A combinatorial proof for the largest power of 2 in the number of involutions

Jang Soo Kim

KAIST

The 60th Séminaire Lotharingien de Combinatoire
April 1st, 2008

Definition of $\tau_p(n)$

- $\mathfrak{S}_n$: the set of permutations of $[n] = \{1, 2, \ldots, n\}$
- A : a finitely generated group
- $h_n(A) :=$ the number of homomorphisms from A to $\mathfrak{S}_n$
- $m_A(d) :=$ the number of subgroups of index d in A

Wohlfahrt (1977)

$$\sum_{n \geq 0} \frac{h_n(A)}{n!} x^n = \exp\left(\sum_{d \geq 1} \frac{m_A(d)}{d} x^d \right)$$

- p : a prime number
- $\mathbb{Z}/p\mathbb{Z}$: the cyclic group of order p
- $\tau_p(n) := h_n(\mathbb{Z}/p\mathbb{Z})$ is the number of $\pi \in \mathfrak{S}_n$ satisfying $\pi^p = 1$

Then

$$\sum_{n \geq 0} \frac{\tau_p(n)}{n!} x^n = \exp\left(x + \frac{x^p}{p} \right)$$

Some results for $\mathrm{ord}_p(\tau_p(n))$

- $\mathrm{ord}_p(n) := \max\{k : p^k | n\}$
- $\mathrm{ord}_3(72) = \mathrm{ord}_3(2^3 \cdot 3^2) = 2$

Chowla, Herstein and Moore (1952)

$$\mathrm{ord}_2(\tau_2(n)) \geq \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor$$

Grady and Newman (1994)

$$\mathrm{ord}_p(\tau_p(n)) \geq \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor$$

Ochiai (1999) found $\mathrm{ord}_p(\tau_p(n))$ for all primes $p \leq 23$. In particular, if $p = 2$ then Ochiai's result is the following:
Let $n \equiv r \mod 4$ with $r = 0, 1, 2, 3$. Then

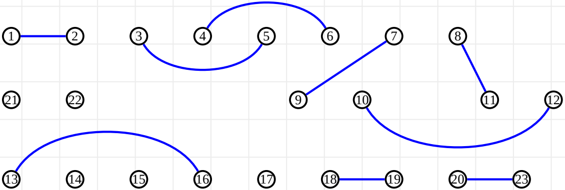
$$\mathrm{ord}_2(\tau_2(n)) = \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor + \delta_{r,3}$$

Case $p = 2$: involutions

- $\tau_2(n)$ = the number of $\pi \in \mathfrak{S}_n$ with $\pi^2 = 1$, which is called an involution.
- $\mathcal{I}_n :=$ the set of involutions in $\mathfrak{S}_n$
- $t_n := |\mathcal{I}_n| = \tau_2(n)$
- $\pi \in \mathcal{I}_n \leftrightarrow$ an incomplete matching on n vertices

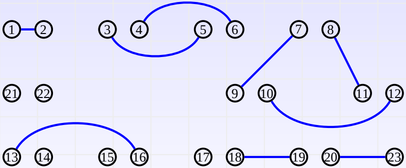
Example

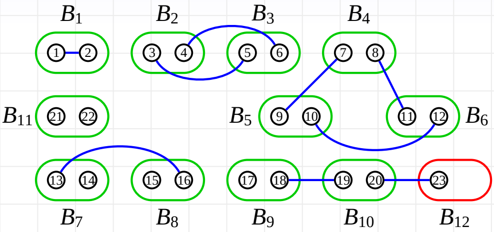
$\pi = (1\,2)(3\,5)(4\,6)(7\,9)(8\,11)(10\,12)(13\,16)(18\,19)(20\,23)$ in cycle notation



We call each connected component a fixed point or an edge.

