Workshop on Proof Complexity, St. Petersburg

Gentzen and Frege systems for QBF

Ján Pich
University of Leeds

17 May 2016

joint work with Olaf Beyersdorff

overview:

overview:

Propositional proof systems: Frege, Extended Frege (EF)

overview:

Propositional proof systems:	Frege, Extended Frege (EF)
QBF proof systems:	Frege $+ \forall$red, EF $+ \forall$red

overview:

Propositional proof systems: Frege, Extended Frege (EF)

QBF proof systems: Frege + ∀red, EF + ∀red

I. Gentzen vs. Frege in QBF

G_1^* p-simulates EF + ∀red

i.e. Gentzen systems prove theorems more efficiently than QBF Frege

overview:

Propositional proof systems: Frege, Extended Frege (EF)
QBF proof systems: Frege + ∀red, EF + ∀red

I. Gentzen vs. Frege in QBF

$$\mathrm{G}_1^* \text{ p-simulates EF} + \forall\text{red}$$

i.e. Gentzen systems prove theorems more efficiently than QBF Frege

II. First-order version of EF + ∀red

$$\text{EF} + \forall\text{red is intuitionistic } S^1_2$$

i.e. theorems of intuitionistic S^1_2 have short proofs in EF + ∀red

overview:

Propositional proof systems: Frege, Extended Frege (EF)

QBF proof systems: Frege + ∀red, EF + ∀red

I. Gentzen vs. Frege in QBF

$$G_1^* \text{ p-simulates EF} + \forall\text{red}$$

i.e. Gentzen systems prove theorems more efficiently than QBF Frege

II. First-order version of EF + ∀red

$$\text{EF} + \forall\text{red is intuitionistic } S_2^1$$

i.e. theorems of intuitionistic S_2^1 have short proofs in EF + ∀red

III. Characterizing lower bounds for QBF **Frege**

$$\exists \text{ hard theorems for EF} + \forall\text{red}$$

$$\Leftrightarrow$$

$$\text{PSPACE} \not\subseteq \text{P/poly or } \exists \text{ hard theorems for EF}$$

Frege systems: common systems for propositional logic
- operate with propositional formulas
- finite set of derivation rules

e.g.

$$\frac{\phi \qquad \phi \rightarrow \psi}{\psi} \text{ (modus ponens)}$$

Frege systems: common systems for propositional logic
- operate with propositional formulas
- finite set of derivation rules

e.g.

$$\frac{\phi \qquad \phi \to \psi}{\psi} \text{ (modus ponens)}$$

EF systems: operate with circuits

QBFs: $\forall x\, \phi(x) \Leftrightarrow \phi(0) \wedge \phi(1)$
$\exists x\, \phi(x) \Leftrightarrow \phi(0) \vee \phi(1)$

QBFs: $\forall x\, \phi(x) \Leftrightarrow \phi(0) \wedge \phi(1)$
$\exists x\, \phi(x) \Leftrightarrow \phi(0) \vee \phi(1)$

QBF Frege systems [Beyersdorff, Bonacina, Chew]

Frege + $\forall$red: a refutation of a QBF $Q\,\phi$ is a sequence of formulas $L_1, \ldots, L_l$ where $L_1 = \phi, L_l = \emptyset$ and each L_i is derived using a Frege derivation rule or $\forall$red rule:

$$\frac{L_j(u)}{L_j(u/B)}$$

- where u is
  1. universally quantified (in the prefix Q)
  2. the innermost (w.r.t. Q) among the variables of L_j
- B is a formula containing only variables left of u

QBFs: $\forall x\, \phi(x) \Leftrightarrow \phi(0) \wedge \phi(1)$
$\exists x\, \phi(x) \Leftrightarrow \phi(0) \vee \phi(1)$

QBF Frege systems [Beyersdorff, Bonacina, Chew]

