Other Measures and Methods for Resolution

Plan

1. Space Complexity in Resolution
2. Space lower bounds for Random Formulas
3. Combinatorial Characterization of width
4. Width vs Space
5. Feasible Interpolation for Resolution and size lower bounds
6. Proof Search, Automatizability and Interpolation
7. Non automatizability for Resolution

Space Complexity in Resolution

Resolution Space

Memory configuration: A set of clauses M

Refutation: $P=M_0, M_1, \ldots, M_k$

* M_0 is empty
* M_k contains the empty clause.
* M_{t+1} is obtained from M_t by:

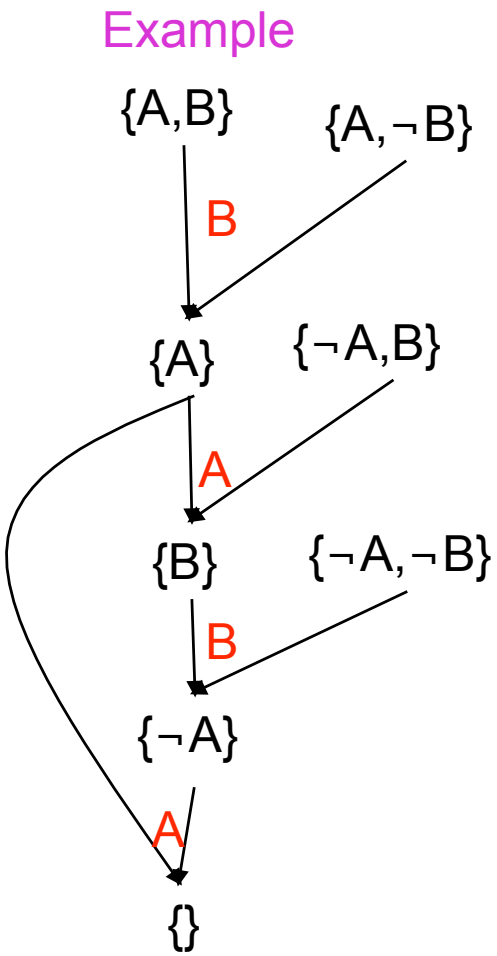
1. Axiom Download: $M_{t+1} = M_t + C \in F$.
2. Inference step: $M_{t+1} = M_t$ + some C derived by resolution from a pair of clauses in M_t.
3. Memory Erasure: M_{t+1} is a subset of M_t.

$Sp(P) = \max_{t\in[k]}\{|M_t|\}$.

$Sp_R(F) = \min\{\text{Space}(P): P \text{ refutation of } F\}$.

Resolution Space: Example

Time		Memory		
0				
1	{A,B}			
2	{A,B}	{A,¬B}		
3	{A,B}	{A,¬B}	{A}	
4	{A,¬B}	{A}		
5	{A}			
6	{¬A,¬B}	{A}		
7	{¬A,¬B}	{A}	{B}	
8	{A}	{B}		
9	{A}	{B}	{¬A,¬B}	
10	{A}	{B}	{¬A,¬B}	{¬A}
11	{A}	{B}	{¬A}	
12	{A}	{B}	{¬A}	{}



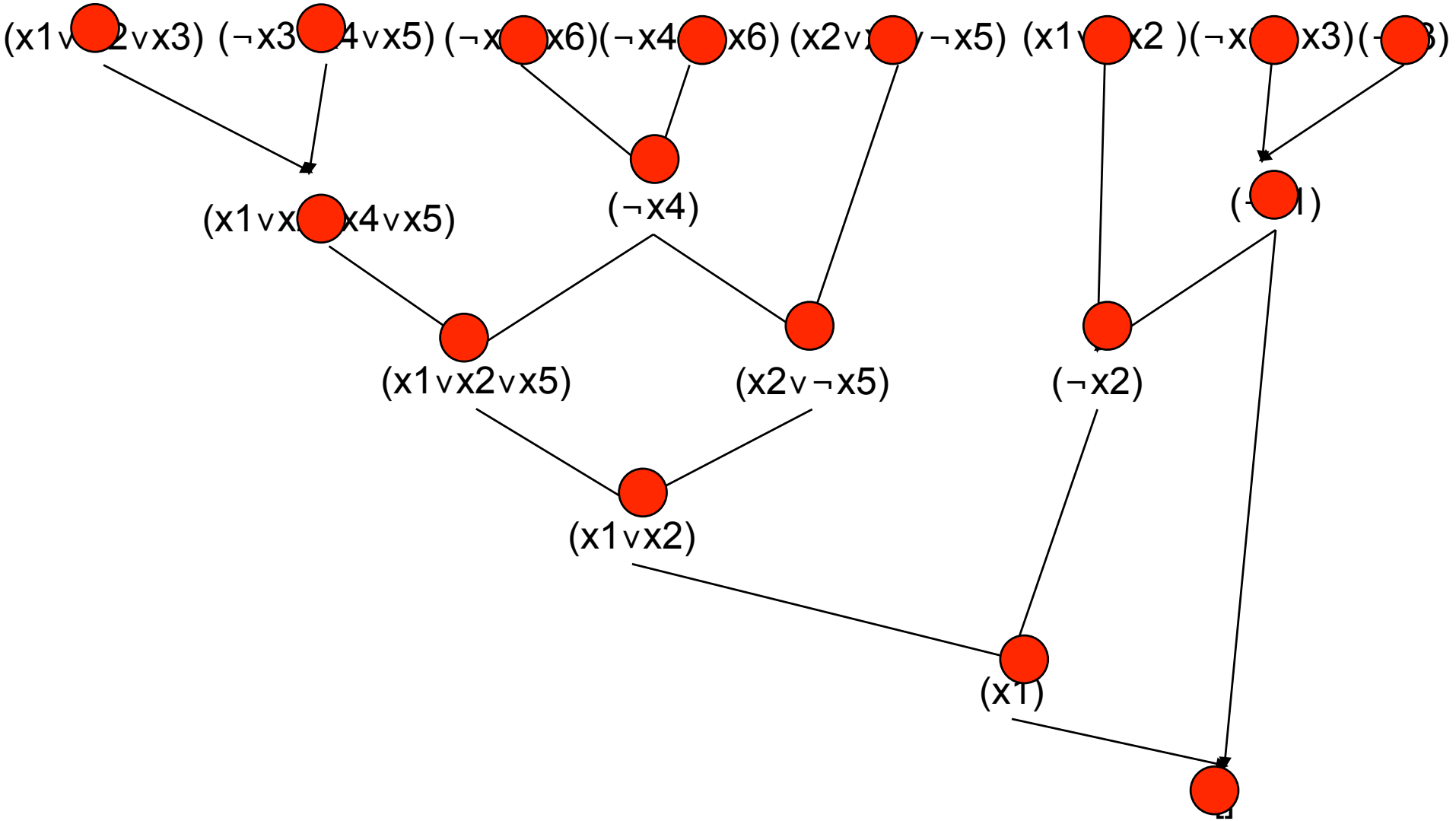
Resolution Space: Game definition

Let G_P be the graph associated to a refutation P:

$Sp(P) = pn(G_P)$.

$Sp_R(F) = \min \{pn(G_P)$: P refutation of F$\}$.

Resolution Space: Game definition



Why Resolution Space ?

[ET99] [ABRW00]

A natural complexity measure. Analog of Computation Space.

Automated Theorem Proving:

the search space for a proof of F is lower bounded by $Sp_R(F)$.

Thm[ET99] $Sp_R(F) \leq \log S_{\mathbf{TLR}}(F)$.

