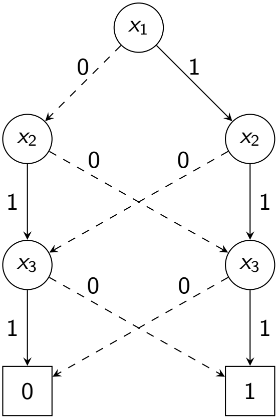
On OBDD based algorithms and proof systems that dynamically change order of variables

Dmitry Itsykson
(joint work with Alexander Knop, Andrey Romashchenko and Dmitry Sokolov)

Steklov Institute of Mathematics at St. Petersburg

May 19, 2016

Ordered binary decision diagram (OBDD)



- OBDD represents Boolean function $\{0,1\}^n \to \{0,1\}$
- π is order of variables; if $i < j$, then $x_{\pi(j)}$ can't appear before $x_{\pi(i)}$.

Operations with OBDD

Given	Compute	Complexity
D^π	whether D^π is satisfiable	$O(\|D\|)$
D^π	$(\neg D)^\pi$	$O(\|D\|)$
D_1^π, D_2^π	$(D_1 \wedge D_2)^\pi$	$O(\|D_1\| \times \|D_2\|)$
D_1^π, D_2^π	$(D_1 \vee D_2)^\pi$	$O(\|D_1\| \times \|D_2\|)$
D^π, x is a variable	$(\exists x D)^\pi$	$O(\|D\|)$
D^π, ρ	$(D\|_\rho)^\pi$	$O(\|D\|)$
$D_1^{\pi_1}, \pi_2$	$D_2^{\pi_2}$ such that $D_1^{\pi_1} \equiv D_2^{\pi_2}$	$poly(\|D_1\| \times \|D_2\|)$
D^π	min D_0^π such that $D_0 \equiv D$	$O(\|D\|)$
$D_1^{\pi_1}, D_2^{\pi_2}, D_3^{\pi_1}$	whether $D_3 \equiv D_1 \wedge D_2$	NP-hard

$D_1 \equiv D_2$ if D_1 and D_2 represents the same Boolean function.

Outline

- OBDD($\wedge$, weakening)-proof system
- Lower bounds for OBDD($\wedge$, reorder)-proof system
- Lower bounds for OBDD($\wedge, \exists$, reorder)-algorithms

OBDD(∧, weakening)-proofs

- $\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_t$ is unsatisfiable CNF.
- Choose order π; every C_i is represented as π-ordered OBDD.
- Join (conjunction) rule: $\frac{D_1^\pi, D_2^\pi}{(D_1 \wedge D_2)^\pi}$
- Weakening rule: $\frac{D^\pi}{D_1^\pi}$ if $D \models D_1$.
- Proof of unsatisfiability of ϕ: derivation a constant false OBDD.
- [Atserias, Kolaitis, Vardi, 2004] OBDD(∧, weakening) simulates CP* $\implies$ PHP_n^{n+1} has proofs of poly size.
- OBDD(∧, weakening) is stronger than Resolution
- Unsatisfiable linear systems over GF(2) have short proofs
- [Segerlind, 2007] $2^{n^{\Omega(1)}}$-lower bound for tree-like OBDD(∧, weakening)-proofs
- [Krajicek, 2008] $2^{n^{\Omega(1)}}$-lower bound for dag-like OBDD(∧, weakening)-proofs

OBDD($\wedge$, weakening)-proofs

- $\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_t$ is unsatisfiable CNF.
- Choose order π; every C_i is represented as π-ordered OBDD.
- Join (conjunction) rule: $\frac{D_1^\pi, D_2^\pi}{(D_1 \wedge D_2)^\pi}$
- Weakening rule: $\frac{D^\pi}{D_1^\pi}$ if $D \models D_1$.
- Proof of unsatisfiability of ϕ: derivation a constant false OBDD.
- [Atserias, Kolaitis, Vardi, 2004] OBDD($\wedge$, weakening) simulates CP* $\implies$ PHP_n^{n+1} has proofs of poly size.
- OBDD($\wedge$, weakening) is stronger than Resolution
- Unsatisfiable linear systems over GF(2) have short proofs
- [Segerlind, 2007] $2^{n^{\Omega(1)}}$-lower bound for tree-like OBDD($\wedge$, weakening)-proofs
- [Krajicek, 2008] $2^{n^{\Omega(1)}}$-lower bound for dag-like OBDD($\wedge$, weakening)-proofs

