MMD Wykład 1.

Bogdan Chlebus

Teoria liczb I. Będziemy rozważali własności zbioru liczb całkowitych $\mathbb{Z}$. Niech zmienne oznaczają liczby z $\mathbb{Z}$, chyba że jest powiedziane inaczej. Liczby całkowite nie zawsze możemy dzielić przez siebie, ale zawsze możemy *dzielić z resztą*: Niech $b > 0$, wtedy dla każdej całkowitej a istnieją jednoznacznie wyznaczone: *dzielnik* q i *reszta* r, takie że spełnione są jednocześnie:

$$a = b \cdot q + r \qquad \text{i} \qquad 0 \leq r < b \ .$$

Oto uzasadnienie: Rozważmy zbiór liczb postaci $x_t = a - b \cdot t$, dla $t \in \mathbb{Z}$. Istnieje wśród nich liczba nieujemna, zatem istnieje q takie, że x_q najmniejszy element spośród $x_t \geq 0$. Określmy r jako $a - b \cdot q$. Wtedy $r \geq 0$, a gdyby $r \geq b$ to $0 \leq a - b \cdot (q+1) < a - b \cdot q$, co jest sprzeczne z wyborem q.

Dla $b \neq 0$, jeżeli $a = b \cdot c$, to a jest *wielokrotnością* b; a jeżeli także $b > 0$ to mówimy, że b jest *dzielnikiem* a, co oznaczamy przez $b \mid a$, a zaprzeczenie przez $b \nmid a$. Każda liczba $a > 1$ ma co najmniej dwa dzielniki: 1 i a. Jeżeli są to *jedyne* dzielniki a to jest ona *liczbą pierwszą*, w przeciwnym przypadku jest *złożona*. Oto pierwsze dziesięć liczb pierwszych: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Liczba 1 *nie jest* pierwsza!

Niech $a \cdot b \neq 0$. Jeżeli s jest wspólnym dzielnikiem a i b oraz ma własność, że jeżeli $d \mid a$ oraz $d \mid b$ to $d \mid s$, to takie s oznaczamy NWD(a,b) lub krócej (a,b). Pokażemy, że (a,b) zawsze istnieje. Niepusty zbiór $X \subseteq \mathbb{Z}$ nazwiemy *ideałem*, gdy jest zamknięty na operacje dodawania i odejmowania, to znaczy: jeżeli $x_1, x_2 \in X$ to także $x_1 + x_2, x_1 - x_2 \in X$. Stąd wynika, że jeżeli $x \in X$ to $a \cdot x \in X$, dla dowolnej liczby $a \in \mathbb{Z}$. Zbiór wielokrotności liczby x nazywamy *ideałem generowanym przez* x, a x jego *generatorem*. Jeżeli $X = \{0\}$ to X generowany przez 0, a dla innych ideałów X niech g najmniejsza liczba dodatnia w X. Pokażemy, że X jest generowany przez g. Rzeczywiście, jeżeli nie byłaby to prawda, to niech y najmniejszy dodatni element w zbiorze X, który nie jest wielokrotnością g. Podzielmy y z resztą przez g: dostajemy $y = b \cdot g + r$, gdzie $0 < r < g$. Jest to sprzeczność, bowiem $r \in X$. Wróćmy do istnienia (a,b). Zbiór liczb postaci $a \cdot x + b \cdot y$ jest ideałem. Niech s będzie jego generatorem, w szczególności zachodzi $s = a \cdot x + b \cdot y$, dla pewnych x, y. Mamy $s \mid a$ oraz $s \mid b$ ponieważ a i b są w ideale generowanym przez s. Z drugiej strony, jeżeli $d \mid a$ oraz $d \mid b$ to $d \mid (a \cdot x + b \cdot y)$. To pokazuje istnienie (a,b). Jednoznaczność wynika z faktu, że jeżeli $x \mid y$ oraz $y \mid x$ to $x = y$, dla $x > 0$ oraz $y > 0$. Nazwa NWD bierze się stąd, że (a,b) jest największym wspólnym dzielnikiem a i b.

Liczba (a,b) jest jednoznacznie wyznaczona przez następującą definicję rekurencyjną, gdzie co najmniej jedna z liczb a i b jest różna od zera:

$$\begin{aligned} (0,a) &= a && \text{dla } a > 0 \\ (b,a) &= (a \bmod b, b) && \text{dla } b > 0 \end{aligned} \tag{1}$$

Obliczanie NWD przez rozwijanie tej rekurencji nazywa się *algorytmem Euklidesa*. Na przykład: $(18,12) = (12,18) = (6,12) = (0,6) = 6$. Pokażemy poprawność tej konstrukcji. Prawdziwość równości (1) wynika stąd, że zbiór wspólnych dzielników pary liczb a i

b jest taki sam jak dla pary $a \bmod b$ i b, bowiem $a \bmod b = a - b \cdot \lfloor a/b \rfloor$. Odwołujemy się do już określonych wartości, ponieważ $b > a \bmod b$. To pokazuje poprawność algorytmu.

Algorytm Euklidesa daje więcej: pozwala znaleźć liczby całkowite a_1 i b_1 takie, że

$$a_1 \cdot a + b_1 \cdot b = (a, b) \ .$$

Pokazujemy to przez indukcję. Jeżeli $b = 0$ to $b_1 = 0$ i $a_1 = 1$. W przeciwnym przypadku niech $c = a \bmod b$. Z założenia indukcyjnego znamy b' i c' takie, że $b'b + c'c = (b, c)$. Ale zachodzi $c = a - \lfloor a/b \rfloor \cdot b$ oraz $(b, c) = (a, b)$. Stąd:

$$b' \cdot b + c' \cdot \left(a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b\right) = c' \cdot a + \left(b' - c' \cdot \left\lfloor \frac{a}{b} \right\rfloor\right) \cdot b = (a, b) \ ,$$

co kończy dowód.

Jeżeli $(a, b) = 1$ to a i b są *względnie pierwsze*, co oznaczamy także przez $a \perp b$. Ma miejsce *lemat Euklidesa:* jeżeli $a \mid b \cdot c$ oraz $a \perp b$, to zachodzi $a \mid c$. Mianowicie, mnożymy równanie $1 = a_1 \cdot a + b_1 \cdot b$ stronami przez c i dostajemy $c = a_1 \cdot a \cdot c + b_1 \cdot b \cdot c$. Ponieważ prawa strona jest podzielna przez a, zatem także lewa.

Każda liczba całkowita $a > 0$ jest przedstawialna w postaci iloczynu

$$a = \prod_{i=1}^{m} b_i \ , \tag{2}$$

gdzie liczby b_i sa pierwsze, mogą się powtarzać, i gdzie przyjmujemy, że pusty iloczyn ma wartość 1. Istnienie takiego rozkładu wynika przez indukcję z definicji liczby złożonej. *Podstawowe twierdzenie arytmetyki* mówi, że rozkład (2) jest wyznaczony jednoznacznie z dokładnością do kolejności czynników. Oto dowód, przez indukcję po a. Dla $a = 1$ może to być tylko pusty iloczyn. Niech $a > 1$. Rozważmy dwa takie rozkłady na czynniki pierwsze:

$$a = b_1 \cdot \ldots \cdot b_m = c_1 \cdot \ldots \cdot c_k \ ,$$

gdzie $b_1 \leq \ldots \leq b_m$, oraz $c_1 \leq \ldots \leq c_k$. Pokażemy najpierw, że $b_1 = c_1$. Jeżeli $b_1 < c_1$ to istnieją f i g takie, że $f \cdot b_1 + g \cdot c_1 = 1$, bowiem liczby pierwsze są względnie pierwsze. Stąd

$$f \cdot b_1 \cdot c_2 \ldots c_k + g \cdot c_1 \cdot c_2 \ldots c_k = c_2 \ldots c_k \ .$$

Liczba b_1 dzieli lewą stronę a zatem i prawą. Z lematu Euklidesa zachodzi $b_1 \mid c_i$, dla pewnego $2 \leq i \leq k$, a zatem $b_1 = c_i \geq c_1 > b_1$ – sprzeczność. Przypadek $b_1 > c_1$ jest symetryczny. Zatem $b_1 = c_1$. Liczba a/b_1 ma jednoznaczny rozkład z założenia indukcyjnego, co kończy dowód.

Podstawowe twierdzenie arytmetyki pozwala lepiej zrozumieć podzielność. Niech

$$a = p_{i_1}^{\alpha_1} \cdot p_{i_2}^{\alpha_2} \cdot \ldots \cdot p_{i_m}^{\alpha_m} \ ,$$

gdzie $p_{i_1} < p_{i_2} < \ldots < p_{i_m}$ to liczby pierwsze. Pokazaliśmy, że taki rozkład jest jednoznaczny. Warunek $b \mid a$ jest równoważny następującej postaci b:

$$b = p_{i_1}^{\beta_1} \cdot p_{i_2}^{\beta_2} \cdot \ldots \cdot p_{i_m}^{\beta_m} \ ,$$

gdzie $0 \leq \beta_i \leq \alpha_i$. Stąd wynika, że jeżeli $b \mid a$ oraz $c \mid a$, gdzie $b \perp c$, to także $(b \cdot c) \mid a$. Podobnie do NWD określamy NWW(a, b), czyli *najmniejszą wspólną wielokrotność*: jest to najmniejsza liczba c taka, że jeżeli $a \mid d$ oraz $b \mid d$ to $c \mid d$. Jej istnienie wynika od razu z podstawowego twierdzenia arytmetyki. Funkcje NWD i NWW można naturalnie rozszerzyć na przypadek dowolnej liczby argumentów.

Jeżeli $a - b$ jest wielokrotnością $n > 0$ to mówimy, że a i b *przystają do siebie modulo* n, i zapisujemy jako *kongruencję:* $a \equiv b \pmod{n}$, gdzie liczbę n nazywamy *modułem*. Jeżeli moduł jest ustalony, to przystawanie jest relacją równoważności, oraz kongruencje możemy dodawać, odejmować i mnożyć stronami. Na przykład: jeżeli $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$ to $ac \equiv bd \pmod{n}$. Wynika to z równości $ac - bd = (a - b)c + (c - d)b$. Czasem można obie strony kongruencji skrócić przez dzielenie. Mianowicie, jeżeli zachodzi przystawanie

$$ad \equiv bd \pmod{n} \tag{3}$$

oraz $d \perp n$ to zachodzi także $a \equiv b \pmod{n}$. Wynika to z tego, że liczby względnie pierwsze z n mają odwrotności przy mnożeniu modulo n. Mianowicie, wiemy ze istnieja d' i n' takie, ze $d'd + n'n = 1$. Stad $d'd \equiv 1 \pmod{n}$, czyli mnożenie przez d' (modulo n) to jak dzielenie przez d. Wystarczy pomnożyć kongruencję (3) przez $d' \equiv d' \pmod{n}$. Podobna sytuacja zachodzi dla kongruencji postaci $ad \equiv bd \pmod{nd}$, która jest równoważna kongruencji $a \equiv b \pmod{n}$. To wynika z rozdzielności mnożenia względem funkcji mod, bowiem równoważne są: $a \equiv b \pmod{n}$ w.t.w. $a \bmod n = b \bmod n$ w.t.w. $ad \bmod nd = bd \bmod nd$ w.t.w. $ad \equiv bd \pmod{nd}$.

Czasem jedną kongruencję można zamienić na układ kilku kongruencji: na przykład kongruencja $a \equiv b \pmod{m \cdot n}$, gdzie $m \perp n$, jest równoważna dwóm kongruencjom: $a \equiv b \pmod{m}$ i $a \equiv b \pmod{n}$, bowiem $n \mid x$ i $m \mid x$ w.t.w. gdy $(m \cdot n) \mid x$. Ogólnie, mając przedstawienie modułu kongruencji jako iloczynu k liczb względnie pierwszych możemy otrzymać równoważną koniunkcję k kongruencji.

To prowadzi do *chińskiego twierdzenia o resztach*: Niech $n = n_1 \cdot \ldots \cdot n_k$, gdzie $n_1, \ldots, n_k$ parami względnie pierwsze, wtedy dla każdego ciągu $\langle a_1, \ldots, a_k \rangle$ istnieje dokładnie jedna liczba a taka, że $0 \leq a < n$ oraz $a \equiv a_i \pmod{n_i}$ dla $1 \leq i \leq k$. Dla dowodu, przyporządkujmy każdej liczbie b ciąg reszt $\langle b_i \rangle$, dla $1 \leq i \leq k$, określony przez $b_i = b \bmod n_i$. Zachodzą następujące dwa fakty:
(1) Jest co najwyżej n różnych ciągów reszt, co jest jasne.
(2) Jeżeli $0 \leq c_1 < c_2 < n$ to ciągi reszt liczb c_1 i c_2 są różne. Rzeczywiscie: zachodzenie każdej z kongruencji $c_1 \equiv c_2 \pmod{n_i}$ dla $1 \leq i \leq k$ implikuje $c_1 \equiv c_2 \pmod{n}$, czyli $n \mid (c_2 - c_1)$, co jest niemożliwe, jako że $0 < c_2 - c_1 < n$.
Razem (1) i (2) dają wzajemnie jednoznaczną odpowiedniość pomiędzy ciągami reszt i liczbami z przedziału $[0..n - 1]$.

Podobnie dostajemy małe twierdzenie Fermata: Niech $a \perp b$. Rozważmy ciąg liczb:

$$0 \bmod b, \quad a \bmod b, \quad 2a \bmod b, \quad \ldots, \quad (b-1) \cdot a \bmod b\ . \tag{4}$$

Są one parami różne bowiem kongruencja $ia \equiv ja \pmod{b}$ jest równoważna kongruencji $i \equiv j \pmod{b}$. Widzimy, że ciag (4) to permutacja liczb $0, 1, \ldots, b - 1$. Opuśćmy w nim

0, a pozostałe pomnóżmy przez siebie na dwa sposoby:

$$a \cdot 2a \cdot \ldots \cdot (b-1)a \equiv (a \bmod b)(2a \bmod b) \ldots ((b-1)a \bmod b) \equiv (b-1)! \pmod b \ .$$

Stąd $(b-1)! \cdot a^{b-1} \equiv (b-1)! (\bmod b)$. Jeżeli b jest liczbą pierwszą, to każda liczba $0 < x < b$ jest z nią względnie pierwsza, i możemy kongruencję skrócić przez $(b-1)!$. To jest właśnie małe twierdzenie Fermata: o ile b jest liczbą pierwszą i $a \perp b$ to zachodzi:

$$a^{b-1} \equiv 1 \pmod b \ . \tag{5}$$

Euler pokazał jak uogólnić (5) opuszczając założenie, że b jest pierwsza. *Funkcja Eulera* $\phi(b)$, dla $b > 0$, jest określona jako liczność zbioru $A_b = \{k : 1 \leq k \leq b \quad \text{oraz} \quad k \perp b\}$. *Twierdzenie Eulera* mówi, że jeżeli $a \perp b$, to zachodzi kongruencja:

$$a^{\phi(b)} \equiv 1 \pmod b \ .$$

Dowód jest podobny jak dla małego twierdzenia Fermata: Niech $a_1, \ldots, a_{\phi(b)}$ to elementy zbioru A_b. Wystarczy pokazać że ciąg

$$aa_1 \bmod b, \quad aa_2 \bmod b, \quad \ldots, \quad aa_{\phi(b)} \bmod b$$

to permutacja A_b. Rzeczywiście, po pierwsze

$$aa_i \bmod b = aa_i - b \left\lfloor \frac{aa_i}{b} \right\rfloor \in A_b \ ,$$

gdyż wspólny dzielnik tej liczby i b byłby dzielnikiem $a \cdot a_i$. Po drugie, gdyby zachodziło $aa_i \equiv aa_j (\bmod b)$, dla $i > j$, to $b \mid a(a_i - a_j)$, co nie jest możliwe, gdyż $(a, b) = 1$ oraz $0 < a_i - a_j < b$. To kończy dowód.

Jeżeli $x \perp m$ to najmniejsze k takie, że $x^k \equiv 1 (\bmod m)$ nazywamy *rzędem x modulo m*, i oznaczamy $\mathrm{ord}_m(k)$. Zauważmy, że dla $x \perp m$, zachodzi $x^k \equiv 1 (\bmod m)$ w.t.w. gdy $\mathrm{ord}_m(x) \mid k$. Jeżeli rząd x modulo m jest równy $\phi(m)$ to x nazywamy *pierwotnym pierwiastkiem modulo m*. Gdy x ma taką własność, to jego kolejne potęgi $1, x, x^2, x^3, \ldots, x^{\phi(m)-1}$ przebiegają wszystkie elementy zbioru A_m. Jeżeli $y \in A_m$ oraz $y \equiv x^i (\bmod m)$ to liczbę i nazywamy *indeksem y modulo m* i oznaczamy $\mathrm{ind}_m(y)$. Funkcje ind są dyskretnymi odpowiednikami funkcji logarytmicznych.

Funkcja określona na liczbach całkowitych dodatnich i o wartościach liczbowych nazywa się *funkcją arytmetyczną*. Funkcja Eulera ϕ jest przykładem takiej ciekawej funkcji. Pokażemy teraz jej kilka własności. Oczywiście $\phi(p) = p - 1$ gdy p jest liczbą pierwszą. Jeżeli $b = p^k$, dla p pierwszej, to w przedziale $[1..b]$ tylko wielokrotności p nie są względnie pierwsze z b, a tych jest dokładnie p^{k-1}, są nimi: $p, 2p, \ldots, p^k - p, p^k$. Czyli $\phi(p^k) = p^k - p^{k-1}$. Rozważymy teraz ogólniejszy przypadek: niech $a = b \cdot c$ gdzie $(b, c) = 1$. Zachodzi $(x, a) = 1$ w.t.w. gdy $(x, b) = 1$ i $(x, c) = 1$, a z chińskiego twierdzenia o resztach wynika, że liczba $0 \leq x < a$ jest jednoznacznie wyznaczona przez $x \bmod b$ i $x \bmod c$. Stąd $\phi(a) = \phi(b) \cdot \phi(c)$. Funkcja arytmetyczna f jest *multiplikatywna* gdy $f(a) = f(b) \cdot f(c)$, dla $a = b \cdot c$ i $b \perp c$. Pokazaliśmy, że funkcja Eulera ϕ jest multiplikatywna. Jeżeli f jest funkcją multiplikatywną to $f(a) = \prod_{i=1}^{k} f(p_i^{\alpha_i})$, gdzie $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ jest rozkładem a

na czynniki pierwsze. Biorąc $f(p^\alpha) = p^\alpha - p^{\alpha-1}$, dostajemy *wzór iloczynowy dla funkcji Eulera:*

$$\phi(a) = a \prod_{p|a} \left(1 - \frac{1}{p}\right) \ ,$$

gdzie p przebiega liczby pierwsze.

Już Euklides pokazał, że istnieje nieskończenie wiele liczb pierwszych. W przeciwnym przypadku bowiem, gdyby $a_1, \ldots, a_n$ były wszystkimi liczbami pierwszymi to rozważmy najmniejszy dzielnik liczby $x = a_1 \cdot a_2 \cdot \ldots \cdot a_n + 1$, spośród tych większych od 1. Jest on liczbą pierwszą, z przechodniości relacji bycia dzielnikiem. Z drugiej strony, jest on różny od każdej z liczb a_i, gdyż żadna z nich nie dzieli liczby x.

