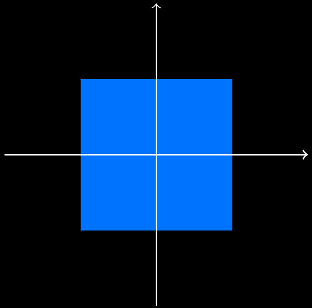
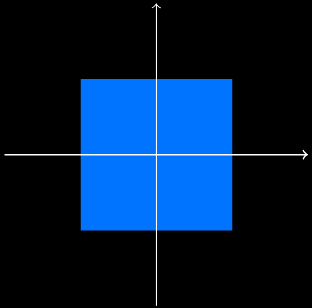
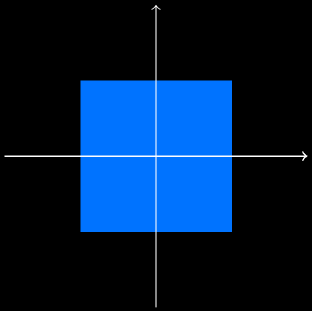
SYMMETRY BREAKING FOR QUANTIFIED BOOLEAN FORMULAS

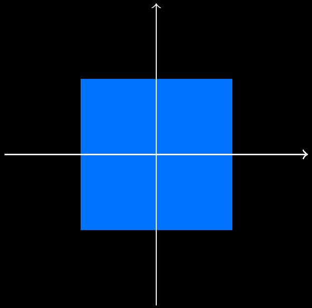
Manuel Kauers · JKU

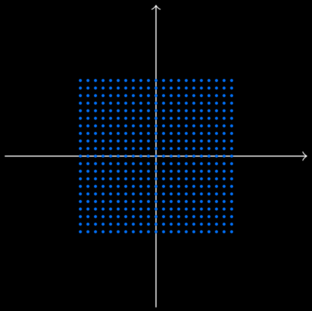
Joint work with Martina Seidl (SAT'18)

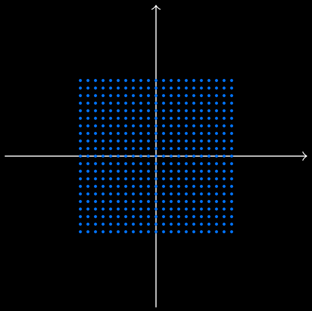












- The square is a certain subset of the plane $\mathbb{R}^2$

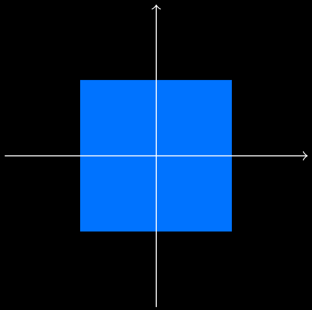
- The square is a certain subset of the plane $\mathbb{R}^2$
- A symmetry of the square is a bijective function $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ which preserves the square

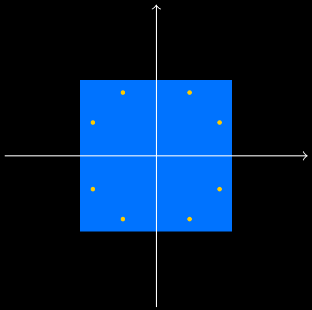
- The square is a certain subset of the plane $\mathbb{R}^2$
- A symmetry of the square is a bijective function $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ which preserves the square
- Symmetries form a group with composition

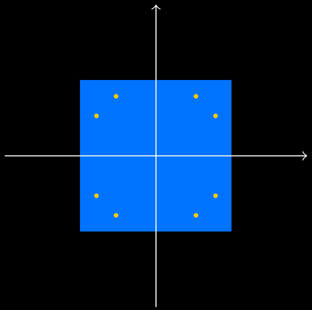
- The square is a certain subset of the plane $\mathbb{R}^2$
- A symmetry of the square is a bijective function $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ which preserves the square
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of "easy" symmetries, for example, linear transformations

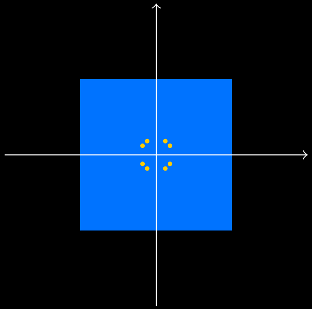
- The square is a certain subset of the plane $\mathbb{R}^2$
- A symmetry of the square is a bijective function $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ which preserves the square
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of "easy" symmetries, for example, linear transformations
- Any such a subgroup splits the square into orbits

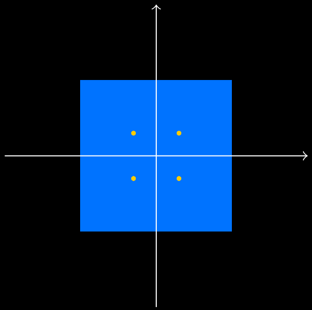
- The square is a certain subset of the plane $\mathbb{R}^2$
- A symmetry of the square is a bijective function $f\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ which preserves the square
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of "easy" symmetries, for example, linear transformations
- Any such a subgroup splits the square into orbits
- An orbit is a set of points which can be mapped to one another by a symmetry

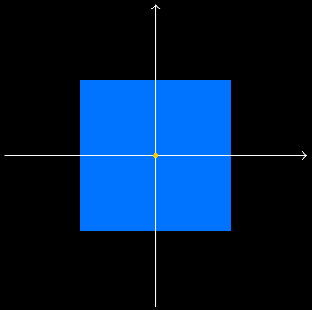













00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111


00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111

- A symmetry of a set of bit strings is a bijection $\{0,1\}^n \to \{0,1\}^n$ which maps the set to itself

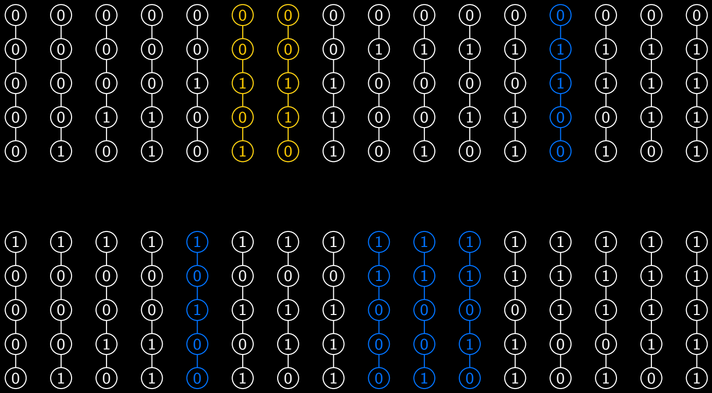
- A symmetry of a set of bit strings is a bijection $\{0,1\}^n \to \{0,1\}^n$ which maps the set to itself
- Symmetries form a group with composition

