Propositional Proof Complexity of Paris-Harrington Tautologies

Massimo Lauria
(joint work with Lorenzo Carlucci and Nicola Galesi)

Math Institute
Czech Academy of Science, Prague

Bertinoro, RaTLoCC 2011

A computational question:

Q: how hard is it to prove a **propositional** theorem?

$=$

Q: how hard is it to show that a CNF is unsatisfiable?

A computational question:

Q: how hard is it to prove a **propositional** theorem?

$=$

Q: how hard is it to show that a CNF is unsatisfiable?

Clote [Clo95] proposes:

Maybe combinatorial independence from some strong arithmetic theory leads to hard propositional tautologies.

This approach has some limits...

- Functions which grow too fast may cause **LARGE** formulas with trivial proof complexity.
  E.g., a formula on N variable and $2^{\frac{N}{100}}$ clauses.
- Useless in the context of Bounded Arithmetic.
- Large gaps between **UPPER and LOWER BOUNDS** makes difficult to properly evaluate what is efficient.

This approach has some limits...

- Functions which grow too fast may cause **LARGE** formulas with trivial proof complexity.
  E.g., a formula on N variable and $2^{\frac{N}{100}}$ clauses.
- Useless in the context of Bounded Arithmetic.
- Large gaps between **UPPER and LOWER BOUNDS** makes difficult to properly evaluate what is efficient.

In this talk...

We do not shy away... instead we focus on a **sufficiently weak** version of the Paris-Harrington numbers. The choice allows non-trivial results.

Proof system as a verification process (refutational style)

A deterministic polynomial time machine $V(\cdot, \cdot)$

- $\psi \in$ UNSAT $\quad$ $V(\psi, \pi)$ accept for some proof π
- $\psi \notin$ UNSAT $\quad$ $V(\psi, \pi)$ reject for any string π

If $V(\psi, \pi)$ accepts then π is a “refutation” of ψ.

Central question of Proof Complexity

Is there a proof system such that the shortest refutation for an unsatisfiable ψ has size $\mathrm{poly}(|\psi|)$?

Central question of Proof Complexity

There is a proof system such that the shortest refutation for an unsatisfiable ψ has size $\mathrm{poly}(|\psi|)$

$$\Longleftrightarrow$$

$$\mathsf{NP} = \mathsf{coNP}$$

Too difficult, the community focuses on simple proof systems.

We study the **length** of refutations $\psi \vdash \square$ in...

- RES: proof lines are clauses

$$\frac{A \vee x \quad \neg x \vee B}{A \vee B}$$ Cut on literals

- RES (2): proof lines are 2-DNFs

$$\frac{A \vee xy \quad \neg x \vee \neg y \vee B}{A \vee B}$$ Cut on 2-terms.

- BD-FREGE: sequent calculus on bounded depth formulas.

Paris-Harrington Numbers

If a graph is big enough, at least one of a specific set of sub-configurations must be present.

—Ramsey type statements —

Paris-Harrington for graphs

There exists a minimum number $R(k;m)$ such that any graph on the integers $[k, R(k;m)]$ contains

- either a clique of size m,
- or a "large" stable set S (i.e., $|S| = \min S$).

Paris-Harrington formulas

- Vertices $V = \{k, \ldots, N\}$,
- Variables E_{ij} for $\{i,j\} \in \binom{V}{2}$

$$\neg\mathsf{Cli}(X) = \bigvee_{\{i,j\}\in\binom{X}{2}} \neg E_{ij} \qquad \neg\mathsf{Ind}(X) = \bigvee_{\{i,j\}\in\binom{X}{2}} E_{ij}$$

$$\mathsf{PH}(N;k,m) := \left(\bigwedge_{X\subseteq V,|X|=m} \neg\mathsf{Cli}(X)\right) \wedge \left(\bigwedge_{X\subseteq V,|X|=\min X} \neg\mathsf{Ind}(X)\right)$$

"$N \geq R(k;m)$" if and only if $\mathsf{PH}(N;k,m)$ is unsatisfiable.

About Paris-Harrington Numbers

Mills [Mil85] gives a β such that for big enough k and $m \geq 3$

$$R(k;m) \leq k^{2^{\beta m}}$$

We are going to study the proof complexity of $\mathrm{PH}(k^{2^{\beta m}};k,m)$

Previous results

(about Ramsey tautologies for graphs)

Ramsey formulas

RAM$(N;a,b)$: (negation of) Ramsey theorem for graph

"There is a graph of N vertices with no a-cliques and no b-stables"

$$\text{RAM}(N;a,b) := \left(\bigwedge_{X\subseteq\{1\ldots N\},|X|=a} \neg\text{Cli}(X)\right) \wedge \left(\bigwedge_{X\subseteq\{1\ldots N\},|X|=b} \neg\text{Ind}(X)\right)$$

[Pud91] RAM$(4^k;k,k)$ is easy in BD-Frege.

[Kra01] PHP$_n^{n^4}$ hard for RES(2) implies RAM$(4^k;k,k)$ hard for RES.

[Kra11] RAM$(r(k,k);k,k)$ his hard for BD-Frege.

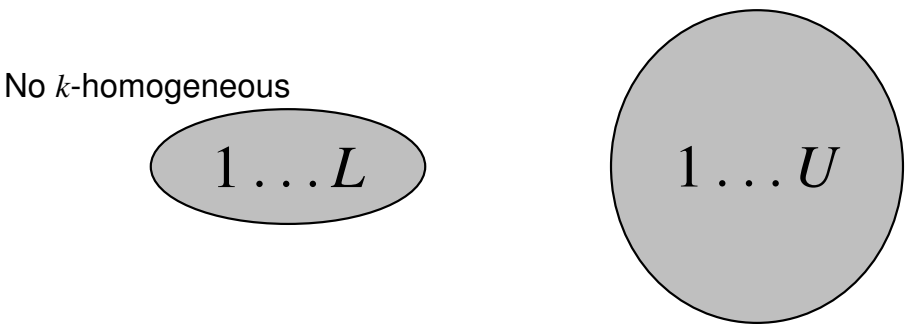
Lower bounds by Krajíček (I): reduction from PHP

PHP_n^m: (negation of) Pigeonhole principle for $m > n$

"There exist an injective mapping from m to n"

Let $r(k,k)$ the critical Ramsey value and $L < r(k,k) \leq U$.

- Fix a satisfying assignment for $\text{RAM}(L; k, k)$.



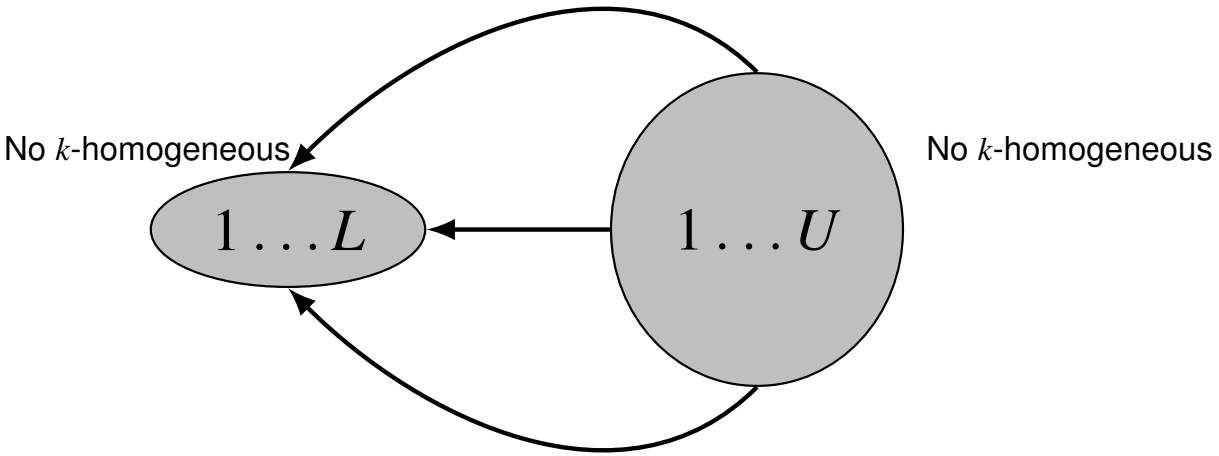
Lower bounds by Krajíček (I): reduction from PHP

PHP_n^m: (negation of) Pigeonhole principle for $m > n$

"There exist an injective mapping from m to n"

Let $r(k,k)$ the critical Ramsey value and $L < r(k,k) \leq U$.

- Fix a satisfying assignment for $\text{RAM}(L;k,k)$.
- An injection from U to L allows to satisfy $\text{RAM}(U;k,k)$.