Oto inny dowód, podany przez Eulera. Wychodzimy od następującej tożsamości, gdzie p przebiega wszystkie liczby pierwsze:

$$\prod_p \frac{1}{1 - p^{-1}} = \prod_p \Big(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\Big) = \sum_{n \geq 1} \frac{1}{n} \ . \tag{6}$$

Druga z równości (6) wynika z podstawowego twierdzenia arytmetyki. Gdyby było skończenie wiele liczb pierwszych, to lewa strona (6) byłaby skończona, a wiemy, że prawa jest nieograniczona, jako że $H_n \sim \ln n$.

Niech funkcja $\pi(n)$ oznacza liczność zbioru liczb pierwszych nie większych niż n. Pokażemy oszacowanie funkcji $\pi(n)$. Zaczniemy od dowodu nierówności $\prod_{p \leq n} p \leq 4^n$, gdzie p przebiega liczby pierwsze, który przeprowadzimy przez indukcję po n. Dla $n \leq 4$ sprawdzamy bezpośrednio. Możemy założyć, że n nieparzyste. W iloczynie

$$\prod_{p \leq n} p = \prod_{p \leq \frac{n+1}{2}} p \cdot \prod_{\frac{n+1}{2} < p \leq n} p$$

pierwszy czynnik jest nie większy niż $4^{\frac{n+1}{2}}$, z założenia indukcyjnego, a drugi jest nie większy niż $\binom{n}{(n+1)/2}$, ponieważ w ułamku $n^{\underline{i}}/i!$, dla $i = \frac{n+1}{2}$, mianownik nie skróci żadnej liczby pierwszej $p > \frac{n+1}{2}$ w liczniku. Ponieważ $\binom{n}{(n+1)/2} \leq 2^{n-1}$, razem mamy

$$\prod_{p \leq n} p \leq 4^{\frac{n+1}{2}} \cdot 2^{n-1} \leq 4^n \ . \tag{7}$$

Niech $p_1 < p_2 < p_3 < \ldots$ kolejne liczby pierwsze. Niech k największa liczba taka, że $p_k \leq n$, czyli $\pi(n) = k$. Mamy

$$4^n \geq \prod_{i=1}^{k} p_i \geq k! > \left(\frac{k}{e}\right)^k \ ,$$

zatem $n \cdot \ln 4 > k \cdot (\ln k - 1)$. Stąd wynika, że $\pi(n) = \mathcal{O}(n/\log n)$.

Oto dowód mocniejszego *twierdzenia Czebyszewa*: $\pi(n) = \Theta(n/\log n)$. Określmy funkcje $\vartheta(n) = \sum_{p \leq n} \ln p$ oraz $\psi(n) = \sum_{p^k \leq n} \ln p$. Nierówność (7) oznacza $\vartheta(n) = \mathcal{O}(n)$. Mamy:

$$0 < \psi(n) - \vartheta(n) \leq \sum_{2 \leq i \leq \log_2 n} \sum_{p \leq n^{1/i}} \ln p \leq \ln n \sum_{2 \leq i \leq \log_2 n} \sqrt{n} = o(n) \ . \tag{8}$$

Rozważmy całkę $S = \int_0^1 x^n(1-x)^n\,dx$. Obliczamy ją jako sumę całek jednomianów otrzymanych z wzoru na dwumian. S jest wtedy sumą ułamków, w których mianownikach nie występuje czynnik większy niż $2n+1$. Zatem $S \cdot \mathrm{NWW}(1,2,3,\ldots,2n+1) \geq 1$ bo jest to liczba naturalna. Mamy także $0 \leq x(1-x) \leq 1/4$, dla $0 \leq x \leq 1$, a zatem $S \leq 4^{-n}$. Razem dostajemy $\mathrm{NWW}(1,2,\ldots,2n+1) \geq S^{-1} \geq 4^n$. Stąd wynika $\psi(n) = \Omega(n)$, co pociąga za sobą $\vartheta(n) = \Theta(n)$ na mocy (8). Na koniec sumujemy przez części:

$$\begin{aligned}
\pi(n) &= \sum_{p\leq n} 1 = \sum_{2\leq i\leq n} \frac{\vartheta(i)-\vartheta(i-1)}{\ln i} \\
&= \sum_{1\leq i<n} \frac{\Delta\vartheta(i)}{\ln(i+1)} \\
&= \frac{\vartheta(i)}{\ln(i+1)}\bigg|_1^n - \sum_{1\leq i<n} \vartheta(i+1)\cdot\Delta\ln^{-1}(i+1) \\
&= \Theta(n/\log n)\ ,
\end{aligned}$$

ponieważ $\vartheta(i) = \Theta(i)$ oraz, jak pokazaliśmy w wykładzie MD 9, zachodzi

$$\sum_{2\leq i\leq n} i\cdot\Delta(\ln^{-1} i) = \mathcal{O}(n/\log^2 n)\ .$$

Zadania

1. Pokaż, że iloczyn k kolejnych liczb naturalnych jest zawsze podzielny przez $k!$.

2. Pokaż, że jeżeli liczba $2^n - 1$ jest pierwsza to n też jest pierwsza.

3. Pokaż, że jeżeli liczba postaci $2^n + 1$ jest pierwsza to n jest potegą 2. Liczby postaci $2^{2^n} + 1 = f_n$ to *liczby Fermata*. Pokaż równość $\prod_{i=0}^n f_i = f_{n+1} - 2$. Wywnioskuj stąd, że każde dwie różne liczby Fermata są względnie pierwsze.

4. Pokaż, że $\left(n^i - 1, n^j - 1\right) = n^{(i,j)} - 1$, dla $n > 1$ i całkowitych i, j.

5. Pokaż, że jeżeli równość (1) zastąpimy przez $(a,b) = (b,a)$ oraz $(b,a) = (a-b,b)$ dla $b < a$, to otrzymamy nadal poprawny algorytm Euklidesa, chociaż wolniejszy.

6. Pokaż kolejno następujące własności liczb Fibonacci'ego:
(i) $(F_a, F_{a+1}) = 1$; (ii) $(F_a, F_b) = (F_{b-a}, F_a)$, dla $b > a$; (iii) $(F_a, F_b) = F_{(a,b)}$.
Wskazówka: skorzystaj z równości $F_{n+k} = F_k \cdot F_{n+1} + F_{k-1} \cdot F_n$ dla punktu (ii).

7. Pokaż, że algorytm Euklidesa wykona $\mathcal{O}(\log(\min\{a,b\}))$ operacji dzielenia z resztą aby znaleźć (a,b). Pokaż, że liczba dzieleń jaką wykona algorytm Euklidesa obliczający $(F_n, F_{n+1}) = 1$, jest równa $n = \Omega(\log F_n)$.

8. Pokaż, że mnożenie jest rozdzielne względem funkcji mod:

$$x(y \bmod z) = xy \bmod xz\ .$$

9. Opisz wartości funkcji $\mathrm{NWD}(a,b)$ i $\mathrm{NWW}(a,b)$ w terminach rozkładu argumentów a i b na czynniki pierwsze.

10. Pokaż, że $\mathrm{NWD}(a,b) \cdot \mathrm{NWW}(a,b) = a \cdot b$.

11. Niech $n > 0$ oraz $d = (a,n)$. Pokaż, że równanie $ax \equiv b \pmod{n}$ ma d rozwiązań gdy $d \mid b$, oraz nie ma rozwiązań gdy $d \nmid b$.

12. Pokaz *twierdzenie Wilsona:* dla $n > 1$ ma miejsce $(n-1)! \equiv -1 \pmod{n}$ w.t.w. gdy n jest liczbą pierwszą.
Wskazówka: jeżeli n pierwsza, to każda liczba $1 \leq i \leq n-1$ ma odwrotność modulo n.

13. Wyprowadź wzór iloczynowy na funkcję Eulera ϕ z formuły sita.
Wskazówka: wykonaj mnożenie w tym wzorze.

14. Oto konstruktywna wersja chińskiego twierdzenie o resztach: Dana liczba $n = \prod_{i=1}^{k} n_i$, gdzie $n_i \perp n_j$ dla $i \neq j$. Pokaż, że jeżeli $\frac{n}{n_i} \cdot b_i \equiv 1 \pmod{n_i}$, to liczba

$$x = \Big(\sum_{j=1}^{k} \frac{n}{n_j} \cdot b_j \cdot a_j\Big) \bmod n$$

spełnia $0 \leq x < n$, oraz $x \equiv a_i \pmod{n_i}$, dla $1 \leq i \leq k$.

15. Pokaż, że jeżeli p, q pierwsze, i $p \mid 2^q - 1$ to $p > q$.
Wskazówka: Pokaż, że $\mathrm{ord}_p(2) = q$.

16. Sprawdź, że $m = 8$ jest najmniejszą liczbą, dla której nie ma pierwiastka pierwotnego modulo m.

17. Pokaż, że istnieje nieskończenie wiele liczb pierwszych postaci $4 \cdot n + 1$ i postaci $4 \cdot n + 3$.
Wskazówka: dowód Euklidesa nieskończoności zbioru liczb pierwszych.

18. Niech $d(k)$ oznacza liczbę dzielników k. Pokaż

$$\sum_{k=1}^{n} d(k) = n \ln n + \mathcal{O}(n) \ .$$

MMD Wykład 2.

Bogdan Chlebus

Teoria liczb II. Jeżeli f i g są dwiema funkcjami arytmetycznymi to ich *iloczyn Dirichleta* określamy wzorem

$$f * g = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) \ .$$

Ta operacja jest przemienna i łączna. Przemienność wynika stąd, że jeżeli d przebiega dzielniki n to n/d też to robi. Dla dowodu łączności, zauważmy, że zachodzi równość

$$(f * (g * h))(n) = \sum_{x \cdot y = n} f(x) \cdot (g * h)(y) = \sum_{x \cdot y = n} f(x) \sum_{t \cdot z = y} g(t) \cdot h(z) = \sum_{x \cdot t \cdot z = n} f(x) g(t) h(z).$$

Ostatnia suma nie zależy od rozmieszczenia nawiasów, taką samą dostaniemy dla wyrażenia $((f * g) * h)$.

Identycznością mnożenia $*$ jest funkcja $[n = 1]$, w tym sensie, że zachodzi:

$$(f * [n = 1])(n) = \sum_{d|n} f(d)[n/d = 1] = f(n) \ .$$

Odwrotnością f, oznaczaną f^{-1}, jest taka funkcja arytmetyczna, ze $f * f^{-1} = [n = 1]$. Na przykład, niech j oznacza funkcję dającą wartość 1 dla każdego argumentu, pokażemy, że jej odwrotnością jest funkcja Möbiusa μ, gdzie $\mu(1) = 1$, $\mu(n) = (-1)^k$ gdy n jest iloczynem k różnych liczb pierwszych, i $\mu(n) = 0$ w pozostałych przypadkach. Pamiętamy, że funkcja Möbiusa μ ma własność $\sum_{d|n} \mu(d) = [n = 1]$. To oznacza, że $\mu * j = [n = 1]$, czyli $\mu^{-1} = j$ i $j^{-1} = \mu$. Jako zastosowanie tych rozważań pokażemy *wzór Möbiusa na odwracanie:*

$$f(n) = \sum_{d|n} g(d) \qquad \text{w.t.w.} \qquad g(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right) \ .$$

Zauważmy, że lewe równanie oznacza $f = g * j$. Mnożąc stronami przez μ dostajemy

$$f * \mu = (g * j) * \mu = g * (j * \mu) = g * [n = 1] = g \ .$$

Podobnie, prawe rownanie oznacza $g = f * \mu$. Mnożąc obie strony przez j dostajemy

$$g * j = (f * \mu) * j = f * (\mu * j) = f * [n = 1] = f \ .$$

Przykład: Po wykonaniu mnożenia we wzorze iloczynowym na funkcję Eulera ϕ mamy:

$$\phi(n) = n \cdot \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \frac{n}{d} \cdot \mu(d) = \sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right) \ . \tag{1}$$

Kładąc $g(k) = \phi(k)$, $f(k) = k$ i odwracając dostajemy $n = \sum_{d|n} \phi(d)$. $\Diamond$

Przykład: Niech będzie ustalony alfabet składający się z k liter. *Słowem długości* n nazwiemy n-permutację liter z powtórzeniami. Słowa są *równoważne* gdy jedno można otrzymać z drugiego przez cykliczne przesunięcie. Znajdziemy liczbę W_n klas abstrakcji tej relacji równoważności. Powiemy, że liczba d jest *okresem* słowa w gdy jest najmniejszą spośród liczb $x > 0$ takich, że cykliczne przesunięcie w o x pozycji daje znów w. Słowa, których okres jest równy ich długości nazwiemy *nieokresowymi*. Jeżeli d jest okresem słowa długości n to $d \mid n$. Liczność zbioru słów długości n o okresie d, gdzie $d \mid n$, jest równa liczności zbioru słow nieokresowych długości d, oznaczmy tę liczbę przez N_d. Cykliczne przesunięcie słowa nieokresowego też jest nieokresowe, zatem $W_n = \sum_{d|n} \frac{N_d}{d}$. Mamy także $k^n = \sum_{d|n} N_d$, stąd ze wzoru Möbiusa na odwracanie $N_d = \sum_{d|n} k^d \cdot \mu\left(\frac{n}{d}\right)$. Razem:

$$W_n = \sum_{d|n} \frac{1}{d} \cdot N_d = \sum_{d|n} \frac{1}{d} \sum_{c|d} k^c \cdot \mu\left(\frac{d}{c}\right) = \sum_{c|n} \sum_{i|\frac{n}{c}} \frac{1}{i \cdot c} \cdot k^c \cdot \mu(i)$$
$$= \sum_{c|n} \frac{k^c}{c} \sum_{i|\frac{n}{c}} \frac{\mu(i)}{i} = \sum_{c|n} \frac{k^c}{c} \cdot \phi\left(\frac{n}{c}\right) \cdot \frac{c}{n} = \frac{1}{n} \sum_{c|n} \phi(c) \cdot k^{n/c} \ ,$$

gdzie skorzystaliśmy z (1). $\Diamond$

Niech F, G funkcje. Pokażemy następujące wynikanie dla rzeczywistego $x > 0$:

$$\text{jeżeli } G(x) = \sum_{k=1}^{\lfloor x \rfloor} F\left(\frac{x}{k}\right) \text{ to zachodzi } F(x) = \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot G\left(\frac{x}{k}\right) \ , \tag{2}$$

które jest inną wersją wzoru Möbiusa na odwracanie. Obliczamy prawą sumę w (2):

$$\sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot G\left(\frac{x}{k}\right) = \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot \sum_{i=1}^{\lfloor x/k \rfloor} F\left(\frac{x}{i \cdot k}\right) = \sum_{n=1}^{\lfloor x \rfloor} F\left(\frac{x}{n}\right) \cdot \sum_{k|n} \mu(k)$$
$$= \sum_{n=1}^{\lfloor x \rfloor} F\left(\frac{x}{n}\right) \cdot [n = 1] = F(x) \ .$$

Przykład: Wyznaczymy rząd wielkości funkcji $B(x)$, dla rzeczywistego $x > 1$, równej liczności zbioru liczb bezkwadratowych nie większych niż x, gdzie liczba naturalna jest *bezkwadratowa* gdy nie jest podzielna przez kwadrat liczby pierwszej. Zauważmy, że w przedziale $[1, x]$ jest $B(x/k^2)$ liczb naturalnych takich, że k jest największą liczbą o własności $k^2 \mid \lfloor x \rfloor$. Stąd $\lfloor x \rfloor = \sum_{k=1}^{\lfloor \sqrt{x} \rfloor} B\left(\frac{x}{k^2}\right)$. Zastępując x przez x^2 dostajemy

$$\lfloor x^2 \rfloor = \sum_{k=1}^{\lfloor x \rfloor} B\left(\frac{x^2}{k^2}\right) \ .$$

Stosując odwracanie (2) mamy:

$$B(x^2) = \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot \left\lfloor \frac{x^2}{k^2} \right\rfloor \ .$$

Zastępujemy $\lfloor x^2/k^2 \rfloor$ przez $x^2/k^2 + \mathcal{O}(1)$, co upraszcza wzór do postaci:

$$B(x^2) = x^2 \sum_{k=1}^{\lfloor x \rfloor} \frac{\mu(k)}{k^2} + \mathcal{O}(x) \ .$$

Powtórnie wracamy z x^2 do x:

$$B(x) = x \cdot \sum_{k=1}^{\lfloor \sqrt{x} \rfloor} \frac{\mu(k)}{k^2} + \mathcal{O}(\sqrt{x}) = x \cdot \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} + \mathcal{O}\Big(x \cdot \sum_{k>\sqrt{x}} \frac{1}{k^2}\Big) + \mathcal{O}(\sqrt{x}) \ .$$

Korzystając z $\sum_{k>y} k^{-a} = \mathcal{O}(y^{1-a})$, dla $a > 1$, mamy $B(x) = A \cdot x + \mathcal{O}(\sqrt{x})$, gdzie $A = \sum_{k\geq 1} \frac{\mu(k)}{k^2}$. Ale zauważmy, że z multiplikatywności funkcji μ wynika:

$$A = \sum_{k\geq 1} \frac{\mu(k)}{k^2} = \prod_p \big(1 + \mu(p) \cdot p^{-2} + \mu(p^2) \cdot p^{-4} + \ldots\big) = \prod_p \big(1 - p^{-2}\big) \ .$$

Jednocześnie $\frac{1}{1-p^{-2}} = 1 + p^{-2} + p^{-4} + \ldots$, a stąd

$$A^{-1} = \prod_p \frac{1}{1-p^{-2}} = \sum_{n\geq 1} \frac{1}{n^2} = \zeta(2) \ .$$

Wiadomo z analizy, że $\zeta(2) = \frac{\pi^2}{6}$, a zatem ostatecznie $B(x) = \frac{6}{\pi^2} \cdot x + \mathcal{O}(\sqrt{x})$. $\Diamond$

Algorytmy arytmetyki liczb całkowitych. Liczby przedstawiamy zwykle w układzie pozycyjnym gdy badamy algorytmiczne aspekty arytmetyki. Jeżeli podstawą układu jest liczba $s > 1$, a skończony ciąg liczb $a_0, \ldots, a_n$ ma wlasność $0 \leq a_i < s$, to napis

$$(a_n a_{n-1} \ldots a_0)_s \tag{3}$$

będzie oznaczał liczbę $a = a_0 + a_1 s + \cdots + a_i s^i + \cdots + a_n s^n$. Liczby całkowite z przedziału $[0..s-1]$ nazywamy *cyframi*. Interpretując s jako zmienną widzimy że liczba a to wartość wielomianu o współczynnikach $a_0, \ldots, a_n$ w punkcie s; nic dziwnego ze operacje na liczbach całkowitych w układzie pozycyjnym przypominają operacje na wielomianach. W implementacjach komputerowych stosuje się zwykle układ binarny, to znaczy $s = 2$. Wtedy cyfry a_i mają wartosci 0 lub 1. Ograniczymy sie do tego przypadku; gdy $s = 2$ to s opuszczamy w napisach (3).

