32nd Weak Arithmetics Days
Athens, Greece

Circuit Lower Bounds in Bounded Arithmetics

Ján Pich

Charles University in Prague

June 21, 2013

Motivation Feasible witnessing of existential quantifiers in complexity-theoretic statements

e.g. Can it happen that P$\neq$NP but there is no efficient method how to witness errors of p-time algorithms attempting to solve NP problems?

Motivation Feasible witnessing of existential quantifiers in complexity-theoretic statements

e.g. Can it happen that P$\neq$NP but there is no efficient method how to witness errors of p-time algorithms attempting to solve NP problems?

p-time witnessing of $\exists$ quantifiers	„ $\Leftrightarrow$ "	provability in S^1_2

Language

$L_{bit} : 0, S, +, \cdot, =, \leq$

Language

L_{bit} : $0, S, +, \cdot, =, \leq$

$\lfloor x/2 \rfloor$

$|x|$ (the length of the binary representation of x)

$\#$ ($x \# y = 2^{|x| \cdot |y|}$)

x_i (the i-th bit of the binary representation of x)

Language

L_{bit} : $0, S, +, \cdot, =, \leq$

$\lfloor x/2 \rfloor$

$|x|$ (the length of the binary representation of x)

$\#$ $(x \# y = 2^{|x| \cdot |y|})$

x_i (the i-th bit of the binary representation of x)

Bounded quantifiers: $\exists x, x \leq t$; $\forall x, x \leq t$

Sharply bounded quantifiers: $\exists x, x \leq |t|$; $\forall x, x \leq |t|$

(t is a term not containing x)

Language

L_{bit} : $0, S, +, \cdot, =, \leq$

$\lfloor x/2 \rfloor$

$|x|$ (the length of the binary representation of x)

$\#$ ($x \# y = 2^{|x| \cdot |y|}$)

x_i (the i-th bit of the binary representation of x)

Bounded quantifiers: $\exists x, x \leq t$; $\forall x, x \leq t$

Sharply bounded quantifiers: $\exists x, x \leq |t|$; $\forall x, x \leq |t|$

(t is a term not containing x)

$\Sigma_0^b(bit)$ $(=\Pi_0^b(bit))$: L_{bit}-formulas with all quantifiers sharply bounded

$\Sigma_{i+1}^b(bit)$ formulas: constructed from $\Pi_i^b(bit)$ by sharply bounded and existential bounded quantifiers

$\Pi_{i+1}^b(bit)$ formulas: constructed from $\Sigma_i^b(bit)$ by sharply bounded and universal bounded quantifiers

Circuit lower bounds

k, n_0 constants

$LB(SAT, n^k) \equiv$
$\quad \forall 1^n > n_0$ (shortcut for $\forall m, n$ such that $m > n_0 \wedge |m| = n$)
$\quad\quad \forall C \qquad (circuit\ with\ n\ inputs)$
$\quad\quad\quad \exists y\ (formula), a\ (assignment\ of\ \mathrm{y})\ |a| < |y| = n$
$\quad\quad\quad\quad \forall w\ (computation\ of\ C), z\ (assignment\ of\ \mathrm{y})\ |w| \leq n^k, |z| < |y|$
$\quad\quad\quad [Comp(C, y, w) \rightarrow$
$\quad\quad\quad\quad (C(y; w) = 1 \wedge \neg SAT(y, z)) \vee (C(y; w) = 0 \wedge SAT(y, a))]$

$Comp(C, y, w) \equiv$ "w is computation of circuit C on input y"
$SAT(y, z) \equiv$ "3-CNF formula y is satisfied by assignment z"
$C(y; w) = 1/0 \equiv$ "w is accepting/rejecting computation of C on input y"

Circuit lower bounds

k, n_0 constants

$LB(SAT, n^k) \equiv$
$\quad \forall 1^n > n_0$ (shortcut for $\forall m, n$ such that $m > n_0 \wedge |m| = n$)
$\quad\quad \forall C \quad (circuit\ with\ n\ inputs)$
$\quad\quad\quad \exists y\ (formula), a\ (assignment\ of$ y) $|a| < |y| = n$
$\quad\quad\quad\quad \forall w\ (computation\ of\ \ C), z\ (assignment\ of$ y) $|w| \leq n^k, |z| < |y|$
$\quad\quad\quad [Comp(C, y, w) \rightarrow$
$\quad\quad\quad\quad (C(y; w) = 1 \wedge \neg SAT(y, z)) \vee (C(y; w) = 0 \wedge SAT(y, a))]$