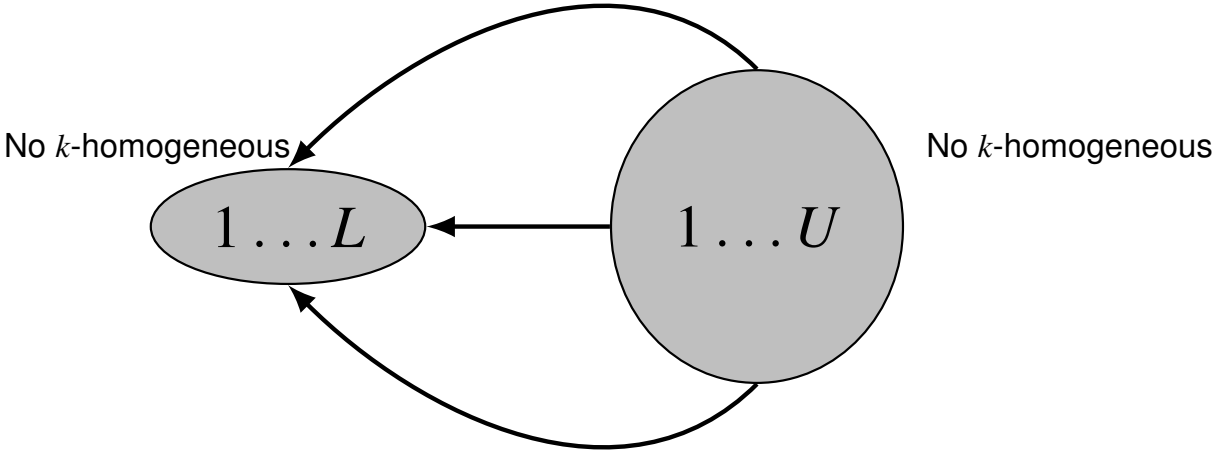
Lower bounds by Krajíček (I): reduction from PHP

PHP_n^m: (negation of) Pigeonhole principle for $m > n$

"There exist an injective mapping from m to n"

Let $r(k,k)$ the critical Ramsey value and $L < r(k,k) \leq U$.

- Fix a satisfying assignment for $\text{RAM}(L;k,k)$.
- An injection from U to L allows to satisfy $\text{RAM}(U;k,k)$.
- Refuting $\text{RAM}(U;k,k)$ allows to exclude such injections.



Lower bounds by Krajíček (II)

Theorem 1 ([Kra11])

$\textsc{Ram}(r(k,k);k,k)$ *is hard for BD-Frege*

Proof.

Fix $n = r(k,k) - 1$. $\textsc{Php}_n^{n+1}$ is hard for BD-Frege. □

Theorem 2 ([Kra01])

If $\textsc{Php}_n^{n^4}$ *is hard for* $\textsc{Res}(2)$ *then* $\textsc{Ram}(4^k;k,k)$ *is hard for* $\textsc{Res}$.

Proof.

It is known that $2^{k/2} < r(k,k) \leq 4^k$. Fix $n = 2^{k/2}$. □

Upper bound by Pudlák (I)

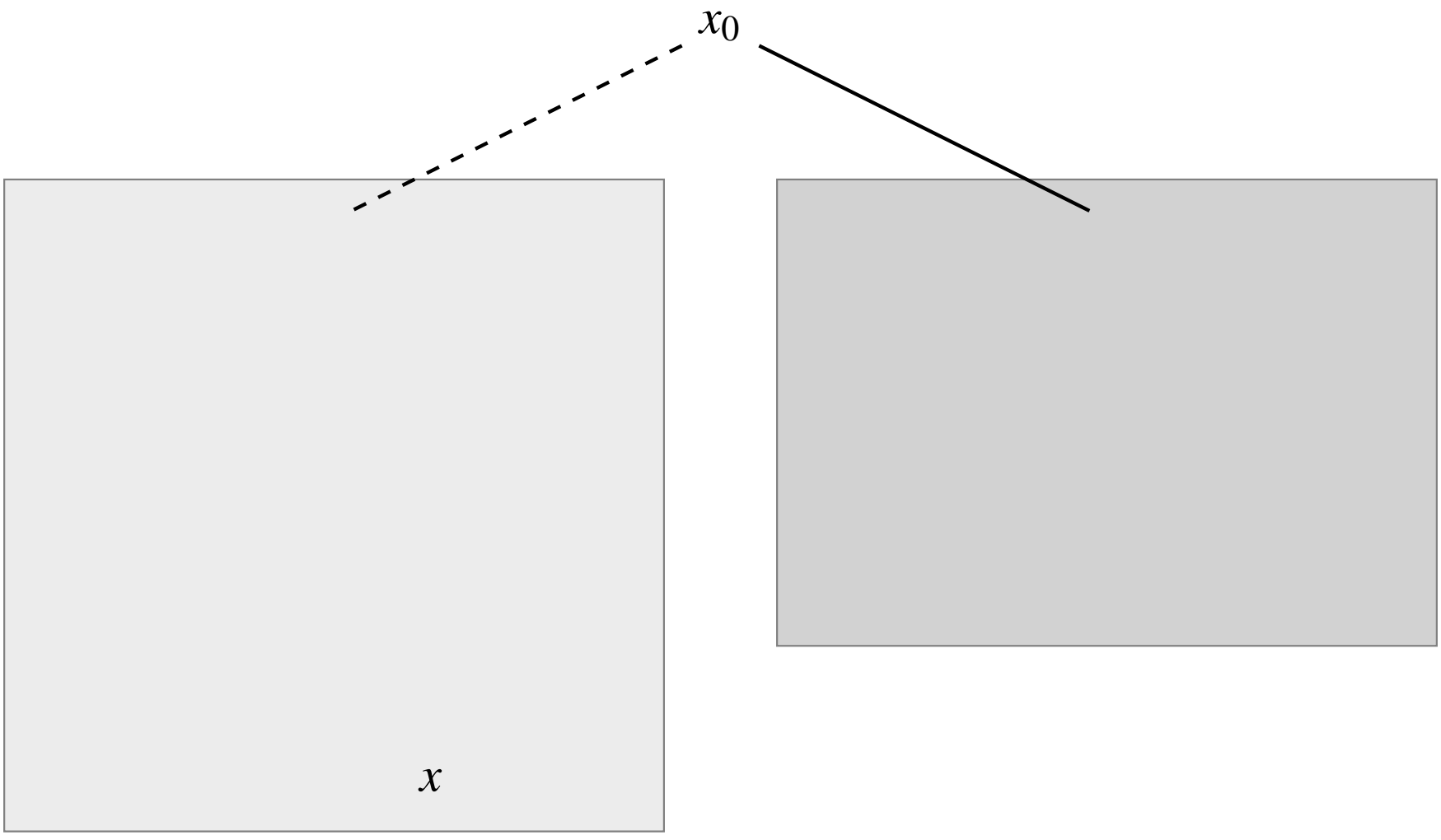
Upper bounds for Ramsey numbers $r(a, b)$ can be proved by defining the following search procedure where each vertex is reachable in a unique way.

Upper bound by Pudlák (II)