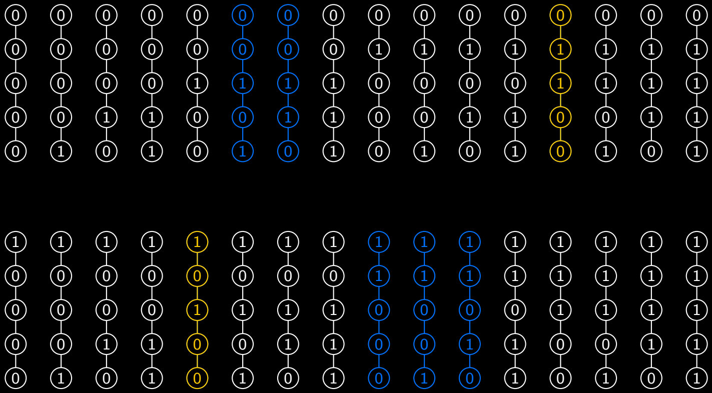
- A symmetry of a set of bit strings is a bijection $\{0,1\}^n \to \{0,1\}^n$ which maps the set to itself
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of “easy” symmetries, for example, only permuting or flipping coordinates

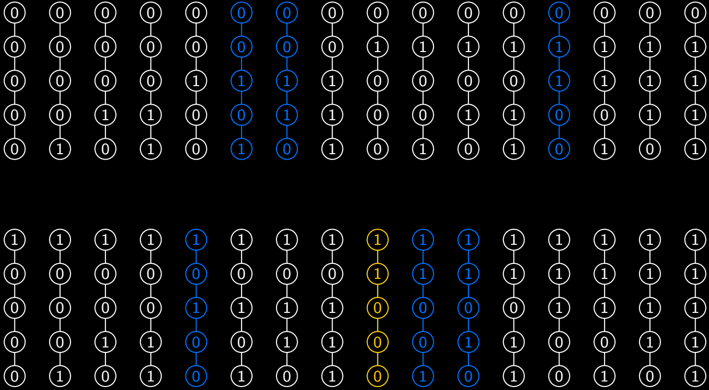
- A symmetry of a set of bit strings is a bijection $\{0,1\}^n \to \{0,1\}^n$ which maps the set to itself
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of “easy” symmetries, for example, only permuting or flipping coordinates
- Any such subgroup splits the set into orbits

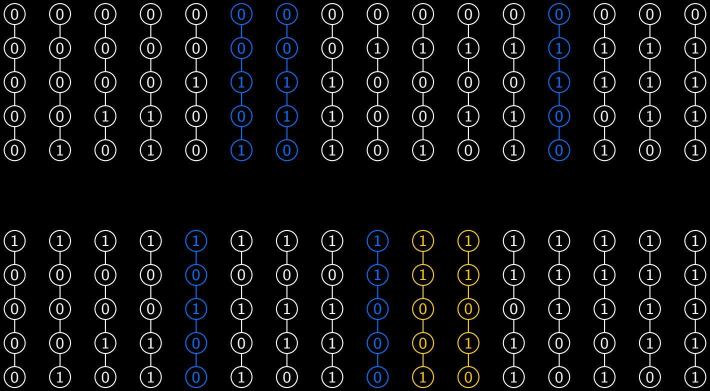
- A symmetry of a set of bit strings is a bijection $\{0,1\}^n \to \{0,1\}^n$ which maps the set to itself
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of "easy" symmetries, for example, only permuting or flipping coordinates
- Any such subgroup splits the set into orbits
- An orbit is a set of bit strings which can be mapped to one another by a symmetry


00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111

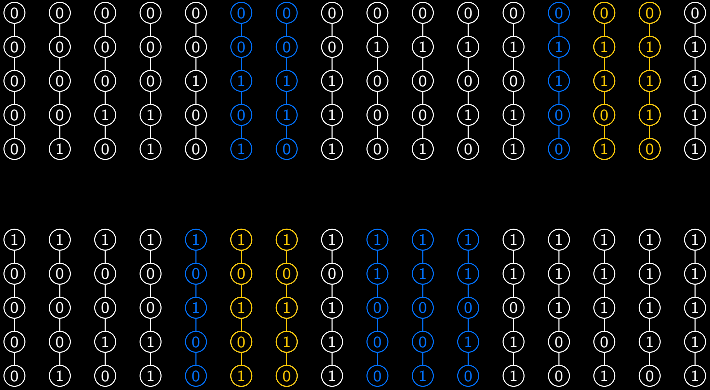

00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111


00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111




00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111


00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111


00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
10000
10001
10010
10011
10100
10101
10110
10111
11000
11001
11010
11011
11100
11101
11110
11111

- Let Σ be a set of (unquantified) Boolean formulas, and $\phi \in \Sigma$.

- Let Σ be a set of (unquantified) Boolean formulas, and $\phi \in \Sigma$.
- A symmetry of ϕ is a bijection $\Sigma \to \Sigma$ which maps ϕ to an equivalent formula

- Let Σ be a set of (unquantified) Boolean formulas, and $\phi \in \Sigma$.
- A symmetry of ϕ is a bijection $\Sigma \to \Sigma$ which maps ϕ to an equivalent formula
- Symmetries form a group with composition

- Let Σ be a set of (unquantified) Boolean formulas, and $\phi \in \Sigma$.
- A symmetry of ϕ is a bijection $\Sigma \to \Sigma$ which maps ϕ to an equivalent formula
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of "easy" symmetries, for example, only permuting or flipping literals

- Let Σ be a set of (unquantified) Boolean formulas, and $\phi \in \Sigma$.
- A symmetry of ϕ is a bijection $\Sigma \to \Sigma$ which maps ϕ to an equivalent formula
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of “easy” symmetries, for example, only permuting or flipping literals
- Any such subgroup splits Σ into orbits

- Let Σ be a set of (unquantified) Boolean formulas, and $\phi \in \Sigma$.
- A symmetry of ϕ is a bijection $\Sigma \to \Sigma$ which maps ϕ to an equivalent formula
- Symmetries form a group with composition
- We may restrict ourselves to a subgroup of "easy" symmetries, for example, only permuting or flipping literals
- Any such subgroup splits Σ into orbits
- All formulas in the orbit containing ϕ are equivalent to ϕ

What is a symmetry breaker?

