On Some Conjectures in Proof Complexity

Pavel Pudlák

Mathematical Institute, Academy of Sciences, Prague

Dagstuhl 14.10.2014

Overview

1. Motivation: feasible incompleteness, axiomatic appraoch
2. Syntactically vs. semantically defined classes, deterministic vs. nondeterministic conjectures
3. Finite Σ_1^b reflection principle
4. Herbrand Consistency Search
5. Universal and existential conjectures
6. Problems

Feasible Incompleteness

"feasible"

1. sentence and propositions speak about finite objects,
2. proofs of them are short and easily constructable.

"feasibly incomplete" = not feasibly complete

Feasible Incompleteness

"feasible"

1. sentence and propositions speak about finite objects,
2. proofs of them are short and easily constructable.

"feasibly incomplete" = not feasibly complete

"finite version of the 2nd incompleteness theorem"

Gödel, Kreisel, H. Friedman, Cook

basic examples

S, T first order theories, finitely axiomatized, containing a fragment of arithmetic so that they are Σ-complete.

$Con_T(n) :=$ no contradiction of length $\leq n$ in T

Conjecture

If T is sufficiently stronger than S and S is consistent, then S-proofs of $Con_T(n)$ do not have polynomial length (in n).

basic examples

S, T first order theories, finitely axiomatized, containing a fragment of arithmetic so that they are Σ-complete.

$Con_T(n) :=$ no contradiction of length $\leq n$ in T

Conjecture

If T is sufficiently stronger than S and S is consistent, then S-proofs of $Con_T(n)$ do not have polynomial length (in n).

Conjecture

NP $\neq$ coNP

Syntactically and semantically defined classes

Examples

1. **P, NP** syntactically; they have complete problems
2. **NP** $\cap$ **coNP** semantically; probably does not have
3. **BPP** ?

Syntactically and semantically defined classes

Examples

1. **P, NP** syntactically; they have complete problems
2. **NP** $\cap$ **coNP** semantically; probably does not have
3. **BPP** ?

- To show that a language X is in a semantically defined class $\mathcal{C}$, we need a proof.
- One theory (e.g. ZFC) does not suffice to prove "$X \in \mathcal{C}$" for all X in $\mathcal{C}$.

Syntactically and semantically defined classes

Examples

1. **P, NP** syntactically; they have complete problems
2. **NP** $\cap$ **coNP** semantically; probably does not have
3. **BPP** ?

- To show that a language X is in a semantically defined class $\mathcal{C}$, we need a proof.
- One theory (e.g. ZFC) does not suffice to prove "$X \in \mathcal{C}$" for all X in $\mathcal{C}$. ($\Leftrightarrow$ X is not a syntactical class)

Deterministic vs. nondeterministic

Conjecture (deterministic)

If T is sufficiently stronger than S and S is consistent, then S-proofs of $Con_T(n)$ cannot be constructed in polynomial time.

(equivalent to the non-existence of a p-optimal proof system for **TAUT**)

Conjecture (nondeterministic)

If T is sufficiently stronger than S and S is consistent, then S-proofs of $Con_T(n)$ do not have polynomial length.

(equivalent to the non-existence of a length-optimal proof system for **TAUT**)

Conjecture

P $\neq$ **NP**

Conjecture

NP $\neq$ **coNP**

Conjecture

P $\neq$ **NP**

Conjecture

NP $\neq$ **coNP**

Nondeterministic conjectures are stronger.

Reflection principles

Let T be an (arithmetical) theory and ϕ a sentence. Then $Rfn_T(\phi)$ denotes the sentence

$$\forall u(Pr_T(u, \lceil \phi \rceil) \rightarrow \phi),$$

where $Pr_T(u, \lceil \phi \rceil)$ says that u is a proof of ϕ in T and $\lceil \phi \rceil$ is the Gödel number of ϕ.

Reflection principles

Let T be an (arithmetical) theory and ϕ a sentence. Then $Rfn_T(\phi)$ denotes the sentence

$$\forall u(Pr_T(u, \lceil \phi \rceil) \rightarrow \phi),$$

where $Pr_T(u, \lceil \phi \rceil)$ says that u is a proof of ϕ in T and $\lceil \phi \rceil$ is the Gödel number of ϕ.

Fact $Rfn_T(0 = 1)$ is Con_T.

Reflection principles

Let T be an (arithmetical) theory and ϕ a sentence. Then $Rfn_T(\phi)$ denotes the sentence

$$\forall u(Pr_T(u, \lceil \phi \rceil) \rightarrow \phi),$$

where $Pr_T(u, \lceil \phi \rceil)$ says that u is a proof of ϕ in T and $\lceil \phi \rceil$ is the Gödel number of ϕ.

