The Solution of the Generalized Pei Huisheng Problem

Wolfram Bentz

University of Hull

Joint work with João Araújo (Universade Aberta/CEMAT), James Mitchell (University of St Andrews), and Csaba Schneider (Universidade Federal de Minas Gerais)

York Semigroup

York, November 4, 2015

- Throughout, X will be a finite non-empty set.

- Throughout, X will be a finite non-empty set.
- Let $T(X) = X^X$, the semigroup of all maps from X to X under composition.

- Throughout, X will be a finite non-empty set.
- Let $T(X) = X^X$, the semigroup of all maps from X to X under composition.
- We will write "semigroup style": transformation are "applied" on the right of arguments (such as in $(x)t$), and we compose left to right, i.e. $(x)f \circ g = ((x)f)g$.

- Throughout, X will be a finite non-empty set.
- Let $T(X) = X^X$, the semigroup of all maps from X to X under composition.
- We will write "semigroup style": transformation are "applied" on the right of arguments (such as in $(x)t$), and we compose left to right, i.e. $(x)f \circ g = ((x)f)g$.
- Let $\mathcal{P}$ be a partition of X. We let $T(X, \mathcal{P})$ be the subset of $T(X)$ consisting of all transformations that preserve $\mathcal{P}$, i.e. those $f \in T(X)$ that satisfy $(x, y) \in \mathcal{P} \Rightarrow (xf, yf) \in \mathcal{P}$.

- Throughout, X will be a finite non-empty set.
- Let $T(X) = X^X$, the semigroup of all maps from X to X under composition.
- We will write "semigroup style": transformation are "applied" on the right of arguments (such as in $(x)t$), and we compose left to right, i.e. $(x)f \circ g = ((x)f)g$.
- Let $\mathcal{P}$ be a partition of X. We let $T(X, \mathcal{P})$ be the subset of $T(X)$ consisting of all transformations that preserve $\mathcal{P}$, i.e. those $f \in T(X)$ that satisfy $(x, y) \in \mathcal{P} \Rightarrow (xf, yf) \in \mathcal{P}$.
- $T(X, \mathcal{P})$ is clearly a subsemigroup of $T(X)$, in fact, it is the endomorphism monoid of the relational structure $(X; \mathcal{P})$.

- Throughout, X will be a finite non-empty set.
- Let $T(X) = X^X$, the semigroup of all maps from X to X under composition.
- We will write "semigroup style": transformation are "applied" on the right of arguments (such as in $(x)t$), and we compose left to right, i.e. $(x)f \circ g = ((x)f)g$.
- Let $\mathcal{P}$ be a partition of X. We let $T(X, \mathcal{P})$ be the subset of $T(X)$ consisting of all transformations that preserve $\mathcal{P}$, i.e. those $f \in T(X)$ that satisfy $(x, y) \in \mathcal{P} \Rightarrow (xf, yf) \in \mathcal{P}$.
- $T(X, \mathcal{P})$ is clearly a subsemigroup of $T(X)$, in fact, it is the endomorphism monoid of the relational structure $(X; \mathcal{P})$.
- We are concerned with determining ranks of semigroups, i.e. the sizes of the smallest generating sets.

Pei Huisheng Problem

Pei Huisheng Problem

- Original Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ a *uniform* partition of X. Determine the rank of $T(X, P)$.

Pei Huisheng Problem

- Original Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ a *uniform* partition of X. Determine the rank of $T(X, P)$.
- Solved by Araújo and Schneider in 2009.

Pei Huisheng Problem

- Original Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ a *uniform* partition of X. Determine the rank of $T(X, P)$.
- Solved by Araújo and Schneider in 2009.
- General Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ an *arbitray* partition of X. Determine the rank of $T(X, P)$.

Pei Huisheng Problem

- Original Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ a *uniform* partition of X. Determine the rank of $T(X,P)$.
- Solved by Araújo and Schneider in 2009.
- General Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ an *arbitray* partition of X. Determine the rank of $T(X,P)$.
- Solution published in the Mathematical Proceedings of the Cambridge Philosophical Society in 2015.

Pei Huisheng Problem

- Original Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ a *uniform* partition of X. Determine the rank of $T(X, P)$.
- Solved by Araújo and Schneider in 2009.
- General Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ an *arbitray* partition of X. Determine the rank of $T(X, P)$.
- Solution published in the Mathematical Proceedings of the Cambridge Philosophical Society in 2015.
- First paper on transformation semigroups published in the proceedings in 20 years

Pei Huisheng Problem

- Original Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ a *uniform* partition of X. Determine the rank of $T(X, P)$.
- Solved by Araújo and Schneider in 2009.
- General Pei Huisheng Problem: Let X be a finite non-empty set, and $\mathcal{P}$ an *arbitray* partition of X. Determine the rank of $T(X, P)$.
- Solution published in the Mathematical Proceedings of the Cambridge Philosophical Society in 2015.
- First paper on transformation semigroups published in the proceedings in 20 years (according to João).

