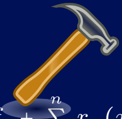
(Semi)Algebraic Proofs over $\{\pm 1\}$ Variables



$$\sum_{u=1}^{a} p_u f_u + \sum_{w=1}^{n} r_w (x^2 - 1) + \sum_{v=1}^{b} q_v^2 h_v = -1$$

Dmitry Sokolov

Banff International Research Station
January 20, 2020

LUND UNIVERSITY

KØBENHAVNS UNIVERSITET

Notation

$$(\mathcal{F}, \mathcal{H}) = \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ f_2(x_1, \dots, x_n) = 0 \\ \dots \\ f_a(x_1, \dots, x_n) = 0 \\ \hline h_1(x_1, \dots, x_n) > 0 \\ h_2(x_1, \dots, x_n) > 0 \\ \dots \\ h_s(x_1, \dots, x_n) > 0 \end{cases}$$

f_i, h_j are polynomials.

Notation

$$(\mathcal{F}, \mathcal{H}) = \begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_a(x_1, \ldots, x_n) = 0 \\ \hline h_1(x_1, \ldots, x_n) > 0 \\ h_2(x_1, \ldots, x_n) > 0 \\ \ldots \\ h_s(x_1, \ldots, x_n) > 0 \end{cases}$$

f_i, h_j are polynomials.

Range axiom R_i for a variable x_i:

- $\{\mathbf{0}, \mathbf{1}\}$ basis: $x_i^2 - x_i$;
- $\{\pm\mathbf{1}\}$ basis: $x_i^2 - 1$.

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

The **Polynomial Calculus** ($\texttt{PCR}^{\mathbb{F}}$) proof of $\mathcal{F}$ is a sequence $(p_1, p_2, p_3, \ldots, p_\ell)$:

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

The **Polynomial Calculus** ($\mathtt{PCR}^{\mathbb{F}}$) proof of $\mathcal{F}$ is a sequence $(p_1, p_2, p_3, \ldots, p_\ell)$:

- $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{R_j\}$;

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

The **Polynomial Calculus** ($\mathrm{PCR}^{\mathbb{F}}$) proof of $\mathcal{F}$ is a sequence $(p_1, p_2, p_3, \ldots, p_\ell)$:

- $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{R_j\}$;
- $p_i = x_j p_k$ for some j and $k < i$;

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

The **Polynomial Calculus** ($\mathtt{PCR}^{\mathbb{F}}$) proof of $\mathcal{F}$ is a sequence $(p_1, p_2, p_3, \ldots, p_\ell)$:

- $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{R_j\}$;
- $p_i = x_j p_k$ for some j and $k < i$;
- $p_i = \alpha p_k + \beta p_s$ for some $k, s < i$ and $\alpha, \beta \in \mathbb{F}$;

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

The **Polynomial Calculus** ($\mathtt{PCR}^{\mathbb{F}}$) proof of $\mathcal{F}$ is a sequence $(p_1, p_2, p_3, \ldots, p_\ell)$:

- $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{R_j\}$;
- $p_i = x_j p_k$ for some j and $k < i$;
- $p_i = \alpha p_k + \beta p_s$ for some $k, s < i$ and $\alpha, \beta \in \mathbb{F}$;
- $p_\ell = 1$.

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

The **Polynomial Calculus** ($\mathrm{PCR}^{\mathbb{F}}$) proof of $\mathcal{F}$ is a sequence $(p_1, p_2, p_3, \dots, p_\ell)$:

- $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{R_j\}$;
- $p_i = x_j p_k$ for some j and $k < i$;
- $p_i = \alpha p_k + \beta p_s$ for some $k, s < i$ and $\alpha, \beta \in \mathbb{F}$;
- $p_\ell = 1$.

$$\mathcal{F} = \begin{cases} xy - 1 = 0 \\ yz + 1 = 0 \\ x + z - 2 = 0 \end{cases}$$

Proof Systems

The **Sum-of-Squares** (SOS) proof of $(\mathcal{F}, \mathcal{H})$:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{n} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$f_u \in \mathcal{F}, h_v \in \mathcal{H} \cup 1$

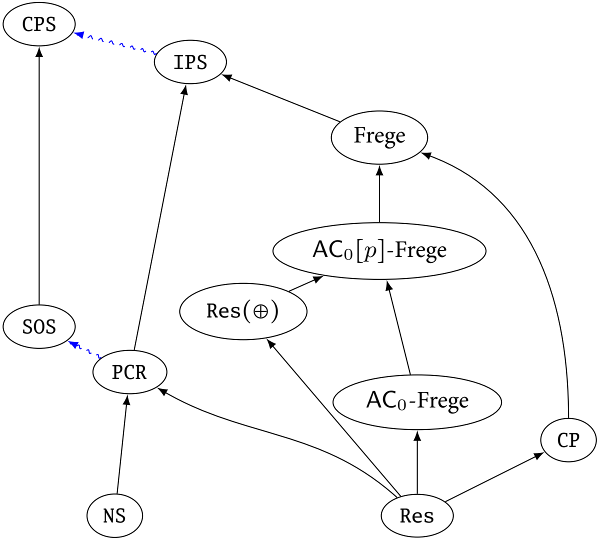
The **Polynomial Calculus** ($\mathrm{PCR}^{\mathbb{F}}$) proof of $\mathcal{F}$ is a sequence $(p_1, p_2, p_3, \ldots, p_\ell)$:

- $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{R_j\}$;
- $p_i = x_j p_k$ for some j and $k < i$;
- $p_i = \alpha p_k + \beta p_s$ for some $k, s < i$ and $\alpha, \beta \in \mathbb{F}$;
- $p_\ell = 1$.

