Nullstellensatz and Positivstellensatz

from

cut-elimination

Christophe Raffalli

LAMA, UMR 5127

Proof theory ?

What is it ?

Study of proof transformations

What are its applications ?

- Algorithm discovery (not today)
- Proving new theorems (today, just a first small step)

What is a proof ?

- Resolution proof $\Longrightarrow$???
- Hilbert system $\Longrightarrow$ first-order theory: $\mathsf{K}\,x\,y = x$ and $\mathsf{S}\,x\,y\,z = x\,z\,(y\,z)$
- Natural deduction $\Longrightarrow$ λ-calculus, $\lambda\mu$-calculus
- Sequent calculus $\Longrightarrow$ the nicest system from the view point of algebra

Why so many structures ?

What is a proof ?

- Resolution proof $\Longrightarrow$???
- Hilbert system $\Longrightarrow$ first-order theory: $\mathsf{K}\,x\,y = x$ and $\mathsf{S}\,x\,y\,z = x\,z\,(y\,z)$
- Natural deduction $\Longrightarrow$ λ-calculus, $\lambda\mu$-calculus
- Sequent calculus $\Longrightarrow$ the nicest system from the view point of algebra

Why so many structures ?

Why so many rings ?

What is a proof ?

- Resolution proof $\Longrightarrow$???
- Hilbert system $\Longrightarrow$ first-order theory: $\mathsf{K}\,x\,y = x$ and $\mathsf{S}\,x\,y\,z = x\,z\,(y\,z)$
- Natural deduction $\Longrightarrow$ λ-calculus, $\lambda\mu$-calculus
- Sequent calculus $\Longrightarrow$ the nicest system from the view point of algebra

Why so many structures ?

Proof as algorithm ... extends polynomials.

Proof transformations

Proof reduction/normalisation (not today)

- Correct program extraction
- Algorithm discovery: when using a non constructive lemma

Proof of A to proof of B transformation

- Alternative to model theory (today).
- When the theory is complete equivalent to proving $A \Rightarrow B$ (today).
- Alternative to a proof of $A \Rightarrow B$ (future, depend upon the theories)

Hilberts' nullstellensatz

If

- $\mathbb{A}$ is an integral domain,
- $P_1, \ldots, P_n, Q \in \mathbb{A}[X_1, \ldots, X_d]$,
- $P_1 = \ldots = P_n = 0 \Rightarrow Q = 0$ true in the algebraic closure,

then

$$\exists e \in \mathbb{N} \text{ and } \exists A_1, \ldots, A_n \in \mathbb{A}[X_1, \ldots, X_d] \text{ such that}$$
$$Q^e = A_1 P_1 + \ldots + A_n P_n,$$

or

Q is in the radical ideal generated by $P_1, \ldots, P_n$.

Hilbert, Hermann, Kollár, ...

Exponential bounds when $Q = 1$ and Rabinowitsch trick ($P_0 = 1 - QY$)

Hilberts' 17th problem, positivstellenstaz

Can we write a positive polynomial as a sum of squares of rational fractions?

Motzkin's polynomial requires fractions:

$$1 + x^2y^4 + x^4y^2 - 3x^2y^2$$

If

- $\mathbb{A}$ is a totally ordered ring,
- $P_1, \ldots, P_n, Q \in \mathbb{A}[X_1, \ldots, X_d]$,
- $P_1 \geqslant 0, \ldots, P_n \geqslant 0 \Rightarrow Q \geqslant 0$ (i.e. $P_1 \geqslant 0, \ldots, P_n \geqslant 0, -Q > 0 \Rightarrow \bot$) in the real closure,

then

$$\exists e \in \mathbb{N} \text{ and } \exists C_1, \ldots, C_n \in \mathscr{C}[P_1, \ldots, P_n, -Q] \text{ such that}$$
$$C_1P_1 + \ldots + C_nP_n + (-Q)^e = 0,$$

Artin, Kreisel, Krivine, Stengle, Coste, Roy, Lombardi, Perrucci

Positivstellenstaz, effective proofs

- Hörmander tableau (generalisation of Sturm's sequences) or cylindrical decomposition to decide the sign on $\mathbb{R}^n$.
- Each step of the proof transforms algebraic certificates.
- The final certificate is what we want.