Linear lower bounds on space give *exponential* lower bounds on treelike size.

History of Results

1. Haken ’98: Raised the question of proof space
2. Esteban,Toran 99. Defined Resolution Space
    1. $Sp_R(F) \leq |Vars(F)|+1$
3. Toran 00. Lower bounds for PHP and Tseitin Formulas
4. Alekhnovich, Ben-Sasson, Razborov,Wigderson 00:
    - Definition of Space for other proof systems
    - Lower bound techniques for space (weak)
5. Ben-Sasson Galesi 03: Lower bounds for Random k-CNF
6. Atserias, Dalmau 04 $Sp_R(F) \geq w_R(F)$ (Space lower bounded by width)
7. Nordstrom 08. Separations between space and width

Notions Results and Techniques

1. [BSG] lower bound proof for Random k-CNF
    1. Main technique used by Atserias in another field

2. [AD] results on space vs width

3. Statement of Nordstrom's Separation

Space Lower Bounds for Random Formulas

Random k-CNF

F~**F(n,Dn)**: Pick Dn clauses at random from all $2^k \cdot \binom{n}{k}$ clauses. D is the clause density.

There is a sharp threshold between satisfiability and unsatisfiability [Friedgut].

Conjecture: There exists a satisfiability threshold constant.

If *D> 4.579*... then whp *F* is unsatisfiable [Jason et. Al 2000].

If *D<3.145*... then whp *F* is satisfiable [Achlioptas 2000].

Lower bounds

Thm With high probability, *F*~***F(n,Dn)*** has

$$Sp_R(F)=\Omega(n/D).$$

Cor With high probability, *F*~***F(n,Dn)*** *has*

$$S_{\mathbf{TLR}}(F) = \exp(\Omega(n/D)).$$

Proof Outline

1. Define G(F), the graph of F.

2. With high probability *G(F)* is an expander.

3. Define the Matching Game on a graph *G* and the associated Matching Space .

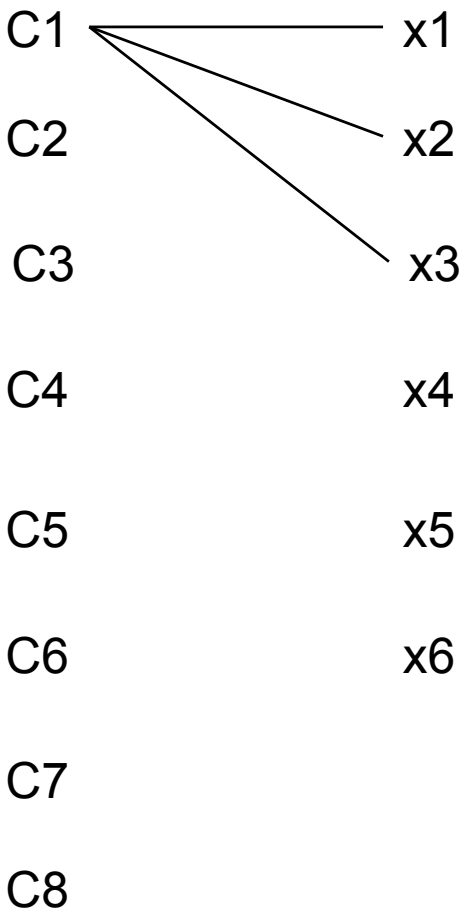
4. Space(F) ≥ Matching-Space(G(F))

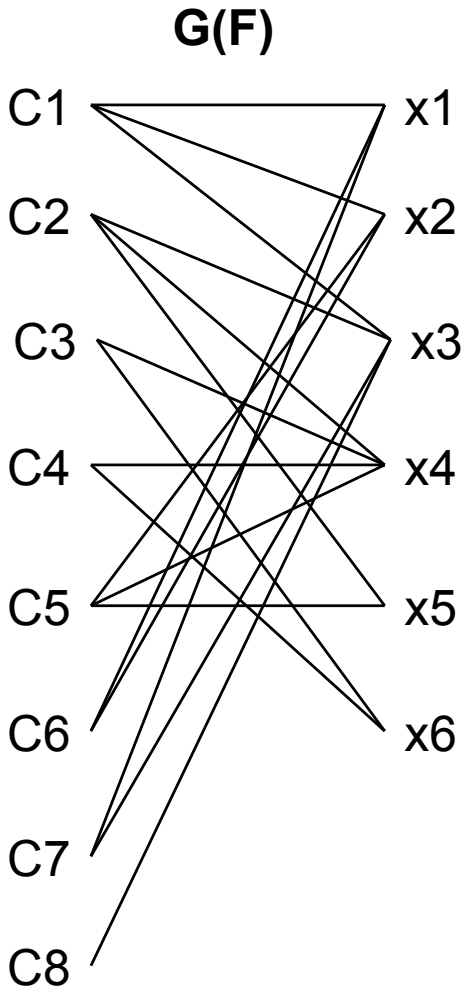
5. If *G* is an expander then Matching-Space(G) is large.

CNF's as Bipartite Graphs

$(x1 \vee x2 \vee x3)(\neg x3 \vee x4 \vee x5)(\neg x4 \vee x6)\ (\neg x4 \vee \neg x6)\ (x2 \vee x4 \vee \neg x5)\ (x1 \vee \neg x2)(\neg x1 \vee x3)\ (\neg x3)$

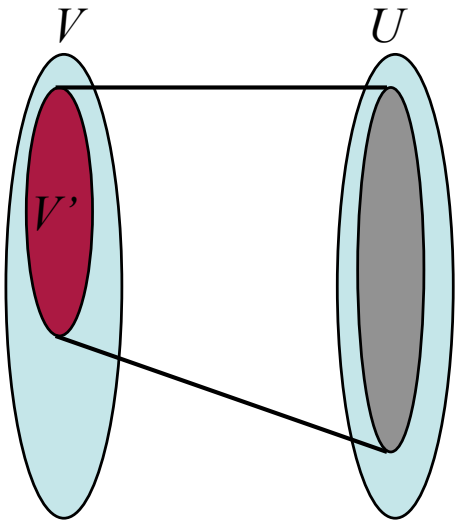
C1 C2 C3 C4 C5 C6 C7 C8





Bipartite Expander Graphs

Dfn A bipartite *G* is called an *(r,ε)*-expander if for all subsets *V'* of the left hand side:



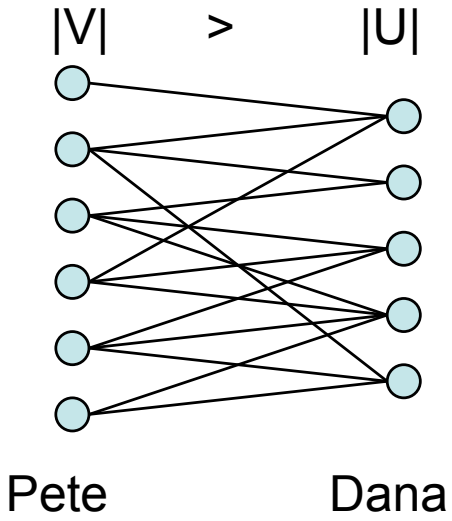
If $|V'| \leq r$ then $|N(V')| \geq (1+\varepsilon)|V'|$

Thm [CS87, BKPS98, BW99]:
For ***F~F(n,Dn)***, whp

G(F) is a $(\Omega(n/D), \varepsilon)$-expander,

for some constant $\varepsilon > 0$.

Matching Game



Pete Aim: There is **no matching** from V to U.
Dana Aim: **Force** a Perfect Matching from V to U
Pete's Goal: Prove the claim using pebbles.