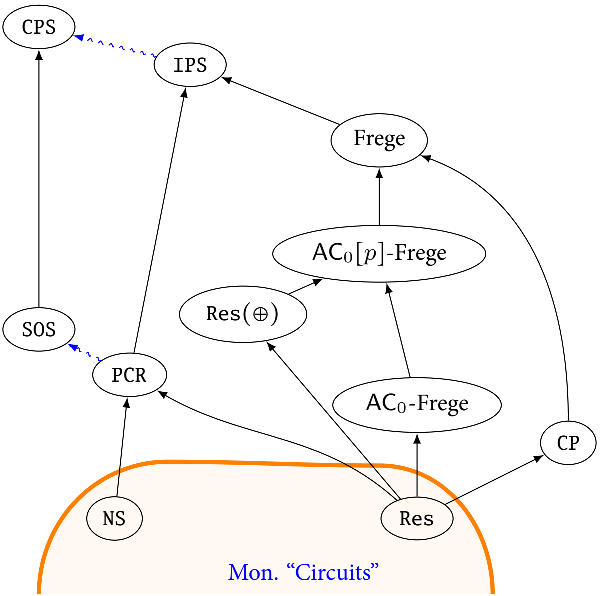
$$\mathcal{F} = \begin{cases} xy - 1 = 0 \\ yz + 1 = 0 \\ x + z - 2 = 0 \end{cases}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{x + z - 2}{xy + yz - 2y} \qquad \dfrac{xy - 1 \qquad yz + 1}{xy + yz}}{2y}}{2y^2} \qquad y^2 - 1}{1}$$

Hierarchy

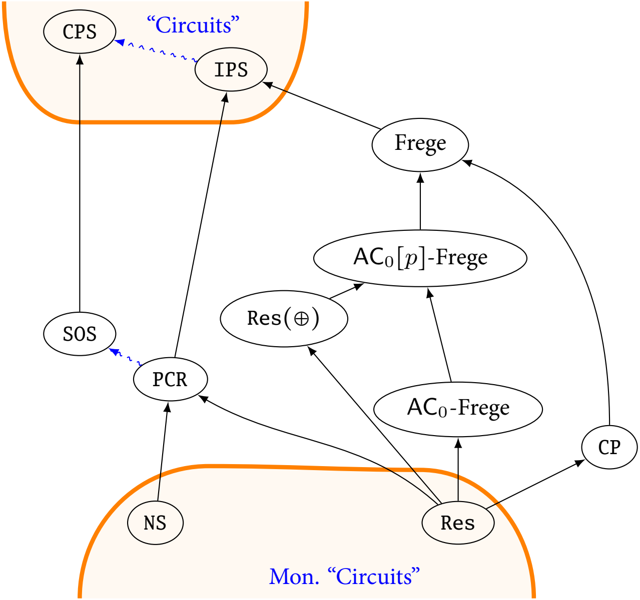


Hierarchy

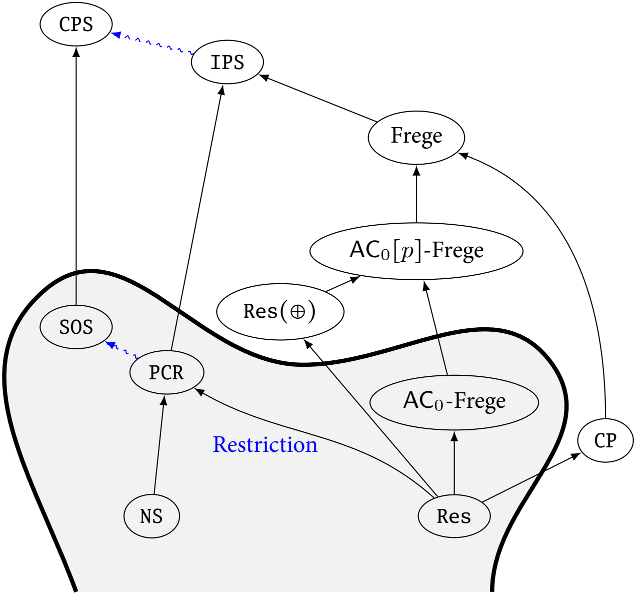


CPS
IPS
Frege
$AC_0[p]$-Frege
Res(⊕)
SOS
PCR
AC_0-Frege
CP
NS
Res
Mon. "Circuits"

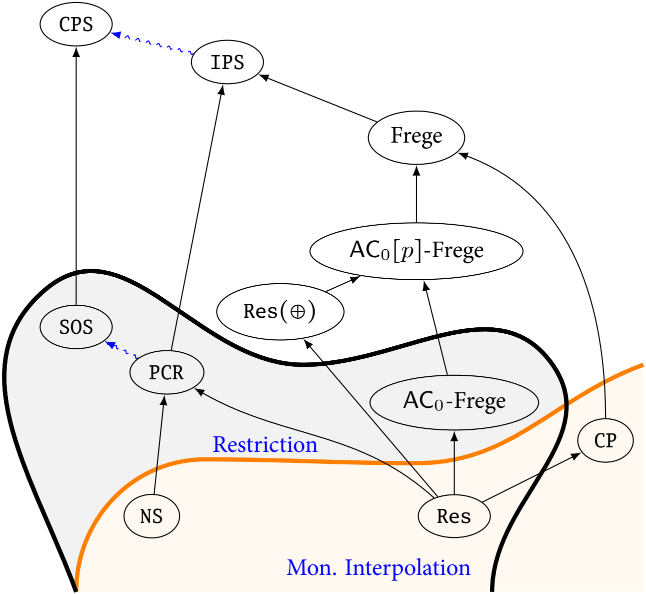
Hierarchy


CPS
"Circuits"
IPS
Frege
$AC_0[p]$-Frege
Res(⊕)
SOS
PCR
AC_0-Frege
CP
NS
Res
Mon. "Circuits"

