A note on Natural Proofs and Intuitionism*

Kaveh Ghasemloo
University of Toronto

Ján Pich
Charles University in Prague

1 Introduction

Natural proofs introduced by Razborov and Rudich [11] can be used to obtain a conditional unprovability of circuit lower bounds in theories admitting certain interpolation properties. Similar interpolation properties are known to hold in intuitionistic logic. We discuss what consequences this has for the provability of circuit lower bounds in intuitionistic theories.

2 Formalization

We work in first-order theories with the usual language of arithmetic containing symbols 0, S, $+$, $\cdot$, $=$, $\leq$. To encode reasoning about computation it is natural to consider also symbols $\lfloor x/2 \rfloor$, $|x|$ for the length of binary representation of x, and $\#$ with the intended meaning $x\#y = 2^{|x|\cdot|y|}$. All theories we consider contain a set of BASIC axioms capturing the usual properties of these symbols, cf. [2].

One of the most important theories we investigate is S^1_2 which is a fragment of Peano arithmetic consisting of BASIC axioms and polynomial induction:

$$A(0) \wedge \forall x(A(\lfloor x/2 \rfloor) \rightarrow A(x)) \rightarrow \forall x A(x)$$

for all Σ^b_1-formulas A.

Here Σ^b_1-formulas are formulas constructed from sharply bounded formulas by means of $\vee, \wedge$, sharply bounded, and existential bounded quantifiers where

*The major part of this research was done during a special MALOA semester in Logic and Complexity in Prague, 2011.

sharply bounded quantifiers are $\exists x \leq |t|$ or $\forall x \leq |t|$ for x not occurring in term t, existential bounded quantifiers are $\exists x \leq t$ for x not occurring in t, and sharply bounded formulas are formulas with all quantifiers sharply bounded. Analogously, Π^b_1-formulas are negations of Σ^b_1-formulas. All NP resp. coNP properties are Σ^b_1-definable resp. Π^b_1-definable, see [7, 13, 14].

For any k, denote by $Comp_{|y|^k}(C, w, y) \rightarrow C(y) \neq x$ a sharply bounded formula with free variables C, w, x, y defining the relation "If C encodes an $|y|^k$-size circuit with $|y|$ inputs, one output and w is computation of C on input y, then C on y does not output x". See Appendix for the details.

Then for any k we define $LB_{tt}(f, n^k)$ as

$$\forall C, W\ \exists y \leq |f|\ (Comp_{|y|^k}(C, [W]_y, y) \rightarrow C(y) \neq f(y))$$

where f is a free variable representing truth table of a function on $n = |y|$ variables, so $|f| = 2^n$, $f(y)$ is f_y, the y-th bit of f, and $[W]_y$ is the y-th element of a sequence of strings encoded in W (possibly computations of C on all inputs of size $||f||$).

Next, we write $LB_{tt}(SAT, n^k)$ for

$$\forall C, W\ \exists y \leq |f|\ ((f(y) = 1 \leftrightarrow \exists z, |z| \leq |y| SAT(y, z)) \rightarrow (Comp_{|y|^k}(C, [W]_y, y) \rightarrow C(y) \neq f(y)))$$

where $SAT(y, z)$ says that "y encodes a propositional formula satisfied by z". All quantifiers in $SAT(y, z)$ can be bounded by $|f|$, see Appendix. Analogously define $LB_{tt}(f \oplus SAT, n^k)$.

$LB_{tt}(f, n^k)$ is universal closure of a sharply bounded formula. Moreover, $\forall C, \forall W$ are bounded quantifiers. The same is true for $LB(SAT, n^k)$ and $LB_{tt}(f \oplus SAT, n^k)$. Note also that even subexponential circuit lower bounds (with the precise bound depending on the details of the encoding of circuits) can be expressed in this way as universal closured of sharply bounded formulas by choosing different bounds on size of C, W.

3 Feasible interpolation and feasible disjunction property

We say that a first-order theory T admits **feasible interpolation property** (FIP) if whenever $T \vdash A(x) \vee B(x)$ for Π^b_1-formulas A, B with free variable x, there are poly-size circuits $C_n, n \geq 1$ which for each a of size $|a| = n$ find a true statement among $A(a), B(a)$.