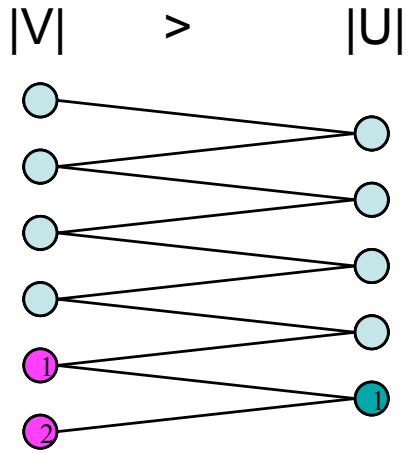
Move 1
Pete Move: **Places a pebble on a node of V**
Dana Move: **Places a pebble on anode of U node to keep matching**

Move 2
Pete Move: **Removes a pebble from a node of V**
Dana Move: **Removes the corresponding pebble from U**

Easy for Pete: Using $|U|+1$ fingers.

MSpace(G): Minimal # fingers needed to prove the claim.

Matching Game Simulation



Pete:QED! Dana

Matching Space=2

Space vs Matching Space

Thm $Sp_R(F) \geq MSpace(G(F))$

Proof

Assume Dana has a winning strategy when Pete uses ***p* fingers**. We prove that every set of clauses refutable using **space *p*** is satisfiable.

Given $P=M_0,M_1, ..., M_k$, use Dana's strategy to inductively find restrictions $\{\rho_1, \rho_2, ..., \rho_k\}$ such that

1. $|\rho_t| \leq |M_t|$
2. M_t is satisfied by ρ_t.

By cases on the rule to obtain M_t

Axiom download

$M_t = M_{t-1} + C$, C *initial Clause*

Space $\leq p \Rightarrow |M_{t-1}| \leq p-1$. Then $|M_t| \leq p$.

So use variable *x* given by Dana to satisfy C and

Define $\rho_t = \rho_{t-1} \cup \{x=1\}$

1. $|\rho_t| \leq |M_t|$
2. M_t is satisfied by ρ_t.

Inference Steps

By the soundness of resolution ρ_{t-1} satisfies M_t and $|M_t| > |M_{t-1}|$. Hence set $\rho_t = \rho_{t-1}$.

1. $|\rho_t| \leq |M_t|$

2. M_t is satisfied by ρ_t.

Memory Erasure

Locality lemma

If ρ satisfies *M*, then there is a subrestriction ρ' of ρ satisfying *M,* and such that $|\rho'| \leq |M|$. [Exercise]

$M_t = M_{t-1} - C$, for some C.

ρ_{t-1} satisfies M_t. We apply the Locality Lemma to M_t and set $\rho_t = \rho'$. Then

1. $|\rho_t| \leq |M_t|$
2. M_t is satisfied by ρ_t

Main theorem

Dfn A bipartite *G* is called an *(r, ε)*-expander if for all subsets *V'* of the left hand side:

If $|V'| \leq r$ then $|N(V')| \geq (1+\varepsilon)|V'|$.

Main Thm:
If *G* is an *(r, ε)*-expander, then MSpace(G)> ε r/(2+ ε).

Putting all Together

Thm For F~$\boldsymbol{F(n,Dn)}$, whp $G(F)$ is an $(\Omega(n/D), \varepsilon)$ -expander, for some constant $\varepsilon > 0$.

Main Thm

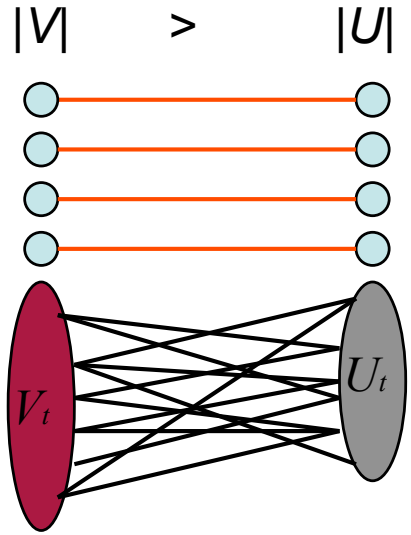
If G is an (r, ε)-expander, then $MSpace(G) > \varepsilon\, r/(2+\varepsilon)$

Then

1. whp MSpace(G(F))= Ω(n/D).

2. whp Space(F)= Ω(n/D).

Main Theorem



E_t = *matching* at time t
$s_t = |E_t|$

V_t, U_t = unmatched vertices.

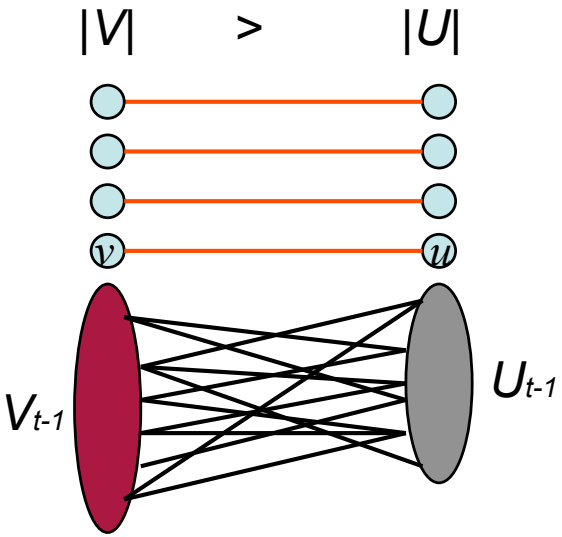
Dana's Strategy: Maintain the property:

For all $V' \subseteq V_t$ $|V'| \leq r - s_t$ there is a matching of V' into U_t.

Let t be **first time** property **fails**.

Claim: At time t, $s_t > \varepsilon\, r/(2+\varepsilon)$.

Pete Removes a Pebble



$V_t = V_{t-1}+\{v\}$

$U_t = U_{t-1}+\{u\}$

$s_t = s_{t-1}-1$

Claim: $|V'| = r - s_t$.

Proof:
Assume $|V'| < r - s_t$, i.e. $|V'| \leq r - s_{t-1}$ then
V' is matchbale into U_t
* If $v \notin V'$ then V' is matchable into U_{t-1}.
* If $v \in V'$ then match v to u, and match remaining vertices into U_{t-1}.

Contradiction with Dana strategy

$\exists V'$ minimal unmatchable into U_t, $|V'| \leq r - s_t$

Pete Removes a Pebble

V' minimal unmatchable , $|V'| = r - s_t$.

Hall's theorem: If V' is minimal unmatchable, then $|N(V')| < |V'|$.

$|V'| + s_t > |N(V')|$

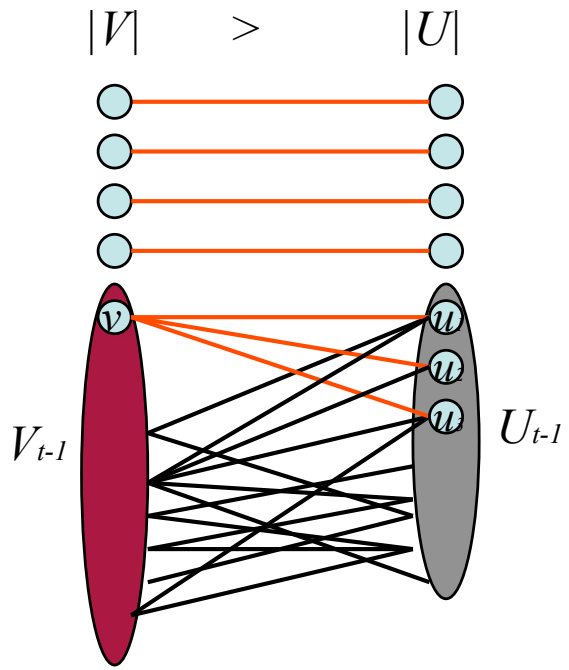
$|N(V')| \geq (1+\varepsilon)\,|V'|$ (expansion)

$|V'| + s_t > (1+\varepsilon)\,|V'|$

$s_t > \varepsilon\,|V'| = \varepsilon(r - s_t)$.