$Comp(C, y, w) \equiv$ "w is computation of circuit C on input y"
$SAT(y, z) \quad\quad \equiv$ "3-CNF formula y is satisfied by assignment z"
$C(y; w) = 1/0 \equiv$ "w is accepting/rejecting computation of C on input y"

$Comp, SAT, C(y; w) = 1/0$ are $\Sigma_0^b(bit) \Rightarrow LB(SAT, n^k)$ is $\Sigma_2^b(bit)$

Theory $S_2^1(bit)$

axioms: BASIC(bit) (capturing basic properties of symbols of L_{bit})
polynomial induction for $\Sigma_1^b(bit)$-formulas A:

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

Theory $S^1_2(bit)$

axioms: BASIC(bit) (capturing basic properties of symbols of L_{bit})
polynomial induction for $\Sigma^b_1(bit)$-formulas A:

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

Theorem (Buss '86)

$S^1_2(bit) \vdash \exists y A(x, y)$ for $\Sigma^b_0(bit)$-formula $A \Rightarrow \exists$ p-time function f s.t. $A(x, f(x))$ holds for any x.

Theory $S^1_2(bit)$

axioms: BASIC(bit) (capturing basic properties of symbols of L_{bit})
polynomial induction for $\Sigma^b_1(bit)$-formulas A:

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

Theorem (Buss '86)

$S^1_2(bit) \vdash \exists y A(x,y)$ for $\Sigma^b_0(bit)$-formula $A \Rightarrow \exists$ p-time function f s.t. $A(x, f(x))$ holds for any x.

Theorem (Krajíček '93)

$S^1_2(bit) \vdash \exists y \forall z \leq t A(x,y,z)$ for $\Sigma^b_0(bit)$-formula $A \Rightarrow \exists$ p-time algorithm S s.t. for any x

either $\forall z \leq t A(x, S(x), z)$ or for some z_1 $\neg A(x, S(x), z_1)$

In the latter case

either $\forall z \leq t A(x, S(x, z_1), z)$ or for some z_2 $\neg A(x, S(x, z_1), z_2)$

...

after $k \leq poly(n)$ rounds $\forall z \leq t A(x, S(x, z_1, ..., z_k), z)$

Equivalent formalizations of $LB(SAT, n^k)$

e.g.

$$SCE(SAT, n^k) \equiv$$
$$\forall 1^n > n_0 \forall C\ \exists y, a\ |a| < |y| = n\ \forall w, z |w| \leq n^k, |z| < |y|$$
$$SAT(y, a) \wedge (C(y; w) = z \rightarrow \neg SAT(y, z))$$

for n_0, k constants

Equivalent formalizations of $LB(SAT, n^k)$

e.g.

$$SCE(SAT, n^k) \equiv$$
$$\forall 1^n > n_0 \forall C\ \exists y, a\ |a| < |y| = n\ \forall w, z |w| \leq n^k, |z| < |y|$$
$$SAT(y, a) \wedge (C(y; w) = z \rightarrow \neg SAT(y, z))$$

for n_0, k constants

Proposition

$S^1_2(bit)$ proves

$$SCE(SAT, n^{2k}) \rightarrow LB(SAT, n^k)$$
$$LB(SAT, n^{2k}) \rightarrow SCE(SAT, n^k)$$

where n_0 is arbitrary but the same constant in the assumption and the conclusion of each implication

$LB(SAT, n^k) \in P \equiv$

$\exists$ p-time algorithm S s.t. for any n^k-size circuit C S outputs y, a s.t. $LB(C, y, a)$:

$$C(y) = 0 \wedge SAT(y, a) \ or \ C(y) = 1 \wedge \forall z \neg SAT(y, z)$$

$LB(SAT, n^k) \in P \equiv$

$\exists$ p-time algorithm S s.t. for any n^k-size circuit C S outputs y, a s.t. $LB(C, y, a)$:

$$C(y) = 0 \wedge SAT(y, a) \text{ or } C(y) = 1 \wedge \forall z \neg SAT(y, z)$$

