Bullet Notes on The Width Method for Resolution and Sums-of-Squares Proofs

Albert Atserias,
Universitat Politècnica de Catalunya

PhD Open Course, University of Warsaw
January 25-27, 2018.

1 Day 1: 1h30 + 1h00

1.1 Definitions

- Propositional variables $X_1, \ldots, X_n$, values in $\{0, 1\}$.
- Literals: variables X_i and negations of variables $\overline{X_i}$; notation $X^0 = X$ and $X^1 = \overline{X}$.
- Clauses: sets or disjunctions of literals: $\ell_1 \vee \cdots \vee \ell_k$; width of the clause: k; letters A, B, C.
- CNF formulas: sets or conjunctions of clauses: $C_1 \wedge \cdots \wedge C_m$; letters F, G, H.
- k-CNF formulas: CNFs with clauses of width at most k.
- Truth assignments $f : \{X_1, \ldots, X_n\} \to \{0, 1\}$; letters f, g, h.
- Notation $f \models F$ or $f(F) = 1$ means that f satisfies F.
- Notation $F \models G$ means that $f \models F$ implies $f \models G$ for every f.
- $F \models G$ minimally means that if $H \subsetneq F$, then $H \not\models G$.

- Resolution rule: from $A \vee X$ and $B \vee \overline{X}$ derive $A \vee B$; notation $\mathrm{RES}(A \vee X, B \vee \overline{X}, X) = A \vee B$.
- Resolution proof of C from a given CNF F:
- A sequence $C_1, C_2, \ldots, C_m$ with $C_m = C$, each C_i in F or derived from C_j, C_k with $j, k < i$.
- Resolution refutation of F: a proof of the empty clause from F.

- Proof graph: one vertex for each C_i, arcs going forward from premises to conclusions.
- Size of a proof: number of symbols to write down.
- Length of a proof: number of vertices in proof graph.
- Space of a proof: size of the largest edge-cut of the form $(C_1, \ldots, C_t), (C_t, \ldots, C_m)$.
- Width of a proof: width of the widest clause $C_1, \ldots, C_m$.

1.2 Examples of formulas

- Pebbling formulas Peb(G) for connected directed acyclic graph G:
- Have a variable X_u for each vertex $u \in V(G)$.
- Have a clause $\overline{X_{u_1}} \vee \cdots \vee \overline{X_{u_d}} \vee X_w$ for each w with in-neighbours $u_1, \ldots, u_d$.
- Have a clause $\overline{X_t}$ for some sink t.
- Note that for each source s we have X_s as a clause.
- Forward refutation: length = $|E(G)|$, width = maximum degree plus one.
- Backward refutation: length = $|V(G)|$, width = depends on the traversal and could be big.

- Ordering principle OP_n: "every finite partial order has minimal elements".
- Have a variable X_{ij} for each $i, j \in [n]$.
- Have a clause $I_i := \overline{X_{ii}}$ for each $i \in [n]$.
- Have a clause $T_{ijk} := \overline{X_{ij}} \vee \overline{X_{jk}} \vee X_{ik}$ for each triple $i, j, k \in [n]$.
- Have a clause $A_i := X_{1i} \vee X_{2i} \vee \cdots \vee X_{ni}$ for each $i \in [n]$.
- Note: $\overline{X_{ij}} \vee \overline{X_{ji}}$ follows from taking $k = i$.

- A small refutation of OP_n in n stages, from stage n down to stage 1:
- At stage m derive $P_{j,m} := \bigvee_{i \in [m]: i \neq j} X_{ij}$ for all $j \in [m]$.
- If we succeed, we are good: $P_{1,1} = \square$.
- For $m = n$, derive $P_{j,n}$ by cut on $A_j = X_{1j} \vee \cdots \vee X_{nj}$ with $I_j = \overline{X_{jj}}$.
- We use $P_{m,m}$ and $P_{j,m}$ to derive the $P_{j,m-1}$ in $m-1$ substages, $m-1$ down to 1:
- Observe that $P_{j,m} = P_{j,m-1} \vee X_{m,j}$.
- At stage k derive $Q_{j,k} := \bigvee_{i \in [m]: i < k} X_{im} \vee \neg X_{mj} \vee \bigvee_{i \in [m-1]: i \geq k} X_{ij}$.
- For $k = m-1$, derive $Q_{j,m-1}$ by cut on $P_{m,m}$ and $T_{m-1,m,j}$.
- For $k = m-2$, derive $Q_{j,m-2}$ by cut on $Q_{j,m-1}$ and $T_{m-1,m,j}$.
- For $k = m-3$, derive $Q_{j,m-3}$ by cut on $Q_{j,m-2}$ and $T_{m-2,m,j}$.
- ...
- For $k = 1$, derive $Q_{j,1}$ by cut on $Q_{j,2}$ and $T_{2,m,j}$.
- We got $Q_{j,1} = \neg X_{mj} \vee P_{j,m-1} \vee X_{jj}$.
- Kill X_{jj} by cut with I_j, and cut with $P_{j,m} = P_{j,m-1} \vee X_{mj}$ to get $P_{j,m-1}$.
- $\square$
- Length = $n(n+1)/2$.

- Pigeonhole principle formulas PHP_n^{n+1}: "every map from $[n+1]$ to $[n]$ has a collision".
- Have one variable X_{ij} for each $i \in [n+1]$ and $j \in [n]$.
- Have one clause $X_{i1} \vee \cdots \vee X_{in}$ for each $i \in [n+1]$.
- Have one clause $\overline{X_{i_1 j}} \vee \overline{X_{i_2 j}}$ for each $j \in [n]$, $i_1, i_2 \in [n+1]$, $i_1 \neq i_2$.

