Quantified Boolean Formulas:

Solving and Proofs

Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena
https://github.com/JoshuaBlinkhorn/QBF

Overview of Universal Expansion

- A method of deleting universal variables from a QBF
- After expansion we have only existential variables, i.e. a propositional formula
- This propositional formula is called the expansion of Φ, written $\exp(\Phi)$
- Semantics preserved: $\exp(\Phi)$ is satisfiable if, and only if, Φ is true
- Expansion introduces new variables and increases the formula size (exponentially in the worst case)

Expansion of One Universal Variable

- Consider a QBF with a single universal variable

$$\Phi = \exists x \forall u \exists y \cdot F(x, u, y)$$

- Eliminate variable u by expansion

$$\exists x \exists y_0 \exists y_1 \cdot F(x, 0, y_0) \wedge F(x, 1, y_1)$$

- We use two copies of y and two copies of F to respect the dependence of y on the expanded variable u
- Expanding u does not change the truth value
- The resulting formula has only existential variables, so it is essentially a propositional formula

$$\exp(\Phi) = F(x, 0, y_0) \wedge F(x, 1, y_1)$$

- $\exp(\Phi)$ is satisfiable if, and only if, Φ is true

Expansion of Two Universal Variables

- Consider a QBF with two universal variables

$$\Phi = \exists x \forall u \exists y \forall v \exists z \cdot F(x, u, y, v, z)$$

- Eliminate variable u by expansion

$$\exists x \exists y_0 \exists y_1 \forall v \exists z_0 \exists z_1 \cdot F(x, 0, y_0, v, z_0) \wedge F(x, 1, y_1, v, z_1)$$

- Eliminate variable v by expansion

$$\exists x \exists y_0 \exists y_1 \exists z_{00} \exists z_{01} \exists z_{10} \exists z_{11} \cdot F(x, 0, y_0, 0, z_{00}) \wedge$$
$$F(x, 0, y_0, 1, z_{01}) \wedge F(x, 1, y_1, 0, z_{10}) \wedge F(x, 1, y_1, 1, z_{11})$$

- Neither expansion changes the truth value

$$\exp(\Phi) = F(x, 0, y_0, 0, z_{00}) \wedge F(x, 0, y_0, 1, z_{01}) \wedge$$
$$F(x, 1, y_1, 0, z_{10}) \wedge F(x, 1, y_1, 1, z_{11})$$

- $\exp(\Phi)$ is satisfiable if, and only if, Φ is true

Annotating with assignments

- In general, if there are n universal variables, the expansion is conjunction of 2^n substitution instances of the matrix
- Each substitution instance corresponds to one of the 2^n universal assingments
- To respect dependencies, variables must be copied
- In a substitution instance corresponding to $\alpha \in \langle \text{vars}_\forall(\Phi) \rangle$, a variable x is annotated with the restriction of α to its dependency set $L(x)$

$$\Phi = \exists x \forall u \exists y \forall v \exists z \cdot F(x, u, y, v, z)$$

$$\exp(\Phi) = \dots \wedge F(x, 0, y_0, 1, z_{01}) \wedge \dots$$
$$\exp(\Phi) = \dots \wedge F(x, 0, y_{u \mapsto 0}, 1, z_{u \mapsto 0, v \mapsto 1}) \wedge \dots$$

Universal Expansion in General

- The expansion of a QBF $\Phi = \mathcal{Q} \cdot F$ is the CNF

$$\mathsf{exp}(\Phi) := \bigcup_{\alpha \in \langle \mathsf{vars}_\forall(\Phi) \rangle} F\left[\alpha \cup \left\{x \mapsto x_{\alpha \restriction L(x)} : x \in \mathsf{vars}_\exists(\Phi)\right\}\right]$$

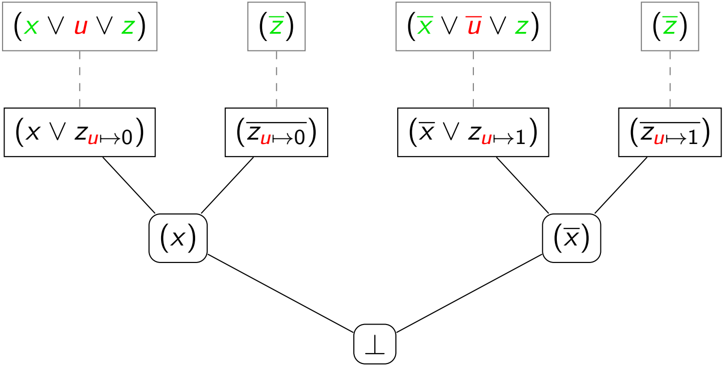
- Proposition: For any QBF Φ, $\mathsf{exp}(\Phi)$ is satisfiable if, and only if, Φ is true.
- In fact, there is a natural one-one correspondence between satisfying assignments of $\mathsf{exp}(\Phi)$ and models of Φ.