$LB(SAT, n^k)$ has an S-T protocol with l rounds $\equiv$

$\exists$ p-time algorithm S s.t. for any function T:

S		T
n^k-size circuit C	$\longrightarrow$	y_1, a_1 s.t. either $LB(C, y_1, a_1)$ or otherwise
w_1, z_1 certifying $\neg LB(C, y_1, a_1)$	$\longleftarrow$	
having C, w_1, z_1	$\longrightarrow$	y_2, a_2 s.t. either $LB(C, y_2, a_2)$ or otherwise
w_2, z_2 certifying $\neg LB(C, y_2, a_2)$	$\longleftarrow$	
	...	
$C, w_1, z_1, ...w_l, z_l$	$\longrightarrow$	y, a s.t. $LB(C, y, a)$

Proposition

$S_2^1(bit) \vdash LB(SAT, n^k) \Rightarrow$ $LB(SAT, n^k)$ has an S-T protocol with $poly(n)$ rounds

$S_2^1(bit) \vdash SCE(SAT, n^k) \Rightarrow$ $SCE(SAT, n^k) \in P$

Proposition

$S^1_2(bit) \vdash LB(SAT, n^k) \Rightarrow$ $LB(SAT, n^k)$ has an S-T protocol with $poly(n)$ rounds

$S^1_2(bit) \vdash SCE(SAT, n^k) \Rightarrow$ $SCE(SAT, n^k) \in P$

Proposition [Atserias-Krajíček (private communication)]

$\exists$ one-way permutation secure against p-size circuits
$\exists h \in E$ hard on average for subexponential circuits

$$\Rightarrow$$

$SCE(SAT, n^k) \in$P and
$LB(SAT, n^k)$ has an S-T protocol with 1 round (1 advice of T)

Theories weaker than $S^1_2(bit)$

T_{NC^1}: true universal theory in the language containing names for all uniform NC^1 algorithms

Theorem (KPT)

$T_{NC1} \vdash \exists y A(x,y)$ for open formula $A \Rightarrow \exists$ function f in uniform NC^1 s.t. $A(x, f(x))$ holds for any x.

$T_{NC^1} \vdash \exists y \forall z A(x,y,z)$ for open formula $A \Rightarrow \exists$ functions $f_1, ..., f_k$ in uniform NC^1 s.t.
$T_{NC^1} \vdash A(x, f_1(x), z_1) \vee A(x, f_2(x, z_1), z_2) \vee .. \vee A(x, f(x, z_1, ..., z_{k-1}), z_k)$

Theories weaker than $S^1_2(bit)$

T_{NC^1}: true universal theory in the language containing names for all uniform NC^1 algorithms

Theorem (KPT)

$T_{NC1} \vdash \exists y A(x,y)$ for open formula $A \Rightarrow \exists$ function f in uniform NC^1 s.t. $A(x, f(x))$ holds for any x.

$T_{NC^1} \vdash \exists y \forall z A(x,y,z)$ for open formula $A \Rightarrow \exists$ functions $f_1, ..., f_k$ in uniform NC^1 s.t.
$T_{NC^1} \vdash A(x, f_1(x), z_1) \vee A(x, f_2(x, z_1), z_2) \vee .. \vee A(x, f(x, z_1, ..., z_{k-1}), z_k)$

$LB(SAT, n^k)$ has the form

$$\exists y \forall z A(x,y,z)$$

for an open formula A in the language of T_{NC^1}

Another formalization of circuit lower bounds

$$
\begin{aligned}
&LB_2(SAT, n^k) \equiv \\
&\quad \forall 1^n > n_0 \forall C \\
&\qquad \exists y, a, w\ |a| < |y| = n,\ |w| \le n^k \\
&\qquad\quad \forall z,\ |z| < |y| \\
&\qquad \neg Circ(C, y, w) \vee \\
&\qquad\quad (C(y; w) = 0 \wedge SAT(y, a)) \vee (C(y; w) = 1 \wedge \neg SAT(y, z))
\end{aligned}
$$