Theorem 1 (Razborov [10], Krajíček [8]). [1] *If there is a strong pseudorandom generator, then for any sufficiently big k, no sufficiently strong theory admitting FIP proves $LB_{tt}(SAT, n^k)$.*

For a definition of strong pseudorandom generator see [11]. By a sufficiently strong theory we mean a theory that can

1. define $x \oplus y$ (the bit-wise sum mod 2) from x and y
2. prove that if circuit C outputs y and circuit D outputs $x \oplus y$ then circuit $C \oplus D$ outputs x

The second condition means that we can concatenate two strings (the instructions of $C \oplus D$ are the instructions of C concatenated with the instructions of D and finitely many instructions defining the output of the form $x \oplus y$) so that the i-th bit of $C \oplus D$ is the i-th bit of C if $i \leq |C|$ and the $(|C| + i)$-th bit of $C \oplus D$ is the i-th bit of D if $i \leq |D|$. Again, the precise formulation depends on the encoding of circuits.

To obtain a sufficiently strong theory it suffices to have the least number principle for sharply bounded formulas with BASIC or simply extend the language by symbol $\oplus$ and a symbol for concatenation together with adding basic axioms defining their properties.

Krajíček-Pudlák [9] (Theorem 1) showed that if S^1_2 has FIP then factoring is easy. Therefore, it might be useful to consider a different form of interpolation:

A first-order theory T admits **feasible disjunction property** (FDP) if there is a polynomial p s.t. whenever $T \vdash A(x) \vee B(x)$ for Π^b_1-formulas A, B with free variable x, then for each a there is a $p(|a|)$-size T-proof of $A(I_a)$ or a $p(|a|)$-size T-proof of $B(I_a)$ where I_a is the binary numeral for a, i.e. $I_0 = 0, I_{2n} = 2I_n$ and $I_{2n+1} = 2I_n + 1$.

[1] This is a simplified version capturing the essence of Razborov's result who obtained it for theory $S^2_2(\alpha)$. Krajíček [8] found a simpler proof using FIP.

Theorem 2 (Rudich [12]). [2] *If there is a super-bit, then for any sufficiently big k, no sufficiently strong theory admitting FDP proves $LB_{tt}(SAT, n^k)$.*

In order to use FDP Rudich needed to assume the existence of super-bits:

A P/poly function $g_n : \{0,1\}^n \mapsto \{0,1\}^{n+1}$ is a super-bit if and only if for some ϵ, for all non-deterministic circuits C of size $S \leq 2^{n^\epsilon}$:

$$Prob_y[C(y) = 1] - Prob_x[C(g_n(x)) = 1] < 1/S$$

It is not known whether FDP (e.g. in S_2^1) breaks any hardness assumption.

The mentioned unprovability results use Razborov's trick which says that if we know that SAT_n does not have n^k size circuits, then for any function f on n variables we know that f or $f \oplus SAT_n$ is hard for $n^{k/3}$-size circuits where $f \oplus SAT_n$ is bitwise sum of the truth table of f and the truth table of SAT_n. Therefore, at least half of functions f on n variables need circuit of size $> n^{k/3}$.

If the trick is performed in any theory T with FIP resp. FDP, then

$$T \vdash LB_{tt}(f, n^{k/3}) \vee LB_{tt}(f \oplus SAT, n^{k/3})$$

implies that we have P/poly resp. NP/poly circuits which for at least half of functions f represented by their truth tables recognize that $f \notin$SIZE$(n^{k/3})$ and never accept f in SIZE$(n^{k/3})$. Such properties are called *P/poly* resp. *NP/poly* natural against SIZE$(n^{k/3})$, [11, 12]. Proofs that imply the existence of such properties are informally called natural proofs. By [11] and [12], if k is sufficiently big, their existence breaks pseudorandom generators resp. super-bits what leads to the conditional unprovability.

4 Intuitionism

FDP is similar to disjunction property which usually holds in intuitionistic theories. In fact, whenever $A(x) \vee B(x)$ is provable in intuitionistic predicate logic, for each a we can efficiently extrapolate an intuitionistic proof of $A(a)$ or an intuitionistic proof of $B(a)$:

[2] Originally formulated in terms of propositional logic with $n^{\log n}$ bound on SAT.

