Some consequences of cryptographical conjectures for S_2^1 and EF

Jan Krajíček* and Pavel Pudlák*

Mathematical Institute of the Academy of Sciences
Žitná 25, Praha 1, 115 67, Czech Republic

Abstract. We show that there is a pair of disjoint $\mathcal{NP}$-sets, whose disjointness is provable in S_2^1 and which cannot be separated by a set in $\mathcal{P}/poly$, if the cryptosystem RSA is secure. Further we show that factoring and the discrete logarithm are implicitly definable in any extension of S_2^1 admitting an $\mathcal{NP}$ -definition of primes about which it can prove that no number satisfying the definition is composite.
As a corollary we obtain that the Extended Frege (EF) proof system does not admit feasible interpolation theorem unless the RSA cryptosystem is not secure, and that an extension of EF by tautologies τ_p (p primes), formalizing that p is not composite, as additional axioms does not admit feasible interpolation theorem unless factoring and the discrete logarithm are in $\mathcal{P}/poly$.[2]

The $\mathcal{NP} \neq co\mathcal{NP}$ conjecture is equivalent to the statement that no propositional proof system (as defined in [6]) admits polynomial size proofs of all tautologies. However, only for few proof systems occurring in the literature explicit superpolynomial lower bounds are known; see [9] for a survey (and for important connections to bounded arithmetic).

The following approach to proving lower bounds for propositional proof system was proposed in [8].[3] Various interesting tautologies expressing some finite combinatorial principles (e.g., modular counting principles as in [8]) can be formulated in a form of an implication

$$\alpha(\overline{x}, \overline{y}) \rightarrow \beta(\overline{x}, \overline{z})$$

* Partially supported by the grant No. A1019602 of the Academy of Sciences of the Czech Republic, and by the grant No. 93 025 of the US-Czechoslovak Science and Technology Program.

[2] This paper is a revised version of a preliminary report which appeared under the same title in *Logic and Computational Complexity* (Proc. of the meeting held in Indianapolis, October 1994), Ed. D. Leivant, Springer-Verlag, Lecture Notes in Computer Science, Vol. **960**, (1995), pp.210-220.

[3] Mundici [17, 18, 19, 20] studied earlier the question to estimate the complexity of an interpolant of an implication in terms of the size of the implication. He linked the problem to open problems in complexity theory about classes $\mathcal{P}/poly$, $\mathcal{NP}$, $co\mathcal{NP}$, $\mathcal{NC}^1$ and similar. He also singled out the class of *natural*proof systems, those being proof systems admitting a form of effective interpolation (described below). He did not considered length-of-proofs questions.

where $\overline{x}$ are the only atoms common to both α and β (equivalently we may think of refutations of $\alpha, \neg\beta$, as we shall, in fact, do). An interpolant for the implication is a formula $\gamma(\overline{x})$ such that both implications

$$\alpha \to \gamma \text{ and } \gamma \to \beta$$

are tautologies. Equivalently, an interpolant for the implication is any set I separating the sets

$$A := \{\overline{\epsilon} \in \{0,1\}^n \mid \exists \overline{y} \in \{0,1\}^k; \alpha(\overline{\epsilon}, \overline{y}) \text{ is true } \}$$

$$B := \{\overline{\epsilon} \in \{0,1\}^n \mid \exists \overline{z} \in \{0,1\}^\ell; \neg\beta(\overline{\epsilon}, \overline{z}) \text{ is true } \}$$

that is,

$$A \subseteq I \quad \text{and} \quad I \cap B = \emptyset$$

We say that a proof system P admits *effective interpolation* if there is a polynomial $p(x)$ such that whenever m is the minimal size of a P-proof of $\alpha \to \beta$ then there is an interpolant whose circuit-size is at most $p(m)$. Then any two sets A, B (definable in a way as above) that cannot be separated by a set of small circuit complexity give rise to an implication whose all P-proofs must be large. Thus we get in this way lower bounds for proof systems admitting effective interpolation.

This idea works for some proof systems, most notably for resolution and cutting planes proof systems (see [27, 2, 10, 4, 25, 11, 26, 12]). In this paper we study limitations to this method. In particular, we shall show that Extended Frege proof system does not admit effective interpolation unless the RSA cryptosystem is not secure.

The assumption about RSA is stronger than $\mathcal{P}/poly \neq \mathcal{NP}$, so it will be very difficult to prove. However, the system has been extensively tested and its security seems very likely. Thus our result essentially rules out the possibility of applying effective interpolation for proving lower bounds for EF or any stronger proof system.

Our proof can be briefly described as follows. The security of RSA gives a pair A, B of disjoint $\mathcal{NP}$-sets that cannot be separated by a set in $\mathcal{P}/poly$. Given the pair we construct a sequence of tautologies of the form $\alpha_n \to \beta_n$ whose interpolants must have large circuit complexity. We shall show, on the other hand, that these implications have polynomial size proof in EF. This violates effective interpolation.

