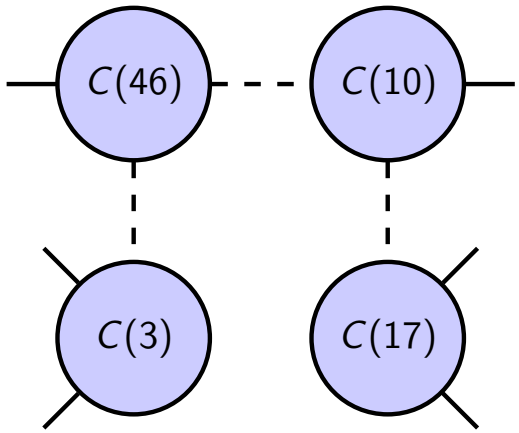
1-factors of $\mathrm{CG}(\Omega_p)$

EXAMPLE: $\mathrm{CG}(\Omega_{109})$



1-factors of $\mathrm{CG}(\Omega_p)$





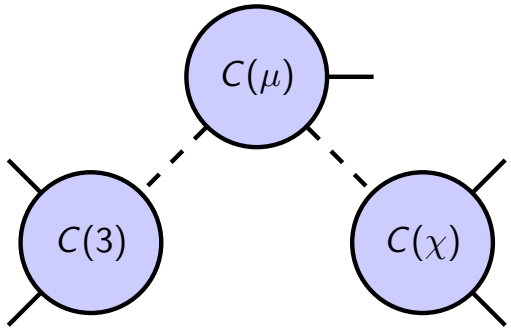
Theorem (Petersen, 1891)

A 2-connected 3-regular graph (multigraph without loops) has a 1-factor.

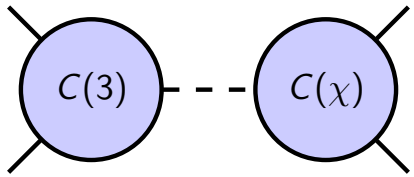
Theorem (Plesník, 1974)

Let G be an $(r-1)$-edge-connected r-regular graph of even order, then, for any $r-1$ edge $e_1, e_2, \ldots, e_{r-1} \in E(G)$, there exists a 1-factor of G excluding $\{e_1, e_2, \ldots, e_{r-1}\}$.

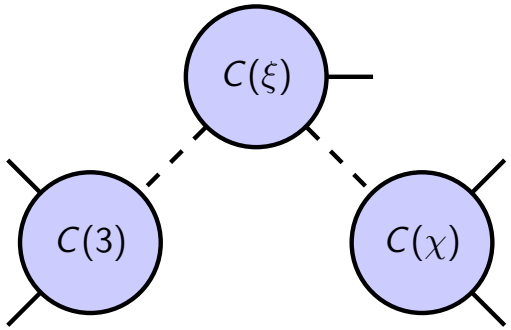
1-factors of $\mathrm{CG}(\Omega_p)$



(a) $p \equiv 29, 41 \pmod{60}$



(b) $p \equiv 5 \pmod{12}$ and $p \not\equiv 29, 41 \pmod{60}$



(c) $p \equiv 1 \pmod{12}$ and $p \not\equiv 1, 49 \pmod{60}$

Corollary

For prime $p \equiv 1, 5 \pmod{12}$ and $p \not\equiv 1, 49 \pmod{60}$, $\mathrm{CG}(\Omega_p)$ has a 1-factor if it is bridgeless.

Theorem (Direct Construction)

