On symmetry groups of Boolean and other functions

Eszter K. Horváth, Szeged

Co-authors: Géza Makay, Reinhard Pöschel

Novi Sad, 2012, March 16.

Symmetry group (invariance group)

$f : \{0,1\}^n \to \{0,1\}$, $\sigma \in S_n$

f^σ is defined by $f^\sigma(x_1, \ldots, x_n) := f(x_{\sigma 1}, \ldots, x_{\sigma n})$

σ is called a *symmetry* of f, if $f^\sigma = f$
we denote this by $\sigma \vdash f$

Definition
Let $f : \{0,1,\ldots,k-1\}^n \to \{0,1,\ldots\ k-1\}$. We say that f is invariant under the permutation $\sigma \in S_n$ and write $\sigma \vdash f$, if for all $(x_1, \ldots, x_n) \in \{0,1,\ldots,k-1\}^n$, $f(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n})$.

Representability

All subgroup $G \leq S_n$ is representable as the invariance group of a n-ary function on a k-element set if and only if $k \geq n$.

Threshold functions

A Boolean function is called a *threshold function* if there exist real numbers $w_1, ..., w_n$, t such that

$$f(x_1, \ldots, x_n) = 1 \quad \text{iff} \quad \sum_{i=1}^{n} w_i x_i \geq t.$$

Theorem (E. K. Horváth, 1994.) The invariance group of threshold functions is isomorphic to a direct product of symmetric groups.

Results on symmetry groups

P. Clote and E. Kranakis, *Boolean functions, invariance groups, and parallel complexity*. SIAM J. Comput. 20, (1991), 553–590. 2327,

A. Kisielewicz, *Symmetry groups of Boolean functions and constructions of permutation groups*. J. of Algebra 1998, (1998), 379–403.

B. Wnuk, *On symmetry groups of algebraic operations. (Polish)*. Zeszyty Nauk. Wy. Szkoy Ped. w Opolu Mat., 21 (1980), Algebra, Dydakt. Mat., Geom., Zastos. Mat.2327.

Galois connection

The correspondence $\vdash$ induces a Galois connection between permutations and Boolean functions.

For $F \subseteq O_k^{(n)}$ and $G \subseteq S_n$ let

$$F^{\vdash} := \{\sigma \in S_n \mid \forall f \in F : \sigma \vdash f\}$$

$$G^{\vdash} := \{f \in O_k^{(n)} \mid \forall \sigma \in G : \sigma \vdash f\}$$

$$\overline{F} := (F^{\vdash})^{\vdash}$$

$$\overline{G} := (G^{\vdash})^{\vdash}$$

Galois closed groups

Lemma
The permutation group G is the symmetry group of a (single) k-valued Boolean function for some natural number k if and only if it is Galois closed.

Sketch of Proof
Let $f_i(a) = 1$ if and only if $f(a) = i$ for $i \in \{1, \ldots, k\}$ and $a \in \{0,1\}^n$.