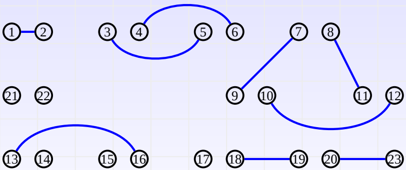
$\phi(\pi)$: the block graph

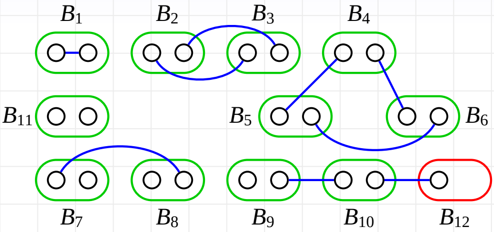




- Normal blocks contain two vertices.
- The special block contains only one vertex. (exists only if n is odd)

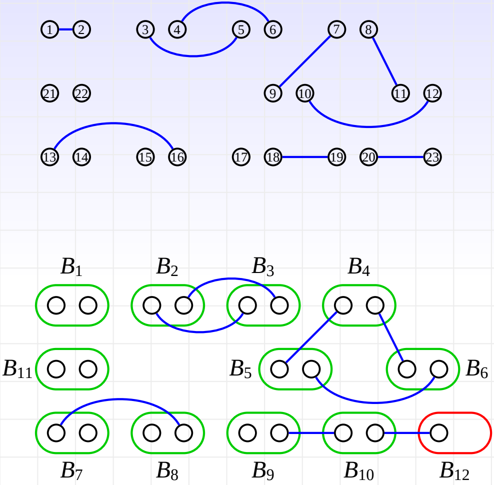
$\phi(\pi)$: the block graph





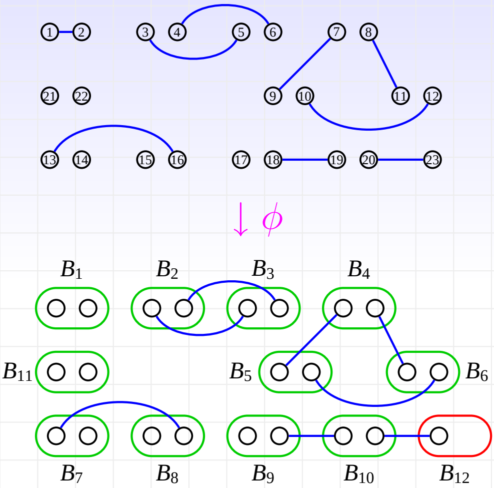
- Normal blocks contain two vertices.
- The special block contains only one vertex. (exists only if n is odd)

$\phi(\pi)$: the block graph



- Normal blocks contain two vertices.
- The special block contains only one vertex. (exists only if n is odd)

$\phi(\pi)$: the block graph



- Normal blocks contain two vertices.
- The special block contains only one vertex. (exists only if n is odd)

Dividing $\mathcal{I}_n$ into $\phi^{-1}(G)$

$\mathfrak{G}_n :=$ the set of block graphs $\phi(\pi)$ for $\pi \in \mathcal{I}_n$, i.e., the image $\phi(\mathcal{I}_n)$
$\phi^{-1}(G) := \{\pi : \phi(\pi) = G\}$

$$\mathcal{I}_n = \bigcup_{G \in \mathfrak{G}_n} \phi^{-1}(G)$$

$$t_n = \sum_{G \in \mathfrak{G}_n} |\phi^{-1}(G)|$$

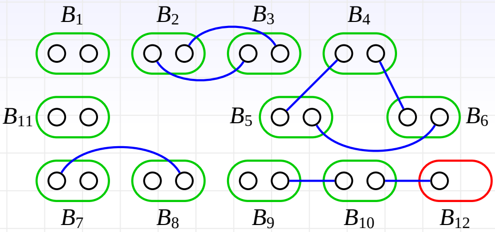
- How to find $|\phi^{-1}(G)|$ for $G \in \mathfrak{G}_n$?
- Each $\pi \in \phi^{-1}(G)$ can be constructed by
  - labeling vertices with $2i-1$ and $2i$ in the normal block B_i of G,
  - adding an edge between the vertices in isolated normal blocks.

Lemma

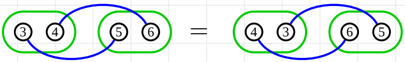
Let $G \in \mathfrak{G}_n$ and $m(G)$ denote the number of 2-block-cycles in G.

$$|\phi^{-1}(G)| = 2^{\lfloor \frac{n}{2} \rfloor - m(G)}$$

Proof.