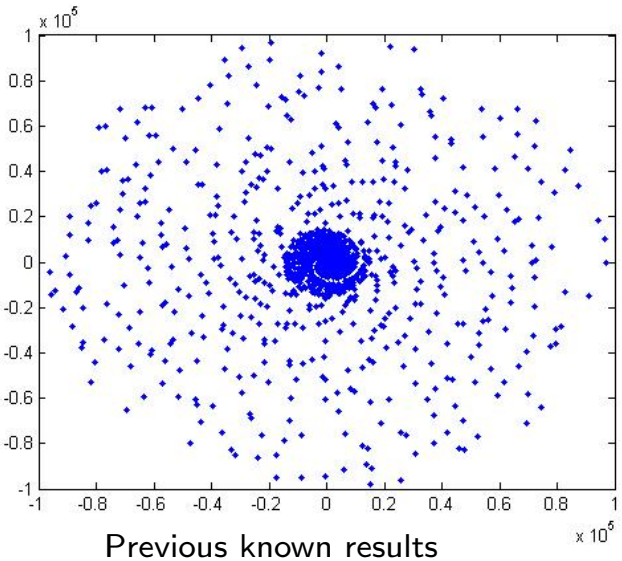
For prime $p \equiv 1, 5 \pmod{12}$ and $p \not\equiv 1, 49 \pmod{60}$, if $\mathrm{CG}(\Omega_p)$ is bridgeless, then an affine-invariant sSQS(2p) exists.

Results by computer search

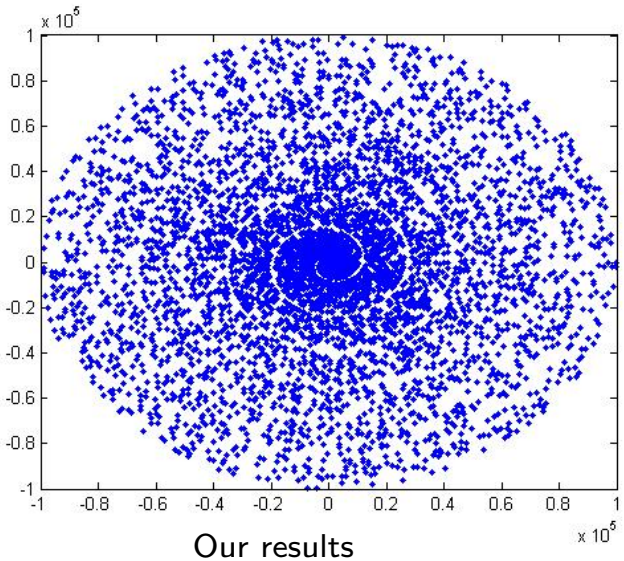
In practice, the best known 1-factor algorithm for 2-connected 3-regular graphs has complexity $O(n \log^2 n)$. (Diks and Stańczyk, 2010)

Theorem (by computer search)

$\mathrm{CG}(\Omega_p)$ *has a 1-factor for all primes* $p < 100,000$ *with* $p \equiv 1, 5 \pmod{12}$.