Needs a lot of clever ideas ! Some of them which we will reuse (not all).

xxxstellenstaz from cut-elimination

- Start from a proof given by any algorithm
- Translate it in a specific sequent calculus
- Eliminate cuts
- Final transformations of the proof for existential axioms
- Extract the certificate

Friedman, Whiteley (1989), this work

Polynomial BDD (An intermediate certificate)

- Start from a proof given by any algorithm
- Translate it in a specific sequent calculus
- Eliminate cuts
- Final transformations of the proof for existential axioms
- Extract the PBDD
- Compute the final certificate (3 ways)

new way: lower degree, no control on the zero of the denominator

Formula and sequent

Formula

- $P \in \mathbb{A}[\mathcal{V}]$ means $P = 0$ or $P \geqslant 0$ ($\mathcal{V}$ a countable set of variables $\{X_1, \ldots, X_n, \ldots\}$)
- $A \vee B$ disjunction
- $\neg A$ negation
- $\forall X\ A$
- $A \Rightarrow B := (\neg A) \vee B$
- $A \wedge B := \neg(\neg A \vee \neg B)$
- $\exists X\ A := \neg(\forall X\ \neg A)$

Sequent (Two sets of formulae)

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_p$$

Deduction rules

upper sequents are provable (premises) $\Longrightarrow$ the lower one (conclusion) is too.

$$\frac{}{\Gamma, A \vdash A, \Delta}\text{Axiom} \qquad \frac{\Gamma \vdash \Delta, A \quad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}\text{Cut}$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\neg_l \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\neg_r$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\vee_l \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\vee_r$$

$$\frac{\Gamma, A[X \leftarrow P], \forall X\ A \vdash \Delta}{\Gamma, \forall X\ A \vdash \Delta}\forall_l \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall X\ A, \Delta}\forall_r^*$$

Gentzen's cut elimination theorem (consistency)

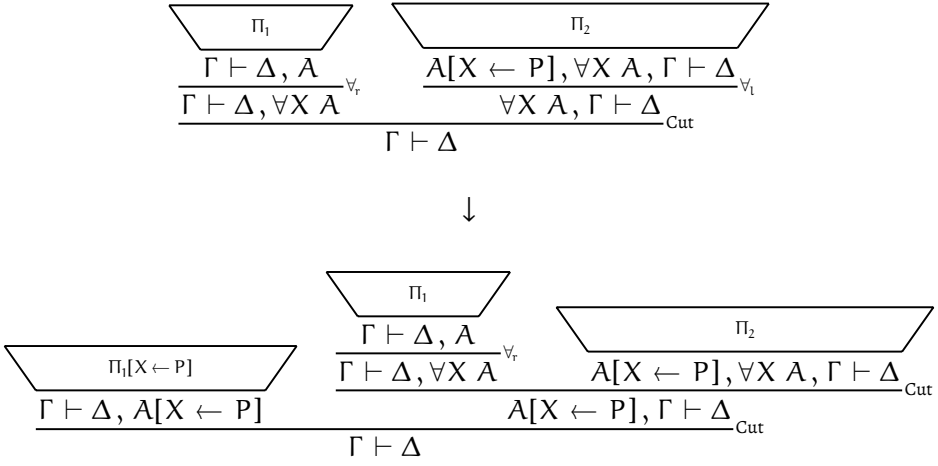
Commutation

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\Gamma, B[X \leftarrow P], \forall X\ B \vdash \Delta, A}}{\Gamma, \forall X\ B \vdash \Delta, A}\forall_l \qquad \dfrac{\Pi_2}{A, \Gamma, \forall X\ B \vdash \Delta}}{\Gamma, \forall X\ B \vdash \Delta}\text{Cut}$$

$$\downarrow$$

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\Gamma, B[X \leftarrow P], \forall X\ B \vdash \Delta, A} \qquad \dfrac{\dfrac{\Pi_2}{A, \Gamma \vdash \Delta}}{A, \Gamma, B[X \leftarrow P], \forall X\ B \vdash \Delta}\text{Weak}_l}{\Gamma, B[X \leftarrow P], \forall X\ B \vdash \Delta}\text{Cut}}{\Gamma, \forall X\ B \vdash \Delta}\forall_l$$

Reduction


Π1
Γ ⊢ Δ, A
∀r
Γ ⊢ Δ, ∀X A
Π2
A[X ← P], ∀X A, Γ ⊢ Δ
∀l
∀X A, Γ ⊢ Δ
Cut
Γ ⊢ Δ
↓
Π1[X ← P]
Γ ⊢ Δ, A[X ← P]
Π1
Γ ⊢ Δ, A
∀r
Γ ⊢ Δ, ∀X A
Π2
A[X ← P], ∀X A, Γ ⊢ Δ
Cut
A[X ← P], Γ ⊢ Δ
Cut
Γ ⊢ Δ

Algebraic axiom

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta}\, \mathcal{G}-\text{Axiom}$$