Fact $Rfn_T(0 = 1)$ is Con_T.

Let $\sigma(y)$ be a universal Σ_1 formula.

$$\Sigma_1 RFN_T \ := \ \forall u, y(Pr_T(u, \lceil \sigma(\bar{y}) \rceil) \rightarrow \sigma(y))$$

the uniform Σ_1-reflection principle.

The uniform Σ_1^b-reflection principle

$$\Sigma_1^b RFN_T \ := \ \forall u, y(Pr_T(u, \lceil \sigma'(\bar{y}) \rceil) \rightarrow \sigma'(y))$$

where $\sigma'(y)$ be a universal Σ_1^b formula.

Finite Σ_1^b reflection principle

Definition

Let T be a theory, $A(x, y) \in L(PV)$ (i.e., A represents a binary relation decidable in polynomial time), $n \in \mathbb{N}$. Then $\Sigma_1^b Rfn_T^A(n)$ will denote the sentence:

$$\forall u, |u| \leq \bar{n}\, \forall x, |x| \leq \bar{n}\ (Pr_T(u, \lceil \exists y, |y| \leq \bar{n}\ A(\bar{x}, y) \rceil) \rightarrow \exists z, |z| \leq \bar{n}\ A(x, z))$$

Finite Σ_1^b reflection principle

Definition

Let T be a theory, $A(x, y) \in L(PV)$ (i.e., A represents a binary relation decidable in polynomial time), $n \in \mathbb{N}$. Then $\Sigma_1^b Rfn_T^A(n)$ will denote the sentence:

$$\forall u, |u| \leq \bar{n}\, \forall x, |x| \leq \bar{n}\ (Pr_T(u, \lceil \exists y, |y| \leq \bar{n}\ A(\bar{x}, y) \rceil) \rightarrow \exists z, |z| \leq \bar{n}\ A(x, z))$$

$Con_T(n)$ is $\Sigma_1^b Rfn_T^A(n)$ for A equal to $0 = 1$

Finite Σ_1^b reflection principle

Definition

Let T be a theory, $A(x, y) \in L(PV)$ (i.e., A represents a binary relation decidable in polynomial time), $n \in \mathbb{N}$. Then $\Sigma_1^b Rfn_T^A(n)$ will denote the sentence:

$$\forall u, |u| \leq \bar{n}\, \forall x, |x| \leq \bar{n}\ (Pr_T(u, \lceil \exists y, |y| \leq \bar{n}\ A(\bar{x}, y) \rceil) \rightarrow \exists z, |z| \leq \bar{n}\ A(x, z))$$

$Con_T(n)$ is $\Sigma_1^b Rfn_T^A(n)$ for A equal to $0 = 1$

$\Sigma_1^b RFN_T(n)$ will denote $\Sigma_1^b Rfn_T^A(n)$ for a fixed universal polynomial time relation A.

Conjecture

There is no consistent theory S such that for every consistent theory T, proofs of $\Sigma_1^b RFN_T(n)$ in S can be constructed in polynomial time.

Conjecture

There is no consistent theory S such that for every consistent theory T, proofs of $\Sigma_1^b RFN_T(n)$ in S can be constructed in polynomial time.

Conjecture (nondeterministic version)

There is no consistent theory S such that for every consistent theory T, there are proofs of $\Sigma_1^b RFN_T(n)$ in S of polynomial length.

Proposition

If **P=NP**, *then there exists a consistent theory* S *such that for every consistent theory* T *and every* $B \in L(PV)$, *proofs of* $\Sigma^b_1 Rfn^B_T(n)$ *in* S *can be constructed in polynomial time.*

Proof.

Note that

- If T is consistent, then the sentences $\Sigma^b_1 Rfn^B_T(n)$ are true.
- If **P=NP**, then we can test in polynomial time whether $\Sigma^b_1 Rfn^B_T(n)$ is true.

So we axiomatize S by the true sentences of this form.

(One can also formalize it by a finite number of axioms.) □

Proof systems for **SAT**

A proof system for **SAT** is an $A(x, y) \in L(PV)$ which is sound and complete when interpreted as "y is a proof of $x \in$ **SAT**".

A polynomial simulation of A by B is an $f \in$ **FP** such that $A(x, y) \rightarrow B(x, f(x, y))$.

Proof systems for **SAT**

A proof system for **SAT** is an $A(x, y) \in L(PV)$ which is sound and complete when interpreted as "y is a proof of $x \in$ **SAT**".