Previous known results



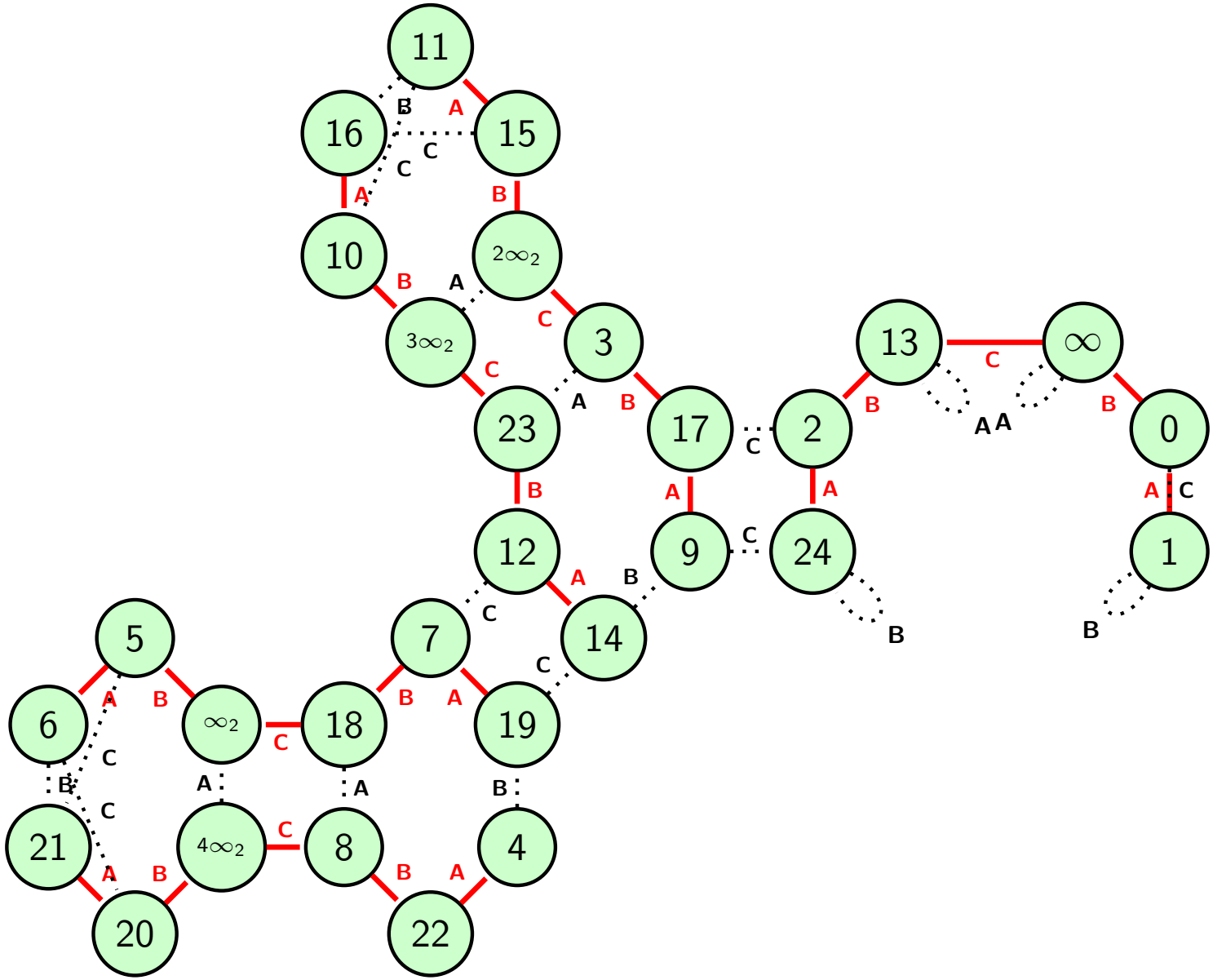
Our results

Existence of sSQS($2p$), for primes $p < 100,000$.

$(p \cos p, p \sin p) \in \mathbb{R}^2$.

L: Previous known results
R: Our results

Subgraphs isomorphic to $\mathrm{LG}^*(\mathscr{P}(\mathbb{F}_5))$ embedding in $\mathrm{LG}(\mathscr{P}(\mathbb{Z}_{25}))$.



Recursive Constructions

Theorem (Recursive Construction)