The main result

Theorem

If $|X| \geq 4$, then the rank of $T(X, \mathcal{P})$ is given by

$$\max\{2, 2p + q + g(t)\} + \binom{p+q}{2} + 2p + q + g'(t) - 1 + l + h(p, q, t),$$

where (with $\sim$ being the equivalence relation "has the same cardinality")

- $t = |\{P \in \mathcal{P}\} : |P| = 1\}|$.
- $q = |\{[P] \in (\mathcal{P}/\sim) : |P| \geq 2, |[P]| = 1\}|$,
- $p = |\{[P] \in (\mathcal{P}/\sim) : |P| \geq 2, |[P]| \geq 2\}|$,
- *l is the number of values s for which $\mathcal{P}$ has a block of size $s \geq 2$, but no block of size $s - 1$,*
- $g(0) = g(1) = 0$ *and* $g(t) = 1$ *for* $t \geq 2$,
- $g'(0) = 0$ *and* $g'(t) = 1$ *for* $t \geq 1$.
- $h(p, q, 0) = 0$, $h(p, q, 1) = p + q$ *and* $h(p, q, t) = p + q + 1$, *if* $t \geq 2$.

The main result simplified

Theorem

Let $|X| \geq 4$, and $\mathcal{P}$ a non-trivial partition of X without singleton parts. Then the rank of $T(X, \mathcal{P})$ is given by

$$\binom{p+q}{2} + 4p + 2q - 1 + l$$

where

- *q is the number of values s for which $\mathcal{P}$ has a unique block of size s,*
- *p is the number of values s for which $\mathcal{P}$ has at least two blocks of size s,*
- *l is the number of values s for which $\mathcal{P}$ has a block of size s, but no block of size $s-1$.*

Splitting the problem

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

- This is well defined, as f preserves $\mathcal{P}$.

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

- This is well defined, as f preserves $\mathcal{P}$.
- Consider the following subsets of $T(X, \mathcal{P})$:

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

- This is well defined, as f preserves $\mathcal{P}$.
- Consider the following subsets of $T(X, \mathcal{P})$:
    1. The set $S(X, \mathcal{P})$ of all permutations in $\mathcal{P}$,

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

- This is well defined, as f preserves $\mathcal{P}$.
- Consider the following subsets of $T(X, \mathcal{P})$:
  1. The set $S(X, \mathcal{P})$ of all permutations in $\mathcal{P}$,
  2. The set $\Sigma(X, \mathcal{P})$ of all $f \in T(X, \mathcal{P})$ such that $\bar{f}$ is a permutation.

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

- This is well defined, as f preserves $\mathcal{P}$.
- Consider the following subsets of $T(X, \mathcal{P})$:
  1. The set $S(X, \mathcal{P})$ of all permutations in $\mathcal{P}$,
  2. The set $\Sigma(X, \mathcal{P})$ of all $f \in T(X, \mathcal{P})$ such that $\bar{f}$ is a permutation.
- Both $T(X, \mathcal{P}) \setminus S(X, \mathcal{P})$ and $T(X, \mathcal{P}) \setminus \Sigma(X, \mathcal{P})$ are ideals.

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

- This is well defined, as f preserves $\mathcal{P}$.
- Consider the following subsets of $T(X, \mathcal{P})$:
  1. The set $S(X, \mathcal{P})$ of all permutations in $\mathcal{P}$,
  2. The set $\Sigma(X, \mathcal{P})$ of all $f \in T(X, \mathcal{P})$ such that $\bar{f}$ is a permutation.
- Both $T(X, \mathcal{P}) \setminus S(X, \mathcal{P})$ and $T(X, \mathcal{P}) \setminus \Sigma(X, \mathcal{P})$ are ideals.
- Hence $S(X, \mathcal{P})$ must be generated by elements from $S(X, \mathcal{P})$ (and analog for $\Sigma(X, \mathcal{P})$).

Splitting the problem

- For $f \in T(X, \mathcal{P})$ let $\bar{f} \in T(\mathcal{P})$ be given by

$$([x])\bar{f} = (x)f \text{ for all } [x] \in P.$$

- This is well defined, as f preserves $\mathcal{P}$.
- Consider the following subsets of $T(X, \mathcal{P})$:
  1. The set $S(X, \mathcal{P})$ of all permutations in $\mathcal{P}$,
  2. The set $\Sigma(X, \mathcal{P})$ of all $f \in T(X, \mathcal{P})$ such that $\bar{f}$ is a permutation.
- Both $T(X, \mathcal{P}) \setminus S(X, \mathcal{P})$ and $T(X, \mathcal{P}) \setminus \Sigma(X, \mathcal{P})$ are ideals.
- Hence $S(X, \mathcal{P})$ must be generated by elements from $S(X, \mathcal{P})$ (and analog for $\Sigma(X, \mathcal{P})$).
- For any semigroup S and any $X \subseteq S$, we define rank$(S : X)$, the *relative rank* of S over X, as the cardinality of the smallest set W for which $S = \langle X \cup W \rangle$.