It would be very tedious and formal to construct the EF-proofs explicitly. We use instead a relation between EF and a first-order theory S^1_2. In particular, a provability of the disjointness in S^1_2 implies the existence of polynomial size EF-proofs of the implications $\alpha_n \to \beta_n$ (those proofs can be, in principle, explicitly constructed). Moreover, this relation also allows us to deduce some independence results for S^1_2 from the RSA assumption. Namely, S^1_2 proves neither Fermat's little theorem nor the weak pigeonhole principle for polynomial-time functions.

We shall consider two additional cryptographical assumptions: the hardness of factoring and of the discrete logarithm. The security of RSA presupposes the hardness of factoring but it is open if it suffices. We shall prove a similar results using these assumptions but only for a theory presumably stronger than S^1_2. These results imply similarly the impossibility of effective interpolation for the quantified propositional proof system G (its fragment G_3, in fact).

Defining S^1_2 and presenting the basic results about this theory would make this paper too long. A reader not familiar with this subject may consult [9].

The symbol (a, b) denotes the greatest common divisor. Δ^b_1-formulas are everywhere in the paper meant as Δ^b_1 w.r.t. S^1_2.

1 A disjoint $\mathcal{NP}$ -pair based on RSA

RSA is the most commonly used public key cryptosystem, see [29]. It works as follows. For two sufficiently large primes p and q we take $n := p \cdot q$. An encoding key, that is public, is a pair (n, e), where $1 < e < n$. An $x < n$ is encoded by $y := x^e \bmod n$. The secret decoding key is a number d such that $e \cdot d \equiv 1 \bmod \varphi(n)$, where $\varphi(n)$ is the Euler function. To decode x from y compute $x := y^d \bmod n$.

RSA can be used to encode securely single bits by encoding a random even (resp. odd) $x < n$ if the bit is 0 (resp. 1). The security of this probabilistic encryption is know to be as good as that of RSA, see [1]. Our pair of disjoint $\mathcal{NP}$ -sets is based on it.

For $i = 0, 1$, let

$$A_i =_{df} \{(n, e, y);\ \exists x, d, r < n\ (x \equiv i \bmod 2 \wedge x^e \equiv y \bmod n$$

$$\wedge\ y^d \equiv x \bmod n \wedge y^r \equiv 1 \bmod n \wedge (e, r) = 1\}\ .$$

One can check that exponentiation modulo a number $n \geq 2$ is definable and satisfies the usual relations in S^1_2, namely $x^{y+z} \equiv x^y x^z \bmod n$, $x^{yz} \equiv (x^y)^z \bmod n$. Assuming that RSA is secure against an adversary computing functions in $\mathcal{P}/poly$, this pair cannot be separated by a set in $\mathcal{P}/poly$, if one considers only those n's which are products of two primes. Hence it cannot be separated by such a set in general either.

Theorem 1.

$$S^1_2 \vdash A_0 \cap A_1 = \emptyset.$$

Consequently, assuming that RSA is secure against an adversary computing functions in $\mathcal{P}/poly$, not all Δ^b_1-implications provable in S^1_2 admit an interpolant in $\mathcal{P}/poly$.

Proof.

We shall show in S^1_2 that for every y there is at most one $x < n$ which satisfies the defining formula of either A_0 or A_1. The proof is easy, since we put everything in the definition. So suppose that for some $x_0, x_1 < n$, r_0 (we do not need r_1), d_0, d_1, $y^{r_0} \equiv 1 \bmod n$, $(e, r_0) = 1$ and

$$x_i^e \equiv y \bmod n \wedge y^{d_i} \equiv x_i \bmod n,$$

for $i = 0, 1$. We have

$$x_i^{r_0} \equiv (y^{d_i})^{r_0} \equiv (y^{r_0})^{d_i} \equiv 1 \bmod n,$$

for $i = 0, 1$. Using Euclid's algorithm we can show that there exists an inverse d' to e modulo r_0. Thus, using $x_i^{r_0} \equiv 1 \bmod n$, for $i = 0, 1$ it holds

$$y^{d'} \equiv x_i^{ed'} \equiv x_i \bmod n,$$

whence $x_0 = x_1$.

