Backtrack:

An algorithm to traverse the tree formed by a stabilizer chain.

Aims: find all/one elements satisfying certain property.

Ex: • Centralizer and Normalizer in permutation groups.

• Conjugating element

• Set stabilizer

• Graph isomorphism

The tree of a Stabilizer Chain C

- root - empty node
- first layer - the representatives of the first transversal
- children of a node at level/depth d -

  - the orbit of transversal $(C, d+1)$ shifted by the corresponding representative to the node

Let $G = \langle (1,2,3,4) =: a,\ (2,3) =: b \rangle$

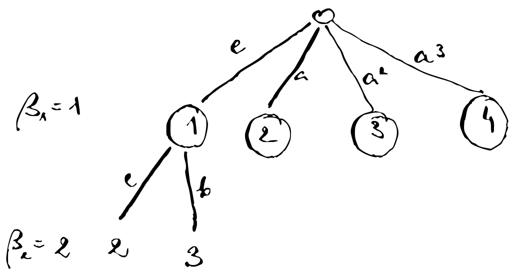
then part of the stabilizer chain looks as follows:

$$\beta_1 = 1;\ S_1 = [a, b],\ T_1 = \begin{cases} [1, 2, 3, 4] \\ [e, a, a^2, a^3] \end{cases}$$

$$\beta_2 = 2;\ S_2 = [a b \overline{ab}^{-1} = a b a^{-2} = b]$$

$$T_2 = \begin{cases} [2, 3] \\ [e, b] \end{cases}$$

Let's look at the search tree:



It is tempting to say that branches under β^g corresponds to $\beta_2^{g r}$ for r in T_2.

however if we choose $g = a^3$

then $\beta_1 = 1 \to 4$, but $\beta_2 = 2 \longrightarrow 1$

which is stabilized by S_2!

(so there'd be only one branch under 4)

Instead we go "bottom up" $\to$

the choice for g influences where β_2 is sent, but in a <u>bijective</u> manner!

ALGORITHM: Backtrack!

INPUT: • L - an (empty) list
• $\mathcal{C}$ - stabilizer chain for $\mathcal{G} = \langle S \rangle$
• $g = e$ - an element of $\mathcal{G}$.
• $d = 1$ - depth

OUTPUT: • L - a list of all elements of $\mathcal{G}$.

```
begin
   T = transversal(C, d)
   for δ ∈ T
      if length(C) = d      // we're in a leaf node
         push g·T[δ] to L
      else
         Backtrack!(L, C, g·T[δ], d+1)
      end
   end
   return L
end
```

• We can add a predicate p and only push when $p(g \cdot T[\delta])$ is satisfied.

• <u>Problem:</u> this runs over all leafs when sometimes whole branches can be discarded by the predicate

• <u>Solution:</u> Add a <u>problem specific</u> <u>oracle</u> for $\delta \in T$ and avoid descendig into the whole branch.

- General procedure:

Given a group G and P, a problem to solve

- find the optimal basis β for the problem
- use the existing SC to complete $SC(\beta)$ (e.g. knowing the order of G helps, there are algorithms for transforming one basis to another)
- use backtrack + check for P to prune the search tree.

Ex. Searching in $Sym(5)$ for g such that

$$(1,2)(3,4,5)^g = (2,4)(1,5,3)$$

$\beta = (1,2,\dots)$

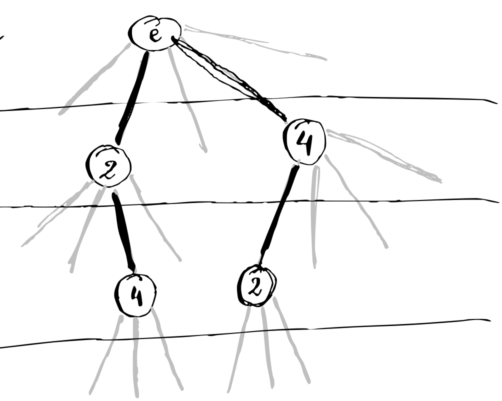
We immediately know that $(1,2) \longrightarrow (2,4)$

$1 \mapsto 2$
$1 \mapsto 4$ are the only acceptable choices.

$\beta_1 = 1$

$\beta_2 = 2$

now



Let $G = \langle \underbrace{(1,3,5,7)(2,4,6,8)}_{a} \;,\; \underbrace{(1,3,8)(4,5,7)}_{b} \rangle$

$\beta_1 = 1 \quad S_1 = [a, b]$

$\Delta_1 = [1, 3, 5, 8, 7, 2, 4, 6]$

$T_1 = [e, a, a^2, ab, a^3, aba, a^3b \;\; a^3ba]$

$b \cdot a^{-1} = \underbrace{(2,8,7)(3,6,4)}$

$\beta_2 = 2, \quad S_2 = [c]$

$\Delta_2 = [2, 8, 7]$

$T_2 = [e, c \;\; c^2]$

---

find $C_G(x)$ for $x = (1,2,4)(5,6,8)$

$C_G(x) = \{ g \in G : xg = gx \}$

1) make sure x is in G:

$\beta_1^x = 1^x = 2 \qquad g_1 = x \cdot \underbrace{(aba)}_{r_1}^{-1}$

$\beta_2^{g} = 2^{g} = 2^{x a^{-1} b^{-1} a^{-1}} = 8$

$(1,2,4)(5,6,8)(1,7,5,3)(2,8,6,4)(1,3,8)(4,5,7)$

$g_2 = g_1 \cdot c^{-1} = g_1 \cdot (ba^{-1})^{-1} = x \cdot a^{-1} b^{-1} \cancel{a^{-1}} \cancel{a} b^{-1} = x \cdot a^{-1} \underline{\underline{b^{-2}}}_{b}$

$= x a^{-1} b$

2) Oracle for the centralizer

condition: g must preserve cycle structure

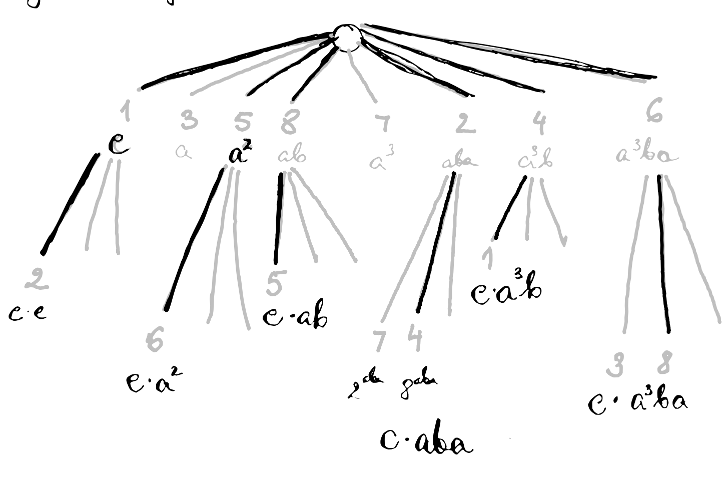
$1 \to 2 \quad \Rightarrow 2 \to 4$

$1 \to 4 \quad \Rightarrow 2 \to 1$

$1 \to 5 \quad \Rightarrow 2 \to 6$

$1 \to 6 \quad \Rightarrow 2 \to 8$

$1 \to 8 \quad \Rightarrow 2 \to 5$



Ex 3: Setwise Stabilizer.

$X \subset \Omega$, $(\beta_1, \dots, \beta_k)$ chosen from X
$\Rightarrow \mathrm{Stab}_{G}(X) \geq G^{(k+1)}$.

Finish the basis and do the backtrack search for $\beta_i^g \in \{\beta_1, \dots, \beta_k\}$ for $i \leq k$.

Ex 4: Conjugating element

x, y - permutations ; $\exists ? g$ s.t. $x^g = g^{-1} x g = y$?

1) Necessary condition - cycle structures of x and y must agree.
2) Pick β_1 in a rare, long cycle of x
   ↳ few possibilities for mapping the cycle
   ↳ it suffices to consider only a single image of β_1 for each cycle of the same length:
   if g conjugates x to y $\Rightarrow$ $g y^k$ does
   ↳ next choices for the basis → subsequent pts on the cycle (their image is determined by β_1^g)

- **Note:** Modern versions of backtrack = "Partition backtrack"
  nodes are partitions of Ω which must map to itself. Every base image added = one element subset + refinement of the other subsets.

Groups defined by properties

- Centralizer, Normalizer
- Set stabilizer
- given $a, b \in G$ are they conjugated?
  If so find all $g \in G$ s.t. $g^{-1}ag = b$.

  Note: if $g^{-1}ag = b$ let's try with $g' = xgy$

  $$g'^{-1}ag' = y^{-1}g^{-1}x^{-1}axgy \underset{\text{if } a \in C_G(a)}{=} y^{-1}g^{-1}agy = y^{-1}by \underset{\text{if } b \in C_G(b)}{=} b$$

  $\Rightarrow$ any solution g comes with $C_G(b)\, g\, C_G(a)$ other solutions.

- Graph isomorphism:
  If $h: A \to B$ is an isomorphism,
  so is every element of $\mathrm{Aut}(A)\, h\, \mathrm{Aut}(B)$.

Finding a subgroup: P

- start with $K = \langle e \rangle$, whenever a new elt g satisfying the predicate (associated to P) is found
  update $K := \langle K, g \rangle$ ← build the stabilizer chain for K along!
- descend down the SC and find $P \cap G^{(i+1)}$ before considering elts from $G^{(i)}$ // depth first search
- this builds a sgs for K $\Rightarrow$
  the tests if a newly found g is in K are cheap!

Lemma:

Suppose that $K = G^{(i)} \cap P$ and N is a node prescribing the image of $(\beta_1, \dots, \beta_i)$. If a child g of N satisfies the predicate of P then we set $K = \langle K, g\rangle$ and we can prune the whole subtree under N.