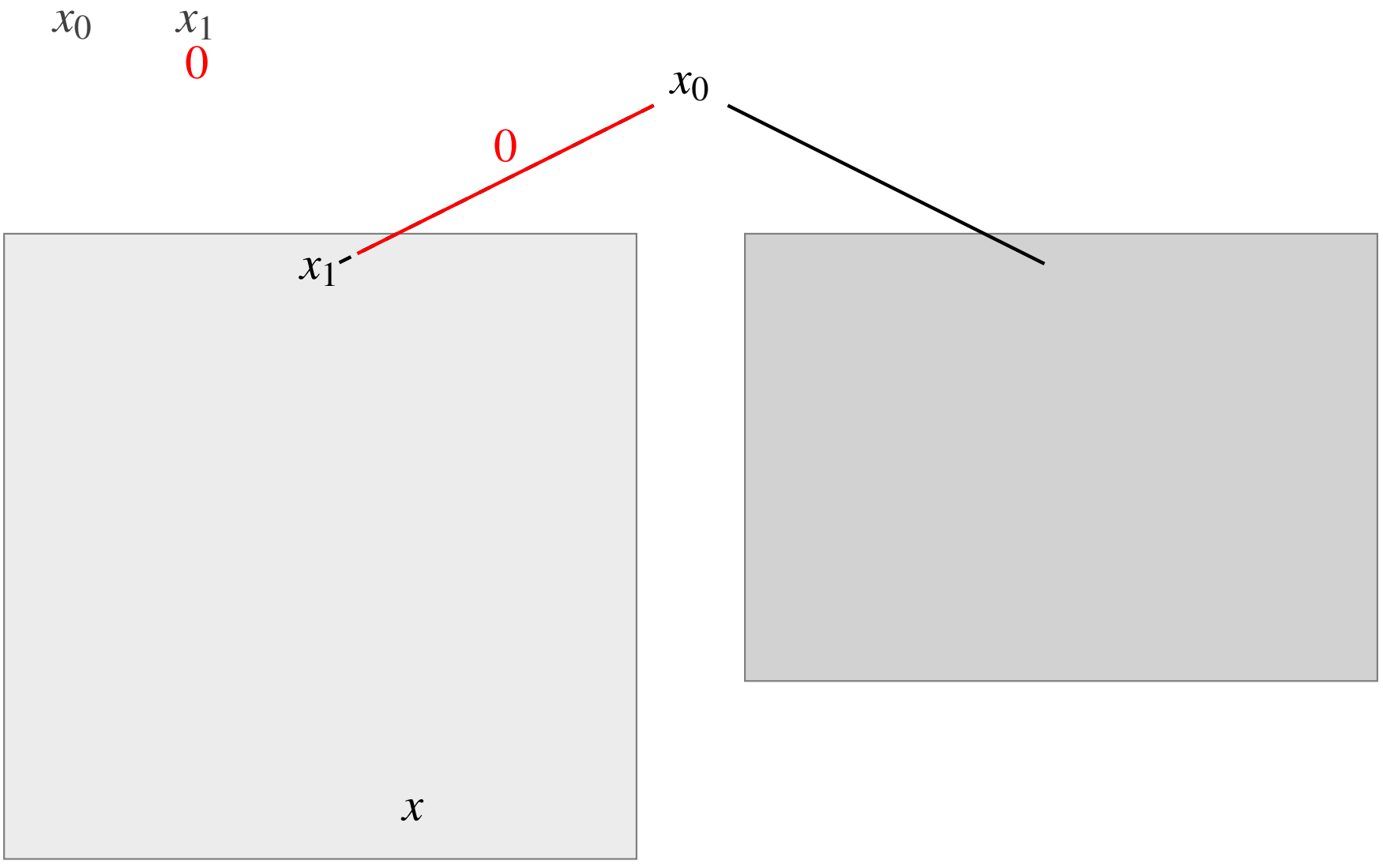
x_0

x

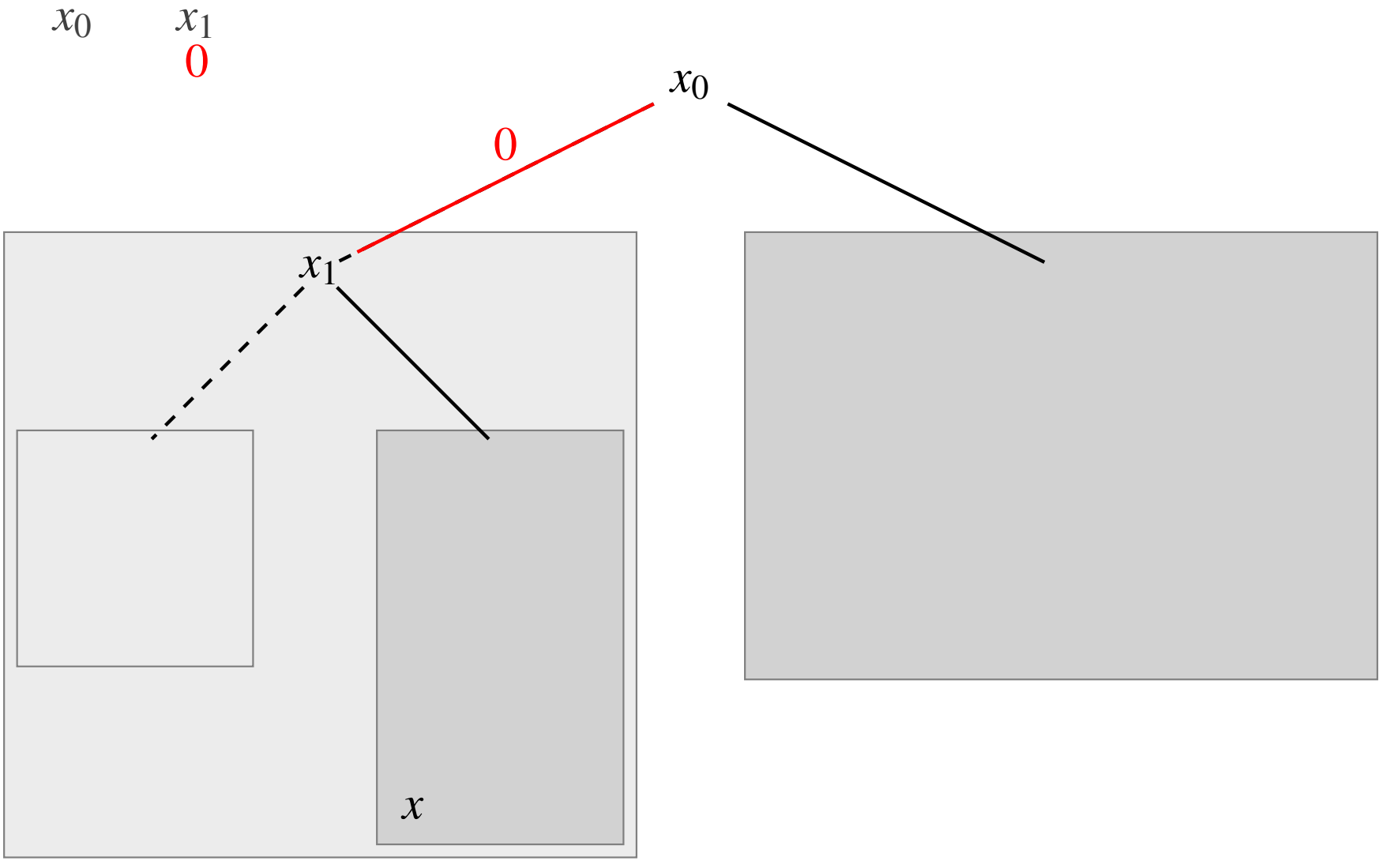
Upper bound by Pudlák (II)



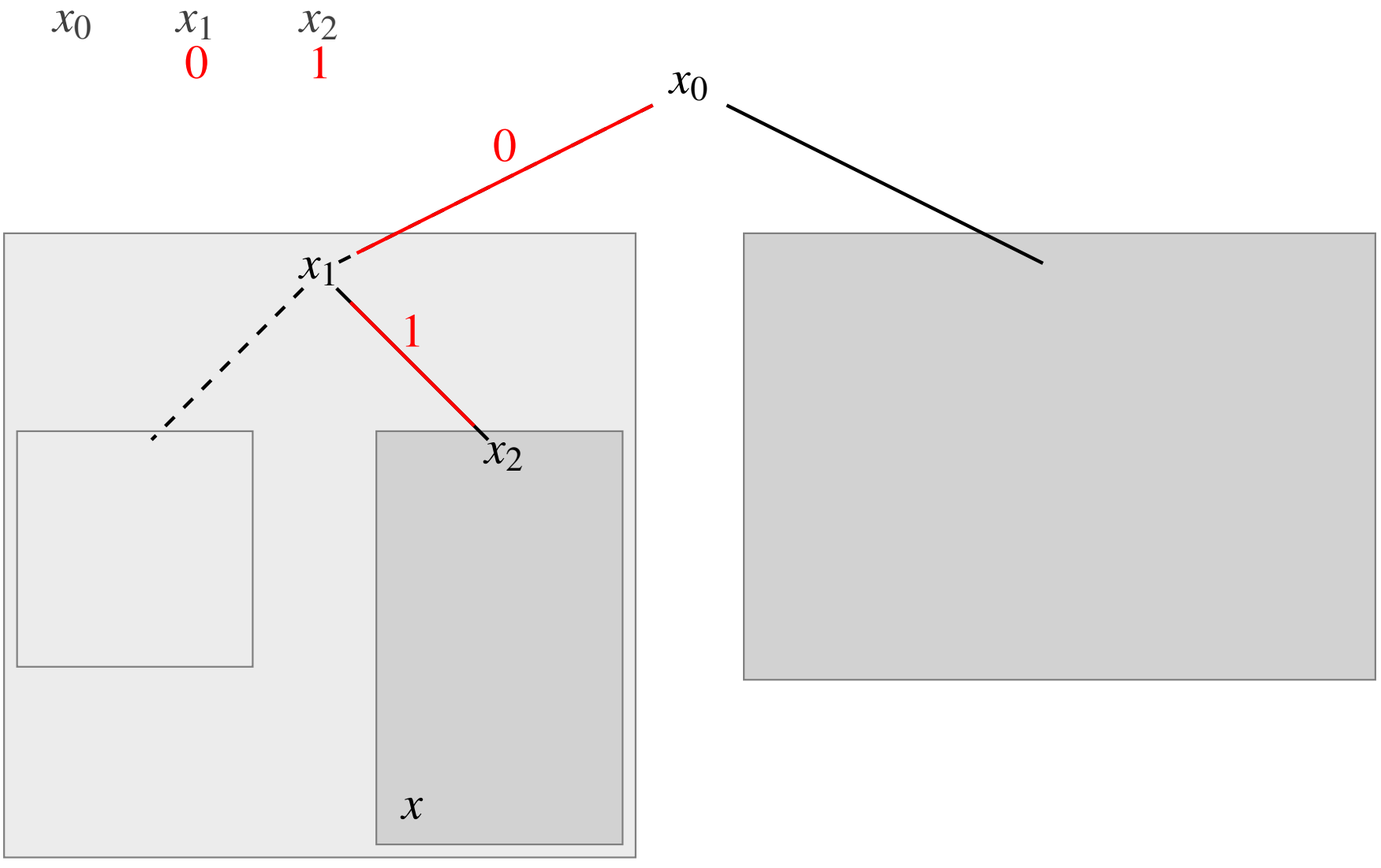
Upper bound by Pudlák (II)