The statement $A_0 \cap A_1 = \emptyset$ can be written as the following implication

$$\alpha_0(n, e, y, x_0, d_0, r_0) \to \neg\alpha_1(n, e, y, x_1, d_1, r_1)$$

where α_i are Δ_1^b-formulas such that the Σ_1^b-formulas $\exists x, d, r < n\ \alpha_i(n, e, y, x, d, r)$ define A_i, for $i = 0, 1$. Any interpolant of this implication separates A_0 from A_1. This yields the second part of the theorem. □

The advantage of this pair is that we do not have to mention primes as it is the case with other examples based on conjectured one-way functions. The problem with primes is that it is unlikely that the $\mathcal{NP}$-definition of primes of Pratt [24] is provably in S_2^1 equivalent to the natural $co\mathcal{NP}$-definition. If it were so, we would immediately get a polynomial time algorithm for factoring. Let $Composite(a) := \exists u, v < a, u \cdot v = a$.

Proposition 2. *Suppose S_2^1 proves $\neg A(a) \to Composite(a)$ where $A(a)$ is a Σ_1^b formula defining primes in the standard model. Then there exists a polynomial time algorithm for factoring.*

Proof.
Assume that $S_2^1 \vdash \neg A(a) \to Composite(a)$. Then we can prove by $\Sigma_1^b LIND$

$$\forall x > 1 \exists y > 1 (A(y) \wedge y | x).$$

Namely, take y of minimal length such that $1 < y \wedge y|x$. Then $A(y)$ holds as otherwise $Composite(y)$ would follow and we would get a proper divisor of x of length smaller than that of y.

Now we can apply Buss's theorem [3] which gives a polynomial time algorithm which finds a prime divisor y of x.

□

The reader might compare this statement with Theorem 12.

The definition of the sets A_i we use is by no means unique and various modifications are possible. Razborov suggested to replace $y^d \equiv x \bmod n \wedge y^r \equiv 1 \bmod n$ by $x^r \equiv 1 \bmod n$. Buss pointed out that by posing an extra condition $(y, n) = 1$ in the definition we may drop r altogether (note that $y^r \equiv 1 (\bmod\ n)$ implies that y, n are coprime). That is because we can define then $r := d \cdot e - 1$ for which

$$y^{r+1} \equiv y^{de} \equiv x^e \equiv y \pmod n$$

This implies, using the new condition $(y, n) = 1$, that

$$y^r \equiv 1 \pmod n$$

and the proof of Theorem 1 continues as before, using $d' := d$.

However, some condition implying $\exists r(y^r \equiv 1 \bmod n)$ seems to be needed, as the next theorem shows.

Theorem 3. *If RSA is secure, then*

$$S^1_2 \not\vdash \forall n > 1 \forall y,\ (y, n) = 1 \rightarrow \exists r > 0\ (y^r \equiv 1 \bmod n)\ .$$

Proof.

Suppose the converse. Then, again by Buss's theorem, we get an r by a polynomial time algorithm. Such an r suffices to break the RSA. Namely, if $y \equiv x^e \bmod n$ and $(e, r') = 1$, where r' is the order of y, then $r'|r$ and hence also $r'|r_0$ for $r_0 = r/(e, r)$. Thus we have also $(e, r_0) = 1$ and $y^{r_0} \equiv 1 \bmod n$, and we compute the inverse of e modulo r_0 and continue as in the proof of Theorem 1. □

In particular, if RSA is secure then S^1_2 cannot prove Fermat-Euler theorem. Surely it is possible to get a lot of independence results using such assumptions, however the above sentence is rather special, since it easily follows from the weak Pigeon Hole Principle (WPHP). Thus we get:

Corollary 4. *If RSA is secure, then* $S^1_2 \not\vdash WPHP(\Delta^b_1)$.

Proof.

Fix n and y prime to each other and take the function $r \mapsto y^r \bmod n$. By $WPHP$ we get $r_1 < r_2 < 2n$ such that $y^{r_1} \equiv y^{r_2} \not\equiv 0 \bmod n$, whence $y^{r_2 - r_1} \equiv 1 \bmod n$. □

Note, in particular, that as S_2 proves $WPHP(\Delta^b_1)$ (by [22]) this gives another proof of the conditional separation $S^1_2 \neq S_2$ based on a different structural complexity conjecture than the proof of [16]. Moreover, it follows from [16, 7] that $PV \not\vdash WPHP(\Delta^b_1)$ and $S^1_2 \not\vdash PHP(\Delta^b_1)$ (assuming that $NP \not\subseteq P/poly$ and $L^{NP} \neq \Delta^p_2$ respectively) but not the conclusion of Corollary 4.

2 Implicit definability of factoring and the discrete logarithm

Assume that S^1_2 proves

$$A(x,y) \wedge A(x',y) \to x = x'$$

for some Σ^b_1-formula A. In other words, it implicitly defines a (partial) function $x := f(y)$ such that

$$\exists x A(x,y) \to A(f(y),y) \ .$$

We show that in a natural extension of S^1_2 factoring and the discrete logarithm are implicitly definable in this way.

