Szansa na sukces

Metoda probabilistyczna gościła już na łamach *Delty* (np. w numerach 12/2006 i 4/2015), byłoby jednak nieprawdopodobnie głupio pominąć ją w numerze poświęconym dowodom. W najbardziej podstawowej wersji może się ona okazać przydatna w sytuacji, gdy chcemy wykazać istnienie obiektu spełniającego określone warunki – wówczas możemy spróbować przedstawić schemat losowania badanych obiektów, w którym z dodatnim prawdopodobieństwem wynik będzie spełniał przedstawione żądania. Opis ten może brzmieć dość enigmatycznie, powinien stać się bardziej zrozumiały po lekturze poniższego rozumowania, uchodzącego za jeden z pierwszych przykładów zastosowania metody probabilistycznej.

Rozważmy graf pełny, którego każde dwa wierzchołki są połączone krawędzią w kolorze niebieskim bądź czerwonym. Okazuje się, co udowodnił Frank Ramsey w 1930 roku, że dla dowolnie zadanych liczb naturalnych k, l, jeśli liczba wierzchołków w grafie pełnym jest dostatecznie duża, istnieje w nim podgraf o k wierzchołkach połączonych wyłącznie niebieskimi krawędziami lub podgraf o l wierzchołkach, z których każde dwa połączone są krawędziami czerwonymi.

Podgraf danego grafu powstaje przez usunięcie z niego pewnej liczby wierzchołków wraz ze wszystkimi przylegającymi do nich krawędziami.

Najmniejszy z tych „dostatecznie dużych” rozmiarów wyjściowego grafu nazywamy *liczbą Ramseya* i oznaczamy przez $R(k,l)$.

Więcej o liczbach Ramseya przeczytać można w *Delcie* 3/2008.

W 1947 roku Paul Erdős przedstawił następujące oszacowanie z dołu liczby $R(k,k)$

$$(\star) \qquad \binom{R(k,k)}{k} \geqslant 2^{\binom{k}{2}-1}.$$

Oto jak uzyskał ten wynik: rozważmy graf o n wierzchołkach, gdzie n jest „niedostatecznie duże”, czyli $\binom{n}{k} < 2^{\binom{k}{2}-1}$. Pokażemy, że możemy pokolorować krawędzie tego grafu w taki sposób, by nie istniał podgraf rozmiaru k o wszystkich krawędziach w tym samym kolorze; zatem natychmiastowym wnioskiem będzie nierówność $(\star)$.

Każdą z krawędzi naszego grafu pomalujmy na niebiesko z prawdopodobieństwem $\frac{1}{2}$ lub na czerwono z tym samym prawdopodobieństwem. Wybierzmy dowolny podgraf o k wierzchołkach – wówczas zdarzenie, polegające na pomalowaniu wszystkich krawędzi wybranego podgrafu (których jest $\frac{k(k-1)}{2}$, inaczej $\binom{k}{2}$) na ten sam kolor, ma prawdopodobieństwo $2 \cdot 2^{-\binom{k}{2}}$. Podgrafów o k wierzchołkach jest jednak $\binom{n}{k}$. Szansa na to, że pewien z tych podgrafów ma krawędzie pomalowane na jeden kolor, nie przekracza $\binom{n}{k} 2^{1-\binom{k}{2}}$, zatem zgodnie z założeniem o „niedostatecznie dużym” n jest mniejsza od 1. W tej sytuacji szansa na to, że żaden z podgrafów o k wierzchołkach nie ma wszystkich krawędzi w tym samym kolorze, jest dodatnia, co dowodzi istnienia żądanego kolorowania.

Skorzystaliśmy z fundamentalnej nierówności rachunku prawdopodobieństwa, zgodnie z którą prawdopodobieństwo (przeliczalnej) alternatywy zdarzeń nie przekracza sumy prawdopodobieństw tych zdarzeń.

Łukasz RAJKOWSKI

Jak się pozbyć losowości?

W informatyce *losowość* jest bardzo przydatna. Często bardzo ułatwia rozumowania, pozwala na piękne i klarowne argumenty używające, na przykład, metody probabilistycznej. Nieraz łatwo znaleźć algorytm używający losowości (*randomizowany*) i działający szybko, podczas gdy znalezienie szybkiego algorytmu deterministycznego jest trudne lub w ogóle takiego nie znamy. Z losowością jest jednak pewien problem. Chciałoby się wiedzieć coś na pewno, a nie tylko z dużą dozą prawdopodobieństwa. Szczęśliwie okazuje się, że czasami da się tę losowość wprowadzić, a potem wyeliminować. Ta ostatnia operacja, eliminacja losowości, nazywa się *derandomizacją*.

