The

Function Technique

Eduardo Pinheiro

Paul Ilardi

Athanasios E. Papathanasiou

Outline

- Intro
- Basic Definitions
- One-way functions and the Classes P, NP, UP
- Unambiguous and Bounded Ambiguity one-way functions
- A look to the next talk...

Intro

- One-way functions are important for
  - Cryptography: Key components in the construction of protocols.
  - Complexity Theory: Unsuccessfully used to show that there exist two NP-complete sets that are not the same set in disguise.
- Their existence is unknown.
- **BUT:** Good candidates have been found.
- And complete characterizations. They exist:
  - if and only if two famous complexity classes are different.
  - if and only if pseudo-random generators exist (average-case cryptography).

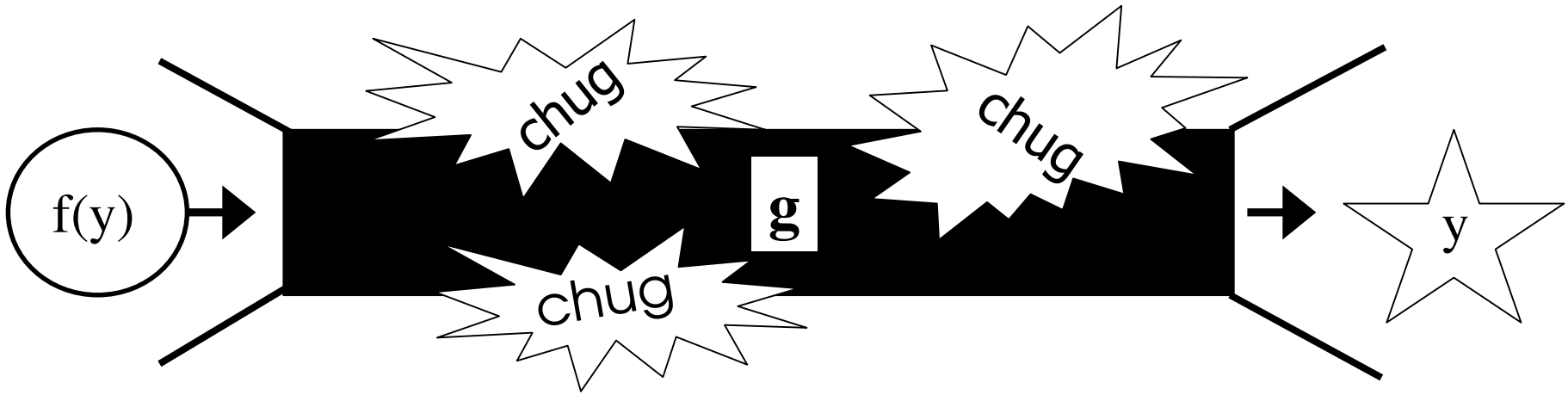
Basic Definitions

- ***Function:*** f:A→B is a **binary relation** between A and B which includes at **most** one pair <a, b>, a in A, b in B.
- ***Domain:*** The set of all x: $(\exists y) < x, y > \in f$
- ***Range:*** The set of all y: $(\exists x) < x, y > \in f$
- ***Total Function:*** Its domain coincides with A.
- ***Partial or Non-Total:*** otherwise
- ***Injective or 1-to-1:*** $\forall a, a' \in A, a \neq a' \Rightarrow f(a) \neq f(a')$
- ***Surjective:*** B = Range(f)
- ***Bijective:*** Both injective and surjective.

Definitions: Invertible Functions

- It is ***Poly-Time Invertible*** if there is a polynomial-time computable function g such that:

$$(\forall y \in range(f))$$
$$\left[y \in domain(g) \wedge g(y) \in domain(f) \wedge f(g(y)) = y\right]$$