OBDD($\wedge$, weakening)-proofs

- $\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_t$ is unsatisfiable CNF.
- Choose order π; every C_i is represented as π-ordered OBDD.
- Join (conjunction) rule: $\frac{D_1^\pi, D_2^\pi}{(D_1 \wedge D_2)^\pi}$
- Weakening rule: $\frac{D^\pi}{D_1^\pi}$ if $D \models D_1$.
- Proof of unsatisfiability of ϕ: derivation a constant false OBDD.
- [Atserias, Kolaitis, Vardi, 2004] OBDD($\wedge$, weakening) simulates CP* $\implies$ PHP_n^{n+1} has proofs of poly size.
- OBDD($\wedge$, weakening) is stronger than Resolution
- Unsatisfiable linear systems over GF(2) have short proofs
- [Segerlind, 2007] $2^{n^{\Omega(1)}}$-lower bound for tree-like OBDD($\wedge$, weakening)-proofs
- [Krajicek, 2008] $2^{n^{\Omega(1)}}$-lower bound for dag-like OBDD($\wedge$, weakening)-proofs

OBDD($\wedge$, weakening)-proofs

- $\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_t$ is unsatisfiable CNF.
- Choose order π; every C_i is represented as π-ordered OBDD.
- Join (conjunction) rule: $\frac{D_1^\pi, D_2^\pi}{(D_1 \wedge D_2)^\pi}$
- Weakening rule: $\frac{D^\pi}{D_1^\pi}$ if $D \models D_1$.
- Proof of unsatisfiability of ϕ: derivation a constant false OBDD.
- [Atserias, Kolaitis, Vardi, 2004] OBDD($\wedge$, weakening) simulates CP* $\implies$ PHP$_n^{n+1}$ has proofs of poly size.
- OBDD($\wedge$, weakening) is stronger than Resolution
- Unsatisfiable linear systems over GF(2) have short proofs
- [Segerlind, 2007] $2^{n^{\Omega(1)}}$-lower bound for tree-like OBDD($\wedge$, weakening)-proofs
- [Krajicek, 2008] $2^{n^{\Omega(1)}}$-lower bound for dag-like OBDD($\wedge$, weakening)-proofs

OBDD($\wedge$)-proofs

- [Groote, Zantema, 2003; Tveretina et al., 2009] OBDD($\wedge$)-proof system is incomparable with resolution
- [Tveretina et al., 2009] PHP_n^{n+1} requires OBDD($\wedge$)-proofs of size $2^{\Omega(n)}$
- [Friedman, Xu, 2013] Random 3CNFs are hard for OBDD($\wedge$)-proofs in two particular cases:
  - with a fixed order of the variables
  - with fixed orders of application of rules

Reordering rule

- Reordering rule: $\frac{D_1^{\pi_1}}{D_2^{\pi_2}}$ if $D_1^{\pi_1} \equiv D_2^{\pi_2}$
- Join (conjunction) rule: $\frac{D_1^{\pi}, D_2^{\pi}}{(D_1 \wedge D_2)^{\pi}}$
- OBDD($\wedge$, reorder)-proof system:
  - We exponentially separate OBDD($\wedge$, reorder) from OBDD($\wedge$)
  - Lower bound $2^{\Omega(n)}$ for PHP_n^{n+1}.
  - Lower bound $2^{\Omega(n)}$ for Tseitin formulas.

