Feasible Interpolation

Sebastian Müller

Faculty of Mathematics and Physics
Charles University
Prague

28.11.2010

Interpolation Theorems

Graph Properties

Feasible Interpolation

Limits to the Method

Definition

A *clause* is a set of propositional literals. It is interpreted as the disjunction of its elements. Thus, we say that a clause is refuted if all literals it contains are set to false.

Claim

A Resolution-refutation of a set of clauses $A_1, \ldots, A_n$ can be equivalently defined as an LK-proof of the sequent

$$A_1, \ldots, A_n \longrightarrow$$

without using any $\bigvee$ or $\bigwedge$.

Definition

Let $A(\bar{p}, \bar{q}) \rightarrow \neg B(\bar{p}, \bar{r})$ for propositional formulas A, B. An *interpolant* for that implication is a boolean function $I(\bar{p})$ in the common variables of A and B such that

- $A(\bar{p}, \bar{q}) \rightarrow I(\bar{p})$ and
- $I(\bar{p}) \rightarrow \neg B(\bar{p}, \bar{r})$

Definition (Circuit Complexity)

Let $f(\bar{p})$ be a boolean function. The *circuit complexity* of f is the minimal size of a ($NC^1/poly$ family of) circuit computing f. The *monotone circuit complexity* of f is the minimal size of a ($NC^1/poly$ family of) monotone circuit computing f.

Theorem (Krajíček 97)

Let $\mathcal{C} := \{A_1, \ldots, A_m, B_1, \ldots, B_\ell\}$ be a set of clauses, such that A_i and B_i have common variables p_j and variables q_j that only appear in A_i and r_j that only appear in B_i.
If $\mathcal{C}$ has a Resolution refutation with k clauses, then the implication

$$\bigwedge_{i<m} A_i \rightarrow \neg \bigwedge_{j\leq\ell} B_j$$

has an interpolating circuit $I(\bar{p})$ of circuit-size $k \cdot n^{O(1)}$.
Moreover, if all atoms $\bar{p}$ occur only positively in A_i or only negatively in B_i, then $I(\bar{p})$ is monotone.

Encoding a Graph

We can encode a graph $G = (V, E)$ with n vertices using propositional variables $p^G_{i,j}$ for $i, j \leq n$, such that

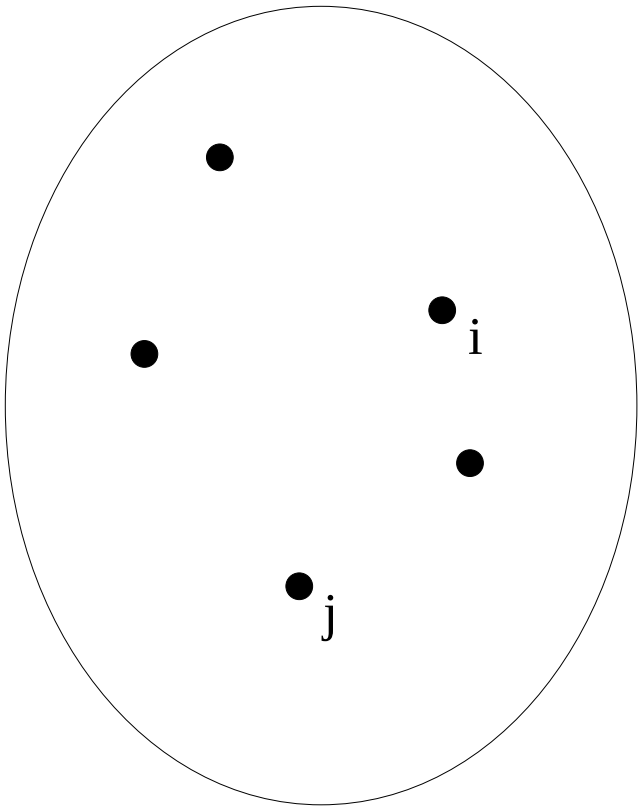
$$p^G_{i,j} \leftrightarrow E(v_i, v_j).$$

We can use additional variables p^{cl}_{i,j_1} and p^{co}_{i,j_2}, for $i \leq n,\ j_1 \leq k$ and $j_2 \leq c$ to code k-cliques and c-colorings in G.