Conditions:

1. $\mathcal{R}$ generalises the usual axiom
2. $\mathcal{R}$ allows weakening, reordering and contraction
3. $\mathcal{R}$ allows substitution
4. $\mathcal{R}$ allows cuts

Algebraic axiom

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta}\, \mathcal{G}-\text{Axiom}$$

Conditions:

1. $\mathcal{R}$ generalises the usual axiom
2. $\mathcal{R}$ allows weakening, reordering and contraction
3. $\mathcal{R}$ allows substitution
4. $\mathcal{R}$ allows cuts

$$\forall P\ \exists J\ ((P), (P), J) \in \mathcal{R} \quad (1)$$

Algebraic axiom

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta} \mathcal{G}\text{-Axiom}$$

Conditions:

1. $\mathcal{R}$ generalises the usual axiom
2. $\mathcal{R}$ allows weakening, reordering and contraction
3. $\mathcal{R}$ allows substitution
4. $\mathcal{R}$ allows cuts

$$\overrightarrow{P_1} \sqsubset \overrightarrow{P_2}, \overrightarrow{Q_1} \sqsubset \overrightarrow{Q_2}, \left(\overrightarrow{P_1}, \overrightarrow{Q_1}, J\right) \in \mathcal{R} \Rightarrow \exists J' \left(\overrightarrow{P_2}, \overrightarrow{Q_2}, J'\right) \in \mathcal{R} \quad (2)$$

Algebraic axiom

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta}\, \mathcal{G}\text{-Axiom}$$

Conditions:

1. $\mathcal{R}$ generalises the usual axiom
2. $\mathcal{R}$ allows weakening, reordering and contraction
3. $\mathcal{R}$ allows substitution
4. $\mathcal{R}$ allows cuts

$$\left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R} \Rightarrow \exists J' \left(\overrightarrow{P}[X \leftarrow T], \overrightarrow{Q}[X \leftarrow T], J'\right) \in \mathcal{R} \quad (3)$$

Algebraic axiom

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta}\, \mathcal{G}-\text{Axiom}$$

Conditions:

1. $\mathcal{R}$ generalises the usual axiom
2. $\mathcal{R}$ allows weakening, reordering and contraction
3. $\mathcal{R}$ allows substitution
4. $\mathcal{R}$ allows cuts

$$\left(\overrightarrow{P}, \left(\overrightarrow{Q}, T\right), J_1\right) \in \mathcal{R}, \left(\left(\overrightarrow{P}, T\right), \overrightarrow{Q}, J_2\right) \in \mathcal{R} \Rightarrow \exists J_3 \ \left(\overrightarrow{P}, \overrightarrow{Q}, J_3\right) \in \mathcal{R} \quad (4)$$

Examples

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta}\,\mathcal{R}$$

nullstellensatz

$$\left(\overrightarrow{P}, \overrightarrow{Q}, \left(\overrightarrow{A}, \overrightarrow{e}\right)\right) \in \mathcal{R} \iff A_1P_1 + \ldots + A_nP_n = Q_1^{e_1} \ldots Q_m^{e_m}$$

positivstellensatz

$$\left(\overrightarrow{P}, \overrightarrow{Q}, \left(\overrightarrow{C}, \overrightarrow{e}\right)\right) \in \mathcal{R} \iff C_1P_1 + \ldots + C_nP_n + (-Q_1)^{e_1} \ldots (-Q_m)^{e_m} = 0$$

$$C_i \in \mathscr{C}(P_1, \ldots, P_n, -Q_1, \ldots, -Q_m)$$

To check:

1. Consistency : the 4 previous properties
2. Completeness : proving the ring / ordered ring axioms

Proof of (4)

From axioms proving $\Gamma \vdash \Delta, Q$ et $Q, \Gamma \vdash \Delta$

$\Rightarrow C_1 + C_2 Q + M_1 = 0$ et $C_3 + C_4(-Q) + (-Q)^e M_2 = 0$

$\Rightarrow C_2(-Q) = C_1 + M_1$

$\Rightarrow C_2^e C_3 + C_4 C_2^{e-1}(C_1 + M_1) + (C_1 + M_1)^e M_2 = 0$

$\Rightarrow C_5 + M_1^e M_2 = 0$

$$C_i \in \mathscr{C}(\Gamma, -\Delta),\ M_i \in \mathscr{M}(-\Delta)$$

Some axioms

- $P \geqslant 0 := P$
- $P > 0 := \neg(-P)$
- $P = 0 := P \wedge -P$ (good in negative position)
- $P = 0 := -P^2$ (good in positive position)

$$P \geqslant 0 \vee P < 0 \iff \vdash P \vee \neg(P)$$

$$P > 0 \Rightarrow P \geqslant 0 \iff \vdash \neg\neg(-P) \vee P \Longleftarrow P^2 + (-P)P = 0$$