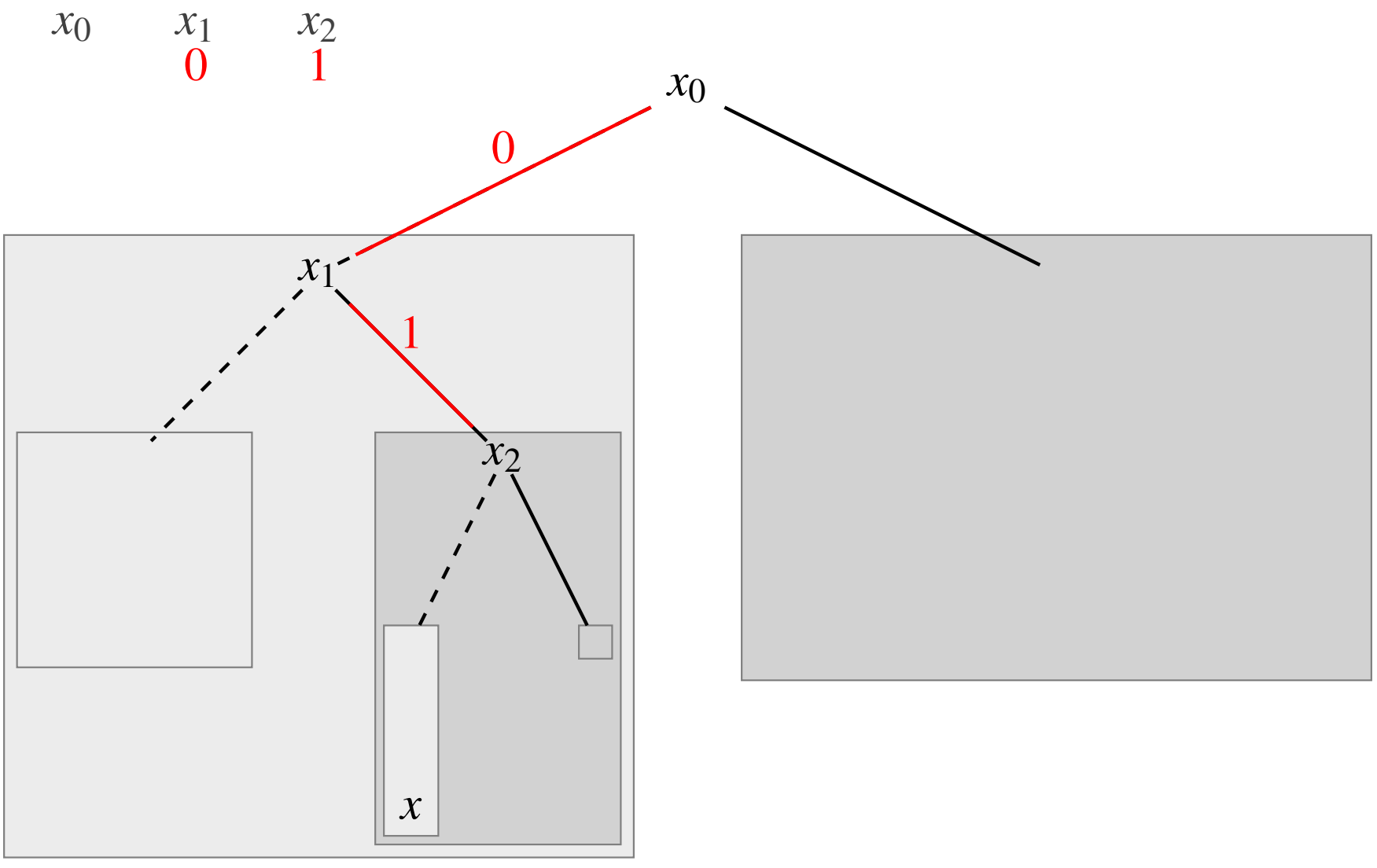
Upper bound by Pudlák (II)



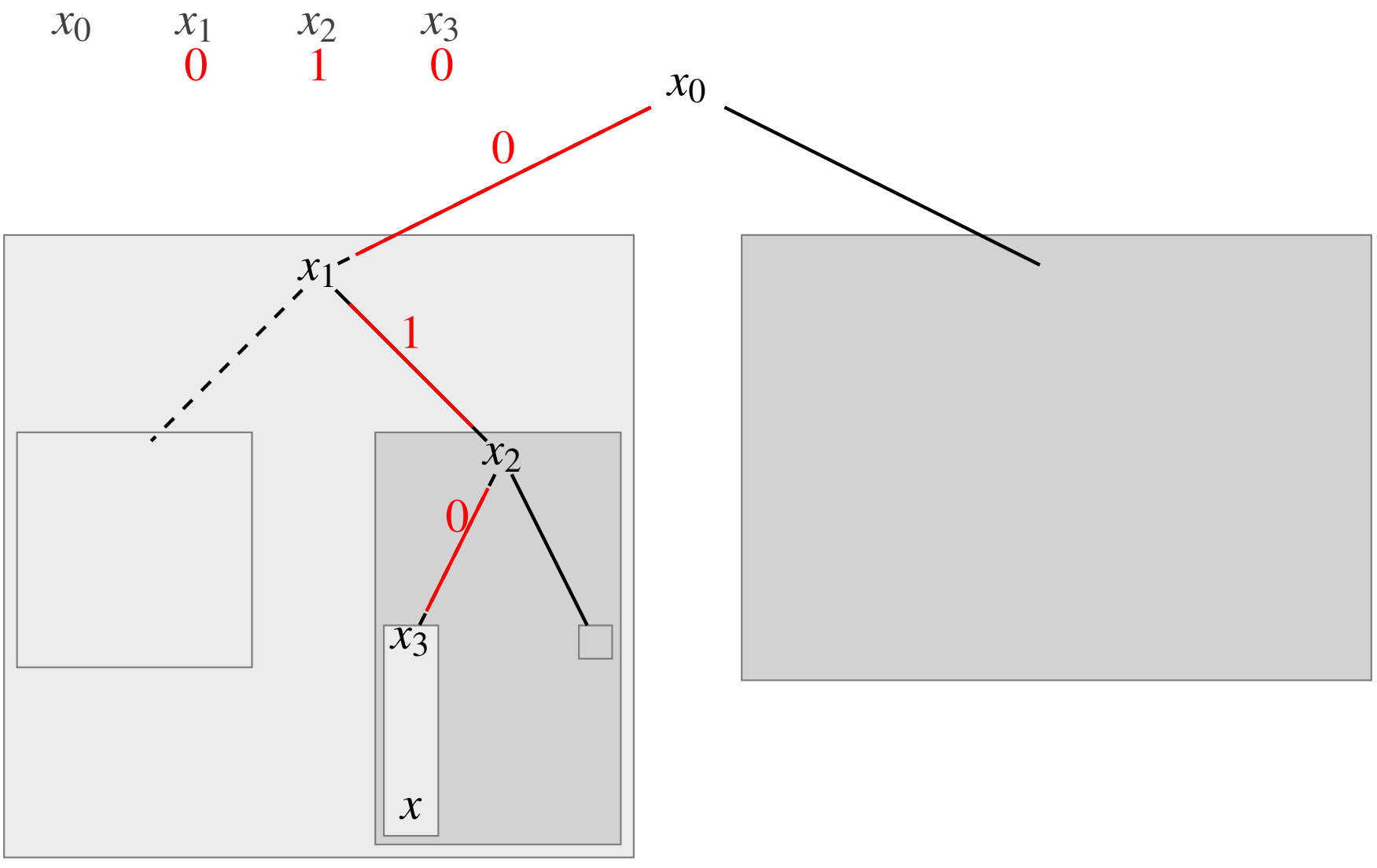
Upper bound by Pudlák (II)