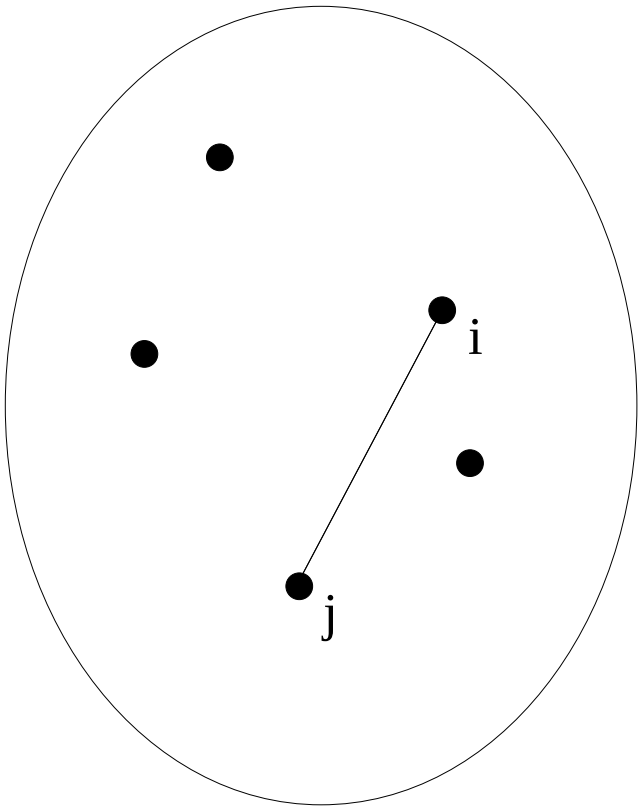
$$p^{co}_{i,j} \leftrightarrow v_i \text{ is colored with color } j$$

and

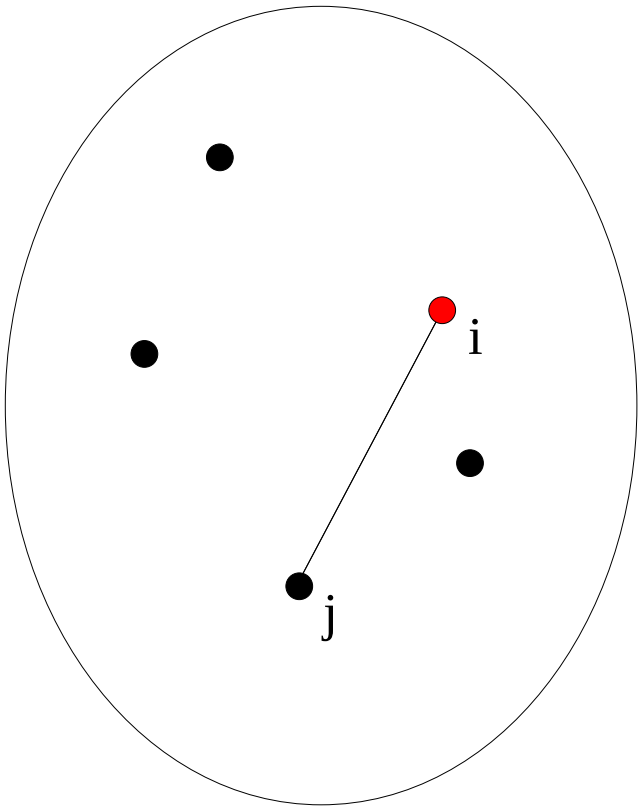
$$p^{cl}_{i,j} \leftrightarrow v_i \text{ is the } j^{th} \text{ member of the clique.}$$