Reordering rule

- Reordering rule: $\frac{D_1^{\pi_1}}{D_2^{\pi_2}}$ if $D_1^{\pi_1} \equiv D_2^{\pi_2}$
- Join (conjunction) rule: $\frac{D_1^{\pi}, D_2^{\pi}}{(D_1 \wedge D_2)^{\pi}}$
- OBDD($\wedge$, reorder)-proof system:
    - We exponentially separate OBDD($\wedge$, reorder) from OBDD($\wedge$)
    - Lower bound $2^{\Omega(n)}$ for PHP_n^{n+1}.
    - Lower bound $2^{\Omega(n)}$ for Tseitin formulas.

Lower bound method for OBDD($\wedge$, reorder)

Let $\Phi = \bigwedge_{i \in I} C_i$ be minimally unsatisfiable CNF

1. Φ' is a satisfiable formula associated with Φ. Roughly speaking: Φ' is Φ without several clauses.
   - For Φ=PHP_n^{n+1}, Φ'=PHP_n^n
   - For unsatisfiable Tseitin formulas, Φ' is satisfiable Tseitin formula.
2. Prove that any OBDD representation of Φ' has large size.
3. The last step: $\frac{F_1^\pi \wedge F_2^\pi}{0}$. F_1, F_2 are satisfiable and $F_1 \equiv \bigwedge_{i \in I_1} C_i, F_2 \equiv \bigwedge_{i \in I_2} C_i$ and $I_1 \neq I_2$, $I_1 \cup I_2 = I$.
4. Find partial substitution ρ_1, ρ_2 with same support: $F_1|_{\rho_1} \wedge F_2|_{\rho_2}$ is a hard satisfiable formula for OBDD. Hence either $F_1|_\rho^\pi$ or $F_2|_\rho^\pi$ is hard for OBDD, hence F_1 or F_2 is hard for OBDD.

Lower bounds for OBDD

For particular order π:

- F, $S = \{x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(\ell)}\}$.
- Let $\rho_1, \rho_2, \dots, \rho_k$ be partial substitution with support S such that $F|_{\rho_1}, F|_{\rho_2}, \dots, F|_{\rho_k}$ are different functions.
- Then every π-OBDD for F has at least k vertices.

For all orders:

- For arbitrary S that consists of ℓ variables.

Lower bounds for OBDD

For particular order π:

- F, $S = \{x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(\ell)}\}$.
- Let $\rho_1, \rho_2, \dots, \rho_k$ be partial substitution with support S such that $F|_{\rho_1}, F|_{\rho_2}, \dots, F|_{\rho_k}$ are different functions.
- Then every π-OBDD for F has at least k vertices.

For all orders:

- For arbitrary S that consists of ℓ variables.

Tseitin formulas

- $G(V, E)$ is undirected constant-degree graph;
- For every $e \in E$: x_e Boolean variable;
- $c : V \to \{0, 1\}$ labelling function
- $TS_{G,c} = \bigwedge_{v \in v} \left(\bigoplus_{u:(u,v) \in E} x_{(u,v)} = c(v) \right)$

Lemma. $TS_{G,c}$ is satisfiable iff for every connected component U, $\bigoplus_{v \in U} c(v) = 0$.

OBDD for satisfiable Tseitin formula

- Let $TS_{G,c}$ be satisfiable Tseitin formula.
- Consider some order π;
- Let S be a set that consists first ℓ edges according π
- Consider some substitution ρ with support S.
- $TS_{G,c}|_\rho = TS_{G',c+f}$, where $G'(V, E \setminus S)$ and $f : V \to \{0,1\}$ is a modification of labels made by ρ.
- Different functions: different f and $TS_{G',c+f}$ is satisfiable.
- We estimate the number of f such that
  - $TS_{G',c+f}$ is satisfiable
  - f can be obtained by a substitution $\iff$ $TS_{G'',f}$ is satisfiable, where $G''(V, S)$.
- $\sharp G' + \sharp G''$ linear conditions on f.
- Hence number of different functions at least $2^{n-\sharp G'-\sharp G''}$