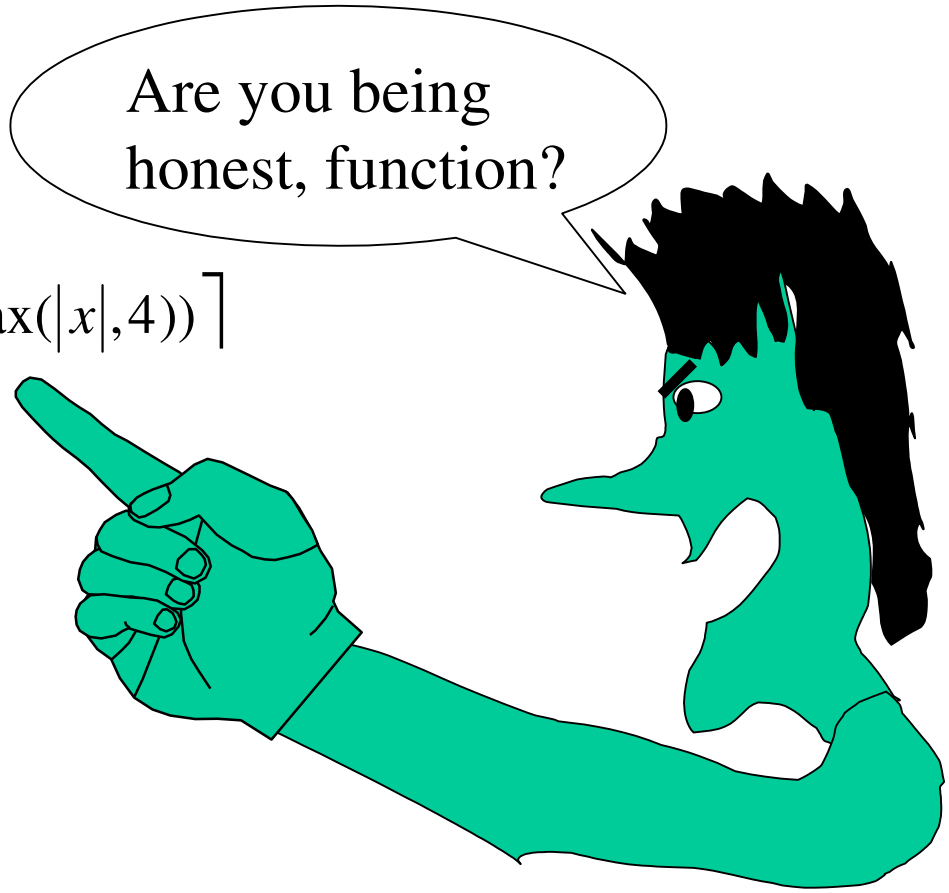
Definitions: Honest Functions

- A (possibly non-total) function is ***honest*** if:

$$(\exists\ \textit{polynomial}\ q)(\forall y \in \textit{range}(f))(\exists x)\left[|x| \leq q(|y|) \wedge f(x) = y\right]$$

- *Each element of **y** of the range of **f** has some inverse whose length is at most polynomially longer than the length of y.*

Non-Honesty Example



$$f(x) = 1^{\lceil \log\log\log(\max(|x|,4)) \rceil}$$

- **Nope**, because length(x) is exponentially longer than length(*f(x)*).

$$\forall y \in Range(f) : \left|f^{-1}(y)\right| \in (2^{2^{2^{|y-1|}}}, 2^{2^{2^{|y|}}}]$$

Definitions:One-Way Functions

- A (possibly non-total) function f is *one-way* if:

1. f is **polynomial-time** computable,
2. f is **not** polynomial-time invertible, and
3. f is **honest**.

Importance of Honesty Condition

$$f(x) = 1^{\lceil \log \log \log(\max(|x|, 4)) \rceil}$$

- The non-poly-time-invertability of our example function is just an artifact of the dramatically length-decreasing nature of *f*.
- *Not*-helpful in Cryptography
- Neither in Theory
- So, the honesty condition reassures us that if f is not poly-time invertible the reason is **not** a length trick