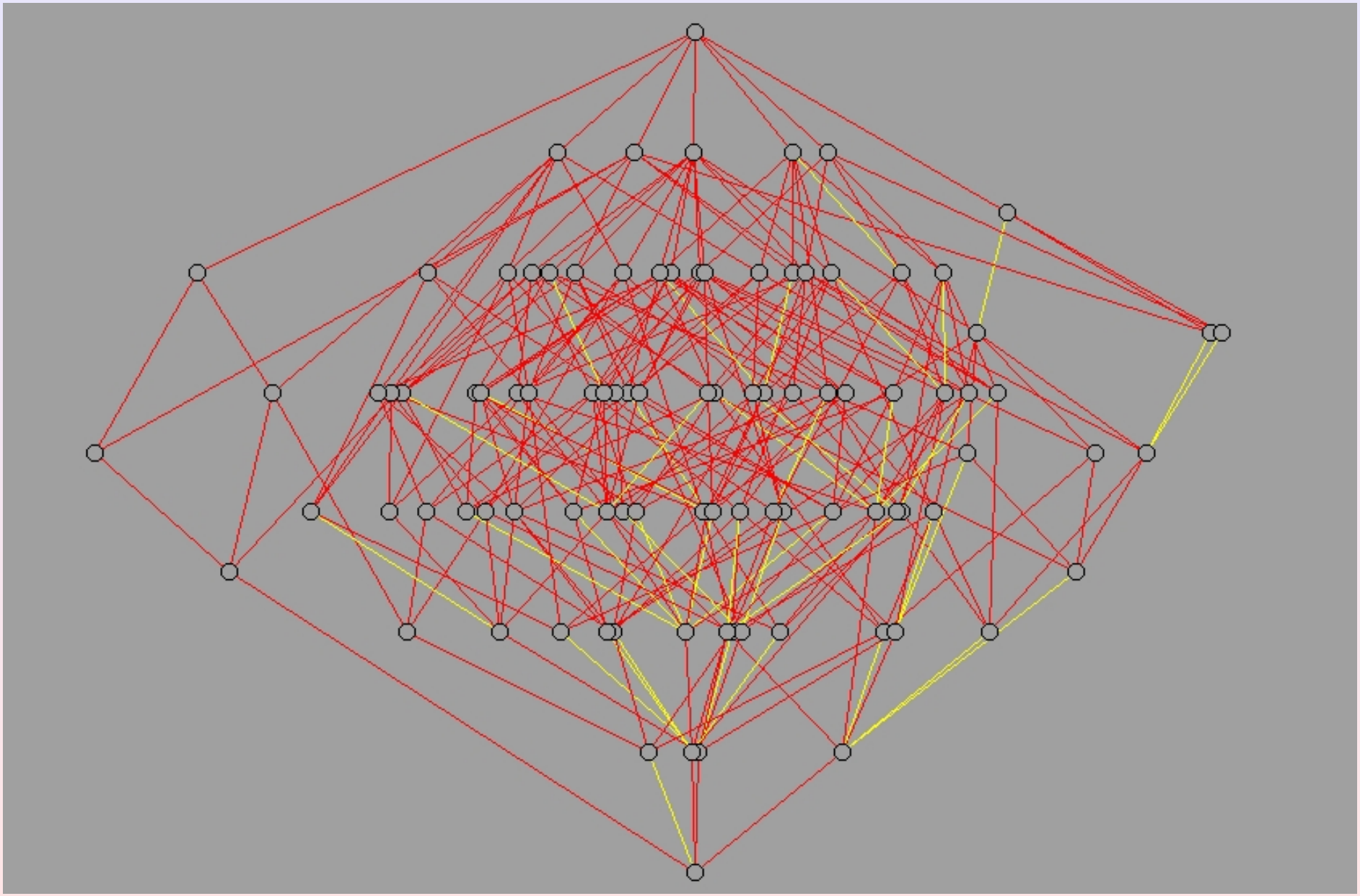
Characterization of the closures

Theorem [K. Kearnes] Let $G \leq S_n$. Then

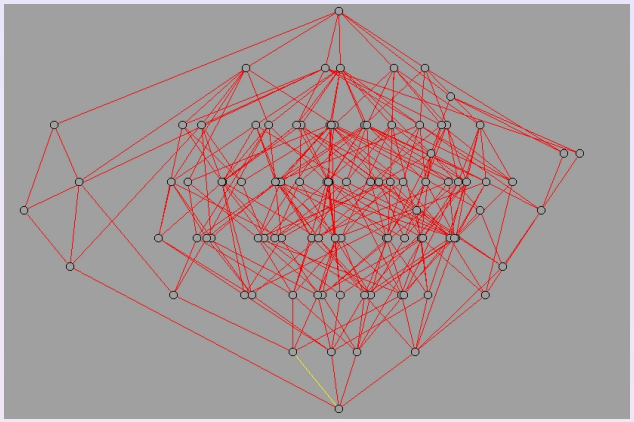
$$\overline{G}^{(k)} = \bigcap_{a \in \{0,1,\ldots,k-1\}^n} (S_n)_a \cdot G,$$