What is a symmetry breaker?

- Let G be a group of Boolean isomorphisms $\Sigma \to \Sigma$

What is a symmetry breaker?

- Let G be a group of Boolean isomorphisms $\Sigma \to \Sigma$
- A formula $\psi \in \Sigma$ is a (syntactic) symmetry breaker for G if

$$\forall\ \sigma \in \{0,1\}^n\ \exists\ g \in G : [\,g(\psi)\,]_\sigma = \top$$

What is a symmetry breaker?

- Let G be a group of Boolean isomorphisms $\Sigma \to \Sigma$
- A formula $\psi \in \Sigma$ is a (syntactic) symmetry breaker for G if

$$\forall\ \sigma \in \{0,1\}^n\ \exists\ g \in G : [\, g(\psi)\,]_\sigma = \top$$

- Key fact: if G is a symmetry group for $\phi \in \Sigma$ and ψ is a symmetry breaker for G then ϕ has a solution if and only if $\phi \wedge \psi$ has a solution.

What is a symmetry breaker?

- Let G be a group of bijective functions $\{0,1\}^n \rightarrow \{0,1\}^n$

What is a symmetry breaker?

- Let G be a group of bijective functions $\{0,1\}^n \to \{0,1\}^n$
- A formula $\psi \in \Sigma$ is a (semantic) symmetry breaker for G if

$$\forall\ \sigma \in \{0,1\}^n\ \exists\ g \in G : [\psi]_{g(\sigma)} = \top$$

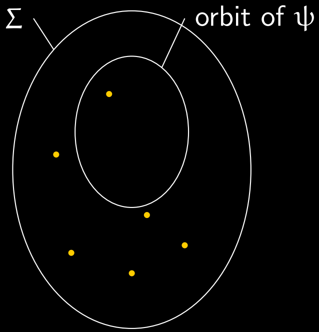
What is a symmetry breaker?

- Let G be a group of bijective functions $\{0,1\}^n \rightarrow \{0,1\}^n$
- A formula $\psi \in \Sigma$ is a (semantic) symmetry breaker for G if

$$\forall\ \sigma \in \{0,1\}^n\ \exists\ g \in G : [\psi]_{g(\sigma)} = \top$$

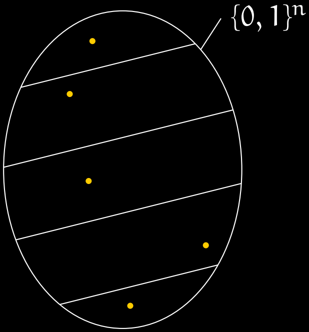
- Key fact: if G is a symmetry group of the solution set of $\phi \in \Sigma$ and ψ is a symmetry breaker for G then ϕ has a solution if and only if $\phi \wedge \psi$ has a solution.

syntactic



every $\sigma \in \{0,1\}^n$ is
a solution of at least one
formula in the orbit of ψ

semantic



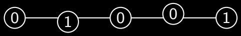
every orbit of $\{0,1\}^n$
contains at least one
solution of ψ

For SAT, there is no difference if we restrict to “easy” symmetries.

$$\phi(\ x_1\ ,\ x_2\ ,\ x_3\ ,\ x_4\ ,\ x_5\ )$$

For SAT, there is no difference if we restrict to “easy” symmetries.

$$\phi(\ x_1\ ,\ x_2\ ,\ x_3\ ,\ x_4\ ,\ x_5\ )$$



For SAT, there is no difference if we restrict to "easy" symmetries.

$$\phi(\ x_1\ ,\ x_4\ ,\ x_3\ ,\ x_2\ ,\ x_5\ )$$

For SAT, there is no difference if we restrict to “easy” symmetries.

$$\phi(\ x_1\ ,\ x_4\ ,\ \overline{x_3}\ ,\ x_2\ ,\ x_5\ )$$

How to construct a symmetry breaker?

How to construct a symmetry breaker?

- Idea: impose an order on the bit strings and take a formula which kills all non-minimal elements of each orbit.

How to construct a symmetry breaker?

- Idea: impose an order on the bit strings and take a formula which kills all non-minimal elements of each orbit.
- Then the minimal elements of each orbit survive, and all we need is at least one survivor per orbit.

$$\psi = \bigwedge_{g \in G} \Big((x_1, \ldots, x_n) \leq (g(x_1), \ldots, g(x_n)) \Big)$$

How to construct a symmetry breaker?

- Idea: impose an order on the bit strings and take a formula which kills all non-minimal elements of each orbit.
- Then the minimal elements of each orbit survive, and all we need is at least one survivor per orbit.

$$\psi = \bigwedge_{g \in G} \bigwedge_{i=1}^{n} \Big(\bigwedge_{j<i} (x_j = g(x_j)) \to (x_i \leq g(x_i)) \Big)$$

How to construct a symmetry breaker?

- Idea: impose an order on the bit strings and take a formula which kills all non-minimal elements of each orbit.
- Then the minimal elements of each orbit survive, and all we need is at least one survivor per orbit.

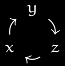
$$\psi = \bigwedge_{g \in G} \bigwedge_{i=1}^{n} \Big(\bigwedge_{j<i} (x_j = g(x_j)) \rightarrow (x_i \leq g(x_i)) \Big)$$

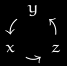
- Observe that we use a "syntactic" group but a "semantic" justification.

Example

- Consider the formula $\phi = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

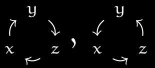
Example

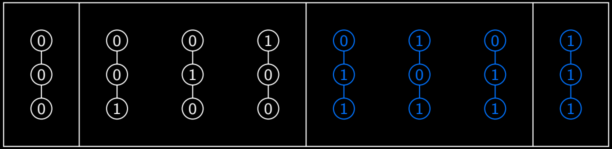
- Consider the formula $\phi = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$
- Consider the symmetry group $G = \{\mathrm{id},$ 

, 

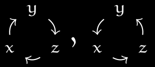
$\}$

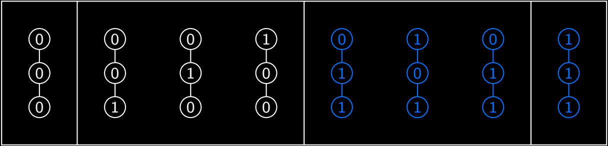
Example

- Consider the formula $\phi = (x \lor y) \land (y \lor z) \land (z \lor x)$
- Consider the symmetry group $G = \{$id,  $\}$



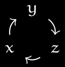
Example

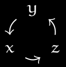
- Consider the formula $\phi = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$
- Consider the symmetry group $G = \{\mathrm{id},$  $\}$