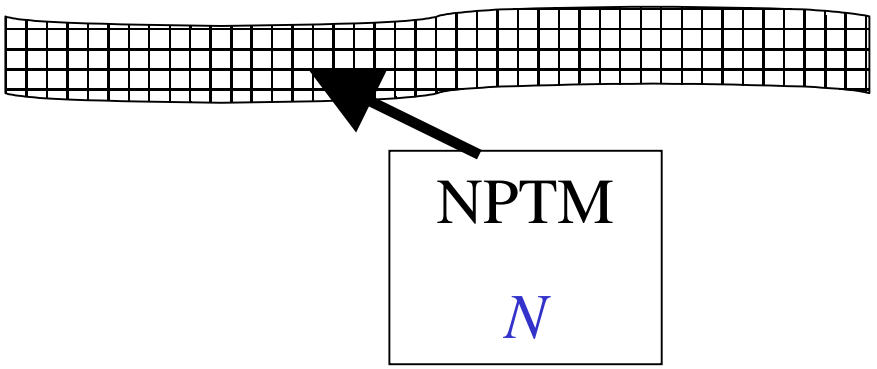
UP, $UP_{\leq k}$ Definitions

- $L \in$ UP iff there is a *NDTM* N, that:
  - accepts L,
  - N(x) has exactly 1 accepting path for $x \in L$,
- L is in $UP_{\leq k}$ iff there is a *NDTM* N that:
  - accepts L,
  - N(x) has at most k accepting paths for $x \in L$.

First Theorem

Theorem 1: One-way functions exist if and only if P≠NP.

Proof: ⇐Assume P ≠NP. Let A be in NP-P. There exist NPTM N such that $A = L(N)$.



Consider:

$$f(\langle x,y\rangle) = \begin{cases} 0x, \text{ if } y \text{ is an accepting path of } N(x) \\ 1x, \text{ otherwise} \end{cases}$$

First Theorem (cont.)

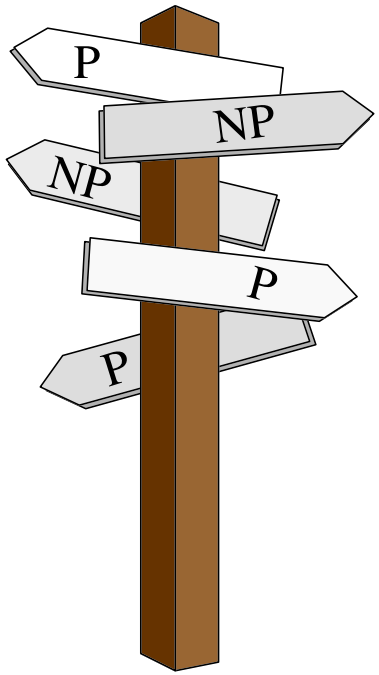
Suppose that f can be polynomial-time inverted by g as follows:

- On any input y: $g(0x) = \langle x,y \rangle$, test if y is an accepting path of $N(x)$. If so, accept, otherwise reject.

- But then $A \in$ P! Our assumption was that $A \in$ NP-P.

CONTRADICTION!!!

So f is a polynomial-time computable, honest function that is not polynomial-time invertible, i.e. ONE-WAY!



First Theorem (cont.)

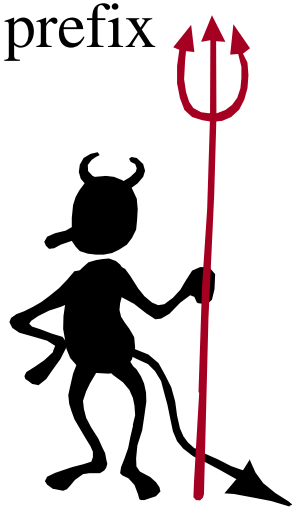
Proof: ⇐ Assume f is a one-way function.

Let p be the honesty polynomial for f. Consider the following language:

$$L = \{\langle z, pre\rangle \mid (\exists y)[|y| \le p(|z|) \wedge f(pre \cdot y) = z]\}$$

L is clearly in NP. If L were in P, we could invert it by prefix search:

Is $<z, \varepsilon>$ in L? If so, is $f(\varepsilon)=z$? If yes, function is invertable.
Is $<z, 0>$ in L? If so, is $f(0)=z$? If yes, function is invertable with prefix *0* else check if $<z, 1>$ is in L? If so, is $f(1)=z$? If yes, function is inverted with *1* as a prefix.
Next do the same with the second bit.
This can be used to find each bit successively.



This search grows polynomially, bounded by $p(|z|)$.

