Albina Lialina
albinapt1u@gmail.com

Abstract

We consider the problem of finding a simultaneous root to a system

$$\begin{cases} P_1(\overline{x}) = 0 \\ \dots \\ P_m(\overline{x}) = 0, \end{cases}$$

where P_i are polynomials of degree at most d and coefficients from $\mathbb{F}_2$ and $\overline{x}$ also is from $\mathbb{F}_2$. It is well known that this problem is NP-complete, and we will prove better than brute force bound $O^*(2^{(n-n/(2.7d))})$.

The task of finding the solution reduces to a decision problem. In its turn, the task of deciding whether there is a solution reduces to computing the parity of the number of such solutions. It can be done by isolation technique proposed by Valiant and Vazirani, which inserts $O(n)$ random linear equations into the system. And the new system with good probability has only one solution if the old one had any.

So, we want to compute the parity of the number of solutions. We will solve this problem recursively. The following scheme illustrate the reduction to instance of itself. From now on all arithmetic is over $\mathbb{F}_2$.

1. **Parity as a sum**
   Determining the parity of the number o solutions amounts to computing the sum
   $$I_F = \sum_{x \in \{0,1\}^n} F(x),$$
   where $F(x) = (1 + P_1(x)) \dots (1 + P_m(x))$.

2. **Approximation F by probabilistic polynomials**
   The degree of F could be as big as dm. It is inconvenient for us so we approximate F with independently chosen polynomials $f_1, f_2, \dots f_s$, where every $f_i = (1 + R_1(x)) \dots (1 + R_l(x))$. All R_j are chosen independently for all f_i.

3. **Summing in parts**
   To make the algorithm faster we use the following trick. We draw $A \sqcup B = \{1, \dots n\}$. Then for every function f we have
   $$I_f = \sum_{X \in \{1,\dots n\}} f(X) = \sum_{Z \subset B} \sum_{X \subset A} f(X \cup Z) := \sum_{Z \subset B} I_{f|_A^{Z \to B}}.$$
   The last equality is just a notation that we are going to use further.

4. **Approximation of I_F**
   Suppose we have summed each approximation $f_1, f_2, \dots f_s$ in parts. Then to count I_F we use the majority function.
   $$I_Z = MAJ(I_{f_1|_A^{Z \to B}}, I_{f_2|_A^{Z \to B}}, \dots, I_{f_s|_A^{Z \to B}}),$$
   then we show that with a good probability $I_F = \sum\limits_{Z \subset B} I_Z$.

5. **Summing the parts and reduction to Parity**
Recall that $f_i = (1 + R_1(x)) \dots (1 + R_l(x))$. Let's denote

$$Q_j = R_j|_A^{Z \to B},$$

then to sum the parts we need to compute the following

$$f|_A^{Z \to B}(x) = (1 + Q_1(x)) \dots (1 + Q_l(x)),$$

which is equivalent to computing the parity of the number of solutions of the following system

$$\begin{cases} Q_1(\overline{x}) = 0 \\ \dots \\ Q_l(\overline{x}) = 0, \end{cases}.$$

That is how we got reduction to several smaller but similar problems. And if you choose all the parameters wisely we get the bound that was mentioned above.