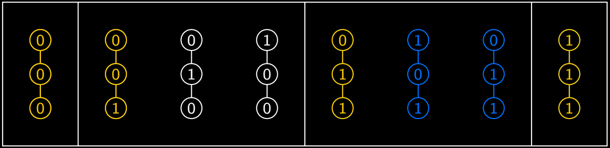
- $\psi = (x \to y) \wedge (y \to z)$ is a symmetry breaker for G

Example

- Consider the formula $\phi = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$
- Consider the symmetry group $G = \{\mathrm{id},$ 

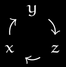
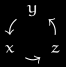
, 

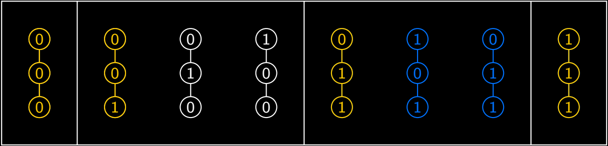
$\}$



- $\psi = (x \rightarrow y) \wedge (y \rightarrow z)$ is a symmetry breaker for G

Example

- Consider the formula $\phi = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$
- Consider the symmetry group $G = \{\text{id},$  ,  $\}$

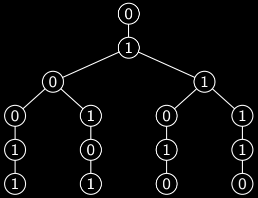


- $\psi = (x \rightarrow y) \wedge (y \rightarrow z)$ is a symmetry breaker for G
- Instead of solving ϕ, we can solve $\phi \wedge \psi$.

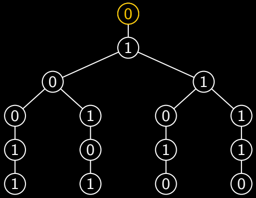
What about QBF?

$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6.\phi(x_1, x_2, x_3, x_4, x_5, x_6)$$

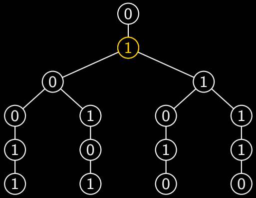
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6.\phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



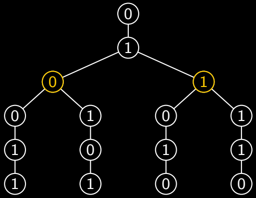
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



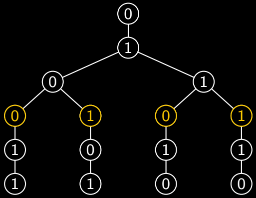
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



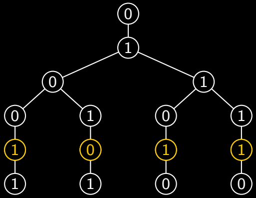
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



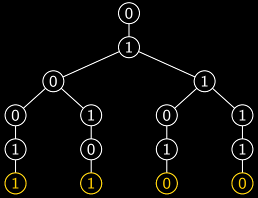
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6.\phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



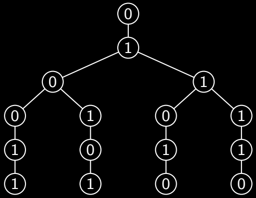
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



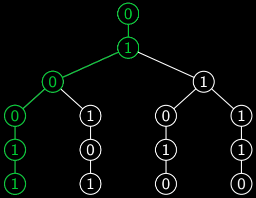
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



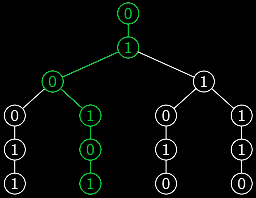
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6.\phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



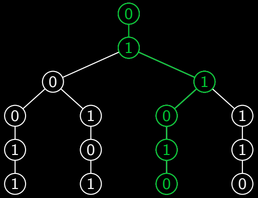
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



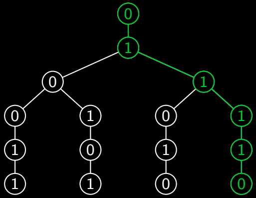
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



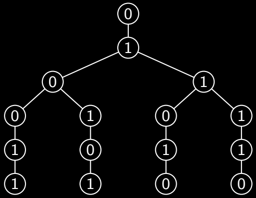
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6. \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



Given a quantifier prefix P, we write $\mathbb{S}(P)$ for the corresponding set of tree assignments.

Syntactic symmetries

Syntactic symmetries

- bijectively map (unquantified) formulas to (unquantified) formulas

Syntactic symmetries

- bijectively map (unquantified) formulas to (unquantified) formulas
- it is not necessary, but common, that literals are mapped to literals

Syntactic symmetries

- bijectively map (unquantified) formulas to (unquantified) formulas
- it is not necessary, but common, that literals are mapped to literals
- must respect logical connectives: $f(\phi_1 \wedge \phi_2) = f(\phi_1) \wedge f(\phi_2)$, etc.

Syntactic symmetries

- bijectively map (unquantified) formulas to (unquantified) formulas
- it is not necessary, but common, that literals are mapped to literals
- must respect logical connectives: $f(\phi_1 \wedge \phi_2) = f(\phi_1) \wedge f(\phi_2)$, etc.
- must respect quantifier blocks: $f(x_i)$ must only contain variables in the same block as x_i

Syntactic symmetries

- bijectively map (unquantified) formulas to (unquantified) formulas
- it is not necessary, but common, that literals are mapped to literals
- must respect logical connectives: $f(\phi_1 \wedge \phi_2) = f(\phi_1) \wedge f(\phi_2)$, etc.
- must respect quantifier blocks: $f(x_i)$ must only contain variables in the same block as x_i

Semantic symmetries

Syntactic symmetries

- bijectively map (unquantified) formulas to (unquantified) formulas
- it is not necessary, but common, that literals are mapped to literals
- must respect logical connectives: $f(\phi_1 \wedge \phi_2) = f(\phi_1) \wedge f(\phi_2)$, etc.
- must respect quantifier blocks: $f(x_i)$ must only contain variables in the same block as x_i