Let $C(p,w)$ be a Δ^b_1-formula saying that

$$w = (g, p, q_1, e_1, \ldots, q_t, e_t, w_1, \ldots, w_t)$$

such that:

1. $g \in Z^*_p$ and $g^{p-1} \equiv 1 \bmod p$
2. $p - 1 = \Pi_{i \le t} q_i^{e_i}$
3. $g^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p$, for all $i \le t$
4. $C(q_i, w_i)$, for all $i \le t$.

The $\mathcal{NP}$-definition of primes by Pratt [24] is $\exists w \le t(a) C(a,w)$ for a suitable term $t(a)$. We shall denote the definition by $Pratt(a)$. Denote by Φ the following $\forall \Pi^b_1$-formula:

$$\Phi := \forall x, Pratt(x) \to \neg Composite(x).$$

Theorem 5. *The theory $S^1_2 + \Phi$ implicitly defines factoring, i.e. it proves the sequent:*

$$(p, q, p', q' \in Pratt), p \le q, p' \le q', p \cdot q = a, p' \cdot q' = a \longrightarrow p = p' \wedge \ q = q' \ .$$

Proof.
We first show in $S^1_2 + \Phi$ the following

Claim: $(Pratt(p) \wedge p|ab) \ \to \ (p|a \vee p|b)$.

Assume $Pratt(p)$ and $p|ab$ but that p does not divide a. Then (a,p) (which is definable in S^1_2) must be equal to 1 by Φ and we get (also in S^1_2)

$$pu + av = 1$$

for some u, v, and so also:

$$pub + avb = b \ .$$

By $p|ab$, p divides the left-hand side and hence $p|b$ as well. This proves the claim.
To prove the theorem let

$$pq = p'q' \ .$$

Then $p|p'q'$ and by the claim $p|p'$ or $p|q'$. But, by Φ, this implies that $p = p'$ or $p = q'$. The same holds for q and, by the assumption $p \leq q$ and $p' \leq q'$, we get $p = p'$ and $q = q'$.

□

Corollary 6. *Unless factoring is in $\mathcal{P}/poly$, not all Δ_1^b-implications provable in $S_2^1 + \Phi$ admit an interpolant in $\mathcal{P}/poly$.*

Proof.
Recall that $Pratt(a)$ is the Σ_1^b-formula $\exists w \leq t(a), C(a, w)$. Denote by $D(a, w)$ the Δ_1^b-formula $(w \leq t(a) \wedge C(a, w))$ and by $(a)_i$ the Δ_1^b-definable function computing the i^{th} bit of a. By Theorem 5 all Δ_1^b-implications

$$D(p, u), D(q, v), p \leq q, p \cdot q = a, (p)_i = 1 \longrightarrow$$

$$\longrightarrow \neg D(p', u'), \neg D(q', v'), p' > q', p' \cdot q' \neq a, (p')_i = 1$$

(and similarly with $(q)_i$ and $(q')_i$ in place of $(p)_i$ and $(p')_i$) are provable in $S_2^1 + \Phi$. Interpolants of such implications compute bits $(p)_i$ and $(q)_i$ from a, hence one of them is not in $\mathcal{P}/poly$ unless factoring itself is in $\mathcal{P}/poly$.

□

Now we want a similar statement for the discrete logarithm.

Theorem 7. *The theory $S_2^1 + \Phi$ implicitly defines the discrete logarithm, i.e. it proves the sequent:*

$$C(p, w), y \equiv g^x \bmod p, y \equiv g^{x'} \bmod p, x < p, x' < p \longrightarrow x = x' .$$

Proof.
Assume $x - x' = r > 0$. As $g^x \equiv g^{x'} \bmod p$ we have $g^r \equiv 1 \bmod p$. By $C(p, w)$ also $g^{p-1} \equiv 1 \bmod p$ and hence also $g^s \equiv 1 \bmod p$, where $s = (r, p-1)$. Note that $s < p - 1$ as $r < p - 1$.

For all $i \leq t$ we have $(q_i^{e_i}, \frac{p-1}{q_i^{e_i}}) = 1$; we could put this condition into $C(p, w)$ but it follows from the claim in the proof of Theorem 5 and the following corollary of Φ:

Claim: $Pratt(q) \wedge a|q^u \rightarrow a = q^v$, some $v \leq u$.

If $a|q^u$ then $ab = q^u$ for some b and hence $q|ab$. By the claim from Theorem 5, $q|a$ or $q|b$. Iterating this u-times gives $a = q^v$, $b = q^{v'}$, for some v, v'.