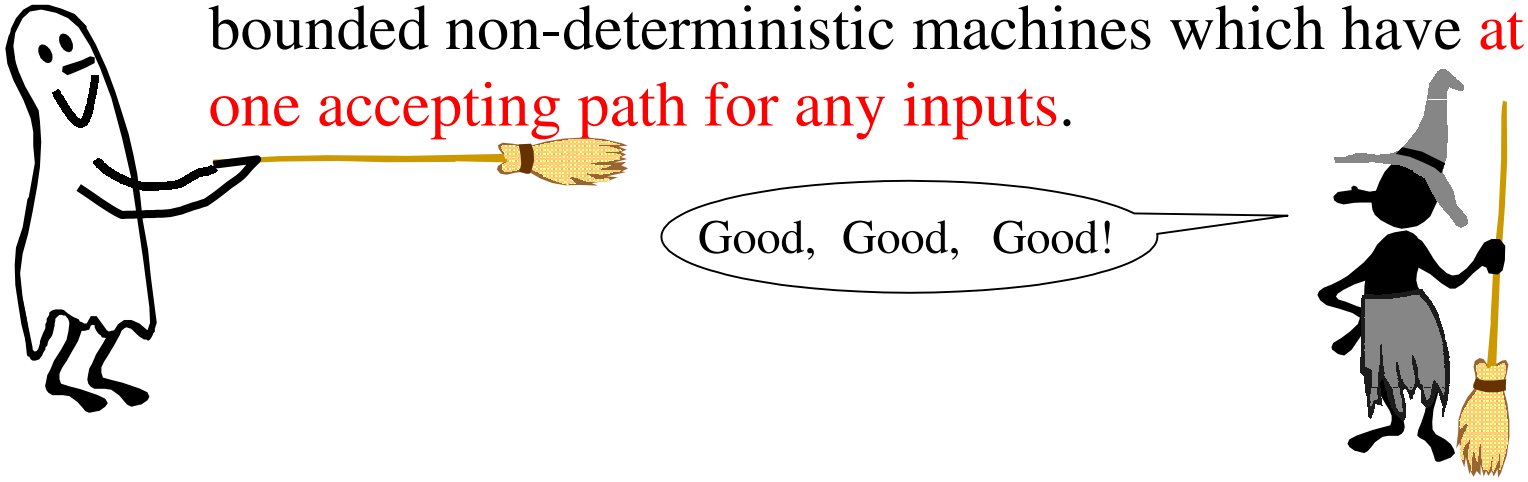
First Theorem (Part II)

- One-to-one one-way functions exist if and only if P ≠ UP.
- But, before the proof, some definitions:
- One-to-one functions are

$$f : \Sigma^* \rightarrow \Sigma^*$$

$$(\forall y \in \mathit{range}\ (f))[\ \|\{ x \mid f(x) = y \}\| = 1]$$

- UP is the class of sets accepted by polynomial-time bounded non-deterministic machines which have at most one accepting path for any inputs.



First Theorem (Part II)

- One-to-one one-way functions exist if and only if P ≠ UP.
- Similar proof, but

$$f(\langle x,y\rangle) = \begin{cases} 0x, \text{ if } y \text{ is an accepting path of } N(x) \\ 1\langle x,y\rangle, \text{ otherwise.} \end{cases}$$

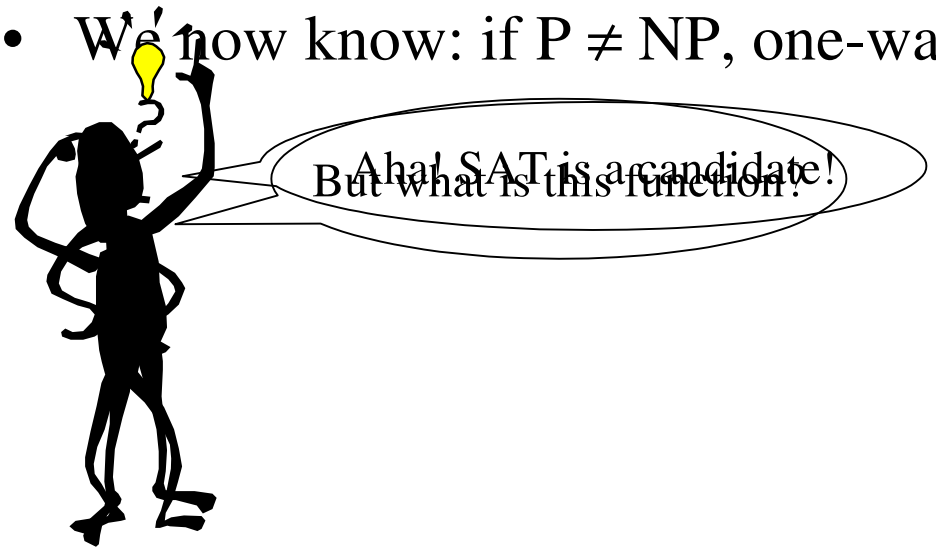
f is clearly one-to-one.

