Resolution with Small Symmetries

Nikita Gaevoy

Technion – Israel Institute of Technology

April 2, 2024

Definitions

Definition

A mapping φ of literals into literals is a k-symmetry if and only if it satisfies the following two conditions:

1. $\varphi(\neg x) = \neg\varphi(x)$.
2. All variables except k mapped into themselves (i.e. $\varphi(x) = x$).

Definitions

Definition

A mapping φ of literals into literals is a k-symmetry if and only if it satisfies the following two conditions:

1. $\varphi(\neg x) = \neg\varphi(x)$.
2. All variables except k mapped into themselves (i.e. $\varphi(x) = x$).

Definition

Resolution with k-symmetries is a proof system with the following 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 φ 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 of the entire input formula.
- A local symmetry is a symmetry of a part of the input formula.
- A dynamic symmetry is a symmetry of any set of clauses, both from the input formula and inferred.

Types of symmetries

Definition

- A global symmetry is a symmetry of the entire input formula.
- A local symmetry is a symmetry of a part of the input formula.
- A dynamic symmetry is a symmetry of any set of clauses, both from the input formula and inferred.

- Global symmetries are strictly weaker than local symmetries, which are weaker than dynamic symmetries.
- The lower bounds for Resolution with static (i.e., global and local) symmetries are known (Arai and Urquhart 2000; Szeider 2005), but for Resolution with dynamic symmetries, it is a long-standing open problem.

Example

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

- Use the resolution rule: $\dfrac{x_1 \vee x_2 \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$.

Example

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

- Use the resolution rule: $\dfrac{x_1 \vee x_2 \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$.
- Use a local 5-symmetry that negates x_1 and swaps $x_2 \leftrightarrow x_4$ and $x_3 \leftrightarrow x_5$: $\dfrac{\neg x_1 \vee x_4 \qquad x_5 \vee \neg x_4}{\neg x_1 \vee x_5}$.

Example

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

- Use the resolution rule: $\dfrac{x_1 \vee x_2 \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$.
- Use a local 5-symmetry that negates x_1 and swaps $x_2 \leftrightarrow x_4$ and $x_3 \leftrightarrow x_5$: $\dfrac{\neg x_1 \vee x_4 \qquad x_5 \vee \neg x_4}{\neg x_1 \vee x_5}$.
- This symmetry is not global because of the last clause.

Example

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

- Use the resolution rule: $\dfrac{x_1 \vee x_2 \qquad x_3 \vee \neg x_2}{x_1 \vee x_3}$.
- Use a local 5-symmetry that negates x_1 and swaps $x_2 \leftrightarrow x_4$ and $x_3 \leftrightarrow x_5$: $\dfrac{\neg x_1 \vee x_4 \qquad x_5 \vee \neg x_4}{\neg x_1 \vee x_5}$.
- This symmetry is not global because of the last clause.
- Infer $\dfrac{x_1 \vee x_3 \qquad \neg x_1 \vee x_5}{x_3 \vee x_5}$ by applying to the inference of $\neg x_1 \vee x_5$ a dynamic 3-symmetry φ defined as follows:

$$\begin{aligned}\varphi(x_4) &= x_1\\ \varphi(x_1) &= \neg x_3\\ \varphi(x_3) &= x_4\end{aligned}$$

Connection to the practice

- Many sets of practical formulas have symmetries. One example is the formulas that emerge from bounded model checking.
- Two main approaches to exploiting those symmetries are symmetry breaking (Sakallah 2009) and 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 the formulas that emerge from bounded model checking.
- Two main approaches to exploiting those symmetries are symmetry breaking (Sakallah 2009) and 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
Preserves only the satisfiability of the formula	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

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

The power of small symmetries

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

Syntactic version of Resolution with symmetries

- Proofs in our new proof system consist of entries. Each entry is a pair of a clause and a symmetry graph $\langle C, G \rangle$.

Syntactic version of Resolution with symmetries

- Proofs in our new proof system consist of entries. Each entry is a pair of a clause and a symmetry graph $\langle C, G \rangle$.
- Symmetry graphs are directed acyclic graphs with the following properties:
  - Each vertex of the graph is labeled with a symmetry.
  - There is a vertex, which we call the source, such that every other vertex is reachable from it. The source is labeled with the trivial symmetry.
- Going along the edges in a symmetry graph corresponds to applying symmetries to the clause.