- There are two ways to label vertices (or add an edge) in a normal block.
- In this counting, a 2-block-cycle doubles the number of $\pi \in \phi^{-1}(G)$.



Deriving a formula for t_n

$g_n :=$ the number of $G \in \mathfrak{G}_n$ without 2-block-cycles
The number of $G \in \mathfrak{G}_n$ with exactly i 2-block-cycles is equal to

$$\binom{\lfloor \frac{n}{2} \rfloor}{2i} (2i)!! g_{n-4i}$$

where $m!!$ denotes the product of all positive odd integers at most m.
Let $n = 4k + r$ for $0 \leq r \leq 3$.

$$\begin{aligned} t_n &= \sum_{G \in \mathfrak{G}_n} |\phi^{-1}(G)| = \sum_{G \in \mathfrak{G}_n} 2^{\lfloor \frac{n}{2} \rfloor - m(G)} \\ &= \sum_{i=0}^{\lfloor \frac{n}{4} \rfloor} 2^{\lfloor \frac{n}{2} \rfloor - i} \binom{\lfloor \frac{n}{2} \rfloor}{2i} (2i)!! g_{n-4i} \\ &= 2^{\lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{4} \rfloor} \sum_{i=0}^{k} 2^i \binom{k}{i} \frac{(2k + \lfloor \frac{r}{2} \rfloor)!!}{(2i + \lfloor \frac{r}{2} \rfloor)!!} g_{4i+r} \end{aligned}$$

Finding $\mathrm{ord}_2(t_n)$

Theorem

Let $n = 4k + r$ *for* $0 \le r \le 3$. *Then*

$$t_n = 2^{\lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{4} \rfloor} \sum_{i=0}^{k} 2^i \binom{k}{i} \frac{(2k + \lfloor \frac{r}{2} \rfloor)!!}{(2i + \lfloor \frac{r}{2} \rfloor)!!} g_{4i+r}$$

where g_n *denotes the number of* $G \in \mathfrak{G}_n$ *without 2-block-cycles.*

$$g_{2n+1} = g_{2n} + n g_{2n-1}$$

n	0	1	2	3	4	5	6	7
g_n	1	1	1	2	2	6	8	26

For all $i \neq 0$ and $r = 0, 1, 2, 3$,

$$\mathrm{ord}_2 \left(2^0 \binom{k}{0} \frac{(2k + \lfloor \frac{r}{2} \rfloor)!!}{(\lfloor \frac{r}{2} \rfloor)!!} g_r \right) < \mathrm{ord}_2 \left(2^i \binom{k}{i} \frac{(2k + \lfloor \frac{r}{2} \rfloor)!!}{(2i + \lfloor \frac{r}{2} \rfloor)!!} g_{4i+r} \right)$$

Thus

$$\mathrm{ord}_2(t_n) = \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor + \delta_{r,3}$$

Weights on involutions

Let $\pi \in \mathcal{I}_n$, an incomplete matching.
$\mathrm{fix}(\pi) :=$ the number of fixed points in π
$\mathrm{edge}(\pi) :=$ the number of edges in π
$\mathrm{wt}(\pi) := x^{\mathrm{fix}(\pi)} y^{\mathrm{edge}(\pi)}$

$$t_n(x,y) := \sum_{\pi \in \mathcal{I}_n} \mathrm{wt}(\pi)$$

Note that $t_n(x,-1)$ is the Hermite polynomial.

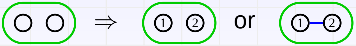
$$t_n(x,y) = \sum_{\pi \in \mathcal{I}_n} \mathrm{wt}(\pi) = \sum_{G \in \mathfrak{G}_n} \sum_{\pi \in \phi^{-1}(G)} \mathrm{wt}(\pi)$$

We want to define $\mathrm{wt}(G)$ satisfying

$$\sum_{\pi \in \phi^{-1}(G)} \mathrm{wt}(\pi) = |\phi^{-1}(G)| \mathrm{wt}(G)$$

Defining $\mathrm{wt}(G)$ satisfying $\mathrm{wt}(G) = \frac{1}{|\phi^{-1}(G)|}\sum_{\pi\in\phi^{-1}(G)} \mathrm{wt}(\pi)$

Recall ▸ the map ϕ and $\mathrm{wt}(\pi) = x^{\mathrm{fix}(\pi)}y^{\mathrm{edge}(\pi)}$.
All edges and the fixed points remain the same except those in isolated normal blocks.



