Semi-Algebraic Proof Systems for QBF

Olaf Beyersdorff[1] Ilario Bonacina[2] **Kaspar Kasche**[1]
Meena Mahajan[3] Luc Spachmann[1]

[1] Friedrich Schiller University Jena
[2] UPC Barcelona
[3] The Institute of Mathematical Sciences, Chennai

August 12, 2025

Proof Systems

Why?

- theoretical insights and connections to complexity theory
- certifying solvers

How?

- Proof system P
- Formula φ, UNSAT resp. false QBF
- proof π of φ in P

Proof systems

Resolution

QU-Resolution

Proof systems

Resolution	QU-Resolution
geometric (Cutting Planes)	Q-Cutting Planes

Proof systems

Resolution	QU-Resolution
geometric (Cutting Planes)	Q-Cutting Planes
logical (Frege)	Q-Frege

Proof systems

Resolution	QU-Resolution
geometric (Cutting Planes)	Q-Cutting Planes
logical (Frege)	Q-Frege
(semi-)algebraic	**?**

Proof systems

Resolution	(line-based)	QU-Resolution
geometric (Cutting Planes)	(line-based)	Q-Cutting Planes
logical (Frege)	(line-based)	Q-Frege
(semi-)algebraic	(static)	**?**

universal reduction

$$\frac{L}{L[u=b]}(\forall\text{red});\, b \in \{0,1\},\, u \text{ is universal and rightmost in } L$$

- turns (almost) all line-based propositional proof systems into QBF systems (Beyersdorff, Bonacina, Chew, and Jan Pich 2020).

Roadmap

- *define* QBF versions of semi-algebraic proof systems
- see *simulations* and *separations* between these systems
- look at techniques for *upper* and *lower bounds*

Quantified Boolean Formulas

- extension of propositional logic
- prenex form: $\exists X_1 \forall U_1 \exists X_2 \dots \forall U_d \exists X_{d+1} : \varphi$
- recursive definition of truth value:
  - $(\forall u : Q)$ is true if both $Q[u = 0]$ and $Q[u = 1]$ are true
  - $(\exists x : Q)$ is true if $Q[u = 0]$ or $Q[u = 1]$ is true
- variables can be 0 or 1

The Evaluation Game

- two players, existential ($\exists$) and universal ($\forall$)
- assign their respective variables in order according to the prefix
- universal player wins if matrix becomes false, otherwise existential player wins

On a QBF Q, the universal player has a winning strategy if and only if Q is false.

(Semi-)Algebraic proof systems for UNSAT

- to apply to CNF: convert clauses to monomials
- $a \vee b \vee \overline{c}$ becomes $\overline{a} \cdot \overline{b} \cdot c$
- monomial is 0 iff clause is satisfied, positive otherwise

(Semi-)Algebraic Proof Systems for UNSAT

Proof is algebraic identity in $\mathbb{Q}$:

$$\sum q_p p \qquad\qquad + q + 1 = 0$$

- p are input clauses or additional axioms
  - $x^2 - x = 0$
  - $x + \overline{x} - 1 = 0$
- q_p are arbitrary polynomials
- q is nonnegative on Boolean inputs
  - Nullstellensatz: $q = 0$
  - Sherali-Adams: q only has nonnegative coefficients
  - Sum Of Squares: q is sum of squares

(Semi-)Algebraic Proof Systems for QBF

QBF given: $\exists X_1 \forall U_1 \exists X_2 \dots \forall U_d \exists X_{d+1} : \varphi$

Proof is algebraic identity in $\mathbb{Q}$:

$$\sum q_p p + \sum \mathbf{q_u}(\mathbf{1} - \mathbf{2u}) + q + 1 = 0$$

- p are input clauses or additional axioms
  - $x^2 - x = 0$
  - $x + \overline{x} - 1 = 0$
- q_p are arbitrary polynomials
- polynomial q_u for every universal variable u; only in variables left of u
- q is nonnegative on Boolean inputs
  - Q-Nullstellensatz: $q = 0$
  - Q-Sherali-Adams: q only has nonnegative coefficients
  - Q-Sum Of Squares: q is sum of squares

Soundness

$$\sum q_p p + \sum q_u(1-2u) + q + 1 = 0$$

Soundness: A true QBF cannot have a valid refutation.