$s_t > \varepsilon\, r/(1+\varepsilon) > \varepsilon\, r/(2+\varepsilon)$.

Pete Place a Pebble



Claim: *V' is unmatchable into* U_{t-1}.

Hence: $|\cup_{[d]} V_i| > r - s_t$.

Hence: there is some $I \subseteq [d]$ such that
$(r - s_t)/2 < |\cup_I V_i| \leq r - s_t$.

$V'' = \cup_I V_i$.

Claim: $|N(V'') \cap U_{t-1}| \leq |V''|$.

$V_t = V_{t-1} - \{v\}$ $s_t = s_{t-1} - 1$

∀ neighbor u_i of v in U_{t-1}, ∃ V_i minimal unmatchable into $U_{t-1} - \{u_i\}$, $|V_i| \leq r - s_t$.

$V' = \cup_{[d]} V_i + \{v\}$

Pete Place a Pebble

$|V''| \geq |N(V'') \cap U_{t-1}|$.

$|V''| + s_t - 1 \geq |N(V'')|$

$|N(V'')| \geq (1+\varepsilon)\,|V''|$ (expansion)

$(r - s_t)/2 < |V''| \leq r - st$

.

.

.

$s_t > \varepsilon\, r/(2+\varepsilon)$.

Combinatorial Characterization of Resolution width

Combinatorial Relational Structures

Language

L ={R_1,…,R_m} be a finite relational language

L-Structure **A**

Is a tuple $\mathbf{A} = (A, R_1^A, R_1^A, \cdots R_m^A)$ where A is the universe and the R's are relations on A in L

Homomorphism $\mathbf{A} = (A, R_1^A, R_1^A, \cdots R_m^A)$ $\mathbf{B} = (B, R_1^B, R_1^B, \cdots R_m^B)$

A and B two L-structures

A partial hom from A to B is any function from A' to B, where A'$\subseteq$ A.

For all R $\in$ L and for all a_1,…,$a_s \in$ A'

f(a_1,..,a_s)$\in R^A$ iff (f(a_1),….f(a_s))$\in R^B$

Homomorphism problem and SAT

Homomorphism problem on Relational Structures

Given two finite relational structures A and B (over the same language) is there an homomorphism from A to B ?

Obs [Kolaitis Vardi]

SAT on r-CNF can be identified with the homomorphism problem on relational structures

Informally

A: the set of variables and clauses

B: is the set of assignments

Hom: the set of truth assignments of variables that makes clauses TRUE

Existential k-pebble games

Dfn Two players game over two Relational Structures A and B. Spoiler has k pebbles.

At each round
Move 1
Spoiler: places a pebble on a element of A
Duplicator: answers placing one of her pebble on an element of B

Move2
Spoiler: removes a pebble from a pebbled element of A
Duplicator: removes the pebbles from the corresponding element

Spoiler wins if at some round the set of pebbled pairs of A and B
Is not a partial homomorphism

Otherwise Duplicator wins

Existential Games on r-CNF [EkPG]

Dfn [AtseriasDalmau] F be a r-CNF. Duplicator wins the Existential k-game on F if there is a family H of partial assignments that do not falsify any clause of F s.t.

1. If $f \in H$, then $|Dom(F)| \leq k$
2. If $f \in H$ and $g \subseteq f$, then $g \in H$
3. If $f \in H$, $|Dom(f)| < k$ and x is variable, then there is a $g \in H$ s.t. $f \subseteq g$ and $g \in H$

In words H is a set of p.a. f not falsifying F s.t.

- f assigns no more than k variables
- H is close under sub-assignments
- (forcing) Any p.a. f assigning less than k variables can always be extended to any variable still preserving belonging to H

Main Theorem

Thm[AD] Let F be a r-CNF.

$w_R(F) \leq k$ iff Spoiler wins the existential (k+1)-pebble game in F

Proof

Lem1: If there is no refutation of F with width k, then Duplicator wins E(k+1)PG on F

Lem2: If Duplicator wins the E(k+1)PG on F then there is no width k refutation of F

Lemma 1

Consider $Res^k(F)$ and define

$$H=\{f : dom(f)\leq k+1 \text{ and } \forall C\in Res^k(F), f(C)\neq 0\}$$

(partial assignments of size at most k+1 which do not falsify any clause in $Res^k(F)$)

1. $H\neq \emptyset$ (since empty f is in H)
2. closed under sub-assignments (by def)

Assume (3) i.e. forcing, is not true.
Then for $f \in H$ and x a var:

1. $\exists\ C \in Res^k(F)$ s.t. $f(C)\neq 0$ and $f\cup\{x=0\}(C)=0 \Rightarrow x\in C$
2. $\exists\ D \in Res^k(F)$ s.t. $f(D)\neq 0$ and $f\cup\{x=1\}(D)=0 \Rightarrow \neg x\in D$

but then $f(C-\{x\}\cup D-\{\neg x\})=0$ and $C-\{x\}\cup D-\{\neg x\}\in Res^k(F)$.
Contradiction

Lemma 2

Assume H is a winning strategy for E(k+1)PG on F.
show by induction on the resolution proof of width k, that no assignment in H falsifies a clause in the proof.
[Exercise 1]

Argue that there is no refutation of width k [Exercise 2]

Width vs Space

Thm[AD] Let F be a UNSAT r-CNF. Then

$$Sp_R(F) \geq w_R(F)-r+1$$

Proof.
There is no proof of width $w_R(F)-1$. then Duplicator wins the $Ew_R(F)PG$ on F [lemma1].

Lemma Let F be UNSAT r-CNF
If Duplicator wins the E(k+r-1)PG on F, then $Sp_R(F) \geq k$

Lemma

Lemma Let F be UNSAT r-CNF
If Duplicator wins the E(k+r-1)PG on F, then $Sp_R(F) \geq k$

Proof.
Similar to [BSG] proof that space is lower bounded by Matching space.

H be a Duplicator winning strategy for the E(k+r-1)PG on F.

Prove that any Resolution refutation of F of space less than k is satisfiable, building for each round i a p.a. f_i in H that satisfies the content of memory at round i [Exercise 3]

Nordstrom`s Separation

[AD] Open question Is there a formula requiring “high” space” in Resolution but having refutations with “small” width?

[Nordstrom 08] STOC 08

There are k-CNF formulas of size O(n) s.t.

1. $S_{DLR}(F) \leq O(n)$
2. $w_R(F) \leq O(1)$
3. $Sp_R(F) \geq \Theta(n/\log n)$

Open Problems

Many Open Problems, essentially related to understanding better space measure and extending to stronger systems lower bounds and techniques

[BenSasson Nordstrom 09]
Space hierarchy separation for Resolution + k-DNF

Feasible Interpolation and size lower bounds

Interpolation and Complexity

[Krajicek 94] Estimate the size of the circuit of the interpolant in terms of the length of the proof fo the implicant.