Put weight $\frac{x^2+y}{2}$ on each isolated normal block.

$$\mathrm{wt}(G) := \left(\frac{x^2+y}{2}\right)^{\mathrm{inb(G)}} x^{\mathrm{fix(G')}} y^{\mathrm{edge(G')}}$$

Here G' denotes the block graph obtained from G by removing the isolated normal blocks.

$$\mathrm{wt}(G) = \frac{1}{|\phi^{-1}(G)|}\sum_{\pi\in\phi^{-1}(G)} \mathrm{wt}(\pi)$$

Note that $\mathrm{wt}(G)$ is an integer if $(x,y) = (1,1)$ or $(1,-1)$.

The weighted sum of involutions, $t_n(x, y)$

$$\sum_{\pi \in \phi^{-1}(G)} \mathrm{wt}(\pi) = |\phi^{-1}(G)| \mathrm{wt}(G) = 2^{\lfloor \frac{n}{2} \rfloor - m(G)} \mathrm{wt}(G)$$

$g_n(x, y) :=$ the weighted sum of $G \in \mathfrak{G}_n$ without 2-block-cycles

The weighted sum of $G \in \mathfrak{G}_n$ with exactly i 2-block-cycles is equal to

$$\binom{\lfloor \frac{n}{2} \rfloor}{2i} (2i)!! y^{2i} g_{n-4i}(x, y)$$

$$t_n(x, y) = \sum_{G \in \mathfrak{G}_n} \sum_{\pi \in \phi^{-1}(G)} \mathrm{wt}(\pi) = \sum_{G \in \mathfrak{G}_n} |\phi^{-1}(G)| \mathrm{wt}(G)$$

$$= 2^{\lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{4} \rfloor} \sum_{i=0}^{k} 2^i \binom{k}{i} \frac{(2k + \lfloor \frac{r}{2} \rfloor)!!}{(2i + \lfloor \frac{r}{2} \rfloor)!!} y^{2k-2i} g_{4i+r}(x, y)$$

In particular, if $(x, y) = (1, -1)$ then

$$t_n(1, -1) = 2^{\lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{4} \rfloor} \sum_{i=0}^{k} 2^i \binom{k}{i} \frac{(2k + \lfloor \frac{r}{2} \rfloor)!!}{(2i + \lfloor \frac{r}{2} \rfloor)!!} g_{4i+r}(1, -1)$$

Properties of $g_n(x, y)$

Recurrence relation:

$$
\begin{aligned}
g_{2n+1}(x,y) &= x \cdot g_{2n}(x,y) + ny \cdot g_{2n-1}(x,y) \\
g_{2n}(x,y) &= \frac{x^2+y}{2} g_{2n-2}(x,y) + (n-1)xy \cdot g_{2n-3}(x,y) \\
&\quad + 2\binom{n-1}{2} y^2 \cdot g_{2n-4}(x,y) + 3\binom{n-1}{3} y^4 \cdot g_{2n-8}(x,y)
\end{aligned}
$$

Using the recurrence, we obtain the following.

- Let $n = 8k + r$ where $0 \leq r < 8$. Then

$$
g_n(1,1) \equiv \begin{cases} (-1)^{\lfloor \frac{k}{2} \rfloor} \mod 4 & \text{if } r = 0, 1, 2, \\ 2 \mod 4 & \text{if } r = 3, 4, 5, 7, \\ 0 \mod 4 & \text{if } r = 6. \end{cases}
$$

- If $n \geq 8$ then $g_n(1, -1)$ is even.
- If $k \geq 2$ then $\mathrm{ord}_2(g_{4k+2}(1, -1)) \geq 2$.