Algorytmy wykonujące operacje arytmetyczne opiszemy w terminach operacji bitowych. *Czasem pracy algorytmu* nazwiemy maksymalną liczbę operacji bitowych dla danych odpowiedniego rozmiaru, wyrażoną jako funkcja rozmiaru danych. Liczba n zapisuje się przy pomocy $1 + \lfloor \lg n \rfloor$ cyfr binarnych, przyjmujemy tę właśnie liczbę cyfr binarnych jako rozmiar danych, gdy danymi jest liczba n. Przyjmujemy, że algorytm jest *efektywny* lub *praktyczny* gdy czas pracy jest ograniczony przez wielomian od rozmiaru danych.

Sumą dwóch liczb $a = (a_n \ldots a_0)$ i $b = (b_n \ldots b_0)$ jest $c = (c_{n+1} c_n \ldots c_0)$, gdzie $c_i = a_i + b_i + d_i \bmod 2$, $c_{n+1} = d_{n+1}$, a przeniesienia d_i dane są wzorami: $d_0 = 0$, $d_{i+1} = \big\lfloor \frac{a_i + b_i + d_i}{2} \big\rfloor$.

Liczba operacji bitowych jest $\mathcal{O}(\log a + \log b)$. Nie można wykonać dodawania szybciej, gdyż co najmniej tyle czasu zajmie przeczytanie danych.

Iloczyn liczb a i b można obliczyć jako sumę $\sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j 2^{i+j}$. Mnożenie przez potęgę 2 jest łatwe: to "przesunięcie", czyli dopisanie odpowiedniej liczby zer. Przyjmujemy, że jest to także operacja bitowa o stałym koszcie. Jest n^2 par cyfr liczb a i b, stąd łączny czas takiego mnożenia jest $\mathcal{O}(n^2) = \mathcal{O}(\log a \cdot \log b)$. Czy można szybciej? Wydaje sie, że nie, gdyż każda para cyfr liczb a i b "musi" być rozważona oddzielnie, ale takie intuicje są zawodne. Dla ilustracji pokażemy algorytm o czasie działania mniejszego rzędu niż $\log a \cdot \log b$. Jest on zbudowany zgodnie z paradygmatem dziel i zwyciężaj.

Dla uproszczenia oznaczeń, niech liczby a i b maja parzystą liczbę bitow, czyli $n = 2i-1$. Dzielimy a i b na połowy:

$$\begin{aligned} a_L = (a_{2i-1} \ldots a_i) \quad ; \quad a_R = (a_{i-1} \ldots a_0)\ ; \\ b_L = (b_{2i-1} \ldots b_i) \quad ; \quad b_R = (b_{i-1} \ldots b_0)\ ; \end{aligned}$$

czyli $a = 2^i \cdot a_L + a_R$, $b = 2^i \cdot b_L + b_R$. Zauważmy, że obliczenie iloczynu według wzoru

$$a \cdot b = (2^i \cdot a_L + a_R) \cdot (2^i \cdot b_L + b_R) = 2^{2i} \cdot a_L \cdot b_L + 2^i \cdot (a_L \cdot b_R + a_R \cdot b_L) + a_R \cdot b_R$$

wymagałoby czterech mnożeń liczb o połowę krótszych, oraz dodawań i przesunieć. To prowadzi do równania rekurencyjnego

$$T'(n) = 4 \cdot T'\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + \mathcal{O}(n) \tag{4}$$

na czas pracy dla mnożenia, mierzony liczbą operacji bitowych, gdzie przesunięcia i dodawania dają składnik $\mathcal{O}(n)$. Rozwiązanie spełnia $T'(n) = \Theta(n^2)$. Pomysł na ulepszenie polega na zastosowaniu wzoru wymagającego tylko trzech mnożeń:

$$a \cdot b = (2^{2i} + 2^i) \cdot a_L \cdot b_L + 2^i \cdot (a_L - a_R) \cdot (b_R - b_L) + (2^i + 1) \cdot a_R \cdot b_R\ .$$

To prowadzi do równania

$$T(n) = 3 \cdot T\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + \mathcal{O}(n) \tag{5}$$

na liczbę operacji bitowych. Szacujemy rozwiązanie równania (5) przez rozwinięcie. Napiszmy równanie (5) w postaci $T(n) = 3 \cdot T\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + c \cdot n$, gdzie $c > 0$ stała. Niech $n = 2^k$, wtedy

$$\begin{aligned} T(2^k) &= 3 \cdot T(2^{k-1}) + c \cdot 2^k = 3(3T(2^{k-2}) + c2^{k-1}) + c \cdot 2^k = 3^2 \cdot T(2^{k-2}) + c(3 \cdot 2^{k-1} + 2^k) \\ &= 3^k \cdot T(1) + c \sum_{j=0}^{k} 3^j \cdot 2^{k-j} = 3^k \cdot T(1) + c \cdot 2^k \cdot \sum_{j=0}^{k} \left(\frac{3}{2}\right)^j = 3^k \cdot T(1) + c \cdot 2^k \cdot \frac{(3/2)^{k+1} - 1}{1/2} \\ &= \Theta(3^k) = \Theta(2^{k \cdot \log_2 3}) = \Theta((2^k)^{\log_2 3}) = \Theta(n^{\log_2 3})\ . \end{aligned}$$

Ponieważ $(2n)^{\log_2 3} = \Theta(n^{\log_2 3})$, mamy, że $T(n) = \Theta(n^{\log_2 3})$ dla $n \to \infty$. Zatem dostaliśmy algorytm o czasie działania rzędu $n^{\log_2 3} = o(n^2)$.

Rozważymy teraz podnoszenie do potęgi. Korzystamy z wzoru $a^b = \prod_{i=0}^{n} a^{2^i \cdot b_i}$. Zauważmy także, że $x^{2^{k+1}} = \left(x^{2^k}\right)^2$. Liczby postaci a^{2^i} otrzymujemy przez kolejne podnoszenie do kwadratu. Wraz z otrzymaniem kolejnej a^{2^i}, mnożymy ją przez wynik częściowy, o ile $b_i = 1$. Łączna liczba mnożeń wynosi $\mathcal{O}(n) = \mathcal{O}(\log a + \log b)$ i otrzymujemy algorytm efektywny. Rozważone algorytmy dla dodawania, mnożenia i potęgowania przenoszą się na działania modulo ustalona liczba całkowita m, czyli na *arytmetykę modularną*. Dzielenie z resztą przez m wykonujemy analogicznie do algorytmu dzielenia wielomianów z resztą.

Szyfrowanie przy pomocy arytmetyki modularnej. *Szyfr blokowy* dzieli komunikat (ciąg bitów) na bloki o ustalonym rozmiarze, każdy szyfruje oddzielnie. Blok traktujemy jak liczbę w zbiorze $[0..n-1]$. Ogólnie, jeżeli rozważane liczby są ze zbioru $[0..n-1]$ oraz wykonujemy na nich operacje arytmetyczne modulo n, to taką strukturę oznaczamy przez $\mathbb{Z}/(n)$.

Funkcja $f : X \to Y$ jest *w jedną stronę* jeżeli "łatwo" można obliczyć wartość $f(x)$, dla $x \in X$, natomiast dla danego $y \in Y$ jest "trudno" znaleźć $x \in X$ taki, że $f(x) = y$. Słowo 'trudno' oznacza tutaj: praktycznie niemożliwe z dużym prawdopodobienstwem, ze względu na długi czas pracy każdego, nawet randomizowanego, algorytmu. Przykładem kandydata na taką funkcję jest zwykłe mnożenie: łatwo jest mnożyć, natomiast trudno rozłożyć na czynniki. Podobnie podnoszenie do potęgi w $\mathbb{Z}/(p)$, gdzie p pierwsza: funkcja $a^k \bmod p$ od zmiennej k, przy ustalonych a i p, jest łatwa do obliczenia, natomiast funkcja odwrotna, *dyskretny logarytm* (czyli indeks względem pierwiastka pierwotnego), jest trudna.

Przykład: protokól ustalania klucza. Czy A i B mogą ustalić tajny klucz, wymieniając komunikaty otwartym kanałem informacyjnym? Na pozór jest to niemożliwe. Pokażemy jak to zrobić, przy pewnych założeniach kryptograficznych. Niech n odpowiednio duża liczba i $m \in \mathbb{Z}/(n)$. A i B uzgadniają te liczby w sposób otwarty. A wybiera sobie $a \in \mathbb{Z}/(n)$, B wybiera sobie $b \in \mathbb{Z}/(n)$; te liczby mają być tajne. A oblicza $a_1 = m^a \bmod n$, wysyła a_1 do B. Podobnie B, oblicza $b_1 = m^b \bmod n$, wysyła b_1 do A. Następnie A oblicza $c = b_1^a \bmod n = m^{ab} \bmod n$, jednocześnie B oblicza $c = a_1^b \bmod n = m^{ab} \bmod n$. Liczba c to ustalony tajny klucz. Podsłuchujący poznał liczby: n, m, $m^a \bmod n$, $m^b \bmod n$. Nie wiadomo jak na ich podstawie szybko obliczyć $c = m^{ab} \bmod n$, ale problem dyskretnego logarytmu nie pomoże, o ile jest trudny. $\Diamond$

Przykład: szyfr z kluczem publicznym. Niech p i q dwie duże różne liczby pierwsze. Określamy $n = p \cdot q$. Wtedy funkcja Eulera ma wartość $\phi(n) = (p-1)(q-1)$. Niech $e \perp \phi(n)$, oraz d odwrotność e modulo $\phi(n)$, czyli zachodzi kongruencja $ed \equiv 1 \pmod{\phi(n)}$. Para $\langle n, e\rangle$ jest *kluczem publicznym*, natomiast trójka $k = \langle p, q, d\rangle$ jest *kluczem prywatnym*. Dla przesłania komunikatu x obliczamy i wysyłamy:

$$E_k(x) = x^e \bmod n \ .$$

Odczytujemy szyfrogram y obliczając

$$D_k(y) = y^d \bmod n \ .$$

Ta metoda nazywa się RSA. Oto dlaczego jest ona poprawna:

$$D_k(E_k(x)) = (x^e \bmod n)^d \bmod n = x^{ed} \bmod n = \left(x^{\phi(n)}\right)^a \cdot x \bmod n \ ,$$

ponieważ $ed = a \cdot \phi(n) + 1$. Jeżeli $x \perp n$, to z twierdzenia Eulera $x^{\phi(n)} \equiv 1 (\bmod n)$, i mamy poprawność: $D_k(E_k(x)) = x$. W przeciwnym przypadku: $p \mid x$ lub $q \mid x$. Rozważmy przypadek gdy $x = b \cdot p$, dla $b \perp q$. Trzeba pokazać $(bp)^{ed} \equiv bp (\bmod pq)$, co jest równoważne $b^{ed} p^{ed-1} \equiv b (\bmod q)$. Skracając obie strony kongruencji przez b dostajemy $(bp)^{a(p-1)(q-1)} \equiv 1 (\bmod q)$, co wynika z małego twierdzenia Fermata.

Jeżeli znamy rozkład $n = p \cdot q$, to znamy od razu $\phi(n) = (p-1)(q-1)$. Liczbę e możemy znaleźć losując liczby z $\mathbb{Z}/(n)$ i sprawdzając algorytmem Euklidesa czy są względnie pierwsze z $\phi(n)$. Jednocześnie z dokonywaniem tego wyboru znajdujemy jej odwrotność d modulo $\phi(n)$. Bezpieczeństwo RSA opiera sie na hipotezie trudności znalezienia d na podstawie tylko liczb n i e. Umiejętność szybkiego rozkładania na czynniki pozwala złamać RSA, ale nie wiadomo czy w drugą stronę też tak jest, czyli czy szybki algorytm do łamania RSA da algorytm szybkiego rozkładu na czynniki. Znane sa inne metody szyfrowania, których bezpieczeństwo jest równoważne temu, że znajdowanie rozkładu na czynniki jest trudne. $\Diamond$

Wiemy jak działa mechanizm RSA, ale nie wiemy jeszcze jak go zbudować. Jak znaleźć dwie duże liczby pierwsze p i q? Przy obecnie znanych algorytmach rozkładu na czynniki i szybkości komputerów, powinne one mieć więcej niż 200 cyfr dziesiętnych. Najprościej brać losowe liczby z odpowiedniego przedziału i sprawdzać czy są pierwsze, bowiem liczb pierwszych jest wystarczająco dużo. Jak sprawdzać czy liczba jest pierwsza to ciekawy problem, ale wykracza on poza tematykę tego wykładu.

Zadania

1. Pokaż, że równości $\sum_{d|n} \mu(d) = [n = 1]$ jednoznacznie określają funkcję Möbiusa μ.

2. Pokaż, że funkcja Möbiusa μ jest multiplikatywna.

3. Pokaż, że jeżeli funkcja arytmetyczna f postaci $f(a) = \sum_{d|a} g(d)$ jest multiplikatywna, to funkcja arytmetyczna g też jest multiplikatywna.

4. Jeżeli funkcja arytmetyczna f spełnia warunek $f(1) \neq 0$ to istnieje odwrotność f w sensie iloczynu Dirichleta.

5. Pokaż implikację odwrotną do (2).

6. Niech f, g funkcje arytmetyczne. Pokaż, że równości $\sum_{d|n} f(d) = g(n)$, dla $n > 0$, są równoważne równościom $\sum_{n \leq x} g(n) = \sum_{n \leq x} f(n) \cdot \lfloor \frac{x}{n} \rfloor$, dla rzeczywistych $x > 0$.

7. Niech $d(n)$ oznacza liczbę dzielników n, a $\sigma(n)$ sumę dzielników n. Znajdź wzory na $d(n)$ i $\sigma(n)$ w zależności od rozkładu n na czynniki pierwsze.

8. Pokaż, że liczba pierwsza p wchodzi w rozkład na czynniki pierwsze $n!$ z wykładnikiem

$$\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

9. Pokaż następującą równość, dla $n \geq 1$:

$$\sum_{1 \leq k \leq n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor = 1 .$$

10. Pokaż szacowanie

$$\sum_{1 \leq k \leq n} \phi(k) = \frac{3}{\pi^2} \cdot n^2 + \mathcal{O}(n \log n) .$$

Wskazówka: skorzystaj z równości (1).

11. Pokaż że każda liczba całkowita $a \geq 0$ ma dokładnie jeden zapis w układzie pozycyjnym o podstawie $s > 1$.

12. Pokaż dla $a, b, n > 0$ zachodzi: $a^b \bmod n = (a \bmod n)^b \bmod n$.

13. Pokaż, że dzielenie z resztą liczb x i y można wykonać za pomocą $\mathcal{O}(\log x \cdot \log y)$ operacji bitowych.

14. Pokaż, że algorytm Euklidesa znajduje (x, y) wykonując $\mathcal{O}(\log x \cdot \log y)$ operacji bitowych.
Wskazówka: Po drodze obliczamy dzielniki, ich iloczyn jest nie większy od x i od y.

15. Pokaż, że rozwiązanie równania (4) spełnia $T'(n) = \Theta(n^2)$.

16. Chcielibyśmy przesyłać komunikaty tak, by odbiorca był pewien ich autentyczności. Niech tajność bedzie tym razem bez znaczenia. Pokaż jak do tego celu użyć RSA.
Wskazówka: składanie transformacji E_k i D_k ze sobą jest przemienne.

17. Zaproponuj jak za pomocą RSA zapewnić tajność i autentyczność jednocześnie.

MMD Wykład 3.

Bogdan Chlebus

Grupy. Niech na zbiorze T będzie określone dwuargumentowe działanie $*$ i wyróżniony element $e \in T$. Trójka $G = \langle T, *, e\rangle$ jest *grupą* gdy

- działanie $*$ jest *łączne*, czyli $(x * y) * z = x * (y * z)$, dla $x, y, z \in T$;
- element e jest *neutralny*, czyli $x * e = e * x = x$, dla $x \in T$;
- istnieje *odwrotność* x^{-1} każdego $x \in T$, która spełnia $x * x^{-1} = x^{-1} * x = e$.

Jeżeli dodatkowo zachodzi

- *przemienność* $*$, czyli $x * y = y * x$ dla $x, y \in T$,

to grupa jest *przemienna* lub *abelowa*. Zamiast $x \in T$ będziemy czasem pisać $x \in G$, a zamiast $x * y$ po prostu xy. Jest jeden element neutralny w grupie: gdyby bowiem e' też neutralny, to $e = ee' = e'$. Dla każdego $x \in X$, istnieje dokładnie jeden element odwrotny x^{-1}: gdyby bowiem x' i x'' dwa odwrotne do x to

$$x' = ex' = (x''x)x' = x''(xx') = x''e = x'' \ .$$

Jeżeli $U \subseteq T$ i $G' = \langle U, *, e\rangle$ jest grupą, to mówimy, że G' jest *podgrupą* grupy G, co oznaczamy przez $G' \subseteq G$. Aby G' była podgrupą wystarczy: (a) $e \in U$, (b) jeżeli $y_1, y_2 \in U$ to $y_1 y_2 \in U$, (c) jeżeli $y \in U$ to $y^{-1} \in U$. Niech $A \subseteq T$. *Podgrupa G generowana przez A*, oznaczana $G(A)$, to taka podgrupa, że każda podgrupa G' zawierająca A zawiera także $G(A)$. Zauważmy, że przecięcie wszystkich podgrup zawierających A jest równe grupie $G(A)$. Można ją także opisać inaczej: składa sie z elementów postaci $b_1 * \ldots * b_i * \ldots * b_k$, dla $k \geq 1$, gdzie $b_i \in A$ lub $b_i^{-1} \in A$. Rzeczywiście, jest to podgrupa G, i jeżeli podgrupa G zawiera A to także zawiera takie iloczyny. Każda grupa jest generowana przez jakiś swój podzbiór, na przykład przez zbiór swoich wszystkich elementów. Jeżeli G ma jeden generator $g \in G$, to G nazywamy *cykliczną* i piszemy $G = G(g)$. Przykładem nieskończonej grupy cyklicznej jest $\langle \mathbb{Z}, +, 0\rangle$, generatorem jest 1. Przykładem skończonej grupy cyklicznej jest $\mathbb{Z}_n = \langle [0..n-1], +, 0\rangle$, gdzie dodawanie modulo n, generatorem jest 1. *Rząd* skończonej grupy G to liczba jej elementów, oznaczana $|G|$. Jeżeli $x \in G$, to elementy $x^0 = e, x^1 = x, x^2 = xx, x^3 = xxx, \ldots$ należą do podgrupy generowanej przez x. Element x jest *rzędu k*, gdy $k > 0$ to najmniejsza liczba całkowita taka że $x^k = e$; rząd x oznaczamy $r(x)$, jest to także rząd podgrupy generowanej przez x. Zachodzi $a^i = e$ w.t.w. gdy $r(a) \mid i$.