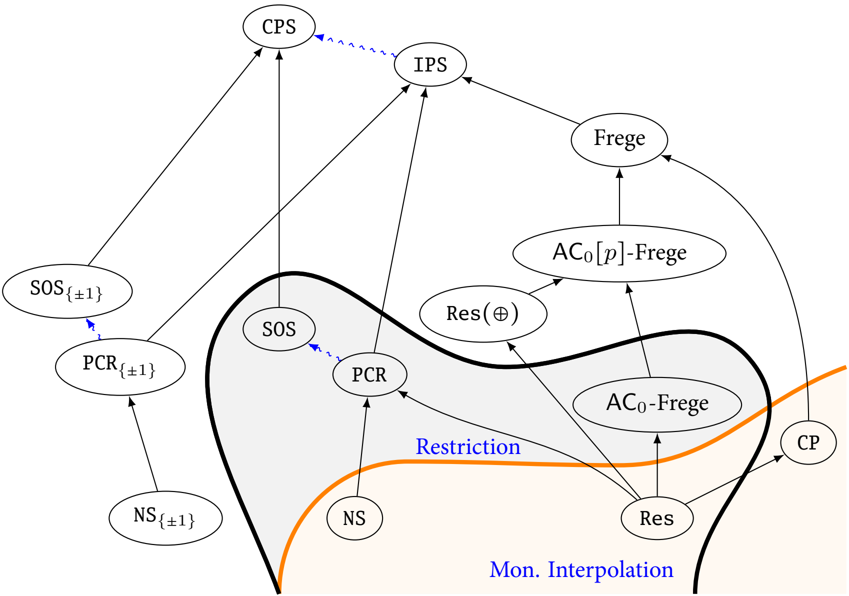
Hierarchy


CPS
IPS
Frege
$AC_0[p]$-Frege
Res(⊕)
SOS
PCR
AC_0-Frege
Restriction
CP
NS
Res

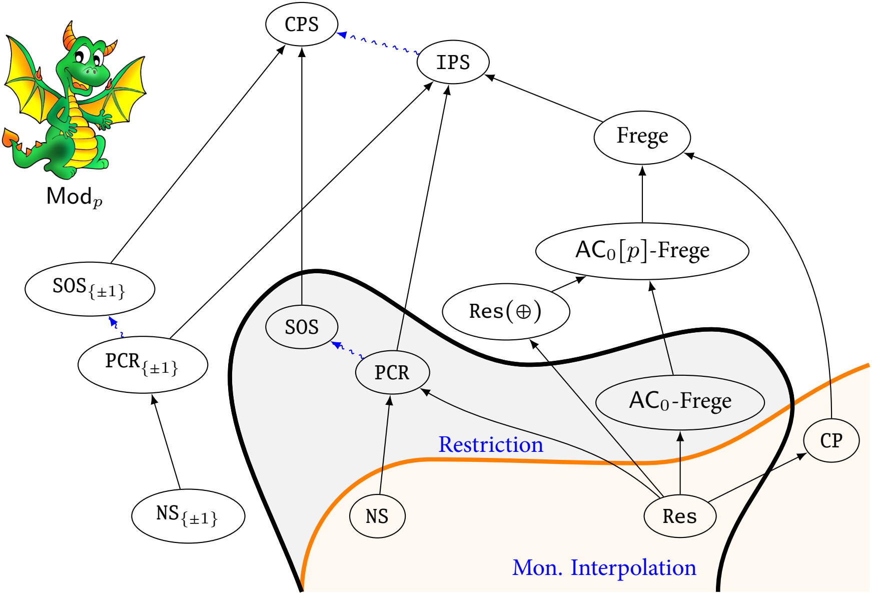
Hierarchy


CPS
IPS
Frege
$AC_0[p]$-Frege
Res(⊕)
SOS
PCR
AC_0-Frege
Restriction
CP
NS
Res
Mon. Interpolation

