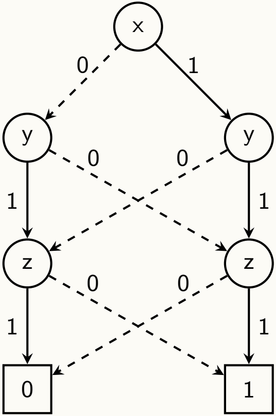
Branching Program Complexity of Canonical Search Problems and Proof Complexity of Formulas

Authors:
Alexander Knop

Institute:
UC San Diego

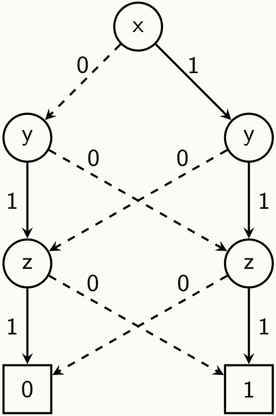
Branching Programs



Branching Programs are dag's such that:

- each node is labeled by a variable and has out-degree 2 (one edge is labeled by a 0 and one is labeled by 1);
- each leaf is labeled by an output value.

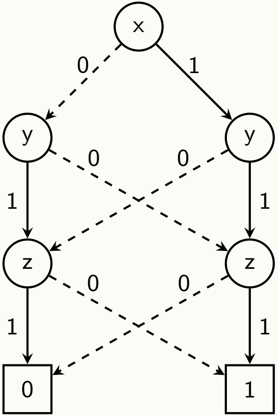
Branching Programs



A branching program is read-b if it reads each variable at most b times.

We say that a branching program is b-OBDD if it is a read-b branching program reading all the variables in the same order b times.

Branching Programs



A branching program is $(1, +b)$-BP if in every path it reads all the variables except b of them only once.

Search Problems

DEFINITION

Let $\phi = \bigwedge_{i=1}^{m} C_i$ be an unsatisfiable CNF. $\text{Search}_\phi \subseteq \{0,1\}^n \times [n]$ is a relation such that

$$(x, i) \in \text{Search}_\phi \iff C_i(x) = 0.$$

Search Problems

THEOREM (CHVÁTAL AND SZEMERÉDI, 1991)

Let $\phi = \bigwedge_{i=1}^{m} C_i$ *be an unsatisfiable CNF.*
The minimal size of a regular (ordered) resolution refutation of ϕ *is equal to the minimal size of a read-once branching program (*OBDD*) for* Search_ϕ.

Search Problems

THEOREM (CHVÁTAL AND SZEMERÉDI, 1991)

Let $\phi = \bigwedge_{i=1}^{m} C_i$ *be an unsatisfiable CNF.*
The minimal size of a regular (ordered) resolution refutation of ϕ *is equal to the minimal size of a read-once branching program (*OBDD*) for* Search_ϕ*.*

This theorem does not hold for resolution and unrestricted branching programs.

$\mathcal{C}$-IPS

DEFINITION

Let $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$. We say that an arithmetic circuit $C \in \mathcal{C}$ is a $\mathcal{C}$-**IPS** proof of the unsatisfiability of $f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0$ if

- $C(x_1, \ldots, x_n, 0, \ldots, 0) = 0$ and
- $C(x_1, \ldots, x_n, f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) = 1$.

$\mathcal{C}$-**IPS**

DEFINITION

Let $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$. We say that an arithmetic circuit $C \in \mathcal{C}$ is a $\mathcal{C}$-**IPS** proof of the unsatisfiability of $f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0$ if

- $C(x_1, \ldots, x_n, 0, \ldots, 0) = 0$ and
- $C(x_1, \ldots, x_n, f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) = 1.$

Forbes et al. considered roABP-**IPS**, the proof system where C is a read-once oblivious algebraic branching program.

$\mathcal{C}$-**PS**$_1$

DEFINITION

Let $\phi = \bigwedge_{i=1}^{m} F_i$. We say that a branching program $C \in \mathcal{C}$ (C depends on $x_1, \ldots, x_n, y_1, \ldots, y_m$) is a $\mathcal{C}$-**PS**$_1$ refutation of ϕ if

- $C(x_1, \ldots, x_n, 1, \ldots, 1) = 1$,
- $C(x_1, \ldots, x_n, F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)) = 0$, and
- on any path in C all the variables $y_1, \ldots, y_m$ occur altogether at most once.