The QBF Proof System $\forall$Exp+Res

Definition: A $\forall$Exp+Res refutation of a QBF Φ is a Resolution refutation of $\exp(\Phi)$.

Example ∀Exp+Res Refutation

$$\Phi = \exists x \forall u \exists z \cdot (x \vee u \vee z) \wedge (\overline{x} \vee \overline{u} \vee z) \wedge (\overline{z})$$
$$\exp(\Phi) = (x \vee z_{u\mapsto 0}) \wedge (\overline{z_{u\mapsto 0}}) \wedge (\overline{x} \vee z_{u\mapsto 1}) \wedge (\overline{z_{u\mapsto 1}})$$



Which lower bound techniques apply?

Techniques for propositional proof systems

- size-width relation [Ben-Sasson & Wigderson 01]
- feasible interpolation [Krajíček 97]
- game-theoretic techniques [Pudlák, Buss, Impagliazzo, . . .]

In QBF proof systems

- size-width relations fail for QBF resolution systems
- feasible interpolation holds for QBF resolution systems
- game-theoretic techniques work for weak tree-like systems [Beyersdorff et. al 16, 17, Chen 16]

We need new techniques

- not derived from propositional proof complexity

Lower Bounds via Semantic Measures

- Many QBF proof systems have strategy extraction
- From a refutation, we effeciently compute a countermodel
- Hence, if the countermodel is 'large', so is the refutation
- Gives rise to lower bound techniques based on semantic measures: definitions of countermodel 'size'
- For example, minimal range of a countermodel

Definitions

- The partial expansion of a QBF $\Phi = \mathcal{Q} \cdot F$ w.r.t. a set of universal assignments $R \subseteq \langle \text{vars}_\forall(\Phi) \rangle$ is the CNF

$$\exp(\Phi, R) := \bigcup_{\alpha \in R} F\left[\alpha \cup \left\{x \mapsto x_{\alpha \restriction L(x)} : x \in \text{vars}_\exists(\Phi)\right\}\right]$$

- A countermodel for a QBF F is a function $f : \langle \text{vars}_\exists(F) \rangle \to \langle \text{vars}_\forall(F) \rangle$ such that
  - dependency: for each $u \in \text{vars}_{\forall(F)}$ and $\alpha, \beta \in \langle \text{vars}_\exists(F) \rangle$, if α, β agree on $L(u)$, then $f(\alpha), f(\beta)$ agree on u.
  - semantic for each $\alpha \in \langle \text{vars}_\exists(F) \rangle$, $\alpha \cup f(\alpha)$ falsifies the matrix of F.

A Lower Bound Technique

Theorem: Let Φ be a QBF, and let $R \subseteq \langle \mathsf{vars}_\forall(\Phi) \rangle$. The partial expansion $\exp(\Phi, R)$ is unsatisfiable if, and only if, $R \supseteq \mathsf{rng}(h)$ for some countermodel h of Φ.

Definition: We define $\sigma(\Phi)$ as the minumum cardinality of the range of a countermodel for a false QBF Q:

$$\sigma(\Phi) := \min\{|\mathsf{rng}(h)| : h \text{ is a countermodel for } \Phi\}$$

Corollary: Any $\forall$Exp+Res refutation of a false QBF Φ has size at least $\sigma(\Phi)$.

- If a partial expansion of Φ is unsatisfiable, it contains at least $\sigma(\Phi)$ non-trivial conjuncts
- So a $\forall$Exp+Res refutation of Φ requires at least $\sigma(\Phi)$ axioms

Application to the Equality Formulas

$$EQ_n := \exists x_1 \cdots x_n \forall u_1 \cdots u_n \exists z_1 \cdots z_n .$$
$$\left(\bigwedge_{i \in [n]} (x_i \vee u_i \vee z_i) \right) \wedge \left(\bigwedge_{i \in [n]} (\overline{x_i} \vee \overline{u_i} \vee z_i) \right) \wedge \left(\bigvee_{i \in [n]} \overline{z_i} \right)$$

- The countermodel is unique:

$$\begin{array}{rcccl} h & : & \langle \mathrm{vars}_{\exists}(EQ_n) \rangle & \rightarrow & \langle \mathrm{vars}_{\forall}(EQ_n) \rangle \\ & & \alpha & \mapsto & \{ u_1 \mapsto \alpha(x_1), \ldots, u_n \mapsto \alpha(x_n) \} \end{array}$$

- Clear: $\mathrm{rng}(h) = \langle \mathrm{vars}_{\forall}(EQ_n) \rangle$ and $|\mathrm{rng}(h)| = 2^n$
- So $\sigma(EQ_n) = 2^n$, and we apply the technique
- Any $\forall$Exp+Res refutation of EQ_n has size at least 2^n

Theorem: The equality formulas require exponential size $\forall$Exp+Res refutations.

