My favorite proof method

Lightning talk

Presented by:
Pedro Bonilla Nadal (pedrobn@)

31 de agosto de 2021

Overview

Existence by probability

Some theorems

Constructivist approach

Existence by probability

A new proof method

The probabilistic method is a useful method to prove the existence of objects with an specific property.

1. Define the space.
2. Define how to generate objects.
3. Check the probability on a random object.
4. Profit.

- Philosophy: instead of giving the object explicitly, we consider a random object and compute the probability of satisfying the property.
- Great for decision problems.
- Many of its examples are thanks to Paul Erdős.

Some theorems

SAT problem

Given a propositional logic formula, check out whether it exists a truth assignment that satisfy the formula.

Example

- $(x \vee y) \wedge (\neg y \vee \neg x)$ is satisfiable by $x \to \top, y \to \bot$.
- $(\neg x \vee y) \wedge (z \vee \neg y) \wedge (\neg z) \wedge (x)$ is not satisfiable.

Usually formulas are presented as disjoints of clauses (also called conjunctions), as in the example. Therefore the problem is to solve every clause at the same time. Original NP-complete problem. Finally, $\Gamma^*_G(A)$ is the graph with vertex the clauses of a formula G, and there is an edge between C and D iff they conflict in some variable.

Lovasz Local Lemma

Theorem (Lovász Local Lemma for SAT)

Let $F = C_1 \wedge ... \wedge C_n$ be a formula. If there exists a mapping $\mu : \{C_1, ..., C_n\} \to (0, 1)$ that associates a number with each clause in the formula. We define the event:

$$A_i = \left[C_i \quad \begin{array}{c} \text{being falsified by a random} \\ \text{truth assignment} \end{array} \right],$$

If it happens

$$\forall i \in 1, .., , n : P() \leq \mu() \prod_{D \in \Gamma_G^*(C)} (1 - \mu(D)),$$

then the $P(\cap_{i=1}^{n} \neg A_i)$ F is satisfiable.

Corollary

Corollary
Let F be a formula on which each clause have k variables. If $\forall C \in F$ and $|\Gamma_F(C)| \leq 2^k/e - 1$ then F is satisfiable.

Constructivist approach

The revenge of the contructivist I

Moser proves that there exists an algorithm such that it gives an assignment satisfying the SAT formula, should it happen that the formula satisfies 2 conditions. This is no a big deal, as a backtrack would be also capable of providing the solution, given that we know its existence. Not so trivial is that it would run in $O(|F|)$.

Thanks for coming.