Dane dwie grupy $G = \langle T, *, e\rangle$ oraz $G' = \langle T', *', e'\rangle$. Przekształcenie $f : T \to T'$ jest *homomorfizmem* gdy $f(x * y) = f(x) *' f(y)$ dla wszystkich $x, y \in T$. Wtedy także $f(e) = e'$, ponieważ $f(x) = f(e * x) = f(e) *' f(x)$. Także $f(x^{-1}) = f(x)^{-1}$, ponieważ $e' = f(e) = f(x * x^{-1}) = f(x) *' f(x^{-1})$. Jeżeli homomorfizm jest wzajemnie jednoznaczny, to nazywamy go *izomorfizmem*. Jeżeli G jest generowana przez zbiór A to homomorfizm określony na A jest wyznaczony jednoznacznie na całej G. Stąd wynika także, że dwie

grupy cykliczne tego samego rzędu są izomorficzne: izomorfizm f z $G = G(a)$ na $G' = G'(b)$ określamy kładąc $f(a) = b$. W szczególności, każda skończona grupa cykliczna rzędu n jest izomorficzna z $\mathbb{Z}_n$, a każda nieskończona z $\langle \mathbb{Z}, +, 0 \rangle$.

Jeżeli $H \subseteq G$ jest podgrupą, to *warstwą lewostronną G względem H* nazywamy każdy podzbiór postaci $xH = \{xh : h \in H\}$. Podobnie *warstwy prawostronne* są postaci $Hx = \{hx : h \in H\}$. Warstwy, lewo lub prawostronne, odpowiednio, względem H stanowią podział G, to znaczy są rozłączne i wypełniają całą grupę G. Rzeczywiście: Po pierwsze $x = xe \in xH$. Po drugie, jeżeli $x_1H \cap x_2H \neq \emptyset$, to niech $x_1h_1 = x_2h_2$. Stąd $x_1 = x_2h_2h_1^{-1}$ czyli $x_1H = x_2h_2h_1^{-1}H \subseteq x_2H$. Podobnie $x_2H \subseteq x_1H$. Każda warstwa względem H jest równoliczna z H ponieważ przekształcenie przyporządkowujące xh elementowi $h \in H$, dla ustalonego x, jest różnowartościowe. Stąd dostajemy *twierdzenie Lagrange'a*: rząd podgrupy jest dzielnikiem rzędu grupy.

Niech $G = G(g)$ grupa cykliczna oraz $|G| = n$. Jaki jest rząd g^i? Zachodzi $(g^i)^k = e$ w.t.w. gdy $n \mid i{\cdot}k = \frac{i}{(n,i)}{\cdot}k{\cdot}(n,i)$. Ponieważ $n \perp \frac{i}{(n,i)}$, jest to równoważne $n \mid k{\cdot}(n,i)$, czyli $\frac{n}{(n,i)} \mid k$. Najmniejsze takie k jest równe $\frac{n}{(n,i)}$. Stąd wynika, że jest $\phi(n)$ generatorów G. Ile jest elementów rzędu d w G? Oznaczmy tę liczbę przez $s(d)$. Z twierdzenia Lagrange'a wynika, że jeżeli $s(d) > 0$ to $d \mid n$. Także jeżeli $d \mid n$ to $g^{n/d}$ ma rząd d, zatem $s(d) > 0$. Rozważmy podgrupę $G_d \subseteq G$ generowaną przez $a = g^{n/d}$. Jeżeli $1 \leq i \leq d$ oraz $i \perp d$ to a^i generuje G_d, zatem jest rzędu d w G. Stąd $s(d) \geq \phi(d)$. Mamy także $\sum_{d|n} s(d) = n$, ponieważ każde g^i, dla $1 \leq i \leq n$, jest jakiegoś rzędu $d \mid n$. Ale $\sum_{d|n} \phi(d) = n$, zatem ostatecznie $s(d) = \phi(d)$, dla $d \mid n$.

Zbiór przekształceń wzajemnie jednoznacznych zbioru Y na siebie stanowi grupę z działaniem składania przekształceń: jeżeli $f, g : Y \to Y$ to fg w punkcie $y \in Y$ przyjmuje wartość $f(g(y))$. Elementem neutralnym jest identyczność, a odwrotnością przekształcenie odwrotne. Tę grupę oznaczamy przez $S(Y)$ i nazywamy *grupą symetryczną*. Jeżeli $Y = \{1, \ldots, n\}$ to grupę symetryczną $S(Y)$ oznaczamy przez S_n, jest to grupa permutacji $\{1, \ldots, n\}$. Ta grupa nie jest przemienna: wystarczy by $f(1) = 2$, $g(2) = 1$, oraz $g(1) = 2$, $f(2) = 3$, wtedy $fg \neq gf$. Grupa S_n jest generowana przez cykle, co wynika z rozkładu permutacji na cykle, ponieważ każdy z nich jest permutacją podzbioru rozłącznego z pozostałymi. Nazwijmy *transpozycją* cykl długości dwa. Już transpozycje generują S_n ponieważ zachodzi równość:

$$[1, 2, \ldots, k] = [1, k][1, k-1] \ldots [1, 3][1, 2] \; .$$

Transpozycje nie są przemienne, także rozkład na transpozycje nie jest jednoznaczny. Jeżeli permutację $f \in S_n$ przedstawimy w postaci złożenia transpozycji, to wszystkie takie rozkłady bedą miały parzystą lub wszystkie nieparzystą liczbę transpozycji, zależnie od tego czy f jest *parzysta* czy *nieparzysta*, odpowiednio. Wynika to z następującej własności transpozycji: permutacja $[a, b]\sigma$ ma o jeden cykl więcej niż σ, gdy a i b są w tym samym cyklu σ, oraz o jeden cykl mniej niż σ, gdy a i b są w różnych cyklach σ. Sprawdzenie tego jest bezpośrednie:

$$[a, b][a, x_1, \ldots, x_k, b, y_1, \ldots, y_i] = [a, x_1, \ldots, x_k][b, y_1, \ldots, y_i] \; ,$$
$$[a, b][a, x_1, \ldots, x_k][b, y_1, \ldots, y_i] = [a, x_1, \ldots, x_k, b, y_1, \ldots, y_i] \; .$$

Zatem, jeżeli mamy przedstawienie permutacji $f \in S_n$ o k cyklach w postaci złożenia t transpozycji, to pewne $n-k$ transpozycje zmniejszają liczbę cykli z początkowo równej n (liczba cykli permutacji identycznościowej) do k, ale pozostałe transpozycje zwiększające muszą być zbilansowane przez zmniejszające liczbę cykli o jeden. Czyli parzystość liczby t jest równa parzystości liczby $n-k$.

Twierdzenie Caley'a mówi, ze każda grupa skończona rzędu n jest izomorficzna z pewną podgrupą S_n. Zauważmy mianowicie, że każdemu elementowi $x \in G$ można przyporządkować permutację P_x wzorem $P_x(g) = xg$. Permutacje postaci P_x tworzą podgrupę S_n. Własność homomorfizmu zachodzi, ponieważ

$$P_{xy}(g) = (xy)g = x(yg) = P_x(P_y(g)) \ .$$

Jest to izomorfizm, ponieważ jeżeli $P_{x_1} = P_{x_2}$ to $P_{x_1}(g) = P_{x_2}(g)$ dla każdego g, czyli $x_1 g = x_2 g$, a zatem $x_1 = x_2$. Tę konstrukcję uogólniamy do szerszego pojecia *reprezentacji* grupy G w grupie symetrycznej $S(X)$, zastepując w definicji izomorfizm przez homomorfizm $h : G \to S(X)$. Mówimy wtedy, że G *działa* na X. Dla prostoty oznaczeń piszemy gx zamiast $h(g)(x)$, gdzie $g \in G, x \in X$. Takie przyporządkowanie h jest homomorfizmem, gdy zachodzi równość $g_1(g_2 x) = (g_1 g_2)x$, dla $g_1, g_2 \in G, x \in X$. Mówimy, że $x, x' \in X$ są *G-równoważne* gdy $x' = gx$ dla pewnego $g \in G$. Relacja G-równoważności jest relacją równoważności, w tym sensie, że jest zwrotna, symetryczna i przechodnia. W problemach zliczania, gdy X jest zbiorem konfiguracji kombinatorycznych, równoważność konfiguracji określa się często przez działanie pewnej grupy G, przy czym chcemy znaleźć liczbę nierównoważnych konfiguracji, czyli inaczej liczbę klas abstrakcji relacji G-równoważności.

Orbitą elementu $x \in X$ nazywamy zbiór $Gx = \{gx : g \in G\}$. Orbity to klasy abstrakcji relacji G-równoważności. Wprowadzamy jeszcze oznaczenie $G_x = \{g \in G : gx = x\}$, zbior G_x nazywamy *stabilizatorem* punktu x. Dualnie, określamy $X_g = \{x \in X : gx = x\}$, jest to zbiór punktów stałych względem $g \in G$. Zbiór G_x jest podgrupą G. Zauważmy, że warstwy G_x odpowiadają elementom orbity Gx; rzeczywiscie, równoważne są:

$$g_1 x = g_2 x \text{ w.t.w. } g_1^{-1} g_2 x = x \text{ w.t.w. } g_1^{-1} g_2 \in G_x \text{ w.t.w. } g_2 \in g_1 G_x.$$

Stąd i z twierdzenia Lagrange'a dostajemy wzór

$$|G_x| \cdot |Gx| = |G| \ .$$

W większości zastosowań grupa G działa *wiernie* na X, to znaczy G jest podgrupą $S(X)$. Wtedy fx oznacza po prostu $f(x)$. Jeżeli $G = G(f)$ jest cykliczną grupą permutacji X, to orbita $x \in X$ składa się z punktów $x, fx, f^2 x, \ldots$, czyli z elementów w cyklu permutacji f, do którego należy x. (Czasem cykle permutacji nazywa się jej orbitami.)

Lemat Burnside'a mówi, że liczba orbit jest równa (średniej) liczbie punktów stałych X przypadających na element grupy G, czyli $|G|^{-1} \sum_{g \in G} |X_g|$. Oto wyprowadzenie tego wzoru. Liczbę par $\langle x, g \rangle$ takich że $x = gx$ można policzyć na dwa sposoby:
$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$. Stąd

$$|G|^{-1} \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|/|G| = \sum_{x \in X} 1/|Gx| \ .$$

Z prawej strony, każda wartość $|Gx|^{-1}$ jest dodawana $|Gx|$ razy, ponieważ taka jest liczność orbity Gx, dając w sumie jedynkę dla każdej orbity, co kończy dowód.

Przykład: Wyprowadzimy wzór na liczbę naszyjników z n korali, każdy mający kolor spośród k możliwych, przy czym cykliczne przesunięcie kolorów daje ten sam naszyjnik. Jest to przeformułowanie problemu o klasach abstrakcji cyklicznych słow nad alfabetem k elementowym. Używając terminologii grup, widzimy, że na n-permutacjach z powtórzeniami zbioru k elementowego działa wiernie grupa cykliczna rzędu n. Jej generator, oznaczmy go przez s, przesuwa kolory cyklicznie o jedną pozycję. Wyznaczymy liczbę kolorowań X_{s^i} stałych względem przesunięcia o i pozycji. Niech $(n, i) = d$. Wtedy rząd $r(s^i) = n/d$. Ustalenie koloru na jakiejś pozycji wymusza ten sam kolor na całej orbicie długości n/d. Takich orbit jest d, czyli $|X_{s^i}| = k^d$. Jest $\phi(x)$ elementów rzędu x w grupie cyklicznej rzędu n, gdzie $x \mid n$. Z lematu Burnside'a liczba naszyjników jest równa $\frac{1}{n}\sum_{d|n} \phi(n/d)k^d$. $\Diamond$

Rozważmy tę metodę w ogólnym przypadku. *Kolorowanie* to funkcja $f : X \to K$ w pewien zbiór K *kolorów*. Przypuśćmy, że mamy grupę G skladającą się z permutacji zbioru X, którego elementy kolorujemy. Chcielibyśmy rozszerzyć działanie G z X na zbiór F kolorowań X. Możemy to zrobić następująco: wartością działania $g \in G$ na kolorowaniu $f \in F$ jest fg^{-1}. Sprawdzamy bezpośrednio, że jest to homomorfizm:

$$g_1(g_2(f)) = fg_2^{-1}g_1^{-1} = f(g_1g_2)^{-1} = (g_1g_2)(f) \ ,$$

gdzie $g_1, g_2 \in G$. Niech $c(g)$, dla $g \in G$, będzie liczbą cykli g. Liczbę nierównoważnych kolorowań dana jest wzorem

$$\frac{1}{\mid G \mid} \sum_{g \in G} m^{c(g)}, \tag{1}$$

gdzie $m = |K|$. Rzeczywiście, z lematu Burnside'a wystarczy pokazać, że $|F_g| = m^{c(g)}$. Kolorowanie należy do F_g, gdy dla $x \in X$ wszystkie elementy x, gx, $g^2x, \ldots$, mają taki sam kolor, czyli elementy w każdym cyklu g mają taki sam kolor.

Strukturę cykli w grupie permutacji $G \subseteq S_n$ wygodnie jest opisać odpowiednią funkcją tworzącą, która w tym przypadku jest wielomianem od n zmiennych. Nazywamy ją *indeksem cyklowym*, określona jest przez wzór:

$$I_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} x_1^{g_1} x_2^{g_2} \cdots x_n^{g_n} \ ,$$

gdzie g_i to liczba cykli długości i w g. Formułę (1) można teraz zapisać jako $I_G(m, \ldots, m)$.

Przykład. Obliczymy indeks cyklowy dla grupy izometrii czworościanu foremnego (*izometria* to przekształcenie wzajemnie jednoznaczne figury geometrycznej w siebie, które zachowuje odległość). Izometria jest jednoznacznie wyznaczona przez obraz ustalonego wierzchołka i obrazy incydentnych z nim krawędzi: są 4 wierzchołki i 3 krawędzie, krawędzie możemy dowolnie permutować. Razem jest $24 = 4!$ izometrii, czyli jest to grupa izomorficzna z S_4. Oto rodzaje rozkładów na cykle w S_4:

$[a][b][c][d]$: 1 permutacja daje x_1^4;
$[a,b][c,d]$: 3 permutacje dają x_2^2;
$[a,b,c,d]$: 6 permutacji daje x_4.
$[a,b][c][d]$: 6 permutacji daje $x_1^2x_2$;
$[a,b,c][d]$: 8 permutacji daje x_1x_3;

Czyli indeks cyklowy równy $I_{S_4}(x_1,x_2,x_3,x_4) = \frac{1}{24}\big(x_1^4 + 6x_1^2x_2 + 3x_2^2 + 8x_1x_3 + 6x_4\big)$. Stąd dostajemy, że liczba pokolorowań czworościanu foremnego m kolorami, tak by nie były równoważne względem grupy izometrii, jest równa:

$$I_{S_4}(m,m,m,m) = \frac{1}{24}m^4 + \frac{1}{4}m^3 + \frac{11}{24}m^2 + \frac{1}{4}m \ .$$

$\Diamond$

Przykład: Niech G to grupa izometrii n-kąta foremnego, gdzie n nieparzyste. Pokażemy, że indeks cyklowy $I_G(x_1,\ldots,x_n)$ jest równy

$$\frac{1}{2n}\Big(nx_1x_2^{\frac{n-1}{2}} + \sum_{d|n}\phi(d)x_d^{n/d}\Big) \ .$$

Grupa składa się z n obrotów (jest to podgrupa cykliczna), oraz n symetrii osiowych. Każda symetria osiowa ma oś przechodzącą przez wierzchołek, czyli ma jeden cykl długości 1, oraz przecina w połowie jedną krawędź, czyli ma $\frac{n-1}{2}$ cykli długości 2. To daje pierwszy składnik. Drugi pochodzi od obrotów, odpowiada wzorowi na liczbę naszyjników. $\Diamond$

Opiszemy uogólnienie formuły $I_G(m,\ldots,m)$, dającej liczbę pokolorowań m kolorami, na przypadek kolorowań spełniajacych dodatkowe warunki. Nazwy kolorów $t_i \in K$, dla $1 \le i \le m = |K|$, będziemy traktowali jako zmienne. *Wagą kolorowania* f, oznaczaną $w(f)$, nazywamy jednomian $t_1^{a_1}t_2^{a_2}\ldots t_m^{a_m}$ gdy f nadaje kolor t_i dokładnie a_i punktom. Szukamy funkcji tworzącej (wielomianu) bedącej sumą wag wszystkich kolorowań, które nie są wzajemnie G-równoważne. *Twierdzenie Polya* mówi, że ta funkcja ma postać

$$I_G\Big(\sum_{t\in K} t, \sum_{t\in K} t^2, \ldots, \sum_{t\in K} t^n\Big),$$

gdzie $I_G(x_1,\ldots,x_n)$ jest indeksem cyklowym G. Dowód jest modyfikacją poprzednich rozumowań. Rozszerzamy już wprowadzoną notację na przypadek kolorowań:

$F_g = \{f \in F : f = fg^{-1}\}$ to zbiór kolorowań równoważnych względem $g \in G$.
$G_f = \{g \in G : fg^{-1} = f\}$ to stabilizator f, dla $f \in F$.
$Gf = \{f' \in F : f' = fg^{-1}$ i $g \in G\}$ to orbita f, dla $f \in F$.

Nowe oznaczenie to $W_g = \sum_{f\in F_g} w(f)$, czyli suma wag kolorowań z F_g. Pamiętamy, że zachodzi wzór $|G| = |G_f| \cdot |Gf|$. Niech R będzie zbiorem orbit G. Dla $r \in R$, waga orbity r, oznaczana $w(r)$, to waga $w(f)$ dla dowolnego $f \in r$. Rozważmy sumę wag kolorowań f po wszystkich parach $\langle f,g\rangle$ takich, że $f = fg^{-1}$. Jest ona równa $\sum_{g\in G} W_g = \sum_{f\in F} w(f)|G_f|$. Dostajemy uogólnienie lematu Burnside'a:

$$|G|^{-1}\sum_{g\in G} W_g = \sum_{f\in F} w(f)|G_f||G|^{-1} = \sum_{f\in F} |Gf|^{-1}w(f) = \sum_{r\in R} w(r)$$

Przekształcimy lewą stronę, by otrzymać twierdzenie Polya. Weźmy permutację $g \in G$ mającą g_i cykli długości i. Niech $x_1^{g_1} \dots x_n^{g_n}$ odpowiedni jednomian w $I_G(x_1, \dots, x_n)$. Elementy w cyklu muszą mieć ten sam kolor. Formalna suma kolorowań cyklu długości b jest równa $\sum_{t \in K} t^b$. Cykle kolorujemy niezależnie, stąd wkład g do W_g jest równy iloczynowi $(\sum_{t \in K} t^{g_1}) \cdot \dots \cdot (\sum_{t \in K} t^{g_n})$, co kończy dowód twierdzenia Polya.