Frege + ∀red: a refutation of a QBF $Q\,\phi$ is a sequence of formulas $L_1, \ldots, L_l$ where $L_1 = \phi, L_l = \emptyset$ and each L_i is derived using a Frege derivation rule or ∀red rule:

$$\frac{L_j(u)}{L_j(u/B)}$$

- where u is
  1. universally quantified (in the prefix Q)
  2. the innermost (w.r.t. Q) among the variables of L_j
- B is a formula containing only variables left of u

EF + ∀red : Frege + ∀red but with circuits

Gentzen's sequent systems: [Cook, Morioka] [Krajíček, Pudlák]

LK: operates with sequents $\Gamma \longrightarrow \Delta$ (i.e. $\bigwedge_{\phi \in \Gamma} \phi \models \bigvee_{\psi \in \Delta} \psi$)
e.g.

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta} \text{ (cut rule)}$$

Gentzen's sequent systems: [Cook, Morioka] [Krajíček, Pudlák]

LK: operates with sequents $\Gamma \longrightarrow \Delta$ (i.e. $\bigwedge_{\phi \in \Gamma} \phi \models \bigvee_{\psi \in \Delta} \psi$)
e.g.

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta} \text{ (cut rule)}$$

G: LK + QBFs in sequents and quantification rules

$$\frac{\phi(x/\psi), \Gamma \longrightarrow \Delta}{\forall x\, \phi, \Gamma \longrightarrow \Delta} (\forall\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/p)}{\Gamma \longrightarrow \Delta, \forall x\, \phi} (\forall\text{-r})$$

$$\frac{\phi(x/p), \Gamma \longrightarrow \Delta}{\exists x\, \phi, \Gamma \longrightarrow \Delta} (\exists\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/\psi)}{\Gamma \longrightarrow \Delta, \exists x\, \phi} (\exists\text{-r})$$

for quantifier-free formulas ψ

Gentzen's sequent systems: [Cook, Morioka] [Krajíček, Pudlák]

LK: operates with sequents $\Gamma \longrightarrow \Delta$ (i.e. $\bigwedge_{\phi \in \Gamma} \phi \models \bigvee_{\psi \in \Delta} \psi$)
e.g.

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta} \text{ (cut rule)}$$

G: LK + QBFs in sequents and quantification rules

$$\frac{\phi(x/\psi), \Gamma \longrightarrow \Delta}{\forall x\, \phi, \Gamma \longrightarrow \Delta} (\forall\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/p)}{\Gamma \longrightarrow \Delta, \forall x\, \phi} (\forall\text{-r})$$

$$\frac{\phi(x/p), \Gamma \longrightarrow \Delta}{\exists x\, \phi, \Gamma \longrightarrow \Delta} (\exists\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/\psi)}{\Gamma \longrightarrow \Delta, \exists x\, \phi} (\exists\text{-r})$$

for quantifier-free formulas ψ

G_1: G with cut furmulas of the form $\exists x\, A(x, y)$ for propositional A

Gentzen's sequent systems: [Cook, Morioka] [~~Krajíček, Pudlák~~]

LK: operates with sequents $\Gamma \longrightarrow \Delta$ (i.e. $\bigwedge_{\phi \in \Gamma} \phi \models \bigvee_{\psi \in \Delta} \psi$)
e.g.

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta} \text{(cut rule)}$$

G: LK + QBFs in sequents and quantification rules

$$\frac{\phi(x/\psi), \Gamma \longrightarrow \Delta}{\forall x\, \phi, \Gamma \longrightarrow \Delta} (\forall\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/p)}{\Gamma \longrightarrow \Delta, \forall x\, \phi} (\forall\text{-r})$$

$$\frac{\phi(x/p), \Gamma \longrightarrow \Delta}{\exists x\, \phi, \Gamma \longrightarrow \Delta} (\exists\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/\psi)}{\Gamma \longrightarrow \Delta, \exists x\, \phi} (\exists\text{-r})$$

for quantifier-free formulas ψ

G_1: G with cut furmulas of the form $\exists x\, A(x, y)$ for propositional A

G_0: G but cut furmulas are propositional

Gentzen's sequent systems: [Cook, Morioka] [~~Krajíček, Pudlák~~]

LK: operates with sequents $\Gamma \longrightarrow \Delta$ (i.e. $\bigwedge_{\phi \in \Gamma} \phi \models \bigvee_{\psi \in \Delta} \psi$)
e.g.