A polynomial simulation of A by B is an $f \in$ **FP** such that $A(x, y) \rightarrow B(x, f(x, y))$.

Examples

1. $sat(x, y)$ — the standard proof system for **SAT**, where y is a satisfying assignment for x.

Proof systems for **SAT**

A proof system for **SAT** is an $A(x, y) \in L(PV)$ which is sound and complete when interpreted as "y is a proof of $x \in$ **SAT**".

A polynomial simulation of A by B is an $f \in$ **FP** such that $A(x, y) \rightarrow B(x, f(x, y))$.

Examples

1. $sat(x, y)$ — the standard proof system for **SAT**, where y is a satisfying assignment for x.
2. $sat(x, y)$, or y is a witness (using [AKS]) that n is not a prime if x is the proposition "n is not a prime".

If factoring is hard, 2. is not reducible to 1.

Proposition

Suppose that S is a consistent theory such that for every consistent theory T and every $B \in L(PV)$, proofs of $\Sigma_1^b Rfn_T^B(n)$ in S can be constructed in polynomial time.
Then there exists a p-optimal proof system for **SAT**.

Proposition

Suppose that S is a consistent theory such that for every consistent theory T and every $B \in L(PV)$, proofs of $\Sigma^b_1 Rfn^B_T(n)$ in S can be constructed in polynomial time.
Then there exists a p-optimal proof system for **SAT**.

Proof.

Given S, define a proof system for **SAT** by:

- y is a proof of $x \Leftrightarrow y$ is an S proof of $\exists z\ sat(\bar{x}, z)$.

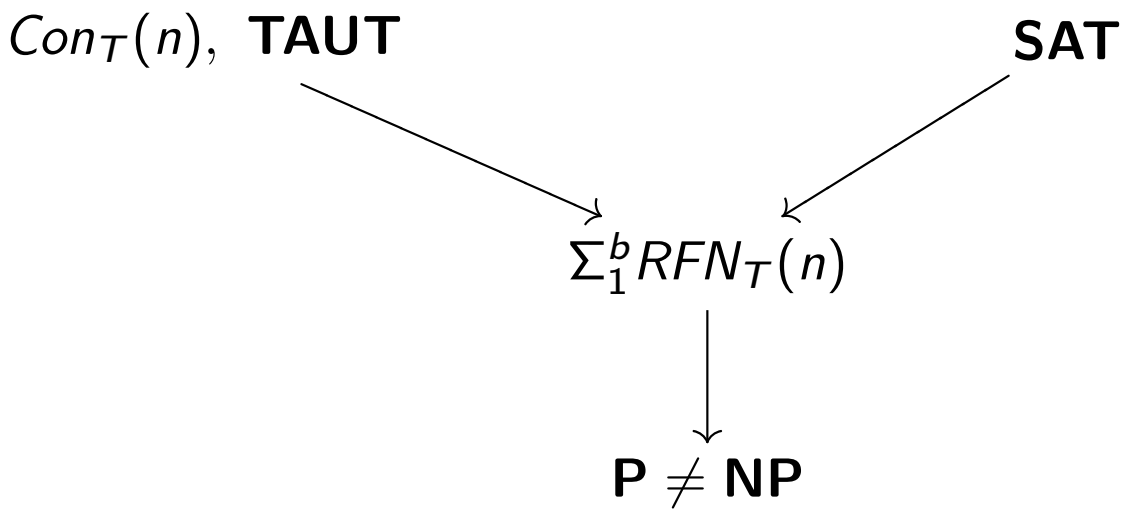
If A is a proof system for **SAT**, then let T be axiomatized by

$$\forall x, y(A(x, y) \rightarrow \exists z\ sat(x, z)).$$

Given an A-proof of ϕ, we can construct a T-proof of

$$\exists z\ sat(\bar{\phi}, z),$$

from which we get an S-proof of the same using $\Sigma^b_1 Rfn^B_T(n)$ with $n = |\phi|$ and $B(x, y) = sat(x, y)$. □



legend:

- $Con_T(n)$ — for no consistent S, we can construct S-proofs of $Con_T(n)$ in poly. time
- $\Sigma_1^b RFN_T(n)$ — for no consistent S, we can construct S-proofs of $\Sigma_1^b RFN_T(n)$ in poly. time
- **TAUT** — no optimal proof system for **TAUT**
- **SAT** — no optimal proof system for **SAT**

Total Polynomial Search

Definition

TPS $:= \{R \in \mathbf{P} \ ; \ \forall x \exists y, |y| \leq |x| \ R(x,y)\}$

Other notation **TFNP**, $\mathbf{NPMV_t}$.