Przykład: Kolorujemy wierzchołki czworościanu foremnego dwoma kolorami a i b. Z twierdzenia Polya funkcja tworzaca możliwych kolorowań powstaje z $I_{S_4}(x_1, x_2, x_3, x_4)$ przez podstawienie $a^i + b^i$ zamiast x_i. Dostajemy

$$\frac{1}{24}\big((a+b)^4 + 6(a+b)^2(a^2+b^2) + 3(a^2+b^2)^2 + 8(a+b)(a^3+b^3) + 6(a^4+b^4)\big) \\ = a^4 + a^3b + a^2b^2 + ab^3 + b^4 \ .$$

Jednomiany odpowiadają kolorowaniom, na przykład a^1b^3 odpowiada kolorowaniom, w których a występuje jeden a b trzy razy. Przy każdym jednomianie stoi współczynnik równy 1, czyli liczba wystąpień kolorów wyznacza jednoznacznie kolorowanie, co wynika także z tego, że grupą izometrii czworościanu jest pełna grupa symetryczna S_4. $\Diamond$

Zadania

1. Pokaż, że na zbiorze $\{e, a, b, c\}$ można określić grupę w dokładnie jeden sposób tak, by e był elementem neutralnym, oraz $a^2 = b^2 = c^2 = e$. Ta grupa nazywana jest *czwórkową grupą Kleina.*

2. Znajdź wszystkie grupy o odpowiednio $1, 2, 3, 4, 5$ elementach.

3. Znajdź grupę nieprzemienną najmniejszego rzędu.

4. Pokaż równoważność: ściany każdej mapy można pokolorować czterema kolorami w.t.w. gdy każda mapa kubiczna ma krawędziową liczbę chromatyczną równą 3. *Wskazówka:* Niech ściany kolorowane elementami czwórkowej grupy Kleina, a krawędzie różnymi od e elementami tej grupy.

5. Niech x będzie n-permutacją zawierajacą i_k cykli długości k, dla $1 \leq k \leq n$. Jaki jest rząd x?

6. Pokaż na przykładach, że transpozycje nie są przemienne, oraz że rozkład permutacji na transpozycje nie jest jednoznaczny.

7. Dany graf prosty $G = \langle V, E \rangle$, gdzie $V = [1..n]$. Rozważmy rodzinę transpozycji $T_G = \{[a, b] : \{a, b\} \in E\}$. Pokaż, że T_G generuję grupę S_n wszystkich permutacji V w.t.w. gdy G jest spójny.

8. W permutacji $a_1 a_2 \dots a_n$ liczb $\{1, 2, \dots, n\}$, każda para $\langle a_i, a_j \rangle$ taka, że $i < j$ oraz $a_i > a_j$ nazywa sie *inwersją.* Pokaż, że permutacja jest parzysta wtedy i tylko wtedy gdy jej liczba inwersji jest parzysta.

9. Czy zbiór wszystkich parzystych, odpowiednio nieparzystych, permutacji w S_n tworzy podgrupę?

10. Pokaż, że G_x jest podgrupą G, gdy $x \in X$ i G działa na X.

11. Niech G to grupa izometrii sześciokąta foremnego, a H to jej podgrupa składająca sie tylko z obrotów względem środka. Rozważamy kolorowania wierzchołków wielokąta dwoma kolorami.

    (a) Znajdź dwa kolorowania, które nie są H-równoważne natomiast są G-równoważne.

    (b) Znajdź wszystkie klasy abstrakcji relacji H-równoważności i G-równoważności.

    (c) Znajdź liczby takich klas z wzoru (1).

    (d) Znajdź indeksy cyklowe G i H, a stąd odpowiednie liczby klas.

    (e) Znajdź, z twierdzenia Polya, liczbę nierównoważnych kolorowań względem działania H i G takich, że jest i wystapień koloru białego oraz $6-i$ wystąpień koloru czarnego, dla każdego $1 \leq i \leq 6$.

12. Pokaż, że indeks cyklowy grupy izometrii n-kąta foremnego, gdzie n parzyste, jest równy
$$\frac{1}{2n}\Big(\frac{n}{2} \cdot x_1^2 x_2^{\frac{n}{2}-1} + \frac{n}{2} \cdot x_2^{\frac{n}{2}} + \sum_{d|n} \phi(d) x_d^{n/d}\Big) \ .$$

13. Znajdź indeks cyklowy grupy izometrii prostopadłościanu o długościach krawędzi równych 1 i 2.
Wskazówka: ta grupa ma rząd 16.

14. Znajdź indeks cyklowy grupy izometrii sześcianu.
Wskazówka: ta grupa ma rząd 48.

15. Na ile sposobów można pokolorować szachownicę rozmiaru $n \times n$ za pomocą m kolorów tak, by żadne kolorowanie nie było obrazem innego przy izometrii szachownicy?

MMD Wykład 4.

Bogdan Chlebus

Ciała skończone. Niech na zbiorze X będą określone działania *dodawania* $+$ i *mnożenia* $\cdot$, oraz wyróżnione elementy $0, 1 \in X$. Struktura algebraiczna $F = \langle X, +, \cdot, 0, 1\rangle$ jest *ciałem* gdy:

- $\langle X, +, 0\rangle$ jest grupą przemienną (nazywaną *addytywną*);
- $\langle X - \{0\}, \cdot, 1\rangle$ jest grupą przemienną (nazywana *multiplikatywną*);
- mnożenie jest rozdzielne względem dodawania: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;
- $0 \neq 1$.

Zwykle opuszczamy $\cdot$ jako symbol mnożenia i piszemy ab zamiast $a \cdot b$. Grupę multiplikatywną ciała F oznaczamy przez F^*. Jeżeli w definicji ciała opuścimy wymaganie dzielenia przez elementy różne od zera, to taka struktura nazywa się *pierścieniem przemiennym z jedynką*, lub krócej *pierścieniem*. Na przykład liczby całkowite $\mathbb{Z}$ z działaniami arytmetycznymi są pierścieniem. Także $\mathbb{Z}$ z działaniami modulo n jest pierścieniem, oznaczamy go przez $\mathbb{Z}/(n)$. *Rząd* pierścienia S (lub ciała) to liczba jego elementów, oznaczana przez $|S|$. Jeżeli $Y \subseteq X$ zawiera 0 i 1 oraz jest zamknięty na działania ciała F, to $\langle Y, +, \cdot, 0, 1\rangle$ też jest ciałem, nazywamy go *podciałem* ciała F. Jeżeli $A \subseteq X$, to przecięcie wszystkich podciał F zawierających A nazywamy *podciałem generowanym przez* A.

Jeżeli $x \cdot y = 0$ w pierścieniu, gdzie $x \neq 0$, $y \neq 0$, to x i y są *dzielnikami zera*. W ciałach takich nie ma, bowiem jeżeli $x \cdot y = 0$ i $x \neq 0$ to mamy:

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0 \ .$$

Na przykład $3 \cdot 4 \bmod 6 = 0$, zatem $\mathbb{Z}/(6)$ nie jest ciałem. Jeżeli p jest liczbą pierwszą, to $\mathbb{Z}/(p)$ jest ciałem. Mianowicie: jeżeli $1 < a < p$ to $(a, p) = 1$, zatem istnieją b i c całkowite takie, że $ab + cp = 1$. Stąd $a \cdot b \equiv 1 (\bmod\ p)$ i $b \bmod p$ jest odwrotnością liczby a.

Elementy $1, 1 + 1, 1 + 1 + 1, \ldots$ to *liczby* ciała, tworzą one *podciało proste*. Jeżeli ciało jest skończone to istnieją całkowite $n > m > 0$ takie, że $\sum_{i=1}^{n} 1 = \sum_{i=1}^{m} 1$, to znaczy $\sum_{i=1}^{n-m} 1 = 0$. Najmniejszą liczbę k o własności

$$\underbrace{1 + \cdots + 1}_{k} = 0$$

nazywamy *charakterystyką ciała*. Jeżeli sumy jedynek są zawsze różne od zera, to ciało ma *charakterystykę 0*. Charakterystyka ciała jest liczbą pierwszą, o ile jest różna od zera. Gdyby bowiem była liczbą złożoną postaci $n \cdot m$, to

$$\sum_{i=1}^{n \cdot m} 1 = \sum_{i=1}^{n} 1 \cdot \sum_{i=1}^{m} 1 = 0 \ ,$$

a stąd $\sum_{i=1}^{n} 1 = 0$ lub $\sum_{i=1}^{m} 1 = 0$ bo w ciele nie ma dzielników zera. Dwa ciała F_1 i F_2 o zbiorach elementów X i Y, odpowiednio, są *izomorficzne*, jeżeli istnieje taka funkcja

$f : X \to Y$ wzajemnie jednoznaczna, która jest izomorfizmem addytywnych i multiplikatywnych grup ciał F_1 i F_2. Ciała izomorficzne mają takie same własności wyrażalne w terminach ich struktury addytywnej i multiplikatywnej. Podciało proste ciała charakterystyki p jest izomorficzne z ciałem $\mathbb{Z}/(p)$. Mianowicie: izomorfizm określamy przyporządkowując $\sum_{i=1}^{n} 1 \in F$ liczbie $n \in \mathbb{Z}/(p)$, sprawdzenie własności izomorfizmu jest bezpośrednie. Jeżeli F jest podciałem ciała G to możemy traktować elementy F jako skalary a elementy G jako wektory i dostajemy przestrzeń liniową nad ciałem F. Jeżeli G jest skończone to ta przestrzeń jest skończonego wymiaru, niech b_1, $b_2, \ldots$, b_m wektory bazy i q rząd F. Każdy element G przedstawia się jednoznacznie w postaci $a_1 b_1 + \cdots + a_m b_m$, gdzie $a_i \in F$. Takich wyrażeń jest dokładnie q^m, i to jest rząd ciała G. Jeżeli $F \subseteq G$ ciała, to wymiar przestrzeni G nad ciałem F ozanaczamy przez $[G : F]$. Dla $F \subseteq G \subseteq H$ ciał, zachodzi

$$[H : F] = [H : G] \cdot [G : F] \ .$$

Każde ciało H charakterystyki $p > 0$ ma podciało proste o p elementach, stad rząd H jest postaci p^n, a podciała H mają rzędy postaci p^m, gdzie $m \mid n$.

Zbiór wielomianów o współczynnikach z ciała F oznaczamy przez $F[x]$, jest to pierścień bez dzielników zera. Stopień wielomianu P oznaczamy przez $\deg P$. Pierścień $F[x]$ ma wiele własności pierścienia liczb całkowitych $\mathbb{Z}$. Na przykład, można dzielić z resztą: jeżeli P i Q wielomiany, $\deg Q > 0$ to istnieją wielomiany A i R takie, że $P = A \cdot Q + R$ i $\deg R < \deg Q$. Taką resztę R oznaczamy przez $P \bmod Q$, a gdy jest równa zero to Q jest *dzielnikiem* P, co oznaczamy $Q \mid P$. Istnienie A i R pokazujemy przez indukcję, dowód przez algorytm, podobny do algorytmu dzielenia liczb całkowitych zapisanych w układzie pozycyjnym. Pokażemy jednoznaczność takiego dzielenia: jeżeli $P = B \cdot Q + S$ gdzie $\deg S < \deg Q$ to

$$0 = (A - B) \cdot Q + (R - S) \ ;$$

z faktu $\deg(R - S) < \deg Q$ wynika że $A = B$, a stąd dalej $R = S$.

Ideałem pierścienia $\langle X, +, \cdot, 0, 1\rangle$ jest taki zbiór $I \subseteq X$, że jeżeli $x, y \in I$ to $x + y \in I$, oraz jeżeli $x \in I$ i $r \in X$ to $x \cdot r \in I$. Ideał *generowany przez zbiór* $A \subseteq X$ to najmniejszy ideał zawierający A, jego elementy są postaci $a_1 r_1 + a_2 r_2 + \ldots + a_k r_k$, gdzie $a_i \in A$, $r_i \in X$. W pierścieniu wielomianów $F[x]$ o współczynnikach z ciała, każdy ideał $I \neq \{0\}$ jest *główny,* to znaczy jest generowany przez jeden element. Niech mianowicie $G \in I$ wielomian najmniejszego stopnia w I, spośród różnych od zera. Jeżeli $P \in I$, to przez podzielenie z resztą mamy $P = G \cdot Q + R$, gdzie $\deg R < \deg G$. Ponieważ $R \in I$, z wyboru G mamy $R = 0$, czyli $G \mid P$. Zatem I to zbiór wielokrotności G, czyli I jest generowany przez G.

Określimy NWD dla wielomianów, oznaczenie (P, Q) jak dla liczb całkowitych. Wielomian jest *unormowany*, gdy jego współczynnik przy najwyższej potędze jest równy 1. Dla $P, Q \in F[x]$, określamy (P, Q) jako taki wielomian unormowany, że jest on dzielnikiem P i Q, i jeżeli jakiś wielomian $A \in F[x]$ dzieli jednocześnie P i Q to także dzieli (P, Q). Dowód istnienia: Niech G generator ideału generowanego przez P i Q. Każdy wielomian postaci $A \cdot P + B \cdot Q$ jest wielokrotnością G. Wielomian G po *unormowaniu*, czyli podzieleniu przez współczynnik przy najwyższej potędze zmiennej, daje szukany wielomian.

Dowód jednoznaczności: istnieje dokładnie jeden wielomian unormowany będący wielokrotnością G. Widzimy, że istnieją $A, B \in F[x]$ takie, że $A \cdot P + B \cdot Q = (P, Q)$. NWD można znaleźć algorytmem Euklidesa:

$$(P, Q) = \begin{cases} P & \text{jeżeli } \deg Q = 0 < \deg P \ , \\ (P \bmod Q, Q) & \text{jeżeli } 0 < \deg Q \leq \deg P \ . \end{cases}$$

Odpowiednikiem w $F[x]$ liczb pierwszych są wielomiany nierozkładalne: $P \in F[x]$ jest *nierozkładalny*, gdy rozkład $P = Q \cdot R$ implikuje że $Q \in F$ lub $R \in F$. Zachodzi następujący odpowiednik lematu Euklidesa: jeżeli P nierozkładalny i $P \mid A \cdot B$ to $P \mid A$ lub $P \mid B$. Mianowicie, jeżeli P nie dzieli A to $(P, A) = 1$, istnieją C i D takie, że $CP + DA = 1$, a stąd $CPB + DAB = B$. Ponieważ P dzieli lewą stronę więc i prawą. Także podobnie pokazujemy twierdzenie o jednoznaczności rozkładu: każdy unormowany wielomian $P \in F[x]$, dla którego $\deg P > 0$, rozkłada się jednoznacznie, z dokładnością do porządku czynników, na iloczyn unormowanych wielomianów nierozkładalnych stopni większych od zera. Dowód przez indukcję. Weźmy dwa możliwe rozkłady $A_1 \ldots A_k = B_1 \ldots B_n$, uporządkowane względem stopni. Z lematu Euklidesa A_1 dzieli B_i dla pewnego $1 \leq i \leq n$, a stąd $A_1 = B_1$. Zauważmy, że taki *kanoniczny rozkład* zależy od ciała współczynników; na przykład $x^2 - 2$ jest nierozkładalny nad ciałem liczb wymiernych natomiast rozkładalny na iloczyn $(x - \sqrt{2})(x + \sqrt{2})$ nad ciałem liczb rzeczywistych.

Zachodzi równoważność: $f \in F$ jest pierwiastkiem $A(x) \in F[x]$ w.t.w. gdy $(x - f) \mid A(x)$. Rzeczywiscie, wystarczy podzielić z resztą A przez $x - f$, dostajemy $A(x) = (x - f) \cdot B(x) + C$, gdzie $C \in F$. Jeżeli $n = \deg A(x)$ to $A(x)$ nie może się dzielić przez więcej niż n różnych czynników o stopniach większych od zera, a zatem wielomian stopnia n nad cialem F ma nie więcej niż n pierwiastków w F.

Dla wielomianu P okreslamy relację $A \equiv B \pmod P$ w.t.w. gdy $P \mid (A - B)$. Jest to relacja rownowaznosci, kazda klasa jest reprezentowana przez reszte modulo P. Na zbiorze klas rownowaznosci (lub reszt) okreslamy dzialania

$$[A] + [B] = [A + B], \qquad [A] \cdot [B] = [A \cdot B] \ .$$

Pierścień reszt z $F[x]$ modulo $P \in F[x]$ oznaczamy przez $F[x]/P$. Jeżeli $P \in F[x]$ jest nierozkładalny stopnia m, oraz $|F| = q$, to pierścień $F[x]/P$ jest ciałem o q^m elementach. Dlaczego taki rząd: reszta jest jednoznacznie określona przez ciąg współczynników dlugości m, takich ciągów jest ich q^m. Dlaczego cialo: trzeba pokazac istnienie elementow odwrotnych. Niech A reszta taka, ze $A \not\equiv 0 \pmod P$. Jest $q^m - 1$ wielomianow postaci $A \cdot B$, gdzie $\deg B < m$, $B \neq 0$. Jezeli $AB_1 \equiv AB_2 \pmod P$ to $P \mid A(B_1 - B_2)$. Poniewaz P nierozkladalny i nie dzieli A wiec $P \mid (B_1 - B_2)$, ale $\deg(B_1 - B_2) < m$ czyli $B_1 = B_2$. Zatem reszty $AB \bmod P$ przebiegają wszystkie niezerowe wielomiany stopnia mniejszego niz $\deg P$, w szczegolnosci $A \cdot B \equiv 1 \pmod P$, dla pewnego B, czyli $[B]$ jest odwrotnoscia klasy $[A]$. Jeżeli mamy wielomian $R \in \mathbb{Z}/(p)[x]$ nierozkładalny nad $\mathbb{Z}/(p)$, to pozwala on zbudować ciało o p^k elementach, gdzie $k = \deg R$.

Przykład: Zbudujemy cialo o $4 = 2^2$ elementach. Potrzebujemy mieć nierozkładalny wielomian stopnia 2 nad $\mathbb{Z}/(2)$. Rozkładalne są trzy:

- $x \cdot x = x^2$;

- $x \cdot (x+1) = x^2 + x$;
- $(x+1) \cdot (x+1) = x^2 + 1$.

Zatem $P = x^2 + x + 1$ nierozkładalny. Elementy ciała reprezentujemy przez 0, 1, x, $x+1$. Oto przykłady mnożenia w tym ciele:

- $(x+1)(x+1) = x^2 + 1 \bmod P = 1 \cdot (x^2 + x + 1) + x \bmod P = x$;
- $x(x+1) = x^2 + x \bmod P = 1 \cdot (x^2 + x + 1) + 1 \bmod P = 1$.