- Systems of parity equations.
- Have n variables $X_1, \ldots, X_n$.
- Have m equations on three variables each: $X_{i_\ell} \oplus X_{j_\ell} \oplus X_{k_\ell} = b_\ell$ encoded as four clauses.
- Make sure each variable appears an even number of times but $b_1 \oplus \cdots \oplus b_m = 1$.

- Tseitin systems TSEITIN(G) for a 3-regular graph G with labelling $\ell : V(G) \to \{0,1\}$.
- Have one variable X_e for each edge $e \in E(G)$.
- Have one equation $X_{\{u,v_1\}} \oplus X_{\{u,v_2\}} \vee X_{\{u,v_3\}} = \ell(u)$ for each u with neighborhood v_1, v_2, v_3.
- Make sure that $\bigoplus_{u \in V(G)} \ell(u) = 1$.

- Random k-CNF formulas $F(n, m, k)$.
- Variables: $X_1, \ldots, X_n$.
- Clauses: randomly choose m clauses with k different variables uniformly and independently.
- Note: choices are made with replacement, so some clause could repeat.

1.3 Width lower bounds from expansion

- Let $F = C_1 \wedge \cdots \wedge C_m$ be a k-CNF with variables $X_1, \ldots, X_n$.
- Let $G(F)$ be its *bipartite clause-to-variable graph*:
- Clauses on the left, variables on the right, edges indicate occurrence.
- Note that left-degree is $\leq k$.

- Fix a biparite graph $G = (U \dot\cup V, E \subseteq U \times V)$ with left-degree at most k.
- For a set $A \subseteq U$, let $N(A) = \{v : \exists u \in A \text{ s.t. } (u,v) \in E\}$; neighborhood of A.
- For a set $A \subseteq U$, let $\partial(A) = \{v : \exists! u \in A \text{ s.t. } (u,v) \in E\}$; boundary of A.
- G is (s,e)-expander if for every $A \subseteq U$ with $|A| \leq s$ we have $|N(A)| \geq e|A|$.
- G is (s,f)-boundary expander if for every $A \subseteq U$ with $|A| \leq s$ we have $|\partial(A)| \geq f|A|$.
- Note that $f \leq e \leq k$. Equalities achieved if neighborhoods are disjoint and degrees are k.

- Fact 1: If G is (s, e)-expander, then it is also $(s, 2e - k)$-boundary expander.
- Proof: Fix $A \subseteq U$ with $|A| \leq s$ and estimate $E(A, V) = \{(u, v) \in E : u \in A, v \in V\}$:
- $|E(A, V)| \leq k|A|$; because k is a bound on the left-degree.
- $|E(A, V)| \geq |\partial(A)| + 2|N(A) \setminus \partial(A)|$; every $v \in N(A) \setminus \partial(A)$ has degree ≥ 2 in A.
- Solving for $|\partial(A)|$ we get $|\partial(A)| \geq 2|N(A)| - k|A| \geq 2e|A| - k|A| = (2e - k)|A|$. $\square$

- Fact 2: If $G(F)$ is (s, f)-boundy. exp., $f \geq 1$, and $A \subseteq F$ has $|A| \leq s$, then A is satisfiable.
- Proof: Use the variables in $\partial(G)$ to satisfy the clauses in G without conflicts. $\square$

- Fact 3: If $A \subseteq F$ and $A \models C$ minimally, then $\partial(A) \subseteq \text{vars}(C)$.
- Note that Fact 3 implies Fact 2 with $f \geq 1$ replaced by the weaker $f > 0$:
- Take minimal $A \models \square$. Then $A \neq \emptyset$ but $\partial(A) \subseteq \emptyset$, so $|A| > s$.
- Proof of Fact 3: Take $x \in \partial(C) \setminus \text{vars}(C)$ and let $D \in A$ be unique such that $x \in \text{vars}(D)$.
- Let f be such that $f \models A \setminus \{D\}$ and $f \not\models C$.
- Define g by flipping f at x, i.e., $g := f[x := \overline{f(x)}]$.
- Use boundary condition to check that $g \models A$.
- But then $g \models C$ by minimality of $A \models C$.
- Hence $x \in \text{vars}(C)$ because f and g differ only at x. $\square$

- Theorem: If $G(F)$ is (s, f)-boundy. exp., $(f \geq 1,)$ then width of refuting F is at least $fs/2$.
- Proof: For C, define $\mu(C) = \min\{|A| : A \subseteq F,\ A \models C\}$.
- Note $\mu(C) \leq 1$ for $C \in F$.
- Note $\mu(\square) \geq s + 1$ by Fact 2.
- Note $\mu(A \vee B) \leq \mu(A \vee X) + \mu(B \vee \overline{X})$; subadditive.
- In particular $\mu(A \vee B) \leq 2 \max\{\mu(A \vee X), \mu(B \vee \overline{X})\}$.
- Conclude: every refutation $C_1, C_2, \ldots, \square$ of F contains a clause C_i with $s/2 \leq \mu(C_i) \leq s$.
- Graphically: tag each C_i by its $\mu(C_i)$ and recall that it starts at ≤ 1 and ends at $\geq s + 1$.
- Let $A \subseteq F$ with $A \models C_i$ minimally, so $|A| = \mu(C_i)$.
- Apply Fact 3 to conclude $|\text{vars}(C_i)| \geq |\partial(A)| \geq f|A| \geq fs/2$. $\square$

- Corollary: If $F_n \sim F(n, 5n, 3)$, then every resolution refutation of F_n has width $\Omega(n)$ w.h.p.