R is reducible to Q if there are $f, g \in \mathbf{FP}$ such that for all x and z,

$$Q(f(x), z) \ \Rightarrow \ R(x, g(x,z)).$$

Total Polynomial Search

Definition

$\mathbf{TPS} := \{R \in \mathbf{P} \ ; \ \forall x \exists y, |y| \leq |x| \ R(x,y)\}$

Other notation $\mathbf{TFNP}$, $\mathbf{NPMV_t}$.

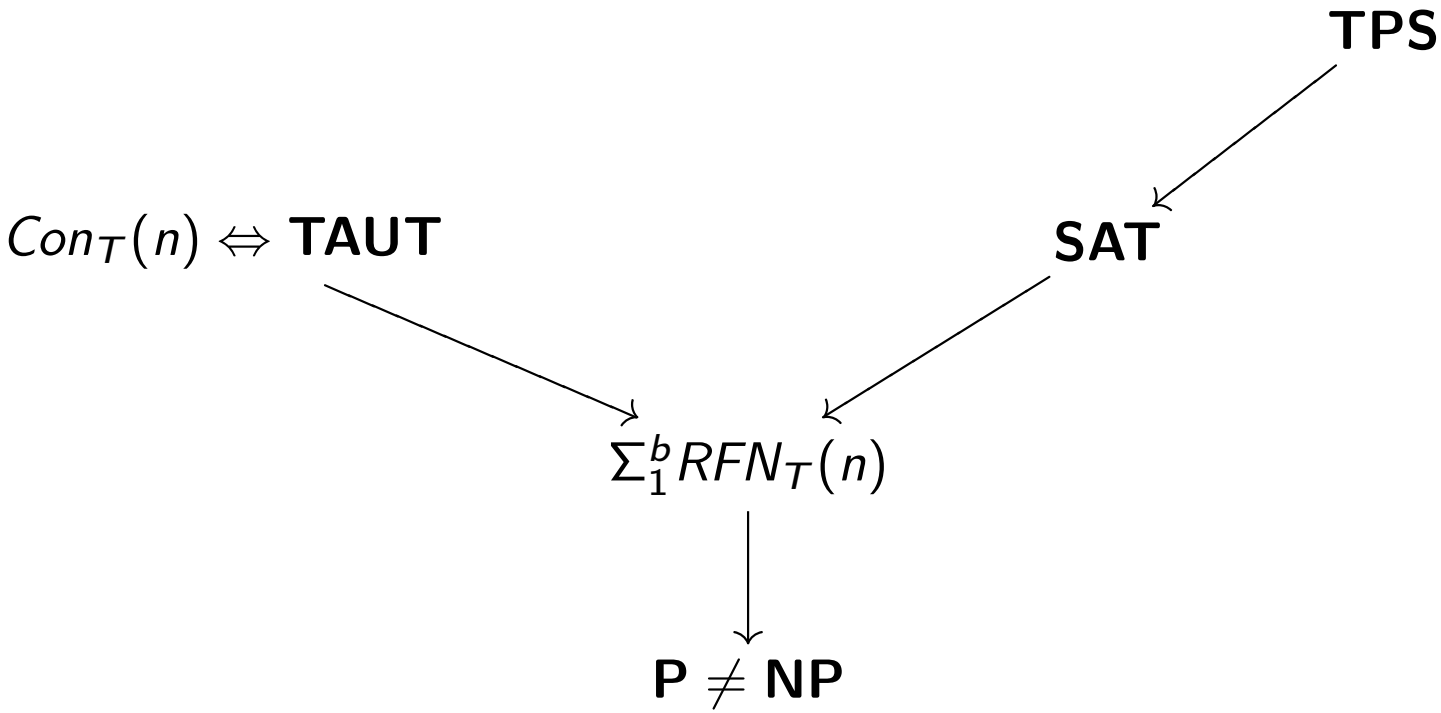
R is reducible to Q if there are $f, g \in \mathbf{FP}$ such that for all x and z,

$$Q(f(x), z) \ \Rightarrow \ R(x, g(x, z)).$$

Conjecture

There is no complete **TPS** *problem.*

Essentially, it means that **TPS** is not syntactical.



legend:

- $Con_T(n)$ ($\Sigma_1^b RFN_T(n)$) — for no consistent S we can construct S-proofs of $Con_T(n)$ ($\Sigma_1^b RFN_T(n)$) in poly. time
- **TAUT** (**SAT**) — no optimal proof system for **TAUT** (**SAT**)
- **TPS** — no complete total poly. search problem problem