$\mathrm{ord}_2(t_n(1,-1))$

Using the recurrence, we obtain $t_n(1,-1)$ for $n \le 9$.

n	0	1	2	3	4	5	6	7	8	9
$g_n(1,-1)$	1	1	0	-1	-1	1	2	-1	-6	-2

Recall

$$t_n(1,-1) = 2^{\lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{4} \rfloor} \sum_{i=0}^{k} 2^i \binom{k}{i} \frac{(2k + \lfloor \frac{r}{2} \rfloor)!!}{(2i + \lfloor \frac{r}{2} \rfloor)!!} g_{4i+r}(1,-1).$$

Using the properties of $g_n(1,-1)$ and some elementary number theory, we can obtain $\mathrm{ord}_2(t_n(1,-1))$.

n	$\mathrm{ord}_2(t_n)$	$\mathrm{ord}_2(t_n(1,-1))$
$4k$	k	k
$4k+1$	k	k
$4k+2$	$k+1$	$k+3+\mathrm{ord}_2(k)$
$4k+3$	$k+2$	$k+1$

Even involutions and odd involutions

A permutation π is even if $\operatorname{sign}(\pi) = 1$, and odd if $\operatorname{sign}(\pi) = -1$.
Note that

$$t_n(1, -1) = \sum_{\pi \in \mathcal{I}_n} \operatorname{sign}(\pi).$$

t_n^{even} := the number of even involutions in $\mathcal{I}_n$
t_n^{odd} := the number of odd involutions in $\mathcal{I}_n$

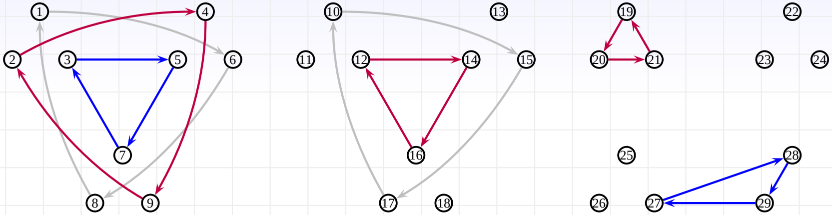
$$t_n^{\text{even}} = \frac{1}{2}\left(t_n + t_n(1, -1)\right), \quad t_n^{\text{odd}} = \frac{1}{2}\left(t_n - t_n(1, -1)\right)$$

n	$\operatorname{ord}_2(t_n)$	$\operatorname{ord}_2(t_n(1,-1))$	$\operatorname{ord}_2(t_n^{\text{even}})$	$\operatorname{ord}_2(t_n^{\text{odd}})$
$4k$	k	k	$k + \chi_{\text{odd}}(k)$	??
$4k+1$	k	k	??	$k + \operatorname{ord}_2(k) + \chi_{\text{even}}(k)$
$4k+2$	$k+1$	$k + 3 + \operatorname{ord}_2(k)$	k	k
$4k+3$	$k+2$	$k+1$	k	k

$\chi_{\text{even}}(k)$ is 1 if k is even, and 0 otherwise.
$\chi_{\text{odd}}(k)$ is 1 if k is odd, and 0 otherwise.

Case $p \geq 3$: $\pi^p = 1$, fixed points and p-cycles

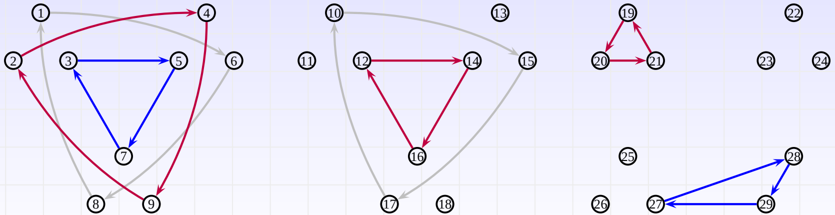
- p : a prime number ≥ 3
- $\tau_p(n)$: the number of $\pi \in \mathfrak{S}_n$ with $\pi^p = 1$
- $\mathfrak{S}_{n,p} := \{\pi \in \mathfrak{S}_n : \pi^p = 1\}$
- $\pi \in \mathfrak{S}_{n,p}$ is a directed graph consisting of fixed points and p-cycles.