OBDD for satisfiable Tseitin formula

- Let $TS_{G,c}$ be satisfiable Tseitin formula.
- Consider some order π;
- Let S be a set that consists first ℓ edges according π
- Consider some substitution ρ with support S.
- $TS_{G,c}|_{\rho} = TS_{G',c+f}$, where $G'(V, E \setminus S)$ and $f : V \to \{0,1\}$ is a modification of labels made by ρ.
- Different functions: different f and $TS_{G',c+f}$ is satisfiable.
- We estimate the number of f such that
  - $TS_{G',c+f}$ is satisfiable
  - f can be obtained by a substitution $\iff$ $TS_{G'',f}$ is satisfiable, where $G''(V, S)$.
- $\sharp G' + \sharp G''$ linear conditions on f.
- Hence number of different functions at least $2^{n-\sharp G'-\sharp G''}$

Tseitin formulas on expanders

Theorem. If $G(V, E)$ is good enough expander with $|V| = n$ then $\exists \ell$: $\forall S \subseteq E$ if $|S| = \ell$ then $\sharp G'(V, E \setminus S) + \sharp G''(V, S) \leq (1 - \epsilon)n$.

Corollary. Every OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.

Corollary. If G differs from good enough expander by at most $o(n)$ edges, then OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.

Lemma. Good enough expander is connected and remains connected after deleting of any two vertices and edges from the shortest path between them.

Tseitin formulas on expanders

Theorem. If $G(V, E)$ is good enough expander with $|V| = n$ then $\exists \ell$: $\forall S \subseteq E$ if $|S| = \ell$ then $\sharp G'(V, E \setminus S) + \sharp G''(V, S) \leq (1-\epsilon)n$.
Corollary. Every OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.

Corollary. If G differs from good enough expander by at most $o(n)$ edges, then OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.

Lemma. Good enough expander is connected and remains connected after deleting of any two vertices and edges from the shortest path between them.

Tseitin formulas on expanders

Theorem. If $G(V, E)$ is good enough expander with $|V| = n$ then $\exists \ell$: $\forall S \subseteq E$ if $|S| = \ell$ then $\sharp G'(V, E \setminus S) + \sharp G''(V, S) \leq (1 - \epsilon)n$.
Corollary. Every OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.
Corollary. If G differs from good enough expander by at most $o(n)$ edges, then OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.
Lemma. Good enough expander is connected and remains connected after deleting of any two vertices and edges from the shortest path between them.

Tseitin formulas on expanders

Theorem. If $G(V,E)$ is good enough expander with $|V| = n$ then $\exists\ell$: $\forall S \subseteq E$ if $|S| = \ell$ then $\sharp G'(V, E \setminus S) + \sharp G''(V, S) \le (1-\epsilon)n$.

Corollary. Every OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.

Corollary. If G differs from good enough expander by at most $o(n)$ edges, then OBDD representation of satisfiable $TS_{G,c}$ has size at least $2^{\Omega(n)}$.

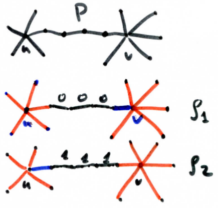
Lemma. Good enough expander is connected and remains connected after deleting of any two vertices and edges from the shortest path between them.

Lower bound for unsatisfiable Tseitin formula

Theorem. If $G(V,E)$ is good enough expander with $|V| = n$ and $TS_{G,c}$ is unsatisfiable then the size of any OBDD($\wedge$, reorder)-proof of $TS_{G,c}$ is at least $2^{\Omega}(n)$.

Proof.

- The last step: $\frac{F_1^\pi \wedge F_2^\pi}{0}$. F_1, F_2 are satisfiable.
- Let F_1 does not contains C_u and F_2 does not contain C_v and $(u,v) \notin E$
- Let P be the shortest uv-path



$F_1|_{\rho_1} \wedge F_2|_{\rho_2}$ is almost satisfiable $TS_{\tilde{G},c'}$, where $\tilde{G}(V \setminus \{u,v\}, E \setminus P)$.

