# Weak Pigeonhole Principles, Circuits for Approximate Counting, and Bounded-Depth Proofs


Albert Atserias

Universitat Politècnica de Catalunya

Barcelona, Spain

# Proof complexity

Algorithms & complexity: P-algorithms

Proof complexity: NP-algorithms

**Main motivations:**

**1980s and 1990s**:

NP vs. co-NP (Cook-Reckhow, ...)

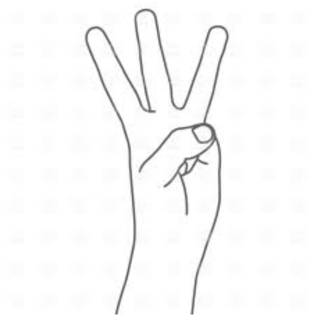
Foundations of mathematics (Paris-Wilkie,...)

**2000s and 2010s**:

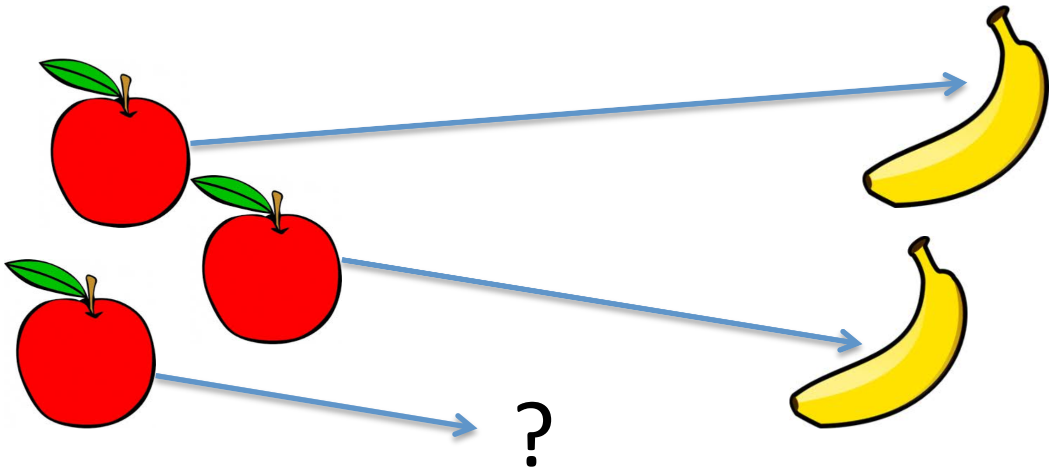
A theory of automated theorem proving (SAT)

Analysis of hard instances for specific algs

# Bijections



# Injections



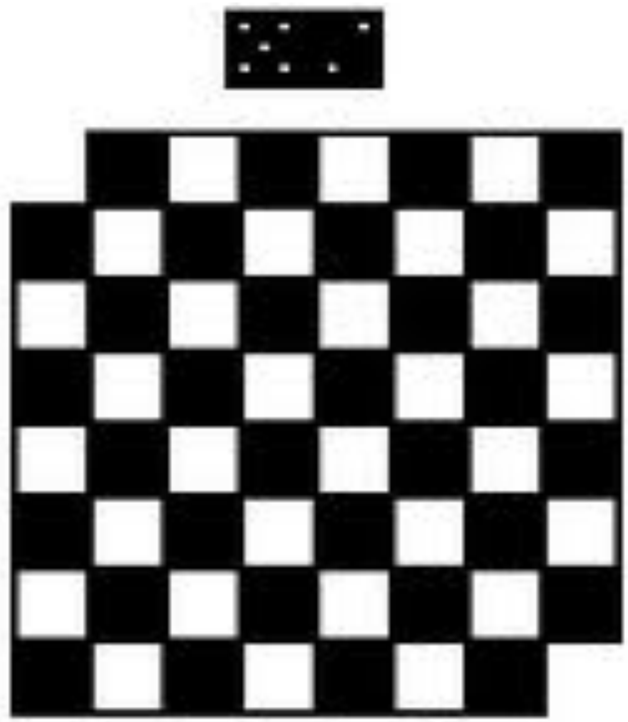

Pigeonhole Principle:

there is no injective map from {1,…,n+1} into {1,…,n}

# Pigeonhole Principle

1. **Often quite hidden**:

   e.g. mutilated chessboard puzzle



http://community.fortunecity.ws

# Pigeonhole Principle

**2. Often applied to (exponentially) large sets:**

e.g. every x with $(x,q) = 1$ has an "order mod q"