$\Diamond$

Pokażemy, że dla każdej liczby pierwszej p i $n > 0$ istnieje cialo o p^n elementach. Jeżeli $n = 1$ to ciało $\mathbb{Z}/(p)$. Niech $n > 1$, rozwazmy $R(x) = x^{p^n} - x$. Weźmy dowolny czynnik $C_1 \mid R$ stopnia > 1 nierozkladalny nad $\mathbb{Z}/(p)$, o ile istnieje. Niech F_1 to ciało reszt modulo C_1, zawiera ono $\mathbb{Z}/(p)$ i R jest nad nim rozkładalny, bo zawiera pierwiastek $[x]$. Jeżeli R rozkłada się nad F_1 na czynniki liniowe, to zatrzymujemy budowę ciągu ciał, w przeciwnym przypadku weźmy czynnik $C_2 \mid R$, gdzie $\deg C_2 > 1$, nierozkładalny nad F_1, i niech F_2 bedzie ciałem reszt modulo C_2. Postepujemy dalej podobnie, aż otrzymamy ciało F' w którym R rozkłada się na czynniki liniowe. Mają miejsce dwa fakty:

1. Zera wielomianu $R = x^{p^n} - x$ w F' tworzą podciało, oznaczmy je przez $\hat{F}$;
2. Wielomian $R = x^{p^n} - x$ ma w F' dokładnie p^n różnych zer.

Pierwsza własność wynika z tożsamości $(a+b)^p = a^p + b^p$ prawdziwej w dowolnym ciele charakterystyki p (ćwiczenie). Dokładniej, trzeba pokazać, że jeżeli $a, b \in \hat{F}$, to $a+b \in \hat{F}$ i $a \cdot b \in \hat{F}$. Sprawdzamy:

$$(a+b)^{p^n} = (a^p + b^p)^{p^{n-1}} = \left(a^{p^2} + b^{p^2}\right)^{p^{n-2}} = \ldots = a^{p^n} + b^{p^n} = a + b \ ,$$

oraz $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n}$.

Własnosc druga oznacza, ze R nie ma w $\hat{F}$ pierwiastkow wielokrotnych. Określmy pochodna wielomianu: jezeli $A(x) = \sum_{i=0}^{k} a_i x^i$, to *pochodną* A jest $A'(x) = \sum_{i=1}^{k} i a_i x^{i-1}$. Pochodna ma nastepujace wlasnosci: $(A+B)' = A' + B'$, $(A \cdot B)' = AB' + A'B$ (ćwiczenie). Niech $A(x)$ ma pierwiastek a co najmniej dwukrotny, to znaczy $A(x) = (x-a)^2 \cdot B(x)$. Wtedy $A'(x) = 2(x-a)B(x) + (x-a)^2 B'(x)$. Stad $(x-a) \mid A$ i $(x-a) \mid A'$, czyli $(A, A') \neq 1$. Sprawdzamy, że $\left(x^{p^n} - x\right)' = p^n x^{p^n - 1} - 1 = -1$, poniewaz $p^n = 0$. Stad $x^{p^n} - x$ nie ma pierwiastkow wielokrotnych w zadnym ciele charakterystyki p, zatem ma p^n pierwiastków w ciele F'.

Naszym celem jest teraz pokazanie, że rząd ciała skończonego określa je jednoznacznie, z dokładnością do izomorfizmu. Zaczniemy od ogólnej własności grup przemiennych. Niech G grupa przemienna, oraz $x, y \in G$ takie, że $r(x) \perp r(y)$. Niech $g \in G(x) \cap G(y)$. Wtedy $g = x^k = y^n$, zatem $g^{r(x)} = x^{r(x)k} = e$, podobnie $g^{r(y)} = e$. Stąd $r(g) \mid (r(x), r(y)) = 1$ czyli $g = e$. Mamy $r(xy) \leq r(x)r(y)$ ponieważ $(xy)^{r(x)r(y)} = e$. Z drugiej strony, jeżeli

$(xy)^m = e$ to $x^m = y^{-m}$, zatem $x^m, y^m \in G(x) \cap G(y)$, czyli $x^m = e$ i $y^m = e$, zatem $r(x) \mid m$ i $r(y) \mid m$, stąd $r(x) \cdot r(y) \mid m$, czyli $r(xy) \geq r(x)r(y)$. Dostaliśmy równość $r(xy) = r(x)r(y)$.

Niech F pewne ciało rzędu $q = p^n$. Pokażemy że grupa multiplikatywna F^* jest cykliczna, jej generator nazywamy *elementem pierwotnym*. Mamy $|F^*| = q - 1$. Rozważmy element $a \in F^*$ o maksymalnym rzędzie $u = r(a)$. Zachodzi $u \leq q - 1$. Wystarczy pokazać, że dowolny element F^* spełnia równanie $x^u - 1 = 0$, ponieważ wtedy wielomian $x^u - 1$ ma $q - 1$ roznych pierwiastkow w F, zatem $q - 1 \leq u$, czyli razem $q - 1 = u$ i a jest generatorem. Niech $b \in F^*$ dowolny element różny od 1, niech $v = r(b)$. Jezeli $b^u \neq 1$ to $v \nmid u$. Niech $v = p_1^{s_1} \cdot \ldots \cdot p_k^{s_k}$, $u = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k}$ rozkłady na czynniki pierwsze, gdzie $s_i \geq 0$, $t_i \geq 0$. Istnieje $1 \leq i \leq k$ takie, że $s_i > t_i$, na przykład niech $i = 1$. Rozważamy $a' = a^{u/p_2^{t_2} \ldots p_k^{t_k}}$ oraz $b' = b^{v/p_1^{s_1}}$. Mamy $r(a') = p_2^{t_2} \cdot \ldots \cdot p_k^{t_k}$ oraz $r(b') = p_1^{t_1}$, czyli $r(a') \perp r(b')$. Zatem $r(a' \cdot b') = r(a') \cdot r(b') = p_1^{s_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_k^{t_k} > u$ - sprzeczność z założeniem $b^u \neq 1$. Czyli rzeczywiście a jest generatorem F^*. Każdy element F^* spełnia równanie $x^{p^n - 1} - 1 = 0$, co jest odpowiednikiem małego twierdzenia Fermata dla ciał skończonych. Stąd mamy, że każdy element F jest pierwiastkiem wielomianu $x^{p^n} - x$, zatem ma miejsce rozkład postaci

$$x^{p^n} - x = \prod_{a \in F} (x - a) \ .$$

W szczególności każdy element $a \in F$ jest pierwiastkiem jakiegoś wielomianu o współczynnikach z $\mathbb{Z}/(p)$. Unormowany generator ideału wszystkich wielomianów R o współczynnikach z $\mathbb{Z}/(p)$ takich, że $R(a) = 0$ nazywamy *wielomianem minimalnym* dla $a \in F$ i oznaczamy przez $M_a(x)$. Oto istotne własności $M_a(x)$:

- jest nierozkładalny nad $\mathbb{Z}/(p)$;
- dzieli $Q \in \mathbb{Z}/(p)[x]$ w.t.w. gdy $Q(a) = 0$;
- jest wielomianem najmniejszego stopnia spośród $Q \in \mathbb{Z}/(p)[x]$ takich, że $Q(a) = 0$.

W szczegolnosci $M_a(x) \mid x^{p^n} - x$. Niech F_a oznacza podciało F generowane przez $\mathbb{Z}/(p)$ i a. Pokażemy, że ciało F_a jest izomorficzne z $\mathbb{Z}/(p)[x]/M_a(x)$. Mianowicie: $1, a, a^2, \ldots, a^{k-1}$ tworzą bazę F_a nad $\mathbb{Z}/(p)$, gdzie $k = \deg M_a(x)$. Przyporządkowanie elementowi $b = \sum_{i=0}^{k-1} c_i \cdot a^i \in F_a$ reszty $\sum_{i=0}^{k-1} c_i \cdot x^i$ określa izomorfizm, gdzie $c_i \in \mathbb{Z}/(p)$. Zauważmy, że b jest wartością w punkcie a wielomianu o współczynnikach c_i. Takie wielomiany możemy dodawać "po współrzędnych", to daje izomorfizm dodawania. Sprawdzenie dla mnożenia opiera się na tym, że zachodzi $M_a(a) = 0$ w F, oraz $M_a(x) = 0$ w $\mathbb{Z}/(p)[x]/M_a(x)$. Jeżeli a jest elementem pierwotnym F, to $F_a = F$, bowiem F_a zawiera wszystkie potęgi a. Dla takiego a zachodzi $\deg M_a(x) = n = [F : \mathbb{Z}/(p)]$. Przy okazji pokazaliśmy, że dla każdego $n \geq 1$ istnieje wielomian nierozkładalny nad $\mathbb{Z}/(p)$ stopnia n.

Niech G inne ciało rzędu p^n. Ponieważ $M_a(x) \mid x^q - x$, oraz $x^q - x$ rozkłada się w G na czynniki liniowe, istnieje element b w G dla którego $M_a(x)$ jest jego wielomianem minimalnym. Stąd $G = G_b$ też jest izomorficzne z $\mathbb{Z}/(p)[x]/M_a(x)$. Jedyne ciało o $q = p^n$ elementach oznaczamy przez $\mathrm{GF}(q)$ lub $\mathbb{F}_q$.

Czy każdy wielomian $R \in \mathbb{F}_p[x]$ nierozkładalny nad $\mathbb{F}_p$ stopnia m ma pierwiastek w ciele rzędu p^m? Tak, ponieważ ma w ciele $\mathbb{F}_p[x]/R$, a jest to ciało rzędu p^m, które jest jedyne z dokładnością do izomorfizmu. Zachodzi mocniejszy fakt: $x^{p^m} - x$ jest iloczynem wszystkich unormowanych wielomianow nierozkladalnych R nad $\mathbb{F}_p$, takich, że $\deg R \mid m$. Mianowicie, niech R nierozkładalny i $k = \deg R$. Jeżeli $k \mid m$ to także $x^{p^k} - x \mid x^{p^m} - x$, ponieważ $p^k - 1 \mid p^m - 1$, zatem $\mathrm{GF}(p^k)$ jest podciałem $\mathrm{GF}(p^m)$, jako zbiór tych elementów $\mathrm{GF}(p^m)$, które są pierwiastkami $x^{p^k} - x$. W ciele $F' = \mathbb{F}_p[x]/R$ element $[x]$ jest pierwiastkiem R. Także $[F' : \mathbb{F}_p] = k$, czyli F' jest izomorficzny z $\mathrm{GF}(p^k)$. Stąd R ma pierwiastek w $\mathrm{GF}(p^k)$, a zatem także w $\mathrm{GF}(p^m)$. Taki pierwiastek $a \in \mathrm{GF}(p^m)$ jest pierwiastkiem $x^{p^m} - x$, czyli $R \mid x^{p^m} - x$, ponieważ R jest wielomianem minimalnym dla a. Teraz w drugą stronę: Niech $R \in \mathbb{F}_p[x]$ nierozkładalny nad $\mathbb{F}_p$ i $R \mid x^{p^m} - x$, oraz $k = \deg R$. R ma pierwiastek a w $\mathrm{GF}(p^m)$. Podciało $F'' \subseteq \mathrm{GF}(p^m)$ generowane przez $\mathbb{F}_p$ i a ma wymiar k jako przestrzeń liniowa. Ale $[\mathrm{GF}(p^m) : F''] \cdot [F'' : \mathrm{GF}(p)] = m$, zatem $k \mid m$. Na koniec, ponieważ $x^{p^m} - x$ nie ma pierwiastków wielokrotnych, każdy R unormowany nierozkładalny nad $\mathbb{F}_p$ występuje dokładnie raz jako czynnik $x^{p^m} - x$.

Niech $W_p(d)$ oznacza liczbę unormowanych wielomianów $R \in \mathbb{F}_p[x]$ stopnia d nierozkładalnych nad $\mathbb{F}_p$. Z powyższych rozważań, przez przyrównanie p^n i sumy stopni dzielników $x^{p^n} - x$, wynika, że $p^n = \sum_{d|n} d \cdot W_p(d)$. Z wzoru Möbiusa na odwracanie dostajemy, że liczba unormowanych wielomianów nierozkładalnych nad $GF(p)$ stopnia n jest równa

$$W_p(n) = \frac{1}{n} \sum_{d|n} \mu(n/d) \cdot p^d \ .$$

Zadania

1. Niech G grupa abelowa, $x, y \in G$ takie, że $r(x) \perp r(y)$. Pokaż, że $G(x, y) = G(xy)$.

2. Znajdz wszystkie nierozkładalne wielomiany stopnia 3 w $\mathbb{F}_2[x]$. Rozłóż $x^{2^3} + x$ na czynniki nierozkładalne nad $\mathbb{F}_2$.

3. Czy wielomian $x^4 + 1$ jest rozkładalny nad $\mathbb{F}_3$?

4. Pokaż, że jezeli p jest pierwsza oraz $0 < k < p$, to $\binom{p}{k} \equiv 0 \pmod{p}$. Wywnioskuj, że w ciele charakterystyki p zachodzi wzór $(a + b)^p = a^p + b^p$.

5. Pokaż, że dla ciał $F \subseteq G \subseteq H$ jest prawdziwy wzór $[H : F] = [H : G] \cdot [G : F]$.

6. Niech symbol $'$ oznacza pochodną wielomianu. Pokaż wzory

$$(P + Q)' = P' + Q' \quad \text{oraz} \quad (P \cdot Q)' = P \cdot Q' + P' \cdot Q \ .$$

7. Pokaż że stopnie wielomianów minimalnych elementów $\mathrm{GF}(p^n)$ są nie większe niż n.

8. Zbuduj $\mathrm{GF}(3^2)$, znajdz w nim element pierwotny i jego wielomian minimalny.

9. Niech $R(x) \in \mathbb{F}_p[x]$ nierozkładalny nad F_p, oraz $k = \deg R$. Czy jest prawdziwa równoważność: $[x]$ jest pierwotny w $\mathbb{F}[x]/R(x)$ w.t.w. gdy $R(x)$ jest wielomianem minimalnym elementu pierwotnego w $\mathrm{GF}(p^k)$?

10. Ile jest elementów pierwotnych w ciele $\mathbb{F}_q$?

11. Podaj wszystkie liczby całkowite $3 \leq q \leq 97$, będące potęgami liczb pierwszych, takie, że w ciele $\mathbb{F}_q$ każdy element różny od 0 i od 1 jest pierwotny.

12. Pokaż, że liczbami ciała charakterystyki p są dokładnie te elementy a, które spełniają równość $a^p = a$.

13. *Automorfizmem ciała* F jest izomorfizm F z F. Zbiór automorfizmów ciała tworzy grupę, ze składaniem przekształceń jako działaniem grupowym. Pokaż, że przekształcenie $a \mapsto a^p$ jest automorfizmem, który generuje grupę wszystkich automorfizmów ciała skończonego charakterystyki p.

14. Pokaż, że jeżeli σ jest automorfizmem ciała F, oraz $a \in F$, to a i $\sigma(a)$ mają ten sam wielomian minimalny.

15. Liczba różnych elementów ciała charakterystyki p, które są postaci $u, u^p, u^{p^2}, \ldots$, to *stopień* u. Pokaż, że jeżeli r jest stopniem u to wielomianem minimalnym u jest

$$R(x) = \prod_{i=0}^{r-1} \left(x - u^{p^i}\right) .$$

Wskazówka: Pokaż, że $[R(x)]^p = R(x^p)$.

16. Niech α element pierwotny ciala charakterystyki 2. Pokaż, że α oraz α^3 maja rozne wielomiany minimalne.

17. Niech α element pierwotny ciala $\mathrm{GF}(p^m)$. Pokaż, że α^g ma wielomian minimalny stopnia i, gdzie liczba i jest minimalna o takiej własności, że $g \equiv g \cdot p^i \pmod{p^m - 1}$.

18. Wybieramy losowy wielomian stopnia n z $\mathbb{F}_p[x]$. Pokaż, że prawdopodobieństwo wybrania wielomianu nierozkładalnego wynosi $\frac{1}{n \cdot p}\left(1 + \mathcal{O}(p^{-n/2})\right)$.

MMD Wykład 5.

Bogdan Chlebus

Prawdopodobieństwo. *Dyskretna przestrzeń probabilistyczna* składa się z przeliczalnego zbioru *zdarzeń elementarnych* $\Omega = \{\omega_1, \omega_2, \ldots\}$, gdzie dla każdego $\omega \in \Omega$ określone jest jego *prawdopodobieństwo* $\mathsf{P}[\omega] \in [0,1]$. Podzbiór $A \subseteq \Omega$ nazywamy *zdarzeniem*, jego prawdopodobieństwo określamy wzorem $\mathsf{P}[A] = \sum_{\omega \in A} \mathsf{P}[\omega]$. Od funkcji P wymagamy, by $\mathsf{P}[\Omega] = 1$.

Probabilistyka powstała z rozważań nad grami hazardowymi. Stąd czesto spotykane przykłady ilustrujące pojecie przestrzeni probabilistycznej opisane sa w jezyku rzutów kostką lub monetą. Pamiętajmy jednak, że takie doświadczenia to zjawiska fizyczne, natomiast my rozważamy formalne modele. Na przykład niech $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6\}$ to zbiór możliwych wyników rzutu kostką, określamy $\mathsf{P}[\omega_i] = 1/6$, dla $1 \leq i \leq 6$, wtedy prawdopodobienstwo wyrzucenia parzystej liczby oczek to $\mathsf{P}[\omega_2, \omega_4, \omega_6] = \mathsf{P}[\omega_2] + \mathsf{P}[\omega_4] + \mathsf{P}[\omega_6] = 1/6 + 1/6 + 1/6 = 1/2$. Zauważmy, że przyjęcie wszystkich prawdopodobieństw zdarzeń elementarnych równych sobie nie jest konieczne, i każde inne 6 liczb byłoby formalnie poprawne, pod warunkiem że byłyby nieujemne i sumowały się do 1. Ten konkretny wybór odpowiada idealnej kostce.

Jeżeli mamy przestrzeń probabilistyczną gdzie zdarzeniami elementarnymi są konfiguracje kombinatoryczne, i w której wszystkie zdarzenia elementarne mają takie same prawdopodobieństwa, to zwykle mówimy krótko, że odpowiednie konfiguracje są *losowe*. Na przykład określenia *losowy wybór kuli z urny* lub *losowa permutacja n liczb* oznaczają, że każdą wybieramy z takim samym prawdopodobieństwem.

Niech $-A$ oznacza $\Omega - A$. Z definicji prawdopodobieństwa $\mathsf{P}[-A] = 1 - \mathsf{P}[A]$. Jeżeli $A \cap B = \emptyset$ to $\mathsf{P}[A \cup B] = \mathsf{P}[A] + \mathsf{P}[B]$, takze $\mathsf{P}[\bigcup_{i=1}^{\infty} A_i] = \sum_{i=1}^{\infty} \mathsf{P}[A_i]$, o ile $A_i \cap A_k = \emptyset$ dla $i \neq k$. Ogólniej mamy $\mathsf{P}[A \cup B] = \mathsf{P}[A] + \mathsf{P}[B - A] = \mathsf{P}[A] + \mathsf{P}[B] - \mathsf{P}[A \cap B]$. Ten wzór ma postać najprostszej wersji formuły sita, gdy liczność zbioru zastąpimy prawdopodobieństwem, prawdziwe są wzory będące odpowiednikami ogólnych formuł włączania-wyłączania (ćwiczenie).

