Complementi di Algoritmi e Strutture Dati

Le classi di complessità probabilistiche

Docente: *Nicolò Cesa-Bianchi* versione 20 marzo 2018

Un algoritmo probabilistico per un problema di decisione $X = (\mathcal{I}, q)$ può essere visto come un algoritmo deterministico che ha accesso ad una stringa Z di bit casuali. L'algoritmo calcola una funzione $B : \mathcal{I} \times \{0,1\}^* \to \{0,1\}$ tale che, per ogni $I \in \mathcal{I}$, $B(I, Z) = q(I)$ con una certa probabilità rispetto all'estrazione della stringa Z.

In analogia con la definizione della classe $\mathcal{NP}$, possiamo definire le classi di problemi di decisione solubili in tempo polinomiale da diversi tipi di algoritmi probabilistici rivisitando la nozione di certificatore polinomiale.

La classe di problemi di decisione risolti da algoritmi Montecarlo two-sided è la classe $\mathcal{BPP}$. Un problema di decisione $X = (\mathcal{I}, q)$ appartiene alla classe $\mathcal{BPP}$ se esiste una funzione $B : \mathcal{I} \times \{0,1\}^* \to \{0,1\}$ calcolabile in tempo polinomiale e un polinomio $p(\cdot)$ tali che, per ogni istanza $I \in \mathcal{I}$, essi soddisfano

$$\mathbb{P}\big(B(I, Z) \neq q(I)\big) \leq \frac{1}{3} \tag{1}$$

dove la probabilità è calcolata rispetto all'estrazione di Z con probabilità uniforme da $\{0,1\}^{p(|I|)}$.

Si noti che la costante $\frac{1}{3}$ è arbitraria dato che, come abbiamo visto, la probabilità di errore di un algoritmo two-sided può essere ridotta tramite il meccanismo di amplificazione. Infatti, una definizione equivalente di $\mathcal{BPP}$ sostituisce (1) con

$$\mathbb{P}\big(B(I, Z) \neq q(I)\big) \leq \frac{1}{2} - \frac{1}{p'(|I|)}$$

dove $p'(\cdot)$ è un polinomio. Il meccanismo di amplificazione tramite Lemma di Chernoff-Hoeffding implica che è sufficiente eseguire l'algoritmo un numero di volte pari a ordine di $p'(|I|)^2$ per ottenere una probabilità di errore limitata da $\frac{1}{3}$. Dato che $p'(\cdot)$ è un polinomio, l'algoritmo risultante è ancora polinomiale in $|I|$.

Si noti che $\mathcal{P} \subseteq \mathcal{BPP}$, dato che avendo un algoritmo polinomiale per calcolare la funzione di decisione q possiamo implementare il certificatore B in tempo polinomiale con probabilità di errore pari a zero. Non è invece noto se $\mathcal{P} \equiv \mathcal{BPP}$, ovvero se ogni algoritmo Montecarlo two-sided possa essere "derandomizzato" in modo da ottenere un algoritmo deterministico polinomiale per lo stesso problema. Non è neanche noto se $\mathcal{BPP} \subseteq \mathcal{NP}$. D'altra parte, dato che la condizione (1) è simmetrica rispetto al valore di $q(I)$, ne deduciamo che $\mathcal{BPP}$ è chiusa rispetto al complemento, ovvero $\mathcal{BPP} \equiv \text{co}{-}\mathcal{BPP}$.

La classe di problemi di decisione risolti da algoritmi Montecarlo one-sided è la classe $\mathcal{RP}$. Un problema di decisione $X = (\mathcal{I}, q)$ appartiene alla classe $\mathcal{RP}$ se esiste una funzione $B : \mathcal{I} \times \{0,1\}^* \to \{0,1\}$ calcolabile in tempo polinomiale e un polinomio $p(\cdot)$ tali che, per ogni istanza $I \in \mathcal{I}$, essi soddisfano

$$\begin{aligned} &\mathbb{P}\big(B(I, Z) = 1\big) \geq \tfrac{1}{2} && \text{se } q(I) = 1, \\ &\forall z \in \{0,1\}^{p(|I|)} \quad B(I, z) = 0 && \text{se } q(I) = 0 \end{aligned} \tag{2}$$

dove la probabilità nella prima condizione di (2) è calcolata rispetto all'estrazione di Z con probabilità uniforme da $\{0,1\}^{p(|I|)}$.