OBDD($\wedge$, weakening, reorder)

Open questions:

- To separate OBDD($\wedge$, weakening, reorder)-proof system and OBDD($\wedge$, weakening)-proof system.
- Prove superpolynomial lower bound for OBDD($\wedge$, weakening, reorder)-proofs

Symbolic quantifier elimination

OBDD($\wedge, \exists$)-algorithms [Pan, Vardi, 2004] for SAT.
Input: CNF formula ϕ

1. Choose order π, D^{π}. Initially $D \equiv 1$.
2. $S := \{$clauses of $\phi\}$.
3. While $S \neq \emptyset$ apply the following operations:
   - Conjunction ($\wedge$) Choose $C \in S$; $S := S - C$; $D^{\pi} := D^{\pi} \wedge C$
   - Projection ($\exists$) If x does not appear in S, then $D^{\pi} := (\exists x D)^{\pi}$
4. If $S = \emptyset$ then report whether D is satisfiable or not.

Running time is polynomially connected with the size of the largest D.

OBDD($\wedge, \exists$)-algorithms

Upper bounds:

- [Chén, Zhang, 2009] Pigeonhole principle PHP_n^{n+1} is easy for OBDD($\wedge, \exists$)-algorithms.
- Tseitin formulas are easy for OBDD($\wedge, \exists$)-algorithms.
  - $\exists x \begin{cases} x + y + z = 1 \\ x + t + f = 0 \end{cases} \iff y + z + t + f = 1.$
  - Sum up all equalities in the connected component.

Lower bounds:

- Follows from lower bounds for (tree-like) OBDD($\wedge$, weakening)-proofs.

OBDD($\wedge, \exists$, reorder)-algorithms

- (reorder) Choose π' and $F^{\pi'}$ such that $F \equiv D$; $\pi := \pi'$ and $D := F$.

Our goals:

- Lower bounds for OBDD($\wedge, \exists$, reorder)-algorithms
- Lower bound of type $2^{\Omega(n)}$, where n is number of variables
- Lower bound for natural formulas.

Theorem. There is a randomized construction of a family of satisfiable formulas F_n on n variables in $O(1)$-CNF such that every OBDD($\wedge, \exists$, reorder)-algorithm runs at least $2^{\Omega(n)}$ steps on F_n. Formula F_n represents a system of linear equations over $\mathbb{F}_2$ based on checksum matrix of some linear code.

OBDD($\wedge, \exists$, reorder)-algorithms

- (reorder) Choose π' and $F^{\pi'}$ such that $F \equiv D$; $\pi := \pi'$ and $D := F$.

Our goals:

- Lower bounds for OBDD($\wedge, \exists$, reorder)-algorithms
- Lower bound of type $2^{\Omega(n)}$, where n is number of variables
- Lower bound for natural formulas.

Theorem. There is a randomized construction of a family of satisfiable formulas F_n on n variables in $O(1)$-CNF such that every OBDD($\wedge, \exists$, reorder)-algorithm runs at least $2^{\Omega(n)}$ steps on F_n. Formula F_n represents a system of linear equations over $\mathbb{F}_2$ based on checksum matrix of some linear code.

OBDD size for codes

- A code $C \subseteq \{0,1\}^n$ recovers ρ fraction of erasures by a list of size L (or C is (ρ, L)-erasure list-decodable) if for all $w \in \{0,1,\square\}^n$ with at most ρ fraction of $\square$ there are at most L codewords that are consistent with w.

Lemma. If $C \subseteq \{0,1\}^n$ is $(\frac{1}{2}+\epsilon, L)$-erasure list-decodable, then any OBDD for χ_C has OBDD size at least $\frac{|C|}{L^2}$. Moreover for every $i_1, i_2, \ldots, i_k \in [n]$ if $k \le 2\epsilon n$, then $\exists x_{i_1} \ldots \exists x_{i_k} \chi_C$ has OBDD size at least $\frac{|C|}{L^2}$.

Proof.

- Consider some order π
- $\exists x_{n-k+1} \ldots \exists x_n \chi_C(x_1, x_2, \ldots, x_n)$
- We show that there are many substitutions to the first $\frac{n-k}{2}$ variables that produce different functions.
- S is a set of all $\frac{n-k}{2}$-size prefixes of C.
- $L+1$ different codewords can't have same prefixes since $n - \frac{n-k}{2} \le (\frac{1}{2}+\epsilon)n$. Hence $|S| \ge \frac{|C|}{L}$.