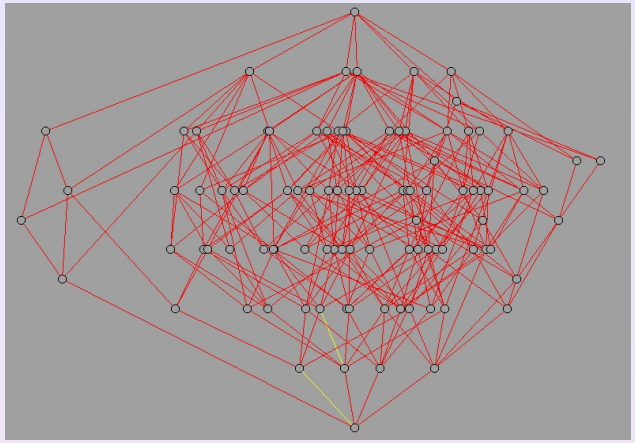
where $(S_n)_a := \{\sigma \in S_n \mid a^\sigma = a\}$ is the stabilizer for $a = (a_1, \ldots, a_n) \in \{0, 1, \ldots, k-1\}^n$.

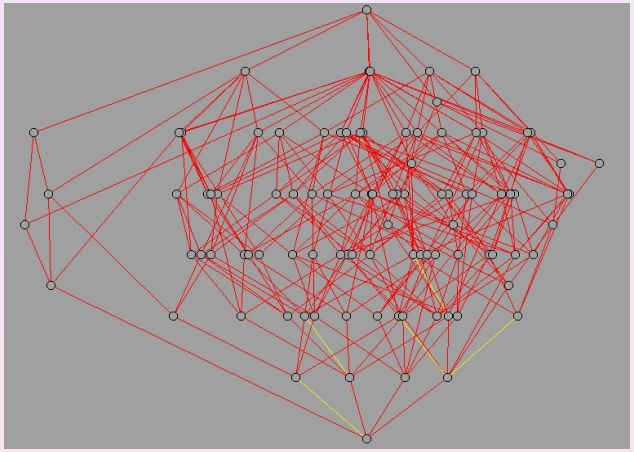
n=7, k=2

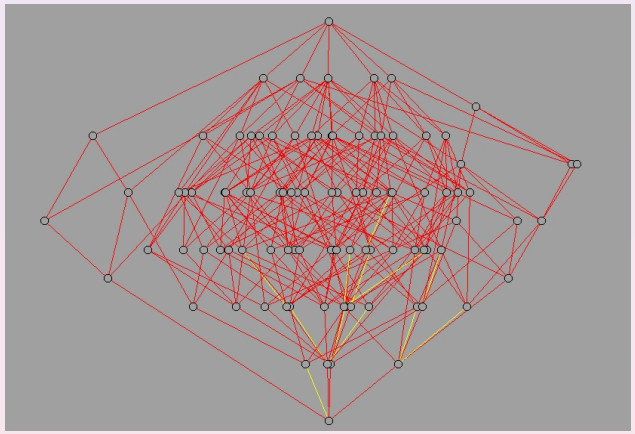


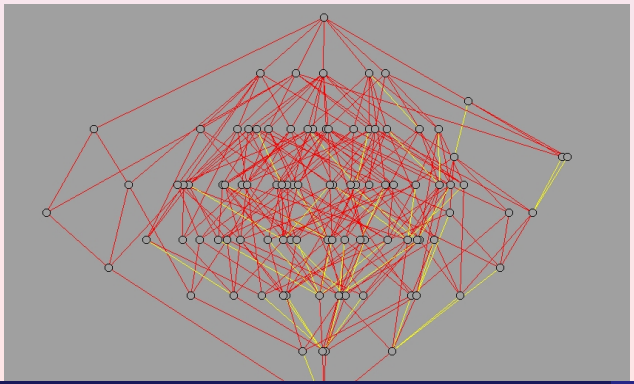
n=7



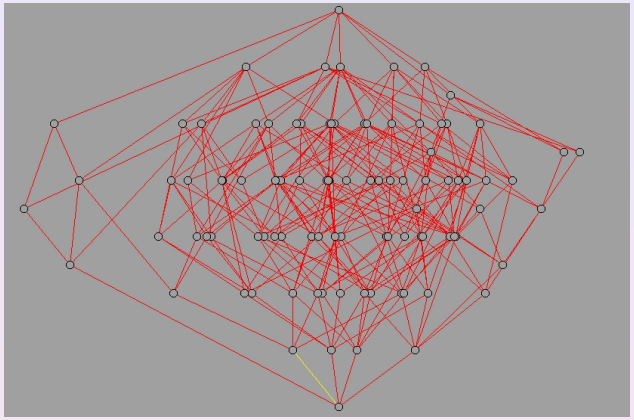


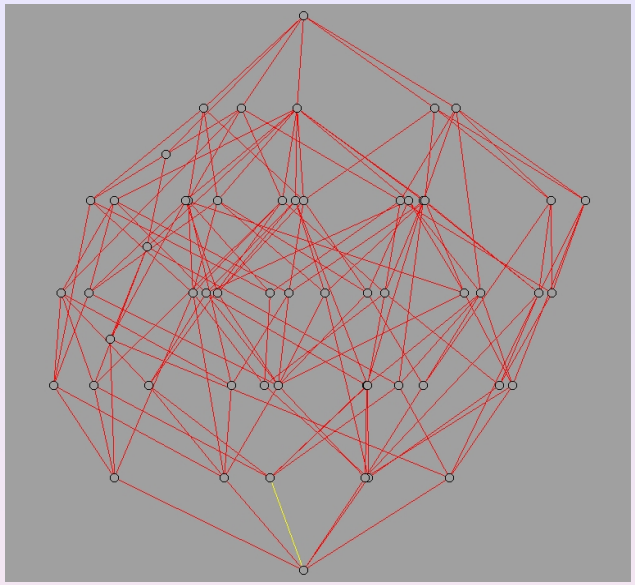


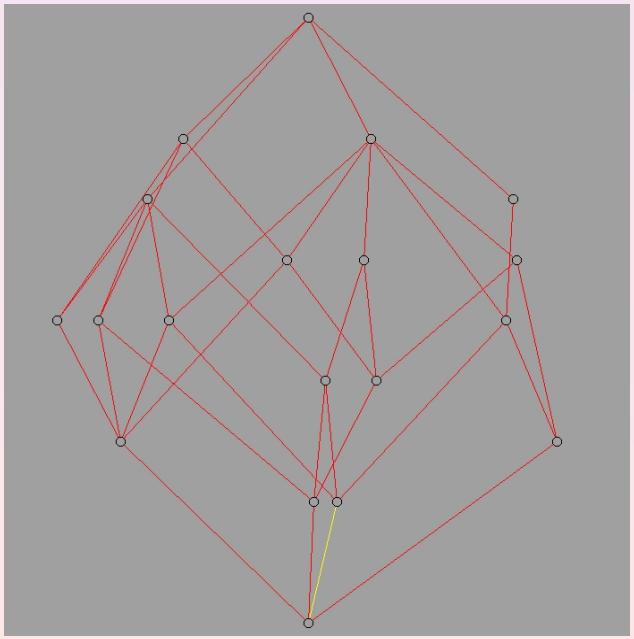