1.4 Basic architecture of a CDCL SAT-solver (a theoretician's view)

- Unit clause: a clause with a single literal.
- Unit clause propagation (UCP): If F has a unit clause, choose one, resolve, set, and repeat.
- Observation: Final result does not depend on the choices made.

- Horn clause: one that has at most one positive literal.
- Horn CNF: one that has only Horn clauses.

- Fact: If $A \vee X$ and $B \vee \overline{X}$ are Horn, then $A \vee B$ is Horn (perhaps A or B or both empty).
- Proof: A must be all-negative and B must be Horn. $\square$

- Fact: If F is an unsatisfiable Horn CNF with m clauses, then UCP on F derives $\square$.
- Proof: By induction on sum of widths of all clauses.
- Case 1: all variables appear with both signs.
- Since F is unsatisfiable, it has an all-positive clause A.
- For being Horn, this all-positive clause is a unit clause $A = X$.
- As X appears with both signs, UCP resolves at least once with some $B = C \vee \overline{X}$ in F.
- The formula $(F \setminus \{B\}) \cup \{C\}$ is again an unsatisfiable Horn CNF.
- Its sum of widths is strictly smaller. Induct.
- Case 2: some variable appears with one sign only.
- Let A be a clause that contains one such variable X.
- Then $F \setminus \{A\}$ is still an unsatisfiable Horn CNF: else satisfy also A by assigning X.
- The sum of the widths of $F \setminus \{A\}$ is strictly smaller. Induct. $\square$

- Operation (conceptual simplification):
- Start at $F_1 = F$ and build a sequence $F_1 \subset F_2 \subset F_3 \subset \cdots$ in rounds:
- The i-th round:
- Start at empty assignment and grow a partial assignment setting one variable at a time.
- Notation: Ex: $S_i = (x_5 \stackrel{B_1}{=} a_1,\ x_2 \stackrel{B_2}{=} a_2,\ x_3 \stackrel{d}{=} a_3,\ x_8 \stackrel{B_4}{=} a_4,\ x_4 \stackrel{d}{=} a_5,\ x_6 \stackrel{d}{=} a_6,\ x_9 \stackrel{B_7}{=} a_9)$.
- $\stackrel{B}{=}$ means that the assignment was set by UCP on clause $B \in F_i$.
- $\stackrel{d}{=}$ means that the assignment was set by a *decision*: a choice, a heuristic, a coin-flip, ...
- UCP has higher priority: no new decisions until UCP terminates.

- If a clause from F_i is falsified by S_i: stop the round and analyze the conflict:
- *Learn* a clause C_i derived from F_i by resolution, is not in F_i, and is falsified by S_i.
- If $C_i = \square$, halt.
- Else trail assignments from S until *some* variable in C_i is unset.
- Let $F_{i+1} := F_i \cup \{C_i\}$, and resume *or* restart with the $i+1$-st round.

- All *italic* words in the algorithm denote heuristic choices that are subject to tunning.

- How is C learned at round i? Does it exist?
- Annotate $S = (s_1, s_2, \ldots, s_r)$ by clauses $A_r, \ldots, A_0$ from r down to 0:
- For $j = r$, let A_r be *a* clause from F that is falsified by S.
- For $j < r$:
- If $s_j = (x \stackrel{d}{=} a)$, set $A_{j-1} := A_j$.
- If $s_j = (x \stackrel{B}{=} a)$, set $A_{j-1} = \mathrm{RES}(A_j, B, x)$, or $A_{j-1} := A_j$ if A_j and B are not resolvable.
- Let C be *any* of the A_j's.
- Note: each A_{j-1} is falsified by S. Pf by reverse induction on j: it falsifies A_j and $B \setminus \{x^a\}$.
- Note: $s_r = (x \stackrel{B}{=} a)$ is not a decision, so $A_{r-1} = \mathrm{RES}(A_r, B, x) \neq A_r$.

- Fact: As defined the algorithm is sound and complete.
- Proof: The learned clause C_i prevents the algorithm to produce S_i again. $\square$

- Theoretician's analysis (stated informally):
- Theorem: Under ideal decisions, simulates resolution.
- Theorem: Under random decisions, simulates bounded-width resolution.
- Simulates: the number of required restarts is bounded by poly(length of refutation).

1.5 Problems

- Problem 1:
- Weakening rule (WKG): from A derive $A \vee B$.
- Axiom rule (AX): from nothing derive $X \vee \overline{X}$.
- Show:
- If F has refutation of length m with RES+WKG+AX, then also of length m with RES only.
- Ensure also that width only gets smaller.

- Problem 2:
- Prove: If F is unsatisfiable 2-CNF with n variables, then F has refutation of length $\leq 4n^2$.
- Improve: If F is unsatisfiable 2-CNF with m clauses, then F has refutation of length $\leq 2m$.

- Problem 3:
- Fix an integer $k \geq 2$.
- Find a real c_k such that:
- $\lim_{n\to\infty} \Pr[\ F \text{ is unsat }] = 1$ for F chosen at random from $F(n, c_k n, k)$.
- Bonus:
- Find as small as possible a constant $q_k < 1$ such that:
- For all $q > q_k$, for your c_k, and for F chosen at random from $F(n, c_k n, k)$:
- $\lim_{n\to\infty} \Pr[\ F \text{ has no assignment that satisfies more than } qc_k n \text{ clauses }] = 1$.
- Bonus bonus ($\star$):
- Prove that your q_k can't be chosen smaller.

- Problem 4 ($\star$):
- Find a constant d_3 such that:
- For F chosen at random from $F(n, d_3 n^2, 3)$:
- $\lim_{n\to\infty} \Pr[\ F \text{ has a refutation of length } dn\ ] = 1$.
- Find $m = m(n, k)$, with $m(n, 3) = n^2$, that makes the statement generalize to all $k \geq 2$.