OBDD size for codes

- A code $C \subseteq \{0,1\}^n$ recovers ρ fraction of erasures by a list of size L (or C is (ρ, L)-erasure list-decodable) if for all $w \in \{0,1,\Box\}^n$ with at most ρ fraction of $\Box$ there are at most L codewords that are consistent with w.

Lemma. If $C \subseteq \{0,1\}^n$ is $(\frac{1}{2}+\epsilon, L)$-erasure list-decodable, then any OBDD for χ_C has OBDD size at least $\frac{|C|}{L^2}$. Moreover for every $i_1, i_2, \ldots, i_k \in [n]$ if $k \leq 2\epsilon n$, then $\exists x_{i_1} \ldots \exists x_{i_k} \chi_C$ has OBDD size at least $\frac{|C|}{L^2}$.

Proof.

- Consider some order π
- $\exists x_{n-k+1} \ldots \exists x_n \chi_C(x_1, x_2, \ldots, x_n)$
- We show that there are many substitutions to the first $\frac{n-k}{2}$ variables that produce different functions.
- S is a set of all $\frac{n-k}{2}$-size prefixes of C.
- $L+1$ different codewords can't have same prefixes since $n - \frac{n-k}{2} \leq (\frac{1}{2}+\epsilon)n$. Hence $|S| \geq \frac{|C|}{L}$.

OBDD size for codes

- A code $C \subseteq \{0,1\}^n$ recovers ρ fraction of erasures by a list of size L (or C is (ρ, L)-erasure list-decodable) if for all $w \in \{0,1,\Box\}^n$ with at most ρ fraction of $\Box$ there are at most L codewords that are consistent with w.

Lemma. If $C \subseteq \{0,1\}^n$ is $(\frac{1}{2}+\epsilon, L)$-erasure list-decodable, then any OBDD for χ_C has OBDD size at least $\frac{|C|}{L^2}$. Moreover for every $i_1, i_2, \ldots, i_k \in [n]$ if $k \leq 2\epsilon n$, then $\exists x_{i_1} \ldots \exists x_{i_k} \chi_C$ has OBDD size at least $\frac{|C|}{L^2}$.

Proof.

- Consider some order π
- $\exists x_{n-k+1} \ldots \exists x_n \chi_C(x_1, x_2, \ldots, x_n)$
- We show that there are many substitutions to the first $\frac{n-k}{2}$ variables that produce different functions.
- S is a set of all $\frac{n-k}{2}$-size prefixes of C.
- $L+1$ different codewords can't have same prefixes since $n - \frac{n-k}{2} \leq (\frac{1}{2}+\epsilon)n$. Hence $|S| \geq \frac{|C|}{L}$.

OBDD size for codes

Lemma. If $C \subseteq \{0,1\}^n$ is $(\frac{1}{2}+\epsilon, L)$-erasure list-decodable, then any OBDD for χ_C has ODBB size at least $\frac{|C|}{L^2}$. Moreover for every $i_1, i_2, \ldots, i_k \in [n]$ if $k \leq 2\epsilon n$, then $\exists x_{i_1} \ldots \exists x_{i_k} \chi_C$ has OBDD size at least $\frac{|C|}{L^2}$.

Proof. (Continue)

- S is a set of all $\frac{n-k}{2}$-size prefixes of C. $|S| \geq \frac{|C|}{L}$.
- For every $s \in S$ we define ρ_s that substitutes $x_1 \ldots x_{(n-k)/2} := s$. $\exists x_{n-k+1} \ldots \exists x_n \chi_C(x_1, x_2, \ldots, x_n)|_{\rho_s}$ is satisfiable since s is a prefix of a codeword.
- Let $s_1, s_2, \ldots, s_{L+1}$ be different elements of S. We claim that ρ_{s_i} for $i \in [L+1]$ can't produce the same function.
- Let $s_1 r$ be a prefix of an element of C of size $n-k$.
- $\exists x_{n-k+1} \ldots \exists x_n \chi_C(x_1, x_2, \ldots, x_n)|_{\rho_{s_1}}(r) = 1$, hence for all $i \in [L+1]$, $s_i r$ is $n-k$ prefix of some element of C. Contradiction, since $\square^{\frac{n-k}{2}} r \square^k$ has at most $\frac{1}{2}+\epsilon$ fraction of $\square$.
- Number of different functions $\geq \frac{S}{L} \geq \frac{|C|}{L^2}$.