Jeżeli $\mathsf{P}[B] > 0$ to *prawdopodobieństwo A pod warunkiem B* określamy jako

$$\mathsf{P}[A \mid B] = \frac{\mathsf{P}[A \cap B]}{\mathsf{P}[B]} \ .$$

Liczbę $\mathsf{P}[A \mid B]$ nazywamy *prawdopodobieństwem warunkowym*. Zachodzi wzór $\mathsf{P}[A \cap B] = \mathsf{P}[A \mid B] \cdot \mathsf{P}[B]$. Stąd

$$\mathsf{P}[A] = \mathsf{P}[A \cap B] + \mathsf{P}[A - B] = \mathsf{P}[A \mid B] \cdot \mathsf{P}[B] + \mathsf{P}[A \mid -B] \cdot \mathsf{P}[-B] \ ,$$

o ile $\mathsf{P}[B] > 0$ i $\mathsf{P}[-B] > 0$, co uogólnia się do *wzoru na całkowite prawdopodobieństwo*:

$$\mathsf{P}[A] = \sum_{i=1}^{n} \mathsf{P}[A \mid B_i] \mathsf{P}[B_i] \ ,$$

prawdziwego o ile zbiory $B_1, \ldots, B_n$ są *podziałem* Ω, to znaczy $\bigcup_{i=1}^{n} B_i = \Omega$, $B_i \cap B_j = \emptyset$, dla $i \neq j$, oraz $\mathsf{P}[B_i] > 0$, dla $1 \leq i \leq n$.

Rodzina zdarzeń $\langle A_i \rangle_{i \in S}$ jest *niezależna* gdy $\mathsf{P}[\bigcap_{i \in T} A_i] = \prod_{i \in T} \mathsf{P}[A_i]$, dla każdego skończonego $T \subseteq S$. W przypadku rodziny dwóch zdarzeń A i B, ich niezależność oznacza $\mathsf{P}[A \cap B] = \mathsf{P}[A] \cdot \mathsf{P}[B]$, lub $\mathsf{P}[A \mid B] = \mathsf{P}[A]$ o ile $\mathsf{P}[B] \neq 0$.

Zmienną losową nazywamy funkcję z Ω w zbiór liczb, powiedzmy rzeczywistych $\mathbb{R}$. Zmienna losowa $X : \Omega \to \mathbb{R}$ określa nową przestrzeń probabilistyczną, w której zdarzeniami elementarnymi są wartości X, a prawdopodobieństwo $\mathsf{P}_X[r]$, dla $r \in \mathbb{R}$ będącej wartością X, ustalamy jako $\sum_{\omega \in X^{-1}(r)} \mathsf{P}[\omega]$. Określona w ten sposób przestrzeń to *rozkład prawdopodobieństwa* X. Dla zmiennej losowej X, zdarzenie $\{\omega \in \Omega : X(\omega) = a\}$ oznaczamy skrótem $X = a$. Niech $\langle X_i \rangle_{i \in S}$ bedzie rodziną zmiennych losowych. Jest ona *niezależna*, gdy zdarzenia $\langle X_i = a_i \rangle_{i \in S}$ są niezależne dla dowolnego ciągu liczb $\langle a_i \rangle_{i \in S}$.

Przykład. Zmienna o *rozkładzie Poissona* ma rozkład opisany wzorem

$$\mathsf{P}[X = k] = \frac{\lambda^k}{k!} e^{-\lambda} \ ,$$

dla $k = 0, 1, 2, \ldots$ oraz $\lambda > 0$. Rzucamy monetą X razy, gdzie X ma rozkład Poissona. Niech Y i Z to uzyskane liczby orłów i reszek, odpowiednio. Pokażemy, że Y i Z są niezależne. Liczba wykonanych rzutów równa n z prawdopodobieństwem $\frac{\lambda^n}{n!} e^{-\lambda}$. Prawdopodobieństwo uzyskania i orłów:

$$\mathsf{P}[Y = i] = \sum_{n=0}^{\infty} \mathsf{P}[i \text{ orłów } \mid n \text{ rzutów }] \cdot \mathsf{P}[n \text{ rzutów }]$$

$$= \sum_{n=0}^{\infty} \binom{n}{i} 2^{-n} \cdot \frac{\lambda^n}{n!} e^{-\lambda} = \sum_{n=i}^{\infty} \frac{2^{-n} \lambda^n}{i!(n-i)!} e^{-\lambda} = \left(\frac{\lambda}{2}\right)^i \frac{e^{-\lambda}}{i!} \sum_{n=0}^{\infty} \frac{(\lambda/2)^n}{n!} = \left(\frac{\lambda}{2}\right)^i \frac{e^{-\lambda/2}}{i!} \ .$$

Podobnie $\mathsf{P}[Z = k]$. Stąd

$$\mathsf{P}[Y = i \text{ oraz } Z = k] = \binom{i+k}{i} \cdot 2^{-i-k} \cdot \frac{\lambda^{i+k}}{(i+k)!} \cdot e^{-\lambda}$$

$$= \left(\frac{\lambda}{2}\right)^i \cdot \frac{e^{-\lambda/2}}{i!} \cdot \left(\frac{\lambda}{2}\right)^k \cdot \frac{e^{-\lambda/2}}{k!} = \mathsf{P}[Y = i] \cdot \mathsf{P}[Z = k] \ .$$

$\Diamond$

Wartość oczekiwana zmiennej losowej X, oznaczana $\mathsf{E}[X]$ lub po prostu $\mathsf{E}X$, to liczba $\sum_{\omega \in \Omega} \mathsf{P}[\omega] \cdot X(w)$. Wymagamy, by suma ta była zbieżna bezwzględnie, a stąd niezależna od kolejności sumowania; gdy ten warunek jest spełniony, to mówimy, że X *ma wartość oczekiwaną*. Operator E jest liniowy, w tym sensie, że $\mathsf{E}[aX] = a\mathsf{E}[X]$ oraz $\mathsf{E}[X + Y] = \mathsf{E}[X] + \mathsf{E}[Y]$, dla $a \in \mathbb{R}$, co wynika od razu z definicji. Zauważmy, że nie potrzeba tu zakładać nic o niezależnosci zmiennych losowych X i Y. Jeżeli natomiast X i Y *są* niezależne, to zachodzi wzór $\mathsf{E}[X \cdot Y] = \mathsf{E}[X] \cdot \mathsf{E}[Y]$. Rzeczywiście:

$$\mathsf{E}X \cdot \mathsf{E}Y = \sum_a a \cdot \mathsf{P}[X = a] \cdot \sum_b b \cdot \mathsf{P}[Y = b] = \sum_{a,b} a \cdot b \cdot \mathsf{P}[X = a] \cdot \mathsf{P}[Y = b]$$

$$= \sum_{a,b} a \cdot b \cdot \mathsf{P}[X = a \text{ oraz } Y = b] = \mathsf{E}[X \cdot Y] \ .$$

Innym często używanym parametrem zmiennej losowej X jest jej *wariancja* oznaczana przez $\mathrm{Var}\,X$, równa $\mathsf{E}\,(X - \mathsf{E}\,X)^2$. Wzór na wariancję można przekształcić następująco:

$$\mathrm{Var}\,X = \mathsf{E}\,[X^2 - 2X \cdot \mathsf{E}\,X + (\mathsf{E}\,X)^2] = \mathsf{E}\,X^2 - 2(\mathsf{E}\,X)^2 + (\mathsf{E}\,X)^2 = \mathsf{E}\,[X^2] - (\mathsf{E}\,X)^2 \ .$$

Jeżeli X i Y są niezależne to $\mathrm{Var}\,(X+Y) = \mathrm{Var}\,X + \mathrm{Var}\,Y$. Rzeczywiście:

$$\mathsf{E}\,(X+Y)^2 - (\mathsf{E}\,[X+Y])^2 = \mathsf{E}\,X^2 + \mathsf{E}\,Y^2 + 2\mathsf{E}\,[X \cdot Y] - (\mathsf{E}\,X)^2 - (\mathsf{E}\,Y)^2 - 2\mathsf{E}\,X \cdot \mathsf{E}\,Y \ ,$$

i wystarczy skorzystać z równości $\mathsf{E}\,[X \cdot Y] = \mathsf{E}\,X \cdot \mathsf{E}\,Y$.

Przykład: Powiemy, że zmienna Y ma *rozkład Bernoulli'ego*, gdy $\mathsf{P}[Y=1] = p$ i $\mathsf{P}[Y = 0] = 1 - p$. Zdarzenie $Y = 1$ nazywamy *sukcesem w próbie Bernoulli'ego*. Jeżeli Y jest zmienną o rozkładzie Bernoulli'ego z prawdopodobieństwem sukcesu równym p, to $\mathsf{E}\,Y = p$, $\mathrm{Var}\,Y = p(1-p)$. Zmienna o *rozkładzie dwumianowym* jest postaci $X = \sum_{i=1}^{n} X_i$, gdzie X_i niezależne zmienne o tym samym rozkładzie Bernoulliego. Ta zmienna odpowiada fizycznemu przeprowadzeniu niezależnego ciągu n prób, każda z rozkładem Bernoulliego, co określamy krótko jako *ciąg prób Bernoulli'ego*, i obliczeniu liczby sukcesów. Dokładniej, prawdopodobieństwo k sukcesów w n próbach Bernoulli'ego jest równe:

$$\mathsf{P}[X = k] = \binom{n}{k} p^k (1-p)^{n-k} \ .$$

Piszemy krócej, że X jest zmienną $\mathrm{B}(n,p)$, a $\mathsf{P}[X=k]$ oznaczamy jako $\mathrm{b}(k;n,p)$. Zmienna o rozkładzie dwumianowym jest określona jako suma niezależnych zmiennych, których wartość oczekiwaną i wariancję znamy, stąd dostajemy $\mathsf{E}\,X = np$ i $\mathrm{Var}\,X = np(1-p)$. $\Diamond$

Niech X zmienna losowa o wartościach całkowitych nieujemnych. Pokażemy, że

$$\mathsf{E}\,X = \sum_{k=0}^{\infty} \mathsf{P}[X > k] \ .$$

Wyprowadzenie polega na zmianie kolejności sumowania:

$$\mathsf{E}\,X = \sum_{i=1}^{\infty} i \cdot \mathsf{P}[X=i] = \sum_{i=1}^{\infty} \sum_{k=1}^{i} \mathsf{P}[X=i] = \sum_{k=1}^{\infty} \sum_{i=k}^{\infty} \mathsf{P}[X=i] = \sum_{k=1}^{\infty} \mathsf{P}[X \geq k] \ .$$

Metoda probabilistyczna dowodzi istnienia obiektu kombinatorycznego z odpowiednią własnością poprzez pokazanie, że losowy obiekt ma tę własność z prawdopodobieństwem większym od zera. Podamy klasyczny przykład, w którym oszacujemy od dołu liczby Ramseya. Kolorujemy krawędzie kliki K_n dwoma kolorami, na przykład czerwonym i zielonym. Interesują nas podzbiory wierzchołków K_n takie, że indukowane kliki mają krawędzie tego samego koloru. Przypomnijmy, że dla każdej pary liczb całkowitych $i, j > 0$ istnieje liczba Ramseya $R(i,j)$ taka, że jeżeli $n \geq R(i,j)$ oraz K_n jest pokolorowana jak wyżej, to K_n zawiera albo indukowaną klikę K_i czerwoną lub indukowaną klikę K_j zieloną. Oto jak Erdös oszacował $R(k,k)$. Niech zdarzeniami elementarnymi będą wszystkie możliwe kolorowania K_n, z jednakowym prawdopodobieństwem. Inaczej:

kolorujemy każdą krawędź K_n na zielono lub czerwono z prawdopodobieństwem $1/2$, niezależnie dla różnych krawędzi. Niech zbiór wierzchołków $W \subseteq [1..n]$ ma k elementów. Zdarzenie Z_W, że graf indukowany przez W ma krawędzie jednego koloru, ma prawdopodobieństwo $2/2^{\binom{k}{2}}$. Rozważmy zdarzenie $\bigcup_W Z_W$ po wszystkich $|W| = k$. Szacujemy:

$$\mathsf{P}[\bigcup_W Z_W] \leq \sum_W \mathsf{P}[Z_W] = \binom{n}{k} 2^{1-\binom{k}{2}} .$$

Stąd mamy wynikanie:

$$\text{Jeżeli } \binom{n}{k} 2^{1-\binom{k}{2}} < 1 \text{ to } R(k,k) > n, \tag{1}$$

bowiem z prawdopodobieństwem większym od zera istnieje kolorowanie, które nie zawiera jednokolorowej kliki rozmiaru k. Z nierówności $\binom{n}{k} \leq \left(\frac{ne}{k}\right)^k$ dostajemy $2\left(\frac{ne}{k}\right)^k < 2^{k(k-1)/2}$, a stąd $n < \frac{k2^{k/2}}{e\sqrt{2}}$. Razem:

$$R(k,k) \geq \frac{k2^{k/2}}{e\sqrt{2}} .$$

Pokażemy oszacowanie lepsze o czynnik 2, które korzysta z następującego *lematu lokalnego*: Niech $A_1, \ldots, A_n$ zdarzenia takie, że każde jest niezależne od pozostałych, za wyjątkiem być może nie więcej niż d zdarzeń; wtedy zachodzi $\mathsf{P}[\bigcup_{i=1}^n A_i] < 1$, o ile $\mathsf{P}[A_i] \leq p$ oraz $e \cdot p \cdot (d+1) \leq 1$, gdzie e to podstawa logarytmów naturalnych.

Oto dowód lematu lokalnego: Pokażemy

$$\mathsf{P}[\bigcap_{i=1}^n \overline{A}_i] = \mathsf{P}[\overline{A}_1] \cdot \mathsf{P}[\overline{A}_2 \mid \overline{A}_1] \cdot \mathsf{P}[\overline{A}_3 \mid \overline{A}_1 \cap \overline{A}_2] \cdot \ldots \geq \prod_{i=1}^n \frac{d}{d+1} > 0 .$$

Dla prawdziwości tego wystarczy nierówność $\mathsf{P}[A_i \mid \bigcap_{j=1}^{i-1} \overline{A}_j] \leq \frac{1}{d+1}$. Pokażemy ogólniej:

$$\mathsf{P}[A_i \mid \bigcap_{j \in K} \overline{A}_j] \leq \frac{1}{d+1} ,$$

dla $K \subseteq [1..n]$ oraz $i \notin K$. Dowód przez indukcję po rozmiarze K. Dla $K = \emptyset$ zachodzi. Weźmy $K \neq \emptyset$. Niech $K_0 = \{k \in K : A_i \text{ niezależny od } A_k\}$ oraz $K_1 = K - K_0$. Mamy

$$\mathsf{P}[A_i \mid \bigcap_{j \in K} \overline{A}_j] = \frac{\mathsf{P}[A_i \cap \bigcap_{j \in K} \overline{A}_j]}{\mathsf{P}[\bigcap_{j \in K} \overline{A}_j]} = \frac{\mathsf{P}[A_i \cap \bigcap_{j \in K} \overline{A}_j]}{\mathsf{P}[\bigcap_{j \in K_0} \overline{A}_j]} \cdot \frac{\mathsf{P}[\bigcap_{j \in K_0} \overline{A}_j]}{\mathsf{P}[\bigcap_{j \in K_0} \overline{A}_j \cap \bigcap_{j \in K_1} \overline{A}_j]}$$
$$= \frac{\mathsf{P}[A_i \cap \bigcap_{j \in K} \overline{A}_j \mid \bigcap_{j \in K_0} \overline{A}_j]}{\mathsf{P}[\bigcap_{j \in K_1} \overline{A}_j \mid \bigcap_{j \in K_0} \overline{A}_j]} = \frac{L}{M} .$$

Szacujemy licznik i mianownik:

$$L \leq \mathsf{P}[A_i \mid \bigcap_{j \in K_0} \overline{A}_j] = \mathsf{P}[A_i] \leq \frac{1}{e(d+1)} ,$$

z niezależności A_i od A_j, dla $j \in K_0$. Niech $K_1 = \{A_{j_1}, \ldots, A_{j_s}\}$.

$$M = \mathsf{P}[\bigcap_{l=1}^{s} \overline{A}_{j_l} \mid \bigcap_{j \in K_0} \overline{A}_j] = \prod_{l=1}^{s} \mathsf{P}[\overline{A}_{j_l} \mid \overline{A}_{j_1} \cap \ldots \cap \overline{A}_{j_{l-1}} \cap \bigcap_{j \in K_0} \overline{A}_j]$$
$$\geq \prod_{l=1}^{s} \frac{d}{d+1} \geq \left(1 - \frac{1}{d+1}\right)^d > \frac{1}{e} ,$$

dla $d > 2$, gdzie skorzystaliśmy z założenia indukcyjnego. Razem $L/M \leq 1/(d+1)$. $\square$

Wróćmy do liczb Ramseya. Rozważmy zdarzenia Z_W, gdzie $|W| = k$. Takie dwa zdarzenia Z_{W_1} i Z_{W_2} nie są niezależne o ile $|W_1 \cap W_2| \geq 2$. Stąd d można oszacować przez $\binom{n}{k-2}\binom{k}{2}$, co prowadzi do wynikania:

$$\text{Jeżeli} \quad e\left(\binom{n}{k-2}\binom{k}{2} + 1\right) 2^{1-\binom{k}{2}} < 1 \quad \text{to} \quad R(k,k) > n.$$

Szacując n względem k w poprzedniej implikacji dostajemy następującą nierówność:

$$R(k,k) > \frac{\sqrt{2}}{e} \cdot k \cdot 2^{k/2} .$$

Derandomizacja. Dla danego grafu $G = \langle V, E\rangle$, podzielmy V na dwie części $V = V_0 \cup V_1$, $V_0 \cap V_1 = \emptyset$, i rozważmy zbiór krawędzi $E_0 \subseteq E$, które mają końce w V_0 i V_1. Graf $G_0 = \langle V, E_0\rangle$ jest dwudzielny. Pokażemy, że dla każdego G istnieje taki podział V na części, że $|E_0| \geq \frac{1}{2}|E|$. Rozważmy losowy podział $V = V_0 \cup V_1$, to znaczy dla każdego $v \in V$ z prawdopodobieństwem $1/2$ przydzielmy go do V_0. Rozważmy zmienną losową X_e, dla krawędzi e:

$$X_e = \begin{cases} 0 & \text{jeżeli } e \notin E_0 , \\ 1 & \text{jeżeli } e \in E_0 . \end{cases}$$

Niech $X = \sum_{e \in E} X_e$. Wtedy $\mathsf{E}\, X = \sum_{e \in E} \mathsf{E}\, X_e = \sum_{e \in E} \frac{1}{2} = \frac{1}{2}|E|$. Stąd istnieje takie zdarzenie elementarne, czyli podział $V = V_0 \cup V_1$, dla którego $X \geq \frac{1}{2}|E|$.