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta} \text{(cut rule)}$$

G: LK + QBFs in sequents and quantification rules

$$\frac{\phi(x/\psi), \Gamma \longrightarrow \Delta}{\forall x\, \phi, \Gamma \longrightarrow \Delta} (\forall\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/p)}{\Gamma \longrightarrow \Delta, \forall x\, \phi} (\forall\text{-r})$$

$$\frac{\phi(x/p), \Gamma \longrightarrow \Delta}{\exists x\, \phi, \Gamma \longrightarrow \Delta} (\exists\text{-l}) \qquad \frac{\Gamma \longrightarrow \Delta, \phi(x/\psi)}{\Gamma \longrightarrow \Delta, \exists x\, \phi} (\exists\text{-r})$$

for quantifier-free formulas ψ

G_1: G with cut furmulas of the form $\exists x\, A(x, y)$ for propositional A

G_0: G but cut furmulas are propositional

G_i^*: G_i with tree-like proofs

witnessing properties

[CM]

$$\exists y\, A_n(x,y), \text{ where } A_n \text{ is propositional, have p-size } \mathsf{G}_1^* \text{ proofs}$$
$$\Rightarrow$$
$$\exists f \in \mathsf{P/poly} \text{ s.t. } A_n(x, f(x))$$

witnessing properties

[CM]

$$\exists y\, A_n(x,y), \text{ where } A_n \text{ is propositional, have p-size } G_1^* \text{ proofs}$$
$$\Rightarrow$$
$$\exists f \in P/\text{poly s.t. } A_n(x, f(x))$$

[CM]

$$\exists y\, A_n(x,y), \text{ where } A_n \text{ is propositional, have p-size } G_0 \text{ proofs}$$
$$\Rightarrow$$
$$\exists f \in NC^1 \text{ s.t. } A_n(x, f(x))$$

witnessing properties

[CM]

$$\exists y\, A_n(x,y), \text{ where } A_n \text{ is propositional, have p-size } \mathsf{G}_1^* \text{ proofs}$$
$$\Rightarrow$$
$$\exists f \in \mathsf{P}/\text{poly s.t. } A_n(x, f(x))$$

[CM]

$$\exists y\, A_n(x,y), \text{ where } A_n \text{ is propositional, have p-size } \mathsf{G}_0 \text{ proofs}$$
$$\Rightarrow$$
$$\exists f \in \mathsf{NC}^1 \text{ s.t. } A_n(x, f(x))$$

[BBC]

$$\exists y\, A_n(x,y) \text{ have p-size } \mathsf{EF} + \forall\text{red proofs}$$
$$\Rightarrow$$
$$\exists f \in P/poly \text{ s.t. } A_n(x, f(x))$$

Separations

$\mathsf{NP} \not\subseteq \mathsf{P/poly} \Rightarrow \exists$ formulas with p-size G_1 proofs but no p-size $\mathsf{EF} + \forall\mathsf{red}$ proofs

Separations

NP $\not\subseteq$ P/poly $\Rightarrow$ $\exists$ formulas with p-size G_1 proofs but no p-size EF + $\forall$red proofs

'take $f \notin P/poly$ s.t. $T^1_2 \vdash \exists y\, f(x) = y$'

Separations

$\mathsf{NP} \not\subseteq \mathsf{P/poly} \Rightarrow \exists$ formulas easy for G_0^* but hard for $\mathsf{EF} + \forall\mathsf{red}$

Separations

$\mathsf{NP} \not\subseteq \mathsf{P/poly} \Rightarrow \exists$ formulas easy for G_0^* but hard for $\mathsf{EF} + \forall\mathsf{red}$