Proof (only if direction)

Theorem: Let Φ be a QBF, and let $R \subseteq \langle \text{vars}_{\forall}(\Phi) \rangle$. The partial expansion $\exp(\Phi, R)$ is unsatisfiable if, and only if, $R \supseteq \text{rng}(h)$ for some countermodel h of Φ.

- Proof by induction on the quantifier depth d of Φ
- Quantifier depth is the number of blocks:

  $$\exists X_1 \forall U_1 \exists X_2 \forall U_2 \exists X_3 \cdot \phi(X_1, U_1, X_2, U_2, X_3)$$

  here the quantifier depth is $d = 5$
- Base case $d = 0$ is trivial: $\Phi = \phi(\emptyset)$
- We have $R = \langle \text{vars}_{\forall}(\Phi) \rangle = \emptyset$
- $\exp(\Phi, R) = \phi$
- Note that ϕ is either $\top$ or the empty clause $\perp$
- Suppose $\exp(\Phi)$ is unsatisfiable; then ϕ is the empty clause
- Then Φ has a trivial countermodel h with $\text{rng}(h) = \emptyset \subseteq R$

Proof (only if direction)

Theorem: Let Φ be a QBF, and let $R \subseteq \langle \text{vars}_{\forall}(\Phi) \rangle$. The partial expansion $\exp(\Phi, R)$ is unsatisfiable if, and only if, $R \supseteq \text{rng}(h)$ for some countermodel h of Φ.

- Inductive step $d \geq 1$, universal case: $\Phi = \forall U \mathcal{Q} \cdot \phi(U, \text{vars}(\mathcal{Q}))$
- Suppose that $\exp(\Phi, R)$ is unsatisfiable
- Idea: partition $\exp(\Phi, R)$ into conjucts corresponding to assignments to U
- $R' := \{\alpha\restriction_U : \alpha \in R\}$
- For each $\beta \in R'$, define $R_\beta := \{\alpha \in R : \beta \subseteq \alpha\}$
- Observe that $R = \bigcup_{\beta \in R'} R_\beta$
- Hence $\exp(\Phi, R) = \bigwedge_{\beta \in R'} \exp(\Phi, R_\beta)$
- The conjucts of $\bigwedge_{\beta \in R'} \exp(\Phi, R_\beta)$ are pairwise variable-disjoint
- Hence there exists $\beta \in R'$ such that $\exp(\Phi, R_\beta)$ is unsatisfiable

Proof (only if direction)

Theorem: Let Φ be a QBF, and let $R \subseteq \langle \mathrm{vars}_\forall(\Phi) \rangle$. The partial expansion $\exp(\Phi, R)$ is unsatisfiable if, and only if, $R \supseteq \mathrm{rng}(h)$ for some countermodel h of Φ.

- Fix $\beta \in R'$ such that $\exp(\Phi, R_\beta)$ is unsatisfiable
- Define $S_\beta := \{\alpha \setminus \beta : \alpha \in R_\beta\}$
- Observe that $\exp(\Phi, R_\beta)$ is syntactically equivalent to $\exp(\Phi[\beta], S_\beta)$; just delete β from the annotations
- Hence $\exp(\Phi[\beta], S_\beta)$ is unsatisfiable
- $\Phi[\beta]$ has quantifier depth $d - 1$; by inductive hypothesis:
- $S_\beta \supseteq \mathrm{rng}(h)$ for some countermodel h of $\Phi[\beta]$.
- Form a countermodel h' for Φ simply by adding β to every element of the range of h (check this satisfies the definition)
- $\mathrm{rng}(h') \subseteq R_\beta \subseteq R$

Proof (only if direction)

Theorem: Let Φ be a QBF, and let $R \subseteq \langle \mathsf{vars}_\forall(\Phi) \rangle$. The partial expansion $\exp(\Phi, R)$ is unsatisfiable if, and only if, $R \supseteq \mathrm{rng}(h)$ for some countermodel h of Φ.