Semantic symmetries

- bijectively map tree assignments to tree assignments

Syntactic symmetries

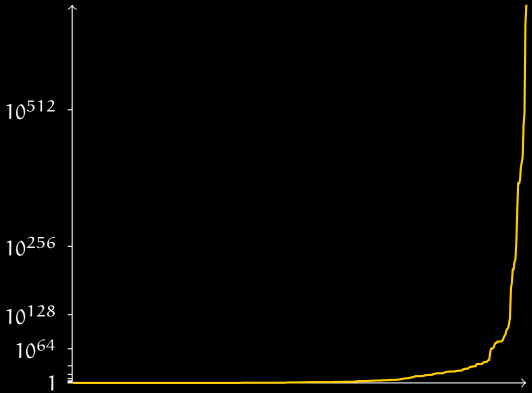
- bijectively map (unquantified) formulas to (unquantified) formulas
- it is not necessary, but common, that literals are mapped to literals
- must respect logical connectives: $f(\phi_1 \wedge \phi_2) = f(\phi_1) \wedge f(\phi_2)$, etc.
- must respect quantifier blocks: $f(x_i)$ must only contain variables in the same block as x_i

Semantic symmetries

- bijectively map tree assignments to tree assignments
- in principle no restrictions

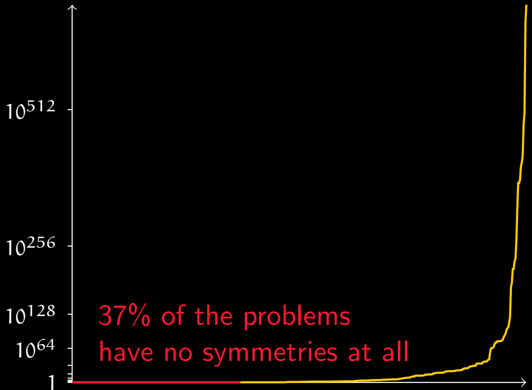
How many symmetries are there?

How many symmetries are there?



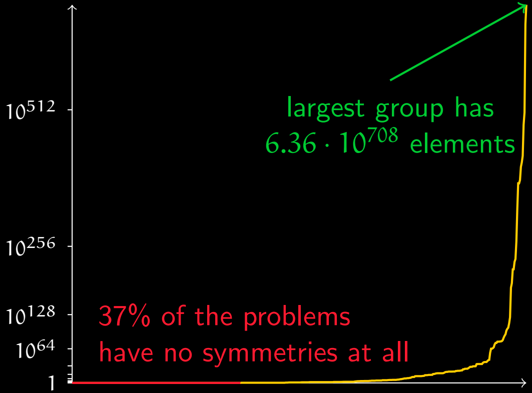
Sizes of syntactic symmetry groups for the 2017 QBFEval benchmark (PCNF track), computed using Saucy and GAP.

How many symmetries are there?



Sizes of syntactic symmetry groups for the 2017 QBFEval benchmark (PCNF track), computed using Saucy and GAP.

How many symmetries are there?



Sizes of syntactic symmetry groups for the 2017 QBFEval benchmark (PCNF track), computed using Saucy and GAP.

Symmetry Breakers for QBF

Symmetry Breakers for QBF

- Let P be a quantifier prefix

Symmetry Breakers for QBF

- Let P be a quantifier prefix
- Let G_{syn} be a group of isomorphisms $\Sigma \to \Sigma$ respecting P

Symmetry Breakers for QBF

- Let P be a quantifier prefix
- Let G_{syn} be a group of isomorphisms $\Sigma \to \Sigma$ respecting P
- Let G_{sem} be a group of bijections $\mathbb{S}(\mathrm{P}) \to \mathbb{S}(\mathrm{P})$

Symmetry Breakers for QBF

- Let P be a quantifier prefix
- Let G_{syn} be a group of isomorphisms $\Sigma \to \Sigma$ respecting P
- Let G_{sem} be a group of bijections $\mathbb{S}(P) \to \mathbb{S}(P)$
- $\psi \in \Sigma$ is a symmetry breaker for G_{syn} and G_{sem} if

$$\forall\, t \in \mathbb{S}(P)\ \exists\, g_{syn} \in G_{syn}\ \exists\, g_{sem} \in G_{sem} : [\, P.g_{syn}(\psi)\,]_{g_{sem}(t)} = \top$$

Symmetry Breakers for QBF

- Let P be a quantifier prefix
- Let G_{syn} be a group of isomorphisms $\Sigma \to \Sigma$ respecting P
- Let G_{sem} be a group of bijections $\mathbb{S}(P) \to \mathbb{S}(P)$
- $\psi \in \Sigma$ is a symmetry breaker for G_{syn} and G_{sem} if

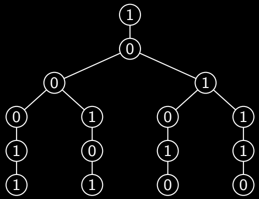
$$\forall\, t \in \mathbb{S}(P)\ \exists\, g_{syn} \in G_{syn}\ \exists\, g_{sem} \in G_{sem} : [\, P.g_{syn}(\psi)\,]_{g_{sem}(t)} = \top$$

- Key fact: If G_{syn} is a syntactic symmetry group for $P.\phi$ and G_{sem} is a semantic symmetry group for $P.\phi$ and ψ is a symmetry breaker for G_{syn} and G_{sem}, then $P.\phi$ has a solution in $\mathbb{S}(P)$ if and only if $P.(\phi \land \psi)$ does.

Easy symmetries

What does permutation of variables mean semantically?

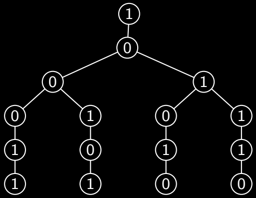
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 : \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



Easy symmetries

What does permutation of variables mean semantically?

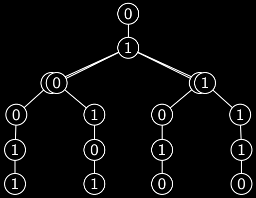
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 : \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



Easy symmetries

What does permutation of variables mean semantically?

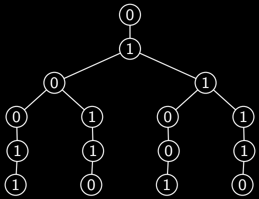
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 : \phi(x_2, x_1, x_3, x_4, x_5, x_6)$$



Easy symmetries

What does permutation of variables mean semantically?

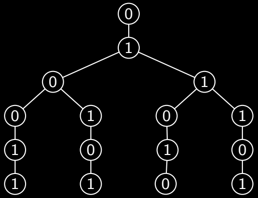
$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 : \phi(x_2, x_1, x_4, x_3, x_5, x_6)$$



Easy symmetries

What does permutation of variables mean semantically?