Syntactic version of Resolution with symmetries

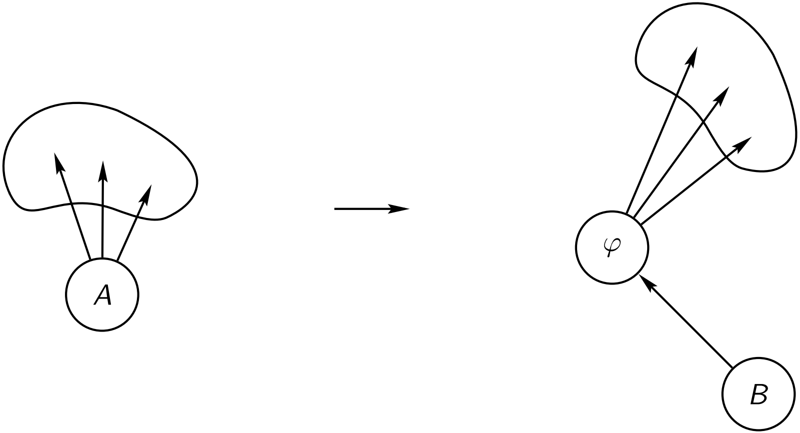
- Proofs in our new proof system consist of entries. Each entry is a pair of a clause and a symmetry graph $\langle C, G\rangle$.
- Symmetry graphs are directed acyclic graphs with the following properties:
  - Each vertex of the graph is labeled with a symmetry.
  - There is a vertex, which we call the source, such that every other vertex is reachable from it. The source is labeled with the trivial symmetry.
- Going along the edges in a symmetry graph corresponds to applying symmetries to the clause.
- Inference rules are:
  - The resolution rule: $\dfrac{\langle A \vee x, G\rangle \qquad \langle B \vee \neg x, G\rangle}{\langle B \vee B, G\rangle}$.
  - A set of rules that modify the symmetry graphs.

Syntactic version of Resolution with symmetries

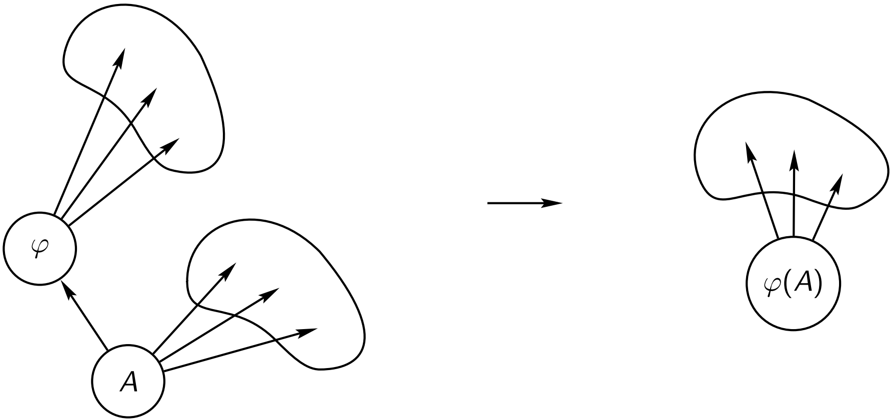
- Proofs in our new proof system consist of entries. Each entry is a pair of a clause and a symmetry graph $\langle C, G \rangle$.
- Symmetry graphs are directed acyclic graphs with the following properties:
  - Each vertex of the graph is labeled with a symmetry.
  - There is a vertex, which we call the source, such that every other vertex is reachable from it. The source is labeled with the trivial symmetry.
- Going along the edges in a symmetry graph corresponds to applying symmetries to the clause.
- Inference rules are:
  - The resolution rule: $\dfrac{\langle A \vee x, G \rangle \qquad \langle B \vee \neg x, G \rangle}{\langle B \vee B, G \rangle}$.
  - A set of rules that modify the symmetry graphs.
- The size of the proof could be measured both as the number of entries and as the total length of those entries.

Edge addition

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

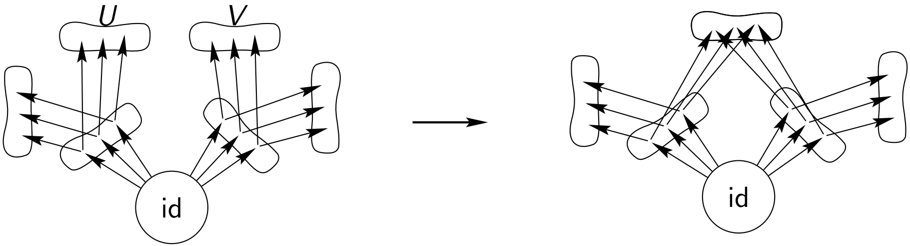


Symmetry rule



Gluing rule

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



1-symmetries

- The syntactic version of Resolution with symmetries allows us to add restrictions on how the symmetries interact.

1-symmetries

- The syntactic version of Resolution with symmetries allows us to add restrictions on how the symmetries interact.
- For example, we can add a restriction that the graph should be layered (i.e., have a rank-function ρ 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 of Resolution with symmetries allows us to add restrictions on how the symmetries interact.
- For example, we can add a restriction that the graph should be layered (i.e., have a rank-function ρ 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 is the threshold function checking that at least two of its inputs are set to true.
  - Lemmas are disjunctions of 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 conjunction.

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

1-symmetries

- The syntactic version of Resolution with symmetries allows us to add restrictions on how the symmetries interact.
- For example, we can add a restriction that the graph should be layered (i.e., have a rank-function ρ 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 is the threshold function checking that at least two of its inputs are set to true.
  - Lemmas are disjunctions of 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 conjunction.

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

- 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 the power of Resolution with k-symmetries depends on the value of k?

Further research

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

Further research

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