Let $m > 2$ be a positive integer,

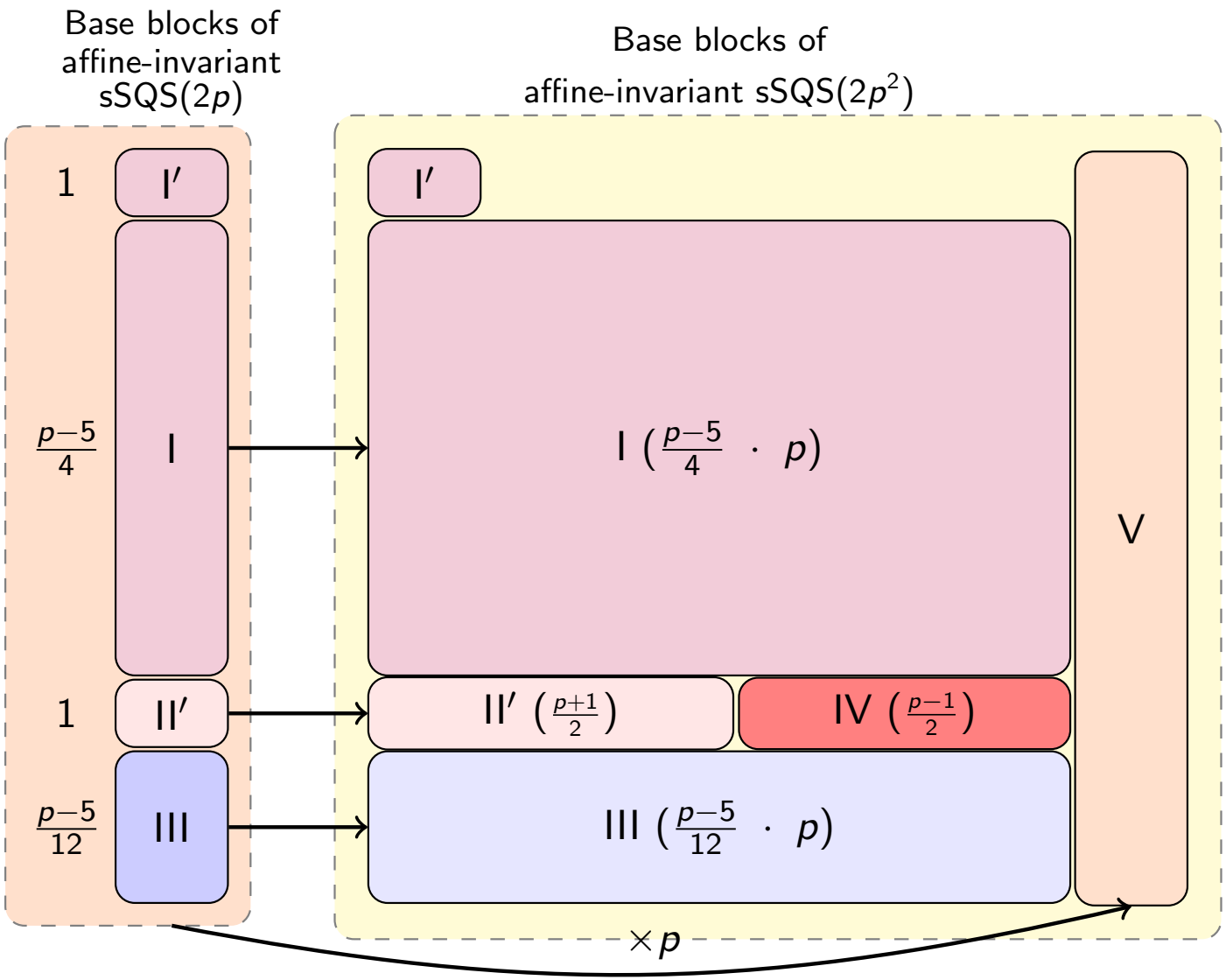
- *for $p \equiv 5 \pmod{12}$, if the affine-invariant sSQS($2p$) exists,*
- *for $p \equiv 1 \pmod{12}$, if*
  - (i) *there exist an affine-invariant sSQS($2p$) and an sSQS($2p^{m-1}$) by our constructions, and,*
  - (ii) *the graph $\mathrm{CG}(\Omega_p + p\mathbb{Z}_{p^{m-1}})$ has a 1-factor,*

then an affine-invariant sSQS($2p^m$) exists.

Theorem (A necessary condition)

An affine-invariant sSQS($2n$) exists for an odd number n, only if every prime divisor p of n satisfies $p \equiv 1, 5 \pmod{12}$.

Main ideas of recursive construction for $p \equiv 5 \pmod{12}$



affine-invariant sSQS($2p$)

$\downarrow$

affine-invariant sSQS($2p^2$)

$\downarrow$

$\vdots$

$\downarrow$

affine-invariant sSQS($2p^m$)

Outline

λ-fold SQS's

Definition

A pair $(V, \mathcal{B})$ is called a λ-fold SQS, if

- V is a finite set of v elements (points).
- $\mathcal{B} \subseteq \binom{V}{4}$ is a collection of quadruples (4-subsets, blocks) of V.
- Each triple (3-subset) of V occurs in exactly λ quadruple in $\mathcal{B}$.

λ-fold SQS's

Definition

A pair $(V, \mathcal{B})$ is called a λ-fold SQS, if

- V is a finite set of v elements (points).
- $\mathcal{B} \subseteq \binom{V}{4}$ is a collection of quadruples (4-subsets, blocks) of V.
- Each triple (3-subset) of V occurs in exactly λ quadruple in $\mathcal{B}$.

A necessary condition for 2-fold SQS(v): $v \equiv 1, 5 \pmod{12}$.

