Algoritmi probabilişti

Radu T. Trîmbiţaş

October 17, 2016

1 Verificarea unor identităţi

Următorul exemplu se referă la verificarea unor identităţi.

Fie $f(x_1, \ldots, x_n)$ un polinom cu coeficienţi raţionali de n variabile de grad cel mult k în fiecare dintre variabile. Vrem să decidem dacă $f \equiv 0$. Ideea de bază este să înlocuim variabilele cu numere aleatoare şi să calculăm valoarea polinomului. Dacă aceasta nu este zero polinomul nu poate fi identic nul. Dacă pentru un număr de încercări suficient de mare, se obţine de fiecare dată valoarea zero, probabilitatea ca polinomul să nu fie identic nul este mică. Vom alege pentru variabile valori întregi din intervalul $[0, N-1]$, independente şi uniform distribuite. Are loc următorul rezultat:

Lemma 1 (Schwarz) *Dacă f nu este identic nul şi valorile ξ_i sunt independente şi uniform distribuite în intervalul $[0, N-1]$, atunci*

$$P\left(f\left(\xi_1, \ldots, \xi_n\right) = 0\right) \leq \frac{kn}{N}.$$

Proof. Se face prin inducţie după n. Lema este adevărată pentru $n = 1$, deoarece un polinom într-o variabilă de grad k poate avea cel mult k rădăcini. Fie $n > 1$ şi să ordonăm f după puterile lui x_1:

$$f = f_0 + f_1 x_1 + f_2 x_1^2 + \cdots + f_t x_1^t,$$

unde $f_0, \ldots, f_t$ sunt polinoame în variabilele $x_2, \ldots, x_n$, termenul f_t nu este identic 0 şi $t \leq k$. Aplicând formula probabilităţii totale avem

$$\begin{aligned}
&P\left(f(\xi_1, \ldots, \xi_n) = 0\right) \leq \\
&P\left(f(\xi_1, \ldots, \xi_n) = 0 | f_t(\xi_2, \ldots, \xi_n) = 0\right) P\left(f_t(\xi_2, \ldots, \xi_n) = 0\right) + \\
&\quad + P\left(f(\xi_1, \ldots, \xi_n) = 0 | f_t(\xi_2, \ldots, \xi_n) \neq 0\right) P\left(f_t(\xi_2, \ldots, \xi_n) \neq 0\right) \\
\leq &P\left(f_t(\xi_2, \ldots, \xi_n) = 0\right) + P\left(f(\xi_1, \ldots, \xi_n) = 0 | f_t(\xi_2, \ldots, \xi_n) \neq 0\right).
\end{aligned}$$

Primul termen poate fi estimat folosind ipoteza inducţiei, iar al doilea este cel mult k/N (căci ξ_1 este independentă de variabilele $\xi_2, \ldots, \xi_n$ şi de aceea dacă

ultimele sunt fixate astfel ca $f_t \neq 0$ şi f ca polinom în x_1 nu este identic nul, atunci probabilitatea ca ξ_1 să fie rădăcină este cel mult k/N). Deci

$$P\left(f(\xi_1, \ldots, \xi_n) = 0\right) \leq \frac{k(n-1)}{N} + \frac{k}{N} \leq \frac{kn}{N}.$$

■

Aceasta ne conduce la următorul algoritm: calculăm $f(\xi_1, \ldots, \xi_n)$ pentru valorile întregi ξ_i care sunt numere (pseudo) aleatoare independente distribuite uniform discret în intervalul $[0, 2kn]$. Dacă obţinem o valoare diferită de 0 ne oprim : f nu este identic nul. Dacă obţinem valoarea 0 repetăm calculul. Dacă obţinem valoarea 0 de, să zicem 100 de ori, ne oprim şi decidem că f este identic nul.

Remark 2 *Dacă numărul de repetări de repetări este l, probabilitatea ca algoritmul să decidă eronat că $f \equiv 0$ este $< 2^{-l}$, deoarece probabilitatea de a greşi la o încercare este $\leq 1/2$, iar încercările sunt independente.*