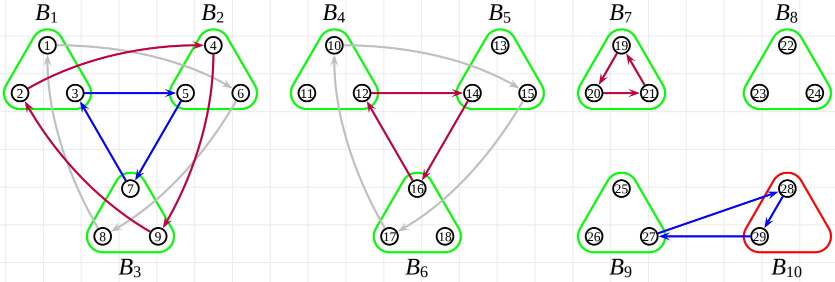


Grady and Newman (1994)

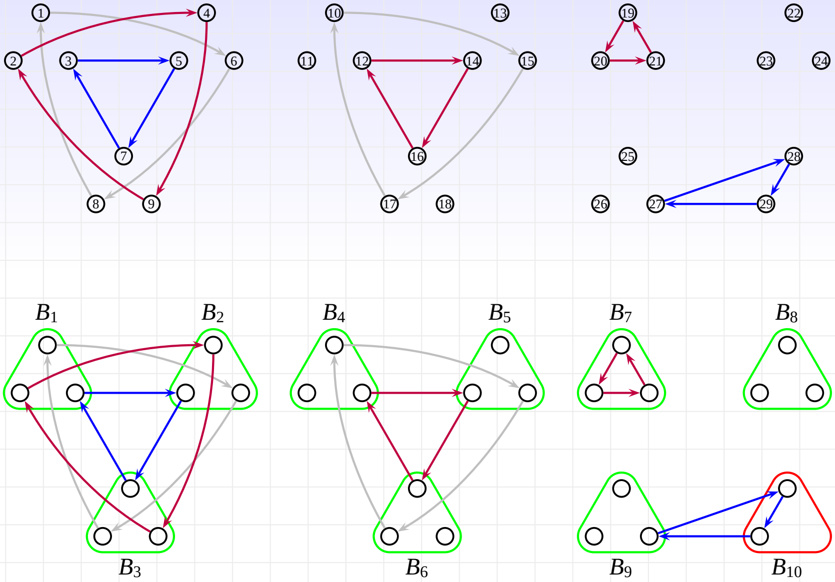
$$\mathrm{ord}_p(\tau_p(n)) \geq \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor$$