(a smallest k such that $x^k = 1 \bmod q$)

1. List $x^1, x^2, x^3, \ldots, x^q \bmod q$. All in $\{1,\ldots,q-1\}$.
2. By PHP, there are $i < j$ s.t. $x^j = x^i \bmod q$.
3. Then $x^{j-i} = 1 \bmod q$.
4. Let k be smallest s.t. $x^k = 1 \bmod q$.

# Pigeonhole Principle

**3. Entails the induction principle:**

e.g. P(0) & (P(x) => P(x+1) for all x < n) => P(n).

1. Assume P(0) & (P(x) => P(x+1) for all x < n).
2. But assume also !P(n).
3. Define the map

| | |
|---|---|
| F(x) = x | when P(x) holds |
| F(x) = x-1 | when P(x) fails |

4. Check F maps {0,…,n} injectively in {0,…,n-1}.

# Questions about PHP

**1. For automated theorem proving:**

Is it available in automatic proof search?

**2. For computational complexity:**

Is the expressive power of counting necessary?

Or does "flat" AND/OR/NOT language suffice?

**3. For mathematical logic:**

How does PHP compare to induction principle?

# Weak PHPs

Weak Pigeonhole Principle:

there is no injective mapping from $\{1,\ldots,2n\}$ into $\{1,\ldots,n\}$

Even Weaker Pigeonhole Principle:

there is no injective mapping from $\{1,\ldots,n^2\}$ into $\{1,\ldots,n\}$

# Remarks about WPHPs

**1. WPHP rather than PHP is often enough:**

Ex 1: every non-zero x has an order mod p

Ex2: existence proofs by probabilistic method

**2. Exact counting looks no longer necessary:**

approximate counting seems enough

**3. Relationship with induction principle:**

Question: How fundamental is WPHP as an axiom?

# Elementary Reasoning: Take 0

**Weak theories of arithmetic:**

- Basic Peano axioms for +, $\cdot$, < (maybe #, exp, …)
- Induction for predicates in (complexity) class C

**Examples:**

- $I\Delta_0$ (induction for linear hierarchy LINH)
- $I\Delta_0$ + # (induction for poly hierarchy PH)
- $I\Delta_0$ + exp (induction for elementary hierarchy)

# Paris-Wilkie(-Woods) Program

**Develop a notion of *feasibly* elementary proof:**

- Infinitude of primes (Euclid)? [Macintyre]
- Bertrand's postulate (Erdös)?
- Quadratic residuocity (Gauss)?

**Exam**

- $I\Delta_0$ -
- $I\Delta_0$ -
- $I\Delta_0$

**Main remaining question about WPHP**:
Does $I\Delta_0$ prove WPHP?

**A different deep open question**:
Is $I\Delta_0$ finitely axiomatizable?

# Elementary Reasoning: Take 1

**Propositional proof complexity:**

- Express the principle in propositional logic
- Study the length of its proofs in standard p.s.

**Examples:**

- Resolution
- Hilbert-style proof systems (a.k.a. Frege)
- Cutting planes, Lovász-Schrijver, SOS
- Etc.

# ABOUT PHP(n+1,n)

# Propositional Encoding of PHP

**Pigeonhole Principle PHP(m,n) with m > n**:

Variables:

$P_{i,j}$ for $1 \le i \le m$, $1 \le j \le n$.

Clauses:

$P_{i,1} \vee \ldots \vee P_{i,n}$ for $1 \le i \le m$

$!P_{i,k} \vee !P_{j,k}$ for $1 \le i < j \le m$, $1 \le k \le n$.

# Propositional Encoding of IND

**Induction Principle IND(n)**:

Variables:

$P_i$ for $0 \leq i \leq n$.

Clauses:

$P_0$

$!P_i \vee P_{i+1}$ for $0 \leq i \leq n-1$.