- Puzzle:
- Show that every unsatisfiable F with n variables has a refutation of space $\leq n + 1$.

2 Day 2: 1h30 + 1h00

2.1 Goal of today's lecture

- Let F be a K-CNF with N variables and M clauses.

- Notation:
- width($F \vdash C$): minimum width of all proofs of C from F.
- tree-length($F \vdash C$): minimum length of all tree-like proofs of C from F.
- dag-length($F \vdash C$): minimum length of all dag-like proofs of C from F.
- Why didn't we distinguish between width of tree-like proofs and width of dag-like proofs?

- Theorem: If tree-length($F \vdash \square$) $\leq S$, then width($F \vdash \square$) $\leq \log_2(S) + K$.
- Corollary: If width($F \vdash \square$) $\geq W$, then dag-length($F \vdash \square$) $\geq 2^{W-K}$.

- Theorem: If dag-length($F \vdash \square$) $\leq S$, then width($F \vdash \square$) $\leq 2\sqrt{2N \ln(S)} + K$.
- Corollary: If width($F \vdash \square$) $\geq W$, then dag-length($F \vdash \square$) $\geq e^{(W-K)^2/8N}$.

2.2 Preliminary lemma

- Notation:
- For a K-CNF formula F:
- $F[X := 0]$: remove every positive occurrence of X, remove every clause that contains $\overline{X}$.
- $F[X := 1]$: remove every negative occurrence of X, remove every clause that contains X.
- For a proof $\Pi : F \vdash \square$:
- $\Pi[X := 0]$: remove every positive occurrence of X, remove every clause that contains $\overline{X}$.
- $\Pi[X := 1]$: remove every negative occurrence of X, remove every clause that contains X.
- Are these proofs? [Cf. Problem 1 of Day 1].

- A lemma that is not strong enough:
- Let $W :=$ width($F \vdash \square$) and $W_a :=$ width($F[X := a] \vdash \square$) for $a = 0, 1$.
- Then $W \leq \max\{1 + W_0, 1 + W_1\}$.
- Proof:
- Add $\overline{X}$ to every clause from where it disappeared in hypotheses of $F[X := 1] \vdash \square$.
- Add X to every clause from where it disappeared in hypotheses of $F[X := 0] \vdash \square$.

- We get proofs $F \vdash \overline{X}$ and $F \vdash X$ with every clause one literal wider.
- Resolve $\overline{X}$ and X. $\square$

- A stronger lemma:
- Let $W := \text{width}(F \vdash \square)$ and $W_a := \text{width}(F[X := a] \vdash \square)$ for $a = 0, 1$.
- Then $W \leq \max\{1 + W_1, W_0, K\}$ and $W \leq \max\{W_1, 1 + W_0, K\}$.
- Proof of $W \leq \max\{1 + W_1, W_0\}$; the other one is symmetric.
- Add $\overline{X}$ to every clause from where it disappeared in $F[X := 1] \vdash \square$.
- We get a proof $F \vdash \overline{X}$ with every clause one literal wider.
- Resolve $\overline{X}$ with every clause in F that contains X to produce $F[X := 0]$.
- Copy the refutation $F[X := 0] \vdash \square$.
- Width: $\leq 1 + W_1$ for the first part, $\leq \max\{W_0, K\}$ for the second. $\square$

2.3 Size-width relationship for tree-like resolution

- Theorem: If tree-length$(F \vdash \square) \leq S$, then width$(F \vdash \square) \leq \log_2(S) + K$.
- Proof: By induction on the number of variables N.
- For $N = 1$, obvious.
- For $N > 1$:
- Fix a tree-like proof Π witnessing tree-length$(F \vdash \square) \leq S$.
- Let X be the variable resolved last.
- Let Π_0 be the subtree that produces X.
- Let Π_1 be the subtree that produces $\overline{X}$.
- Then $\Pi_a[X := a]$ is a refutation $F[X := a] \vdash \square$ for $a = 0, 1$.
- One of the two has length $\leq S/2$, the other still has length $\leq S$.
- Say they're Π_0 and Π_1, respectively.
- Apply induction hypothesis to both.
- Let $W := \text{width}(F \vdash \square)$ and $W_a := \text{width}(F[X := a] \vdash \square)$ for $a = 0, 1$.
- We get $W_0 \leq \log_2(S/2) + K = \log_2(S) - 1 + K$ and $W_1 \leq \log_2(S) + K$.
- By the lemma $W \leq \max\{1 + W_0, W_1, K\} \leq \log_2(S) + K$.
- $\square$

2.4 Size-width relationship for dag-like resolution

- Theorem: If dag-length$(F \vdash \square) \leq S$, then width$(F \vdash \square) \leq 2\sqrt{2N \ln(S)} + K$.
- Proof:
- We prove the following stronger claim:
- For every $N \geq 1$ and $K \geq 1$, every K-CNF F with N variables, every S and every Q:
- If F has ref. with $\leq S$ clauses of width $\geq Q$, then width$(F \vdash \square) \leq Q + 2N \ln(S)/Q + K$.
- Setting $Q = \sqrt{2N \ln(S)}$ gives width$(F \vdash \square) \leq 2\sqrt{2N \ln(S)} + K$.