Splitting the problem

Our result states that under the given conditions

$$\operatorname{rank}(T(X, \mathcal{P})) = \binom{p+q}{2} + 4p + 2q - 1 + l$$

Splitting the problem

Our result states that under the given conditions

$$\mathrm{rank}(T(X,\mathcal{P})) = \binom{p+q}{2} + 4p + 2q - 1 + l$$

$$= \underbrace{2p+q}_{\mathrm{rank}(S(X,\mathcal{P}))} + \underbrace{p+q-1+l}_{\mathrm{rank}(\Sigma(X,\mathcal{P}):S(X,\mathcal{P}))} + \underbrace{\binom{p+q}{2} + p}_{\mathrm{rank}(T(X,P):\Sigma(X,\mathcal{P}))}$$

where

- q is the number of values s for which $\mathcal{P}$ has a unique block of size s,
- p is the number of values s for which $\mathcal{P}$ has at least two blocks of size s,
- l is the number of values s for which $\mathcal{P}$ has a block of size s, but no block of size $s-1$.

Lemma

Let $\mathcal{P}$ be a partition of a set X where the distinct sizes of the $\mathcal{P}$-blocks that appear more than once are denoted n_i, $i = 1, \ldots, p$, and m_i denotes the number of blocks of size n_i. Let l_i, $i = 1, \ldots, q$ be the distinct sizes of $\mathcal{P}$-blocks that appear exactly once. Then the group of units $S(X, \mathcal{P})$ of $T(X, \mathcal{P})$ is isomorphic to

$$(S_{n_1} \wr S_{m_1}) \times \cdots \times (S_{n_p} \wr S_{m_p}) \times S_1 \times \cdots \times S_q.$$

Lemma

Let $\mathcal{P}$ be a partition of a set X where the distinct sizes of the $\mathcal{P}$-blocks that appear more than once are denoted n_i, $i = 1, \ldots, p$, and m_i denotes the number of blocks of size n_i. Let l_i, $i = 1, \ldots, q$ be the distinct sizes of $\mathcal{P}$-blocks that appear exactly once. Then the group of units $S(X, \mathcal{P})$ of $T(X, \mathcal{P})$ is isomorphic to

$$(S_{n_1} \wr S_{m_1}) \times \cdots \times (S_{n_p} \wr S_{m_p}) \times S_1 \times \cdots \times S_q.$$

Theorem

Let $n_1, \ldots, n_k, m_1, \ldots, m_k, l_1, \ldots, l_u$ be integers such that they are all at least 2 and let

$$W = (S_{n_1} \wr S_{m_1}) \times \cdots \times (S_{n_p} \wr S_{m_p}) \times S_{l_1} \times \cdots \times S_{l_q}.$$

If $p \geq 1$ or $q \geq 2$, then the rank of W is $2p + q$.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.
- This group has a quotient G' isomorphic to $C_2 \wr S_m$.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.
- This group has a quotient G' isomorphic to $C_2 \wr S_m$.
- G' can be viewed as the permutation module of S_m over the two element field.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.
- This group has a quotient G' isomorphic to $C_2 \wr S_m$.
- G' can be viewed as the permutation module of S_m over the two element field.
- By standard results from representation theory, this module has a submodule of dimension $m_i - 1$.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.
- This group has a quotient G' isomorphic to $C_2 \wr S_m$.
- G' can be viewed as the permutation module of S_m over the two element field.
- By standard results from representation theory, this module has a submodule of dimension $m_i - 1$.
- Viewing G' as a group again, it follows that G' (and hence G) has a quotient isomorphic to $C_2 \times S_{m_i}$.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.
- This group has a quotient G' isomorphic to $C_2 \wr S_m$.
- G' can be viewed as the permutation module of S_m over the two element field.
- By standard results from representation theory, this module has a submodule of dimension $m_i - 1$.
- Viewing G' as a group again, it follows that G' (and hence G) has a quotient isomorphic to $C_2 \times S_{m_i}$.
- By factoring out $\{e\} \times A_{m_i}$, we conclude that G has a quotient isomorphic to $C_2 \times C_2$.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.
- This group has a quotient G' isomorphic to $C_2 \wr S_m$.
- G' can be viewed as the permutation module of S_m over the two element field.
- By standard results from representation theory, this module has a submodule of dimension $m_i - 1$.
- Viewing G' as a group again, it follows that G' (and hence G) has a quotient isomorphic to $C_2 \times S_{m_i}$.
- By factoring out $\{e\} \times A_{m_i}$, we conclude that G has a quotient isomorphic to $C_2 \times C_2$.
- As every S_{l_i} has a quotient isomorphic to C_2, it follows that W has a quotient isomorphic to C_2^{2p+q}.

