Haken's lower bound for resolution proof of pigeonhole principle

Mélanie Raemy

26.4.04

Schedule of the talk

1. Pigeonhole Principle
2. Resolution refutation proofs
3. Formalization of the Pigeonhole Principle
4. Haken's lower bound

The Pigeonhole Principle - The Erdős-Szekeres theorem

Definition 1. *$A = (a_1, .., a_n)$ is a sequence of n distinct terms.*
$B = (a_{i_1}, .., a_{i_k})$ is a subsequence of k terms of A, where $i_1 < .. < i_k$.

Theorem 1. *(Erdős-Szekeres 1935)*
If $n \geq sr + 1$ then either A has:
an increasing subsequence of $s + 1$ terms or
a decreasing subsequence of $r + 1$ terms (or both).

Consequences:
If A is a sequence of n terms, it contains a monotone subsequence of length $\sqrt{n}$.

Lemma 1. *(Dilworth 1950) In any partial order on a set P of $n \geq rs + 1$ elements, there exists a chain of length $s + 1$ or an antichain of size $r + 1$.*

Proof.

a_i has score (x_i, y_i).
x_i is longest **increasing** subsequence **ending** at a_i.
y_i is longest **decreasing** subsequence **starting** at a_i.

$(x_i, y_i) \neq (x_j, y_j)$ whenever $i \neq j$.
Assume $i < j$, then:
if $a_i < a_j \rightarrow x_i < x_j$
if $a_i > a_j \rightarrow y_i > y_j$.

$\mid A \mid = n \geq rs + 1$
Therefore there is a a_i with coordinate (x_i, y_i) outside the rs-quare.
This particular a_i then has either $x_i \geq s+1$ or $y_i \geq r+1$ or both. $\square$

Resolution refutation proofs

A **Resolution refutation proof** for F
is a sequence of clauses $R = (C_1, .., C_t)$, where $C_t = \Box$

$C_i \in F$ or C_i is derived from two previous clauses by the resolution rule:
$(C' \vee C'')$ can be derived from $(C' \vee x)$ and $(C'' \vee \overline{x})$

The length of the proof $=$ $\#$ of clauses in the derivation

The resolution proof is sound:
$(C' \vee x) \cdot (C'' \vee \overline{x}) \leq (C' \vee C'')$
Resolution is complete:
every unsatisfiable F has a resolution refutation proof.

But how long is the resolution??
The first lower bound was found by Haken for the set of clauses PHP_n^{n+1} formalizing the Pigeonhole principle.

ps: general pigeonhole principle: PHP_n^m
$m - n$ larger makes the proof shorter..

Formalizing the Pigeonhole Principle

Recall: PHP^n_{n-1} states, that n pigeons can not sit in $n-1$ holes.

$x_{i,j} \Leftrightarrow$ pigeon$_i$ sits in hole$_j$

PHP^n_{n-1} denotes the set of clauses:

(i) $x_{i,1} \vee x_{i,2} \vee .. \vee x_{i,n-1}$ for $i = 1..n$
(every pigeon sits in at least one hole)

(ii) $\overline{x}_{i,k} \vee \overline{x}_{j,k}$ for $1 \leq i \neq j \leq n$; $1 \leq k \leq n-1$.
(no two pigeons sit in the same hole)

By the pigeonhole principle, the And of the clauses in set PHP^n_{n-1} is **unsatisfiable**.

Haken's lower bound

Theorem 2. *(Haken 1985)*
For a sufficiently large n*, any Resolution proof of* PHP^n_{n-1} *requires length* $2^{\Omega(n)}$.

The Proof

Definition 2. *A* ***critical assignment*** *is a one-to-one mapping of $n-1$ pigeons to $n-1$ holes, with one pigeon unset.*
Having pigeon$_i$ unset defines a ***i-critical assignm****.*

Presenting the assignments of the $x_{i,j}$ as a matrix, the critical assignments would look like this:

Positive Pseudo-proofs

Replace $\overline{x}_{i,j}$ in all Clauses C by
$C_{i,j} \rightleftharpoons x_{1,j} \vee .. \vee x_{i-1,j} \vee x_{i+1,j} \vee .. \vee x_{n,j}$

Definition 3. *The resulting sequence of positive clauses $R^+ = (C_1^+, .., C_t^+)$ is a* ***positive pseudo-proof of*** PHP_{n-1}^n

Remark:
This is no longer a valid resolution refutation proof!
But **with respect to critical assignments**, it holds:
$C_1^+(\alpha) \cdot C_2^+(\alpha) \leq C^+(\alpha)$ if
C is derived from C_1, C_2 in original proof R.

Lemma 2. $C^+(\alpha) = C(\alpha)$ $\forall$ *critical* α.