Let $A(\mathbf{p},\mathbf{q}) \wedge B(\mathbf{p},\mathbf{r})$ a UNSAT CNF

An Interpolant $C(\mathbf{p})$ is a circuit s.t.

$$C(\mathbf{a}) = \begin{cases} 0 & A(\mathbf{a},\mathbf{q}) \text{ UNSAT} \\ 1 & B(\mathbf{a},\mathbf{r}) \text{ UNSAT} \end{cases}$$

Feasible Interpolation for Resolution

Thm [Pudlak 96]

Let P be a DLR refutations of $A_i(\mathbf{p},\mathbf{q}) \wedge B_j(\mathbf{p},\mathbf{r})$, $i \in I$ $j \in J$. Then there exists a boolean circuit $C(\mathbf{p})$ on gates $\{\neg, \wedge, \vee, \text{sel}\}$ s.t. for every truth assignment **a** to the common variables **p**

$$C(\mathbf{a}) = \begin{cases} 0 & A(\mathbf{a},\mathbf{q}) \text{ UNSAT} \\ 1 & B(\mathbf{a},\mathbf{r}) \text{ UNSAT} \end{cases}$$

1. C is of size O(|P|) (#gates).

2. If the common variables **p** occur only **positively** in A and **negatively** in B, then C is monotone, i.e. on gates $\{\wedge, \vee\}$

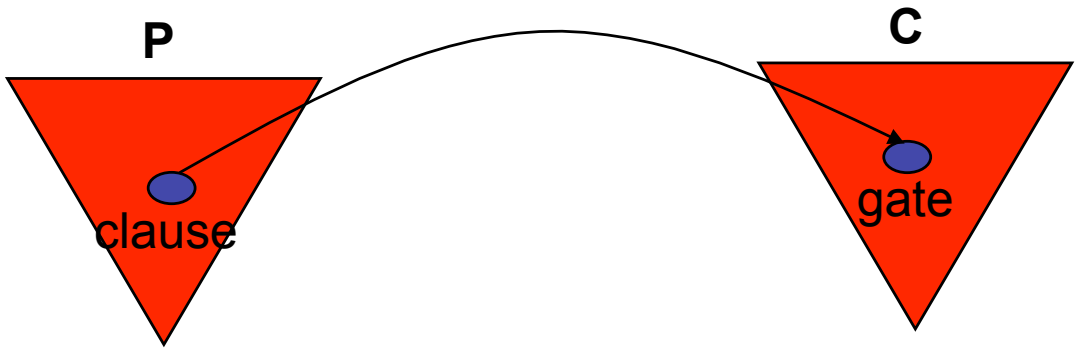
3. If P is TLR, then C is a formula (treelike circuit)

Proof Idea

Proof Idea

Given an assignment **a** to common variables **p**, trasform the proof into a proof of the only $A_i(\mathbf{a},\mathbf{q})$ or $B_j(\mathbf{a},\mathbf{r})$ where all clause are either q-clauses (discend only from A) or r-clauses (discend only from B).

The circuit C will have one gate for each clause in the original proof . At a gate C computes if the corresponding clause in the proof is transfomed into a q-clause or a r-clause under **a.**



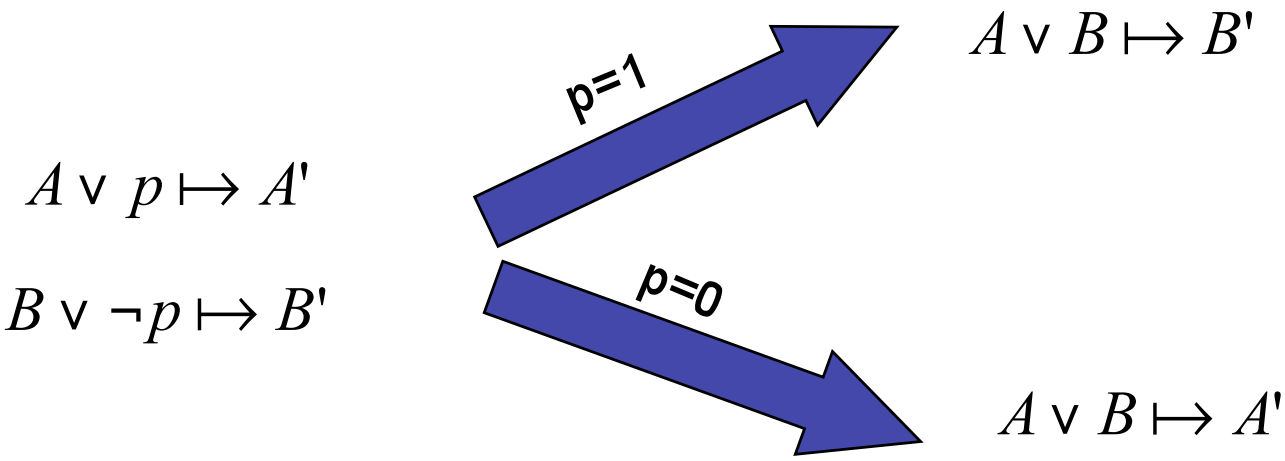
Proof Details

First step. Transform the proof

Base: C in F:easy.

Induction: First Case

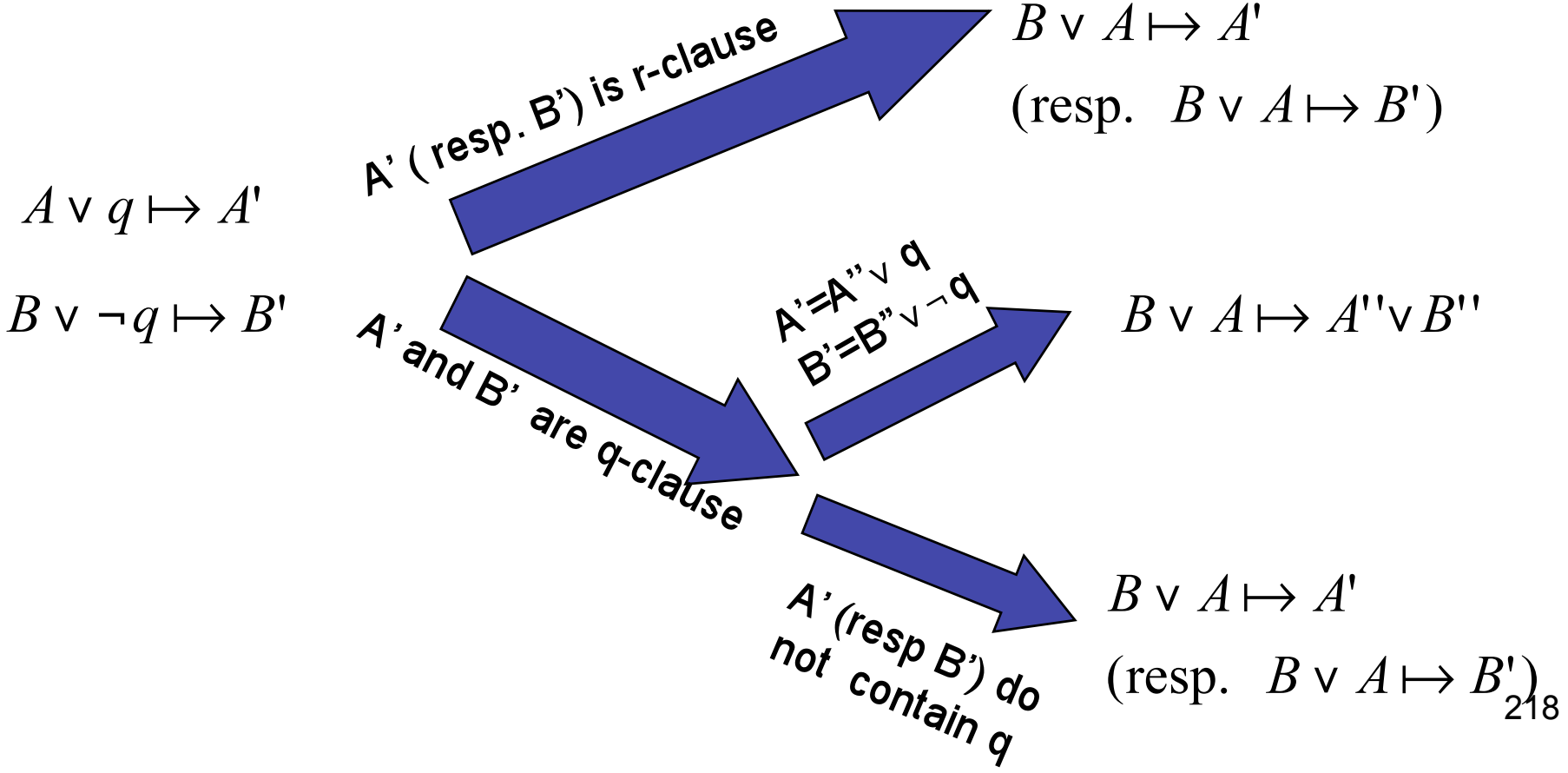
$$\frac{A \vee p \qquad \neg p \vee B}{A \vee B}$$



