Lecture 2— Resolution lower bound for Pigeohole principle

Massimo Lauria — lauria.massimo@gmail.com

Office 1107, Ookayama West 8th Building

Friday — October 23th, 2015 (This document was updated on June 21, 2017)

We give the proof that resolution requires large refutation for the pigeonhole principle.

A notation I forgot to define in the first lecture.

Definition 1 (Derivation)**.** *We denote as $\phi \vdash_{\pi} C$ the fact that π is a derivation of C from ϕ. We may omit π depending on the context.*

Lower bound for resolution refutations of pigeonhole principle

The pigeonhole principle claims that whenever we want to put $n+1$ pigeons into n holes, there must be a hole containing two pigeons. This seemly innocent claim is the primitive form of essentially all counting and probabilistic arguments, and it is often the endpoint of impossibility results. This statement can be encoded as an unsatisfiable CNF formula

$$\bigvee_{j\in[n]} p_{i,j} \qquad \text{for every } i \in [n+1]; \tag{1}$$

$$\bar{p}_{i,j} \vee \bar{p}_{i',j} \qquad \text{for every distinct } i, i' \in [n+1] \text{ and } j \in [n]; \tag{2}$$

where the first clauses claim that all pigeons must have a hole (*pigeon axioms*) and the other clauses claim that no two pigeons can sit in the same hole (*hole axioms*).

Exercise 2. Find a pigeohole principle resolution refutation of size $2^{O(n\log n)}$.

Exercise 3. Find a pigeohole principle resolution refutation of size $2^{O(n)}$.

Maybe the most famous result in proof complexity is the fact that any resolution refutation of this formula requires length $2^{\Omega(n)}$. The original result is due to Haken but we are going to show a proof due to Pavel Pudlák, which is based of the interpretation of resolution as a Prosecutor/Defendant game.[1]

The intuition of the game is that the Prosecutor (female) claim that the formula ϕ is unsatisfiable and the Defendant (male) claims that ϕ is satisfiable, and that he actually knows a satisfying assignment. The goal of the Prosecutor is to publicly uncover the Defendant lie. At each round the Prosecutor moves and she can either

- Ask Defendant for the value of some variable x_i, and save his answer to a public record;
- delete some information from the public record.

[1] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985; and Pavel Pudlák. Proofs as games. *American Mathematical Monthly*, pages 541–550, 2000

The Defendant must answer to all questions with either 0 or 1, but he is allowed to answer differently to the same question, if the previous answer is not on the public record.[2]

> The Prosecutor wins when the partial assignment on the public record falsifies one of the initial clauses of ϕ. The Defendant wins if he has a way to play the game forever without getting caught.

Exercise 4. Prove that the Prosecutor can only win if ϕ is unsatisfiable.

This game is interesting because any resolution refutation can be transformed in a strategy for the Prosecutor to catch the Defendant, and vice versa, keeping essentially the same size. Therefore it is possible to prove resolution lower bounds by showing lower bounds for the size of the Prosecutor strategy.

Lemma 5. *Consider a resolution refutation of ϕ of size s, there is a Prosecutor strategy of size at most $3s$ for the Prosecutor/Defendant game on ϕ.*

Proof sketch. I suggest to see the paper for all the details of this proof.[3] The idea is that the Prosecutor would walk backward along the refutation of ϕ, keeping a pointer on some clause in it. She keeps the invariant that her public record is exactly the smallest partial assignment falsifing that clause. She starts at the empty clause C_ℓ, and indeed her record at the beginning of the game is the empty record. At each point during the game, the Prosecutor points to a clause C_i and its record corresponds to the assignment $\neg C_i$. If C_i was derived by weakening from some C_j, then the assignment $\neg C_j$ is just a sub assignment of $\neg C_i$. The Prosecutor deletes $\neg C_i \setminus \neg C_j$ and point to clause C_j. If $C_i = A \vee B$ for some $C_j = A \vee x$ and $C_{j'} = \bar{x} \vee B$, then Prosecutor queries variable x and save its answer to the record. Let's assume the answer is 0, then the record now contains $\neg C_i \cup \{x = 0\}$ which falsifies $A \vee x$. The Prosecutor now will remove some of the variable assignment from the record to get exactly the negation of $A \vee x$. If the Defendant answers 1 then Prosecutor acts in essentially the same way, but he ends up with the negation of $\bar{x} \vee B$ on the record. Therefore now the Prosecutor points to either C_j or $C_{j'}$. You can see that Prosecutor is walking the refutation backward. At some point she ends up at one of the initial clauses of ϕ, and with its negation on the public record, therefore she wins. We stress that this describes a valid Prosecutor strategy because it is well defined whatever the Defendant answers. The Prosecutor does two moves per resolution inference, so the size doubles. □

Exercise 6. Show that from any Prosecutor strategy there is a corresponding resolution refutation of essentially the same size. Furthermore, if the Prosecutor never deletes infomation from the record, then the refutation can be made tree-like.

It is important to maintain the following intuition:

- a Prosecutor strategy corresponds to a resolution upper bound;
- a Defendant strategy corresponds to a resolution lower bound.

[2] The strategy of a Prosecutor in this game is essentially a list of records so that for each non-winning record she knows which question to ask, and so that whatever answer she gets the new record is in the list. The "size" of a Prosecutor strategy is the number of records in that list. This explain why the Prosecutor would do the counterintuitive move of deleting information from the public record. In this way she can identify together several games positions, reducing the overall size of the strategy.

[3] Pavel Pudlák. Proofs as games. *American Mathematical Monthly*, pages 541–550, 2000

We now prove the following theorem from[4]. Notice that in that paper Prosecutor is called “Prover” and the Defendant is called “Adversary”.

Theorem 7 (Pudlák, 2000)**.** *There is a positive ε such that any Prosecutor strategy must have size at least $2^{\varepsilon n}$.*

Proof sketch. The Defendant uses a (randomized) strategy so that, with probability 1 against any Prosecutor, make the game reach a “complex record”. Namely a record in which there are $n/4$ pigeons where either a hole is assigned or $n/2$ holes are excluded. It turns out that given any such record, the probability that the gameplay between Prosecutor and Defendant passes through such record is exponentially small. Therefore the Prosecutor strategy must containt an exponential number of such records. For full details see the paper or the proof in class. □

References

[Hak85] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[Pud00] Pavel Pudlák. Proofs as games. *American Mathematical Monthly*, pages 541–550, 2000.

[4] Pavel Pudlák. Proofs as games. *American Mathematical Monthly*, pages 541–550, 2000