# Resolution with Small Symmetries

Nikita Gaevoy

Technion – Israel Institute of Technology

April 2, 2024

# Definitions

## Definition

$\varphi \colon \{\text{Lit}\} \to \{\text{Lit}\}$ is a $k$-**symmetry function** iff:

1. It is an automorphism of literals.
2. All variables except $k$ mapped to themselves (i.e. $\varphi(x) = x$).

# Definitions

## Definition

$\varphi\colon \{\text{Lit}\} \to \{\text{Lit}\}$ is a $k$-**symmetry function** iff:

1. It is an automorphism of literals.
2. All variables except $k$ mapped to themselves (i.e. $\varphi(x) = x$).

## Definition

**Resolution with** $k$**-symmetries** has two rules:

1. Resolution rule.

$$\frac{A \vee x \qquad B \vee \neg x}{A \vee B}$$

2. Symmetry rule.

$$\frac{\varphi(B_1), \varphi(B_2), \ldots, \varphi(B_l)}{\varphi(A)}$$

where $\varphi$ is a $k$-symmetry and $B_1, B_2, \ldots, B_l \vdash^* A$ was inferred before.

# Types of symmetries

## Definition

- A **global** symmetry is a symmetry that uses the entire input formula as premises in the symmetry rule.
- A **local** symmetry is a symmetry that uses parts of input formula as premises in the symmetry rule.
- **Dynamic** symmetries have no additional restrictions.

# Types of symmetries

## Definition

- A **global** symmetry is a symmetry that uses the entire input formula as premises in the symmetry rule.
- A **local** symmetry is a symmetry that uses parts of input formula as premises in the symmetry rule.
- **Dynamic** symmetries have no additional restrictions.

- Resolution with global, local and dynamic symmetries are called SRC-I, SRC-II, and SRC-III, correspondingly.

$$\text{SRC-III} \xmapsto{\text{(Arai and Urquhart 2000)}} \text{SRC-II} \xmapsto{\text{(Urquhart 1999)}} \text{SRC-I}$$

# Types of symmetries

## Definition

- A **global** symmetry is a symmetry that uses the entire input formula as premises in the symmetry rule.
- A **local** symmetry is a symmetry that uses parts of input formula as premises in the symmetry rule.
- **Dynamic** symmetries have no additional restrictions.

- Resolution with global, local and dynamic symmetries are called SRC-I, SRC-II, and SRC-III, correspondingly.

$$\text{SRC-III} \xmapsto{\text{(Arai and Urquhart 2000)}} \text{SRC-II} \xmapsto{\text{(Urquhart 1999)}} \text{SRC-I}$$

- Any formula that is hard for Resolution can be transformed into a formula that is hard for SRC-II (Szeider 2005).
- Superpolynomial lower bounds for SRC-III is a long-standing open problem.

# Example

$$(x_1 \vee x_7) \wedge (x_2 \vee \neg x_7) \wedge (x_3 \vee \neg x_2) \wedge (\neg x_1 \vee x_7) \wedge (x_4 \vee \neg x_7) \wedge (x_5 \vee \neg x_4) \wedge (x_4 \vee x_6)$$

- Use the resolution rule:

$$\dfrac{\dfrac{x_1 \vee x_7 \qquad x_2 \vee \neg x_7}{x_1 \vee x_2} \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$$

# Example

$$(x_1 \vee x_7) \wedge (x_2 \vee \neg x_7) \wedge (x_3 \vee \neg x_2) \wedge (\neg x_1 \vee x_7) \wedge (x_4 \vee \neg x_7) \wedge (x_5 \vee \neg x_4) \wedge (x_4 \vee x_6)$$

- Use the resolution rule:

$$\frac{\dfrac{x_1 \vee x_7 \qquad x_2 \vee \neg x_7}{x_1 \vee x_2} \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$$

- Use a local 5-symmetry that negates $x_1$ and swaps $x_2 \leftrightarrow x_4$ and $x_3 \leftrightarrow x_5$:

$$\frac{\neg x_1 \vee x_7 \qquad x_4 \vee \neg x_7 \qquad x_5 \vee \neg x_4}{\neg x_1 \vee x_5}$$