Theorem 3 (Disjunction property)**.** *If $A \vee B$ is provable in intuitionistic predicate logic, then at least one of A and B is derivable in it (even if A, B share variables).*

Corollary 1. *Intuitionistic predicate logic admits FDP and FIP.*

Proof: If d is a proof of $A(x) \vee B(x)$ in intuitionisti predicate logic, then there is a proof of $A(x)$ or of $B(x)$. It might be much longer than d but it is fixed. W.l.o.g. assume it proves $A(x)$, then for each a of size n we obtain a proof of $A(a)$ just by substitution, hence in linear time. □

Intuitionistic predicate logic can be extended by certain admissible rules that do not help to derive new theorems. One of them is Kreisel-Putnam rule which having $\neg T \to A \vee B$ allows us to derive $(\neg T \to A) \vee (\neg T \to B)$. Therefore, we have FDP in intuitionistic theories where any proof can be seen as a derivation in intuitionistic predicate logic from some axioms of the form $\neg T$. This does not give us FDP in interesting intuitionistic theories which do not seem to have this property, see e.g. iS^1_2 below. Also $T \to (A \vee B)$ does not seem to imply $(T \to A) \vee (T \to B)$ in intuitionistic predicate logic even if A, B are sharply bounded and do not share any variables.

Nevertheless, we have FIP in intuitionistic S^1_2, shortly IS^1_2, which is defined as S^1_2 but with intuitionistic predicate logic and polynomial induction only for Σ^{b+}_1-formulas: Σ^b_1-formulas that do not contain implication or negation signs, cf.[4].

Theorem 4 (Buss [4], Cook-Urquhart [6])**.** [3] *If $IS^1_2 \vdash \exists y A(x, y)$ where A is an arbitrary formula, then there is a p-time function f such that $A(x, f(x))$ holds for any x. Moreover, there is a Σ^{b+}_1 formula $B(x, y)$ such that IS^1_2 proves:*
(1) $\forall x, y(B(x, y) \to A(x, y))$
(2) $\forall x, y, z(B(x, y) \wedge B(x, z) \to y = z)$
(3) $\forall x \exists y B(x, y)$
and there are poly-time functions f, g such that for each n, $g(n)$ s the Godel number of an IS^1_2 proof of $A(I_a, I_{f(a)})$. Here the Godel number is efficient meaning that the length of the Godel number of a proof is bounded by a polynomial in the length of the proof.

[3] Buss proved the theorem without the "moreover" part which was obtained by Cook and Urquhart.

S. Buss also pointed out that IS^1_2 admits FIP and E. Jeřábek noticed that IS^1_2 admits FDP too (private communication).

Corollary 2. *IS^1_2 has FIP and FDP.*

Proof: If $IS^1_2 \vdash A(x) \vee B(x)$ then
$IS^1_2 \vdash \exists y \leq 1(y = 0 \to A(x)) \wedge (y \neq 0 \to B(x))$ because
$IS^1_2 \vdash A(x) \to \exists y \leq 1(y = 0 \to A(x)) \wedge (y \neq 0 \to B(x))$ and
$IS^1_2 \vdash B(x) \to \exists y \leq 1(y = 0 \to A(x)) \wedge (y \neq 0 \to B(x))$. Therefore, Buss's theorem gives us a p-time function witnessing y and FIP in IS^1_2.
Moreover, according the Cook-Urquhart part of Theorem 4
there is a Σ^{b+}_1-formula $C(x, y)$ such that
$IS^1_2 \vdash C(x, y) \to (y = 0 \to A(x)) \wedge (y \neq 0 \to B(x))$
and there are poly-time functions f, g such that for each a,
$g(a)$ is an IS^1_2 proof of $C(I_a, I_{f(a)})$. It follows that for each a
there is a $p(|a|)$-size IS^1_2-proof of $A(I_a)$ or $p(|a|)$-size IS^1_2 proof of $B(I_a)$
where p is some polynomial. □

Consequently, if there is a strong pseudorandom generator, then for sufficiently big k,

$$IS^1_2 \nvdash LB_{tt}(f, n^k) \vee LB_{tt}(f \oplus SAT, n^k)$$

If we want to derive the unprovability of $LB_{tt}(SAT, n^k)$ we need to perform Razborov's trick in IS^1_2. In other words, the question is how to do Razborov's trick constructively.

For this, it would be sufficient to have Π^b_1-conservativity of S^1_2 over IS^1_2, what might remind us of similar results obtained for stronger fragments of arithmetic: PA is Π^0_2-conservative over intuitionistic PA. However, if the conservativity held, S^1_2 would admit FIP and thus factoring would be easy. Nevertheless, in [1] it is shown that S^1_2 is $\forall\Sigma^b_1$-conservative over IS^1_2. This is not sufficient for Razborov's trick where the conservativity is needed for a disjunction of Π^b_1-sentences, but as $LB_{tt}(SAT, n^k)$ is universal closure of a sharply bounded formula, it tells us that

Lemma 1. *If $IS^1_2 \nvdash LB_{tt}(SAT, n^k)$, then $S^1_2 \nvdash LB_{tt}(SAT, n^k)$.*

We can find many derivation rules that would allow us to perform Razborov's trick in IS^1_2 augmented by such rules but unless factoring is easy, we do not have them in IS^1_2 alone. Consider for example the following:

Definition 1 (Derivation rule R)**.** *If* $\forall x \leq t(A(x) \vee B)$ *where* A *is sharply bounded,* B *is* Π^b_1*-formula and* x *does not occur in* B*, then* $\forall x \leq tA(x) \vee B$

Denote IS^1_2 with this rule by IS^1_2*.