Theorem

- *For a prime $p \equiv 1, 5 \pmod{12}$, if $\mathrm{CG}(\Omega_p)$ has a 1-factor, then an affine-invariant 2-fold SQS(p) exists.*
- *For a prime $p \equiv 5 \pmod{12}$, if $\mathrm{CG}(\Omega_p)$ has a 1-factor, then an affine-invariant simple 2-fold SQS(p) exists.*

Affine-invariant simple two-fold SQS(p)

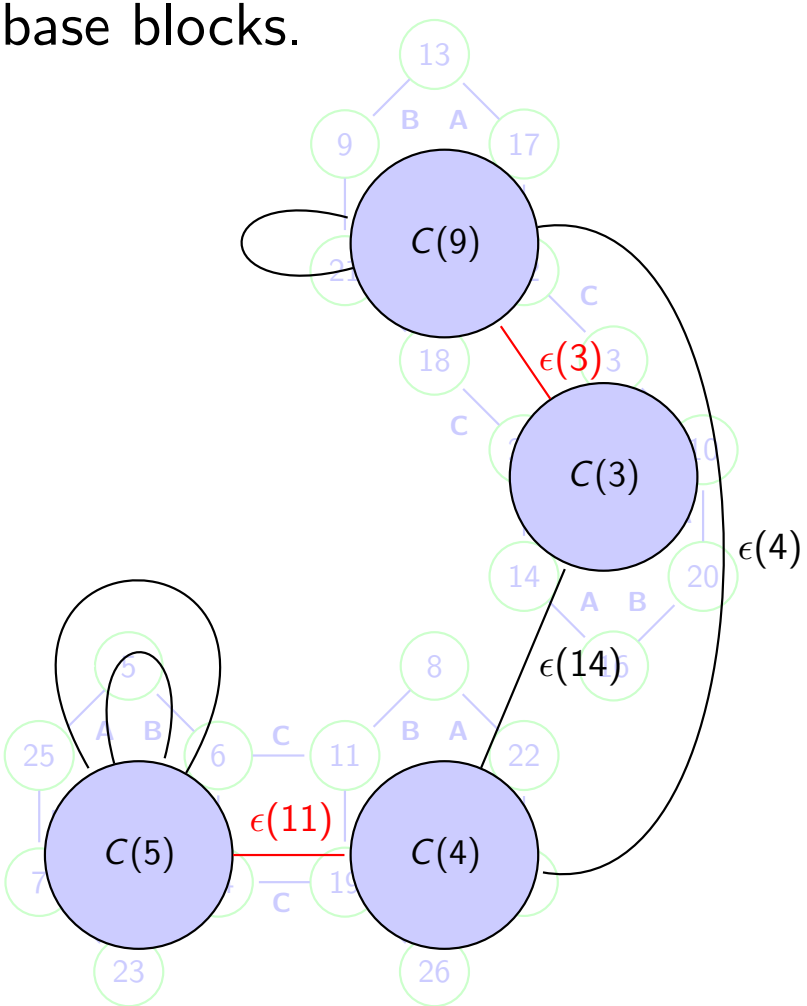
All (pure) triples $\{0, 1, x\}$, for $x \in \mathbb{F}_p \setminus \{0, 1\}$.

$B_0 = \{0, 1, -1, 2\}$. $\mathrm{orb}(B_0)$ contains
$\{0, 1, -1, 2\}$, $\{0, -1, 1, -2\}$,
$\{0, 2^{-1}, -2^{-1}, 1\}$, $\{1, 2^{-1}, \frac{3}{2}, 0\}$,
$\{2, 1, 3, 0\}$, $\{\frac{2}{3}, \frac{1}{3}, 1, 0\}$.

$$C(2) = \{-1, 2, 2^{-1}\} \quad \times 2$$

$$C(3) = \{3, \tfrac{1}{3}, \tfrac{2}{3}, \tfrac{3}{2}, -2^{-1}, -2\}$$

A $(1, 2)$-factor (the complement of 1-factor) of $\mathrm{CG}(\Omega_p)$ gives all the other base blocks.