The rest of the proof goes exactly the same way as before.

The *only if* part changes: assume one-to-one one-way functions exist and f is such a function. L is in UP due to f's one-to-oneness.

First Theorem (Alternate Proof)

- We now know: if P ≠ NP, one-way functions exist.



The SAT function:

$dom(f_{sat}) = \{\langle f, x_1, \ldots, x_n \rangle\}$

f is a representation of an n-valued satisfiable boolean formula.

$\langle x_1, \ldots, x_n \rangle$ is a satisfying assignment of f.

$f_{sat}(\langle f, x_1, \ldots, x_n \rangle) = f$ for every $\langle f, x_1, \ldots, x_n \rangle$ in $dom(f_{sat})$

Unambiguous and Bounded Ambiguity one-way functions

- Since $P \subseteq UP \subseteq NP$, proving $P \neq UP$ is stronger than $P \neq NP$.
- In other words, $P \neq UP \Rightarrow P \neq NP$.
- However the converse is unknown:
  - In some relativized worlds, P=UP and UP≠NP.
  - While in others, P≠UP and UP=NP.
- Given the above, it is possible that one-way functions exist but no one-to-one one-way functions exist.
- However, it has been proven constant-to-one one-way functions exist if and only if one-to-one one-way functions exist.

Ambiguity Definitions

- A k-to-1 function is a function for which maps no more than k values to a single value.
- A function has bounded ambiguity if there is a k such that the function is k-to-1.
- A language is $\mathrm{UP}_{\leq k}$ for $k \geq 1$ if there is a NPTM that accepts the language and for all input there are at most k accepting paths

Theorem 2

- Unambiguous (one-to-one) one-way functions exist iff bounded-ambiguity (k-to-1) one-way functions exist.
- The only-if part is trivial because one-to-one one-way functions have bounded ambiguity.
- The if part is more difficult...

Theorem 2 (cont)

- Lemma 17: Given a NPTM N which has at most *k* accepting paths, the following language $B \in$ UP
  - B={x | N(x) has exactly k accepting paths}
  - Proof:
    - Guess k unique lexicographically ordered paths of N.
    - Check if all k paths are accepted by N.
    - If yes accept.
  - This will have at most one accepting path.

If Part

- Proof by induction of $P=UP \Rightarrow P=UP_{\leq k}$
  - Base case: $P=UP \Rightarrow P=UP_{\leq 1}$
    - Clearly holds
  - Induction step: $P=UP_{\leq k} \Rightarrow P=UP_{\leq k+1}$
    - Assume P=UP
    - Let N be an NPTM that accepts a $UP_{\leq k+1}$ member language
    - L.17: $B'=\{x \mid N(x)$ has exactly k+1 accepting paths$\} \in UP=P$

If Part (cont)