$\mathsf{P/poly} \not\subseteq \mathsf{NC}^1 \Rightarrow \exists$ formulas easy for $\mathsf{EF} + \forall\mathsf{red}$ but hard for G_0

Separations

$\mathsf{NP} \not\subseteq \mathsf{P/poly} \Rightarrow \exists$ formulas easy for G_0^* but hard for $\mathsf{EF}+\forall\mathsf{red}$

$\mathsf{P/poly} \not\subseteq \mathsf{NC}^1 \Rightarrow \exists$ formulas easy for $\mathsf{EF}+\forall\mathsf{red}$ but hard for G_0

Simulations

G_1^* p-simulates $\mathsf{EF}+\forall\mathsf{red}$

i.e. if ϕ has an $\mathsf{EF}+\forall\mathsf{red}$-proof π, it has also a G_1^* proof $f(|\pi|)$ for a poly-time function f

Separations

$\mathsf{NP} \not\subseteq \mathsf{P/poly} \Rightarrow \exists$ formulas easy for G_0^* but hard for $\mathsf{EF} + \forall\mathsf{red}$

$\mathsf{P/poly} \not\subseteq \mathsf{NC}^1 \Rightarrow \exists$ formulas easy for $\mathsf{EF} + \forall\mathsf{red}$ but hard for G_0

Simulations

G_1^* p-simulates $\mathsf{EF} + \forall\mathsf{red}$

i.e. if ϕ has an $\mathsf{EF} + \forall\mathsf{red}$-proof π, it has also a G_1^* proof $f(|\pi|)$ for a poly-time function f

`Open problem`: G_0^* p-simulates $\mathsf{Frege} + \forall\mathsf{red}$?

Formalized strategy extraction

Given an $\mathrm{EF} + \forall\mathrm{red}$ proof π of a QBF

$$\forall x_1 \exists y_1 \ldots \forall x_n \exists y_n \, \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

we can construct in $poly(|\pi|)$-time an EF proof of

$$\bigwedge_{i=1}^{n} (y_i = C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \rightarrow \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

for some circuits C_i.

Formalized strategy extraction

Given an $\mathrm{EF} + \forall\mathrm{red}$ proof π of a QBF

$$\forall x_1 \exists y_1 \dots \forall x_n \exists y_n \, \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

we can construct in $poly(|\pi|)$-time an EF proof of

$$\bigwedge_{i=1}^{n} (y_i = C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \to \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

for some circuits C_i.

Applications:

Simulations (mentioned before)

Normal forms of $\mathrm{EF} + \forall\mathrm{red}$ proofs

Correspondence to intuitionistic theories

Normal forms of EF + ∀red proofs

'Start with EF derivation and finish with ∀red rules'

Normal forms of EF + $\forall$red proofs

'Start with EF derivation and finish with $\forall$red rules'

To refute

$$\exists x_1 \forall y_1 \ldots \exists x_n \forall y_n \, \neg\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

Start with $\neg\phi$ and derive in EF

$$\bigvee_{i=1}^{n} (y_i \neq C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}))$$

Then apply $\forall$red to replace y_i's by $C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})$ and derive $\emptyset$

Normal forms of EF + ∀red proofs

'Start with EF derivation and finish with ∀red rules'

To refute

$$\exists x_1 \forall y_1 \ldots \exists x_n \forall y_n \, \neg\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

Start with $\neg\phi$ and derive in EF

$$\bigvee_{i=1}^{n} (y_i \neq C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}))$$

Then apply ∀red to replace y_i's by $C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})$ and derive $\emptyset$

EF + ∀red p-equivalent to EF + $\forall\text{red}_{0,1}$

Normal forms of EF + ∀red **proofs**

'Start with EF derivation and finish with ∀red rules'

To refute

$$\exists x_1 \forall y_1 \dots \exists x_n \forall y_n \neg\phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

Start with $\neg\phi$ and derive in EF

$$\bigvee_{i=1}^{n} (y_i \neq C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}))$$