Lower bounds for OBDD($\wedge, \exists$, reorder)-algorithms

Theorem. Let A be an $0.97n \times n$ matrix over $\mathbb{F}_2$ such that

- A is a checksum matrix of $(\frac{2}{3}, 10)$-eras. list-decodable code;
- A contains $t = O(1)$ ones in every row;
- Every $\frac{n}{12}$ columns of A contain ones in at least $0.96n$ rows.

Then every OBDD($\wedge, \exists$, reorder)-algorithm runs at least $2^{\Omega(n)}$ steps on the formula that encodes $Ax = 0$.

Proof.

- Let D be the first diagram after $\frac{n}{12}$ applications of $\exists$.
- $D \equiv \exists_1 \dots \exists_{n/12} F$, where F is a conjunction of all clauses from $0.96n$ rows of A and possibly some other clauses.

Lemma. If A is a checksum matrix of (ρ, L)-erasure list-decodable code. A' is obtained from A by removing of k rows, then A is a checksum matrix of $(\rho, 2^k L)$-erasure list-decodable code.

- F is char. function of a $(\frac{2}{3}, 2^{0.1n}100)$-erasure list-decodable code of size at least $|C|$. Hence $|D| \geq 2^{\Omega(n)}$.

Lower bounds for OBDD($\wedge, \exists$, reorder)-algorithms

Theorem. Let A be an $0.97n \times n$ matrix over $\mathbb{F}_2$ such that

- A is a checksum matrix of $(\frac{2}{3}, 10)$-eras. list-decodable code;
- A contains $t = O(1)$ ones in every row;
- Every $\frac{n}{12}$ columns of A contain ones in at least $0.96n$ rows.

Then every OBDD($\wedge, \exists$, reorder)-algorithm runs at least $2^{\Omega(n)}$ steps on the formula that encodes $Ax = 0$.

Proof.

- Let D be the first diagram after $\frac{n}{12}$ applications of $\exists$.
- $D \equiv \exists_1 \dots \exists_{n/12} F$, where F is a conjunction of all clauses from $0.96n$ rows of A and possibly some other clauses.

Lemma. If A is a checksum matrix of (ρ, L)-erasure list-decodable code. A' is obtained from A by removing of k rows, then A is a checksum matrix of $(\rho, 2^k L)$-erasure list-decodable code.

- F is char. function of a $(\frac{2}{3}, 2^{0.1n}100)$-erasure list-decodable code of size at least $|C|$. Hence $|D| \geq 2^{\Omega(n)}$.

Lower bounds for OBDD($\wedge, \exists$, reorder)-algorithms

Theorem. Let A be an $0.97n \times n$ matrix over $\mathbb{F}_2$ such that

- A is a checksum matrix of $(\frac{2}{3}, 10)$-eras. list-decodable code;
- A contains $t = O(1)$ ones in every row;
- Every $\frac{n}{12}$ columns of A contain ones in at least $0.96n$ rows.

Then every OBDD($\wedge, \exists$, reorder)-algorithm runs at least $2^{\Omega(n)}$ steps on the formula that encodes $Ax = 0$.

Proof.

- Let D be the first diagram after $\frac{n}{12}$ applications of $\exists$.
- $D \equiv \exists_1 \dots \exists_{n/12} F$, where F is a conjunction of all clauses from $0.96n$ rows of A and possibly some other clauses.

Lemma. If A is a checksum matrix of (ρ, L)-erasure list-decodable code. A' is obtained from A by removing of k rows, then A is a checksum matrix of $(\rho, 2^k L)$-erasure list-decodable code.