Hierarchy

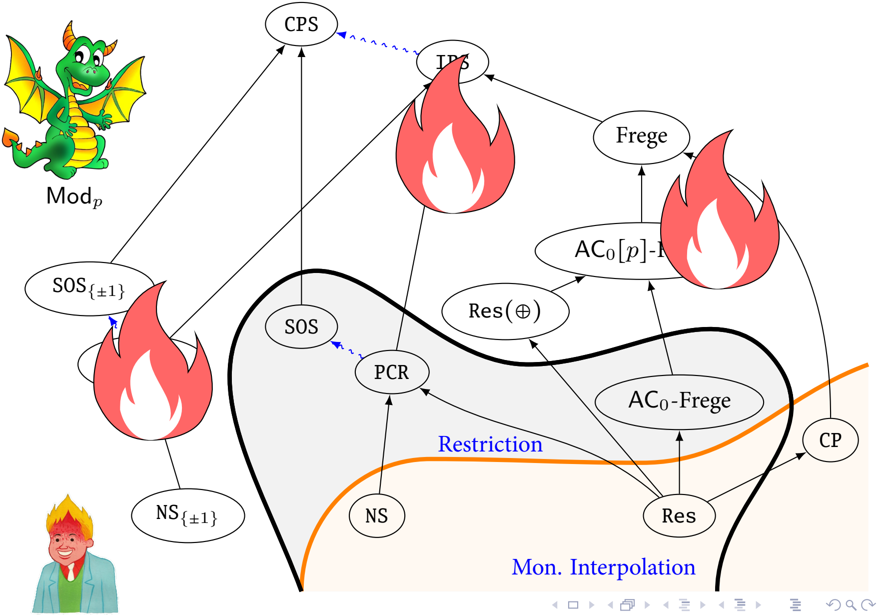

CPS
IPS
Frege
$AC_0[p]$-Frege
$SOS_{\{\pm1\}}$
SOS
Res(⊕)
$PCR_{\{\pm1\}}$
PCR
AC_0-Frege
Restriction
CP
$NS_{\{\pm1\}}$
NS
Res
Mon. Interpolation

Hierarchy



Mod$_p$
CPS
IPS
Frege
$AC_0[p]$-Frege
Res(⊕)
SOS$_{\{\pm 1\}}$
SOS
PCR$_{\{\pm 1\}}$
PCR
AC_0-Frege
Restriction
CP
NS$_{\{\pm 1\}}$
NS
Res
Mon. Interpolation

Hierarchy



Mod$_p$
CPS
Frege
SOS$_{\{\pm 1\}}$
SOS
PCR
Res($\oplus$)
AC$_0$-Frege
Restriction
CP
NS$_{\{\pm 1\}}$
NS
Res
Mon. Interpolation

Results

d_0 is the degree of $(\mathcal{F}, \mathcal{H})$. n is the number of variables of $(\mathcal{F}, \mathcal{H})$.

Theorem

Any $\texttt{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H}) \circ \texttt{MAJ}(z_1, z_2, z_3)$ has size $\exp(\Omega(\frac{(d-d_0)^2}{n}))$.
There d is an $\texttt{SOS}$-degree of $(\mathcal{F}, \mathcal{H})$.

Results

d_0 is the degree of $(\mathcal{F}, \mathcal{H})$. n is the number of variables of $(\mathcal{F}, \mathcal{H})$.

Theorem

Any $\mathtt{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H}) \circ \mathtt{MAJ}(z_1, z_2, z_3)$ has size $\exp(\Omega(\frac{(d-d_0)^2}{n}))$. There d is an $\mathtt{SOS}$-degree of $(\mathcal{F}, \mathcal{H})$.

Theorem

If φ is a random 11-CNF formula then whp any $\mathtt{SOS}_{\{\pm 1\}}$-proof or $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of φ has size $\exp(\Omega(n))$.

Results

d_0 is the degree of $(\mathcal{F}, \mathcal{H})$. n is the number of variables of $(\mathcal{F}, \mathcal{H})$.

Theorem

Any $\texttt{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H}) \circ \texttt{MAJ}(z_1, z_2, z_3)$ has size $\exp(\Omega(\frac{(d-d_0)^2}{n}))$. There d is an $\texttt{SOS}$-degree of $(\mathcal{F}, \mathcal{H})$.

Theorem

If φ is a random 11-CNF formula then whp any $\texttt{SOS}_{\{\pm 1\}}$-proof or $\texttt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of φ has size $\exp(\Omega(n))$.

Theorem

Any $\texttt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of Pigeonhole Principle has size $\exp(\Omega(n))$.

$\texttt{SOS}_{\{\pm 1\}}$ is strictly stronger than $\texttt{PCR}^{\mathbb{R}}_{\{\pm 1\}}$.

Size measure. All operations modulo $\langle R_i \rangle$

Size measure. All operations modulo $\langle R_i \rangle$

$$\texttt{SOS} : \sum_{u=1}^{a} p_u f_u + \sum_{v=1}^{b} q_v^2 h_v = -1$$

$$\text{Size} := \sum_{u=1}^{a} (\texttt{MSize}(p_u) + \texttt{MSize}(f_u)) + \sum_{v=1}^{b} \texttt{MSize}(q_v) + \sum_{h \in \mathcal{H}} \texttt{MSize}(h)$$

$$\texttt{PCR}^{\mathbb{F}} : (p_1, \ldots, p_\ell)$$

$$\text{Size} := \sum_{u=1}^{\ell} (\texttt{MSize}(p_u))$$

Strategy for the $\{0,1\}$ basis ($\texttt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \text{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.

Strategy for the $\{0, 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \deg(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.

Strategy for the $\{0,1\}$ basis ($\texttt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \mathsf{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.

Strategy for the $\{0,1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \mathsf{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.
4. $\pi \restriction (x = 0)$ is still a proof of $\mathcal{F} \restriction (x = 0)$.

Strategy for the $\{0, 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \mathsf{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.
4. $\pi \upharpoonright (x = 0)$ is still a proof of $\mathcal{F} \upharpoonright (x = 0)$.
5. Keep $\mathcal{F} \upharpoonright (x = 0)$ hard in terms of degree.

Strategy for the $\{0,1\}$ basis ($\texttt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \deg(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.
4. $\pi \restriction (x = 0)$ is still a proof of $\mathcal{F} \restriction (x = 0)$.
5. Try to avoid local contradictions in $\mathcal{F} \restriction (x = 0)$.

Strategy for the $\{0, 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi := (p_1, \dots, p_\ell)$ is a proof of $\mathcal{F}$. $H := \{t \mid t \in p_i, \mathsf{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.
4. $\pi \restriction (x = 0)$ is still a proof of $\mathcal{F} \restriction (x = 0)$.
5. Try to avoid local contradictions in $\mathcal{F} \restriction (x = 0)$. 
6. Repeat until we have terms of big degree.