- Proof of the stronger claim:
- By induction on N.
- For $N = 1$, obvious.
- For $N > 1$:
- Fix K, F, S and Q.
- If $Q \geq N$, or if $Q < N$ but $S \geq e^N$, then the claim is obvious.
- Assume $Q < N$ and $S < e^N$.
- Assume Π is ref. with exactly $T \leq S$ clauses of width $\geq Q$.
- The total number of literals in clauses of width $\geq Q$ is $\geq TQ$.
- Pick a variable X that appears in $\geq TQ/N$ clauses of width $\geq Q$.
- $\Pi_a := \Pi[X := a]$ is a refutation $F[X := a] \vdash \square$ for $a = 0, 1$.
- One of the two has $\leq T - TQ/2N \leq S(1 - Q/2N)$ clauses of width $\geq Q$.
- The other still has $\leq T \leq S$ clauses of width $\geq Q$.
- Say they are Π_0 and Π_1, respectively.
- Apply induction hypothesis to both.
- Let $W :=$ width$(F \vdash \square)$ and $W_a :=$ width$(F[X := a] \vdash \square)$ for $a = 0, 1$.
- $W_0 \leq Q + (N - 1) \ln(S(1 - Q/2N))/Q + K \leq Q + N \ln(S(1 - Q/2N))/Q + K$.
- Using $\ln(1 - Q/2N) \leq -Q/2N$ because $0 \leq Q/2N < 1$:
- $W_0 \leq Q + 2N \ln(S)/Q - 1 + K$.
- $W_1 \leq Q + 2N \ln(S)/Q + K$.
- By the lemma $W \leq \max\{1 + W_0, W_1, K\} \leq Q + 2N \ln(S)/Q + K$.
- $\square$

- Corollary: If $F_n \sim F(n, 5n, 3)$, then every resolution refutation of F_n has length $2^{\Omega(n)}$ w.h.p.

2.5 Application to PHP formulas

- How can we do PHP_n^{n+1}?
- Answer: There are direct lower bound proofs, but we can also apply this method.
- But not directly, for several reasons, specially this:
- There is a refutation of width $W = O(n)$, but note $N = \Theta(n^2)$.
- So $(W-K)^2/8N = O(1)$ and $e^{(W-K)^2/8N}$ trivializes.

- Graph pigeonhole formulas $\text{PHP}(H)$ for a graph $H = (U \dot\cup V, E \subseteq U \times V)$ with $|U| > |V|$.
- Have one variable X_{uv} for each $(u,v) \in E$.
- Have one clause $P_u := X_{uv_1} \vee \cdots \vee X_{uv_k}$ for each $u \in U$ with neighborhood $v_1, \ldots, v_k \in V$.
- Have one clause $H^v_{a,b} := \overline{X_{av}} \vee \overline{X_{bv}}$ for each $v \in V$ with $a, b \in U$, $a \neq b$ in neighborhood of v.
- Note: if H has left-degree $k = O(1)$, then $\text{PHP}(H)$ has $N = O(n)$ variables.

- Fact: If dag-length$(\text{PHP}_n^{n+1}) \leq m$, then dag-length$(\text{PHP}(H)) \leq m$ for all $H \subseteq K_{n+1,n}$.
- Proof:
- Assume Π witnesses the hypothesis.
- Plug $X_{uv} := 0$ in it for all $(u,v) \in [n+1] \times [n] \setminus E$.
- The resulting Π' witnesses the conclusion.
- $\square$

- Thus we aim at proving width$(\text{PHP}(H)) = \Omega(n)$ for some H with left-degree $k = O(1)$.
- This would imply dag-length$(\text{PHP}_n^{n+1}) \geq$ dag-length$(\text{PHP}(H)) = 2^{\Omega(n)}$.

- Note: $G(\text{PHP}(H))$ is quite related to H; indeed H is a minor of $G(\text{PHP}(H))$.
- But: the clauses $\overline{X_{u_1v}} \vee \overline{X_{u_2v}}$ spoil any hope of an expansion argument.
- Solution: Redo the width-via-expansion argument for *matching assignments*.

- An assignment $f : \{X_{uv} : (u,v) \in E\} \to \{0,1\}$ is a matching assignment if:
- There exist a (partial) matching $M \subseteq E$ such that $f(X_{uv}) = 1$ iff $(u,v) \in M$.
- Let $\mathscr{M}$ be the set of matching assignments.
- Define $F \models_{\mathscr{M}} G$ if for every $f \in \mathscr{M}$ we have that $f(F) = 1$ implies $f(G) = 1$.
- For $A \subseteq U$, let P_A be the set of clauses P_u for $u \in A$.
- For a clause C, let edges$(C) = \{(u,v) \in E : X_{uv} \in \text{vars}(C)\}$.

- Fact 2': If H is (s, f)-boundy. exp., $f \geq 1$, and $A \subseteq U$, $|A| \leq s$, then P_A is $\mathscr{M}$-satisfiable.
- Proof: Choose the matching from A to $\partial(A)$. $\square$

- Fact 3': If $A \subseteq U$ and $P_A \models_{\mathscr{M}} C$ minimally, then $|(U \times \partial(A)) \cap \text{edges}(C)| \geq |\partial(A)|$.
- Implies Fact 2' with $f \geq 1$ replaced by the weaker $f > 0$:
- Take A minimal s.t. $P_A \models_{\mathscr{M}} \square$. Then $A \neq \emptyset$ but $|\partial(A)| = 0$, so $|A| > s$.
- Proof of Fact 3':
- We show that for all $v \in \partial(A)$ there exists $\hat{u} \in U$ such that $(\hat{u}, v) \in \text{edges}(C)$.
- Let $u \in A$ be unique such that $(u, v) \in E$.
- Let $f \in \mathscr{M}$ be such that $f(P_{A \setminus \{u\}}) = 1$ and $f(C) = 0$; exists by minimality.
- Necessarily $f(X_{uv}) = 0$; else $f(P_A) = 1$ and then $f(C) = 1$ by $P_A \models C$.
- If there does not exists $\hat{u} \in U$ with $(\hat{u}, v) \in E$ and $f(X_{\hat{u}v}) = 1$:
- Define g by flipping f at X_{uv}; note $g \in \mathscr{M}$.
- If there exists $\hat{u} \in U$ with $(\hat{u}, v) \in E$ and $f(X_{\hat{u}v}) = 1$:
- Define g by flipping f at both X_{uv} and $X_{\hat{u}v}$; note $g \in \mathscr{M}$.
- In both cases $g \in \mathscr{M}$, and $g(P_A) = 1$, hence $g(C) = 1$.
- This means that edges(C) contains one of (u, v) or $(\hat{u}, v)$ or both.