Proposition 1. *If* $IS^1_2* = IS^1_2$ *and there is a strong pseudorandom generator then for any sufficiently big* k*,* $S^1_2 \nvdash LB_{tt}(SAT, n^k)$*.*

Proof: If $S^1_2 \vdash LB_{tt}(SAT, n^k)$, then since Razborov's trick is doable in S^1_2
$S^1_2 \vdash \forall C, W, C', W'\ (\exists y \leq |f|\ (Comp_{|y|^k}(C, [W]_y, y) \rightarrow f(y) \neq C(y)) \vee$
$\exists y \leq |f|\ ((f \oplus SAT(y) = 1 \leftrightarrow h(y) = 1) \rightarrow$
$(Comp_{|y|^k}(C', [W']_y, y) \rightarrow h(y) \neq C'(y))))$
By $\forall\Sigma^b_1$-conservativity IS^1_2 proves the same thing and since $IS^1_2 = IS^1_2*$, we can now use rule R in IS^1_2 to derive
$IS^1_2 \vdash LB_{tt}(f, n^{k/3}) \vee LB_{tt}(f \oplus SAT, n^{k/3})$
Finally, FIP in IS^1_2 produces P/poly natural property against SIZE($n^{k/3}$). □

Similar argument shows also that if $IS^1_2 = IS^1_2*$, S^1_2 admits FIP. We could try to obtain the unprovability directly in IS^1_2* without using IS^1_2. The problem is that witnessing by p-time functions seems to be broken in IS^1_2*. Maybe, however, the following kind of NP/poly witnessing analogous to FDP remains.

Definition 2 (NP/poly witnessing in IS^1_2*)**.** *If* $IS^1_2* \vdash \exists y \leq 1A(x, y)$ *for* Π^b_1*-formula* A*, then there are P/poly circuits* C *s.t. for any* x*,* $A(x, 1)$ *holds if and only if there is* z *s.t.* $C(x, z) = 1$*.*

Proposition 2. *If* IS^1_2* *admits NP/poly witnessing and there is a super-bit, then for any sufficiently big* k*,* $S^1_2 \nvdash LB_{tt}(SAT, n^k)$*.*

Proof: Assume $S^1_2 \vdash LB_{tt}(SAT, n^k)$. As in the previous proof we get
$IS^1_2* \vdash LB_{tt}(SAT, n^{k/3}) \vee LB_{tt}(f \oplus SAT, n^{k/3})$ and as in Corollary 2
$IS^1_2* \vdash \exists y \leq 1(y = 0 \rightarrow LB_{tt}(SAT, n^{k/3})) \wedge (y \neq 0 \rightarrow LB_{tt}(f \oplus SAT, n^{k/3}))$
By NP/poly witnessing we now obtain NP/poly property against SIZE($n^{k/3}$) □

5 Acknowledgement

We thank S.Buss and E.Jeřábek for useful comments and discussions. In particular, for pointing out the interpolation properties of IS^1_2.

References

[1] Avigad J.; Interpreting classical theories in constructive ones, Journal of Symbolic Logic, 65(4), 2000

[2] Buss S.R.; Bounded Arithmetic, Bibliopolis, 1986

[3] Buss S.R.; The polynomial-time hierarchy and Intuitionistic Bounded Arithmetic, Structure in Complexity 1986

[4] Buss S.R.; A note on bootstrapping intuitionistic bounded arithmetic, Proof theory: a selection of papers from the Leeds theory Programme, 1990

[5] Buss S.R., and Mints G.; The Complexity of the Disjunction and Existence properties in Intuitionistic Logic, Annals of Pure and Applied Logic, 99, 1999

[6] Cook S., and Urquhart A.; Functional Interpretations of feasibly constructive arithmetic, Annals of Pure and Applied Logic, 63, 1993

[7] Kent C.F.,and Hodgson B.R.; An arithmetic characterization of NP, Theoretical Comput. Sci., 21, 1982