Strategy for the $\{0, 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \mathsf{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.
4. $\pi \restriction (x = 0)$ is still a proof of $\mathcal{F} \restriction (x = 0)$.
5. Try to avoid local contradictions in $\mathcal{F} \restriction (x = 0)$. 
6. Repeat until we have terms of big degree.

We kill all terms of big degree but remaining system is still hard in terms of degree.

Strategy for the $\{0,1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi := (p_1, \dots, p_\ell)$ is a proof of $\mathcal{F}$. $H := \{t \mid t \in p_i, \mathsf{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.
4. $\pi \restriction (x = 0)$ is still a proof of $\mathcal{F} \restriction (x = 0)$.
5. Try to avoid local contradictions in $\mathcal{F} \restriction (x = 0)$. 
6. Repeat until we have terms of big degree.

We kill all terms of big degree but remaining system is still hard in terms of degree.

Degree is the source of hardness.

Strategy for the $\{0,1\}$ basis ($\mathrm{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in p_i, \deg(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Set x to 0 in π. This operation kills all terms that contain x.
4. $\pi \restriction (x = 0)$ is still a proof of $\mathcal{F} \restriction (x = 0)$.
5. Try to avoid local contradictions in $\mathcal{F} \restriction (x = 0)$. 
6. Repeat until we have terms of big degree.

We kill all terms of big degree but remaining system is still hard in terms of degree.

Degree is the source of hardness.

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0.

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0. $x^2 - 1 \restriction (x = 0) \to -1.$

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0. $x^2 - 1 \restriction (x = 0) \to -1.$
2. $\tau(p) \coloneqq \frac{p\restriction(x=-1)+p\restriction(x=1)}{2}$. Consider $\tau(\pi)$.

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0. $x^2 - 1 \restriction (x = 0) \to -1.$
2. $\tau(p) \coloneqq \frac{p\restriction(x=-1)+p\restriction(x=1)}{2}$. Consider $\tau(\pi)$.

$$\frac{p}{\frac{xp}{p}}$$

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0. $\quad x^2 - 1 \upharpoonright (x = 0) \to -1.$
2. $\tau(p) \coloneqq \frac{p\upharpoonright(x=-1)+p\upharpoonright(x=1)}{2}$. Consider $\tau(\pi)$.

$$\frac{p}{\dfrac{xp}{p}} \qquad\qquad \frac{\tau(p)}{\dfrac{\tau(xp)}{\tau(p)}}$$

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0. $\quad x^2 - 1 \restriction (x = 0) \to -1.$
2. $\tau(p) \coloneqq \frac{p\restriction(x=-1)+p\restriction(x=1)}{2}$. Consider $\tau(\pi)$.

$$\frac{\dfrac{p}{xp}}{p} \qquad \frac{\dfrac{\tau(p)}{\tau(xp)}}{\tau(p)} \qquad \frac{\dfrac{p}{0}}{p}$$

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0. $\quad x^2 - 1 \restriction (x = 0) \to -1.$
2. $\tau(p) \coloneqq \frac{p \restriction (x=-1) + p \restriction (x=1)}{2}$. Consider $\tau(\pi)$.

$$\frac{\frac{p}{xp}}{p} \qquad \frac{\frac{\tau(p)}{\tau(xp)}}{\tau(p)} \qquad \frac{\frac{p}{0}}{p}$$

Multiplication is invertible.

Degree and the $\{\pm 1\}$ basis

Set x to 0 in π. This operation kills all terms that contain x

Attempts.

1. Set x to 0. $\quad x^2 - 1 \restriction (x = 0) \to -1.$
2. $\tau(p) \coloneqq \frac{p\restriction(x=-1)+p\restriction(x=1)}{2}$. Consider $\tau(\pi)$.

$$\frac{\frac{p}{xp}}{p} \qquad \frac{\frac{\tau(p)}{\tau(xp)}}{\tau(p)} \qquad \frac{\frac{p}{0}}{p}$$

Multiplication is invertible.

Grigoriev 98; Buss, Grigoriev, Impagliazzo, Pitassi 01; Grigoriev 01

1. Tseitin formulas has small $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ and $\mathrm{SOS}_{\{\pm 1\}}$-proofs.
2. There are Tseitin formulas that has $\mathrm{PCR}^{\mathbb{F}}$ or SOS-degree $\Omega(n)$.

Degree and the $\{\pm 1\}$ basis. Part 2

$\pi \coloneqq (p_1, \ldots, p_\ell)$.
Can we reduce the degree of p_i?

Degree and the $\{\pm 1\}$ basis. Part 2

$\pi \coloneqq (p_1, \ldots, p_\ell)$.
Can we reduce the degree of p_i?

1. $p_i \coloneqq \prod_{i=1}^{n} x_i$

Degree and the $\{\pm 1\}$ basis. Part 2

$\pi \coloneqq (p_1, \ldots, p_\ell)$.
Can we reduce the degree of p_i?

1. $p_i \coloneqq \prod_{i=1}^{n} x_i$ YES

Degree and the $\{\pm 1\}$ basis. Part 2

$\pi \coloneqq (p_1, \ldots, p_\ell)$.
Can we reduce the degree of p_i?

1. $p_i \coloneqq \prod_{i=1}^{n} x_i$ YES

$$\frac{\frac{p}{x_1 p}}{\frac{\vdots}{1}}$$

Degree and the $\{\pm 1\}$ basis. Part 2

$\pi \coloneqq (p_1, \ldots, p_\ell)$.
Can we reduce the degree of p_i?