- Inductive step $d \geq 1$, existential case:
  $\Phi = \exists X \mathcal{Q} \cdot \phi(X, \mathsf{vars}(\mathcal{Q}))$
- Suppose that $\exp(\Phi, R)$ is unsatisfiable
- Idea: restrict by all assignments to X
- let $\alpha \in \langle X \rangle$; observe that $\exp(\Phi, R)[\alpha]$ is unsatisfiable
- observe that $\exp(\Phi, R)[\alpha] = \exp(\Phi[\alpha], R)$
- $\Phi[\alpha]$ has quantifier depth $d - 1$; by inductive hypothesis:
- $R \supseteq \mathrm{rng}(h_\alpha)$ for some countermodel h_α of $\Phi[\alpha]$.

Proof (only if direction)

Theorem: Let Φ be a QBF, and let $R \subseteq \langle \mathsf{vars}_{\forall}(\Phi) \rangle$. The partial expansion $\exp(\Phi, R)$ is unsatisfiable if, and only if, $R \supseteq \mathsf{rng}(h)$ for some countermodel h of Φ.

- For each $\alpha \in \langle X \rangle$, $R \supseteq \mathsf{rng}(h_\alpha)$ for some countermodel h_α of $\Phi[\alpha]$.
- Construct a countermodel for Φ:

  $$\begin{array}{ccccc} h & : & \langle \mathsf{vars}_{\exists}(\Phi) \rangle & \to & \langle \mathsf{vars}_{\forall}(\Phi) \rangle \\ & & \beta & \mapsto & h_{\beta\restriction X}(\beta) \end{array}$$

  and check it satisfies the countermodel definition
- Observe that $\mathsf{rng}(h) = \bigcup_{\alpha \in \langle X \rangle} \mathsf{rng}(h_\alpha) \subseteq R$

A Very Easy ∀Exp+Res Lower Bound

For $n \geq 1$, the pigeonhole formula PHP_n is the conjunction of

- $(x_{i,1} \vee \cdots \vee x_{i,n})$ for $1 \leq i \leq n+1$, and
- $(\overline{x_{i,j}} \vee \overline{x_{i',j}})$ for $1 \leq i < i' \leq n+1$ and $1 \leq j \leq n$.

- Pigeonhole formulas require exponential size resolution refutations
- Form a prenex QBF by quantifying all variables exisentially
- No universal variables - so the expansion is exactly the pigeonhole formula: $PHP_n = \exp(PHP_n)$
- Hence these 'QBFs' require exponential size ∀Exp+Res refutations

Propositional hardness transfers to QBF

- If $\phi_n(X)$ is hard for resolution, then $\exists X \, \phi_n(X)$ is hard for $\forall$Exp+Res.
- propositional hardness (Σ_1): not what we want to study
- we want QBF systems with proof size modulo propositional hardness
- so we need a method of elimating Σ_1 (propositional) hardness from the proof size measure

Oracles

- We borrow an idea from complexity theory
- An oracle is a Turing Machine with a black box that can decide a specified decision problem in a single time step
- For example, a TM with a SAT oracle can solve any NP problem in polynomial time
- Allows us to study complexity modulo NP (or any complexity class)

Genuine QBF hardness

- can be modelled precisely by allowing NP oracles in QBF proofs
- informally: all 'essentially propositional' derivations are allowed in a single inference
- in line with QBF solvers using embedded SAT solvers

Genuine Lower Bounds in $\forall$Exp+Res

- Replace resolution and weakening with the following rule

$$\text{oracle:} \qquad \frac{C_1, \ldots, C_k}{C} \qquad C_1 \wedge \cdots \wedge C_k \vDash C$$

Genuine Lower Bounds in $\forall$Exp+Res

oracle: $$\frac{C_1, \dots, C_k}{C} \qquad C_1 \wedge \dots \wedge C_k \vDash C$$

- The resolution phase is given for free (exactly one inference to refute the expansion)
- Therefore, proof size is effectively defined by the number of axioms
- precisely: given a CNF F, the minimal size of a refutation is the minimal cardinality of an unsatisfiable subset of clauses $(+1)$
- Therefore genuine hardness is characterised by large expansion

Characterisation of Genuine Lower Bounds

Theorem: Let Φ be a QBF, and let $R \subseteq \langle \mathsf{vars}_{\forall}(\Phi) \rangle$. The partial expansion $\mathsf{exp}(\Phi, R)$ is unsatisfiable if, and only if, $R \supseteq \mathsf{rng}(h)$ for some countermodel h of Φ.

- This theorem completely characterises genuine lower bounds in $\forall$Exp+Res
- By characterising expansion size in terms of countermodel range
- There are short (oracle) refutations of Φ if, and only if, $\sigma(\Phi)$ is small