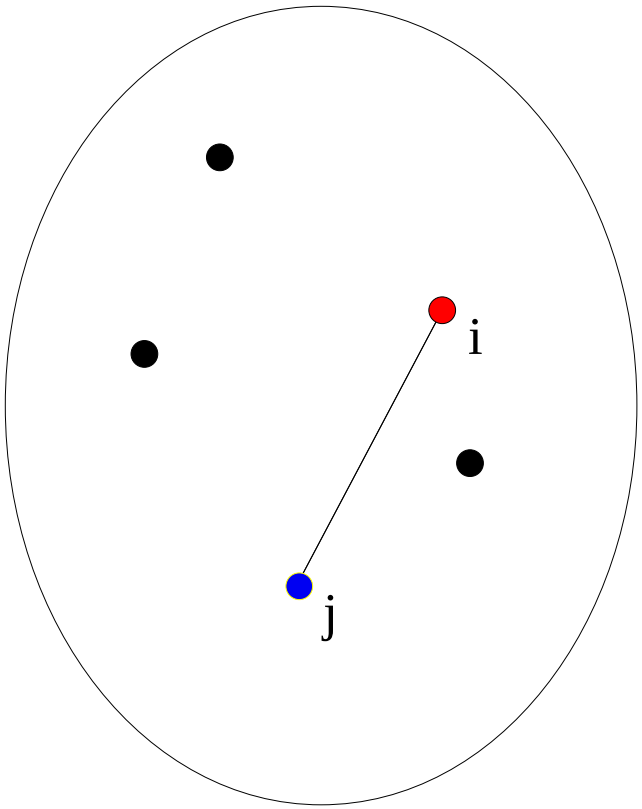
$\neg p^{G}_{k,l} \wedge \neg p^{co}_{k,l} \wedge \neg p^{cl}_{k,l}$ for all l, k.



$$p^G_{i,j} \wedge p^G_{j,i} \wedge p^{cl}_{i,1} \wedge p^{cl}_{j,2}.$$



$$p^G_{i,j} \wedge p^G_{j,i} \wedge p^{co}_{i,red} \wedge p^{cl}_{i,1} \wedge p^{cl}_{j,2}.$$



$$p^G_{i,j} \wedge p^G_{j,i} \wedge p^{co}_{i,red} \wedge p^{co}_{j,blue} \wedge p^{cl}_{i,1} \wedge p^{cl}_{j,2}.$$

Formalizations

Definitions

The following formulas formalize that a graph with n vertices has a c-coloring:

- $\neg(p^G_{i,j} \wedge p^{co}_{i,k} \wedge p^{co}_{j,k})$, for all $i, j \leq n$ and $k \leq c$.
- $\neg(p^{co}_{i,j} \wedge p^{co}_{i,k})$ for all $i \leq n$ and $j, k \leq c$ with $j \neq k$.
- $\bigvee_{j \leq c} p^{co}_{i,j}$ for all $i \leq n$.

We denote the set of these formulas by $\text{Colour}_{n,c}(\bar{p}^G, \bar{p}^{co})$. Observe that it only contains disjunctions of literals.

Formalizations

Definitions

The following formulas formalize that a graph with n vertices has a k-clique:

- $\bigvee_{i \leq n} p^{cl}_{i,j}$ for all $j \leq k$.
- $\neg(p^{cl}_{i,j_1} \wedge p^{cl}_{i,j_2})$ for all $i \leq n$ and $j_1, j_2 \leq k$ with $j_1 \neq j_2$.
- $\neg(\neg p^{G}_{i,j} \wedge p^{co}_{i,j_1} \wedge p^{co}_{j,j_2})$ for all $i \leq n$ and $j_1, j_2 \leq k$.

We denote the set of these formulas by $\text{Clique}_{n,k}(\bar{p}^G, \bar{p}^{cl})$. Observe that it only contains disjunctions of literals.

Big Cliques Exclude Small Colorings

Obviously the following expression holds

$$\text{Clique}_{n,k}(\bar{p}^G, \bar{p}^{cl}) \rightarrow \neg\text{Colour}_{n,c}(\bar{p}^G, \bar{p}^{co})$$

for all $c < k$.
Observe that all literals $\bar{p}^G$ appear only negatively in $\text{Colour}_{n,c}$ and only positively in $\text{Clique}_{n,k}$.

Theorem (Alon, Boppana 87)

Assume that $3 \leq c < k$ *and that* $k \cdot \sqrt{c} \leq \frac{n}{8 \log n}$. *Then every interpolant* $I(\bar{p}^G)$ *for the sequent*

$$\text{Clique}_{n,k}(\bar{p}^G, \bar{p}^{cl}) \rightarrow \neg\text{Colour}_{n,c}(\bar{p}^G, \bar{p}^{co})$$

has monotone circuit complexity

$$2^{\Omega(\sqrt{c})}.$$

Theorem

Resolution has exponential lower bounds.