1. $p_i \coloneqq \prod_{i=1}^{n} x_i$ YES

$$\frac{\dfrac{p}{x_1 p}}{\dfrac{\vdots}{1}}$$

2. $p_i \coloneqq \prod_{i=1}^{n} x_i - 1$

Degree and the $\{\pm 1\}$ basis. Part 2

$\pi \coloneqq (p_1, \ldots, p_\ell)$.
Can we reduce the degree of p_i?

1. $p_i \coloneqq \prod_{i=1}^{n} x_i$ YES

$$\frac{\frac{p}{x_1 p}}{\frac{\vdots}{1}}$$

2. $p_i \coloneqq \prod_{i=1}^{n} x_i - 1$ NOT REALLY

Degree and the $\{\pm 1\}$ basis. Part 2

$\pi \coloneqq (p_1, \ldots, p_\ell)$.
Can we reduce the degree of p_i?

1. $p_i \coloneqq \prod_{i=1}^{n} x_i$ YES

$$\frac{\dfrac{p}{x_1 p}}{\dfrac{\vdots}{1}}$$

2. $p_i \coloneqq \prod_{i=1}^{n} x_i - 1$ NOT REALLY

$p_i \coloneqq \sum_j t_j$. Degree of the symmetric differences between t_j's is the new source of hardness.

Quadratic representation and $\texttt{Split}_x$

$$\pi \coloneqq (p_1, \ldots, p_\ell).\ p_i \coloneqq \sum_j t_{i,j}.$$

Quadratic representation and $\mathtt{Split}_x$

$\pi \coloneqq (p_1, \ldots, p_\ell)$. $p_i \coloneqq \sum_j t_{i,j}$.

$p_i^2 \coloneqq \sum_{j,j'} t_{i,j} t_{i,j'}$.

We want to see all possible pairs, hence we prohibit cancellations.

Quadratic representation (QR)

The **QR** of π is the sequence $(p_1^2, \ldots, p_\ell^2)$ where squares are computed without cancellations.

Quadratic representation and $\texttt{Split}_x$

$\pi \coloneqq (p_1, \ldots, p_\ell)$. $p_i \coloneqq \sum_j t_{i,j}$.

$p_i^2 \coloneqq \sum_{j,j'} t_{i,j} t_{i,j'}$.

We want to see all possible pairs, hence we prohibit cancellations.

Quadratic representation (QR)

The **QR** of π is the sequence $(p_1^2, \ldots, p_\ell^2)$ where squares are computed without cancellations.

Reminder: $\tau(p) \coloneqq \frac{p\restriction(x=-1)+p\restriction(x=1)}{2}$.

Quadratic representation and $\texttt{Split}_x$

$\pi \coloneqq (p_1, \dots, p_\ell)$. $p_i \coloneqq \sum_j t_{i,j}$.

$p_i^2 \coloneqq \sum_{j,j'} t_{i,j} t_{i,j'}$.

We want to see all possible pairs, hence we prohibit cancellations.

Quadratic representation (QR)

The **QR** of π is the sequence $(p_1^2, \dots, p_\ell^2)$ where squares are computed without cancellations.

Reminder: $\tau(p) \coloneqq \frac{p\restriction(x=-1) + p\restriction(x=1)}{2}$.

We want operation that apply τ to the QR of π.

Quadratic representation and $\texttt{Split}_x$

$\pi \coloneqq (p_1, \dots, p_\ell)$. $p_i \coloneqq \sum_j t_{i,j}$.

$p_i^2 \coloneqq \sum_{j,j'} t_{i,j} t_{i,j'}$.

We want to see all possible pairs, hence we prohibit cancellations.

Quadratic representation (QR)

The **QR** of π is the sequence $(p_1^2, \dots, p_\ell^2)$ where squares are computed without cancellations.

Reminder: $\tau(p) \coloneqq \frac{p\restriction(x=-1) + p\restriction(x=1)}{2}$.

We want operation that apply τ to the QR of π.

$\texttt{Split}_x$

$p_i \coloneqq r_i + x q_i$.

$\texttt{Split}_x(\pi) \coloneqq (r_1, q_1, r_2, q_2, r_3, q_3, \dots, r_\ell, q_\ell)$.

Quadratic representation and $\texttt{Split}_x$

$\pi \coloneqq (p_1, \ldots, p_\ell)$. $p_i \coloneqq \sum_j t_{i,j}$.

$p_i^2 \coloneqq \sum_{j,j'} t_{i,j} t_{i,j'}$.

We want to see all possible pairs, hence we prohibit cancellations.

Quadratic representation (QR)

The **QR** of π is the sequence $(p_1^2, \ldots, p_\ell^2)$ where squares are computed without cancellations.

Reminder: $\tau(p) \coloneqq \frac{p\restriction(x=-1) + p\restriction(x=1)}{2}$.

We want operation that apply τ to the QR of π.

$\texttt{Split}_x$

$p_i \coloneqq r_i + x q_i$.

$\texttt{Split}_x(\pi) \coloneqq (r_1, q_1, r_2, q_2, r_3, q_3, \ldots, r_\ell, q_\ell)$.

$\texttt{Split}_x(\pi)$ is a proof of **damaged** version of $\mathcal{F}$.

Strategy for the $\{\pm 1\}$ basis ($\mathrm{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in \text{ QR of } \pi, \deg(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.