# Example

$$(x_1 \vee x_7) \wedge (x_2 \vee \neg x_7) \wedge (x_3 \vee \neg x_2) \wedge (\neg x_1 \vee x_7) \wedge (x_4 \vee \neg x_7) \wedge (x_5 \vee \neg x_4) \wedge (x_4 \vee x_6)$$

- Use the resolution rule:

$$\dfrac{\dfrac{x_1 \vee x_7 \qquad x_2 \vee \neg x_7}{x_1 \vee x_2} \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$$

- Use a local 5-symmetry that negates $x_1$ and swaps $x_2 \leftrightarrow x_4$ and $x_3 \leftrightarrow x_5$:

$$\dfrac{\neg x_1 \vee x_7 \qquad x_4 \vee \neg x_7 \qquad x_5 \vee \neg x_4}{\neg x_1 \vee x_5}$$

- This symmetry is not global because of the last clause.

# Example

$$(x_1 \vee x_7) \wedge (x_2 \vee \neg x_7) \wedge (x_3 \vee \neg x_2) \wedge (\neg x_1 \vee x_7) \wedge (x_4 \vee \neg x_7) \wedge (x_5 \vee \neg x_4) \wedge (x_4 \vee x_6)$$

- Use the resolution rule:

$$\frac{\dfrac{x_1 \vee x_7 \qquad x_2 \vee \neg x_7}{x_1 \vee x_2} \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$$

- Use a local 5-symmetry that negates $x_1$ and swaps $x_2 \leftrightarrow x_4$ and $x_3 \leftrightarrow x_5$:

$$\frac{\neg x_1 \vee x_7 \qquad x_4 \vee \neg x_7 \qquad x_5 \vee \neg x_4}{\neg x_1 \vee x_5}$$

- This symmetry is not global because of the last clause.
- Infer $\dfrac{x_3 \vee \neg x_2 \qquad x_1 \vee x_2 \qquad \neg x_1 \vee x_5}{x_3 \vee x_5}$ by applying to the inference of $\neg x_1 \vee x_5$ a dynamic 5-symmetry $\varphi$ defined as follows:

$$\varphi(x_1) = \neg x_3 \qquad \varphi(x_3) = x_4$$
$$\varphi(x_7) = \neg x_2 \qquad \varphi(x_2) = \neg x_7$$
$$\varphi(x_4) = x_1$$

# Connection to the practice

- Many sets of practical formulas have symmetries. One example is formulas that emerge from bounded model checking.
- Two main approaches to exploiting those symmetries in CDCL-based solvers are:
  - Symmetry breaking (Puget 1993; Sakallah 2009).
  - Symmetry handling, also known as symmetry exploitation (Devriendt, Bogaerts, and Bruynooghe 2017; Ivrii and Strichman 2021).

# Connection to the practice

- Many sets of practical formulas have symmetries. One example is formulas that emerge from bounded model checking.
- Two main approaches to exploiting those symmetries in CDCL-based solvers are:
  - Symmetry breaking (Puget 1993; Sakallah 2009).
  - Symmetry handling, also known as symmetry exploitation (Devriendt, Bogaerts, and Bruynooghe 2017; Ivrii and Strichman 2021).

| Symmetry breaking | Symmetry handling |
|---|---|
| Adds clauses that “break” symmetries | Adds clauses that are symmetric to the inferred ones |
| Maintains equisatisfiability, but removes satisfying assignments | Preserves the set of satisfying assignments |
| Restricted to global symmetries | Works with local and dynamic symmetries |
| Usually performs better when suitable | Essential for the best results in some specialized cases |

# The power of small symmetries

Preliminary results:

- Resolution with global $\mathcal{O}(\log n)$-symmetries polynomially refutes the binary pigeonhole principle, which is hard for SDT (decision trees with symmetries).