Proof Details

Induction: Second Case

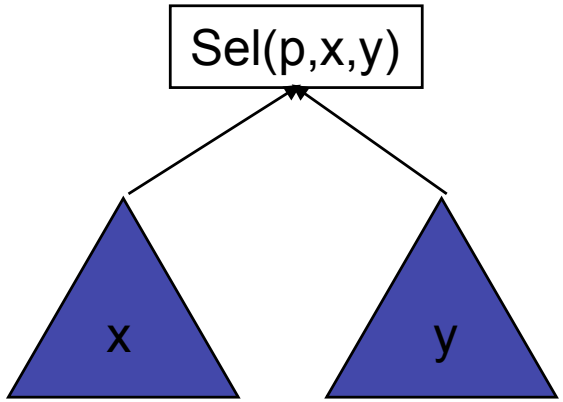
$$\frac{A \vee q \qquad \neg q \vee B}{A \vee B}$$



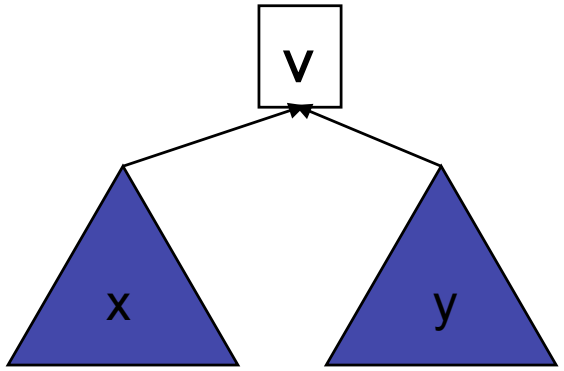
Proof Details

Second Step: Building the circuits. Choose 0 for q-clauses and 1 for r-clauses

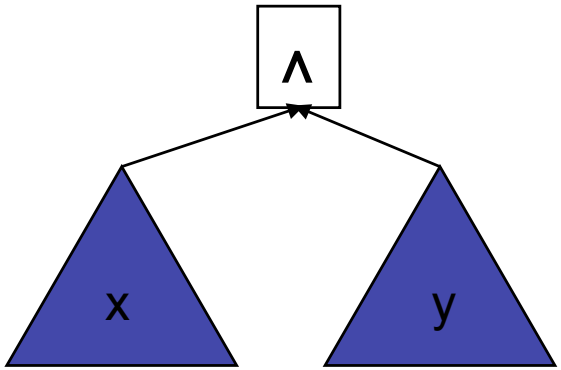
$$\frac{A \vee p \qquad \neg p \vee B}{A \vee B}$$



$$\frac{A \vee q \qquad \neg q \vee B}{A \vee B}$$



$$\frac{A \vee r \qquad \neg r \vee B}{A \vee B}$$



Proof Details

Monotone and treelike Circuits:

First Obs:

If all **p** are positive in **A** then in Case 1 of trasfomation if B' is a q-clause we can take it for A∨B even if p=0.

Then sel(p,x,y) can be simplified in (p∨x)∧y

Second Obs:

By construction the topology of the circuit is the same as that of the proof.

Razborov Lower bound for monotone circuits

Thm [Razborov,Pudlak]

Let C be a monotone circuit whose input variables encode in the usual way a graph oven n variables. Suppose that C outputs 1 on all cliques of size m and outputs 0 on all (m-1)-partite graphs, where m= $\frac{1}{8}(n/\log n)^{2/3}$.

Then C is of size $2^{\Omega((n/\log n)^{1/3})}$

Clique-Co-clique Tautologies

We express the UNSAT formula saying that a graph G contains a m clique and it is m-1 colorable

$p_{i,j} = 1$ iff *(i,j)* is an edge in G. For $1 \le i < j \le n$

$q_{k,i} = 1$ iff i is the k - th node in th m - clique. For $1 \le i \le n, \quad 1 \le k \le m$

$r_{i,l} = 1$ if node i node gets color l. For $1 \le i \le n, \quad 1 \le l \le m-1$

Clique-Co-clique Tautologies

We express the UNSAT formula saying that a graph G contains a m clique and it is m-1 colourable

$$\bigvee_{i=1}^{n} q_{k,i} \quad k = 1 \ldots m$$

$$\bigvee_{k=1}^{m} q_{k,i} \quad i = 1 \ldots n$$

$$q_{k',j} \wedge q_{k,i} \rightarrow p_{i,j} \quad i, j \in [n], k \neq k' \in [m]$$

G is a m-clique
Clique(p,q)

$$\bigvee_{l=1}^{m-1} r_{i,l} \quad i = 1 \ldots n$$

$$r_{i,l} \wedge r_{j,l} \rightarrow \neg p_{i,j} \quad l \in [m-1], i, j \in [n]$$

G is a (m-1)-partite
Colour(p,r)

Lower bounds for Clique-Coclique

Thm [Pudlak] Any resolution refutation of the CNF Clique(**p**,**q**)∧Colour(**p**,**r**) requires size $2^{\Omega((n/\log n)^{1/3})}$

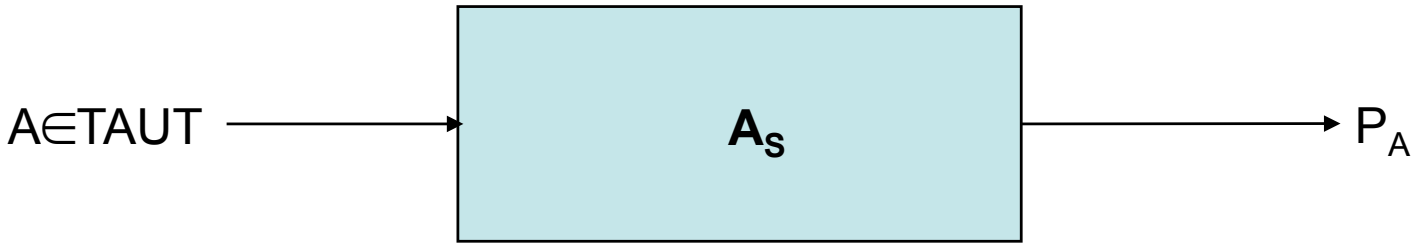
Proof. Set m as in Razborov's theorem. Then no proof can Exist of size smaller than the bound in Razborov theorem. Otherwise by Feasible Interpolation we get a monotone circuit which outputs 1 an all m-clique graphs and 0 an all (m-1)-partitionable graphs.