Strategy for the $\{\pm 1\}$ basis ($\mathsf{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in \text{ QR of } \pi, \deg(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.

Strategy for the $\{\pm 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi := (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H := \{t \mid t \in$ QR of $\pi, \mathtt{deg}(t)$ is big$\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\mathtt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.

Strategy for the $\{\pm 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in$ QR of $\pi, \mathsf{deg}(t)$ is big$\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\mathtt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.
4. $\mathtt{Split}_x(\pi)$ is still a proof of **damaged** $\mathcal{F}$.

Strategy for the $\{\pm 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in$ QR of $\pi, \mathsf{deg}(t)$ is big$\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\mathtt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.
4. $\mathtt{Split}_x(\pi)$ is still a proof of **damaged** $\mathcal{F}$.
5. Try to avoid local contradictions in $\mathtt{Split}_x(\mathcal{F})$. 

Strategy for the $\{\pm 1\}$ basis ($\texttt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \dots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in \text{ QR of } \pi, \texttt{deg}(t) \text{ is big}\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\texttt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.
4. $\texttt{Split}_x(\pi)$ is still a proof of **damaged** $\mathcal{F}$.
5. Try to avoid local contradictions in $\texttt{Split}_x(\mathcal{F})$. 
6. Repeat until we have terms of big degree in the QR.

Strategy for the $\{\pm 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in$ QR of π, $\mathsf{deg}(t)$ is big$\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\mathtt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.
4. $\mathtt{Split}_x(\pi)$ is still a proof of **damaged** $\mathcal{F}$.
5. Try to avoid local contradictions in $\mathtt{Split}_x(\mathcal{F})$. 
6. Repeat until we have terms of big degree in the QR.
7. Try to satisfy all **broken** constraints.

Strategy for the $\{\pm 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in$ QR of π, $\mathsf{deg}(t)$ is big$\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\mathtt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.
4. $\mathtt{Split}_x(\pi)$ is still a proof of **damaged** $\mathcal{F}$.
5. Try to avoid local contradictions in $\mathtt{Split}_x(\mathcal{F})$. 
6. Repeat until we have terms of big degree in the QR.

7. Try to satisfy all **broken** constraints. Impossible for Tseitin formulas.

Strategy for the $\{\pm 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in$ QR of $\pi, \deg(t)$ is big$\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\mathtt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.
4. $\mathtt{Split}_x(\pi)$ is still a proof of **damaged** $\mathcal{F}$.
5. Try to avoid local contradictions in $\mathtt{Split}_x(\mathcal{F})$. 
6. Repeat until we have terms of big degree in the QR.
7. Try to satisfy all **broken** constraints. Impossible for Tseitin formulas.

Lemma

Let π be a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

Strategy for the $\{\pm 1\}$ basis ($\mathtt{PCR}^{\mathbb{F}}$)

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$. $H \coloneqq \{t \mid t \in$ QR of π, $\deg(t)$ is big$\}$.

1. π is small $\Rightarrow$ size of H is small.
2. Pick the most frequent literal x in H.
3. Apply $\mathtt{Split}_x$ to π. This operation kills all terms that contain x in the QR of π.
4. $\mathtt{Split}_x(\pi)$ is still a proof of **damaged** $\mathcal{F}$.
5. Try to avoid local contradictions in $\mathtt{Split}_x(\mathcal{F})$.

6. Repeat until we have terms of big degree in the QR.
7. Try to satisfy all **broken** constraints. Impossible for Tseitin formulas.

Lemma

Let π be a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

This is wrong Lemma, we need to change definition of QR to fix it.

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i ($(\ell_\pi p_i)$) in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i $((\ell_\pi p_i))$ in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \ldots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i $((\ell_\pi p_i))$ in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \ldots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lemma

Let π be a $\texttt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\texttt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

Lazy computations 

$\pi := (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i ($(\ell_\pi p_i)$) in the proof π:

- $(\ell_\pi p)_i := p_i$, if $p_i \in \mathcal{F}$ or $p_i := p_j$ for some $j < i$;
- $(\ell_\pi p)_i := \alpha p_j + \beta p_k$ without cancellations, if $p_i := \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \ldots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lemma

Let π be a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

$$p_i := \sum_j t_{i,j} \text{ and } s_i := \sum_j t_{i,1} t_{i,j} \quad \Rightarrow \quad p_i = t_{i,1} s_i \text{ and } s_i = t_{i,1} p_i.$$

Lazy computations 

$\pi \coloneqq (p_1, \dots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i $((\ell_\pi p_i))$ in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \dots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lemma

Let π be a $\texttt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\texttt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

$$p_i \coloneqq \sum_j t_{i,j} \text{ and } s_i \coloneqq \sum_j t_{i,1} t_{i,j} \qquad \Rightarrow \qquad p_i = t_{i,1} s_i \text{ and } s_i = t_{i,1} p_i.$$

$$\pi'' \coloneqq (s_1, \dots, s_\ell)$$

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i $((\ell_\pi p_i))$ in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \ldots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lemma

Let π be a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

$$p_i \coloneqq \sum_j t_{i,j} \text{ and } s_i \coloneqq \sum_j t_{i,1} t_{i,j} \quad \Rightarrow \quad p_i = t_{i,1} s_i \text{ and } s_i = t_{i,1} p_i.$$

$\pi'' \coloneqq (s_1, \ldots, s_\ell)$

1. $\mathbf{p_i \in \mathcal{F}}$: $\quad s_i = t_{i,1} p_i$.
2. $\mathbf{p_i \coloneqq x p_j}$: $\quad s_i = s_j$.
3. $\mathbf{p_i \coloneqq \alpha p_a + \beta p_b}$:

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i $((\ell_\pi p_i))$ in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \ldots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lemma

Let π be a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

$p_i \coloneqq \sum_j t_{i,j}$ and $s_i \coloneqq \sum_j t_{i,1} t_{i,j} \quad \Rightarrow \quad p_i = t_{i,1} s_i$ and $s_i = t_{i,1} p_i$.