# The power of small symmetries

Preliminary results:

- Resolution with global $\mathcal{O}(\log n)$-symmetries polynomially refutes the binary pigeonhole principle, which is hard for SDT (decision trees with symmetries).
- Resolution with local 3-symmetries (or global 4-symmetries) polynomially refutes Tseitin formulas on a rectangle grid, which are hard for constant-depth Frege.

# Syntactic version of Resolution with symmetries

- Proofs lines ("entries"): $\langle \text{clause } C, \text{symmetry graph } G \rangle$.

# Syntactic version of Resolution with symmetries

- Proofs lines ("entries"): $\langle$clause $C$, symmetry graph $G\rangle$.
- Symmetry graphs are directed acyclic graphs with the following properties:
  - Each vertex of the graph is labeled with a symmetry.
  - There is a source (every other vertex is reachable from it).
  - The source is labeled with the trivial symmetry.
- Going along an edge in a symmetry graph corresponds to applying the symmetry function of the head of this edge to the clause.

# Syntactic version of Resolution with symmetries

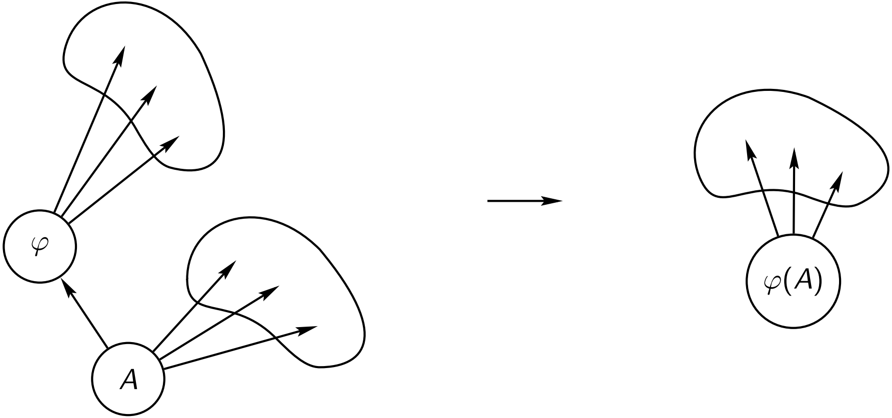
- Proofs lines ("entries"): $\langle \text{clause } C, \text{symmetry graph } G \rangle$.
- Symmetry graphs are directed acyclic graphs with the following properties:
  - Each vertex of the graph is labeled with a symmetry.
  - There is a source (every other vertex is reachable from it).
  - The source is labeled with the trivial symmetry.
- Going along an edge in a symmetry graph corresponds to applying the symmetry function of the head of this edge to the clause.
- Inference rules are:
  - The resolution rule: $\dfrac{\langle A \vee x, G \rangle \qquad \langle B \vee \neg x, G \rangle}{\langle A \vee B, G \rangle}$.
  - A set of rules that modify the symmetry graphs.

# Syntactic version of Resolution with symmetries

- Proofs lines ("entries"): $\langle \text{clause } C, \text{symmetry graph } G\rangle$.
- Symmetry graphs are directed acyclic graphs with the following properties:
  - Each vertex of the graph is labeled with a symmetry.
  - There is a source (every other vertex is reachable from it).
  - The source is labeled with the trivial symmetry.
- Going along an edge in a symmetry graph corresponds to applying the symmetry function of the head of this edge to the clause.
- Inference rules are:
  - The resolution rule: $\dfrac{\langle A \vee x, G\rangle \qquad \langle B \vee \neg x, G\rangle}{\langle A \vee B, G\rangle}$.
  - A set of rules that modify the symmetry graphs.
- Proof size measures (equivalent):
  - The number of entries.
  - The total bit length.