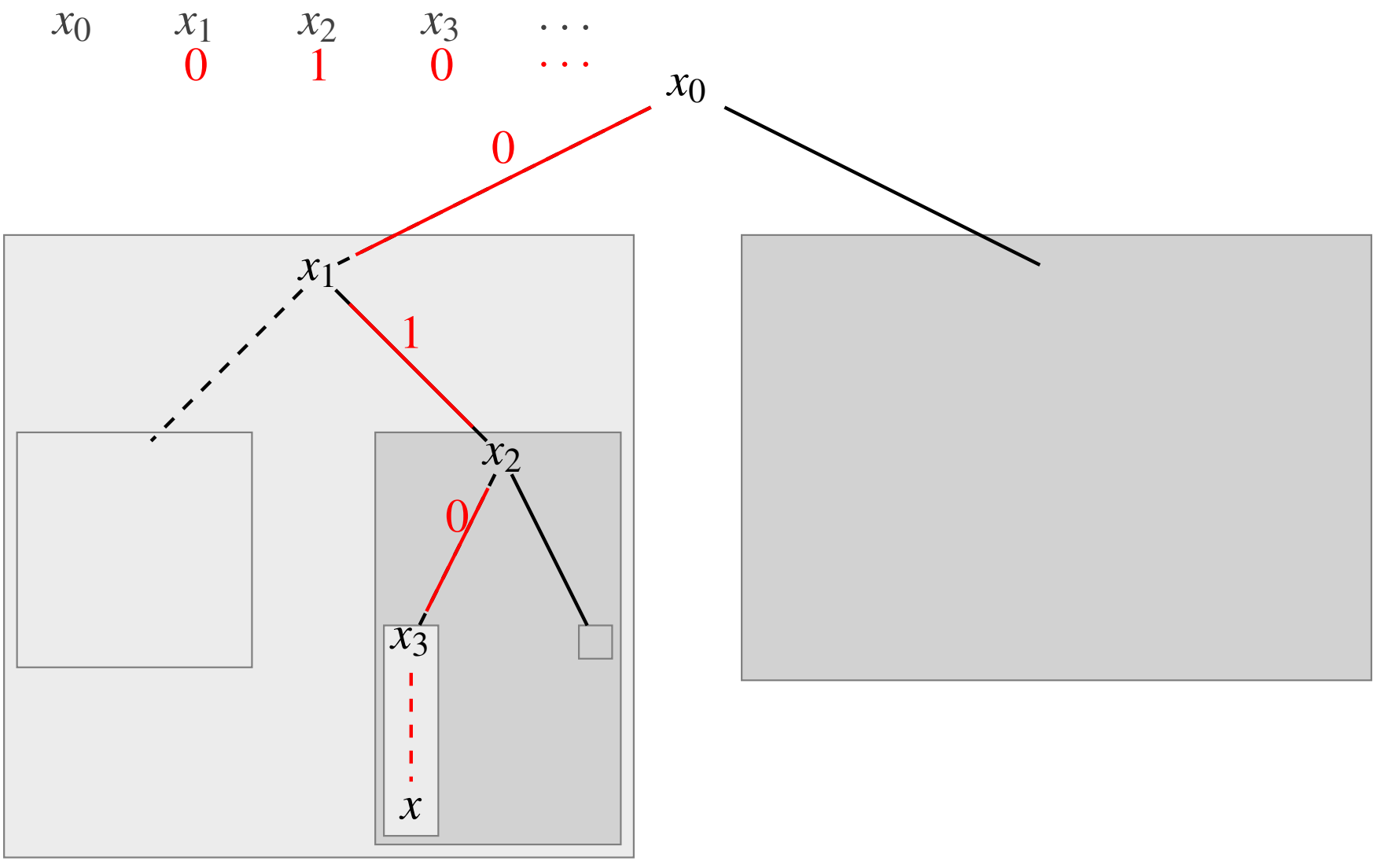
Upper bound by Pudlák (II)



Upper bound by Pudlák (II)



Upper bound by Pudlák (II)



Upper bound for BD-Frege (III): reduction to PHP

There is a known injective mapping that associate vertices of a graph to 0–1 strings in such a way that:

- $k-1$ zeros imply a stable sets of size k;
- $k-1$ ones imply a clique of size k.
- No k-homogeneous sets $\longrightarrow$ **FEW** possible strings.

Upper bound for BD-Frege (III): reduction to PHP

There is a known injective mapping that associate vertices of a graph to 0–1 strings in such a way that:

- $k-1$ zeros imply a stable sets of size k;
- $k-1$ ones imply a clique of size k.
- No k-homogeneous sets $\longrightarrow$ **FEW** possible strings.

If vertices there are **twice** the number of possible strings then BD-Frege can prove a contradiction efficiently.

Proof.

PHP_n^{2n} has short proof in BD-Frege. □

New results

(on PH tautologies)

New result

Carlucci, Galesi, L. (2011)

There are α and β as in [EM81, Mil85] such that, for

$$L = k^{2^{\alpha m}} < R(k,m) \leq N = k^{2^{\beta m}}$$

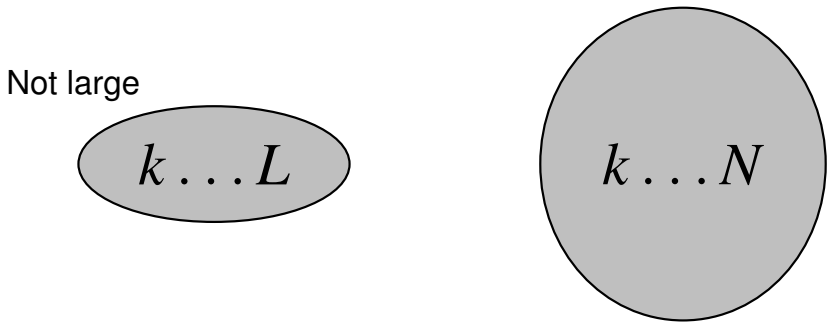
- $\textsc{Ph}(N;k,m)$ has a BD-Frege refutation of size $2^{\Theta(N \log\log N)}$
- If $\textsc{Res}(2)$ complexity of $\textsc{Php}_L^{N-o(N)}$ is $2^{\Omega(L^{1/2+\epsilon})}$ then $\textsc{Ph}(N;k,m)$ requires $\textsc{Res}$ refutation of size $2^{\Omega(L^{1/2+\epsilon})}$

Lower bound

...conditional

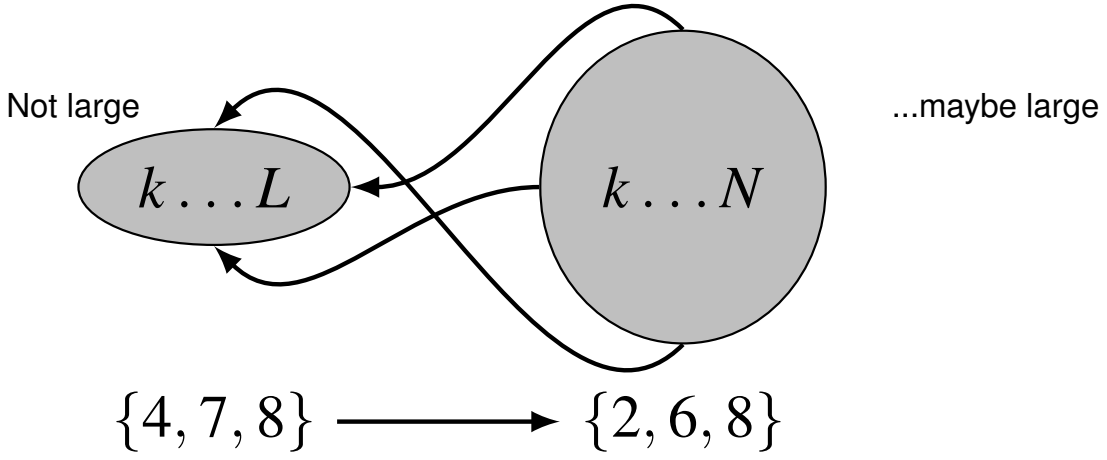
Lower bound: first attempt

Let us reduce from pigeonhole principle, as in Ramsey formulas lower bounds. For $L < R(k, m) \leq N$



Lower bound: first attempt

Let us reduce from pigeonhole principle, as in Ramsey formulas lower bounds. For $L < R(k, m) \leq N$



We need to force the mapping to be non-decreasing, but such a "non-decreasing pigeonhole principle" has short RES refutations.

Lower bound: reduction from off-diagonal Ramsey [EM81]

$$[k, N] = \overbrace{[n_0, n_1 - 1] \cup [n_1, n_2 - 1] \ldots [n_{\frac{m}{2}-3}, n_{\frac{m}{2}-2} - 1] \cup [M, N]}^{\frac{m}{2}-1 \text{ intervals}}$$

Where

- $n_0 := k$ and
- $n_{i+1} := r(3, n_i) + n_i - 1$.
- $M := n_{m/2-2}$.

Lower bound: reduction from off-diagonal Ramsey [EM81]

$$[k, N] = \overbrace{[n_0, n_1 - 1] \cup [n_1, n_2 - 1] \ldots [n_{\frac{m}{2}-3}, n_{\frac{m}{2}-2} - 1] \cup [M, N]}^{\frac{m}{2}-1 \text{ intervals}}$$

- Edges between intervals are all present.
- Fix subgraph $[n_i, n_{i+1} - 1]$ such that it has no triangles and no stable sets of size n_i.

Lower bound: reduction from off-diagonal Ramsey [EM81]

$$[k,N] = \overbrace{[n_0, n_1 - 1] \cup [n_1, n_2 - 1] \ldots [n_{\frac{m}{2}-3}, n_{\frac{m}{2}-2} - 1] \cup [M, N]}^{\frac{m}{2}-1 \text{ intervals}}$$

- Edges between intervals are all present.
- Fix subgraph $[n_i, n_{i+1} - 1]$ such that it has no triangles and no stable sets of size n_i.
- Any large stable implies an M-stable in $[M, N]$.
- Any m-clique implies a triangle in $[M, N]$.

Lower bound: reduction from off-diagonal Ramsey [EM81]

$$[k,N] = \overbrace{[n_0, n_1 - 1] \cup [n_1, n_2 - 1] \ldots [n_{\frac{m}{2}-3}, n_{\frac{m}{2}-2} - 1] \cup [M, N]}^{\frac{m}{2}-1 \text{ intervals}}$$

- Edges between intervals are all present.
- Fix subgraph $[n_i, n_{i+1} - 1]$ such that it has no triangles and no stable sets of size n_i.
- Any large stable implies an M-stable in $[M, N]$.
- Any m-clique implies a triangle in $[M, N]$.
- We use Krajíček l.b. technique for $\textsc{Ram}(|[M, N]|; 3, M)$.