[8] Krajíček, J.; Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic, J. of Symbolic Logic, 62(2), 1997

[9] Krajíček J., and Pudlák P.; Some consequences of cryptographical conjectures for S_2^1 and EF, Logic and Computational Complexity, 960, 1995

[10] Razborov A.A.; Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, Izvestiya of the R.A.N., 59(1), 1995

[11] Razborov A.A., and Rudich S.; Natural Proofs, J.Comp Sys. Sci, 55(1), 1997

[12] Rudich S.; Super-bits, demi-bits, and NP/qpoly natural proofs, Comp. Sci., 1269, 1997

[13] Stockmayer L.J.; The polynomial-time hierarchy, Theoretical Comput. Sci., 3, 1976

[14] Wrathall C.; Complete sets and the polynomial-time hierarchy, Theoretical Comput. Sci., 3, 1976

Appendix

We define here a sharply bounded formula $Comp_{|y|^k}(C, w, y) \rightarrow C(y) \neq x$ which stands for the relation "If C encodes an $|y|^k$-size circuit with $|y|$ inputs, one output and w is computation of C on input y, then C on y does not output x". C will represent a directed graph on $|w|$ vertices.

Let $E_C(i,j)$ be $C_{[i,j]}$ for pairing function $[i,j] = (i+j)(i+j+1)/2 + i$. $E_C(i,j) = 1$, $i,j < |w|$ means that there is an edge in circuit C going from the i-th vertex to the j-th vertex. For $k < |w|$, let $N_C(k)$ be the tuple of bits $(C_{[|w|,|w|]+2k}, C_{[|w|,|w|]+2k+1})$ encoding the connective in the k-th node of circuit C, say $(0,1)$ be $\wedge$, $(1,0)$ be $\vee$, and $(1,1)$ and $(0,0)$ be $\neg$. Therefore, $|C| = [|w|,|w|] + 2|w|$. Then let $Circ(C,y,w)$ be the formula stating that C encodes a $|w|$-size circuit with $|y|$ inputs:

$$\begin{array}{l}
\forall j < |w|, j \geq |y| \\
\quad (N_C(j) = (1,0) \vee N_C(j) = (0,1) \rightarrow \exists i,k < j\ i \neq k \forall l < j, l \neq k, l \neq j \\
\qquad (E_C(i,j) = 1 \wedge E_C(k,j) = 1 \wedge E_C(l,j) = 0)) \wedge \\
\quad (N_C(j) = (1,1) \vee N_C(j) = (0,0) \rightarrow \exists i < j \forall l < j, k \neq i \\
\qquad (E_C(i,j) = 1 \wedge E_C(l,j) = 0))
\end{array}$$

which means that if the j-th node of C is $\wedge$ or $\vee$, there are exactly two previous nodes i,k of C with edges going from i and k to j, if the j-th node of C is $\neg$, there is exactly one previous node i with an edge going from i to j.

$Comp_{|y|^k}(C, w, y) \rightarrow C(y) \neq x$ says that if $Circ(C,y,w)$, $|w| \leq |y|^k$, for each $i < |y|$ the value of w_i is the value of the i-th input bit of y and each w_j is an evaluation of the j-th node of circuit C given w_k's evaluating nodes connected to the j-th node, then the output of C which is chosen as $w_{|w|-1}$ differs from x:

$$\begin{array}{l}
Circ(C,y,w) \wedge |w| \leq |y|^k \wedge \forall i < |y|\ y_i = w_i \wedge \forall j,k,l < |w|[\\
(N_C(j) = (1,0) \wedge E_C(k, j=1) \wedge E_C(l,j) = 1 \rightarrow (w_j = 1 \leftrightarrow w_k = 1 \wedge w_l = 1)) \wedge
\end{array}$$

$(N_C(j) = (0,1) \wedge E_C(k,j) = 1 \wedge E_C(l,j) = 1 \rightarrow (w_j = 1 \leftrightarrow w_k = 1 \vee w_l = 1)) \wedge$
$((N_C(j) = (0,0) \vee N_C(j) = (1,1)) \wedge E_C(k,j) = 1 \rightarrow (w_j = 1 \leftrightarrow w_k = 0))]$
$\rightarrow$
$(w_{|w|-1} = 1 \wedge x \neq 1) \vee (w_{|w|-1} = 0 \wedge x \neq 0)$

$SAT(y,z)$ can be defined similarly, moreover with the evaluation w of y such that $w \leq y$.