Using a simple property of gcd available in S_2^1, namely:

$$(a, u) \cdot (a, v) = (a, u \cdot v) \text{ for } (u, v) = 1$$

we get

$$s = \Pi_{i \leq t}(r, q_i^{e_i}) .$$

We want to show that for some j it holds $(r, q_j^{e_j}) < q_j^{e_j}$. Assume, for the sake of contradiction, that $(r, q_i^{e_i}) = q_i^{e_i}$ for all $i \leq t$. Then by the above

$$s = \Pi_{i \leq t} q_i^{e_i} = p - 1$$

which contradicts to $r < p - 1$. So let $j \leq t$ be a fixed j such that $(r, q_j^{e_j}) < q_j^{e_j}$. Then $(r, q_j^{e_j}) = q_j^{f_j}$, for some $f_j < e_j$. Here we use the above claim again.
Thus we got

$$s = (\ \Pi_{i \leq t, i \neq j} (r, q_i^{e_i}) \ ) \cdot q_j^{f_j}$$

and so

$$s \cdot [\ (\ \Pi_{i \leq t, i \neq j} \frac{q_i^{e_i}}{(r, q_i^{e_i})} \ ) \cdot q_j^{e_j - f_j - 1} \ ] = \frac{p-1}{q_j}$$

as $e_j - f_j - 1 \geq 0$. That is:

$$s | \frac{p-1}{q_j} \ .$$

This yields

$$q^{\frac{p-1}{q_j}} \equiv q^{s \cdot u} \equiv 1^u \equiv 1 \text{ mod } p$$

where u is the bracket $[\ldots]$ in the equation above.

But this contradicts the condition from $C(p, w)$:

$$q^{\frac{p-1}{q_j}} \not\equiv 1 \text{ mod } p \ .$$

□

Similarly to Corollary 6 we get

Corollary 8. *Unless the discrete logarithm is in $\mathcal{P}/poly$, not all Δ_1^b-implications provable in $S_2^1 + \Phi$ admit an interpolant in $\mathcal{P}/poly$.*

It is an interesting open question to determine if Φ is provable in S_2^1. The only obstacle to a proof of Φ in S_2^1 is that we are unable to prove in S_2^1 a corollary of Fermat-Euler theorem:

$$n > 1 \wedge (y, n) = 1 \ \rightarrow \ \exists r < n, y^r \equiv 1 \text{ mod } n \ .$$

To see this assume that $p \in Pratt$ with g the primitive root of p from a witness w of the fact that $p \in Pratt$. For the sake of contradiction assume that $p \in Composite$. Then p is either a product $p = ab$ of two coprime a, b or p is a power $p = a^\ell$ of some $a \notin Composite$ and $\ell \geq 2$ (this is obtained in S_2^1 by looking at a decomposition $p = a \cdot b$ with a of the minimal possible length, employing the claim from the proof of Theorem 7). The corollary of Fermat-Euler theorem would then imply that the orders of g modulo a and b are $r < a$ and $s < b$ respectively. Hence the order of g modulo p is at most $rs \leq (a-1)(b-1) < p-1$ in the case $p = ab$, and at most $ra^{\ell-1} \leq (a-1)a^{\ell-1} < p - 1$ in the case $p = a^\ell$. This contradicts the assumption that g is a primitive root of p.

Note that by Theorem 3 it is unlikely that the above corollary of Fermat-Euler theorem is provable in S_2^1. However, it is provable in T_2^3 (see [23] or [9]). Hence we get the following statement.

Corollary 9. *Unless factoring and the discrete logarithm are in* $\mathcal{P}/poly$ *, not all* Δ_1^b*-implications provable in* T_2^3 *admit an interpolant in* $\mathcal{P}/poly$ *.*

3 Bounds to interpolation theorem for EF

We shall discuss the relation of the above example to a question on interpolation theorems for propositional proof systems studied in [10], and a question of [28] on separating certain pairs of $\mathcal{NP}$ -sets associated with propositional proof systems.

Let us rephrase the first question. Let a propositional proof system P be given. The problem is to determine the complexity of the function $F(d,x)$ which for a proof d of a sequent $\Phi(\bar{p},\bar{q}) \to \Psi(\bar{p},\bar{r})$ and a truth assignment x for $\bar{p}$

- gives 1, if $\exists y \Phi(x,y)$ and
- gives 0, if $\exists z \neg\Psi(x,z)$.

The relation to interpolation theorems is the following. If we fix the sequent and the proof, then

$$\Phi(x,y) \to (F(d,x)=1) \to \Psi(x,z).$$

Thus $F(d,\bar{p})=1$ is like an interpolant. If, in particular, F is in $\mathcal{NC}_1/poly$, then we get an interpolation formula whose size is polynomial in the size of d; if F is in $\mathcal{P}/poly$, then we get an interpolation circuit of polynomial size.

Razborov [28] proposed to study the following pair of disjoint $\mathcal{NP}$ -sets for a proof system P:

$$SAT^* =_{df} \{(\Theta, 1^t); \Theta \text{ is a satisfiable CNF}\},$$

$$REF(P) =_{df} \{(\Theta, 1^t); \Theta \text{ is a CNF and } \neg\Theta \text{ has a } P\text{-proof of length } t\}.$$

(1^t is just a padding of length t.) The problem is: what can be the complexity of a separating set?