Proof (Krajíček 97)

Fix n and $3 < c = \lceil \sqrt{n} \rceil < k$. By Alon & Boppana the sequent

$$\text{Clique}_{n,k}(\bar{p}^G, \bar{p}^{cl}) \rightarrow \neg\text{Colour}_{n,c}(\bar{p}^G, \bar{p}^{co}) \qquad (1)$$

has no interpolants of subexponential (in n) monotone circuit complexity.

Proof cont'd

Now, $\text{Clique}_{n,k}(\bar{p}^G, \bar{p}^{cl})$ and $\text{Colour}_{n,c}(\bar{p}^G, \bar{p}^{co})$ can both be viewed as sets of clauses, since all propositional statements they consist of are disjunctions of literals. We will call the sets of clauses $\mathbf{Clique}_{n,k}$ and $\mathbf{Colour}_{n,c}$ and a proof of (1) is equivalent to a refutation of

$$\mathbf{Clique}_{n,k} \cup \mathbf{Colour}_{n,c}.$$

However, since all literals $\bar{p}^G$ appear only negatively in $\mathbf{Colour}_{n,c}$ (and only positively in $\mathbf{Clique}_{n,k}$) we can use the Interpolation Theorem for Resolution to deduce the existence of a monotone interpolant $I(\bar{p})$ of circuit complexity $k \cdot n^{O(1)}$, where k is the number of clauses in a refutation of

$$\mathbf{Clique}_{n,k} \cup \mathbf{Colour}_{n,c}.$$

Proof cont'd

But since the circuit complexity of I is exponential, we must conclude that $k \in 2^{\Omega(\sqrt{\sqrt{n}})}$ as well.Thus (by taking large enough n's) we can conclude that no subexponential Resolution refutation of

$$\textbf{Clique}_{n,k} \cup \textbf{Colour}_{n,c}$$

exists. □

Corollaries

In a similar way we can deduct lower bounds for various other proof systems such as

- Cutting Planes
- Some fragments of LK
- etc...

We know, however, that this method cannot be applied to strong proof systems (unconditionally in the monotone case and conditionally in the general case).

Theorem (Razborov 95)

The set of clauses

$$\mathbf{Clique}_{n,k} \cup \mathbf{Colour}_{n,c}$$

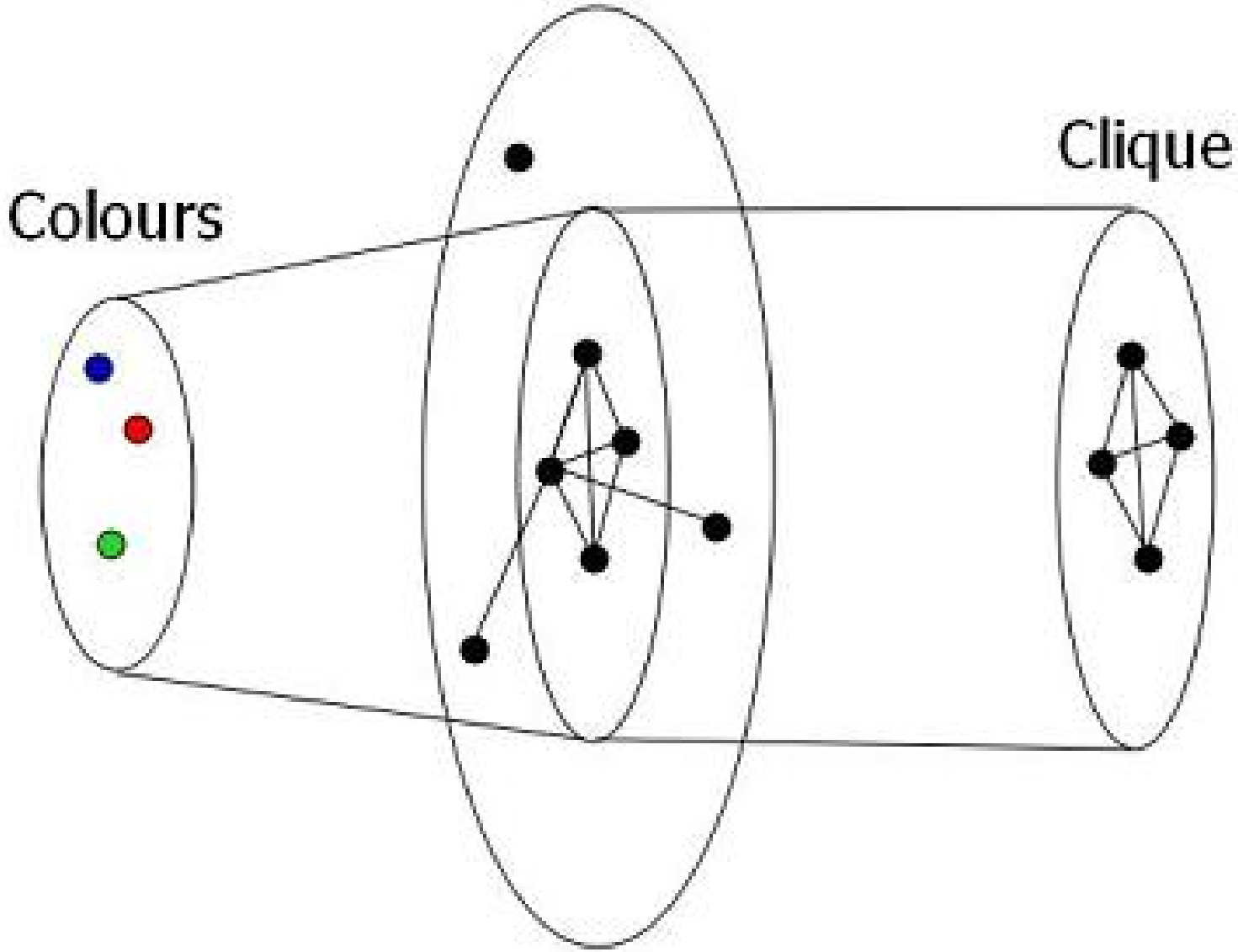
with $c = \sqrt{\sqrt{n}}$ *and* $k = \sqrt{n}$ *has a depth 2 LK refutation of size* $2^{(\log n)^{O(1)}}$ *.However, the implication*