- F is char. function of a $(\frac{2}{3}, 2^{0.1n}100)$-erasure list-decodable code of size at least $|C|$. Hence $|D| \geq 2^{\Omega(n)}$.

Lower bounds for OBDD($\wedge, \exists$, reorder)-algorithms

Theorem. Let A be an $0.97n \times n$ matrix over $\mathbb{F}_2$ such that

- A is a checksum matrix of $(\frac{2}{3}, 10)$-eras. list-decodable code;
- A contains $t = O(1)$ ones in every row;
- Every $\frac{n}{12}$ columns of A contain ones in at least $0.96n$ rows.

Then every OBDD($\wedge, \exists$, reorder)-algorithm runs at least $2^{\Omega(n)}$ steps on the formula that encodes $Ax = 0$.

Proof.

- Let D be the first diagram after $\frac{n}{12}$ applications of $\exists$.
- $D \equiv \exists_1 \ldots \exists_{n/12} F$, where F is a conjunction of all clauses from $0.96n$ rows of A and possibly some other clauses.

Lemma. If A is a checksum matrix of (ρ, L)-erasure list-decodable code. A' is obtained from A by removing of k rows, then A is a checksum matrix of $(\rho, 2^k L)$-erasure list-decodable code.

- F is char. function of a $(\frac{2}{3}, 2^{0.1n}100)$-erasure list-decodable code of size at least $|C|$. Hence $|D| \geq 2^{\Omega(n)}$.

Construction of code

Lemma. [Guruswami, 2003] If C is a code with relative distance δ, then for every $\epsilon > 0$ the code C is $((2-\epsilon)\delta, \frac{2}{\epsilon})$-erasure list-decodable.

[Gallager, 1962]

$$B = \left(\underbrace{\boxed{I_{n/t}}\boxed{I_{n/t}}\dots\boxed{I_{n/t}}}_{t \text{ times}} \right) \text{ is } n/t \times n \text{ matrix with } t \text{ ones per row.}$$

$$A = \begin{pmatrix} [\text{ 1st random perm. of columns of } B] \\ [\text{2nd random perm. of columns of } B] \\ \vdots \\ [r\text{-th random perm. of columns of } B] \end{pmatrix} \text{ is } \tfrac{rn}{t} \times n \text{ matrix}$$

with t ones per row.

Lemma. $\exists t$ such that for $r = 0.97t$ w.h.p A defines a code with relative distance 0.49. W.h.p every $\frac{n}{12}$ columns of A intersects at least $0.96n$ rows.

Construction of code

Lemma. [Guruswami, 2003] If C is a code with relative distance δ, then for every $\epsilon > 0$ the code C is $((2-\epsilon)\delta, \frac{2}{\epsilon})$-erasure list-decodable.

[Gallager, 1962]

$$B = \left(\underbrace{\boxed{I_{n/t}}\boxed{I_{n/t}}\ldots\boxed{I_{n/t}}}_{t \text{ times}} \right) \text{ is } n/t \times n \text{ matrix with } t \text{ ones per row.}$$

$$A = \begin{pmatrix} [\text{ 1st random perm. of columns of } B] \\ [\text{2nd random perm. of columns of } B] \\ \vdots \\ [r\text{-th random perm. of columns of } B] \end{pmatrix} \text{ is } \frac{rn}{t} \times n \text{ matrix}$$

with t ones per row.

Lemma. $\exists t$ such that for $r = 0.97t$ w.h.p A defines a code with relative distance 0.49. W.h.p every $\frac{n}{12}$ columns of A intersects at least $0.96n$ rows.

Open problems

1. Lower bound for OBDD($\wedge$, weakening, reorder)-proofs;
2. Separate OBDD($\wedge$, weakening) and OBDD($\wedge$, weakening, reorder)-proofs;
3. Is it possible to simulate OBDD($\wedge$)-proofs by OBDD($\wedge, \exists$)-algorithms?
4. Prove lower bound for OBDD($\wedge, \exists$, reorder)-algorithms on unsatisfiable linear systems.
5. Compare OBDD($\wedge$)-proofs with constant degree Frege.