We observe that these problems are essentially equivalent. In fact, their equivalence as well as the completeness result for this pair follow simply from known relations between bounded arithmetic and propositional logic (see [10]). For the reader not familiar with those relations we sketch a direct argument.

Let us agree that we shall omit the restriction of being CNF in the definition of SAT^* and $REF(P)$ and, instead, let us take all formulas in some complete basis.

First suppose that we can effectively separate SAT^* and $REF(P)$. We shall show how to interpolate a sequent $\Phi(\bar{p},\bar{q}) \to \Psi(\bar{p},\bar{r})$ with a proof d of length t. Let an assignment a for $\bar{p}$ be given. Consider the formula $\neg\Psi(a,\bar{r})$. If it is satisfiable, then our procedure for separating SAT^* and $REF(P)$ will tell us that and we put $F(d,a)=0$. If, on the other hand, $\Phi(a,\bar{q})$ is satisfiable, then we get a proof of $\Psi(a,\bar{r})$ at most polynomially longer than d, since we only need to evaluate $\Phi(a, \bar{q})$ on the satisfying assignment and then apply the proof of the sequent. Thus our procedure will tell us the answer also in this case.

For the converse we have to assume that the proof system P is sufficiently strong, namely, that it proves instances of its own Reflection Principle by proofs of polynomial size. This is true for EF and its various extensions; if stated carefully, it can be proved also for some (apparently) weaker systems, see [9].

So assume that we can effectively compute an interpolation function $F(d, x)$. Let a formula Θ of length n be given. Consider the reflection principle for $\neg\Theta$:

$$Prf_P^{t,n}(\lceil \neg\Theta \rceil, \bar{q}) \rightarrow \neg\Theta,$$

where the propositional variables $\bar{q}$ encode proofs of length t and $\lceil \neg\Theta \rceil$ is a truth assignment which encodes $\neg\Theta$. Thus the sets of variables of the formulas in the sequent are disjoint, hence F depends only on the proof d of this sequent, which is of polynomial size in t and n. If Θ is satisfiable, then the negation of the consequent is satisfiable, hence $F(d) = 0$; if $\neg\Theta$ has a proof of size $\leq t$, then the antecedent is satisfiable, hence $F(d) = 1$. Thus we can effectively separate SAT^* and $REF(P)$.

Let us note, that the above argument shows that the most difficult sequent for P, from the point of view of interpolation, is

$$Prf_P^{t,n}(\bar{p}, \bar{q}) \rightarrow SatNeg^n(\bar{p}, \bar{r}),$$

where $SatNeg^n(\bar{p}, \bar{r})$ expresses that the negation of the formula coded by $\bar{p}$ is satisfied on the truth assignment coded by $\bar{r}$.

The interest in this problem stems from the fact that an upper bound for interpolation for P can yield a lower bound to the size of P-proofs. The idea, discussed in [8, Sec.5] and implemented for independence results for bounded arithmetic in [27] and for lower bounds for propositional logic in [10], is to prove an upper bound on the complexity of an interpolation function F for a proof system P, and then find a pair of disjoint $\mathcal{NP}$ -sets, which are harder to separate than it is to compute F. The natural encoding of the disjointness condition for the pair thus gives a sequent which cannot have a short P-proof.

On the other hand, if such a sequent does have a short P-proof then one gets a lower bound for the interpolation function for P. In this way Theorem 1 gives:

Corollary 10. *Assuming that RSA is secure against an adversary computing functions in $\mathcal{P}/poly$, no interpolation function for EF is in $\mathcal{P}/poly$, i.e., there is a sequence of sequents which have polynomial size EF-proofs, but do not have polynomial size interpolation circuits.*

Proof.

Let $\exists x, d, r\ \alpha_i(n, e, y, x, d, r)$ be the Σ_1^b-formulas defining A_i, $i = 0, 1$, from Section 1. Since S_2^1 proves

$$\exists x, d, r\ \alpha_0(n, e, y, x, d, r) \rightarrow \neg\exists x, d, r\ \alpha_1(n, e, y, x, d, r),$$

and it is a Π_1^b-formula, the translations of this formula into propositional calculus have polynomial size EF-proofs (see [5, 14] or [9, Chpt.9]). If RSA is secure, we cannot interpolate them by polynomial size circuits.