Search Problems

THEOREM

Let $\phi = \bigwedge_{i=1}^{m} C_i$ *be an unsatisfiable CNF.*
The minimal size of a $(1, +k)$-BP-$\mathbf{PS}_1$ *(*k-OBDD-$\mathbf{PS}_1$*) refutation of* ϕ *is polynomially related to the minimal size of a* $(1, +k)$-BP *(*k-OBDD*) for* Search_ϕ*.*

Search Problems

THEOREM

Let $\phi = \bigwedge_{i=1}^{m} C_i$ *be an unsatisfiable CNF.*
The minimal size of a $(1, +k)$-BP-**PS**$_1$ *(*k-OBDD-**PS**$_1$*) refutation of* ϕ *is polynomially related to the minimal size of a* $(1, +k)$-BP *(*k-OBDD*) for* Search$_\phi$.

Note that regular resolution (ordered resolution) is equivalent to 1-BP-**PS**$_1$ (OBDD-**PS**$_1$).

Communication Complexity I

DEFINITION

Communication complexity of $f\colon \{0,1\}^n \to \{0,1\}$ with respect to a partition Π of $[n]$ ($\mathbf{D}(f,\Pi)$) is the minimal number of bits Alice and Bob need to send to each other to compute $f(x)$ if Alice knows only bits of x with indices from Π_0 and Bob knows only bits of x with indices from Π_1.

Communication Complexity I

DEFINITION

Communication complexity of $f\colon \{0,1\}^n \to \{0,1\}$ with respect to a partition Π of $[n]$ ($\mathbf{D}(f,\Pi)$) is the minimal number of bits Alice and Bob need to send to each other to compute $f(x)$ if Alice knows only bits of x with indices from Π_0 and Bob knows only bits of x with indices from Π_1.

DEFINITION

Best communication complexity of $f\colon \{0,1\}^n \to \{0,1\}$ ($\mathbf{D}^{best}(f)$) is the minimum of $\mathbf{D}(f,\Pi)$ over Π such that $|\Pi_0 - \Pi_1| \leq 1$.

Lower Bounds I

THEOREM

If D is an b-OBDD for Search_ϕ, *then* $\mathbf{D}^{best}(\mathsf{Search}_\phi) \le (2b-1)\lceil \log|D| \rceil$.

Lower Bounds I

THEOREM

If D is an b-OBDD for Search_ϕ, then $\mathbf{D}^{best}(\mathsf{Search}_\phi) \leq (2b-1)\lceil \log|D| \rceil$.

THEOREM (GÖÖS AND PITASSI, 2014)

There are families of formulas ϕ_n in k-CNF and partitions Π_n such that $\mathbf{D}(\mathsf{Search}_{\phi_n}, \Pi_n) \geq \frac{n}{\log n}$.

Lower Bounds I

THEOREM

If D is an b-OBDD for Search_ϕ, then $\mathbf{D}^{best}(\mathsf{Search}_\phi) \le (2b-1)\lceil \log |D| \rceil$.

THEOREM (GÖÖS AND PITASSI, 2014)

There are families of formulas ϕ_n in k-CNF and partitions Π_n such that $\mathbf{D}(\mathsf{Search}_{\phi_n}, \Pi_n) \ge \frac{n}{\log n}$.

THEOREM

There is a transformation $\mathcal{T}$ such that for any large enough ϕ in k-CNF and partition Π, $|\mathcal{T}(\phi)| = \mathrm{poly}(|\phi|)$ *and* $\mathbf{D}(\mathsf{Search}_\phi, \Pi) \le \mathbf{D}^{best}\left(\mathsf{Search}_{\mathcal{T}(\phi)}\right)$.

Tseitin Formulas

DEFINITION

Let G be a connected graph on vertices V ($|V|$ is odd) with edges E. Every edge $e \in E$ has the corresponding propositional variable p_e. For every vertex $v \in V$ we write down a formula in CNF that encodes

$$\sum_{(u,v) \in E} p_{(v,u)} \equiv 1 \pmod 2.$$

The conjunction of these formulas is a Tseitin formula TS_G for the graph G.