- true QBF $\Rightarrow$ existential winning strategy S
- universal player plays randomly

$\Rightarrow$ random distribution on Boolean assignments; matrix is always satisfied

- consider $\mathbb{E}\left[\sum q_p p + \sum q_u(1-2u) + q + 1\right]$

Soundness

$$\sum q_p p + \sum q_u(1-2u) + q + 1 = 0$$

Soundness: A true QBF cannot have a valid refutation.

- true QBF $\Rightarrow$ existential winning strategy S
- universal player plays randomly

$\Rightarrow$ random distribution on Boolean assignments; matrix is always satisfied

- consider $\mathbb{E}\left[\sum q_p p + \sum q_u(1-2u) + q + 1\right]$
  - $\mathbb{E}[q_p p] = 0$ (matrix is satisfied)
  - $\mathbb{E}[q_u(1-2u)] = 0$ (balance between $u = 0$ and $u = 1$)
  - $\mathbb{E}[q] \geq 0$ ($q \geq 0$ always)
  - $\mathbb{E}[1] = 1$

  $\Rightarrow$ $\mathbb{E}\left[\sum q_p p + \sum q_u(1-2u) + q + 1\right] \geq 1$

Size measures

$$\sum q_p p + \sum q_u(1 - 2u) + q + 1 = 0$$

Proof size

The size of a semialgebraic proof is the total number of monomials in all of its polynomials.

Size measures

$$\sum q_p p + \sum q_u(1-2u) + q + 1 = 0$$

Proof size

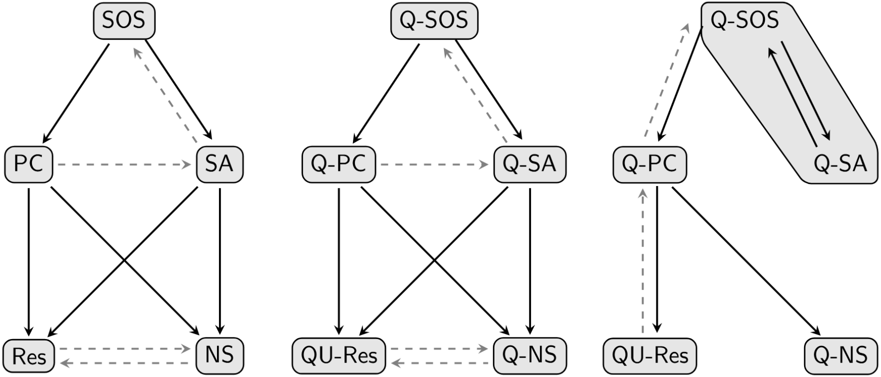
The size of a semialgebraic proof is the total number of monomials in all of its polynomials.

- hard problem for Q-SOS: take hard problem for SOS, add existential quantifiers
- looking for *genuine QBF hardness*

Proof q-size

The q-size of a semialgebraic proof is the total number of monomials in the q_u polynomials.

Simulation order



(a) propositional systems simulations w.r.t. size

(b) QBF systems simulations w.r.t. size

(c) QBF systems simulations w.r.t. qsize

Techniques

- score-based games
- strategy extraction to polynomial threshold functions
- size-degree lower bounds
- Q-pseudo-expectations

The score-based game

- two players, $\exists$ and $\forall$
- go over variables in prefix order
- existential variable: assigned by existential player
- universal variable u:
  - universal player picks preference s_u
  - existential player picks value $u = b$, $b \in \{0, 1\}$
  - universal player scores $s_u(2b - 1)$ points
- universal player wins if matrix is falsified or final score is > 0

The score-based game: example

$$\exists x_1 \forall u_1 \exists x_2 \forall u_2 . (x_1 \vee u_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{u_1} \vee x_2) \wedge (\overline{x_2} \vee u_2)$$

- initial score $= 0$
- Player$_\exists$ sets $x_1 = 1$.