Interporlation and Automatizability

Automatizability

Automatizability [Impagliazzo, Bonet-Pitassi-Raz]

A proof system S is automatizable if there is an algorithm A_S which in input a tautology a gives a proof in S of the tauology A in running in time polynomially bounded in the shortest proof of A in S



Automatizability and Interpolation

Thm[Bonet,Pitassi,Raz]

If a Proof system S is automatizable, then it has Feasible Interpolation

Proof Let D be the algorithm from Automatizability. Assume it answers in time n^c,where n is the size of the shortest proof of the formula on which D is applied.Let $A(x,z) \wedge B(y,z)$ an UNSAT formula.

The circuit interpolating A and B is built as follows:

1. Run D on $A(x,z) \wedge B(y,z)$ and get a refutation of size s.
2. Run D on A(x,z) and return 0 only if D gets a refutation in time s^c.

[Exercise 4] Prove it is sufficient. [Hint: if B is SAT then we know for sure there is refutation of only A of size at most s]

No-Automatizability for Resolution

Cor. To prove no automatizabilty it is sufficient to prove no feasible interpolation.

Question. What happen for system that do have feasible Interpolation like Resolution ?

No-Automatizability for Resolution

Thm[Razborov-Aleknovich00]

Resolution is not Automatizable unless W[P] is in RP

Proof Idea:

1. Consider the optimization problem: Minimum Circuit Satisfying Assignment

   Istance: a monotone circuit C over n variables

   Solution: an input a s.t. C(a)=1

   Objective function: w(a), the hamming weight of a

No-Automatizability for Resolution

2. Given C, build an unsatifiable formula F(C,w,r) and prove that the size of the shortest proof is strongly related to the size of the minimum sat assignment of the circuit

3. Assuming Resolution is automatizable, use the algorithm to find a proof of approximately small size. This gives an approximation of the minimum sat assignment size in poly time.

4. Apply randomized gap amplification procedures to improve the approximation up to an error smaller than one, thus obtaining the exact value.

Conclude that, under automatizability, we can solve MMCSA which is a W[P]-complete problem in Random Polynomial time.

Other Proof Systems

Nicola Galesi
Dipartimento di Informatica
Università degli Studi di Roma "La Sapienza"

2009 August 15 – 16
NoNa Summer School
St Petersburg

Res[k]
Resolution +k-DNF

K-DNF

[Krajicek]

Instead of considering just clauses, i.e. disjunctions of literals, we allow disjunctions of k-conjunctions.

$$x_1 \vee (x_2 \wedge \neg x_3 \wedge x_5) \vee (x_4 \wedge x_3)$$

Res[k] is a calculus that extends resolution to work on k-DNF.

AND Introduction

$$\frac{A \vee \bigwedge_{i \in I} l_i \qquad B \vee \bigwedge_{i \in J} l_i}{A \vee B \vee \bigwedge_{i \in I \cup J} l_i} \quad |I \cup J| \leq k$$

k-resolution

$$\frac{A \vee \bigwedge_{i \in I} l_i \qquad B \vee \bigwedge_{i \in I} \neg l_i}{A \vee B} \quad |I| \leq k$$

History of Result on Res[k]

Res[k] is subsystem of bounded depth Frege. Lower bounds were then known for the PHP[n+1,n].

[Esteban,Atserias,Bonet03] lower bounds in Res[2] for PHP and for Random k-CNF

[Esteban,Galesi,Messner04] Exponential Separation between treelike Res[k] and treelike Res[k+1] and space lower bounds for Res[k] and space separations for treelike Res[k]

[Segerlind,Buss,Impagliazzo05] Exponential separation between Res[k] and Res[k+1].

[Alekhnovich 05] lower bounds for random 3-CNF

[BenSasson,Nordstrom 09] Space separation for Res[k]

Lower bounds for Res[k] [SBI]

General Idea of the proof. Let F be the CNF we want to prove the lower bound for. Let P a Res[k] proof of F.

1. Small restriction switching Lemma. If we hit a k-DNF with "good" random restriction, then w.h.p. we are left with a formula which can be computed by a small height decision tree.

2. Small height in Res[k] implies small width in Resolution

3. Then a width lower bound in Resolution and the existence of "good" random restriction give us Res[k] lower bounds.

Switching Lemma for k-DNF

Let F be a k-DNF.

Defn Ht(F)= height of the shallow DT computing F

Defn Covering number. Let S be a set of variables. If every Term of F contains a variable in S, then S is a covering of F. The covering number of F c(F) is the size of the smallest such a S.

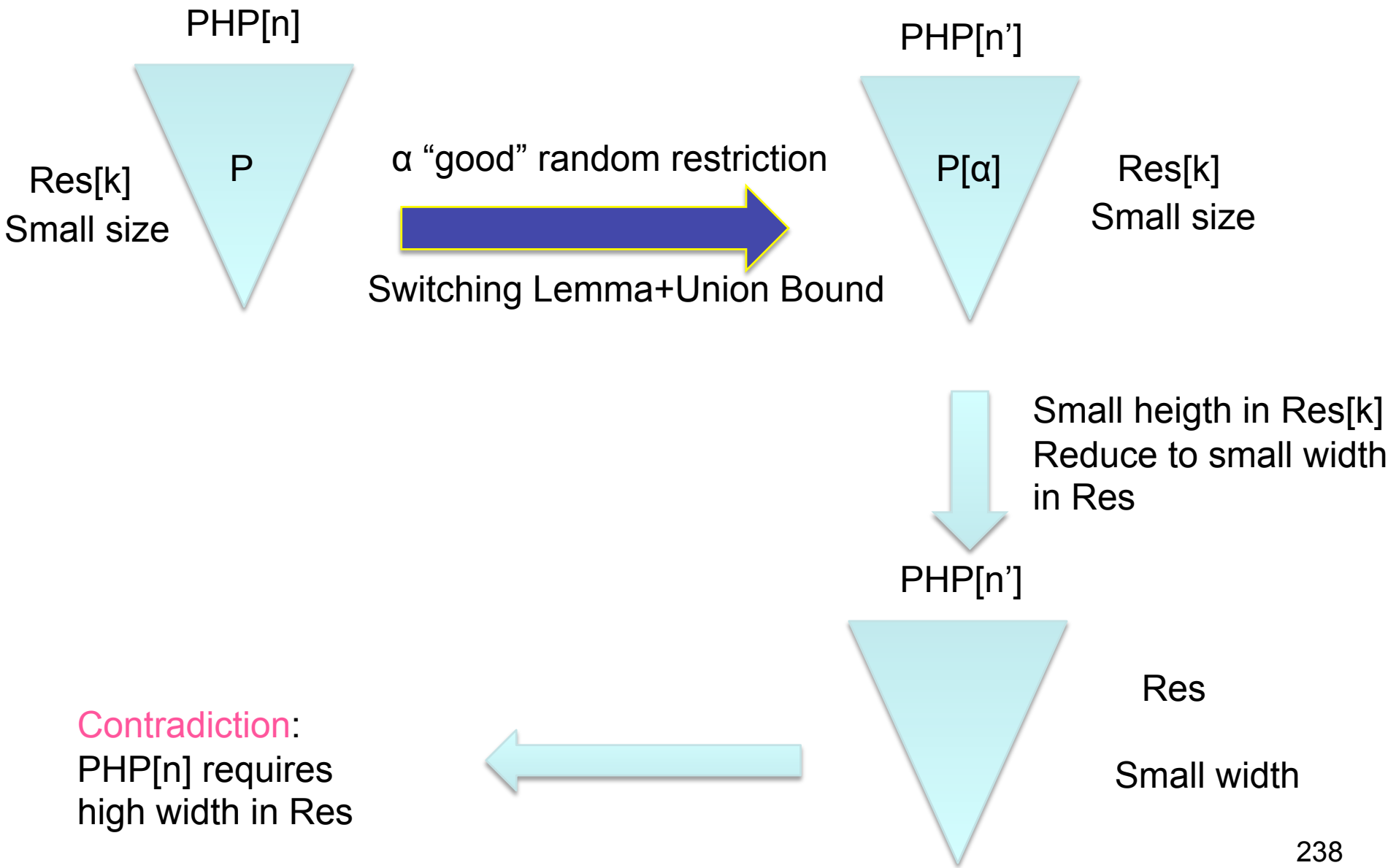
Switching Lemma for k-DNF

Switching Lemma [without parameters].