The rank of W is at least $2p + q$

- Consider $G = S_{n_i} \wr S_{m_i}$.
- This group has a quotient G' isomorphic to $C_2 \wr S_m$.
- G' can be viewed as the permutation module of S_m over the two element field.
- By standard results from representation theory, this module has a submodule of dimension $m_i - 1$.
- Viewing G' as a group again, it follows that G' (and hence G) has a quotient isomorphic to $C_2 \times S_{m_i}$.
- By factoring out $\{e\} \times A_{m_i}$, we conclude that G has a quotient isomorphic to $C_2 \times C_2$.
- As every S_{l_i} has a quotient isomorphic to C_2, it follows that W has a quotient isomorphic to C_2^{2p+q}.
- C_2^{2p+q} cannot be generated by less than $2p + q$ generators, and thus neither can W.

A generating set for W

Lemma

If $q \geq 2$, then $S_{l_1} \times \cdots \times S_{l_q}$ has rank q.
Concretely, for $i \in \{1, \ldots, q-1\}$ define

$$w_i = (e, \ldots, e, \overset{i\text{-th component}}{(1,2)}, \overset{(i+1)\text{-th component}}{z_{i+1}}, e, \ldots, e)$$

and also define

$$w_q = (z_1, e, \ldots, e, (1,2)),$$

where z_i is the odd permutation in $\{(1, 2, \ldots, l_i), (2, 3, \ldots, l_i)\}$.
Then $S_{l_1} \times \cdots \times S_{l_q} = \langle w_1, \ldots, w_q \rangle$.

A generating set for W

Lemma (Araújo, Schneider)

If $m, n \geq 2$, then $S_n \wr S_m = \langle x, y \rangle$, where

$$x = \begin{cases} (e,(1,2),e,\ldots,e)(1,2,\ldots,m) & \text{if either } n \text{ or } m \text{ is odd} \\ (e,(1,2),e,\ldots,e)(2,3,\ldots,m) & \text{otherwise} \end{cases}$$

$$y = ((1,2,\ldots,n),e,\ldots,e)(1,2).$$

- Together, the two lemmas show that $S(X, \mathcal{P}) = 2q + p$, except when $p = 1$.

A generating set for W

Lemma (Araújo, Schneider)

If $m, n \geq 2$, then $S_n \wr S_m = \langle x, y \rangle$, where

$$
\begin{aligned}
x &= \begin{cases} (e, (1,2), e, \ldots, e)(1, 2, \ldots, m) & \text{if either } n \text{ or } m \text{ is odd} \\ (e, (1,2), e, \ldots, e)(2, 3, \ldots, m) & \text{otherwise} \end{cases} \\
y &= ((1, 2, \ldots, n), e, \ldots, e)(1, 2).
\end{aligned}
$$

- Together, the two lemmas show that $S(X, \mathcal{P}) = 2q + p$, except when $p = 1$.
- The remaining case can be handled by similar arguments.

- Recall that $\Sigma(X, \mathcal{P})$ is the set of transformations in $T(X, \mathcal{P})$ which induce a permutation on the blocks of $\mathcal{P}$.

- Recall that $\Sigma(X, \mathcal{P})$ is the set of transformations in $T(X, \mathcal{P})$ which induce a permutation on the blocks of $\mathcal{P}$.
- We next want to show that $\operatorname{rank}(\Sigma(X, \mathcal{P}) : S(X, \mathcal{P}))$

$$= \underbrace{p + q - 1}_{\text{Block Switching}} + \underbrace{l}_{\text{Image reducing}},$$

where

- q is the number of values s for which $\mathcal{P}$ has a unique block of size s,
- p is the number of values s for which $\mathcal{P}$ has at least two blocks of size s,
- l is the number of values s for which $\mathcal{P}$ has a block of size s, but no block of size $s - 1$.

Block switching

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.

Block switching

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p + q - 1$, let $\mathcal{B}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that

Block switching

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p + q - 1$, let $\mathcal{B}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps a block of size l_i injectively to a block of size l_{i+1},

Block switching

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p + q - 1$, let $\mathcal{B}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps a block of size l_i injectively to a block of size l_{i+1},
  2. f maps a block of size l_{i+1} surjectively onto a block of size l_i,

Block switching

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \le p+q-1$, let $\mathcal{B}_i$ be the set of all mappings $f \in \Sigma(X,\mathcal{P})$ such that
  1. f maps a block of size l_i injectively to a block of size l_{i+1},
  2. f maps a block of size l_{i+1} surjectively onto a block of size l_i,
  3. f maps every other block bijectively to a block of the same size.

Block switching

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p + q - 1$, let $\mathcal{B}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps a block of size l_i injectively to a block of size l_{i+1},
  2. f maps a block of size l_{i+1} surjectively onto a block of size l_i,
  3. f maps every other block bijectively to a block of the same size.

Block switching

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p+q-1$, let $\mathcal{B}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps a block of size l_i injectively to a block of size l_{i+1},
  2. f maps a block of size l_{i+1} surjectively onto a block of size l_i,
  3. f maps every other block bijectively to a block of the same size.