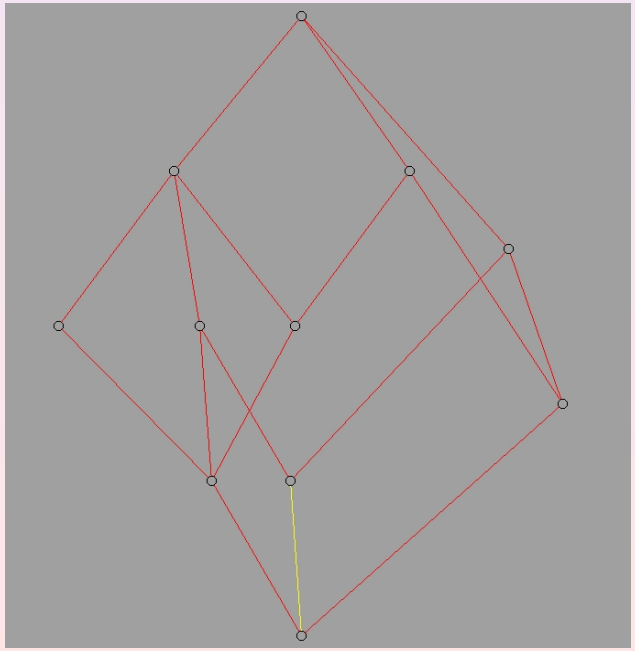


k=n-1









k=n-1

Proposition For $k = n - 1$ each subgroup of S_n except A_n is k-closed.

Proof

Let $a_{(i,j)} = (a_1, \ldots, a_n)$ be an n-tuple from $\{0, 1, \ldots, k-1\}^n$ such that $a_r = a_s \iff \{r, s\} = \{i, j\}$ or $r = s$.

By $\overline{G}^{(k)} = \bigcap_{a \in \{0,1,\ldots,k-1\}^n} (S_n)_a \cdot G$

we have $G \subseteq \overline{G}^{(k)} \subseteq \{\mathbf{id}, (i\,j)\} \cdot G$.