$\square$

The above result means that effective interpolation very likely fails for EF and for stronger systems. Still, it is possible that some weaker version of it is true. In particular, we may replace the condition of non-separability of a disjoint $\mathcal{NP}$ -pair A, B by a set in $\mathcal{P}/poly$ by the following weaker condition: the pair cannot be separated by a pair of disjoint $co\mathcal{NP}$ -sets. That is, there are no disjoint $co\mathcal{NP}$ -sets $A' \supseteq A$ and $B' \supseteq B$. Our example based on RSA does not rule out this version, as A, B are complements of each other so both are $co\mathcal{NP}$ already.

For a proof system P this weaker form of effective interpolation follows easily from what we shall call an *effective disjunction property*:

> *There exists a polynomial $p(x)$ such that whenever α and β are two formulas without a common atom and such that the disjunction $\alpha \vee \beta$ has a P-proof of size m, then one of α, β has a P-proof of size at most $p(m)$.*

Cut-free sequent calculus, resolution and cutting planes (which all have effective interpolation) admit effective disjunction property. We do not know whether it holds for F or EF. Some limitations to it are pointed out in [13].

Note that in [8] it was shown that constant depth Frege systems do not admit $\mathcal{NC}^1$-bound for interpolation unless $\mathcal{P}/poly \subseteq \mathcal{NC}^1$. The next corollary answers a question of [28].

Corollary 11. *Assuming that RSA is secure against an adversary computing functions in a class $\mathcal{C}$ closed under polynomial time reductions, the pair of $\mathcal{NP}$ -sets $(SAT^*, REF(EF))$ cannot be separated by a set in $\mathcal{C}$.*

Proof.

This follows from the discussion above, or using Razborov's completeness result [28] as follows. Represent the sets A_i in V_1^1 using sets encoding the binary representations of numbers. Then, by RSUV-isomorphism [30], we get from Proposition 1:

$$V_1^1 \vdash A_0 \cap A_1 = \emptyset.$$

Since $(SAT^*, REF(EF))$ is complete for such provably disjoint $\mathcal{NP}$-sets, (A_0, A_1) can be reduced to it and we get the corollary. $\square$

4 A problem about EF

Propositions of section 2 show that it is quite important to determine whether the formula Φ is provable in S_2^1 . In fact, for those propositions it would be sufficient to have any $\mathcal{NP}$ -definition of primes (in $\mathbf{N}$) about which S^1_2 can prove that no such prime is composite. The condition $C(p,w)$ in the sequent in Theorem 7 would be then replaced by the conjunction of the first three conditions of $C(p,w)$ together with $\bigwedge_{i<t} w_i \leq t(q_i) \wedge D(q_i, w_i)$, where $D \in \Delta^b_1$ and $\exists w \leq t(a) D(a,w)$ is such an $\mathcal{NP}$ -definition of primes.

The following simple theorem shows that the existence of such a formula is equivalent to a polynomial upper bound on the lengths of EF proofs of primality.

Theorem 12. *The following two propositions are equivalent:*

1. *There is a Σ^b_1-formula $A(a)$ such that:*
   (a) $\{p \in \mathbf{N} \mid A(p)\}$ is the set of primes.
   (b) $S^1_2 \vdash A(a) \to \neg Composite(a)$.
2. *The tautologies τ_p:*
$$\tau_p := \|\neg Composite(a)\|^n(\tilde{p})$$
   (a natural propositional translation of the Π^b_1-sentence $\neg Composite(p)$) have polynomial size EF-proofs for all primes p.

Proof.
If 2. holds then the Σ^b_1-formula formalizing that τ_p has an EF-proof of size $\leq poly(|p|)$, suitable $poly$, satisfies condition 1., as EF is provably sound in S^1_2 .

On the other hand, having A satisfying 1. construct an EF-proof of τ_p as follows. Take a witness to $A(p)$ and prove that $A(p)$ holds, and combine this by modus ponens with a polynomial size EF-proof of the translations of $A(p) \to \neg Composite(p)$, getting just τ_p. For details of the translations see [14] or [9].

□

Hence we have a very interesting problem:

Problem: *Do the tautologies τ_p admit polynomial size EF-proofs?*

We do not know any lower bounds for the tautologies in any proof system. Corollary 9 implies that τ_p have polynomial size G_3-proofs, where G_3 is a fragment of the quantified propositional calculus corresponding to T^3_2 in the same way as EF corresponds to S^1_2 (see [15, 9]).

Acknowledgements

We thank S.Buss, S.Cook and A.A.Razborov for their comments on the preliminary version of this paper. We thank D. Mundici for pointing to us some references to his earlier work.

A preliminary version of this paper has appeared in: *Logic and Computational Complexity* (Proc. of the meeting held in Indianapolis, October 1994), Ed. D. Leivant, Springer-Verlag, Lecture Notes in Computer Science, Vol. **960**, (1995), pp.210-220.