Lemma

If $\langle S(X, \mathcal{P}), U \rangle = \Sigma(X, \mathcal{P})$ for some $U \subseteq \Sigma(X, \mathcal{P})$, then $\mathcal{B}_i \cap U \neq \emptyset$ for every $i \leq p+q-1$.

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \ldots, p + q - 1$

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \ldots, p + q - 1$
- Note that the map f has a defect of $l_{i+1} - l_i$.

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \ldots, p + q - 1$
- Note that the map f has a defect of $l_{i+1} - l_i$.
- Let B be the l_i-block of f that is mapped "upwards".

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \ldots, p+q-1$
- Note that the map f has a defect of $l_{i+1} - l_i$.
- Let B be the l_i-block of f that is mapped "upwards".
- Now suppose that $f = g_1 \ldots g_s$ with generators from $S(X, \mathcal{P})$ and U

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \dots, p + q - 1$
- Note that the map f has a defect of $l_{i+1} - l_i$.
- Let B be the l_i-block of f that is mapped "upwards".
- Now suppose that $f = g_1 \dots g_s$ with generators from $S(X, \mathcal{P})$ and U
- Eventually, some g_j must map $Bg_1 \dots g_{j-1}$ to a block B' of different size k

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \dots, p + q - 1$
- Note that the map f has a defect of $l_{i+1} - l_i$.
- Let B be the l_i-block of f that is mapped "upwards".
- Now suppose that $f = g_1 \dots g_s$ with generators from $S(X, \mathcal{P})$ and U
- Eventually, some g_j must map $Bg_1 \dots g_{j-1}$ to a block B' of different size k
- If $k < l_i$, then B is not mapped injectively, so $k > l_i$.

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \dots, p+q-1$
- Note that the map f has a defect of $l_{i+1} - l_i$.
- Let B be the l_i-block of f that is mapped "upwards".
- Now suppose that $f = g_1 \dots g_s$ with generators from $S(X, \mathcal{P})$ and U
- Eventually, some g_j must map $Bg_1 \dots g_{j-1}$ to a block B' of different size k
- If $k < l_i$, then B is not mapped injectively, so $k > l_i$.
- If $k > l_{i+1}$, then $k - l_i$ elements of B' would not be in the image of $g_1 \dots g_j$, and so the defect of f would exceed $l_{i+1} - l_i$.

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \dots, p + q - 1$
- Note that the map f has a defect of $l_{i+1} - l_i$.
- Let B be the l_i-block of f that is mapped "upwards".
- Now suppose that $f = g_1 \dots g_s$ with generators from $S(X, \mathcal{P})$ and U
- Eventually, some g_j must map $Bg_1 \dots g_{j-1}$ to a block B' of different size k
- If $k < l_i$, then B is not mapped injectively, so $k > l_i$.
- If $k > l_{i+1}$, then $k - l_i$ elements of B' would not be in the image of $g_1 \dots g_j$, and so the defect of f would exceed $l_{i+1} - l_i$.
- Hence $k = l_{i+1}$, and g_i maps B to a block of size l_{i+1}.

Block switching

- Let f be an element of $\mathcal{B}_i$, for $i = 1, \dots, p+q-1$
- Note that the map f has a defect of $l_{i+1} - l_i$.
- Let B be the l_i-block of f that is mapped "upwards".
- Now suppose that $f = g_1 \dots g_s$ with generators from $S(X, \mathcal{P})$ and U
- Eventually, some g_j must map $Bg_1 \dots g_{j-1}$ to a block B' of different size k
- If $k < l_i$, then B is not mapped injectively, so $k > l_i$.
- If $k > l_{i+1}$, then $k - l_i$ elements of B' would not be in the image of $g_1 \dots g_j$, and so the defect of f would exceed $l_{i+1} - l_i$.
- Hence $k = l_{i+1}$, and g_i maps B to a block of size l_{i+1}.
- Applying similar size considerations to the other blocks of $\mathcal{P}$, we can show that $g_j \in \mathcal{B}_i$.

Image reducing

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.

Image reducing

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p + q$, let $\mathcal{C}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that

Image reducing

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p+q$, let $\mathcal{C}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps every block to a block of the same size

Image reducing

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p+q$, let $\mathcal{C}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps every block to a block of the same size
  2. f has a defect of 1.

Image reducing

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p + q$, let $\mathcal{C}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps every block to a block of the same size
  2. f has a defect of 1.

Image reducing

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $i \leq p+q$, let $\mathcal{C}_i$ be the set of all mappings $f \in \Sigma(X,\mathcal{P})$ such that
  1. f maps every block to a block of the same size
  2. f has a defect of 1.