$!P_n$

# Elementary Reasoning: Resolution

**Resolution**:

$$\frac{a_1 \vee \ldots \vee a_r \vee x \qquad b_1 \vee \ldots \vee b_s \vee\, !x}{a_1 \vee \ldots \vee a_r \vee b_1 \vee \ldots \vee b_s}$$

**Goal**:

starting at given clauses,
produce the empty clause

# Proof of Induction Principle

| | | |
|---|---|---|
| 1. | $P_0$ | (given clause) |
| 2. | $!P_0 \vee P_1$ | (given clause) |
| 3. | $P_1$ | (resolve 1 and 2) |
| 4. | $!P_1 \vee P_2$ | (given clause) |
| 5. | $P_2$ | (resolve 3 and 4) |
| … | … | … |
| 2n+1. | $P_n$ | (resolve 2n-1 and 2n) |
| 2n+2. | $!P_n$ | (given clause) |
| 2n+3. | 0 | (resolve 2n+1 and 2n+2) |

# Lower Bound for PHP(n+1,n)

**Theorem [Haken 1986]**

Every resolution proof of PHP(n+1,n) requires $\exp(\Omega(n))$ clauses.

**Bottom line:**

PHP is stronger than IND,
at least in the resolution setting.

# Elementary Reasoning: Frege

**Hilbert style proof system (a.k.a. Frege):**

```
------------------ (Ax)
      A v !A
```

```
            A
------------------ (Wk)
         A v B
```

```
A v C         B v D
------------------- (IC)
A v B v (C & D)
```

```
A v C         B v !C
------------------- (Cut)
         A v B
```

# Complexity of Counting

**Theorem [Wallace 1964]:**

There exist formulas $TH_k(x_1,\dots,x_n)$ of $n^{O(1)}$-size and $O(\log n)$-depth expressing "$x_1+\cdots+x_n > k$".

**Theorem [Ajtai 1983, FSS 1983, Håstad 1986]:**

Depth-d formulas for $TH_{n/2}(x_1,\dots,x_n)$ must have size $\exp(n^{1/O(d)})$.

# Upper bound for PHP(n+1,n)

**Theorem [Buss 1986]:**

PHP(n+1,n) has Frege proofs of size $n^{O(1)}$

with depth-O(log n) formulas.

Proof idea:

1. PHP(n+1, n) => $TH_n(P_{1,1},\ldots,P_{n+1,n})$ (& has small proofs)
2. PHP(n+1, n) => $!TH_n(P_{1,1},\ldots,P_{n+1,n})$ (& has small proofs)
3. Cut to derive 0.

# Tightness of upper bound

**Jewel Theorem of PPC [Ajtai 1988, PBI, KPW]:**

Frege proofs of PHP(n+1,n)

using depth-d formulas

must have size $\exp(\Omega(n^{1/\exp(d)}))$.

**Corollary:**

$I\Delta_0$ + # does not prove PHP

# ON THE WPHP FRONT

# Upper Bound for PHP(2n, n)

**Theorem [Paris-Wilkie-Woods 1988, MPW 2001]:**

PHP(2n, n) has Frege proofs with $(\log n)^{O(1)}$-DNFs of size $\exp((\log n)^{O(1)})$

.

Proof idea:

1: given an alleged injective [2n] -> [n].
2: copy and compose [4n] -> [2n] -> [n].
… …
After log n steps: [$n^2$] -> … -> [2n] -> [n].

Proof idea:

1’: given an alleged injective $[n^2]$ -> $[n]$.
2’: copy and compose $[n^4]$ -> $[n^2]$ -> $[n]$
… …
After log(n)/loglog(n) steps: $[2^n]_{def}$ -> $[n]$.

But:

Definable injective $[2^n]_{def}$ -> $[n]$ does not exist
(by Cantor’s argument)

Iterated composition is definable in depth-2:

$$F(F(F(F(a)))) = b$$
iff
$$\bigvee_{c,\,d,\,e} (F(a) = c \;\&\; F(c) = d \;\&\; F(d) = e \;\&\; F(e) = b)$$

# Better Upper Bound?

**Fact [Stockmeyer 1983, Ajtai 1993]:**

There are depth-O(1) size-$n^{O(1)}$ circuits $C(x_1,\ldots,x_n)$ that on input $x_1,\ldots,x_n$ output w in $\{0,\ldots,n\}$ s.t.

$$0.999 < (x_1+\ldots+x_n)/w < 1.001$$

Proof idea: (a probabilistic algorithm)

1. for k=1,…,n,
2. take a few ran n} of size n/k.
3. output larges ve a j with $x_j = 1$.