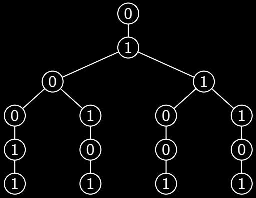
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 : \phi(x_2, x_1, x_4, x_3, x_6, x_5)$$



Easy symmetries

What does permutation of variables mean semantically?

$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6 : \phi(x_2, x_1, x_4, x_3, x_6, x_5)$$



Unlike in SAT, there is no longer a 1:1 correspondence.

- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix

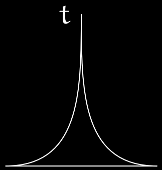
- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P

- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the group of all bijective maps $f \colon \mathbb{S}(P) \to \mathbb{S}(P)$ such that

$$\forall\ t \in \mathbb{S}(P)\ \forall\ \tau \in f(t)\ \exists\ g \in G_{\mathsf{syn}} : g(\tau) \in t$$

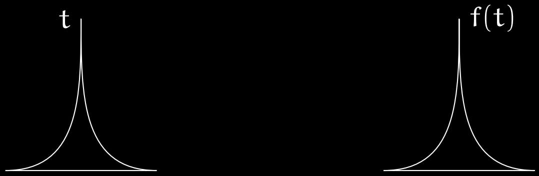
- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the group of all bijective maps $f \colon \mathbb{S}(P) \to \mathbb{S}(P)$ such that

$$\forall\, t \in \mathbb{S}(P)\ \forall\, \tau \in f(t)\ \exists\, g \in G_{\mathsf{syn}} : g(\tau) \in t$$



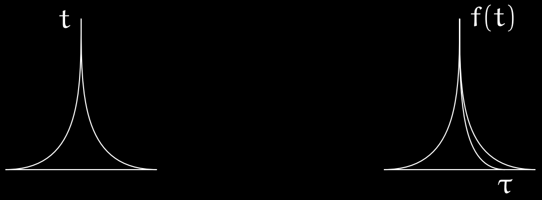
- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the group of all bijective maps $f\colon \mathbb{S}(P) \to \mathbb{S}(P)$ such that

$$\forall\, t \in \mathbb{S}(P)\ \forall\, \tau \in f(t)\ \exists\, g \in G_{\mathsf{syn}} : g(\tau) \in t$$



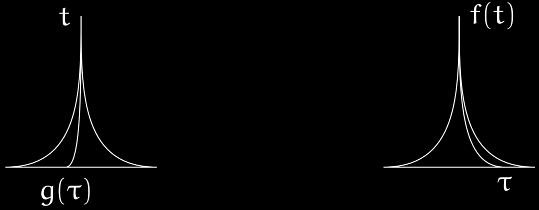
- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the group of all bijective maps $f \colon \mathbb{S}(P) \to \mathbb{S}(P)$ such that

$$\forall\, t \in \mathbb{S}(P)\ \forall\, \tau \in f(t)\ \exists\, g \in G_{\mathsf{syn}} : g(\tau) \in t$$



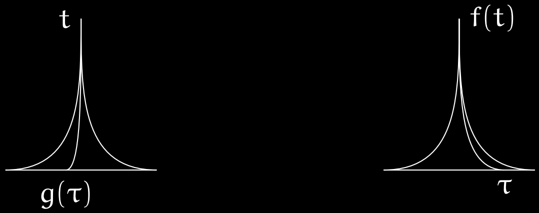
- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the group of all bijective maps $f\colon \mathbb{S}(P) \to \mathbb{S}(P)$ such that

$$\forall\ t \in \mathbb{S}(P)\ \forall\ \tau \in f(t)\ \exists\ g \in G_{\mathsf{syn}} : g(\tau) \in t$$



- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the group of all bijective maps $f \colon \mathbb{S}(P) \to \mathbb{S}(P)$ such that

$$\forall\, t \in \mathbb{S}(P)\ \forall\, \tau \in f(t)\ \exists\, g \in G_{\text{syn}} : g(\tau) \in t$$



- Then G_{sem} is called the associated group for G_{syn}.

- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the associated group of G_{syn}.

- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the associated group of G_{syn}.
- Then

$$\psi = \bigwedge_{g \in G_{\mathsf{syn}}} \bigwedge_{\substack{i=1 \\ Q_i = \exists}}^{n} \left(\bigwedge_{j<i} (x_j = g(x_j)) \rightarrow (x_i \leq g(x_i)) \right)$$

is a symmetry breaker for G_{syn} and G_{sem}.

- Let $P = Q_1 x_1 \cdots Q_n x_n$ be a quantifier prefix
- Let G_{syn} be a group of permutations of literals respecting P
- Let G_{sem} be the associated group of G_{syn}.
- Then

$$\psi = \bigwedge_{g \in G_{\mathsf{syn}}} \bigwedge_{\substack{i=1 \\ Q_i = \exists}}^{n} \Big(\bigwedge_{j<i} (x_j = g(x_j)) \to (x_i \leq g(x_i)) \Big)$$

  is a symmetry breaker for G_{syn} and G_{sem}.
- Observe that only G_{syn} appears in the formula. The group G_{sem} is only used for the justification.

Case study: the Kleine-Büning et al family

	Solving times of DepQBF (in sec) w/o SB		with SB	
n	QRes	LD	QRes	LD
10	0.3	0.5	0.4	0.4
20	160	0.5	0.4	0.4
40	> 3600	0.5	0.4	0.4
80	> 3600	0.7	0.4	0.4
160	> 3600	2.2	0.5	0.4
320	> 3600	12.3	0.6	0.5
640	> 3600	36.8	1.0	0.8
1280	> 3600	241.1	22.6	19.7
2560	> 3600	> 3600	215.7	155.2
5120	> 3600	> 3600	1873.2	1042.6

Case study: the Kleine-Büning et al family

In fact, we can show that there
is a proof of size $O(n)$
when a symmetry breaker is added.

What about the universal quantifiers?

What about the universal quantifiers?

- The symmetry breaker above only affects variables bound by $\exists$

What about the universal quantifiers?

- The symmetry breaker above only affects variables bound by $\exists$
- We can handle variables bound by $\forall$ using duality

What about the universal quantifiers?

- The symmetry breaker above only affects variables bound by $\exists$
- We can handle variables bound by $\forall$ using duality
- A dual assignment for $\Phi = P.\phi$ is an assignment for $\neg\Phi$

What about the universal quantifiers?

- The symmetry breaker above only affects variables bound by $\exists$
- We can handle variables bound by $\forall$ using duality
- A dual assignment for $\Phi = P.\phi$ is an assignment for $\neg\Phi$
- As negation toggles quantifiers, the tree shapes are different

What about the universal quantifiers?