Almost an effective proof of the positivstellensatz

1. Assume $\vdash Q \geqslant 0$ is true
2. $\vdash Q$ is provable in the previous sequent calculus (decidability)
3. $\vdash Q$ is provable by a cut-free proof
4. $T_1^2 + \ldots + T_n^2 + S_1^2(-Q) + \ldots + S_p^2(-Q) + (-Q)^e = 0$

Almost an effective proof of the positivstellensatz

1. Assume $\vdash Q \geqslant 0$ is true in a real closed field $\mathbb{K}$
2. $\vdash Q$ is provable in the previous sequent calculus
   in the ring $\mathbb{A}$ generated by the coefficients (completeness theorem)
3. $\vdash Q$ is provable by a cut-free proof
4. $T_1^2 + \ldots + T_n^2 + S_1^2(-Q) + \ldots + S_p^2(-Q) + (-Q)^e = 0$

From ring to field

$$\frac{\Gamma, P\,X = 1 \vdash \Delta \qquad \Gamma, P = 0 \vdash \Delta}{\Gamma \vdash \Delta}\,\mathrm{Inv}$$

$$\frac{\Gamma, P(X) = 0 \vdash \Delta \qquad \Gamma, P(U)P(V) \geqslant 0 \vdash \Delta}{\Gamma \vdash \Delta}\,\mathrm{Clos}$$

Those rules may be eliminated ... when proving Π_1-formula.

- X not free in Γ and Δ
- Move the rule up to the axioms
- Only barrier: $\forall_l$ absent for cut-free proof of Π_1-formula
- Eliminate the rules

An effective proof of the positivstellensatz

1. Assume $\vdash Q \geqslant 0$ in a real closed field $\mathbb{K}$
2. $\vdash Q$ is provable in the previous sequent calculus with Inv and Clos (decidability)
3. $\vdash Q$ is provable by a cut-free proof
4. $\vdash Q$ is provable by a cut-free proof without Inv and Clos
5. $T_1^2 + \ldots + T_n^2 + S_1^2(-Q) + \ldots + S_p^2(-Q) + (-Q)^e = 0$

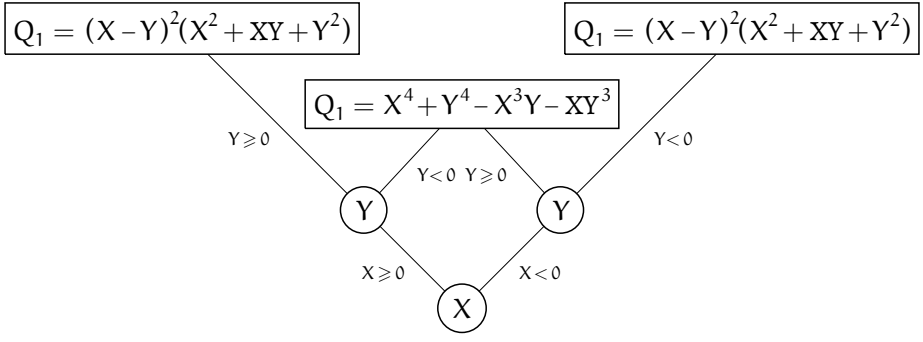
Polynomial BDD: binary trees

- $L(M, k, C) : P_1 \geqslant 0, \ldots, P_m \geqslant 0 ; S_1 > 0, \ldots, S_l > 0 \vdash Q_1, \ldots, Q_p$ if
  - $1 \leqslant k \leqslant n$,
  - $M \in \mathcal{M}(S_1, \ldots, S_l)$ and
  - $C \in \mathcal{C}(P_1, \ldots, P_m, S_1, \ldots, S_l)$,
  - $M\, Q_k = C$
- $If(R, T_1, T_2) \in P_1 \geqslant 0, \ldots, P_m \geqslant 0 ; S_1 > 0, \ldots, S_l > 0 \vdash Q_1, \ldots, Q_p$ if
  - $R \in \mathbb{A}[\mathcal{V}]$,
  - $T_1 : P_1, \ldots, P_m, R ; S_1, \ldots, S_l \vdash Q_1, \ldots, Q_p$ and
  - $T_2 : P_1, \ldots, P_m ; S_1, \ldots, S_l, -R \vdash Q_1, \ldots, Q_p$.