Remove randomness!

# Better Upper Bound?

**Question:**

Does PHP(2n, n) have Frege proofs of size $n^{O(1)}$ using depth-O(1) formulas?

Failed

1. PHP

2. PHP

3. $C(p_{1,1},\ldots,p_{2n,n})_{1.01n} = 0 \Rightarrow C(p_{1,1},\ldots,p_{2n,n})_{1.99n} = 0.$

4. Cut to derive 0.

Problem is:

Steps 1, 2 and 3 need $n^{O(1)}$-size depth-O(1) proofs!

# Lower Bounds for PHP(2n, n)

**The question remains**:

Does jewel theorem extend to PHP(2n, n)?

If yes then $I\Delta_0$ does not prove WPHP

**Theorem [BT1986, ABE2001, SBI2002, R2003]:**

1. Resolution needs size $\exp(\Omega(n))$.
2. Frege with 2-DNFs needs size $\exp(n^{\Omega(1)})$.
3. Frege with $(\log n)^{0.49}$-DNFs needs size $\exp(n^{\Omega(1)})$.
4. Frege with $(\log n)^{0.99}$-DNFs needs size $\exp(n^{\Omega(1)})$.

# RECENT PROGRESS

# Relativized WPHP

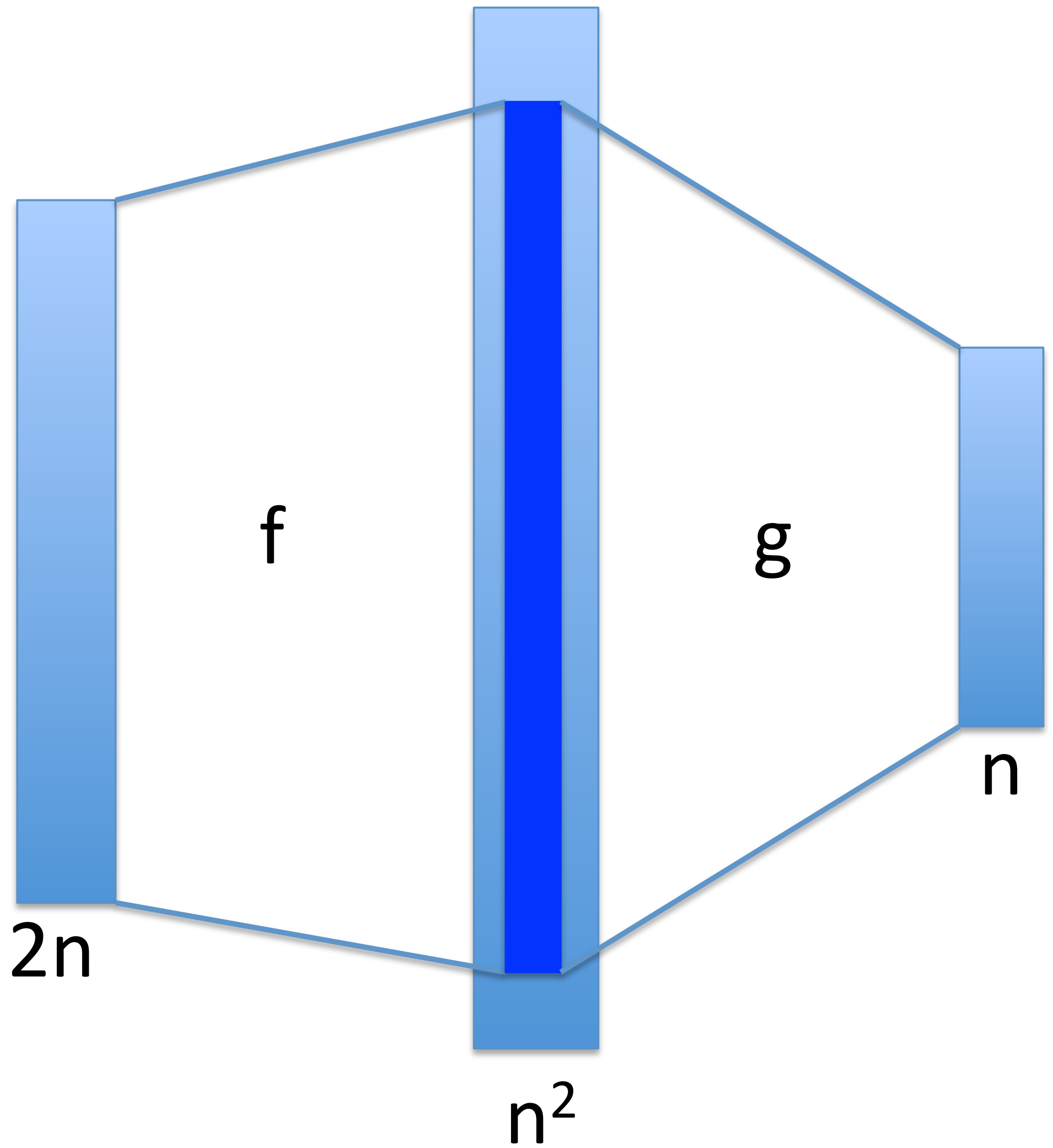
## Relativized Weak Pigeonhole Principle:

if 2n out of $n^2$ pigeons fly into n holes,
then some hole is doubly occupied

## Mapping formulation:

if f maps [2n] into [$n^2$] and
g maps [$n^2$] into [n]
then either f is not injective
or g is not injective on the range of f.

# Mapping view of RPHP(2n, $n^2$, n)



# Propositional Encoding

**RPHP(2n, $n^2$, n)**:

Variables:

$P_{i,j}$ for $1 \le i \le 2n$, $1 \le j \le n^2$.

$R_i$ for $1 \le i \le n^2$.

$Q_{i,j}$ for $1 \le i \le n^2$, $1 \le j \le n$.

Clauses:

$P_{i,1}$ v … v $P_{i,n2}$

$!P_{i,k}$ v $!P_{j,k}$

$!P_{i,j}$ v $R_j$

$!R_i$ v $Qi_{,1}$ v … v $Q_{i,n}$

$!R_i$ v $!R_j$ v $!Q_{i,k}$ v $!Q_{j,k}$

# Remarks about RWPHP

**1. Technical but still natural:**

Example:

Want WPHP on quadratic residues mod n.

But q.r. mod n are not well-characterized.

**2. Approximate counting still looks enough:**

> 1.99 n pigeon-flights

vs.

< 1.01 n pigeon-landings.

# Lower/Upper Bounds for RWPHP

**Theorem [AMO 2013]**

Frege proofs of PHP(2n, $n^2$, n) with DNFs require size $\exp((\log n)^{1.49})$

**Theorem [AMO 2013]**

PHP(2n, $n^2$, n) has Frege proofs with DNFs of size $\exp((\log n)^{O(1)})$.

# Remarks on these Results

**1.** First lower bound for DNF-Frege that does not proceed by reduction to Jewel Theorem of PPC.

**2.** Goes beyond $(\log n)^{0.99}$-DNF-Frege by methods that looked exhausted!

**3.** A quasipolynomial lower bound where quasipolynomial upper bounds exist.

**4.** Upper bound proceeds by showing that WPHP and RWPHP are actually equivalent up to +- 1 depth.

# Upper Bound Proof

Reduction to PHP(2n, n):

If f : [2n] -> [$n^2$] is injective and

g : [$n^2$] -> [n] is injective on Rng(f),

then (f o g) : [2n] -> [n] is injective.

Composition is definable both as 2-DNF and 2-CNF:

$$g(f(a)) = b \quad \text{iff} \quad \begin{array}{l} \bigvee_c (f(a) = c \,\&\, g(c) = b) \\ \bigwedge_c (!f(a) = c \,\&\, g(c) = b) \end{array}$$