Przedstawimy dwie metody derandomizacji. Zrobimy to na przykładzie, choć użyte techniki będą zdecydowanie bardziej ogólne. Rozważmy graf

Rozwiązanie zadania M 1525.
Przeprowadzimy *dowód nie wprost.*

Przypuśćmy, że $n+1$ jest nieparzystą liczbą pierwszą. Wówczas z małego twierdzenia Fermata wynika, że liczba 2^n-1 jest podzielna przez $n+1$, a zatem również

$$n(2^n-1)+(n+1)=n2^n+1$$

jest liczbą podzielną przez $n+1$. To przeczy pierwszości liczby $n2^n+1$, gdyż $n2^n+1>n+1$.
Podobnie, jeżeli $n+2$ jest nieparzystą liczbą pierwszą, to z małego twierdzenia Fermata wynika, że liczba $2^{n+1}-1$ jest podzielna przez $n+2$. Wobec tego również liczba

$$(n+2)2^n-(2^{n+1}-1)=n2^n+1$$

jest podzielna przez $n+2$, ale $n2^n+1>n+2$ na mocy nierówności $n(2^n-1)>1$ prawdziwej dla $n>1$. □

Uwaga. Najmniejszą liczbą $n\geqslant 2$, dla której $n2^n+1$ jest liczbą pierwszą, jest 141. Liczby postaci $n2^n+1$ nazywane są *liczbami Cullena.*

Rozwiązanie zadania M 1526.
Przeprowadzimy *dowód konstruktywny* – zidentyfikujemy rozwiązania danego równania.

Zauważmy, że jeżeli $|x|>2$, to

$$|f(x)|=x^2-2>2|x|-2>2|x|-|x|=|x|,$$

skąd wynika, że dane równanie nie może być spełnione. Wobec tego $|x|\leqslant 2$, a zatem $x=2\cos\varphi$ dla pewnego (a właściwie dwóch) $\varphi\in[0,\pi]$. Zauważmy, że skoro $\cos 2\alpha=2\cos^2\alpha-1$, to

$$f(2\cos\alpha)=4\cos^2\alpha-2=2\cos 2\alpha,$$

wobec czego

$$f(f(f(\ldots f(f(2\cos\varphi))\ldots)))=2\cos 2^n\varphi.$$

Dane równanie przybiera wówczas postać $\cos\varphi=\cos 2^n\varphi$, czyli

$$0=\cos\varphi-\cos 2^n\varphi=$$
$$=2\sin\frac{2^n-1}{2}\varphi\sin\frac{2^n+1}{2}\varphi,$$

skąd $\varphi=2k\pi/(2^n-1)$ lub $\varphi=2k\pi/(2^n+1)$ dla pewnej liczby całkowitej k. Pozostaje zauważyć, że jeżeli $0\leqslant k\leqslant 2^{n-1}-1$, to $0\leqslant 2k\pi/(2^n-1)\leqslant\pi$, jeżeli zaś $0\leqslant k\leqslant 2^{n-1}$, to $0\leqslant 2k\pi/(2^n+1)\leqslant\pi$, przy czym rozwiązania są różne, o ile tylko $k\neq 0$. Tym samym otrzymujemy łącznie $2^{n-1}+2^{n-1}+1-1=2^n$ różnych rozwiązań postaci $x=2\cos\varphi$. □

$G=(V,E)$. Dla podzbioru wierzchołków $S\subseteq V$ nazwiemy jego *cięciem* zbiór $\{(u,v)\in E\mid u\in S, v\notin S\}$, czyli zbiór krawędzi, które mają dokładnie jeden koniec w S. Problem znajdowania S o największym cięciu jest NP-zupełny. Rozważmy jednak podobny problem: znajdowania S takiego, że jego cięcie jest wielkości co najmniej połowy zbioru wszystkich krawędzi, czyli $|E|/2$.

Na pierwszy rzut oka nie jest wcale jasne, czy taki S istnieje. A więc na rozgrzewkę udowodnijmy to. Zachęcamy Czytelników do samodzielnej próby przed przeczytaniem rozwiązania. Rozwiązanie zaś jest zadziwiająco proste. Wylosujmy S, to znaczy każdy wierzchołek wrzućmy niezależnie do S z prawdopodobieństwem $1/2$. Wówczas każda krawędź z E będzie należała do cięcia S z prawdopodobieństwem $1/2$. A zatem średnia wielkość cięcia S to $|E|/2$, czyli na pewno musi istnieć S taki, że jego cięcie ma wielkość przynajmniej $|E|/2$. Powyższy dowód jest jednak *niekonstruktywny*, nie wynika z niego wcale, jak takie cięcie znaleźć. Oczywiście, możemy przejrzeć wszystkie możliwe zbiory S, ale to zajmie czas rzędu 2^n, gdzie $|V|=n$, a my chcemy znaleźć algorytm wielomianowy względem n.