Quindi l'algoritmo è sempre corretto su output 1 mentre sbaglia con probabilità al più $\frac{1}{2}$ su output 0. Anche in questo caso la costante $\frac{1}{2}$ è arbitraria dato che possiamo ridurre la probabilità di errore tramite il meccanismo di amplificazione. Infatti, possiamo dare una definizione equivalente di $\mathcal{RP}$ sostituendo la prima condizione di (2) con

$$\mathbb{P}\big(B(I,Z)=1\big) \geq \frac{1}{p'(|I|)} \qquad \text{se } q(I)=1$$

dove $p'(\cdot)$ è un polinomio. Il meccanismo di amplificazione implica che è sufficiente eseguire l'algoritmo un numero di volte pari a ordine di $p'(|I|)$ per ottenere una probabilità di errore limitata da $\frac{1}{2}$. Dato che $p'(\cdot)$ è un polinomio, l'algoritmo risultante è ancora polinomiale in $|I|$.

Con un ragionamento simile a quello che ci ha portato a concludere che $\mathcal{P} \subseteq \mathcal{BPP}$, possiamo anche dimostrare che $\mathcal{P} \subseteq \mathcal{RP}$. Ma, a differenza di $\mathcal{BPP}$, questa volta possiamo stabilire una relazione fra $\mathcal{RP}$ e $\mathcal{NP}$. Infatti, la definizione di $\mathcal{NP}$ può essere equivalentemente riscritta nel modo seguente. Un problema di decisione $X=(\mathcal{I},q)$ appartiene alla classe $\mathcal{NP}$ se esiste una funzione $B:\mathcal{I}\times\{0,1\}^* \to \{0,1\}$ calcolabile in tempo polinomiale e un polinomio $p(\cdot)$ tali che, per ogni istanza $I\in\mathcal{I}$, essi soddisfano

$$\begin{aligned} &\exists z \in \{0,1\}^{p(|I|)} \quad B(I,z)=1 \quad \text{se } q(I)=1, \\ &\forall z \in \{0,1\}^{p(|I|)} \quad B(I,z)=0 \quad \text{se } q(I)=0. \end{aligned}$$

Dato che per la prima condizione di (2), $\mathbb{P}\big(B(I,Z)=1\big)\geq\frac{1}{2}$ implica $\exists z\in\{0,1\}^{p(|I|)}\ B(I,z)=1$, mentre la seconda condizione di (2) è uguale sia nella definizione di $\mathcal{RP}$ che in quella di $\mathcal{NP}$, concludiamo che $\mathcal{RP}\subseteq\mathcal{NP}$. In altre parole, interpretiamo i bit casuali Z nella definizione di $\mathcal{RP}$ come un certificato del fatto che $q(I)=1$.

La classe co$-\mathcal{RP}$ contiene i problemi che sono complementi di problemi in $\mathcal{RP}$. La definizione di co$-\mathcal{RP}$ è semplicemente ottenuta scrivendo in (2) $q(I)=0$ al posto di $q(I)=1$ e viceversa. Con una dimostrazione simile a quella di $\mathcal{RP}\subseteq\mathcal{NP}$ possiamo dimostrare che co$-\mathcal{RP}\subseteq$ co$-\mathcal{NP}$. Come vale $\mathcal{P}\subseteq\mathcal{RP}$ così possiamo dimostrare che $\mathcal{P}\subseteq$ co$-\mathcal{RP}$.

Possiamo mettere in relazione $\mathcal{RP}$ e co$-\mathcal{RP}$ con $\mathcal{BPP}$ riscrivendo la definizione di quest'ultima come

$$\begin{aligned} &\mathbb{P}\big(B(I,Z)=1\big)\geq\tfrac{2}{3} \quad \text{se } q(I)=1, \\ &\mathbb{P}\big(B(I,Z)=0\big)\geq\tfrac{2}{3} \quad \text{se } q(I)=0. \end{aligned} \tag{3}$$

Ricordando che possiamo amplificare la probabilità di essere corretti nelle definizioni di $\mathcal{RP}$ e co$-\mathcal{RP}$ arriviamo alla conclusione $\mathcal{RP}\subseteq\mathcal{BPP}$ e co$-\mathcal{RP}\subseteq\mathcal{BPP}$.