Lower bound: proof scheme

Given a RES refutation of size S for $\mathrm{PH}(N;k,m)$ there are

$$2^{2^{k/2}} < M < \sqrt{N} \qquad L := r(3,M) - 1 \qquad \text{(see Mills [Mil85])},$$

such that we get

1. a RES refutation of size S of $\mathrm{RAM}(N - o(N); 3, M)$;
2. a RES(2) refutation of size $S \cdot 2^{O(M \log M)}$ of $\mathrm{PHP}_L^{N-o(N)}$, see [Kra01].
3. Knowing that $L \approx \frac{M^2}{\log M}$ we get the statement

If RES(2) complexity of $\mathrm{PHP}_L^{N-o(N)}$ is $2^{\Omega(L^{1/2+\epsilon})}$ then $\mathrm{PH}(N;k,k)$ require RES refutation of size $2^{\Omega(L^{1/2+\epsilon})}$

Comments on the lower bound

If $\textsc{Res}(2)$ complexity of $\textsc{Php}_L^{N-o(N)}$ is $2^{\Omega(L^{1/2+\epsilon})}$ then $\textsc{Ph}(N;k,k)$ require $\textsc{Res}$ refutation of size $2^{\Omega(L^{1/2+\epsilon})}$

- Is the assumption believable? (I think it is)
- Formula $\textsc{Php}_L^{N-o(N)}$ ranges between

$$\textsc{Php}^n_{n/\log n} \quad \ldots \quad \textsc{Php}^{2^{\log^c n}}_n .$$

  depending on L position relative to known bounds.
- If $2^{h(k)}$ is a lower bound then $\sqrt{h(k)} \leq R(k,m)$.

Comments on the lower bound

If $\textsc{Res}(2)$ complexity of $\textsc{Php}_L^{N-o(N)}$ is $2^{\Omega(L^{1/2+\epsilon})}$ then $\textsc{Ph}(N;k,k)$ require $\textsc{Res}$ refutation of size $2^{\Omega(L^{1/2+\epsilon})}$

- Is the assumption believable? (I think it is)
- Formula $\textsc{Php}_L^{N-o(N)}$ ranges between

$$\textsc{Php}^n_{n/\log n} \quad \ldots \quad \textsc{Php}^{2^{\log^c n}}_n .$$

  depending on L position relative to known bounds.
- If $2^{h(k)}$ is a lower bound then $\sqrt{h(k)} \leq R(k,m)$.

Better combinatorial bounds are needed for better results. (Vacuously true, but we provide actual numbers!)

Upper bound

Upper bound: proof scheme

1. A recursive scheme reduces $\text{PH}(N; k, m)$ to $\text{PH}(N; \sqrt{N}, 3)$;
2. $\text{PH}(N; \sqrt{N}, 3)$ is reduced to $\text{RAM}(N - c\sqrt{N}; \sqrt{N}, 3)$;
3. We use Pudlák proof of Ramsey tautologies in BD-Frege.

The recursive scheme at step 1 costs $2^{O(Nm)}$.

BD-Frege refutation of $\text{PH}(N; \sqrt{N}, 3)$ costs $2^{O(N)}$ (step 2 and 3).

Upper bound: the idea of the recursive scheme

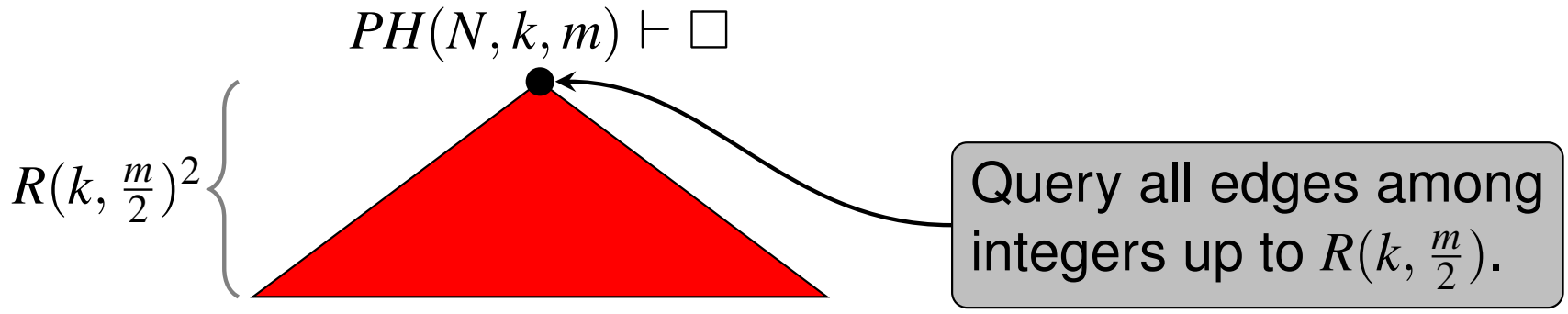
Assume the clique parameter is $m = 3 \cdot 2^l$.

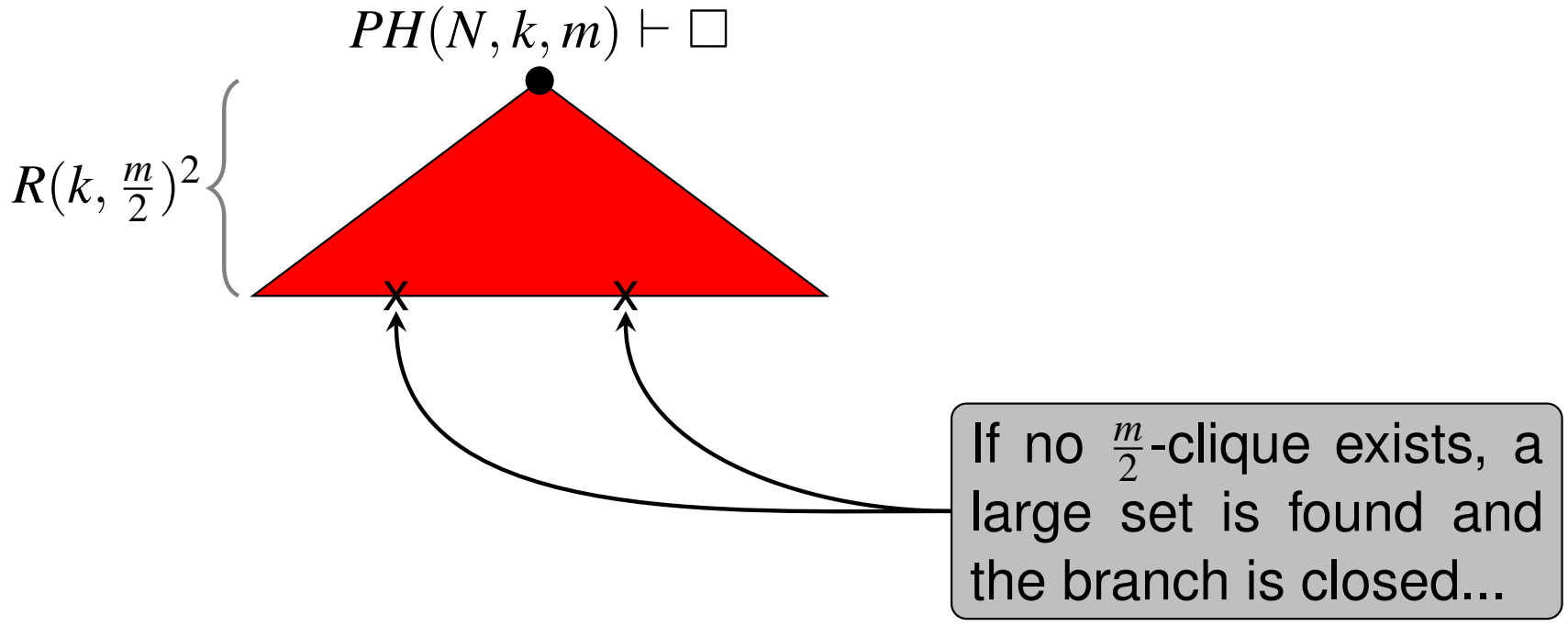
Mills' idea for the upper bound is to self-reduce the problem to the case of $m/2$-clique.