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, T : \overrightarrow{P}; \vdash \overrightarrow{Q}}{\Gamma \vdash \Delta}\,\mathcal{R}$$

Example of PBDD for $\vdash (X^3 - Y^3)(X - Y)$:

$$
\begin{aligned}
&\mathrm{If}(X,\ \mathrm{If}(Y,\ L(1,1,(X-Y)^2(X^2+2XY+Y^2)),\\
&\qquad\qquad L(1,1,(X^4+Y^4-X^3Y-XY^3))),\\
&\qquad\mathrm{If}(Y,\ L(1,1,(X^4+Y^4-X^3Y-XY^3)),\\
&\qquad\qquad L(1,1,(X-Y)^2(X^2+2XY+Y^2))))
\end{aligned}
$$



PBDD as intermediate certificate

- A correct sequent calculus
- Complete too
- Cut elimination costs less
- Recover Stengles's certificate
- Antother certificate is possible

Weak certificates

Assume:

$$P_1, \ldots, P_n \vdash Q$$

- Strong certificate:

$$C + (-Q)^{e_0} = 0 \text{ with } C \in \mathscr{C}(P_1, \ldots, P_n, -Q)$$

- Weak certificate:

$P_1, \ldots, P_n \vdash \bot$ or $C_1 Q = C_2$ with $C_1, C_2 \in \mathscr{C}(P_1, \ldots, P_n)$ and $C_1 \neq 0, C_2 \neq 0$

- Strong certificate from PBDD: product of the degrees
- Weak certificate from PBDD: sum of the degrees
- Unfortunately: still products when eliminating roots

A new way to combine certificates

$T = \mathrm{If}(S, T_1, T_2) : \Gamma ; \Delta \vdash Q$

- from T_1: $C_1 Q = C_2$
- from T_2: $D_1 Q = D_2$

Linear combination eliminating S:

A new way to combine certificates

$T = \mathrm{If}(S, T_1, T_2) : \Gamma ; \Delta \vdash Q$

- from T_1: $(C_1' S\, Q + C_1'' = C_2' S + C_2'')$
- from T_2: $(D_1'(-S)\, Q + D_1'' = D_2'(-S) + D_2'')$

Linear combination eliminating S:

A new way to combine certificates

$T = \mathrm{If}(S, T_1, T_2) : \Gamma ; \Delta \vdash Q$

- from T_1: $(C_1' Q - C_2') S = -C_1'' Q + C_2''$
- from T_2: $(D_1' Q - D_2') (-S) = -D_1'' Q + D_2''$

Linear combination eliminating S:

A new way to combine certificates

$T = \mathrm{If}(S, T_1, T_2) : \Gamma ; \Delta \vdash Q$

- from T_1: $(C_1' Q - C_2')\, S = -C_1'' Q + C_2''$
- from T_2: $(D_1' Q - D_2')\,(-S) = -D_1'' Q + D_2''$

Linear combination eliminating S:

$$(D_1' Q - D_2')(-C_1'' Q + C_2'') + (C_1' Q - C_2')(-D''1 Q + D_2'') = 0$$

A new way to combine certificates

$T = \mathrm{If}(S, T_1, T_2) : \Gamma ; \Delta \vdash Q$

- from T_1: $(C_1' Q - C_2') S = -C_1'' Q + C_2''$
- from T_2: $(D_1' Q - D_2') (-S) = -D_1'' Q + D_2''$

Linear combination eliminating S:

$$(D_1' C_2'' + D_2' C_1'' + C_1' D_2'' + C_2' D_1'') Q = D_1' C_1'' Q^2 + C_1' D_1'' Q^2 + D_2' C_2'' + C_2' D_2''$$

A new way to combine certificates

$T = \mathrm{If}(S, T_1, T_2) : \Gamma ; \Delta \vdash Q$

- from T_1: $(C_1' Q - C_2') S = -C_1'' Q + C_2''$
- from T_2: $(D_1' Q - D_2')(-S) = -D_1'' Q + D_2''$

Linear combination eliminating S:

$$(D_1' C_2'' + D_2' C_1'' + C_1' D_2'' + C_2' D_1'') Q = D_1' C_1'' Q^2 + C_1' D_1'' Q^2 + D_2' C_2'' + C_2' D_2''$$

What to do when this gives 0 ?

Simplification of the PBDD !

Formal roots

root as function symbols

- $\rho(P, A, B)$ a root of P between A and B.
- $1/P$

Equationnal certificates are meaningless with formal roots

May contain roots which do not exists simultaneously.

This does not happens with PBDD

On each branch all roots and inverse are defined.