Then apply ∀red to replace y_i's by $C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$ and derive $\emptyset$

EF + ∀red p-equivalent to EF + $\forall\text{red}_{0,1}$

$$C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}) \neq 0/1 \vee \bigvee_{i=1}^{n-1} (y_i \neq C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}))$$

First-order theories

[Buss]
S^1_2 - $L = \{ 0, S, +, \cdot, \leq, \left\lfloor \frac{x}{2} \right\rfloor, |x|, \# \}$

First-order theories

[Buss]

S_2^1 - $L = \{ 0, S, +, \cdot, \leq, \lfloor \frac{x}{2} \rfloor, |x|, \# \}$

$|x| \sim$ 'the length of the binary representation of x'

$x \# y = 2^{|x| \cdot |y|}$

First-order theories

[Buss]

S_2^1 - $L = \{ 0, S, +, \cdot, \leq, \left\lfloor \frac{x}{2} \right\rfloor, |x|, \# \}$

$|x| \sim$ 'the length of the binary representation of x'

$x \# y = 2^{|x| \cdot |y|}$

Axioms: for symbols in L

First-order theories

[Buss]

S^1_2 - $L = \{\, 0, S, +, \cdot, \leq, \left\lfloor \frac{x}{2} \right\rfloor, |x|, \# \,\}$

$|x| \sim$ 'the length of the binary representation of x'

$x \# y = 2^{|x| \cdot |y|}$

Axioms: for symbols in L

polynomial induction: for Σ^b_1-formulas A

$$A(0) \wedge \forall x \left(A(\left\lfloor \frac{x}{2} \right\rfloor) \rightarrow A(x) \right) \rightarrow \forall x\, A(x)$$

First-order theories

[Buss]

S_2^1 - $L = \{\, 0, S, +, \cdot, \leq, \left\lfloor \frac{x}{2} \right\rfloor, |x|, \# \,\}$

$|x| \sim$ 'the length of the binary representation of x'

$x \# y = 2^{|x| \cdot |y|}$

Axioms: for symbols in L

polynomial induction: for Σ_1^b-formulas A

$$A(0) \wedge \forall x \left(A(\left\lfloor \frac{x}{2} \right\rfloor) \rightarrow A(x) \right) \rightarrow \forall x \, A(x)$$

[Buss] $S_2^1 \vdash \exists y \, A(x, y)$ for Σ_1^b-formula $A \Rightarrow \exists$ p-time f s.t. $A(x, f(x))$

First-order theories

[Buss]
S_2^1 - $L = \{\, 0, S, +, \cdot, \leq, \left\lfloor \frac{x}{2} \right\rfloor, |x|, \# \,\}$
$|x| \sim$ 'the length of the binary representation of x'
$x \# y = 2^{|x| \cdot |y|}$
Axioms: for symbols in L
polynomial induction: for Σ_1^b-formulas A

$$A(0) \wedge \forall x \left(A(\left\lfloor \frac{x}{2} \right\rfloor) \rightarrow A(x) \right) \rightarrow \forall x\, A(x)$$

[Buss] $S_2^1 \vdash \exists y\, A(x, y)$ for Σ_1^b-formula $A \Rightarrow \exists$ p-time f s.t. $A(x, f(x))$

[Buss] [Cook, Urquhart]
IS_2^1 - S_2^1 but with
intuitionistic logic
polynomial induction for Σ_1^{b+} formulas (no $\rightarrow$ or $\neg$ signs)

First-order theories

[Buss]
S^1_2 - $L = \{ 0, S, +, \cdot, \leq, \lfloor \frac{x}{2} \rfloor, |x|, \# \}$
$|x| \sim$ 'the length of the binary representation of x'
$x\#y = 2^{|x|\cdot|y|}$
Axioms: for symbols in L
polynomial induction: for Σ^b_1-formulas A

$$A(0) \wedge \forall x \left(A(\left\lfloor \frac{x}{2} \right\rfloor) \to A(x) \right) \to \forall x \, A(x)$$

