UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Probabilità

Marco Isopi

12. Identità polinomiali e Lemma di Schwartz-Zippel

Scopo della lezione

Obiettivi della lezione:

1. verifica probabilistica delle identità polinomiali;
2. Lemma di Schwartz-Zippel.

Dedicheremo questa lezione a mostrare come un algoritmo randomizzato possa essere estremamente più efficiente della sue controparti deterministiche.

Un esempio di problema reale per il quale esiste un algoritmo randomizzato semplice ed efficiente, ma nessun algoritmo deterministico che giri in tempo polinomiale, è quello di stabilire se due polinomi sono uguali.

Identità polinomiali

Per verifica delle identità polinomiali intenderemo il problema di determinare se un polinomio in n variabili è identicamente nullo oppure no.

Difatti stabilire se il polinomio P è uguale al polinomio Q, equivale a verificare se $P - Q$ è identicamente nullo.

Il problema accetta come input due polinomi P e Q in n variabili a coefficienti, per esempio, reali e e decide se $P = Q$.

Per esempio, se abbiamo $P(x_1, x_2) = (1 + x_1)(1 + x_2)$ e $Q(x_1, x_2) = 1 + x_1 + x_2 + x_1 x_2$, l'algoritmo deve terminare con una risposta affermativa.

Identità polinomiali

Questo problema appare in molti contesti, fra cui la crittografia a chiave pubblica.

Il modo ovvio di attaccare il problema è moltiplicare tutti i fattori, semplificare e controllare se i coefficienti sono tutti nulli.

Sfortunatamente l'esecuzione di un algoritmo che porta a termine questo compito richiede un tempo esponenziale.

Identità polinomiali

Per esempio il polinomio $P(x) = \prod_{i=1}^{n-1}(x_i + x_{i+1})$ scritto in questa forma ha lunghezza $O(n)$, ma una volta sviluppato il prodotto consiste di $O(2^n)$ monomi.

Faremo l'ipotesi che invece si possa calcolare in maniera efficiente il valore di un polinomio dato in un qualunque punto $(x_1, x_2, \ldots, x_n)$.

Facendo uso di questo fatto esibiremo un semplice algoritmo randomizzato per il problema.

Identità polinomiali

Per esempio ci chiediamo se

$$(2x_1 - 5x_2 + x_3)(2x_2 + x_5 - 6)\ldots(x_3 + x_6 - x_{17} + 1)$$

è identicamente nullo oppure no.

Supponiamo di calcolare il valore del polinomio in un certo numero di punti e che il risultato sia sempre nullo.
Possiamo concludere che il polinomio è identicamente nullo?

Naturalmente no.
Ma se i punti sono tanti molto probabilmente sarà nullo.

Lemma di Schwartz-Zippel

Possiamo rendere precisa questa intuizione tramite il

Lemma di Schwartz-Zippel

Sia $P(x_1, x_2, \ldots x_n)$ un polinomio di grado d in n variabili.
Sia S un sottoinsieme finito dei numeri reali.
Scegliamo $r_1, r_2, \ldots, r_n$ a caso da S.

Allora

$$\mathbf{P}\Big(P(r_1, r_2, \ldots r_n) = 0\Big) \leq \frac{d}{|S|}.$$

Lemma di Schwartz-Zippel

Dimostrazione

Iniziamo osservando che se $n = 1$, l'enunciato è vero banalmente. Sappiamo che un polinomio di grado d in una variabile ha al più d radici reali.

Se le radici sono effettivamente d e appartengono tutte all'insieme S, la probabiltà di sceglierne una pescando a caso è proprio $\frac{d}{|S|}$.

Dimostreremo il caso generale per induzione sul numero n di variabili.

Supponiamo vero l'enunciato per tutti i polinomi in al più $n - 1$ variabili.

Lemma di Schwartz-Zippel

Pensiamo a P come un polinomio in x_1 scrivendolo

$$P(x_1, x_2, \ldots x_n) = \sum_{i=0}^{k} x_1^i P_i(x_2, \ldots x_n)$$

dove k è la più alta potenza di x_1 che compare in P.

Per come abbiamo definito k, P_k non può essere identicamente nullo.

Lemma di Schwartz-Zippel

Inoltre il suo grado può essere al massimo $d - k$ e quindi

$$\mathbf{P}\Big(P_k(r_2, \ldots r_n) = 0\Big) \leq \frac{d-k}{|S|}$$

Chiamiamo B l'evento $\{P_k(r_2, \ldots r_n) = 0\}$.

Lemma di Schwartz-Zippel

Scegliamo a caso $r_2, \ldots r_n$ e supponiamo che B non si verifichi.

Definiamo il polinomio di una variabilie

$$f(x_1) = \sum_{i=0}^{k} x_1^i P_i(r_2, \ldots r_n) = P(x_1, r_2, \ldots r_n).$$

Dato che B non si verifica, il coefficiente di x_1^k è diverso da 0 e quindi f non è identicamente nullo.

Lemma di Schwartz-Zippel

Quindi

$$\mathbf{P}\Big(f(x_1) = 0 \mid B^C\Big) \leq \frac{k}{|S|}.$$

Chiamiamo A l'evento $\{P(r_1, r_2, \ldots r_n) = 0\}$.

Abbiamo:

$$\begin{aligned}
\mathbf{P}(A) &= \mathbf{P}(A \cap B) + \mathbf{P}(A \cap B^C) \\
&= \mathbf{P}(A|B)\mathbf{P}(B) + \mathbf{P}(A|B^C)\mathbf{P}(B^C) \\
&\leq \mathbf{P}(B) + \mathbf{P}(A|B^C) \\
&\leq \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}.
\end{aligned}$$

Lemma di Schwartz-Zippel

Abbiamo enunciato e dimostrato il lemma di Schwartz-Zippel per variabili reali, ma l'enunciato e la dimostrazione sono identici se ai reali si sostituisce un qualunque campo.