The score-based game: example

$$\exists x_1 \forall u_1 \exists x_2 \forall u_2 . (x_1 \vee u_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{u_1} \vee x_2) \wedge (\overline{x_2} \vee u_2)$$

- initial score $= 0$
- Player$_\exists$ sets $x_1 = 1$.
- u_1:
  - Player$_\forall$ picks $s_{u_1} = -3$.
  - Player$_\exists$ sets $u_1 = 0$.
  - Player$_\forall$ gains score $s_{u_1}(2u_1 - 1) = 3$. New score: 3

The score-based game: example

$$\exists x_1 \forall u_1 \exists x_2 \forall u_2 . (x_1 \vee u_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{u_1} \vee x_2) \wedge (\overline{x_2} \vee u_2)$$

- initial score $= 0$
- $\text{Player}_\exists$ sets $x_1 = 1$.
- u_1:
  - $\text{Player}_\forall$ picks $s_{u_1} = -3$.
  - $\text{Player}_\exists$ sets $u_1 = 0$.
  - $\text{Player}_\forall$ gains score $s_{u_1}(2u_1 - 1) = 3$. New score: 3
- $\text{Player}_\exists$ sets $x_2 = 0$.

The score-based game: example

$$\exists x_1 \forall u_1 \exists x_2 \forall u_2 . (x_1 \vee u_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{u_1} \vee x_2) \wedge (\overline{x_2} \vee u_2)$$

- initial score $= 0$
- Player$_\exists$ sets $x_1 = 1$.
- u_1:
  - Player$_\forall$ picks $s_{u_1} = -3$.
  - Player$_\exists$ sets $u_1 = 0$.
  - Player$_\forall$ gains score $s_{u_1}(2u_1 - 1) = 3$. New score: 3
- Player$_\exists$ sets $x_2 = 0$.
- u_2:
  - Player$_\forall$ picks $s_{u_2} = 1$.
  - Player$_\exists$ sets $u_1 = 0$.
  - Player$_\forall$ gains score $s_{u_2}(2u_2 - 1) = -1$. New score: 2

The score-based game: example

$$\exists x_1 \forall u_1 \exists x_2 \forall u_2 . (x_1 \vee u_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{u_1} \vee x_2) \wedge (\overline{x_2} \vee u_2)$$

- initial score $= 0$
- Player$_\exists$ sets $x_1 = 1$.
- u_1:
  - Player$_\forall$ picks $s_{u_1} = -3$.
  - Player$_\exists$ sets $u_1 = 0$.
  - Player$_\forall$ gains score $s_{u_1}(2u_1 - 1) = 3$. New score: 3
- Player$_\exists$ sets $x_2 = 0$.
- u_2:
  - Player$_\forall$ picks $s_{u_2} = 1$.
  - Player$_\exists$ sets $u_1 = 0$.
  - Player$_\forall$ gains score $s_{u_2}(2u_2 - 1) = -1$. New score: 2
- φ is true, but score is positive $\Rightarrow$ Player$_\forall$ wins

The score-based game

- universal player can win iff QBF is false (same as evaluation game)
- provides upper bounds for e.g. Majority formulas

Theorem

For a given false QBF, encode the universal winning strategies as polynomials. The minimal number of monomials in such a strategy equals the qsize of the shortest Q-SOS refutation.