Affine-invariant simple two-fold SQS(p^m)

($p \equiv 5 \pmod{12}$) 1-factor of $\mathrm{CG}(\Omega_p) \Longrightarrow$ 1-factor of $\mathrm{CG}(\Omega_{p^2})$.

Theorem (Recursive Construction)

An affine-invariant simple 2-fold SQS(p^m) exists for all primes $p < 100,000$ with $p \equiv 5 \pmod{12}$ and $m \in \mathbb{Z}_{>0}$.

- $\{0, 1, x\}$, $x \in \mathbb{Z}_p \setminus \{0, 1\} + p\mathbb{Z}_p$. ($p\mathbb{Z}_p = p\mathbb{Z}/p^2\mathbb{Z}$.)
  $B_0 = \{0, 1, -1, 2\}$;
  Complement of a 1-factor of $\mathrm{CG}(\Omega_{p^2})$ (a (1,2)-factor).
- $\{0, 1, x\}$, $x \in (\{0, 1\} + p\mathbb{Z}_p) \setminus \{0, 1\}$.
- $\{0, p, x'\}$, $x' \in \mathbb{Z}_{p^2}^{\times}$.
  $B_s = \{0, p, s, s + 2^{-1}p\}$, for $s = g^0, g^1, \ldots, g^{\frac{p-3}{2}}$, $\langle g \rangle = \mathbb{Z}_{p^2}^{\times}$.
- $\{0, p, x'\}$, $x' \in p\mathbb{Z}_p \setminus \{0, p\}$.
  $p\times$ all base blocks of two-fold SQS(p).

Affine-invariant simple two-fold SQS(p^m)

$B_s = \{0, p, s, s + 2^{-1}p\}$, for $s \in S = \{g^0, g^1, \ldots, g^{\frac{p-3}{2}}\}$, $\langle g \rangle = \mathbb{Z}_{p^2}^{\times}$.
$H_{p-1}^0 := \langle g^{p-1} \rangle < \mathbb{Z}_{p^2}^{\times}$.
$H_{p-1}^a := g^a H_{p-1}^0 = \{g^{a+u(p-1)} \mid u = 0, 1, \ldots, p-1\}$. $H_{p-1}^a + p = H_{p-1}^a$.

Lemma

$\bigcup_{s \in S} \mathrm{orb}(B_s)$ contains triples $\{0, p, x\}$ for all $x \in \mathbb{Z}_{p^2}^{\times}$ exactly twice.

$$g^{u(p-1)} B_s = \{0, pg^{u(p-1)}, g^{a+u(p-1)}, g^{a+u(p-1)} + 2^{-1} pg^{u(p-1)}\}$$
$$= \{0, p, g^{a+u(p-1)}, g^{a+u(p-1)} + 2^{-1}p\}.$$

$$g^{u(p-1)} \times (g^{\frac{p-1}{2}} B_s + p) = g^{u(p-1)} \times \{p, 0, p + g^{a+\frac{p-1}{2}}, g^{a+\frac{p-1}{2}} + 2^{-1}p\}$$
$$= \{p, 0, p + g^{a+\frac{p-1}{2}+u(p-1)}, g^{a+\frac{p-1}{2}+u(p-1)} + 2^{-1}p\}$$

Affine-invariant simple two-fold SQS(p^m)

$B_s = \{0, p, s, s + 2^{-1}p\}$, for $s \in S = \{g^0, g^1, \ldots, g^{\frac{p-3}{2}}\}$, $\langle g \rangle = \mathbb{Z}_{p^2}^{\times}$.
$H_{p-1}^0 := \langle g^{p-1} \rangle < \mathbb{Z}_{p^2}^{\times}$.
$H_{p-1}^a := g^a H_{p-1}^0 = \{g^{a+u(p-1)} \mid u = 0, 1, \ldots, p-1\}$. $H_{p-1}^a + p = H_{p-1}^a$.