Proof: any element below N that is in P is also in Kg. (picture proof) $\square$

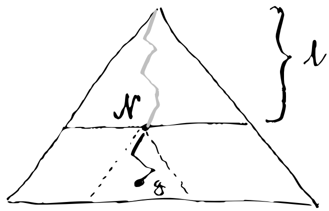
Corollary: When running the backtrack search finding either $g \in P$ or $g \notin P$ is good!
- → if $g \in P$ & $g \notin K \Rightarrow |\langle K, g\rangle| \geq 2|K|$
- → if $g \notin P \Rightarrow$ none of elts in KgK is in P.

Problem: How to test that $h \in KgK$ (for every g found as above)?

Solution: given h find a "canonical representative" of KhK and compare it to the known representatives.

This is hard.

"Canonical" may mean – the least element in KgK when comparing elts by the lexicographical order on $(\beta_1^g, \beta_2^g, \dots)$.



<u>Lemma:</u> Suppose that $K \leq P$ is the group found so far and that $\mathcal{N}$ prescribes the first l-images of β, $(\gamma_1, \dots, \gamma_l)$. If g is a descendant of $\mathcal{N}$, then g is <u>minimal</u> in KgK (in the sense above) if γ_l is <u>minimal</u> in the orbit $\gamma_l^{\mathrm{Stab}_K(\gamma_1, \dots, \gamma_{l-1})}$

<u>Proof:</u>

Suppose that γ_l is not minimal in $\gamma_l^{\mathrm{Stab}_K(\gamma_1, \dots, \gamma_{l-1})}$

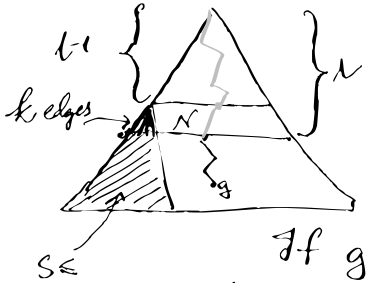
$\Rightarrow \exists\, h \in \mathrm{Stab}_K(\gamma_1, \dots, \gamma_{l-1})$ for which $\gamma_l^h < \gamma_l$

$\Rightarrow \beta_i^{gh} = \gamma_i^h = \gamma_i$ for $i = 1, \dots, l-1$, but

$\beta_l^{gh} = \gamma_l^h < \gamma_l = \beta_l^g$

$\Rightarrow gh \in KgK$ & $gh < g$ in the lex order.

$\lightning$ $\square$



Lemma: Let $K \leq P$, $N \sim (\gamma_1, \dots, \gamma_l)$ be as above.

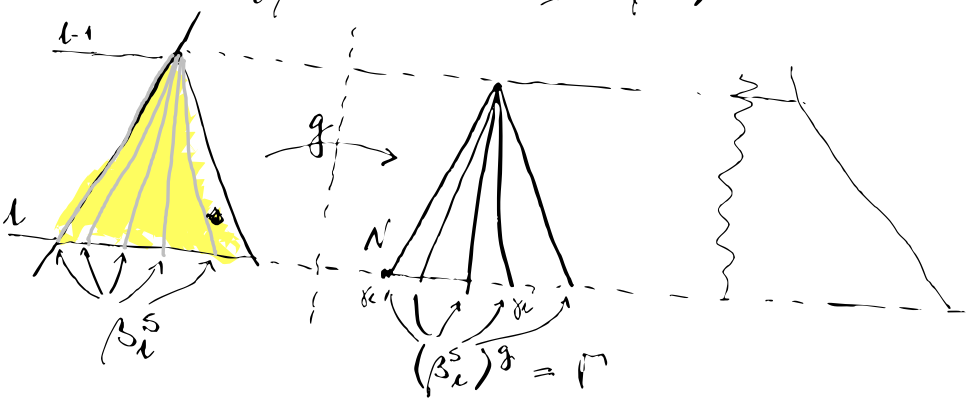
Let $R = \mathrm{Stab}_{\mathcal{G}}(\gamma_1, \dots, \gamma_{l-1})$

$S = \mathrm{Stab}_K(\beta_1, \dots, \beta_{l-1})$

$k = |\beta_l^S|$

If g is a descendant of N and the smallest element of KgK then γ_l is smaller than the $k-1$ last elts of γ_l^R

Let $\Gamma = \{\beta_l^{hg} : h \in S\} = (\beta_l^S)^g$



if γ_l is not minimal in Γ $\Rightarrow$

$\beta_l^{s \cdot g} = \gamma_l' \rightarrow s \cdot g \in Sg \subset Kg \subset KgK$ is smaller than g

Claim:

$\Gamma \subseteq \gamma_l^R$ i.e. γ_l is smaller than all of it its Γ fellows.

Note: $R = \mathrm{Stab}_{\mathcal{G}}(\gamma_1, \dots, \gamma_{l-1}) = g^{-1} \cdot \mathcal{G}^{(l-1)} \cdot g$

If $\gamma \in \Gamma \Rightarrow \gamma = \beta_l^{hg} \Rightarrow \gamma^{\underbrace{g^{-1}h^{-1}g}_{\in R}} = \beta_l^g = \gamma_l$.

where $h \in S$