- Now apply the complexity-measure argument with μ defined as follows:
- Fix a refutation of PHP(H).
- Define $\mu(C) = \min\{|A| : A \subseteq U,\ P_A \models_{\mathscr{M}} C\}$.
- Note $\mu(P_u) \leq 1$ for $u \in U$.
- Note $\mu(\square) \geq s + 1$ by Fact 2'.
- Note $\mu(A \vee B) \leq \mu(A \vee X_{uv}) + \mu(B \vee \overline{X_{uv}})$.
- But there is a problem: also $\mu(H^u_{a,b}) \geq s + 1$.
- Solution: Remove all $\mathscr{M}$-unsatisfiable clauses from the refutation.
- The result is now a refutation of $\{P_u : u \in U\}$ of width no bigger through $\mathscr{M}$-sound inferences.
- Moreover all $\mathscr{M}$-sound inferences still have at most two premises.
- Conclude: Such a refutation $C_1, C_2, \ldots, \square$ contains C_i with $s/2 \leq \mu(C_i) \leq s$.
- Let $A \subseteq U$ with $P_A \models_{\mathscr{M}} C_i$ minimally, so $|A| = \mu(C_i)$.
- Apply Fact 3' to conclude $|\text{edges}(C)| = |\text{vars}(C)| \geq |\partial(A)| \geq f|A| \geq fs/2$.

- Corollary: Every refutation of PHP^{n+1}_n has length $2^{\Omega(n)}$.

2.6 Application to systems of parity equations

- Parity equation: $\bigoplus_{i \in I} X_i = b$ for $b \in \{0, 1\}$; width: $|I|$.
- Gaussian rule: from $\bigoplus_{i \in I} X_i = b$ and $\bigoplus_{j \in J} X_j = c$ derive $\bigoplus_{i \in I \triangle J} X_i = b \bigoplus c$.
- Gaussian proof of equation E from a given system of parity equations S:
- A sequence $E_1, \ldots, E_m$ with $E_m = E$, each E_i in S or derived from E_j, E_k with $j, k < i$.
- Gaussian refutation of S: a proof of $0 = 1$ from S, where 0 on the left stands for $\bigoplus_{i \in \emptyset} X_i$.
- Bipartite equation-to-variable graph $G(S)$:
- Equations on the left, variables on the right, edges indicate occurrence.

- Theorem: If $G(S)$ is (s, f)-boundy. exp., ($f \geq 1$,) then width of Gaussian refuting S is $\geq fs/2$.
- Proof: *Exactly* the same as for CNFs and resolution.
- That proof used only two things:
- 1) The soundness of the (binary) resolution rule.
- 2) The flip property of clauses: if $f(C) = 0$, $x \in \mathrm{vars}(C)$ and $g := f[x := \overline{f(x)}]$, then $g(C) = 1$.
- Gaussian rule and parity equations have those very properties too.
- $\square$

3 Day 3: 1h30 + 1h00

3.1 Polynomials and multilinear polynomials

- Let $\mathbb{R}[Y_1, \ldots, Y_n]$ denote the ring of polynomials on $Y_1, \ldots, Y_n$ with coefficients in $\mathbb{R}$.
- Let I be the ideal generated by $Y_1^2 - 1, \ldots, Y_n^2 - 1$.
- The quotient ring $\mathbb{R}[Y_1, \ldots, Y_n]/I$ is the ring of multilinear polynomials:
- All monomials are of the form $\prod_{i \in I} Y_i$, and all polynomials are of the form $\sum_I c_I \prod_{i \in I} Y_i$.
- We write $P_n := \mathbb{R}[Y_1, \ldots, Y_n]$ and $\mathscr{P}_n := \mathbb{R}[Y_1, \ldots, Y_n]/I$.
- We write $P_{n,d}$ for the subspace of polynomials of degree at most d.
- We write $\mathscr{P}_{n,d}$ for the subspace of multilinear polynomials of degree at most d.

- Note $Y \mapsto X := (1 - Y)/2$ converts from $\{\pm 1\}$ domain to $\{0, 1\}$ domain.
- Note $X \mapsto Y := 1 - 2X$ converts from $\{0, 1\}$ domain to $\{\pm 1\}$ domain.

- Let $\deg(P)$ denote the degree of $P \in P_n$.
- Let $\deg^*(P)$ denote the degree of $P \in P_n$ after multilinearization (i.e. reducing mod I).

3.2 Sums-of-Squares (SOS) Proofs

- Let $S = \{P_1 = 0, \ldots, P_\ell = 0, P_{\ell+1} \geq 0, \ldots, P_m \geq 0\}$ a system of pol. eq.s and ineq.s.
- An SOS proof of $P \geq 0$ from S is an identity $\sum_{i=1}^m P_i Q_i + Q_{m+1} = -1$ where:
- 1) Each Q_i with $i \leq \ell$ is an arbitrary polynomial in P_n.
- 2) Each Q_i with $i \geq \ell + 1$ is a sum-of-squares polynomial (sos): $Q_i = \sum_j Q_{ij}^2$ with $Q_{ij} \in P_n$.
- 3) Identity is in $\mathscr{P}_n = \mathbb{R}[Y_1, \ldots, Y_n]/I$.
- An SOS refutation of S is a proof of $-1 \geq 0$ from S.