Lemma

$\bigcup_{s \in S} \mathrm{orb}(B_s)$ contains triples $\{0, p, x\}$ for all $x \in \mathbb{Z}_{p^2}^{\times}$ exactly twice.

$$g^{u(p-1)} B_s = \{0, pg^{u(p-1)}, g^{a+u(p-1)}, g^{a+u(p-1)} + 2^{-1}pg^{u(p-1)}\}$$
$$= \{0, p, g^{a+u(p-1)}, g^{a+u(p-1)} + 2^{-1}p\}.$$

$$g^{u(p-1)} \times (g^{\frac{p-1}{2}} B_s + p) = g^{u(p-1)} \times \{p, 0, p + g^{a+\frac{p-1}{2}}, g^{a+\frac{p-1}{2}} + 2^{-1}p\}$$
$$= \{p, 0, p + g^{a+\frac{p-1}{2}+u(p-1)}, g^{a+\frac{p-1}{2}+u(p-1)} + 2^{-1}p\}$$

$$x \in \bigcup_{a=0}^{\frac{p-3}{2}} \left(H_{p-1}^a \cup H_{p-1}^{a+\frac{p-1}{2}} \right) = \bigcup_{a=0}^{p-2} H_{p-1}^a = \mathbb{Z}_{p^2}^{\times}$$

Affine-invariant simple two-fold SQS(p^m)

$B_s = \{0, p, s, s + 2^{-1}p\}$, for $s \in S = \{g^0, g^1, \ldots, g^{\frac{p-3}{2}}\}$, $\langle g \rangle = \mathbb{Z}_{p^2}^{\times}$.

Lemma

$\bigcup_{s \in S} \mathrm{orb}(B_s)$ contains triples $\{0, 1, x\}$ for all $x \in (\{0, 1\} + p\mathbb{Z}_p\}) \setminus \{0, 1\}$ exactly twice.

$$
\begin{aligned}
B_s \times s^{-1} &= \{0, s^{-1}p, 1, 1 + (2s)^{-1}p\}, \\
(B_s - p) \times (s - p)^{-1} &= \{-s^{-1}p, 0, 1, 1 - (2s)^{-1}p\}, \\
B_s \times (-s^{-1}) + 1 &= \{1, 1 - s^{-1}p, 0, -(2s)^{-1}p\}, \\
(B_s - p) \times (-(s - p)^{-1}) + 1 &= \{1 + s^{-1}p, 1, 0, (2s)^{-1}p\}.
\end{aligned}
$$

$$
\begin{aligned}
\left\{ \pm s^{-1} \pmod{p} \mid s \in \left\{g^0, g^1, \ldots, g^{\frac{p-3}{2}}\right\} \right\} &= \mathbb{Z}_p^{\times} \\
\left\{ \pm s^{-1}p \pmod{p^2} \mid s \in \left\{g^0, g^1, \ldots, g^{\frac{p-3}{2}}\right\} \right\} &= p\mathbb{Z}_p \setminus \{0\}
\end{aligned}
$$

Future work

- sSQS($2p^2$), $p \equiv 7, 11 \pmod{12}$?
- Optimal OOCs (packing designs)?
- Other affine designs with larger block size ($k \geq 5$) or 3PDs.
- Eigenvalues and 1-factors of 3-uniform regular hypergraphs.

Theorem (Brouwer-Haemers, 2005)

A connected k-regular graph on v vertices with adjacency eigenvalues $k = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_v$ and v even which satisfies

$$\lambda_3 \leq \begin{cases} k - 1 + \frac{3}{k+1} & \text{if } k \text{ even} \\ k - 1 + \frac{3}{k+2} & \text{if } k \text{ odd} \end{cases}$$

has a 1-factor.

Future work

- sSQS($2p^2$), $p \equiv 7, 11 \pmod{12}$?
- Optimal OOCs (packing designs)?
- Other affine designs with larger block size ($k \geq 5$) or 3PDs.
- Eigenvalues and 1-factors of 3-uniform regular hypergraphs.

Theorem (Brouwer-Haemers, 2005)

A connected k-regular graph on v vertices with adjacency eigenvalues $k = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_v$ and v even which satisfies

$$\lambda_3 \leq \begin{cases} k - 1 + \frac{3}{k+1} & \text{if } k \text{ even} \\ k - 1 + \frac{3}{k+2} & \text{if } k \text{ odd} \end{cases}$$

has a 1-factor.

Thank you very much for your attention!