$Circ(C, y, w) \equiv$ "C encodes a $|w|$-size circuit with $|y|$ inputs"

Another formalization of circuit lower bounds

$$
\begin{array}{l}
LB_2(SAT, n^k) \equiv \\
\quad \forall 1^n > n_0 \forall C \\
\qquad \exists y, a, w \ |a| < |y| = n, \ |w| \le n^k \\
\qquad\quad \forall z, \ |z| < |y| \\
\qquad \neg Circ(C, y, w) \vee \\
\qquad\quad (C(y; w) = 0 \wedge SAT(y, a)) \vee (C(y; w) = 1 \wedge \neg SAT(y, z))
\end{array}
$$

$Circ(C, y, w) \equiv$ "C encodes a $|w|$-size circuit with $|y|$ inputs"

$T_{NC^1} \vdash LB_2(SAT, n^k) \Rightarrow$
$LB_2(SAT, n^k)$ has an NC^1 S-T protocol with $O(1)$ rounds
i.e. the algorithm S is in uniform NC^1
and it outputs y, a and also computations w
T replies just with z's

Theorem

$LB_2(SAT, n^{k+1})$ has no NC^1 S-T protocol with $O(1)$ rounds unless $SIZE(n^k) \subseteq NC^1$. Therefore, $T_{NC^1} \nvdash LB_2(SAT, n^{k+1})$ unless $SIZE(n^k) \subseteq NC^1$.

Theorem

$LB_2(SAT, n^{k+1})$ has no NC^1 S-T protocol with $O(1)$ rounds unless $SIZE(n^k) \subseteq NC^1$. Therefore, $T_{NC^1} \nvdash LB_2(SAT, n^{k+1})$ unless $SIZE(n^k) \subseteq NC^1$.

$T_{NC^1} \vdash LB(SAT, n^k) \Rightarrow$

$LB(SAT, n^k)$ has an NC^1 S-T protocol with $O(1)$ rounds
i.e. S is uniform NC^1 and it does not need to output w's

Theorem

$LB_2(SAT, n^{k+1})$ has no NC^1 S-T protocol with $O(1)$ rounds unless $SIZE(n^k) \subseteq NC^1$. Therefore, $T_{NC^1} \nvdash LB_2(SAT, n^{k+1})$ unless $SIZE(n^k) \subseteq NC^1$.

$T_{NC^1} \vdash LB(SAT, n^k) \Rightarrow$
$LB(SAT, n^k)$ has an NC^1 S-T protocol with $O(1)$ rounds
i.e. S is uniform NC^1 and it does not need to output w's

Theorem

$LB(SAT, n^{2kc})$ has no NC^1 S-T protocol with $O(1)$ rounds and $T_{NC^1} \nvdash LB(SAT, n^{2kc})$ for any $k \geq 1, c \geq 4$ unless

$\forall f \in SIZE(n^k)$ can be approximated by formulas F_n of subexponential size $2^{O(n^{2/c})}$ with subexponential advantage

$$P_x[F_n(x) = f(x)] < 1/2 + 1/2^{O(n^{2/c})}$$

see karlin.mff.cuni.cz/$\sim$pich

NC^1 S-T protocol with $O(1)$ rounds for $LB(SAT, n^{2kc})$

$\Rightarrow$

NC^1 S-T protocol finding errors of circuits of the form $f(x|J_y)$ where $f \in SIZE(n^k), x \in \{0,1\}^{n^c}$ and $x|J_y$ is a suitable map:

$$y \in \{0,1\}^n \mapsto x' \in \{0,1\}^{n^{c/2}} \quad \textit{for } x' \subseteq x$$

($f(x|J_y)$ is an n^{2kc}-size circuit with n inputs y)

$\Rightarrow$

$\exists y_1, a_1, ..., y_l, a_l$ s.t. S outputs them for many (cca $1/2^{O(n)}$ of all) x's

$\Rightarrow$

using $y_1, a_1, ..., y_l, a_l$ as nonuniform advice we can simulate the NC^1 S-T protocol by an NC^1 circuit on many inputs and approximate f