Podamy dwie metody. Pierwsza nazywa się metodą *warunkowych wartości oczekiwanych*. Przypuśćmy, że przejrzeliśmy już pewien zbiór wierzchołków $U\subseteq V$ i dla każdego z nich zdecydowaliśmy, czy będzie on należał do S, czy nie. Jaka jest średnia wielkość cięcia S po tym ustaleniu? Przez $E(T,T')$ oznaczmy zbiór krawędzi między zbiorami T i T'. Na razie wiemy, że do cięcia na pewno będzie należała każda krawędź z $E(U\cap S, U\cap\bar{S})$, gdzie $\bar{S}$ to dopełnienie zbioru S. Jeśli chodzi o krawędzie jeszcze nieustalone, to każda krawędź z $E(U\cap S,\bar{U})$ będzie należała do cięcia z prawdopodobieństwem $1/2$. A zatem średnia wartość cięcia po ustaleniu, co się stanie z wierzchołkami z U, wynosi $|E(U\cap S, U\cap\bar{S})|+1/2\cdot|E(U\cap S,\bar{U})|$. Umiemy to obliczyć w czasie wielomianowym, znając U oraz decyzję odnośnie S na nim, czyli $U\cap S$ oraz $U\cap\bar{S}$. Teraz już tylko krok do rozwiązania. Gdy bowiem decydujemy o pierwszym wierzchołku, czy wrzucić go do S, czy nie, to obliczamy, jaka będzie średnia wartość cięcia w obu przypadkach. Ponieważ średnia z tych dwóch liczb jest większa lub równa $|E|/2$ (w tym przypadku równa), to jedna z nich też będzie większa lub równa. Wybieramy więc tę lepszą opcję i zabieramy się za drugi element. Przy dorzucaniu każdego nowego elementu wybieramy tę opcję, która daje większą średnią i w ten sposób po podjęciu decyzji dla wszystkich elementów V otrzymujemy pewien zbiór S, którego cięcie będzie większe lub równe $|E|/2$.

Drugie rozwiązanie jest jeszcze bardziej zaskakujące. Zauważmy, że tak naprawdę nie potrzebujemy wcale, by każdy wierzchołek z V był brany do S niezależnie. Do tego, by każda krawędź (u,v) znalazła się w cięciu S z prawdopodobieństwem $1/2$, wystarczy, by wierzchołki u i v były wzięte do S niezależnie, czyli wystarczy nam, by wybory były parami niezależne. A to jest dużo słabsze wymaganie! Co więcej, okazuje się, że z k niezależnych zmiennych losowych $X_1,\ldots,X_k$ o wartościach w $\{0,1\}$ można łatwo skonstruować 2^k zmiennych losowych parami niezależnych o wartościach w $\{0,1\}$. Po prostu dla każdego podzbioru $A\subseteq\{1,\ldots,k\}$ zmienna X_A jest zdefiniowana jako xor (alternatywa wykluczająca) zmiennych X_i takich, że $i\in A$. Nietrudno zauważyć, że dla dowolnych $A,B\subseteq\{1,\ldots,k\}$, $A\neq B$ zmienne X_A i X_B są niezależne. Dla uproszczenia przyjmijmy, że $|V|=n$ jest potęgą dwójki. A więc nasz algorytm możemy zamienić na taki, który losuje najpierw $\log n$ bitów X_i dla $i\in\{1,\ldots,\log n\}$, a potem gdy podejmuje losową decyzję, czy wrzucić jakiś wierzchołek z V do zbioru S, korzysta ze zmiennych X_A. Taki algorytm też w średnim przypadku skonstruuje cięcie wielkości $|E|/2$. Zauważmy jednak, że zamiast losować te $\log n$ wartości możemy po prostu sprawdzić wszystkie możliwości ich wylosowań, których jest $2^{\log n}=n$. Czyli faktycznie otrzymaliśmy wielomianowy algorytm deterministyczny: przegląda on wszystkie możliwości na $X_1,\ldots,X_{\log n}$, dla każdej symuluje działanie losowego algorytmu, a na koniec wybiera najlepsze rozwiązanie.

Wojciech CZERWIŃSKI