Algorytmy probabilistyczne

Lista zadań nr 5

1. Rangą klucza x w zbiorze S nazywamy liczbę elementów S nie większych niż x. Wykazać, że oczekiwana długość (unikalnej) ścieżki pomiędzy dwoma kluczami x i y z najniższego poziomu w liście z przeskokami wynosi $O(\log r)$, gdzie r oznacza różnicę rang x i y w zbiorze kluczy umieszczonych w tej liście. W takiej ścieżce możemy przechodzić po elementach list w obu kierunkach.

2. Wykazać, że złożoność czasowa operacji $FIND(x, S)$, gdzie S oznacza zbiór kluczy w liście z przeskokami, wynosi $O(\log |S|)$ z dużym prawdopodobieństwem. Użyć nierówności w stylu Chernoffa dla sumy niezależnych zmiennych z rozkładem geometrycznym (wystarczy skorzystać z takiej nierówności - nie trzeba jej udowadniać).

3. Wykazać, że jeśli H jest silnie 2-uniwersalna, to jest 2-uniwersalna.

4. Niech $p \geq m$ będzie liczbą pierwszą. Rozważamy rodzinę funkcji haszujących

$$H = \{h_a : 0 < a < p, h_a(x) = (ax \bmod p) \bmod m\}.$$

Udowodnić, że H nie jest 2-uniwersalna. Następnie pokazać, że dla każdej pary $x \neq y$ ze zbioru $\{0, \ldots, p-1\}$ zachodzi nierówność $\delta(x, y, H) \leq 2|H|/m$

5. Niech $U = \{0,1\}^n$ oraz $M = \{0,1\}^m$. Funkcję haszującą h_A wyznacza macierz 0-1 o $n+1$ wierszach i m kolumnach. Definiujemy ją jako $h_A(x) = x^1 \cdot A \bmod 2$, gdzie wektor x^1 ma rozmiar $n+1$ i powstaje z x przez dopisanie 1 na końcu. Wykazać, że zbiór takich funkcji jest 2-uniwersalny. Czy jest on silnie 2-uniwersalny?

6. W wielozbiorze elementy mogą się powtarzać. Dwa wielozbiory są równe, jeśli mają takie same elementy występujące w nich identyczna liczbę razy. Równość wielozbiorów można sprawdzić sortując je i porównując kolejne elementy (w czasie $O(n \log n)$), gdzie n oznacza rozmiar wielozbioru. Algorytm zrandomizowany może użyć funkcji haszującej z 2-uniwersalnej rodziny H o przeciwdziedzinie rozmiaru cn i w czasie liniowym pozliczać wartości funkcji dla pierwszego i drugiego wielozbioru. Uzupełnić szczegóły i przeanalizować prawdopodobieństwo błędu w takim algorytmie Monte Carlo. Czy można go rozszerzyć do algorytmu Las Vegas?

2 kwietnia 2019

Marek Piotrów