- Degree of the proof: $\max\{\deg(P_i Q_i) : i \in [m]\} \cup \{\deg(Q_{m+1})\}$.
- Note that degree is measured before multilinearization.

3.3 Pseudoexpectations

- Let $S = \{P_1 = 0, \ldots, P_\ell = 0, P_{\ell+1} \geq 0, \ldots, P_m \geq 0\}$ a system of pol. eq.s and ineq.s.
- A degree-d pseudoexpectation is a map $E : \mathscr{P}_{n,d} \to \mathbb{R}$ satisfying:
- 1) E is linear.
- 2) $E(1) = 1$.
- 3) $E(Q) \geq 0$ for every sos Q with $\deg(Q) \leq d$.
- 4) $E(P_i Q) = 0$ for every $i \in [\ell]$ and every Q with $\deg(P_i Q) \leq d$.
- 5) $E(P_i Q) \geq 0$ for every $i \in [m] \setminus [\ell]$ and every sos Q such that $\deg(P_i Q) \leq d$.

- Theorem: The following are equivalent:
- 1) There is a degree-d pseudoexpectation for S.
- 2) There is no degree-d SOS refutation of S.

- Proof of 1) implies 2) is easy.
- Proof of 2) implies 1) requires a specialized zero-gap duality theorem for SDPs.
- Proof of 1) implies 2):
- Assume $\sum_{i=1}^m P_i Q_i + Q_{m+1} = -1$ is a degree-d refutation of S.
- Assume E is a degree-d pseudoexpectation.
- Apply E to the left-hand side. We get:
- $E(\sum_{i=1}^m P_i Q_i + Q_{m+1}) = \sum_{i=1}^m E(P_i Q_i) + E(Q_{m+1}) \geq 0$.
- Apply E to the right-hand side. We get:
- $E(-1) = -E(1) = -1$.
- Conclude: The identity could not possibly hold.
- $\square$ (of 1 implies 2 only).

4 Systems of parity equations and pseudoexpectations

- Observation: $\bigoplus_{i \in I} X_i = b$ maps to $\prod_{i \in I} Y_i - (-1)^b = 0$.
- $S_X = \{ \bigoplus_{i \in I_j} X_i = b_j : j \in [m] \}$ and $S_Y = \{ \prod_{i \in I_j} Y_i - (-1)^{b_j} = 0 : j \in [m] \}$.
- We use S for both. Context tells which.

- Gaussian-width(S): minimal width of all Gaussian refutations of S.
- SOS-degree(S): minimal degree of all SOS refutations of S.

- Let S be a system of parity equations, each of width at most k.
- Let $k \leq \lfloor w/2 \rfloor$.
- Theorem: If Gaussian-width$(S) \geq w+1$, then SOS-degree$(S) \geq \lfloor w/2 \rfloor$.

- Proof: Let $d = \lfloor w/2 \rfloor$. We construct a degree-d pseudoexpectation for S.
- Let's move to the $\prod_{i \in I} Y_i = \pm 1$ notation for Gaussian proofs.

- For $K \subseteq [n]$, $|K| \leq 2d$, define:
- $\dot{\pi}(K) = -1$ if $\prod_{i \in K} Y_i = -1$ has Gaussian proof of width $\leq 2d$.
- $\dot{\pi}(K) = +1$ if $\prod_{i \in K} Y_i = +1$ has Gaussian proof of width $\leq 2d$.
- $\dot{\pi}(K) = \star$ otherwise.
- Well-defined:
- If both -1 and $+1$ were provable, then S would be refutable in width $\leq 2d \leq w$.
- Note that $\dot{\pi}(\emptyset) = +1$.

- For $I, J \subseteq [n]$, $|I| \leq d$ and $|J| \leq d$, define:
- $\pi(I, J) = 0$ if $\dot{\pi}(I \triangle J) = \star$.
- $\pi(I, J) = \dot{\pi}(I \triangle J)$ otherwise.
- It is well-defined: $|I|, |J| \leq d$, hence $|I \triangle J| \leq 2d$.

- For $I, J \subseteq [n]$, $|I| \leq d$ and $|J| \leq d$, define:
- $I \equiv J$ iff $\pi(I, J) \neq 0$ iff $\dot{\pi}(I \triangle J) \neq \star$ iff $\prod_{i \in I \triangle J} Y_i = \dot{\pi}(I \triangle J)$ has proof of width $\leq 2d$.
- It's reflexive: obvious; $\dot{\pi}(\emptyset) = +1$ by resolving some equation from S with itself.
- It's symmetric: obvious; definition depends only on $I \triangle J$.
- It's transitive: because $(I \triangle J) \triangle (J \triangle K) = I \triangle K$, and $|I|, |K| \leq d$ so $|I \triangle K| \leq 2d$.
- Choose K_C a representative of each equivalence class C.

- Observations:
- 1) $\dot{\pi}(I_j) = (-1)^{b_j}$ for all $j \in [m]$. Obvious: $|I_j| \leq k \leq \lfloor w/2 \rfloor = d$.
- 2) $\dot{\pi}(\emptyset) = +1$. Obvious.
- 3) $\dot{\pi}(I \triangle J) = \pi(I, J) = \sum_C \pi(I, K_C)\pi(J, K_C)$.
- Proof of 3):
- First part clear: $\dot{\pi}(I \triangle J) = \pi(I \triangle J, \emptyset) = \pi(I, J)$.