Introduciamo ora la classe $\mathcal{ZPP}\equiv\mathcal{RP}\cap$ co$-\mathcal{RP}$. Un problema di decisione $X=(\mathcal{I},q)$ appartiene alla classe $\mathcal{ZPP}$ se esistono due funzioni $B,B':\mathcal{I}\times\{0,1\}^*\to\{0,1\}$ calcolabili in tempo polinomiale e due polinomi $p(\cdot),p'(\cdot)$ tali che, per ogni istanza $I\in\mathcal{I}$, essi soddisfano

$$\begin{aligned} &\mathbb{P}\big(B(I,Z)=1\big)\geq\tfrac{1}{2} \quad \text{e} \quad \forall z\in\{0,1\}^{p'(|I|)} \quad B'(I,z)=1 \quad \text{se } q(I)=1, \\ &\mathbb{P}\big(B'(I,Z)=0\big)\geq\tfrac{1}{2} \quad \text{e} \quad \forall z\in\{0,1\}^{p(|I|)} \quad B(I,z)=0 \quad \text{se } q(I)=0, \end{aligned} \tag{4}$$

dove le probabilità sono calcolate rispetto all'estrazione di Z con probabilità uniforme da $\{0,1\}^{p(|I|)}$.

Non è difficile vedere che la classe $\mathcal{ZPP}$ è la classe dei problemi risolti da algoritmi Las Vegas che terminano in tempo atteso limitato da un polinomio nella lunghezza dell'istanza. Infatti, se $\mathcal{X} \in \mathcal{ZPP}$ allora posso costruire un algoritmo probabilistico A che, su input $I \in \mathcal{I}$, esegue alternativamente B e B' arrestandosi non appena $B(I,Z) = 1$ oppure $B'(I,Z) = 0$. In entrambi questi casi sappiamo che l'output è corretto, quindi A si arresta sempre con la soluzione corretta. Gli output $B(I,Z) = 0$ e $B'(I,Z) = 1$ sono invece errati con probabilità al più $\frac{1}{2}$. Quindi la probabilità che su una particolare istanza I valga $B(I,Z) = 0$ e $B'(I,Z) = 1$ è al più $\frac{1}{4}$. Se invece $B(I,Z) = B'(I,Z)$ allora $q(I) = B(I,Z) = B'(I,Z)$. Il numero atteso di ripetizioni di B e B' è quindi al più $\frac{4}{3} < 2$. Dato che per ipotesi B e B' terminano entrambi in tempo polinomiale, il tempo atteso di calcolo di A è pure polinomiale.

D'altra parte, sia A è un algoritmo Las Vegas per $(\mathcal{I}, q)$ e sia $\mu(I) < p(|I|)$ il valore atteso del tempo di calcolo $T_A(I)$ di A su input I. Per la disuguaglianza di Markov,

$$\mathbb{P}\big(T_A(I) \geq \lceil 2\mu(I) \rceil\big) \leq \frac{1}{2} \, .$$

Quindi se su input I arresto A dopo $\lceil 2\mu(I) \rceil$ passi, la probabilità che A non abbia terminato è al più $\frac{1}{2}$. Viceversa, quando A termina l'output è sempre corretto. Possiamo quindi costruire due algoritmi A_B e $A_{B'}$ che implementano le funzioni B e B'. A_B esegue A e produce 0 se A non termina. Quindi quando $q(I) = 0$ l'output è deterministicamente 0, mentre quando $q(I) = 1$ l'output è 1 con probabilità almeno $\frac{1}{2}$. In modo simile dimostriamo che $A_{B'}$ implementa B'. Dato che $\mu(I) < p(|I|)$, A_B e $A_{B'}$ terminano entrambi in tempo deterministico polinomiale.

Dato che $\mathcal{P}$ è incluso sia in $\mathcal{RP}$ che in co$-\mathcal{RP}$, abbiamo che $\mathcal{P} \subseteq \mathcal{ZPP}$.