Lemma

Let $\langle S(X,\mathcal{P}), U\rangle = \Sigma(X,\mathcal{P})$ for some $U \subseteq \Sigma(X,\mathcal{P})$. If $i = 1,\ldots,p+q$ is such that $\mathcal{P}$ has no block of size $l_i - 1$, then $\mathcal{C}_i \cap U \neq \emptyset$.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.
- Let $f \in \Sigma(X, \mathcal{P})$ be the function that maps one element of B to another element of B, and is the identity otherwise.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.
- Let $f \in \Sigma(X, \mathcal{P})$ be the function that maps one element of B to another element of B, and is the identity otherwise.
- Suppose that $f = h_1 \cdots h_m$ with $h_i \in S(X, \mathcal{P}) \cup U$.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.
- Let $f \in \Sigma(X, \mathcal{P})$ be the function that maps one element of B to another element of B, and is the identity otherwise.
- Suppose that $f = h_1 \cdots h_m$ with $h_i \in S(X, \mathcal{P}) \cup U$.
- Let z be the smallest index for which the image of $h_1 \cdots h_z$ does not contain a block B' of size l_i, and let B'' be the block for which $(B'')h_z = B'$.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.
- Let $f \in \Sigma(X, \mathcal{P})$ be the function that maps one element of B to another element of B, and is the identity otherwise.
- Suppose that $f = h_1 \cdots h_m$ with $h_i \in S(X, \mathcal{P}) \cup U$.
- Let z be the smallest index for which the image of $h_1 \cdots h_z$ does not contain a block B' of size l_i, and let B'' be the block for which $(B'')h_z = B'$.
- If $|B''| < l_i$ then h_z and hence f would have a defect of at least 2, as there is no block of size $l_i - 1$.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.
- Let $f \in \Sigma(X, \mathcal{P})$ be the function that maps one element of B to another element of B, and is the identity otherwise.
- Suppose that $f = h_1 \cdots h_m$ with $h_i \in S(X, \mathcal{P}) \cup U$.
- Let z be the smallest index for which the image of $h_1 \cdots h_z$ does not contain a block B' of size l_i, and let B'' be the block for which $(B'')h_z = B'$.
- If $|B''| < l_i$ then h_z and hence f would have a defect of at least 2, as there is no block of size $l_i - 1$.
- If $|B''| > l_i$, then $h_z \in \Sigma(X, \mathcal{P})$ must map another block "upwards". This would result in a second block not being contained in the image of f, and a defect of more than 1.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.
- Let $f \in \Sigma(X, \mathcal{P})$ be the function that maps one element of B to another element of B, and is the identity otherwise.
- Suppose that $f = h_1 \cdots h_m$ with $h_i \in S(X, \mathcal{P}) \cup U$.
- Let z be the smallest index for which the image of $h_1 \cdots h_z$ does not contain a block B' of size l_i, and let B'' be the block for which $(B'')h_z = B'$.
- If $|B''| < l_i$ then h_z and hence f would have a defect of at least 2, as there is no block of size $l_i - 1$.
- If $|B''| > l_i$, then $h_z \in \Sigma(X, \mathcal{P})$ must map another block "upwards". This would result in a second block not being contained in the image of f, and a defect of more than 1.
- Hence $|B''| = l_i$, and by minimality of h_z, the mapping from B'' to B' is not injective.

Image reducing

- Let B be a block of size l_i, where i is as in the lemma.
- Let $f \in \Sigma(X,\mathcal{P})$ be the function that maps one element of B to another element of B, and is the identity otherwise.
- Suppose that $f = h_1 \cdots h_m$ with $h_i \in S(X,\mathcal{P}) \cup U$.
- Let z be the smallest index for which the image of $h_1 \cdots h_z$ does not contain a block B' of size l_i, and let B'' be the block for which $(B'')h_z = B'$.
- If $|B''| < l_i$ then h_z and hence f would have a defect of at least 2, as there is no block of size $l_i - 1$.
- If $|B''| > l_i$, then $h_z \in \Sigma(X,\mathcal{P})$ must map another block "upwards". This would result in a second block not being contained in the image of f, and a defect of more than 1.
- Hence $|B''| = l_i$, and by minimality of h_z, the mapping from B'' to B' is not injective.
- Image size now show that all remaining blocks are mapped bijectively. So $h_z \in \mathcal{C}_i$.

The lower bound

It remains to show that we can generate $\Sigma(X, \mathcal{P})$ from $S(X, \mathcal{P})$ and a set of representatives of the relevant $\mathcal{B}_i$ and $\mathcal{C}_i$.

- Assume first that $l_i - l_{i-1} = 1$. Let h be a generator from $\mathcal{B}_{i-1}$. Then we can generate an element of $\mathcal{C}_i$ in the form hgh for a suitable $g \in S(X, \mathcal{P})$.

The lower bound

It remains to show that we can generate $\Sigma(X, \mathcal{P})$ from $S(X, \mathcal{P})$ and a set of representatives of the relevant $\mathcal{B}_i$ and $\mathcal{C}_i$.