Herbrand Consistency Search

Definition

Let Φ be $\forall x_1 \ldots \forall x_k \phi(x_1, \ldots, x_k)$ where ϕ is open. Then $HCS(\Phi)$, the Herbrand Consistency Search for Φ, is the following search problem:

- given terms τ_{ij} in the language of ϕ, $i = 1, \ldots, n$, $j = 1, \ldots, k$, find a truth assignment to the atomic subformulas of $\phi(\tau_{i1}, \ldots, \tau_{ik})$, for $i = 1, \ldots, n$, that makes $\bigwedge_{i=1}^{n} \phi(\tau_{i1}, \ldots, \tau_{ik})$ true.[1]

If Φ is consistent, then $HCS(\Phi) \in \mathbf{TPS}$.

[1] which shows that $\bigvee_{i=1}^{n} \neg\phi(\tau_{i1}, \ldots, \tau_{ik})$ is not a Herbrand proof of $\neg\Phi$.

Examples

1. Skolemization of the theory of dense linear orderings:

$$0 < 1$$

$$\neg x < x,\ x < y \vee x = y \vee y < x,$$

$$x < y \wedge y < z \rightarrow x < z,$$

$$x < f(x, y) \wedge f(x, y) < y,$$

plus the identity and equality axioms. To solve the HCS, we need only to find an interpretation of the terms in a finite linear ordering and then to assign the truth values according to this interpretation.

Examples

1. Skolemization of the theory of dense linear orderings:

$$0 < 1$$

$$\neg x < x,\ x < y \vee x = y \vee y < x,$$

$$x < y \wedge y < z \rightarrow x < z,$$

$$x < f(x, y) \wedge f(x, y) < y,$$

plus the identity and equality axioms. To solve the HCS, we need only to find an interpretation of the terms in a finite linear ordering and then to assign the truth values according to this interpretation.

Solvable in polynomial time.

Examples

1. Skolemization of the theory of dense linear orderings:

$$0 < 1$$

$$\neg x < x,\ x < y \vee x = y \vee y < x,$$

$$x < y \wedge y < z \rightarrow x < z,$$

$$x < f(x, y) \wedge f(x, y) < y,$$

plus the identity and equality axioms. To solve the HCS, we need only to find an interpretation of the terms in a finite linear ordering and then to assign the truth values according to this interpretation.

Solvable in polynomial time.

2. Skolemization of a strong finite fragment of arithmetic. The Skolem functions are not computable, hence interpretation in $\mathbb{N}$ does not help us.

Examples

1. Skolemization of the theory of dense linear orderings:

$$0 < 1$$

$$\neg x < x,\ x < y \vee x = y \vee y < x,$$

$$x < y \wedge y < z \rightarrow x < z,$$

$$x < f(x, y) \wedge f(x, y) < y,$$

plus the identity and equality axioms. To solve the HCS, we need only to find an interpretation of the terms in a finite linear ordering and then to assign the truth values according to this interpretation.

Solvable in polynomial time.

2. Skolemization of a strong finite fragment of arithmetic. The Skolem functions are not computable, hence interpretation in $\mathbb{N}$ does not help us.

Probably not solvable in polynomial time.

Proposition

If $\Phi \vdash \Psi$, *then* $HCS(\Psi)$ *is reducible to* $HCS(\Phi)$.

Proposition

If $\Phi \vdash \Psi$, *then* $HCS(\Psi)$ *is reducible to* $HCS(\Phi)$.

Theorem

For every total polynomial search problem R, *there exist a consistent universal sentence* Φ *such that the problem* R *is reducible to* $HCS(\Phi)$.

Proof-idea.

Given $R \in \mathbf{TPS}$, formalize the sentence $\forall x \exists y, |y| \leq |x|\ R(x, y)$ in a suitable way. □

Proposition

If $\Phi \vdash \Psi$, *then* $HCS(\Psi)$ *is reducible to* $HCS(\Phi)$.

Theorem

For every total polynomial search problem R, *there exist a consistent universal sentence* Φ *such that the problem* R *is reducible to* $HCS(\Phi)$.

Proof-idea.

Given $R \in \mathbf{TPS}$, formalize the sentence $\forall x \exists y, |y| \leq |x|\ R(x, y)$ in a suitable way. □

The conjecture about the nonexistence of a complete problem in **TPS** is equivalent to:

Conjecture

The complexity of $HCS(\Phi)$ *increases with the increasing strength of* Φ.