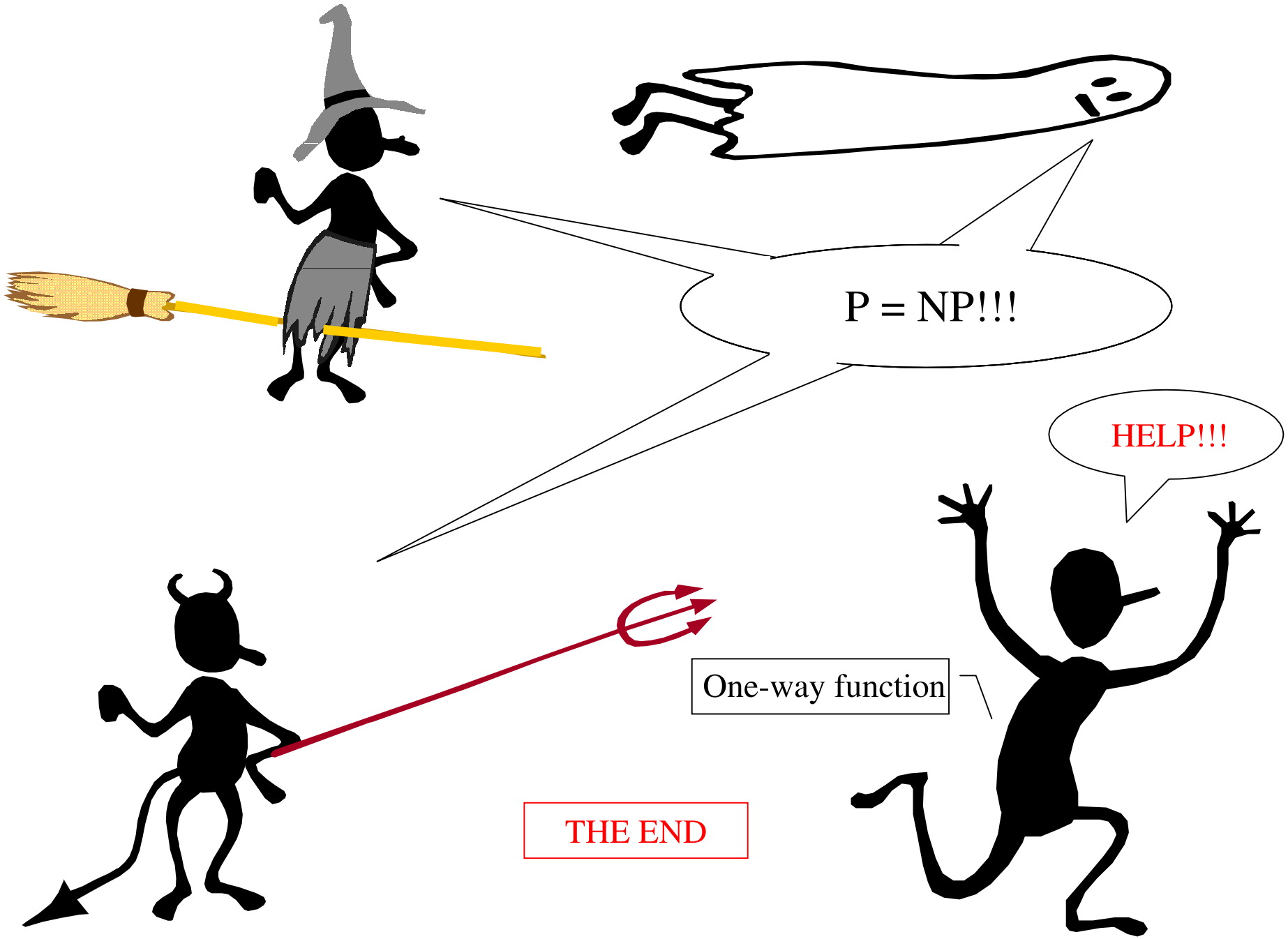
- Assume $D=\{x \mid x \notin B' \wedge x \in L(N)\}$
- $D \in UP_{\leq k}$
- By $P=UP_{\leq k}$: $D \in P$
- Since $L(N) = B' \cup D$ and P is closed under $\cup$
  - $L(N) \in P$
  - So, $P=UP_{\leq k+1}$

If Part (cont)

- We proved $P=UP \Leftrightarrow P=UP_{\leq k}$
- Also, it is easy to prove k-to-1 one-way functions exist iff $P \neq UP_{\leq k}$
- So, k-to-1 one way functions exist iff $P \neq UP$.
- By Thm.1 k-to-1 one way functions exist iff 1-to-1 one way functions exist.

Summary

- Proven
  - P≠NP ⇔ One-way functions exist.
  - P≠UP ⇔ One-to-one one-way functions exist.
  - 1-to-1 one-way functions exist iff
    k-to-1 one-way functions exist.
- The future:
  - Extremely powerful types of one-way functions exist iff the standard types exist.


P = NP!!!
HELP!!!
One-way function
THE END