- Assume first that $l_i - l_{i-1} = 1$. Let h be a generator from $\mathcal{B}_{i-1}$. Then we can generate an element of $\mathcal{C}_i$ in the form hgh for a suitable $g \in S(X, \mathcal{P})$.
- This means that restricted to each block B, we have all permutations and a map of defect 1. From these functions, we can generate $T(B)$.

The lower bound

It remains to show that we can generate $\Sigma(X, \mathcal{P})$ from $S(X, \mathcal{P})$ and a set of representatives of the relevant $\mathcal{B}_i$ and $\mathcal{C}_i$.

- Assume first that $l_i - l_{i-1} = 1$. Let h be a generator from $\mathcal{B}_{i-1}$. Then we can generate an element of $\mathcal{C}_i$ in the form hgh for a suitable $g \in S(X, \mathcal{P})$.
- This means that restricted to each block B, we have all permutations and a map of defect 1. From these functions, we can generate $T(B)$.
- Let $f \in \Sigma(X, \mathcal{P})$. In order to establish that f can be obtained from our generators, it suffices to show that we can recover the permutation $\bar{f}$ of the blocks of $\mathcal{P}$ in such a way that no block dips "too low".

The lower bound

It remains to show that we can generate $\Sigma(X, \mathcal{P})$ from $S(X, \mathcal{P})$ and a set of representatives of the relevant $\mathcal{B}_i$ and $\mathcal{C}_i$.

- Assume first that $l_i - l_{i-1} = 1$. Let h be a generator from $\mathcal{B}_{i-1}$. Then we can generate an element of $\mathcal{C}_i$ in the form hgh for a suitable $g \in S(X, \mathcal{P})$.
- This means that restricted to each block B, we have all permutations and a map of defect 1. From these functions, we can generate $T(B)$.
- Let $f \in \Sigma(X, \mathcal{P})$. In order to establish that f can be obtained from our generators, it suffices to show that we can recover the permutation $\bar{f}$ of the blocks of $\mathcal{P}$ in such a way that no block dips "too low".
- This means that at every stage of the process, the image of any block B must have size at least $\min\{|B|, |Bf|\}$.

We next want to show that rank$(T(X, \mathcal{P}) : \Sigma(X, \mathcal{P}))$

$$= \underbrace{\binom{p+q}{2}}_{\text{Combining different sizes}} + \underbrace{p}_{\text{Combining same sizes}},$$

where

- q is the number of values s for which $\mathcal{P}$ has a unique block of size s,
- p is the number of values s for which $\mathcal{P}$ has at least two blocks of size s.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $1 \leq i < j \leq p + q$, let $\mathcal{A}_{i,j}$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $1 \leq i < j \leq p + q$, let $\mathcal{A}_{i,j}$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are of sizes l_i and l_j,

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $1 \leq i < j \leq p+q$, let $\mathcal{A}_{i,j}$ be the set of all mappings $f \in \Sigma(X,\mathcal{P})$ such that
  1. f maps exactly two blocks together, which are of sizes l_i and l_j,
  2. f maps every other block injectively.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $1 \leq i < j \leq p+q$, let $\mathcal{A}_{i,j}$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are of sizes l_i and l_j,
  2. f maps every other block injectively.
- Note that this implies that every block - other the mentioned block of size l_i - is mapped bijectively to a block of the same size.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $1 \leq i < j \leq p+q$, let $\mathcal{A}_{i,j}$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are of sizes l_i and l_j,
  2. f maps every other block injectively.
- Note that this implies that every block - other the mentioned block of size l_i - is mapped bijectively to a block of the same size.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- For $1 \leq i < j \leq p+q$, let $\mathcal{A}_{i,j}$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are of sizes l_i and l_j,
  2. f maps every other block injectively.
- Note that this implies that every block - other the mentioned block of size l_i - is mapped bijectively to a block of the same size.

Lemma

If $\langle \Sigma(X, \mathcal{P}), U \rangle = T(X, \mathcal{P})$ for some $U \subseteq \Sigma(X, \mathcal{P})$, then $\mathcal{A}_{i,j} \cap U \neq \emptyset$ for all $1 \leq i < j \leq p+q$.

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.
- Now suppose that $f = g_1 \dots g_s$ with generators from $\Sigma(X, \mathcal{P})$ and U

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.
- Now suppose that $f = g_1 \dots g_s$ with generators from $\Sigma(X, \mathcal{P})$ and U
- Let g_k be the first generator not from $\Sigma(X, \mathcal{P})$.

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.
- Now suppose that $f = g_1 \dots g_s$ with generators from $\Sigma(X, \mathcal{P})$ and U
- Let g_k be the first generator not from $\Sigma(X, \mathcal{P})$.
- As f is injective on each block, $g_1 \dots g_{k-1}$ can only permute blocks of the same size.