Now, let $G \leq S_n$ be a subgroup which is not k-closed.

Then $\overline{G}^{(k)}$ contains at least one element of the form $(i\,j) \cdot \sigma$ with $\sigma \in G$, and therefore $\overline{G}^{(k)}$ contains $(i\,j) \cdot \sigma \cdot \sigma^{-1} = (i\,j)$. (For all i and j.)

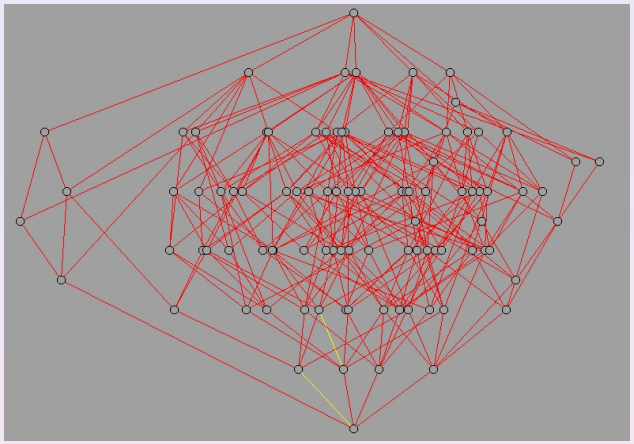
k=n-1

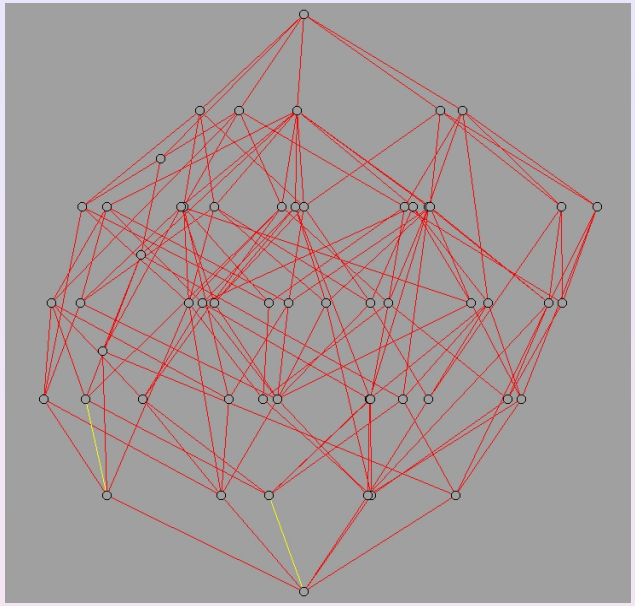
Since i, j were chosen arbitrarily, $\overline{G}^{(k)}$ contains all transpositions, i.e. $\overline{G}^{(k)} = S_n$.