Let D a distribution on partial assignment s.t. for each k-DNF G $\Pr_{\rho \in D}[G[\rho] \neq 1] \leq 1/2^{c(G)}$. Then for every k-DNF F

$$\Pr_{\rho \in D}[Ht(F[\rho]) > 2s] \leq 1/2^{s}$$

Sketch of the proof on PHP[n]



Separations between Res[k] and Res[k+1]

Gop(G). A linear Ordering Principle over the nodes of a dag G.

Lemma1 Gop(G) admits polynomial size Res Refutations, for all G.

Proof. As for LOP

Lemma 2 Let G be a d-regular expander. Then $w_R(Gop(G))>\Omega(e(G))$.

$Gop^{\oplus k}(G)$ as GOP but every $x_{i,j}$ variable is substituted by the formula $PARITY(x_{i,j}^1,...,x_{i,j}^k)$ where $(x_{i,j}^1,...,x_{i,j}^k)$ are new variables

Separations between Res[k] and Res[k+1]

Lemma 1 $Gop^{\oplus k}(G)$ admits polynomial size Res[k] Refutations, for all G.

Proof. Use the Res refutation of Gop(G)

Lemma 2 $Gop^{\oplus k}(G)$ requires exponential size Res[k-1] Resolution refutations when G is the d-regular expander.

Proof. Use the Switching lemma.

Open problems

Complexity of Weak PHP in Res[2]. Related to complexity of Ramsey formulas in Res [see Krajicek's book]

Ramsey formulas:

Ramsey theorem: every graph contains a clique or an independent set of size at least log(n)/2.

Assume G a graph and let n = number of edges,

Variable x_i for each edge $i \in [n]$.

$$\bigwedge_{\substack{I \subseteq [n] \\ |I| = \frac{\log n}{2}}} \left(\left(\bigvee_{i \in I} x_i \right) \wedge \left(\bigvee_{i \in I} \neg x_i \right) \right)$$

Frege systems

Definitions

[Axiom Scheme]

$A \rightarrow (B \rightarrow A)$

$A \rightarrow (B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow (A \rightarrow C)$

$(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

$$\frac{A \quad A \rightarrow B}{B}$$ [Modus Ponens]

Bounded Depth Frege

Defn. Dept of the formula bounded by a costant O(1).

Thm[Beame,Impagliazzo,Krajicek,Pitassi,Pudlak,Woods]
PHP[n] requires exponential size proofs in BddFrege
Proof. Use generalization of Hastad's swtiching lemma

Thm[Maciel,Pitassi,Woods]
Weak PHP admits polynomial size proofs in BddFrege

Extended Frege

Frege + Extension rule $p \leftrightarrow A$

Where p is a new variable not appearing previously in the proof and in the last line.

Great strenght since we can abbreviate big formulas as one variable

Thm[Cook,Rekhow]. PHP[n] has poly size Efrege Proof

Proof.

Let f:[n+1]→[n]. Define:

$$f_i(x) = \begin{cases} f_{i+1}(x) & f_{i+1}(x) \neq i \\ f_{i+1}(i+1) & o.w. \end{cases}$$

PHP Proofs

Claim. If f_{i+1} is 1-1 then f_i is 1-1.

Then a proof of the PHP[n] can be given in this way:
$\neg PHP_{i+1} \rightarrow \neg PHP_i$. Then
$\neg PHP_n \rightarrow \neg PHP_1$. But $\neg PHP_1$ is clearly false and then PHP_n is TRUE.

In eFrege we can mimic this proof as follows. Introduce extension variables

$$q^n_{i,j} \leftrightarrow p_{i,j}$$

$$q^k_{i,j} \leftrightarrow q^{k+1}_{i,j} \vee (q^{k+1}_{i,k} \wedge q^{k+1}_{k+1,j})$$

PHP Proofs

Define A[k] a the PHP[k] on variables q^k.

Then we can prove

$\neg A[k+1] \rightarrow \neg A[k]$ for all k.

A[1] is easily provable in cosnstant size and hence by Modus ponens we get A[n] and hence PHP[n] by definition of A

Thm[Buss]. PHP[n] has polynomial size Frege proofs.

Proof. Counting in NC1 formalized in Frege Proofs

Feasible Interpolation

Thm[Krajicek,Pudlak; Bonet,Pitassi,Raz] Frege does not have Feasible Interpolation.

Proof Idea. Assume one-way funtions exits and let h be a one-way function (i.e. Computable in poly time but difficult to invert)

A(x,z)="h(x)=z and the i-th bit of x is 1"

B(y,z)="h(y)=z and the i-th bit of x is 0"

Since h is 1-way then $A \wedge B$ is UNSAT.

Assume by contradiction the Frege has Feasible Interpolation

Feasible Interpolation

Claim $A \wedge B$ has polynomial size Frege Proofs.

Then the circuit given by the interpolation is deciding in polynomial time the value of the i'th bit of the input of h. Then repeating n times we can invert h efficiently. But this is impossible since h is 1-way. Contradiction, and then Frege does not have Feasible Interpolation.

Open Problems

- Lower bounds for Random k-CNF in BddFrege
- Finding plausible candidates to be hard in Frege
  [Bonet,Buss,Pitassi; Cook,Soltys]

Geometric Systems

Cutting Planes

Linear Inequalities over {0,1} variables

- Clauses $(\neg x4 \vee \neg x2 \vee x6)$ are transformed into

$$(1-x4)+(1-x2)+x6 >= 1$$

- Axioms $x >= 0$ e $1-x >= 0$ to force solution in {0,1}

- Final Contradictions : $0>=1$

Rules

$$\frac{a_1x_1 + \ldots + a_nx_n \geq A \qquad b_1x_1 + \ldots + b_nx_n \geq B}{(a_1+b_1)x_1+\ldots+(a_n+b_n)x_n \geq A+B}$$

$$\frac{a_1x_1 + \ldots + a_nx_n \geq A}{ca_1x_1 + \ldots + ca_nx_n \geq cA}$$

$$\frac{ca_1x_1 + \ldots + ca_nx_n \geq B}{a_1x_1 + \ldots + a_nx_n \geq \lceil B/c \rceil}$$

- Refutation: A sequence of linear inequalities ending in 0>=1

Result for Cutting Planes

- PHP has polynomial size proofs [Exercise]
- CP admits Feasible monotone Interpolation. Hence Lower bound for Clique-Color Tautology

Open Problems

- Find other techniques to prove lower bounds: rank measure still not completely studied
- Prove lower bounds for random formula. There are rank lower bounds for random formulas
- Find proof search algorithm based on CP not similar to and stronger than DPLL