Existential

- Assume:

$$P_1, \ldots, P_n \vdash \exists X\ Q$$

- A normal proof gives a PBDD:

$$T : P_1, \ldots, P_n \vdash Q[X \leftarrow S_1], \ldots, Q[X \leftarrow S_n]$$

- The branch of the PBDD tells you a way to choose the witness.

Implementation: Motzkin polynomial

$$M = (1 + x^4y^2 + y^4x^2)^3 - 27x^6y^6 \geqslant 0$$

Strong Direct ??? Strong from PBDD: degree 72 Weak: degree 48

$$M \left(\left(\frac{100}{9}\left(y^5x^5 - \frac{1}{2}y^6x^3 - \frac{1}{2}y^3x^6\right)^2 + \frac{25}{9}\left(y^6x^5 + y^5x^3 - 2y^3x^5\right)^2 + \frac{50}{3}\left(y^6x^3 - y^3x^6\right)^2 + \frac{50}{3}\left(y^4x^5 - y^3x^5\right)^2 + \frac{5}{9}\left(y^5x^6 - 2y^5x^4 + yx^5\right)^2 + \frac{5}{9}\left(y^3x^6 + y^5x^4 - 2yx^5\right)^2 + \frac{100}{9}\left(y^6x^6 - \frac{1}{2}y^8x^4 - \frac{1}{2}y^4x^8\right)^2 + \frac{25}{9}\left(y^6x^6 + y^8x^4 - 2y^4x^6\right)^2 + \frac{10}{3}\left(y^5x^4 - yx^6\right)^2 + \frac{35}{3}\left(y^3x^6 - yx^8\right)^2 + \right.\right.$$

$$\left.\left.\frac{5}{9}\left(y^5x^7 - 2y^5x^5 + y^3x^5\right)^2 + \frac{100}{9}\left(y^5x^7 - \frac{1}{2}y^5x^5 - \frac{1}{2}y^3x^5\right)^2 + \frac{40}{9}\left(y^7x^7 + y^7x^5 - 2y^5x^5\right)^2 + \frac{55}{3}\left(y^7x^5 - y^5x^5\right)^2 + \frac{20}{3}\left(y^7x^7 - y^5x^5\right)^2 + \frac{5}{9}\left(y^4x^8 - 2y^6x^6 + y^2x^6\right)^2 + \frac{5}{9}\left(y^4x^8 + y^6x^6 - 2y^2x^6\right)^2 + \frac{10}{9}\left(y^6x^8 + y^8x^6 - 2y^5x^6\right)^2 + \frac{10}{9}\left(y^6x^6 + y^8x^6 - 2y^4x^8\right)^2 + \frac{10}{3}\left(y^5x^7 - y^7x^5\right)^2\right)\right) =$$

$$\left(\frac{25}{9}\left(y^8x^{13} + 3y^{10}x^{11} + 3y^{12}x^9 + 3y^8x^9 + y^{14}x^7 - 21y^8x^7 + 3y^{10}x^5 + 3y^6x^5 + 3y^8x^5 + y^6x^3\right)^2 + \frac{200}{3}\left(y^9x^7 - \frac{1}{2}y^8x^7 - \frac{3}{2}y^7x^5 + \frac{1}{2}y^6x^5 + \frac{1}{2}y^5x^7\right)^2 + \frac{100}{9}\left(y^8x^9 + \frac{1}{2}y^8x^7 - \frac{1}{2}y^{10}x^5 - \frac{5}{2}y^8x^5 + \frac{1}{2}y^6x^7\right)^2 + \frac{200}{3}\left(y^8x^7 - \frac{1}{2}y^{10}x^5 - y^8x^5 + \frac{1}{2}y^7x^5\right)^2 + \right.$$

$$\left.\frac{5}{9}\left(y^7x^{14} + 3y^9x^{12} + 3y^{11}x^{10} + 3y^5x^{10} + y^{13}x^8 - 21y^7x^8 + 3y^9x^6 + 3y^3x^6 + 3y^5x^6 + yx^8\right)^2 + \frac{5}{9}\left(y^5x^{10} - y^7x^8 - 2y^9x^6 - y^3x^6 + 5y^5x^4 - 2yx^6\right)^2 + \frac{200}{3}\left(y^9x^{10} - \frac{1}{2}y^{13}x^8 - \frac{3}{2}y^9x^6 + \frac{1}{2}y^8x^4 + \frac{1}{2}y^5x^6\right)^2 + \frac{200}{9}\left(y^8x^{10} + \frac{1}{2}y^{13}x^8 - \frac{1}{2}y^{12}x^6 - \frac{5}{2}y^9x^6 + \frac{1}{2}y^8x^4 + y^5x^6\right)^2 + \right.$$