Majority

Majority(n):

$$\exists x_1 \dots x_n \forall u \exists t_0 \dots t_m . \left(u \leftrightarrow \left(\sum_{i=1}^{n} x_i \geq \frac{n}{2} \right) \text{ encoded using } t_j \text{ variables} \right)$$

Majority

Majority(n):

$$\exists x_1 \dots x_n \forall u \exists t_0 \dots t_m . \left(u \leftrightarrow \left(\sum_{i=1}^{n} x_i \geq \frac{n}{2} \right) \text{ encoded using } t_j \text{ variables} \right)$$

Theorem

The Majority formulas have Q-SOS proofs of qsize $O(n)$.

$$s_u = \sum_{i=1}^{n} x_i - \frac{n}{2} + \frac{1}{4}$$

- $\sum x_i \geq \frac{n}{2}$, $u = 0$: matrix is false
- $\sum x_i \geq \frac{n}{2}$, $u = 1$: s_u is positive, receive positive score
- $\sum x_i < \frac{n}{2}$, $u = 0$: s_u is negative, receive positive score
- $\sum x_i < \frac{n}{2}$, $u = 1$: matrix is false

Strategy extraction

Parity:

$$\exists x_1 \dots x_n \forall u \exists t_1 \dots t_n . (t_1 = x_1) \wedge \bigwedge_{i=2}^{n} (t_i = t_{i-1} \oplus x_i) \wedge (u \neq x_n)$$

Theorem

The Parity formulas require Q-SOS refutations of size $O(2^n)$.

- from a short refutation, we could extract a short polynomial threshold function computing the parity of its inputs
- we know exponential lower bounds for polynomial threshold functions

Size-degree relations

Theorem

If a QBF in n variables has a Q-SOS refutation of qsize s, it has a refutation of existential q-degree $O(\sqrt{n \log s})$.

- existential q-degree: largest number of existential variables of all the monomials in q_u
- proof: very similar to size-width in Ben-Sasson and Wigderson 2001
- linear degree lower bounds lead to exponential size lower bounds

Pseudo-expectations

- variant of lower bound technique from propositional semi-algebraic proof systems
- gives lower bounds on existential q-degree (highest existential degree in q_u polynomials) of proof
- use size-degree to obtain lower bound on proof size

Pseudo-expectations

To rule out a Q-SOS proof $\sum q_p p + \sum q_u(1 - 2u) + q + 1 = 0$, find $\tilde{\mathbb{E}}$ such that:

- $\tilde{\mathbb{E}}$ is linear
- $\tilde{\mathbb{E}}[1] = 1$;
- $\tilde{\mathbb{E}}[q + \sum q_p p] \geq 0$;
- $\tilde{\mathbb{E}}[\sum q_u(1 - 2u)] \geq 0$.

Proof technique: $\tilde{\mathbb{E}}$ exists for any Q-SOS proof of degree $< d$
$\Rightarrow$ minimal proof degree d

Conclusion

$$\sum q_p p + \sum q_u(1 - 2u) + q + 1 = 0$$

- natural extension of Nullstellensatz, Sherali-Adams, and Sum of Squares to QBF
- simulation order is similar to propositional case
- intuition via new score-based game
- variety of lower bounds techniques
  - strategy extraction
  - size-degree relations
  - pseudo-expectations

Bibliography

Ben-Sasson, Eli and Avi Wigderson (2001). "Short proofs are narrow - resolution made simple". In: *J. ACM* 48.2, pp. 149–169. DOI: 10.1145/375827.375835.

Beyersdorff, Olaf, Ilario Bonacina, and Leroy Chew (2016). "Lower Bounds: From Circuits to QBF Proof Systems". In: *Proc. ACM Conference on Innovations in Theoretical Computer Science (ITCS'16)*, pp. 249–260. DOI: 10.1145/2840728.2840740.

Beyersdorff, Olaf, Ilario Bonacina, Leroy Chew, and Jan Pich (2020). "Frege Systems for Quantified Boolean Logic". In: *J. ACM* 67.2. Preliminary versions of this work appeared as Beyersdorff, Bonacina, and Chew 2016 and ; Beyersdorff and Ján Pich 2016., 9:1–9:36. DOI: 10.1145/3381881.

Beyersdorff, Olaf and Ján Pich (2016). "Understanding Gentzen and Frege systems for QBF". In: *Proc. ACM/IEEE Symposium on Logic in Computer Science (LICS)*. DOI: 10.1145/2933575.2933597.