Proof. Suppose $\exists$ $C^+(\alpha) \neq C(\alpha)$.
$\Rightarrow \exists$ $\overline{x}_{i,j} \in C$ s.t. $C_{i,j}(\alpha) \neq \overline{x}_{i,j}(\alpha)$.
$\Leftrightarrow (x_{1,j} \vee .. \vee x_{i-1,j} \vee x_{i+1,j} \vee .. \vee x_{n,j})(\alpha) \neq \overline{x}_{i,j}(\alpha)$.
This is impossible, since α is critical, therefore has exactly one 1 in the column$_j$. $\square$

The length of the pseudo-proof

Remember, that we want to proof Haken's lower bound on the length of the resolution proof!

We will show: $t \geq 2^{\frac{n}{32}}$.
For a contradiction, assume $t < 2^{\frac{n}{32}}$,
t is the number of clauses in R^+.

Definition 4. *A* $\mathbf{long}$ *clause has* $\geq \frac{n^2}{8}$ *variables.*
(more than $\frac{1}{8}$ *of all possible* $n(n-1)$ *variables).*
$\boldsymbol{l}$ *is the number of long clauses in* R.
$l \leq t < 2^{\frac{n}{32}}$.

By the pigeonhole principle, there exists a variable $x_{i,j}$, which occurs in at least $l/8$ of the long clauses.
This special variable is used to eliminate long clauses.

Elimination of the long clauses

Set the special variable $x_{i,j}$ to 1.
Set all $x_{i,j'}, x_{i',j}$ for $j' \neq j$, $i' \neq i$ to 0.
Clauses containing $x_{i,j}$ is set to 1 and therefore disappear from the proof.
The variables set to 0 disappear from all clauses.

We are left with a pseudo-proof of PHP^{n-1}_{n-2} with at most $l(1-1/8)$ long clauses.
Doing this $d = 8log(l)$ times,
we have eliminated all long clauses,
since $l(1-1/8)^d < e^{log(l)-d/8} = 1$.

We are left now with a pseudo-proof of PHP^m_{m-1} with no long clauses. (of length more than $n^2/8$).
But this is a contradiction to the final Lemma, since
$2m^2/9 = 2(n-8log(l))^2/9 > 2(n-n/4)^2/9 = n^2/8$

Final Lemma

Lemma 3. *Any positive pseudo-proof of* PHP^m_{m-1} *must have a clause with at least* $2m^2/9$ *variables.*

Proof. R' is a positive pseudo-proof of PHP^m_{m-1}.

Definition 5. $\forall\, C \in R'$, W *is a* **witness** *of* C *if* W *is a set of clauses from* PHP^m_{m-1},
whose conjunction implies C *for critical assignments.*
($\forall$ *critical* α *:* α *satisfies all* $w \in W \rightarrow \alpha$ *satisfies* C*).*
The **weight of** $C = \#$ *clauses in minimal witness.*
$\forall C\ \exists$ *witness* W.

Clauses of type (ii) is not part of a minimal witness.
Clauses of type (i) have weight 1.
The weight of the final clause is m.
The weight of a clause is at most the sum of the two clauses its been derived from.
There exists a clause of weight s, $m/3 \leq s \leq 2m/3$.

We are going to prove, that
this clause C has at least $2m^2/9$ variables:
Let
$W = \{C_i | i \in S\}, |S| = s,$
$C_i = x_{i,1} \vee x_{i,2}.. \vee x_{i,m-1}$; $C_i \in PHP^m_{m-1}$.
$\wedge C_i \to C$

We'll show,
C has at least $(m-s)s \geq 2m^2/9$ variables.

$i \in S$. Choose i-critical α with $C(\alpha) = 0$.
$\exists$ such α.
$j \notin S$. α' is j-critical .
α' is obtained from α, with row$_i$ and row$_j$ swapped.
If α maps pigeon$_j$ to hole$_k$, then α' maps pigeon$_i$ to hole$_k$. All other entries are equal.

Since $j \notin S$, α' satisfies all $C_i \in W$.
Therefore $C(\alpha') = 1$.
We have already seen: $C(\alpha) = 0$.
But α, α' differ only in $x_{i,k}, x_{j,k}$.
This implies $x_{i,k} \in C$.

To run this argument for this i-critical α,
there are $(m - s)$ possibilities to choose the $j \notin S$.
C contains the variables $x_{i,k_1}, x_{i,k_2}, .., x_{i,k_{m-s}}$

Repeating this for all $i \in S$ (there are s of them), shows us, that there has to be $(m - s)s$ distinct variables in C.

This completes the proof of the final Lemma and therefore the Haken's bound. $\Box$