Tseitin Formulas

DEFINITION

Let G be a connected graph on vertices V ($|V|$ is odd) with edges E. Every edge $e \in E$ has the corresponding propositional variable p_e. For every vertex $v \in V$ we write down a formula in CNF that encodes

$$\sum_{(u,v) \in E} p_{(v,u)} \equiv 1 \pmod 2.$$

The conjunction of these formulas is a Tseitin formula TS_G for the graph G.

Note that if G has small degree, then $\mathbf{D}\left(\mathrm{Search}_{\mathrm{TS}_G}\right) = O(\log |V|)$.

Communication Complexity II

DEFINITION

Communication complexity of $f\colon \{0,1\}^n \to \{0,1\}$ with respect to a partition Π of $[n]$ with k rounds ($\mathbf{D}^{(k)}(f, \Pi)$) is the minimal number of bits Alice and Bob need to send to each other to compute $f(x)$.
Their communication consists of k rounds, on each round one of them sends a string.

Communication Complexity II

DEFINITION

Communication complexity of $f\colon \{0,1\}^n \to \{0,1\}$ with respect to a partition Π of $[n]$ with k rounds ($\mathbf{D}^{(k)}(f, \Pi)$) is the minimal number of bits Alice and Bob need to send to each other to compute $f(x)$.
Their communication consists of k rounds, on each round one of them sends a string.

DEFINITION

Best communication complexity of $f\colon \{0,1\}^n \to \{0,1\}$ ($\mathbf{D}^{(k),best}(f)$) with k rounds is the minimum of $\mathbf{D}^{(k)}(f, \Pi)$ over Π such that $|\Pi_0 - \Pi_1| \leq 1$.

Lower Bounds II

DEFINITION

Let $f\colon \{0,1\}^n \to \{0,1\}$. $\mathsf{KW}(f) \subseteq (f^{-1}(1) \times f^{-1}(0)) \times [n]$ is a relation such that

$$(x, y, i) \in \mathsf{KW}(f) \iff x_i \neq y_i.$$

Lower Bounds II

DEFINITION

Let $f\colon \{0,1\}^n \to \{0,1\}$. $\mathsf{KW}(f) \subseteq (f^{-1}(1) \times f^{-1}(0)) \times [n]$ is a relation such that

$$(x, y, i) \in \mathsf{KW}(f) \iff x_i \neq y_i.$$

THEOREM (HÅSTAD, 1987)

For any $b > 0$, $\mathbf{D}^{(b)}(\mathsf{KW}(\oplus_n)) \geq n^{1/b}$.

Lower Bounds II

THEOREM (HÅSTAD, 1987)

For any $b > 0$, $\mathbf{D}^{(b)}\left(\mathsf{KW}\left(\oplus_n\right)\right) \geq n^{1/b}$.

THEOREM

There are families of graphs G_n *of constant degree and labeling functions* c_n *such that* $\mathbf{D}^{(b),best}\left(\mathsf{Search}_{\mathsf{TS}_G}\right) \geq \mathbf{D}^{(b)}\left(\mathsf{KW}\left(\oplus_{\epsilon n}\right)\right)$ *for some* $\epsilon > 0$ *and any* $b > 0$.

Lower Bounds II

THEOREM (HÅSTAD, 1987)

For any $b > 0$, $\mathbf{D}^{(b)}\left(\mathsf{KW}\left(\oplus_n\right)\right) \geq n^{1/b}$.

THEOREM

There are families of graphs G_n *of constant degree and labeling functions* c_n *such that* $\mathbf{D}^{(b),best}\left(\mathsf{Search}_{\mathsf{TS}_G}\right) \geq \mathbf{D}^{(b)}\left(\mathsf{KW}\left(\oplus_{\epsilon n}\right)\right)$ *for some* $\epsilon > 0$ *and any* $b > 0$.