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.
- Now suppose that $f = g_1 \dots g_s$ with generators from $\Sigma(X, \mathcal{P})$ and U
- Let g_k be the first generator not from $\Sigma(X, \mathcal{P})$.
- As f is injective on each block, $g_1 \dots g_{k-1}$ can only permute blocks of the same size.
- So $|Bg_1 \dots g_{k-1}| = l_i$, and $|B'g_1 \dots g_{k-1}| = l_j$.

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.
- Now suppose that $f = g_1 \dots g_s$ with generators from $\Sigma(X,\mathcal{P})$ and U
- Let g_k be the first generator not from $\Sigma(X,\mathcal{P})$.
- As f is injective on each block, $g_1 \dots g_{k-1}$ can only permute blocks of the same size.
- So $|Bg_1 \dots g_{k-1}| = l_i$, and $|B'g_1 \dots g_{k-1}| = l_j$.
- As $g_k \notin \Sigma(X,\mathcal{P})$, it must map at least two blocks together. This can only be $Bg_1 \dots g_{k-1}$, and $B'g_1 \dots g_{k-1}$.

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.
- Now suppose that $f = g_1 \dots g_s$ with generators from $\Sigma(X, \mathcal{P})$ and U
- Let g_k be the first generator not from $\Sigma(X, \mathcal{P})$.
- As f is injective on each block, $g_1 \dots g_{k-1}$ can only permute blocks of the same size.
- So $|Bg_1 \dots g_{k-1}| = l_i$, and $|B'g_1 \dots g_{k-1}| = l_j$.
- As $g_k \notin \Sigma(X, \mathcal{P})$, it must map at least two blocks together. This can only be $Bg_1 \dots g_{k-1}$, and $B'g_1 \dots g_{k-1}$.
- Counting image sizes, we see that these must be mapped together to a block of size l_j.

Combining

- Let $i < j$ and f such that f maps block B of size l_i to block B' of size l_j, and is the identity everywhere else.
- Now suppose that $f = g_1 \dots g_s$ with generators from $\Sigma(X, \mathcal{P})$ and U
- Let g_k be the first generator not from $\Sigma(X, \mathcal{P})$.
- As f is injective on each block, $g_1 \dots g_{k-1}$ can only permute blocks of the same size.
- So $|Bg_1 \dots g_{k-1}| = l_i$, and $|B'g_1 \dots g_{k-1}| = l_j$.
- As $g_k \notin \Sigma(X, \mathcal{P})$, it must map at least two blocks together. This can only be $Bg_1 \dots g_{k-1}$, and $B'g_1 \dots g_{k-1}$.
- Counting image sizes, we see that these must be mapped together to a block of size l_j.
- By considering image sizes, we can check that $g_k \in \mathcal{A}_{i,j}$.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- Let $1 \leq i \leq p+q$ be such that $\mathcal{P}$ has at least two blocks of size l_i. Let $\mathcal{A}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- Let $1 \leq i \leq p+q$ be such that $\mathcal{P}$ has at least two blocks of size l_i. Let $\mathcal{A}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are both of sizes l_i,

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- Let $1 \leq i \leq p+q$ be such that $\mathcal{P}$ has at least two blocks of size l_i. Let $\mathcal{A}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are both of sizes l_i,
  2. f maps every other block injectively.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- Let $1 \leq i \leq p + q$ be such that $\mathcal{P}$ has at least two blocks of size l_i. Let $\mathcal{A}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are both of sizes l_i,
  2. f maps every other block injectively.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- Let $1 \leq i \leq p+q$ be such that $\mathcal{P}$ has at least two blocks of size l_i. Let $\mathcal{A}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are both of sizes l_i,
  2. f maps every other block injectively.

Lemma

If $\langle \Sigma(X, \mathcal{P}), U \rangle = T(X, \mathcal{P})$ for some $U \subseteq \Sigma(X, \mathcal{P})$, then $\mathcal{A}_i \cap U \neq \emptyset$ for all $1 \leq i \leq p+q$ for which $\mathcal{P}$ has multiple blocks of size l_i.

Combining

- Let $l_1 < l_2 < \cdots < l_{p+q}$ be the distinct sizes of blocks in $\mathcal{P}$.
- Let $1 \leq i \leq p+q$ be such that $\mathcal{P}$ has at least two blocks of size l_i. Let $\mathcal{A}_i$ be the set of all mappings $f \in \Sigma(X, \mathcal{P})$ such that
  1. f maps exactly two blocks together, which are both of sizes l_i,
  2. f maps every other block injectively.

Lemma

If $\langle \Sigma(X,\mathcal{P}), U\rangle = T(X,\mathcal{P})$ for some $U \subseteq \Sigma(X,\mathcal{P})$, then $\mathcal{A}_i \cap U \neq \emptyset$ for all $1 \leq i \leq p+q$ for which $\mathcal{P}$ has multiple blocks of size l_i.

The main theorem now follows once we can show that we can generate $T(X,\mathcal{P})$ from $\Sigma(X,\mathcal{P})$ and a set of representatives of the relevant sets $\mathcal{A}_{i,j}$ and $\mathcal{A}_i$.