$$\left.\frac{10}{3}\left(y^7x^8 - 2y^9x^6 - y^5x^6 + 3y^5x^4 - yx^6\right)^2 + \frac{35}{3}\left(y^5x^{10} - 2y^7x^8 + 2y^5x^6 - yx^8\right)^2 + \frac{200}{3}\left(y^{10}x^8 - \frac{1}{2}y^{12}x^6 - y^9x^6 + \frac{1}{2}y^8x^6\right)^2 + \frac{5}{9}\left(y^9x^{15} + 3y^{11}x^{13} + 3y^{13}x^{11} + 3y^7x^{11} + y^5x^9 - 21y^9x^9 + 3y^{11}x^7 + 3y^9x^7 + 3y^7x^5 + y^9x^5\right)^2 + \right.$$

$$\left.\frac{10}{9}\left(y^7x^{11} - y^9x^9 - 2y^{11}x^7 - y^9x^7 + 5y^7x^5 - 2y^9x^5\right)^2 + \frac{200}{3}\left(y^7x^{11} - \frac{1}{2}y^9x^9 - \frac{3}{2}y^7x^7 + \frac{1}{2}y^7x^5 + \frac{1}{2}y^5x^5\right)^2 + \frac{200}{9}\left(y^7x^{11} + \frac{1}{2}y^9x^9 - \frac{1}{2}y^{11}x^7 - \frac{5}{2}y^9x^7 + \frac{1}{2}y^7x^5 + y^5x^5\right)^2 + \frac{20}{3}\left(y^7x^{11} + y^9x^9 - 3y^9x^7 - y^7x^5 + 2y^7x^7\right)^2 + \frac{5}{9}\left(y^7x^{11} + 2y^9x^9 + y^{11}x^7 - 4y^9x^7 - 4y^7x^5 + 4y^9x^5\right)^2 + \right.$$

$$\left.\frac{100}{9}\left(y^{10}x^{11} + \frac{1}{2}y^{12}x^9 - \frac{1}{2}y^{14}x^7 - \frac{5}{2}y^9x^7 + \frac{1}{2}y^{10}x^5 + y^9x^5\right)^2 + 160\left(y^9x^9 - y^5x^7 - y^7x^5 + y^5x^5\right)^2 + \frac{10}{3}\left(y^9x^9 - 2y^{11}x^7 - y^5x^7 + 3y^7x^5 - y^5x^5\right)^2 + \frac{55}{3}\left(y^9x^9 + y^{11}x^7 - y^5x^7 - 3y^7x^5 + 2y^5x^5\right)^2 + 90\left(y^{11}x^7 - 2y^7x^5 + y^5x^5\right)^2 + \frac{35}{3}\left(y^7x^{11} - 2y^9x^9 + 2y^7x^5 - y^5x^5\right)^2 + \right.$$

$$\left.\frac{200}{3}\left(y^9x^9 - \frac{1}{2}y^{11}x^7 - y^7x^7 + \frac{1}{2}y^7x^5\right)^2 + 20\left(y^7x^{11} - 2y^7x^7 + y^5x^7\right)^2 + \frac{10}{9}\left(y^9x^{12} - y^{13}x^{10} - 2y^{13}x^8 - y^7x^8 + 5y^9x^6 - 2y^5x^8\right)^2 + \frac{5}{9}\left(y^9x^{12} - y^{13}x^{10} - 2y^{13}x^8 - y^9x^8 + 5y^9x^6 - 2y^5x^8\right)^2 + \frac{200}{9}\left(y^9x^{12} + \frac{1}{2}y^{11}x^{10} - \frac{1}{2}y^{13}x^8 - \frac{5}{2}y^9x^8 + \frac{1}{2}y^9x^6 + y^5x^8\right)^2 + \right.$$

$$\left.\frac{20}{3}\left(y^9x^{12} + y^{11}x^{10} - 3y^7x^8 - y^9x^6 + 2y^5x^8\right)^2 + \frac{10}{9}\left(y^9x^{12} + 2y^{11}x^{10} + y^{13}x^8 - 4y^7x^8 - 4y^9x^6 + 4y^5x^8\right)^2 + \frac{10}{3}\left(y^9x^{10} - 2y^{13}x^8 - y^9x^8 + 3y^9x^6 - y^7x^6\right)^2 + \frac{55}{3}\left(y^{11}x^{10} + y^{13}x^8 - y^7x^8 - 3y^9x^6 + 2y^7x^6\right)^2 + \frac{35}{3}\left(y^9x^{12} - 2y^9x^{10} + 2y^9x^6 - y^7x^6\right)^2 + \right.$$