Disjoint pairs

Definition

- Disjoint **NP** pairs,
  $Disj\mathbf{NP} := \{(X, Y)\ ;\ X, Y \in \mathbf{NP}\ \wedge\ X \cap Y = \emptyset\}$;
- Disjoint **coNP** pairs,
  $Disj\mathbf{coNP} := \{(X, Y)\ ;\ X, Y \in \mathbf{coNP}\ \wedge\ X \cap Y = \emptyset\}$

Disjoint pairs

Definition

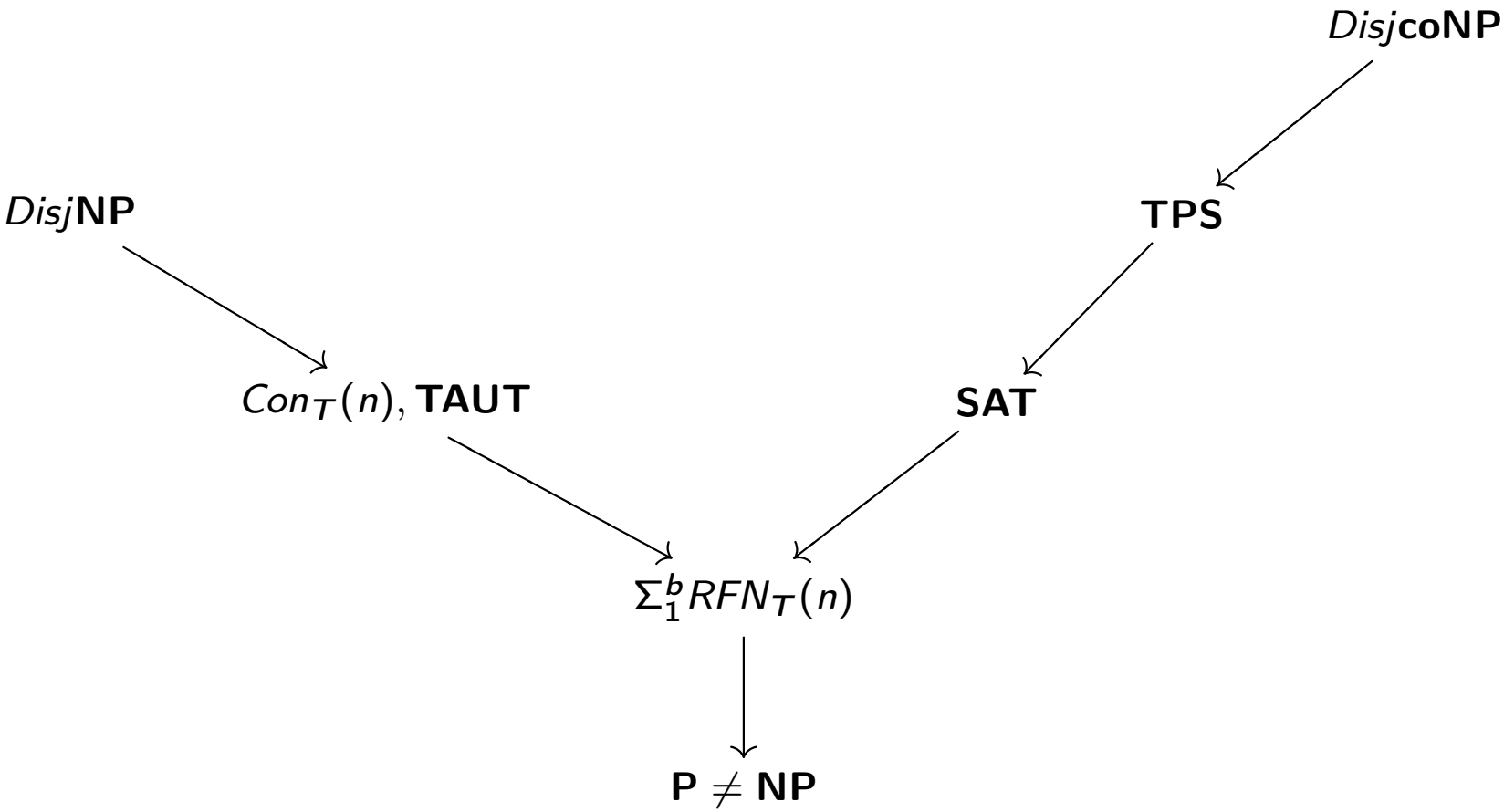
- Disjoint **NP** pairs,
  $Disj\mathbf{NP} := \{(X, Y)\ ;\ X, Y \in \mathbf{NP}\ \wedge\ X \cap Y = \emptyset\}$;
- Disjoint **coNP** pairs,
  $Disj\mathbf{coNP} := \{(X, Y)\ ;\ X, Y \in \mathbf{coNP}\ \wedge\ X \cap Y = \emptyset\}$

Conjecture

*There is no complete pair in Disj***NP**.