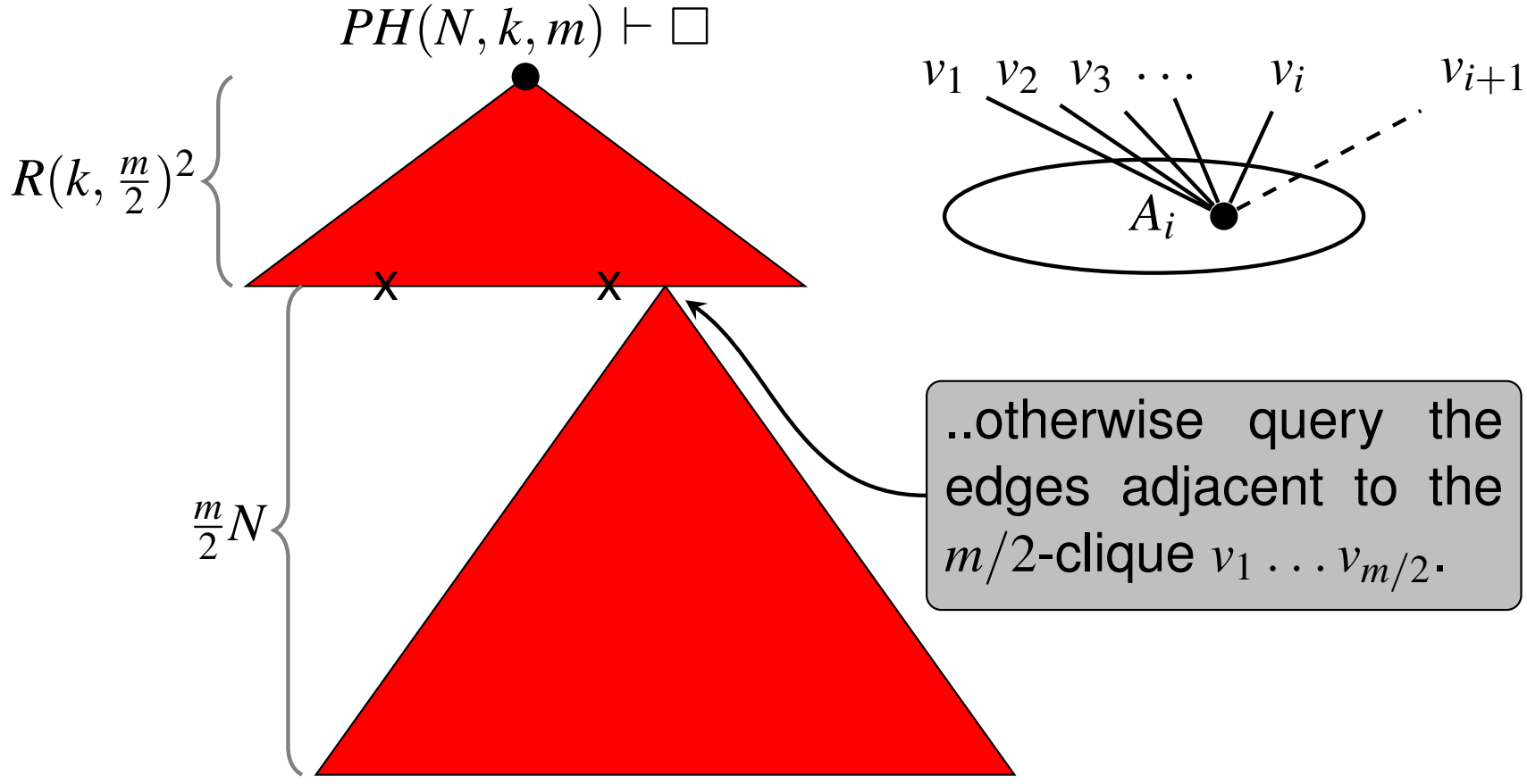
We pay for the halving of m with a shrinking of the interval.

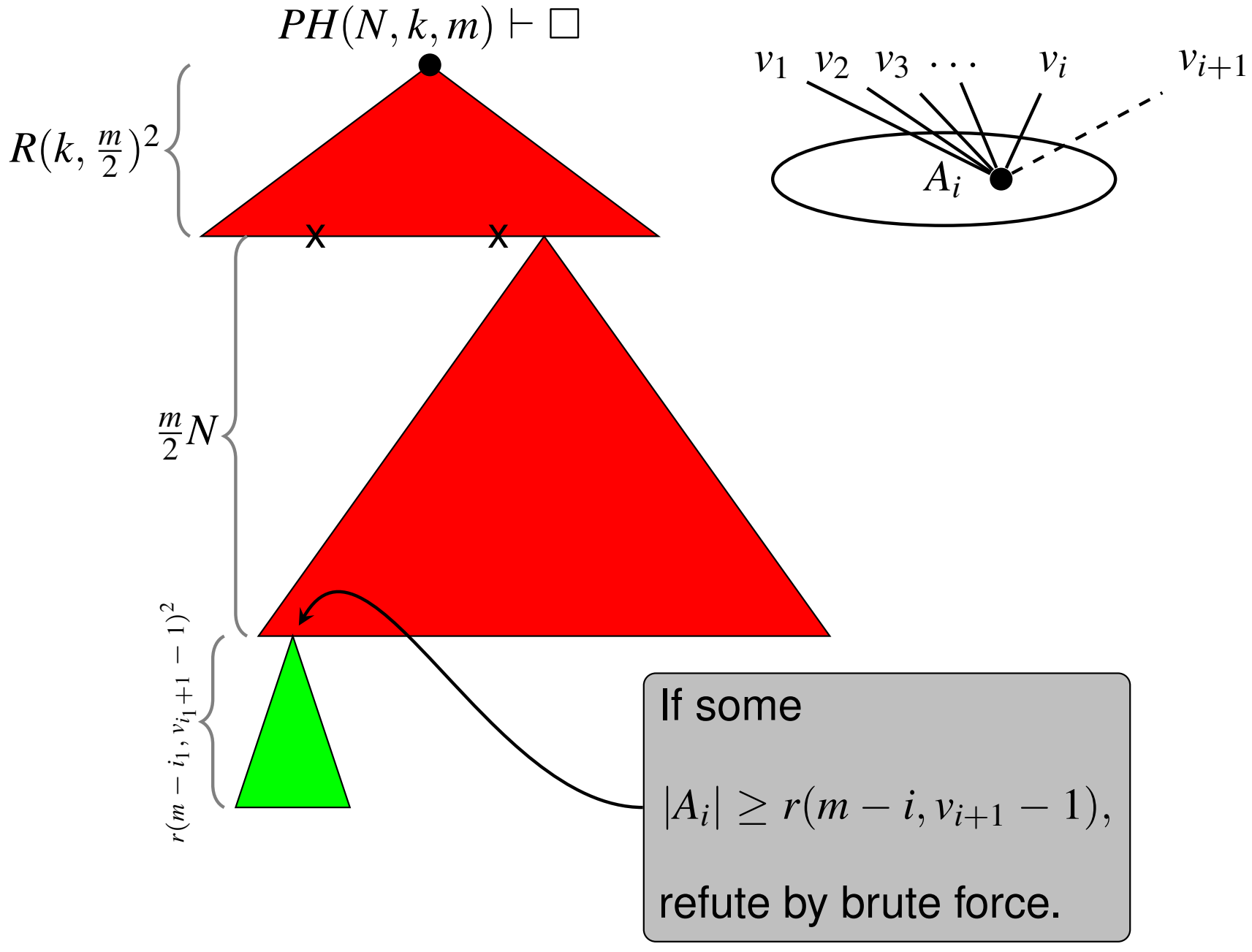
For $N = k^{2^{\beta m}}$ the interval remains big enough for the reduction to be possible until the clique parameter reaches 3.