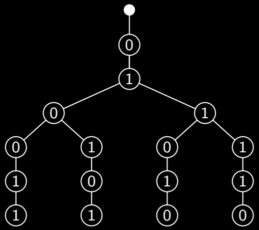
- The symmetry breaker above only affects variables bound by $\exists$
- We can handle variables bound by $\forall$ using duality
- A dual assignment for $\Phi = P.\phi$ is an assignment for $\neg\Phi$
- As negation toggles quantifiers, the tree shapes are different

$$\exists\ x_1, x_2\ \forall\ x_3, x_4\ \exists\ x_5, x_6.\phi(x_1, x_2, x_3, x_4, x_5, x_6)$$

What about the universal quantifiers?

- The symmetry breaker above only affects variables bound by $\exists$
- We can handle variables bound by $\forall$ using duality
- A dual assignment for $\Phi = P.\phi$ is an assignment for $\neg\Phi$
- As negation toggles quantifiers, the tree shapes are different

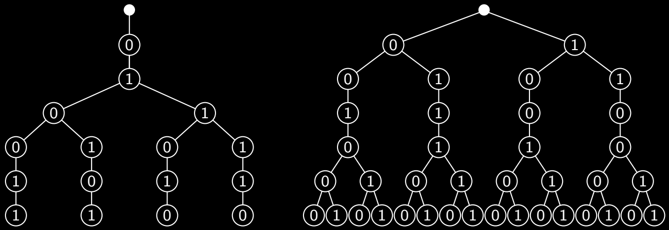
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6.\phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



What about the universal quantifiers?

- The symmetry breaker above only affects variables bound by $\exists$
- We can handle variables bound by $\forall$ using duality
- A dual assignment for $\Phi = P.\phi$ is an assignment for $\neg\Phi$
- As negation toggles quantifiers, the tree shapes are different

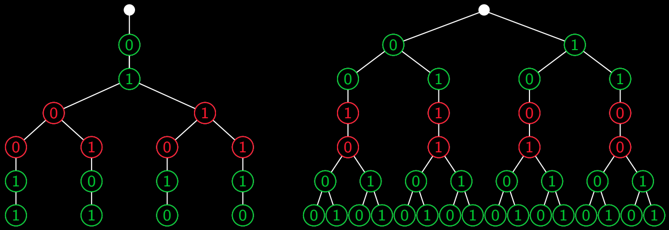
$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



What about the universal quantifiers?

- The symmetry breaker above only affects variables bound by $\exists$
- We can handle variables bound by $\forall$ using duality
- A dual assignment for $\Phi = P.\phi$ is an assignment for $\neg\Phi$
- As negation toggles quantifiers, the tree shapes are different

$$\exists\, x_1, x_2\ \forall\, x_3, x_4\ \exists\, x_5, x_6 . \phi(x_1, x_2, x_3, x_4, x_5, x_6)$$



- Write $\mathbb{S}_{\exists}(\mathrm{P}) = \mathbb{S}(\mathrm{P})$ for the set of tree assignments for prefix P

- Write $\mathbb{S}_\exists(\mathrm{P}) = \mathbb{S}(\mathrm{P})$ for the set of tree assignments for prefix P
- Write $\mathbb{S}_\forall(\mathrm{P})$ for the dual tree assignments for prefix P

- Write $\mathbb{S}_{\exists}(\mathrm{P}) = \mathbb{S}(\mathrm{P})$ for the set of tree assignments for prefix P
- Write $\mathbb{S}_{\forall}(\mathrm{P})$ for the dual tree assignments for prefix P
- Let $\mathrm{G}^{\forall}_{\mathsf{syn}}$ be a group of isomorphisms $\Sigma \to \Sigma$ respecting P

- Write $\mathbb{S}_\exists(\mathrm{P}) = \mathbb{S}(\mathrm{P})$ for the set of tree assignments for prefix P
- Write $\mathbb{S}_\forall(\mathrm{P})$ for the dual tree assignments for prefix P
- Let $\mathsf{G}^\forall_{\mathsf{syn}}$ be a group of isomorphisms $\Sigma \to \Sigma$ respecting P
- Let $\mathsf{G}^\forall_{\mathsf{sem}}$ be a group of bijections $\mathbb{S}_\forall(\mathrm{P}) \to \mathbb{S}_\forall(\mathrm{P})$

- Write $\mathbb{S}_\exists(P) = \mathbb{S}(P)$ for the set of tree assignments for prefix P
- Write $\mathbb{S}_\forall(P)$ for the dual tree assignments for prefix P
- Let $G^\forall_{\mathsf{syn}}$ be a group of isomorphisms $\Sigma \to \Sigma$ respecting P
- Let $G^\forall_{\mathsf{sem}}$ be a group of bijections $\mathbb{S}_\forall(P) \to \mathbb{S}_\forall(P)$
- $\psi \in \Sigma$ is a universal symmetry breaker for $G^\forall_{\mathsf{syn}}$ and $G^\forall_{\mathsf{sem}}$ if

$$\forall\ t \in \mathbb{S}_\forall(P)\ \exists\ g_{\mathsf{syn}} \in G^\forall_{\mathsf{syn}}\ \exists\ g_{\mathsf{sem}} \in G^\forall_{\mathsf{sem}} : [P.g_{\mathsf{syn}}(\psi)]_{g_{\mathsf{sem}}(t)} = \bot$$

- Write $\mathbb{S}_\exists(P) = \mathbb{S}(P)$ for the set of tree assignments for prefix P
- Write $\mathbb{S}_\forall(P)$ for the dual tree assignments for prefix P
- Let $G^\forall_{\mathsf{syn}}$ be a group of isomorphisms $\Sigma \to \Sigma$ respecting P
- Let $G^\forall_{\mathsf{sem}}$ be a group of bijections $\mathbb{S}_\forall(P) \to \mathbb{S}_\forall(P)$
- $\psi \in \Sigma$ is a universal symmetry breaker for $G^\forall_{\mathsf{syn}}$ and $G^\forall_{\mathsf{sem}}$ if

$$\forall\ t \in \mathbb{S}_\forall(P)\ \exists\ g_{\mathsf{syn}} {\in} G^\forall_{\mathsf{syn}}\ \exists\ g_{\mathsf{sem}} {\in} G^\forall_{\mathsf{sem}} : [P.g_{\mathsf{syn}}(\psi)]_{g_{\mathsf{sem}}(t)} = \bot$$

- Symmetry breakers as previously defined will now be called existential symmetry breakers