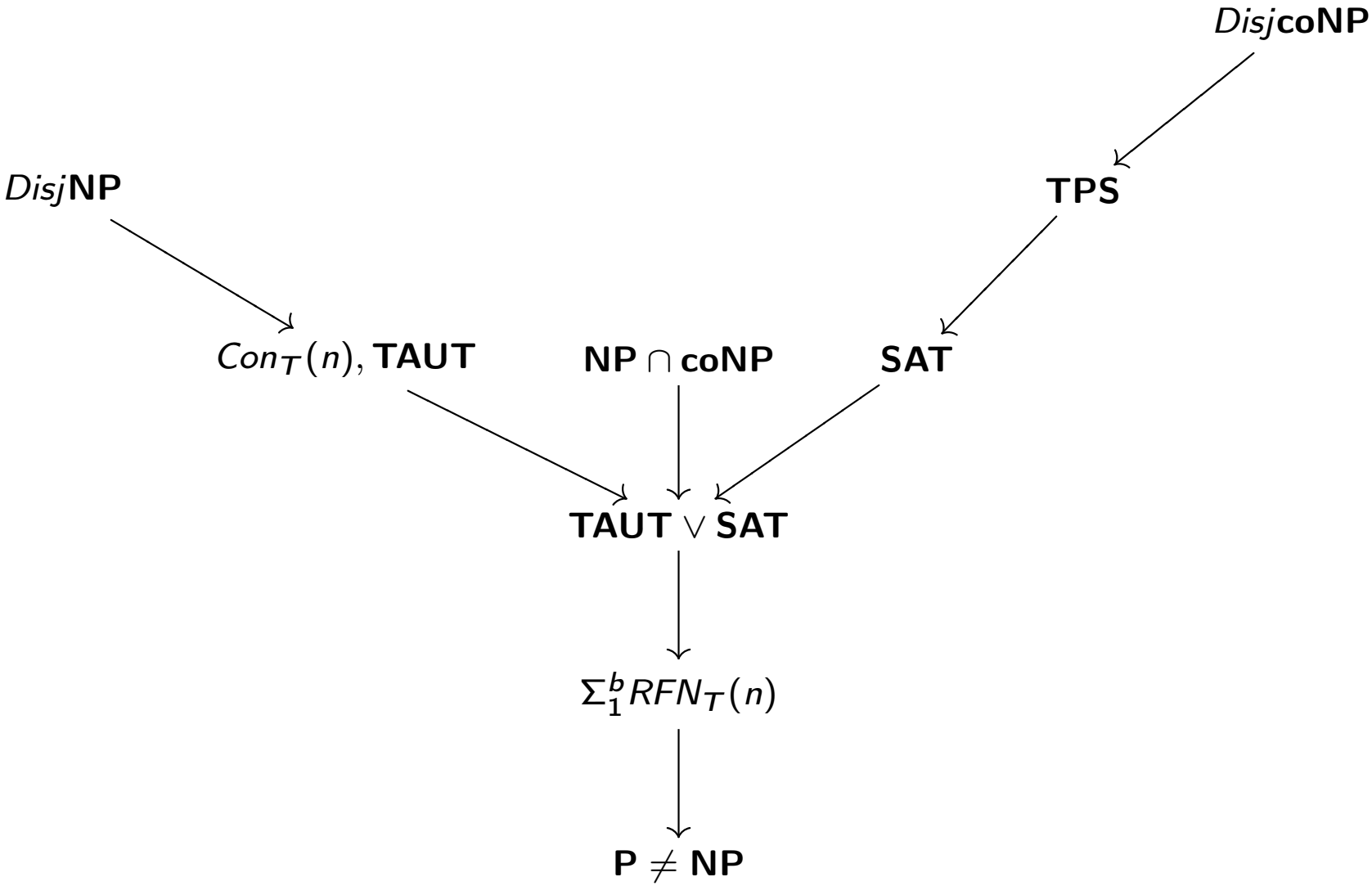
Conjecture

*There is no complete pair in Disj***coNP**.



legend:

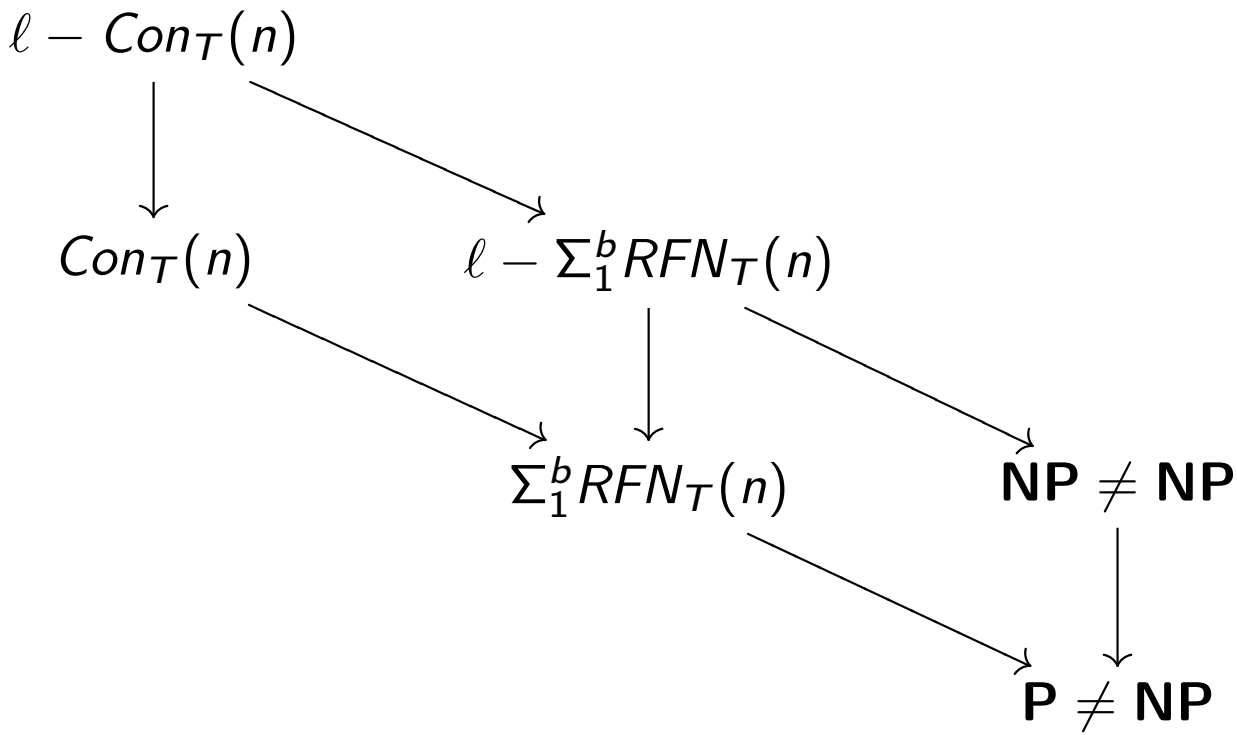
- $Con_T(n)$ ($\Sigma_1^b RFN_T(n)$) — for no consistent S we can construct S-proofs of $Con_T(n)$ ($\Sigma_1^b RFN_T(n)$) in poly. time
- **TAUT** (**SAT**) — no optimal proof system for **TAUT** (**SAT**)
- **TPS** — no complete total poly. search problem problem
- $Disj$**NP** ($Disj$**coNP**) — no complete $Disj$**NP** ($Disj$**coNP**) pair



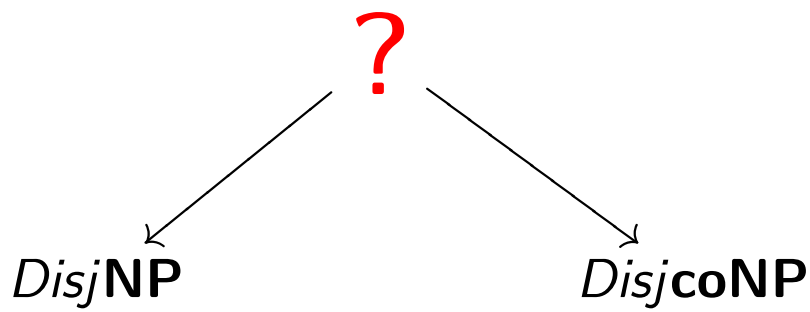
legend:

- **NP** ∩ **coNP** – no complete set in **NP** ∩ **coNP**

Nondeterministic conjectures



Problems

- 

- connections with other open problems/conjectures in computational complexity; in particular noncollaps of **PH**, cryptographic conjectures etc.
- nondeterministic versions
- relativizations

Thank you!