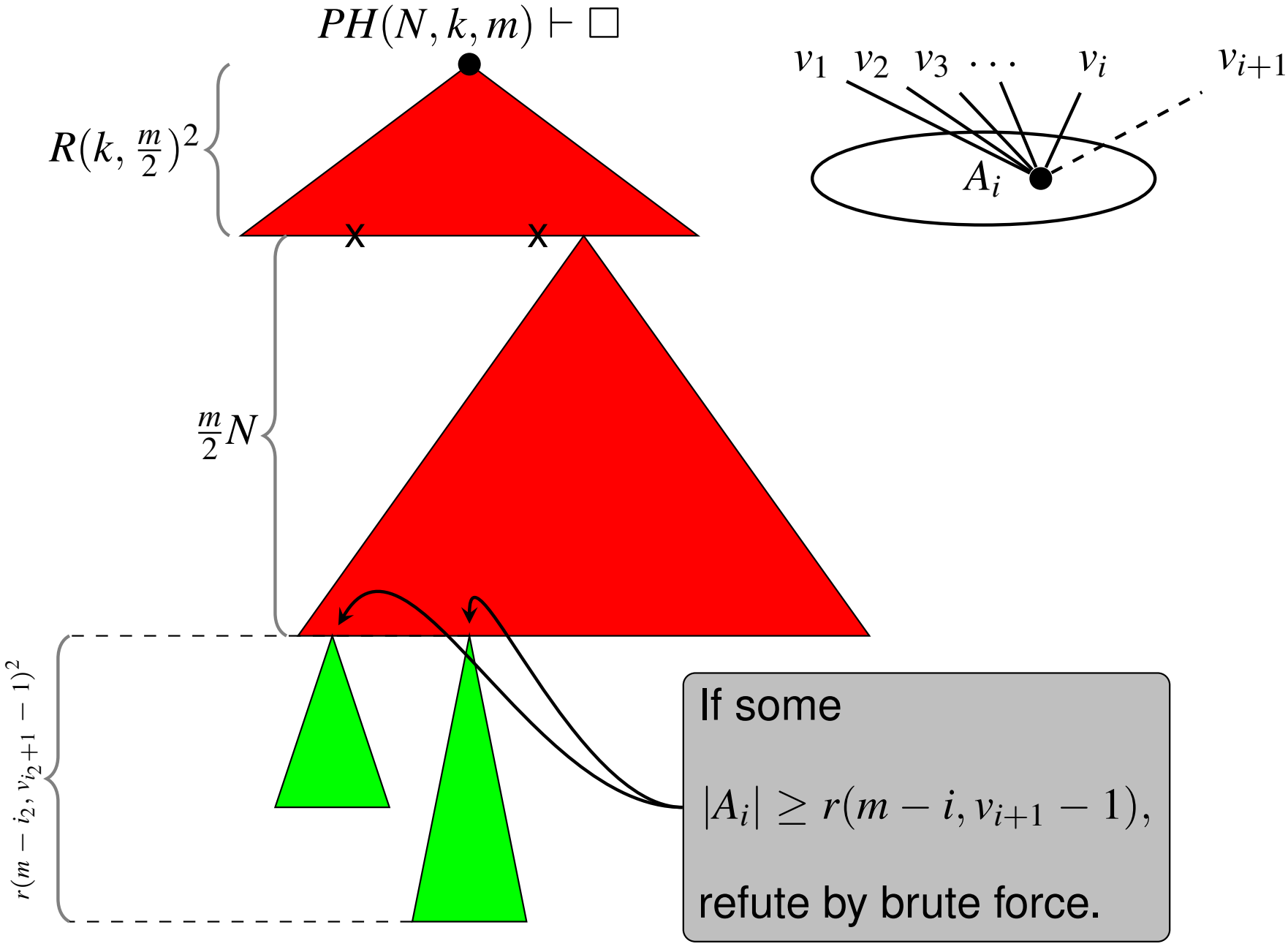
$$PH(N, k, m) \vdash \square$$

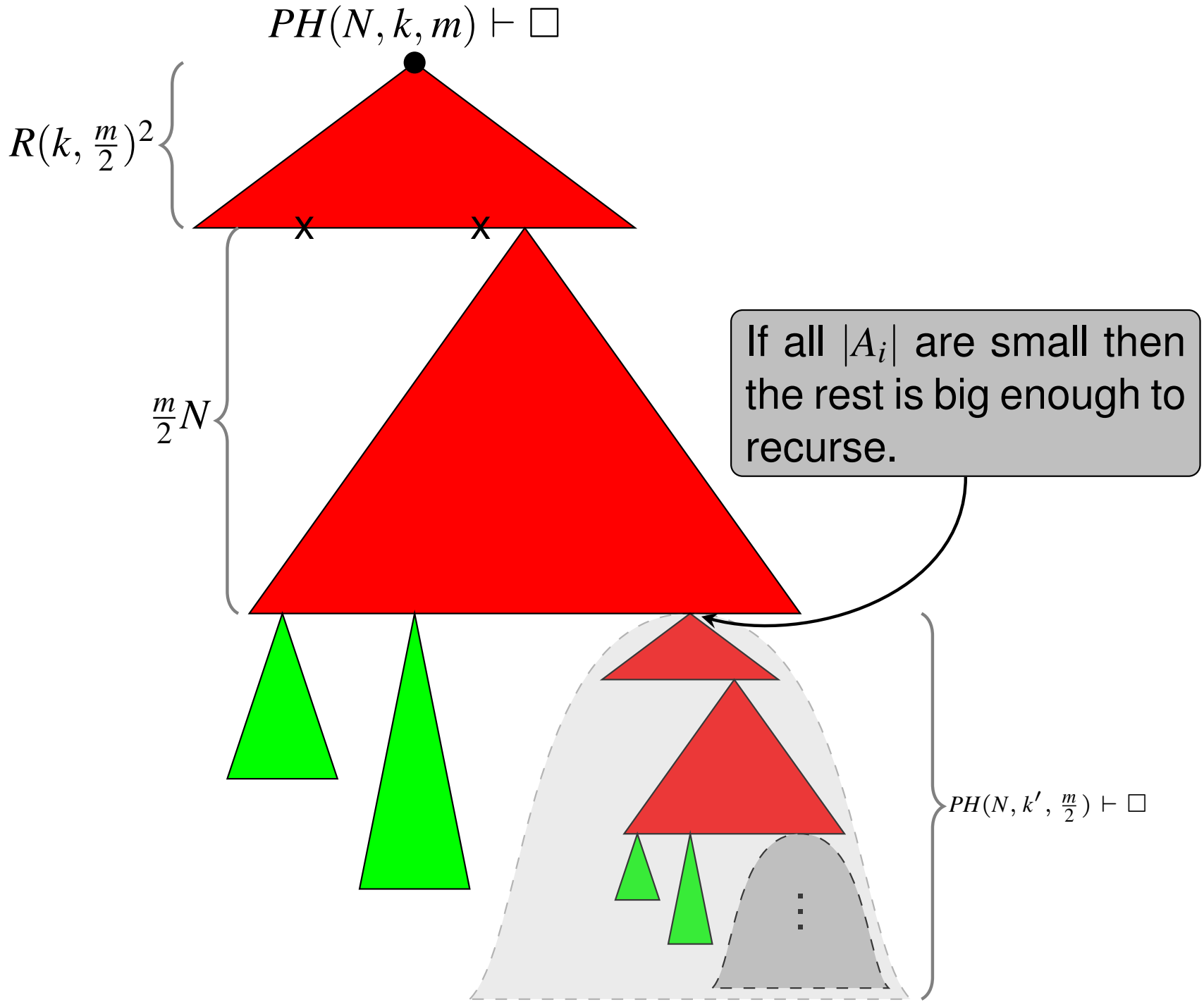

$PH(N,k,m) \vdash \square$
$R(k,\frac{m}{2})^2$
Query all edges among integers up to $R(k,\frac{m}{2})$.


$PH(N,k,m) \vdash \square$
$R(k, \frac{m}{2})^2$
If no $\frac{m}{2}$-clique exists, a large set is found and the branch is closed...


$PH(N,k,m) \vdash \square$
$R(k, \frac{m}{2})^2$
$\frac{m}{2}N$
v_1 v_2 v_3 $\cdots$ v_i v_{i+1}
A_i
..otherwise query the edges adjacent to the $m/2$-clique $v_1 \ldots v_{m/2}$.


$PH(N,k,m) \vdash \square$
$R(k,\frac{m}{2})^2$
$\frac{m}{2}N$
$r(m-i_1, v_{i_1+1}-1)^2$
v_1 v_2 v_3 $\cdots$ v_i v_{i+1}
A_i
If some
$|A_i| \geq r(m-i, v_{i+1}-1)$,
refute by brute force.


$PH(N,k,m) \vdash \square$
$R(k,\frac{m}{2})^2$
$\frac{m}{2}N$
$r(m-i_2, v_{i_2+1}-1)^2$
v_1 v_2 v_3 $\cdots$ v_i v_{i+1}
A_i
If some
$|A_i| \geq r(m-i, v_{i+1}-1)$,
refute by brute force.


$PH(N,k,m) \vdash \square$
$R(k, \frac{m}{2})^2$
$\frac{m}{2}N$
If all $|A_i|$ are small then the rest is big enough to recurse.
$PH(N, k', \frac{m}{2}) \vdash \square$

Comments on the upper bound

PH$(N;k,k)$ has a BD-Frege refutation of size $2^{O(N \log\log N)}$

- PH$(N;k,k)$ has $2^{\Theta(N)}$ clauses (we do almost polynomial).
- A trivial refutation has size 2^{N^2} (we do much better).
- A (less) trivial refutation is $2^{R(k,k)^2}$ (we don't know).

If $R(k,k) \ll \sqrt{N}$ refutation is much smaller than the formula.

Open Problems

- Improve the upper bound from $2^{O(N \log \log N)}$ to $2^{O(N)}$.
- Prove the lower bound with weaker assumptions.
- Solve the $\text{RES}(2)$ proof complexity of weak pigeonhole principle.

- Improve the upper bound from $2^{O(N \log \log N)}$ to $2^{O(N)}$.

Hint: reduce the use of brute force in our proof.

- Prove the lower bound with weaker assumptions.

Hint: reduce from more "balanced" Ramsey formulas.

- Solve the $\text{RES}(2)$ proof complexity of weak pigeonhole principle.

Hint: if you have any, please tell me!

Further details

Conference version:

L. Carlucci, N. Galesi, M. Lauria.
Paris-Harrington Tautologies
26th Conference on Computational Complexity, 2011.

Full version:

L. Carlucci, N. Galesi, M. Lauria.
Paris-Harrington Tautologies
`http://eccc.hpi-web.de/report/2010/153/`

Thank You


Peter Clote.
Cutting planes and Frege proofs.
Information and Computation, 121(1):103–122, 1995.


Paul Erdős and George Mills.
Some bounds for the Ramsey-Paris-Harrington numbers.
Journal of Combinatorial Theory, Series A, 30(1):53–70, 1981.


Jan Krajíček.
On the weak pigeonhole principle.
Fundamenta Mathematicae, 170(1-3):123–140, 2001.


Jan Krajíček.
A note on propositional proof complexity of some Ramsey-type statements.
Archive for Mathematical Logic, 50:245–255, 2011. 10.1007/s00153-010-0212-9.


George Mills.

Ramsey-Paris-Harrington numbers for graphs.
Journal of Combinatorial Theory, Series A, 38(1):30 – 37, 1985.

Pavel Pudlák.
Ramsey's theorem in Bounded Arithmetic.
In *Proceedings of Computer Science Logic 1990*, pages 308–317, 1991.