[Buss] $S^1_2 \vdash \exists y \, A(x, y)$ for Σ^b_1-formula $A \Rightarrow \exists$ p-time f s.t. $A(x, f(x))$

[Buss] [Cook, Urquhart]
IS^1_2 - S^1_2 but with
intuitionistic logic
polynomial induction for Σ^{b+}_1 formulas (no $\to$ or $\neg$ signs)

[Buss] $IS^1_2 \vdash \exists y \, A(x, y) \Rightarrow \exists$ p-time f s.t. $A(x, f(x))$

First-order theories vs propositional

first order statement		QBF formulas
$T(x)$	$\longmapsto$	$T_1(x), T_2(x), \ldots$

First-order theories vs propositional

first order statement		QBF formulas
$T(x)$	$\longmapsto$	$T_1(x), T_2(x), \ldots$

$\forall x\, T(x) \leftrightarrow \forall n \forall x, |x| = n\; T(x)$

First-order theories vs propositional

first order statement		QBF formulas
$T(x)$	$\longmapsto$	$T_1(x), T_2(x), \ldots$

$$\forall x\, T(x) \leftrightarrow \forall n \forall x, |x| = n\, T(x)$$

$$\forall x, |x| = n\, T(x) \leftrightarrow \forall x \text{ 'quantifiers' 'open formula'}$$

First-order theories vs propositional

$$\begin{array}{ccc} \text{first order statement} & & \text{QBF formulas} \\ T(x) & \longmapsto & T_1(x), T_2(x), \ldots \end{array}$$

$$\forall x\, T(x) \leftrightarrow \forall n \forall x, |x| = n\, T(x)$$

$$\forall x, |x| = n\, T(x) \leftrightarrow \forall x \text{ 'quantifiers' 'open formula'}$$

S^1_2 corresponds to G^*_1

$$S^1_2 \vdash T \Rightarrow \exists \text{ p-size } G^*_1 \text{ proofs of } T_n$$

First-order theories vs propositional

first order statement		QBF formulas
$T(x)$	$\longmapsto$	$T_1(x), T_2(x), \ldots$

$$\forall x\, T(x) \leftrightarrow \forall n \forall x, |x| = n\, T(x)$$

$$\forall x, |x| = n\, T(x) \leftrightarrow \forall x \text{ 'quantifiers' 'open formula'}$$

S^1_2 corresponds to G^*_1

$$S^1_2 \vdash T \Rightarrow \exists \text{ p-size } \mathsf{G}^*_1 \text{ proofs of } T_n$$

IS^1_2 corresponds to $\mathsf{EF} + \forall\mathsf{red}$

$$IS^1_2 \vdash T \Rightarrow \exists \text{ p-size } \mathsf{EF} + \forall\mathsf{red} \text{ proofs of } T_n$$

$$IS^1_2 \vdash \text{'}\mathsf{EF} + \forall\mathsf{red} \text{ is sound'}$$

Circuit and proof complexity united

$$\exists \text{ formulas with no p-size EF} + \forall\text{red proofs}$$
$$\Leftrightarrow$$
$$\text{PSPACE} \not\subseteq \text{P/poly or } \exists \text{ formulas with no p-size EF proofs}$$

Circuit and proof complexity united

$$\exists \text{ formulas with no p-size } \mathsf{EF} + \forall\mathsf{red} \text{ proofs}$$
$$\Leftrightarrow$$
$$\mathsf{PSPACE} \not\subseteq \mathsf{P/poly} \text{ or } \exists \text{ formulas with no p-size } \mathsf{EF} \text{ proofs}$$

$$\phi_n \text{ hard formulas for } \mathsf{EF} + \forall\mathsf{red} \wedge \mathsf{PSPACE} \subseteq \mathsf{P/poly}$$
$$\Rightarrow$$
$$\phi_n \text{ are equivalent to hard tautologies}$$

Thank You