References

1. W.B. Alexi, B.Chor, O. Goldreich, C.P. Schnorr (1988) *RSA and Rabin functions: Certain parts are as hard as the whole,* SIAM J. Comp., 17, pp.194-209.
2. Bonet, M. L., Pitassi, T., and Raz, R. (1994) Lower bounds for cutting planes proofs with small coefficients, preprint.
3. S.R. Buss (1986) *Bounded Arithmetic,* Bibliopolis.
4. Clegg, M., Edmonds, J., and Impagliazzo, R. (1996) Using the Groebner basis algorithm to find proofs of unsatisfiability, in: *Proc. the 28th Annual ACM Symp. on Theory of Computing*, ACM Press, pp.174-183.
5. Cook, S. A. (1975) *Feasibly constructive proofs and the propositional calculus,* in: *Proc.* 7^{th} *Annual ACM Symp. on Theory of Computing*, pp. 83-97. ACM Press.
6. Cook, S. A., and Reckhow, A. R. (1979) The relative efficiency of propositional proof systems, *J. Symbolic Logic*, **44(1)**: 36-50.
7. Krajíček, J. (1993) *Fragments of bounded arithmetic and bounded query classes*, Transactions of the A.M.S., **338(2)** : 587-598.
8. ——— (1994) *Lower bounds to the size of constant-depth propositional proofs,* Journal of Symbolic Logic, **59(1)**:73-86.
9. ——— (1995) *Bounded arithmetic, propositional logic and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, *Cambridge University Press*, Cambridge - New York - Melbourne.
10. ——— (1994) *Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, J. Symbolic Logic*, to appear.
11. ——— (1996) *Discretely ordered modules as a first-order extension of the cutting planes proof system*, submitted.
12. ——— (1996) *Interpolation by a game*, submitted.
13. ——— (1997) *On methods for proving lower bounds in propositional logic*, in: *The Tenth International Congress of Logic, Methodology and Philosophy of Science*, Florence (August 19-25, 1995), Eds. M. L. Dalla Chiara, K. Doets, D. Mundici, J. van Benthem, Vol. 1 (*Logic and Scientific Methods*), Kluwer Academic Publ., Dordrecht, pp.69-83.
14. Krajíček, J., and Pudlák, P. (1989) *Propositional proof systems, the consistency of first order theories and the complexity of computations,* J. Symbolic Logic, **54(3)**:1063-1079.
15. ——— (1990) *Quantified Propositional Calculi and Fragments of Bounded Arithmetic*, Zeitschr. f. Mathematische Logik u. Grundlagen d. Mathematik, Bd. 36(1), pp. 29-46.
16. Krajíček, J, Pudlák, P, and Takeuti, G. (1991) *Bounded arithmetic and the polynomial hierarchy,* Annals of Pure and Applied Logic, **52**: 143–153.
17. Mundici, D. (1982) Complexity of Craig's interpolation, *Fundamenta Informaticae*, **5**, pp.261-278.
18. ——— (1983) A lower bound for the complexity of Craig's interpolants in sentential logic, *Archiv fur Math. Logik*, **23** : 27-36.
19. ——— (1984) Tautologies with a unique Craig interpolant, uniform vs. non-uniform complexity, *Annals of Pure and Applied Logic*, **27**, pp.265-273.
20. ——— (1984) NP and Craig's interpolation theorem, Proc. *Logic Colloquium 1982*, North-Holland, pp. 345-358.
21. Papadimitriou, A. (1994) *Computational complexity*, Addison-Wesley.

22. Paris, J, and Wilkie, A. (1985) *Counting problems in bounded arithmetic*, in: Methods in Mathematical Logic, LNM 1130, pp.317-340.Springer.
23. Paris, J. B., Wilkie, A. J., and Woods, A. R. (1988) Provability of the pigeonhole principle and the existence of infinitely many primes, *Journal of Symbolic Logic*, **53**: 1235–1244.
24. Pratt, V.R. (1975) *Every prime has a succinct certificate*, SIAM J. Computing, **4**:214-220.
25. Pudlák, P. (1995) Lower bounds for resolution and cutting planes proofs and monotone computations, *J. Symbolic Logic*, to appear.
26. Pudlák, P. and Sgall, J. (1996) Algebraic models of computation, and interpolation for algebraic proof systems, submitted.
27. A.A. Razborov (1995) Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestiya of the R.A.N.*, **59(1)**, pp.201-224.
28. ——— (1994) *On provably disjoint NP-pairs,* Basic Research in Computer Science Center, Aarhus, RS-94-36, preprint.
29. M. Rivest, A. Shamir and L. Adleman (1978) *A method of obtaining digital signatures and public-key cryptosystems.* ACM Communications 21, pp. 120-126.
30. G. Takeuti (1992) *RSUV isomorphism,* in Arithmetic, Proof Theory and Computational Complexity, Clote and Krajíček eds., Oxford Univ. Press, pp. 364-386.