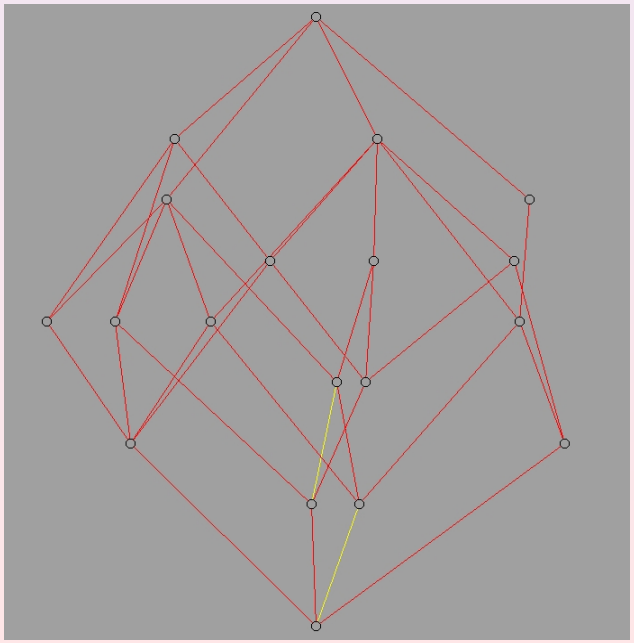
Thus we have $G \leq \overline{G}^{(k)} \subseteq \{\mathbf{id}, (i\,j)\} \cdot G \subseteq S_n = \overline{G}^{(k)}$, i.e., $S_n = \{\mathbf{id}, (i\,j)\} \cdot G$, in particular G is of index 2 in S_n.

The alternating subgroup A_n is the only subgroup of S_n satisfying this.

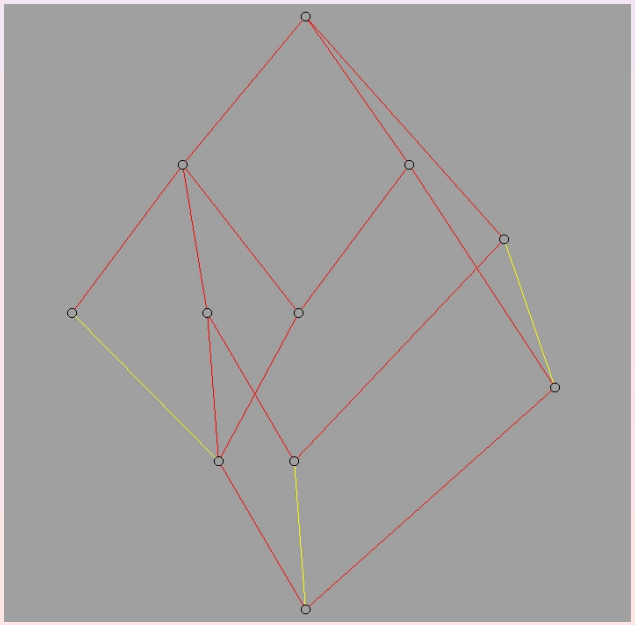
k=n-2







BUT



k=n-2

If G has a common fixed point, say $i \in \{1, \ldots, n\}$, i.e. $i^g = i$ for each $g \in G$, then G can be considered as a subgroup $G^{\downarrow}$ of the full symmetric group $S_{\{1,\ldots,n\}\setminus\{i\}}$ on base set $\{1, \ldots, n\} \setminus \{i\}$.
Conversely, each $H \leq S_{\{1,\ldots,n\}\setminus\{i\}}$ can be embedded canonically into $S_n = S_{\{1,\ldots,n\}}$, yielding $H^{\uparrow} := \{h^{\uparrow} \mid h \in H\}$ with $i^{h\,\uparrow} := i$ and $j^{h^{\uparrow}} := j^h$ for $j \in \{1, \ldots, n\} \setminus \{i\}$.

Clearly, this is one-to-one: $(G^{\downarrow})^{\uparrow} = G$, $(H^{\uparrow})^{\downarrow} = H$ (for each fixed i).