THEOREM

If D *is a* b-OBDD *for* Search_ϕ, *then* $\mathbf{D}^{(2b-1),best}\left(\mathsf{Search}_\phi\right) \leq (2b-1)\lceil \log |D| \rceil$

Separation I

THEOREM (GARG ET AL, 2018)

Any **CP** *refutation of* $\phi \circ \texttt{Ind}_m$ *has size at least* $n^{w(\phi)}$*, where* $w(\phi)$ *is the minimal width of a resolution refutation of* ϕ*.*

Separation I

THEOREM (GARG ET AL, 2018)

Any **CP** *refutation of* $\phi \circ \mathtt{Ind}_m$ *has size at least* $n^{w(\phi)}$*, where* $w(\phi)$ *is the minimal width of a resolution refutation of* ϕ*.*

THEOREM (BONET AND GALESI, 2001)

There is a formula ϕ *such that* $w(\phi) = \Omega(n)$ *and there is an ordered resolution refutation of* ϕ *of size* $\mathrm{poly}(n)$*.*

Separation I

THEOREM (GARG ET AL, 2018)

Any **CP** *refutation of* $\phi \circ \mathtt{Ind}_m$ *has size at least* $n^{w(\phi)}$*, where* $w(\phi)$ *is the minimal width of a resolution refutation of* ϕ*.*

THEOREM (BONET AND GALESI, 2001)

There is a formula ϕ *such that* $w(\phi) = \Omega(n)$ *and there is an ordered resolution refutation of* ϕ *of size* $\mathrm{poly}(n)$*.*

THEOREM

If a formula ϕ *has an* OBDD-$\mathbf{PS}_1$ *refutation of size* S*, then for any gadget* $g : \{0,1\}^k \to \{0,1\}$*,* $\phi \circ g$ *has a* 2-OBDD-$\mathbf{PS}_1$ *refutation of size* $\mathrm{poly}(S, |\phi \circ g|)$*.*

Separation II

THEOREM (ALEKHNOVICH AND RAZBOROV, 2002)

Any resolution refutation of $\phi^{\oplus}$ has size at least $2^{w(\phi)}$, where $w(\phi)$ is the minimal width of a resolution refutation of ϕ.

Separation II

THEOREM (ALEKHNOVICH AND RAZBOROV, 2002)

Any resolution refutation of $\phi^{\oplus}$ has size at least $2^{w(\phi)}$, where $w(\phi)$ is the minimal width of a resolution refutation of ϕ.

THEOREM (BONET AND GALESI, 2001)

There is a formula ϕ in 3-CNF such that $w(\phi) = \Omega(n)$ but there is an ordered resolution refutation of ϕ of size $\mathrm{poly}(n)$.

Separation II

THEOREM (ALEKHNOVICH AND RAZBOROV, 2002)

Any resolution refutation of $\phi^{\oplus}$ has size at least $2^{w(\phi)}$, where $w(\phi)$ is the minimal width of a resolution refutation of ϕ.

THEOREM (BONET AND GALESI, 2001)

There is a formula ϕ in 3-CNF such that $w(\phi) = \Omega(n)$ but there is an ordered resolution refutation of ϕ of size $\mathrm{poly}(n)$.

THEOREM

If a formula ϕ has an OBDD-$\mathbf{PS}_1$ refutation of size S, then for any gadget $g : \{0,1\}^k \to \{0,1\}$, $\phi \circ g$ has a $(1, +2^k)$-BP-$\mathbf{PS}_1$ refutation of size $\mathrm{poly}(S, |\phi \circ g|)$.

Open Questions

1. Is it possible to prove a lower bound on size of $(1, +b)$-BP-$\textbf{PS}_1$ refutations of a formula ϕ for $b > 0$?

Open Questions

1. Is it possible to prove a lower bound on size of $(1, +b)$-BP-$\mathbf{PS}_1$ refutations of a formula ϕ for $b > 0$?
2. Is it possible to show that **CP** does not simulate $(1, +b)$-BP-$\mathbf{PS}_1$?

Open Questions

1. Is it possible to prove a lower bound on size of $(1, +b)$-BP-**PS**$_1$ refutations of a formula ϕ for $b > 0$?
2. Is it possible to show that **CP** does not simulate $(1, +b)$-BP-**PS**$_1$?
3. Are random 3-CNFs exponentially hard for $(1, +b)$-BP-**PS**$_1$ and k-OBDD-**PS**$_1$?