$$\mathrm{Clique}_{n,k} \rightarrow \neg \mathrm{Colour}_{n,c}$$

has no monotone interpolant of monotone circuit-size $2^{n^{o(1)}}$ *.*
(by Alon&Boppana)

Proof

We will argue in Bounded Arithmetic. Let $G = (V, E)$ be a graph with n vertices and let $F_1 : [k] \longrightarrow [n]$ and $F_2 : [n] \longrightarrow [c]$. Now, from the weak pigeonhole principle WPHP_c^k it follows that F_1 cannot be a 1-1 map if F_2 is a coloring of G (because this would imply an injective mapping f from $[k]$ to $[c]$).


Colours
Clique

Proof cont'd

We can $\Delta_1^b(G, F_1, F_2)$-define this f by:

$$\begin{aligned} f(i) = u &\equiv \exists j(F_1(i) = j \wedge F_2(j) = u) \\ &\equiv \forall j(F_1(i) = j \rightarrow F_2(j) = u). \end{aligned}$$

Now, the weak pigeonhole principle says that f cannot be injective (with our choice of parameters for c, k). The weak pigeonhole principle is provable in $T_2^3(G, F_1, F_2)$ and thus f is provably not 1-1 in this theory.

Intermission

Claim

Every such theory T corresponds to a propositional proof system p_T in the following sense:
A Σ_1^b-statement φ is provable in T iff p_T has short proofs (polynomially bounded) of its translation into propositional logic.

Proof cont'd

By translating the proof in $T_2^3(G, F_1, F_2)$ we get a depth 4 tree-like poly-size LK proof of the translation of that statement. From that we can derive a depth 2 quasi-polynomial LK refutation of