In particular, we consider the alternating group A in $S_{\{1,\ldots,n\}\setminus\{i\}}$ and shall use the notation $A_{n-1,(i)}$ for the subgroup $A^{\uparrow}$ of S_n.

k=n-2

Lemma

For $G = H^{\uparrow} \leq S_n$ and the corresponding $G^{\downarrow} = H \leq S_{\{1,\ldots,n\}\setminus\{i\}}$ we have

$$\overline{G}^{(k)} = (\overline{H}^{(k)})^{\uparrow}.$$

Corollary

Let $k = n-2$ and let $G \leq S_n$ be a subgroup with a common fixed point i, i.e., $G = H^{\uparrow}$ for some $H \leq S_{\{1,\ldots,n\}\setminus\{i\}}$. Then G is not k-closed if and only if $G = A_{n-1,(i)}$. In this case we have

$$\overline{A_{n-1,(i)}}^{(k)} = S^{\uparrow}{}_{\{1,\ldots,n\}\setminus\{i\}}.$$

k=n-2

Theorem
Let $2 \leq k = n-2$. Then the only non-k-closed subgroup of S_n are A_n and $A_{n-1,(1)}, \ldots, A_{n-1,(n)}$.

Proof

Let i, j, s, t be distinct elements of $\{1, \ldots, n\}$ and let $a_{ij;st}$ be an n-tuple $(a_1, \ldots, a_n) \in \{0, 1, \ldots, k-1\}^n$ such $a_i = a_j \neq a_s = a_t$ and all other components have different values.

Analogously, let a_{ijs} denote an n-tuple such that $a_i = a_j = a_s$ and all other components are different.

Thus in both cases $\{a_1, \ldots, a_n\} = \{1, \ldots, n-2\}$.

k=n-2

The stabilizers are the following 4- and 6-element groups:

$$\Gamma_{ij;st} := (S_n)_{a_{ij;st}} = \{e, (ij), (st), (ij)(st)\},$$

$$\Gamma_{ijs} := (S_n)_{a_{ijs}} = \{e, (ij), (is), (js), (ijs), (isj)\} = S_{\{i,j,s\}}.$$

Note that both groups are generated by any two of its elements $\neq e$.

k=n-2

If $\pi \in \overline{G}^{(k)} \setminus G$,
then from $\overline{G}^{(k)} \subseteq \Gamma_{ij;st} \cdot G$ we have that there is a $\gamma \in \Gamma_{ij;st}$ and $\sigma \in G$ with $\pi = \gamma\sigma$,
thus $\gamma^{-1}\pi \in G$ and $\gamma = \pi\sigma^{-1} \in \overline{G}^{(k)} \setminus G$,

more concretely we have

$$(ij) \in \overline{G}^{(k)} \setminus G \text{ and } (ij)\pi \in G$$

$$(st) \in \overline{G}^{(k)} \setminus G \text{ and } (st)\pi \in G$$

$$(ij)(st) \in \overline{G}^{(k)} \setminus G \text{ and } (ij)(st)\pi \in G.$$

k=n-2

Analogously, one gets from $\overline{G}^{(k)} \subseteq \Gamma_{ijs} \cdot G$:

$$(ij) \in \overline{G}^{(k)} \setminus G \text{ and } (ij)\pi \in G$$

$$\text{or } (is) \in \overline{G}^{(k)} \setminus G \text{ and } (is)\pi \in G$$

$$\text{or } (js) \in \overline{G}^{(k)} \setminus G \text{ and } (js)\pi \in G$$

$$\text{or } (ijs) \in \overline{G}^{(k)} \setminus G \text{ and } (ijs)\pi \in G$$

$$\text{or } (isj) \in \overline{G}^{(k)} \setminus G \text{ and } (isj)\pi \in G.$$

k=n-2

Claim 1: G contains no transpositions.

Claim 2: $\forall ij; st : (ij)(st) \notin \overline{G}^{(k)} \setminus G$ (where $\{i,j\} \cap \{s,t\} = \emptyset$ is assumed).

Claim 3: $G = A_n$.