- If $I \not\equiv J$, then:
- $\pi(I,J) = 0$ and $\pi(I,K_C)\pi(J,K_C) = 0$ for each equivalence class C.
- If $I \equiv J$, then:
- $\pi(I,K_C)\pi(J,K_C) = 0$ for each $C \neq [I] = [J]$, and
- $\pi(I,K_C)\pi(J,K_C) = \pi(I,J)$ for $C = [I] = [J]$ because:
- If $\prod_{i\in I\triangle K_C} Y_i = \dot{\pi}(I\triangle K_C)$ and $\prod_{i\in J\triangle K_C} Y_i = \dot{\pi}(J\triangle K_C)$ in width $2d$, then:
- $\prod_{i\in I\triangle J} Y_i = \dot{\pi}(I\triangle K_C)\dot{\pi}(J\triangle K_C)$ in width $2d$, because $|I| \leq d$ and $|J| \leq d$.
- Hence $\dot{\pi}(I\triangle J) = \dot{\pi}(I\triangle K_C)\dot{\pi}(J\triangle K_C) = \pi(I,K_C)\pi(J,K_C)$.

- Construction of degree-d pseudoexpectation $E : \mathscr{P}_{n,d} \to \mathbb{R}$.
- For $P = \sum_I c_I \prod_{i\in I} X_i$ with degree $\leq d$, define:
- $E(P) := \sum_I c_I \dot{\pi}(I)$.

- Verification:
- E linear.
- $E(1) = 1$.

- Equations from S without liftings:
- $E(\prod_{i\in I_j} Y_i - (-1)^{b_j}) = E(\prod_{i\in I_j} Y_i) - E((-1)^{b_j}) = \dot{\pi}(I_j) - (-1)^{b_j} = 0$.

- Equations from S lifted by monomial $\prod_{i\in J} Y_i$ with total degree $\leq d$:
- $E((\prod_{i\in I_j} Y_i - (-1)^{b_j}) \prod_{i\in J} Y_i) = \dot{\pi}(I_j\triangle J) - (-1)^{b_j}\dot{\pi}(J) = \dot{\pi}(I_j\triangle J) - \dot{\pi}(I_j)\dot{\pi}(J) = 0$.
- Last equation proved by cases a) $\dot{\pi}(J) = 0$ or b) $\dot{\pi}(J) \neq 0$:
- In case a) we also have $\dot{\pi}(I_j\triangle J) = 0$; else by resolving $I_j\triangle J$ with I_j we get J.
- In case b) we also have $\dot{\pi}(I_j\triangle J) \neq 0$ by resolving I_j with J, and $\dot{\pi}(I_j\triangle J) = \dot{\pi}(I_j)\dot{\pi}(J)$.

- Equations from S lifted by polynomials:
- Apply linearity.

- Squares: sos's follow by linearity.
- First arbitrary products: $P = \sum_I c_I \prod_{i\in I} Y_i$ and $Q = \sum_J d_J \prod_{i\in I} Y_i$, degrees $\leq d/2$.
- $E(PQ) = E((\sum_I c_I \prod_{i\in I} Y_i)(\sum_J d_J \prod_{i\in J} Y_i))$
- $E(PQ) = \sum_{I,J} c_I d_J E(\prod_{i\in I\triangle J} Y_i)$ [working mod $Y_i^2 - 1 = 0$]

- $E(PQ) = \sum_{I,J} c_I d_J \dot{\pi}(I \triangle J)$
- $E(PQ) = \sum_{I,J} c_I d_J \sum_C \pi(I, K_C)\pi(J, K_C)$
- $E(PQ) = \sum_C (\sum_I c_I \pi(I, K_C))(\sum_J d_J \pi(J, K_C))$.
- Now squares: apply with $P = Q$:
- $E(P^2) = \sum_C (\sum_I c_I \pi(I, K_C))^2$, a sum of squares (of reals!), which is non-negative.
- $\square$

4.1 Applications to other systems of polynomials

- Coding clauses as polynomial eq.s. or ineq.s.
- Let $C = X_1 \vee \ldots \vee X_\ell \vee \bar{X}_{\ell+1} \vee \cdots \vee \bar{X}_k$.
- Define $P_C := \prod_{i \in [\ell]}(1 - X_i) \prod_{i \in [k]\setminus[\ell]} X_i$ and code by $P_C = 0$.
- Define $L_C := \sum_{i \in [\ell]} X_i + \sum_{i \in [k]\setminus[\ell]}(1 - X_i) - 1$ and code by $L_C \geq 0$.
- Note: P_C and L_C are written on the X-variables.
- But: We could have written them on the Y-variables.
- Problem: there's an exponential (in k) blow up in monomial size.
- This problem is a minor one if we work with 3-CNF.

- For a clause $C = X_1^a \vee X_2^b \vee X_3^c$:
- Let $E(C)$ be the equation $X_1 \oplus X_2 \oplus X_3 = a \oplus b \oplus c$.
- Observe: $E(C) \models C$ *and* $P(C) = 0$ has a degree-3 proof from $X_1X_2X_3 - (-1)^{a \oplus b \oplus c} = 0$.
- Hence:
- Let $S = \{C_1, \ldots, C_m\}$.
- Let $\hat{S} = \{E(C_1), \ldots, E(C_m)\}$.
- Degree-d refutations of S give degree-$d + 3$ refutations of $\hat{S}$.

- Corollary: If $F_n \sim F(n, 5n, 3)$, then every SOS refutation of F_n has degree $\Omega(n)$ w.h.p.

5 Bibliography

- Ben-Sasson and Wigderson.
- Grigoriev.
- Schoenebeck.