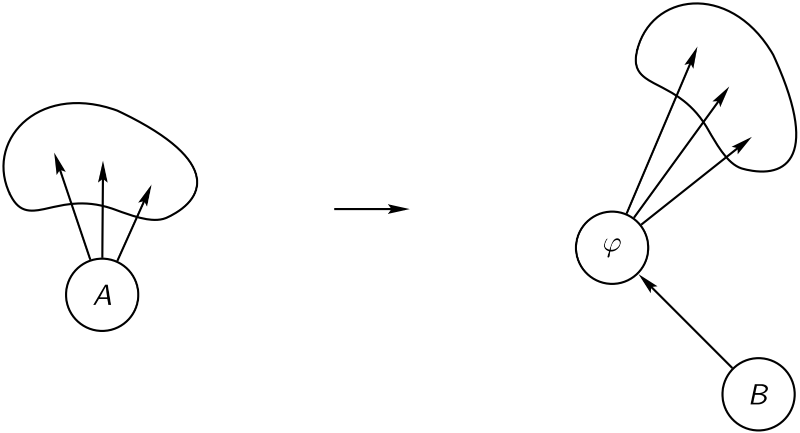
# Symmetry rule

Let $A$ be a clause, and $\varphi$ be a symmetry function.



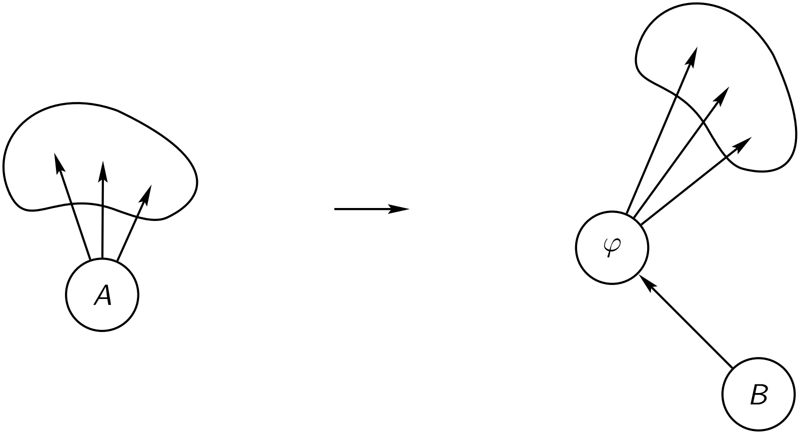
# Edge addition

Let $A$ and $B$ be clauses, and $\varphi$ be a symmetry function such that $\varphi(B) = A$.



# Edge addition

Let $A$ and $B$ be clauses, and $\varphi$ be a symmetry function such that $\varphi(B) = A$.

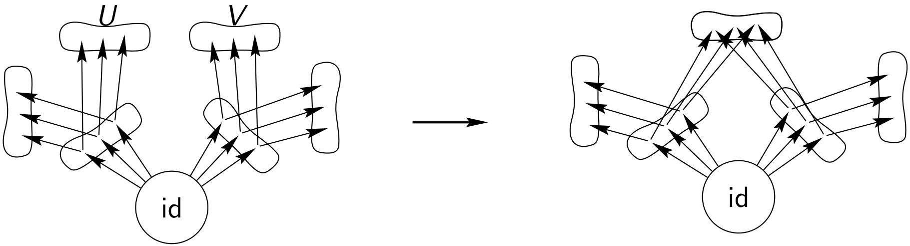



To make this rule the inverse of the symmetry rule, we add the graph combining rule:

$$\frac{\langle C, G\rangle \qquad \langle C, H\rangle}{\langle C, (G+H)/_{\mathrm{src}(G)=\mathrm{src}(H)}\rangle}$$

# Gluing rule

Assume that $V$ and $U$ are isomorphic subgraphs of the symmetry graph.



# 1-symmetries

- The syntactic version allows us to formulate restrictions on interactions between symmetries.

# 1-symmetries

- The syntactic version allows us to formulate restrictions on interactions between symmetries.
- For example, we can restrict us to layered graphs (i.e., graphs with a rank-function $\rho$ on vertices such that an edge $v \to u$ exists iff $\rho(v) < \rho(u)$).
- Resolution with 1-symmetries with this additional restriction forms* a new proof system that we call $G_2$-Frege.