- Write $\mathbb{S}_\exists(P) = \mathbb{S}(P)$ for the set of tree assignments for prefix P
- Write $\mathbb{S}_\forall(P)$ for the dual tree assignments for prefix P
- Let $G^\forall_{\mathsf{syn}}$ be a group of isomorphisms $\Sigma \to \Sigma$ respecting P
- Let $G^\forall_{\mathsf{sem}}$ be a group of bijections $\mathbb{S}_\forall(P) \to \mathbb{S}_\forall(P)$
- $\psi \in \Sigma$ is a universal symmetry breaker for $G^\forall_{\mathsf{syn}}$ and $G^\forall_{\mathsf{sem}}$ if

$$\forall\ t \in \mathbb{S}_\forall(P)\ \exists\ g_{\mathsf{syn}} {\in} G^\forall_{\mathsf{syn}}\ \exists\ g_{\mathsf{sem}} {\in} G^\forall_{\mathsf{sem}} : [P.g_{\mathsf{syn}}(\psi)]_{g_{\mathsf{sem}}(t)} = \bot$$

- Symmetry breakers as previously defined will now be called existential symmetry breakers
- ψ is an existential symmetry breaker iff $\neg\psi$ is a universal symmetry breaker (w.r.t. suitably chosen groups)

Key fact:

- Let $\Phi = P.\phi$ be a QBF

Key fact:

- Let $\Phi = P.\phi$ be a QBF
- Let $G^{\exists}_{\text{syn}}$ and $G^{\forall}_{\text{syn}}$ be two syntactic symmetry groups for Φ

Key fact:

- Let $\Phi = P.\phi$ be a QBF
- Let $G^{\exists}_{\mathsf{syn}}$ and $G^{\forall}_{\mathsf{syn}}$ be two syntactic symmetry groups for Φ
- Let $G^{\exists}_{\mathsf{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\exists}(P)$

Key fact:

- Let $\Phi = P.\phi$ be a QBF
- Let $G^{\exists}_{\mathsf{syn}}$ and $G^{\forall}_{\mathsf{syn}}$ be two syntactic symmetry groups for Φ
- Let $G^{\exists}_{\mathsf{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\exists}(P)$
- Let $G^{\forall}_{\mathsf{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\forall}(P)$

Key fact:

- Let $\Phi = P.\phi$ be a QBF
- Let $G^{\exists}_{\text{syn}}$ and $G^{\forall}_{\text{syn}}$ be two syntactic symmetry groups for Φ
- Let $G^{\exists}_{\text{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\exists}(P)$
- Let $G^{\forall}_{\text{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\forall}(P)$
- Let $\psi_{\exists} \in \Sigma$ be an existential symmetry breaker for $G^{\exists}_{\text{syn}}$, $G^{\exists}_{\text{sem}}$

Key fact:

- Let $\Phi = P.\phi$ be a QBF
- Let $G^{\exists}_{\mathsf{syn}}$ and $G^{\forall}_{\mathsf{syn}}$ be two syntactic symmetry groups for Φ
- Let $G^{\exists}_{\mathsf{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\exists}(P)$
- Let $G^{\forall}_{\mathsf{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\forall}(P)$
- Let $\psi_{\exists} \in \Sigma$ be an existential symmetry breaker for $G^{\exists}_{\mathsf{syn}}$, $G^{\exists}_{\mathsf{sem}}$
- Let $\psi_{\forall} \in \Sigma$ be universal symmetry breaker for $G^{\forall}_{\mathsf{syn}}$, $G^{\forall}_{\mathsf{sem}}$

Key fact:

- Let $\Phi = P.\phi$ be a QBF
- Let $G^{\exists}_{\text{syn}}$ and $G^{\forall}_{\text{syn}}$ be two syntactic symmetry groups for Φ
- Let $G^{\exists}_{\text{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\exists}(P)$
- Let $G^{\forall}_{\text{sem}}$ be a symmetry group for Φ acting on $\mathbb{S}_{\forall}(P)$
- Let $\psi_{\exists} \in \Sigma$ be an existential symmetry breaker for $G^{\exists}_{\text{syn}}$, $G^{\exists}_{\text{sem}}$
- Let $\psi_{\forall} \in \Sigma$ be universal symmetry breaker for $G^{\forall}_{\text{syn}}$, $G^{\forall}_{\text{sem}}$
- Then

$$\begin{aligned} P.\phi \text{ is true } &\iff P.((\phi \wedge \psi_{\exists}) \vee \psi_{\forall}) \text{ is true} \\ &\iff P.((\phi \vee \psi_{\forall}) \wedge \psi_{\exists}) \text{ is true} \end{aligned}$$

Summary

- For QBF, unlike for SAT, syntactic and semantic symmetries are not equivalent

Summary

- For QBF, unlike for SAT, syntactic and semantic symmetries are not equivalent
- For QBF, every syntactic symmetry gives rise to many semantic symmetries

Summary

- For QBF, unlike for SAT, syntactic and semantic symmetries are not equivalent
- For QBF, every syntactic symmetry gives rise to many semantic symmetries
- The following formula is an existential symmetry breaker:

$$\psi = \bigwedge_{g \in G_{\mathsf{syn}}} \bigwedge_{\substack{i=1 \\ Q_i = \exists}}^{n} \left(\bigwedge_{j<i} (x_j = g(x_j)) \rightarrow (x_i \leq g(x_i)) \right)$$

Summary

- For QBF, unlike for SAT, syntactic and semantic symmetries are not equivalent
- For QBF, every syntactic symmetry gives rise to many semantic symmetries
- The following formula is an existential symmetry breaker:

$$\psi = \bigwedge_{g \in G_{\mathsf{syn}}} \bigwedge_{\substack{i=1 \\ Q_i = \exists}}^{n} \left(\bigwedge_{j<i} (x_j = g(x_j)) \rightarrow (x_i \leq g(x_i)) \right)$$

- If ψ is an existential symmetry breaker, then $\neg\psi$ is a universal symmetry breaker

Summary

- For QBF, unlike for SAT, syntactic and semantic symmetries are not equivalent
- For QBF, every syntactic symmetry gives rise to many semantic symmetries
- The following formula is an existential symmetry breaker:

$$\psi = \bigwedge_{g \in G_{syn}} \bigwedge_{\substack{i=1 \\ Q_i = \exists}}^{n} \left(\bigwedge_{j<i} (x_j = g(x_j)) \rightarrow (x_i \leq g(x_i)) \right)$$

- If ψ is an existential symmetry breaker, then $\neg\psi$ is a universal symmetry breaker
- Existential and universal symmetry breakers can be applied simultaneously