$$\textbf{Clique}_{n,k} \cup \textbf{Colour}_{n,c}.$$

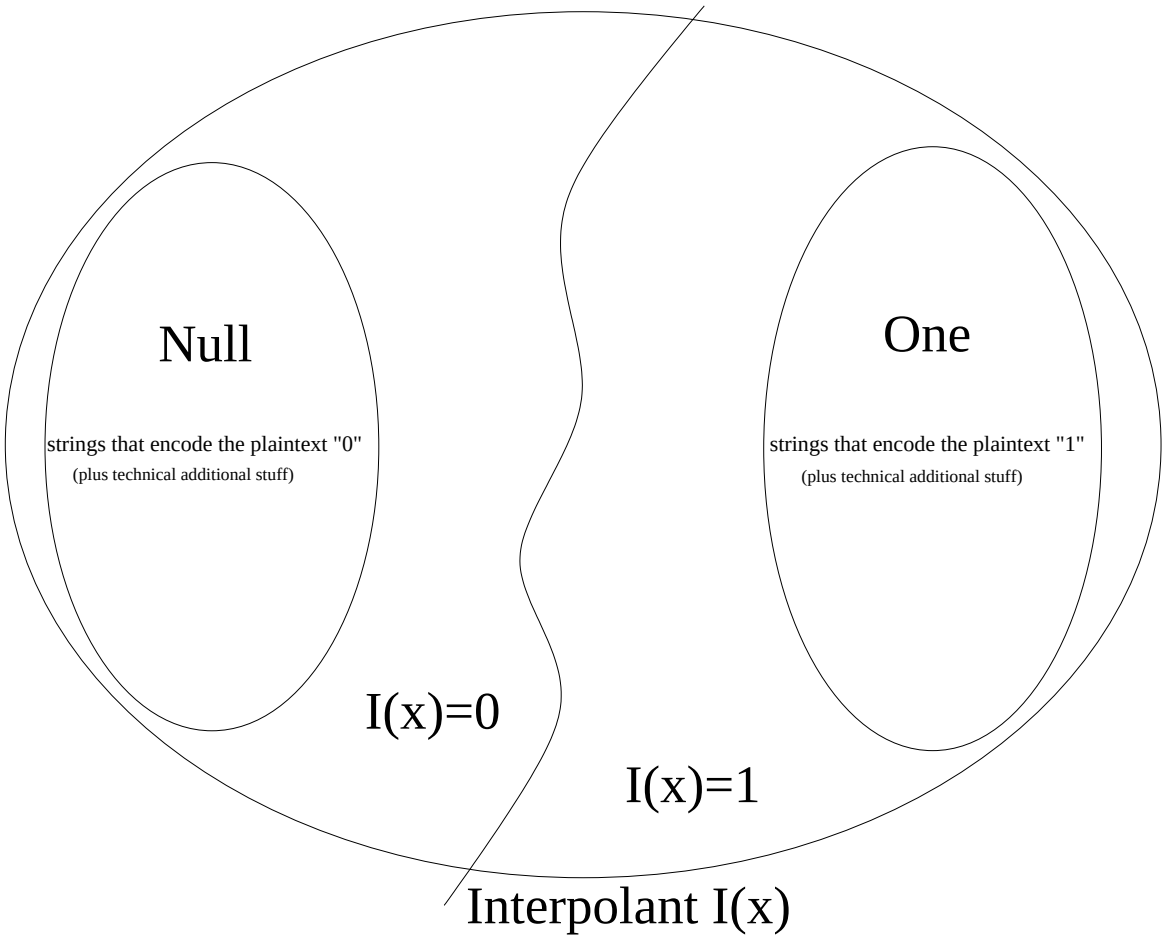
□

Theorem (Krajíček, Pudlák 95)

If RSA *is secure then EF does not have feasible interpolation.*

Proof-sketch by picture

We prove the contrapositive. So assume that EF has feasible interpolation.
Let *Null* be the set of all strings that are codes of the bit 0 and *One* be the set of all strings that are codes of the bit 1 (both padded with additional information to make the appropriate proof work).


Null
strings that encode the plaintext "0"
(plus technical additional stuff)
One
strings that encode the plaintext "1"
(plus technical additional stuff)
I(x)=0
I(x)=1
Interpolant I(x)

Proof cont'd

EF has polynomial sized proofs (of the translation) of the fact that RSA is 1-1 and therefore also proves the disjointness of *Null* and *One*. Observe that this can be written as

$$One(\bar{x}) \rightarrow \neg Null(\bar{x}).$$

Since EF has feasible interpolation there is a boolean function $I(\bar{x})$ that interpolates this implication. This interpolant is an inverse of the RSA-encoding, so RSA is not secure against adversaries of complexity P/poly. □


Dankeschön!!
Спасибо!
Děkuju, soudruzi