# 1-symmetries

- The syntactic version allows us to formulate restrictions on interactions between symmetries.
- For example, we can restrict us to layered graphs (i.e., graphs with a rank-function $\rho$ on vertices such that an edge $v \to u$ exists iff $\rho(v) < \rho(u)$).
- Resolution with 1-symmetries with this additional restriction forms* a new proof system that we call $G_2$-Frege.
- An alternative definition of $G_2$-Frege:
  - $G_2(x_1, x_2, \ldots, x_k) := \sum_j x_j \geq 2$.
  - Proof lines are disjunctions of literals and $G_2$-functions with the additional property that each literal can participate in each lemma only once.
  - The inference rules are the resolution rule and the distributive law for the **last** $G_2$-function.

# 1-symmetries

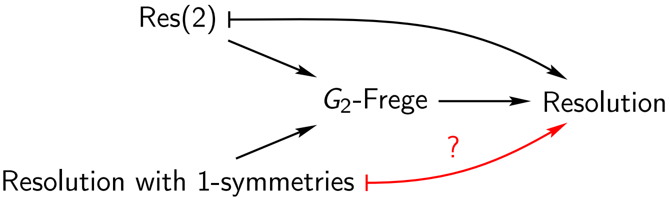
- The syntactic version allows us to formulate restrictions on interactions between symmetries.
- For example, we can restrict us to layered graphs (i.e., graphs with a rank-function $\rho$ on vertices such that an edge $v \to u$ exists iff $\rho(v) < \rho(u)$).
- Resolution with 1-symmetries with this additional restriction forms* a new proof system that we call $G_2$-Frege.
- An alternative definition of $G_2$-Frege:
    - $G_2(x_1, x_2, \ldots, x_k) := \sum_j x_j \geq 2$.
    - Proof lines are disjunctions of literals and $G_2$-functions with the additional property that each literal can participate in each lemma only once.
    - The inference rules are the resolution rule and the distributive law for the **last** $G_2$-function.
- Examples of the inference rules:

$$\frac{G_2(x, y) \vee z \vee t \qquad G_2(x, y) \vee \neg t}{G_2(x, y) \vee z} \qquad \frac{G_2(x, y) \vee G_2(z, t, s)}{G_2(x, y) \vee z \vee t \vee \neg s}$$

$$\frac{G_2(x, y) \vee z \vee t \qquad G_2(x, y) \vee \neg z \vee t \qquad G_2(x, y) \vee z \vee \neg t}{G_2(x, y) \vee G_2(z, t)}$$

# 1-symmetries

- The syntactic version allows us to formulate restrictions on interactions between symmetries.
- For example, we can restrict us to layered graphs (i.e., graphs with a rank-function $\rho$ on vertices such that an edge $v \to u$ exists iff $\rho(v) < \rho(u)$).
- Resolution with 1-symmetries with this additional restriction forms* a new proof system that we call $G_2$-Frege.
- An alternative definition of $G_2$-Frege:
  - $G_2(x_1, x_2, \ldots, x_k) := \sum_j x_j \geq 2$.
  - Proof lines are disjunctions of literals and $G_2$-functions with the additional property that each literal can participate in each lemma only once.
  - The inference rules are the resolution rule and the distributive law for the **last** $G_2$-function.
- $G_2$-Frege is p-simulated by Res(2).



# Further research

1. Proving lower bounds for Resolution with 1-symmetries and then generalizing them to bigger symmetries. How does the power of Resolution with $k$-symmetries depend on the value of $k$?

# Further research

1. Proving lower bounds for Resolution with 1-symmetries and then generalizing them to bigger symmetries. How does the power of Resolution with $k$-symmetries depend on the value of $k$?
2. Finding a proof system stronger than Resolution that is simple enough to be simulated by symmetry handling techniques but also oblivious to the formula encoding.

# Further research

1. Proving lower bounds for Resolution with 1-symmetries and then generalizing them to bigger symmetries. How does the power of Resolution with $k$-symmetries depend on the value of $k$?
2. Finding a proof system stronger than Resolution that is simple enough to be simulated by symmetry handling techniques but also oblivious to the formula encoding.
3. Constructing practical symmetry handling heuristics for the special classes of formulas with suitable structures of symmetries.