$$\left.\frac{10}{9}\left(y^9x^{13} - y^{15}x^{11} - 2y^{17}x^9 - y^9x^9 + 5y^7x^7 - 2y^9x^7\right)^2 + \frac{100}{9}\left(y^9x^{13} + \frac{1}{2}y^{15}x^{11} - \frac{1}{2}y^{17}x^9 - \frac{5}{2}y^9x^9 + \frac{1}{2}y^9x^7 + y^7x^7\right)^2 + \frac{20}{3}\left(y^9x^{13} + y^{15}x^{11} - 3y^9x^9 - y^9x^7 + 2y^7x^7\right)^2 + \frac{10}{9}\left(y^9x^{13} + 2y^{15}x^{11} + y^{17}x^9 - 4y^9x^9 - 4y^9x^7 + 4y^7x^7\right)^2 + \right.$$

$$\left.\frac{5}{9}\left(y^{13}x^{13} + 2y^{15}x^{11} + y^{15}x^9 - 4y^9x^9 - 4y^{11}x^7 + 4y^7x^7\right)^2 + 70\left(y^7x^{11} - y^9x^9 - y^5x^7 + y^7x^7\right)^2 + \frac{55}{3}\left(y^{15}x^{11} + y^{17}x^9 - y^9x^9 - 3y^9x^7 + 2y^9x^7\right)^2 + 20\left(y^9x^9 - y^{13}x^7 - y^5x^7 + y^7x^7\right)^2 + \frac{10}{3}\left(y^{13}x^{11} - y^{13}x^7 - 2y^5x^7 + 2y^7x^7\right)^2 + \frac{5}{9}\left(y^9x^{14} - y^9x^{12} - 2y^{13}x^{10} - y^5x^{10} + 5y^7x^8 - 2y^5x^8\right)^2 + \right.$$

$$\left.\frac{10}{9}\left(y^{15}x^{14} + 2y^{17}x^{12} + y^{19}x^{10} - 4y^9x^{10} - 4y^{11}x^8 + 4y^9x^8\right)^2 + \frac{10}{3}\left(y^9x^{12} - y^{13}x^8 - 2y^5x^8 + 2y^9x^6\right)^2 + \frac{5}{9}\left(y^9x^{15} + 2y^{13}x^{13} + y^{13}x^{11} - 4y^9x^9 + 4y^7x^7\right)^2 + \frac{10}{3}\left(y^9x^{13} - y^{17}x^9 - 2y^9x^9 + 2y^9x^7\right)^2\right)$$

Discussions

- Compute bounds ?
- What cut elimination strategy ?
- More modular/flexible ?
- Easier to extend/adapt ?
- Other proofs by induction on proofs ?

Thanks: Marie-Françoise Roy, Henri Lombardi, Daniel Perrucci

Typography and display by Patoline

Discussions

- Compute bounds ?
  Better to build directly a cut-free proof ?
- What cut elimination strategy ?

- More modular/flexible ?

- Easier to extend/adapt ?

- Other proofs by induction on proofs ?

Thanks: Marie-Françoise Roy, Henri Lombardi, Daniel Perrucci

Typography and display by Patoline

Discussions

- Compute bounds ?
  Better to build directly a cut-free proof ?
- What cut elimination strategy ?
  May lower the degree in practice ?
- More modular/flexible ?

- Easier to extend/adapt ?

- Other proofs by induction on proofs ?

Thanks: Marie-Françoise Roy, Henri Lombardi, Daniel Perrucci

Typography and display by Patoline

Discussions

- Compute bounds ?
  Better to build directly a cut-free proof ?
- What cut elimination strategy ?
  May lower the degree in practice ?
- More modular/flexible ?
  Reveals the role of proof theory.
- Easier to extend/adapt ?

- Other proofs by induction on proofs ?

Thanks: Marie-Françoise Roy, Henri Lombardi, Daniel Perrucci

Typography and display by Patoline

Discussions

- Compute bounds ?
  Better to build directly a cut-free proof ?
- What cut elimination strategy ?
  May lower the degree in practice ?
- More modular/flexible ?
  Reveals the role of proof theory.
- Easier to extend/adapt ?
  Yes ($\exp$, $\cos$, $\sin$, $\partial/\partial X$, $\int$), but which direction ?
- Other proofs by induction on proofs ?

Thanks: Marie-Françoise Roy, Henri Lombardi, Daniel Perrucci

Typography and display by Patoline