π to the directed block graph $\phi_p(\pi)$

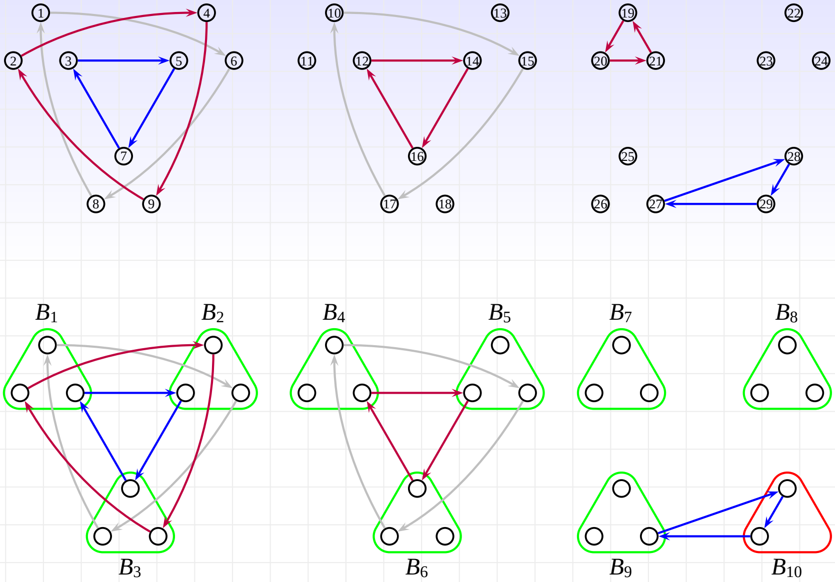




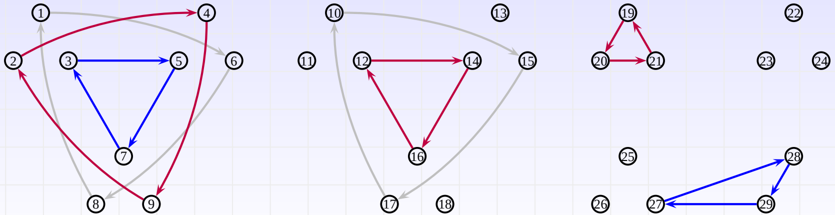
π to the directed block graph $\phi_p(\pi)$



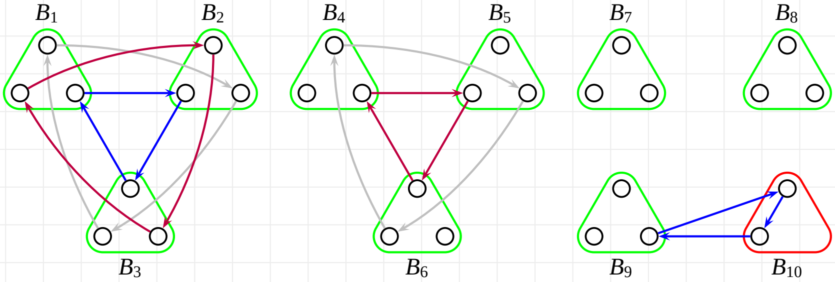
π to the directed block graph $\phi_p(\pi)$



π to the directed block graph $\phi_p(\pi)$



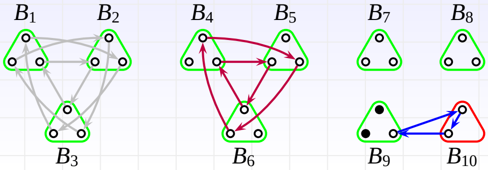
$\downarrow \phi_p$



Finding $|\phi_p^{-1}(G)|$

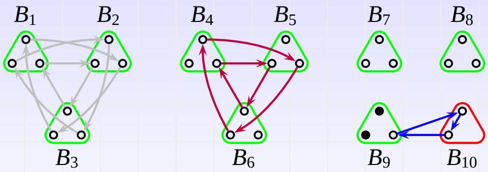
$\mathfrak{G}_{n,p} :=$ the set of directed block graphs $\phi_p(\pi)$ for $\pi \in \mathfrak{S}_{n,p}$

$$\tau_p(n) = |\mathfrak{S}_{n,p}| = \sum_{G \in \mathfrak{G}_{n,p}} |\phi_p^{-1}(G)|$$



- $inb(G) :=$ the number of isolated normal blocks
- Connected components C and C', not contained in an isolated normal block, are called identical if they have the same sequence of visiting blocks.
- Divide all connected components of G, not contained in an isolated normal block, into identical classes.
- $type(G) := (c_1, c_2, \ldots, c_l)$, where c_i denotes the number of components in an identical class.
- In the example, $inb(G) = 2$ and $type(G) = (3, 2, 2, 1, 1, 1, 1)$

Finding $|\phi_p^{-1}(G)|$



Let $n = pk + r$ and $G \in \mathfrak{G}_{n,p}$.
Let $type(G) = (c_1, c_2, \ldots, c_l)$.
Then

$$|\phi_p^{-1}(G)| = \frac{(1+(p-1)!)^{inb(G)}(p!)^{k-inb(G)} r!}{c_1! \cdots c_l!}$$

- $c_i \leq p$ and equality holds only if there are p cycles in p blocks.
- $1 + (p-1)! \equiv 0 \mod p$

$$\mathrm{ord}_p(|\phi_p^{-1}(G)|) \geq \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor$$

$$\mathrm{ord}_p(\tau_p(n)) \geq \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor$$

Thank you for listening!