$\pi'' \coloneqq (s_1, \ldots, s_\ell)$

1. $\mathbf{p_i} \in \boldsymbol{\mathcal{F}}$: $\quad s_i = t_{i,1} p_i$.
2. $\mathbf{p_i} \coloneqq \mathbf{x p_j}$: $\quad s_i = s_j$.
3. $\mathbf{p_i} \coloneqq \boldsymbol{\alpha} \mathbf{p_a} + \boldsymbol{\beta} \mathbf{p_b}$: $\quad q \coloneqq \alpha \sum_j t_{a,1} t_{a,j} + \beta \sum_j t_{a,1} t_{b,j}$.

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i ($(\ell_\pi p_i)$) in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \ldots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lemma

Let π be a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

$$p_i \coloneqq \sum_j t_{i,j} \text{ and } s_i \coloneqq \sum_j t_{i,1} t_{i,j} \quad \Rightarrow \quad p_i = t_{i,1} s_i \text{ and } s_i = t_{i,1} p_i.$$

$\pi'' \coloneqq (s_1, \ldots, s_\ell)$

1. $\mathbf{p_i} \in \boldsymbol{\mathcal{F}}$: $\quad s_i = t_{i,1} p_i$.
2. $\mathbf{p_i} \coloneqq \mathbf{x p_j}$: $\quad s_i = s_j$.
3. $\mathbf{p_i} \coloneqq \boldsymbol{\alpha} \mathbf{p_a} + \boldsymbol{\beta} \mathbf{p_b}$: $\quad q \coloneqq \alpha \sum_j t_{a,1} t_{a,j} + \beta \sum_j t_{a,1} t_{b,j}$.

   $$q = \alpha s_a + \beta \sum_j t_{a,1} t_{b,j} = \alpha s_a + \beta t_{a,1} t_{b,1} \sum_j \beta t_{b,1} t_{b,j} = \alpha s_a + \beta t_{a,1} t_{b,1} s_b.$$

Lazy computations 

$\pi \coloneqq (p_1, \ldots, p_\ell)$ is a proof of $\mathcal{F}$.

Lazy representation of p_i $((\ell_\pi p_i))$ in the proof π:

- $(\ell_\pi p)_i \coloneqq p_i$, if $p_i \in \mathcal{F}$ or $p_i \coloneqq p_j$ for some $j < i$;
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if $p_i \coloneqq \alpha p_j + \beta p_k$.

The fixed **QR** of π is the sequence $((\ell_\pi p)_1^2, \ldots, (\ell_\pi p)_\ell^2)$ where squares are computed without cancellations.

Lemma

Let π be a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ and QR of π has degree d. Then there is a $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof π' of $\mathcal{F}$ of degree $2d$.

$p_i \coloneqq \sum_j t_{i,j}$ and $s_i \coloneqq \sum_j t_{i,1} t_{i,j} \quad \Rightarrow \quad p_i = t_{i,1} s_i$ and $s_i = t_{i,1} p_i$.

$\pi'' \coloneqq (s_1, \ldots, s_\ell)$

1. $\mathbf{p_i} \in \boldsymbol{\mathcal{F}}$: $\quad s_i = t_{i,1} p_i$.
2. $\mathbf{p_i} \coloneqq \mathbf{x p_j}$: $\quad s_i = s_j$.
3. $\mathbf{p_i} \coloneqq \boldsymbol{\alpha} \mathbf{p_a} + \boldsymbol{\beta} \mathbf{p_b}$: $\quad q \coloneqq \alpha \sum_j t_{a,1} t_{a,j} + \beta \sum_j t_{a,1} t_{b,j}$.

   $q = \alpha s_a + \beta \sum_j t_{a,1} t_{b,j} = \alpha s_a + \beta t_{a,1} t_{b,1} \sum_j \beta t_{b,1} t_{b,j} = \alpha s_a + \beta t_{a,1} t_{b,1} s_b$.

   $s_i = \sum_j t_{i,1} t_{i,j}$. Wlog $t_{i,1} \coloneqq t_{a,k}$ hence $s_i = t_{a,k} t_{a,1} q$.

Open problems

1. Lower (or upper!) bound on $\mathtt{PCR}_{\{\pm 1\}}$-proofs of Functional Pigeonhole Principle.
2. Lower bound on $\mathtt{PCR}_{\{0,1\}}$-proofs of Weak Pigeonhole Principle.

Open problems

1. Lower (or upper!) bound on $\mathtt{PCR}_{\{\pm 1\}}$-proofs of Functional Pigeonhole Principle.
2. Lower bound on $\mathtt{PCR}_{\{0,1\}}$-proofs of Weak Pigeonhole Principle.

3. Can we simulate Resolution in $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$?

Open problems

1. Lower (or upper!) bound on $\mathtt{PCR}_{\{\pm 1\}}$-proofs of Functional Pigeonhole Principle.
2. Lower bound on $\mathtt{PCR}_{\{0,1\}}$-proofs of Weak Pigeonhole Principle.

3. Can we simulate Resolution in $\mathtt{PCR}^{\mathbb{F}}_{\{\pm 1\}}$? Conjecture: NO.