Pokażemy jak deterministycznie znaleźć taki podział *metodą warunkowych prawdopodobieństw*. Dla każdego wierzchołka v mamy rozstrzygnąć, gdzie go przydzielić. Uporządkujmy dowolnie $V = \{v_1, \ldots, v_n\}$. Zaczynamy od włożenia v_1 do V_0. Załóżmy, że $v_1, \ldots, v_k$ są już przydzielone. Niech A_k oznacza ten przydział. Rozważmy losowe przydziały pozostałych wierzchołków. Skorzystamy z wzoru

$$\mathsf{E}\,[E_0 \mid A_k] = \frac{1}{2} \cdot \mathsf{E}\,[E_0 \mid A_k \text{ oraz } v_{k+1} \in V_0] + \frac{1}{2} \cdot \mathsf{E}\,[E_0 \mid A_k \text{ oraz } v_{k+1} \in V_1] .$$

Jeżeli wybierzemy maksymalny składnik, a w następnych krokach postąpimy podobnie, to dostaniemy dobry podział. Trzeba tylko obliczyć odpowiednie prawdopodobieństwa warunkowe. Rozważmy pierwszy składnik: $v_1, \ldots, v_k$ już ustalone, dodajmy v_{k+1} do V_0. Każda krawędź e incydentna z v_{k+1} ma koniec v_j; jeżeli $j < k$ to wiadomo, czy należy do E_0, w przeciwnym przypadku daje $1/2$ do wartości oczekiwanej. Otrzymujemy taką regułę: jeżeli v_{k+1} ma więcej sąsiadów w V_0 niż w V_1 to wstaw v_{k+1} do V_1, w przeciwnym przypadku do V_0. Dostajemy prosty deterministyczny algorytm, który można zaimplementować tak, że jego czas działania jest $\mathcal{O}(n+m)$, gdzie m to liczba krawędzi.

Zadania

1. Pokaż odpowiedniki formuł włączania-wyłączania dla zbiorów zdarzeń, zastępując liczbę elementów w zbiorze jego prawdopodobieństwem.

2. Niech B zdarzenie takie, że $\mathsf{P}[B] > 0$, rodzina zbiorów $A_1, \ldots, A_n$ jest podziałem Ω, i $\mathsf{P}[A_k] > 0$ dla $1 \leq k \leq n$. Pokaż następujący *wzór Bayesa:*

$$\mathsf{P}[A_i \mid B] = \frac{\mathsf{P}[B \mid A_i] \cdot \mathsf{P}[A_i]}{\sum_{k=1}^{n} \mathsf{P}[B \mid A_k] \cdot \mathsf{P}[A_k]} \ .$$

3. Urna A zawiera 2 kule białe i 3 kule czarne, a urna B zawiera 3 kule białe i 4 kule czarne. Wybieramy losowo jedną kule z A i jedną kule z B, po czym zamieniamy miejscami. Następnie wybieramy losowo kule z urny A. Jakie jest prawdopodobienstwo, że wybierzemy kulę białą?

4. Urna A zawiera 1 kulę białą i 1 kulę czarną, a urna B zawiera 2 kule białe i 3 kule czarne. Wybieramy losowo urnę po czym losujemy z niej n razy kulę ze zwracaniem, za każdym razem wyciągając kulę czarną. Jakie jest prawdopodobieństwo, że wybraliśmy urnę A?

5. Podaj przykład zmiennej losowej $X \geq 0$ takiej, że $\mathsf{E}\, X < \infty$ oraz $\operatorname{Var} X = \infty$.

6. Niech ξ zmienna losowa o wartościach całkowitych nieujemnych, X_0, X_1, $X_2, \ldots$, ciąg zmiennych losowych o wartościach nieujemnych. Pokaż rowność:
$\mathsf{E}\, X_\xi = \sum_{i \geq 0} \mathsf{P}[\xi = i] \cdot \mathsf{E}\, X_i$, o ile istnieją wszystkie wartości oczekiwane.

7. Pokaż, że jeżeli zdarzenia A i B są niezależne, to zdarzenia $-A$ i $-B$ też są niezależne.

8. Niech X i Y to niezależne zmienne losowe, oraz $f, g : \mathbb{R} \to \mathbb{R}$. Pokaż że $f(X)$ i $g(Y)$ są niezależne.

9. Niech $A_1, \ldots, A_n$ rodzina zdarzeń niezależnych. Pokaż, że, jeżeli $\mathsf{P}[A_i] < 1$ dla każdego i, to także $\mathsf{P}[\bigcup_{1 \leq i \leq n} A_i] < 1$.

10. Oblicz wartość oczekiwaną i wariancję liczby inwersji w losowej n-permutacji.

11. Niech X_n bedzie ciągiem zmiennych $\mathrm{B}(n, p_n)$ takim, że $\mathsf{E}[X_n] = n \cdot p_n$ zbiega do $\lambda > 0$ przy $n \to \infty$. Pokaż, że wtedy $\mathrm{b}(k; n, p)$ zbiega do $\frac{\lambda^k}{k!} e^{-\lambda}$ przy $n \to \infty$.

12. Pokaż, że jeżeli t jest maksymalną liczbą całkowitą n taką, że $\binom{n}{k} < 2^{\binom{k}{2}-1}$ to wtedy $t = \frac{k 2^{k/2}}{e\sqrt{2}}(1 + o(1))$.
Wskazówka: Wzór Stirlinga.

13. Pokaż, że jeżeli t jest maksymalną liczbą całkowitą n taką, że $\binom{k}{2}\binom{n}{k-2} < 2^{\binom{k}{2}-1}$ to wtedy $t = \frac{\sqrt{2}}{e} \cdot k \cdot 2^{k/2} \cdot (1 + o(1))$.

14. Rodzina S podzbiorów zbioru X *jest 2-kolorowalna* jeżeli istnieje kolorowanie X dwoma kolorami takie, że każdy podzbiór X ma elementy różnych kolorów. Pokaż, że każda rodzina n-zbiorów, która ma mniej niż 2^{n-1} elementów jest 2-kolorowalna.
Wskazówka: Pokoloruj elementy X losowo.

15. Pokaż, że istnieje turniej o n wierzchołkach, który zawiera $n!/2^{n-1}$ ścieżek Hamiltona.
Wskazówka: Rozważ klikę K_n z losową orientacją krawędzi.

16. Szukamy rozcięcia o minimalnej liczności w grafie $\langle V, E\rangle$. Rozważmy następujący algorytm. Porządkujemy wszystkie krawędzie w E losowo. Zaczynamy od V i pustego zbioru krawędzi, po czym dodajemy elementy E kolejno aż otrzymany graf będzie miał dokładnie dwie spójne składowe. Krawędzie w E łączące wierzchołki z tych składowych są pseudorozcięciem. Pokaż ile razy (wielomianową liczbę) trzeba to powtórzyć, aby prawdopodobieństwo tego, że natrafimy na minimalne rozcięcie było $1 - \mathcal{O}(c^{-n})$, dla stałej $c > 1$.

17. Pokaż jak znaleźć deterministycznie turniej o n wierzchołkach mający co najmniej $n^{\underline{5}} \cdot 2^{-5}$ cykli długości 5 metodą prawdopodobieństw warunkowych. Oszacuj czas pracy algorytmu.

MMD Wykład 6.

Bogdan Chlebus

Entropia. Niech A będzie skończonym zbiorem nazywanym *alfabetem*, jego elementy nazywamy *symbolami*. Ciągi $x = x_1 \dots x_k$, gdzie $x_i \in A$, nazywamy *słowami nad* A. Słowo x jest długości k, co oznaczamy przez $|x| = k$. Zbiór słów długości k nad A oznaczamy przez A^k, a wszystkich słów przez A^*. Słowo $x \in A^*$ można zakodować posługując się innym alfabetem B, gdy każdy symbol $a \in A$ zastąpimy jego kodem $c(a) \in B^*$, a całe słowo x kodujemy przez $c(x) = c(x_1) \dots c(x_n)$. *Kodem* nazwiemy $C = \{c(a) : a \in A\}$, jego elementy to *słowa kodowe*. Dobry kod powinien być *dekodowalny*, to znaczy słowo postaci $c(x_1) \dots c(x_k)$ powinno jednoznacznie wyznaczać $x_1 \dots x_k$.

Przykład: Niech $A = \{a_1, a_2, a_3\}$, $B = \{0, 1\}$. Określmy kod $c(a_1) = 010$, $c(a_2) = 100$, $c(a_3) = 0$. Ciąg 0100 może kodować a_1a_3 lub a_3a_2, zatem kod nie jest dekodowalny. $\Diamond$

Odtąd określenie 'kod' oznacza 'kod dekodowalny'. Kod jest wygodny do odkodowywania, gdy mając $c(x)$ i czytając kolejno jego pierwsze symbole możemy stwierdzić, że pierwszym symbolem x jest x_1 jak tylko przeczytamy ostatni symbol słowa $c(x_1)$. Takie kody nazywamy prefiksowymi. Formalnie, kod C jest *prefiksowy* gdy żadne słowo w $c_1 \in C$ nie jest przedrostkiem (prefiksem) innego $c_2 \in C$, to znaczy nie istnieje niepuste słowo c_3 takie, że $c_2 = c_1c_3$.

Innym kryterium efektywności kodu jest długość słów $c(x)$ w zależności od x. Przypuśćmy, że źródło wysyła kolejno sygnały, są nimi elementy zbioru $A = \{s_1, \dots, s_n\}$, sygnały mogą się powtarzać, odbieramy je bez zakłóceń. Niech $p = \langle p_1, \dots, p_n \rangle$ to rozkład prawdopodobieństwa na zbiorze sygnałów, to znaczy sygnał s_i wysyłany z prawdopodobieństwem p_i w danym kroku. Sygnały nadchodzą w postaci zakodowanej, jako strumień symboli z pewnego alfabetu B, który interpretujemy jako ciąg słów kodowych kodu $C = \{c_1, \dots, c_n\}$, gdzie sygnal s_i nadawany jako $c_i = c(s_i)$. *Średnia długość kodu* C określamy jako liczbę $\mathrm{L}(C) = \sum_{1 \le i \le n} p_i \cdot |c_i|$. Jeżeli otrzymamy m sygnałów to oczekiwana liczba symboli z B użyta w transmisji jest równa $m \cdot \mathrm{L}(C)$. Podobne zjawisko występuje przy kompresji. Niech $x \in \{0, 1\}^{n \cdot k}$. Podzielmy x na n rozłącznych bloków długości k. Niech dla każdego $a \in A = \{0, 1\}^k$ liczba r_a oznacza liczbę wystąpień a jako bloku w x. Niech C kod otrzymany przez zastąpienie każdego takiego a odpowiadającym mu słowem $c(a) \in \{0, 1\}^*$. Po zakodowaniu x dostajemy $c(x)$ o długości $|c(x)| = \sum_{a \in A} r_a \cdot |c_a|$. Przechodząc do liczb postaci r_a/n jako prawdopodobieństw występowania bloków a w x, mamy, że $|c(x)| = n \cdot \mathrm{L}(C)$. Jeżeli $\mathrm{L}(C) < k$ to słowo $c(x)$ jest skompresowanym zapisem słowa x. Może tak się zdarzyć, jeżeli jest duże zróżnicowanie częstości występowania bloków, i gdy często występujące bloki otrzymają krótsze kody niż te, które występują rzadziej. Jeżeli średnia długość kodu C jest dana wzorem $\mathrm{L}(C) = \sum_{1 \le i \le n} p_i \cdot |c_i|$, to mówimy, że C *jest kodem dla rozkładu prawdopodobieństwa* $\langle p_i \rangle$.

Ciąg sygnałów lub słowo składające się z ciągu symboli mogą nieść jakąś informację. Termin "informacja" używamy tu w znaczeniu "abstrakcyjna miara informacji" a nie jako interpretacja wiadomości zakodowanych w ciągach symboli. Odebranie sygnału lub przeczytanie kolejnego słowa kodowego traktujemy jak zdarzenie o jakimś prawdopodobieństwie. Wydaje się, że miara takiej informacji nie zależy od różnicy pomiędzy otrzy-

mywaniem sygnałów a czytaniem symboli a tylko od prawdopodobieństw ich pojawiania się. Na przykład, jeżeli mamy 2^n zdarzeń elementarnych, każde z prawdopodobieństwem 2^{-n}, to zajście każdego zdarzenia elementarnego niesie informację n, gdyż do rozróżnienia pomiędzy 2^n możliwościami potrzebujemy n bitów zapisu binarnego. Zatem naturalne jest przyjęcie definicji, że *zajście zdarzenia A niesie informację równą* $\lg \frac{1}{\mathsf{P}[A]} = -\lg \mathsf{P}[A]$.

Średnią liczbę bitów potrzebną do zakodowania wartości zmiennej losowej X nazywamy *entropią* X, i oznaczamy $\mathrm{H}(X)$. Jeżeli $\langle p_1, p_2, \ldots \rangle$ jest rozkładem prawdopodobieństwa X to $\mathrm{H}(X) = -\sum_i p_i \cdot \lg p_i$. Ma miejsce $\mathrm{H}(X) \geq 0$ bowiem $\lg p_i \leq 0$. Intuicyjnie $\mathrm{H}(X)$ to miara niepewności o wartość X, lub inaczej średnia ilość informacji jaką dostajemy poznając wartość X.

Niech X określona na przestrzeni probabilistycznej ze zdarzeniami elementarnymi Ω i prawdopodobieństwem P. Niech W_X to zbiór wartości X. Rozkład prawdopodobieństwa X to przestrzeń probabilistyczna o zdarzeniach elementarnych W_X i prawdopodobieństwie $\mathsf{P}_X[r] = \mathsf{P}[X = r]$. Zmiennej X można przyporządkować zmienną losową $p_X(r)$ określoną na zbiorze zdarzeń elementarnych W_X wzorem $p_X(r) = \mathsf{P}_X[r]$. Podobnie X można przyporządkować zmienną losową $p(X)$ określoną na zbiorze zdarzeń elementarnych Ω i określoną wzorem $p(X)(\omega) = \mathsf{P}[X = X(\omega)]$. Entropię $\mathrm{H}(X)$ można wyrazić jako wartość oczekiwaną:

$$\mathrm{H}(X) = \sum_{\omega \in \Omega} \mathsf{P}[\omega] \cdot \lg \frac{1}{\mathsf{P}[X = X(\omega)]} = -\sum_{\omega \in \Omega} \mathsf{P}_X[\omega] \cdot \lg p(X)(\omega) = -\mathsf{E}\ \lg p(X)\ .$$

Podobnie $\mathrm{H}(X) = \sum_{r \in W_X} \mathsf{P}_X[r] \cdot \lg \frac{1}{p_X(r)} = -\mathsf{E}\ \lg p_X$.

Przykład: Niech X przyjmuje wartości a i b, każdą z prawdopodobieństwem $1/2$. Wtedy $\mathrm{H}(X) = \frac{1}{2} \cdot \lg 2 + \frac{1}{2} \cdot \lg 2 = 1$. Jest to zgodne z intuicją: bity 0 i 1 kodują a i b, odpowiednio. Niech Y przyjmuje wartości a i b, każdą z prawdopodobieństwem $1/4$ i $3/4$, odpowiednio. Wtedy $\mathrm{H}(Y) = \frac{1}{4} \cdot \lg 4 + \frac{3}{4} \lg \cdot \frac{4}{3} \approx 0.82 < 1$. To jest niepokojące: jak można zakodować jedną z dwóch wartości Y za pomocą mniej niż jednego bitu? Odpowiedź na ten paradoks leży w określeniu "średnia liczba bitów." Jeżeli kodujemy *ciągi* wartości zmiennych $Y_1, Y_2, \ldots$, niezależnych od siebie i o rozkładzie takim jak Y, to oczekujemy, że m wartości uda się skompresować do rozmiaru bliskiego $\mathrm{H}(Y) \cdot m$, dla dostatecznie dużych m. $\Diamond$

Jeżeli X ma rozkład Bernoulli'ego z prawdopodobieństwem sukcesu p to $\mathrm{H}(X)$ oznaczamy przez $\mathrm{H}(p)$, gdzie funkcję

$$\mathrm{H}(p) = -p \cdot \lg p - (1-p) \cdot \lg(1-p)$$

nazywamy *funkcją entropii*. Jest ona określona na przedziale $[0, 1]$, jest wypukła, ma wartości $\mathrm{H}(0) = \mathrm{H}(1) = 0$, oraz przyjmuje maksimum $\mathrm{H}(\frac{1}{2}) = 1$. Funkcja entropii pojawia się naturalnie w szacowaniu sumy kolejnych współczynników dwumianowych. Niech $0 \leq a \leq \frac{1}{2}$ oraz n liczba naturalna. Wtedy

$$1 = (a + (1-a))^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot (1-a)^{n-k} \geq \sum_{0 \leq k \leq an} \binom{n}{k} (1-a)^n \cdot \left(\frac{a}{1-a}\right)^k$$

$$\geq \sum_{0\leq k\leq an} \binom{n}{k}(1-a)^n\Big(\frac{a}{1-a}\Big)^{an} = \big[(1-a)^{1-a}a^a\big]^n \sum_{0\leq k\leq an}\binom{n}{k} \geq 2^{-n\mathrm{H}(a)} \sum_{0\leq k\leq an}\binom{n}{k} .$$

(W którym miejscu skorzystaliśmy z $a \leq 1/2$?) Stąd dostajemy, że dla $0 \leq a \leq \frac{1}{2}$ zachodzi

$$\sum_{0\leq k\leq an}\binom{n}{k} \leq 2^{\mathrm{H}(a)\cdot n} .$$

Niech $X_1, \ldots X_n$ ciąg niezależnych zmiennych losowych, każda o rozkładzie Bernoulliego z prawdopodobieństwem sukcesu p. Niech $r = \langle r_1 \ldots r_n\rangle \in \{0,1\}^n$. Oznaczmy $\mathsf{P}[r] = \mathsf{P}[X_1 = r_1, \ldots, X_n = r_n]$. Powiemy, że r jest *ϵ-typowy* gdy zachodzą nierówności

$$2^{-n(\mathrm{H}(p)+\epsilon)} \leq \mathsf{P}[r] \leq 2^{-n(\mathrm{H}(p)-\epsilon)} .$$

Pokażemy, że $\mathsf{P}[r \text{ jest } \epsilon\text{-typowy}] > 1-\epsilon$. Ciąg r jest ϵ-typowy w.t.w. gdy

$$\mathrm{H}(p) - \epsilon \leq -\frac{1}{n}\cdot \lg \mathsf{P}[r] \leq \mathrm{H}(p) + \epsilon .$$

Skorzystamy ze słabego prawa wielkich liczb (pokażemy je później), które mówi, że jeżeli $Y_1, \ldots, Y_n \ldots$ ciąg niezależnych zmiennych losowych, każda o takiej samej wartości oczekiwanej μ i wariancji, to ciąg $\mathsf{P}[|\frac{1}{n}\sum_{i=1}^n Y_i - \mu| < \delta]$ zbiega do 1 wraz z $n \to \infty$, dla dowolnego ustalonego $\delta > 0$. Połóżmy $\lg p(X_i)$ za Y_i. Są to niezależne zmienne losowe bowiem X_i są niezależne. Ze słabego prawa wielkich liczb mamy

$$\mathsf{P}\big[\big|-\frac{1}{n}\sum_{i=1}^n \lg p(X_i) - \mathrm{H}(p)\big| < \epsilon\big] > 1-\epsilon ,$$

dla dostatecznie dużych n. Zauważmy, że oszacowaliśmy prawdopodobieństwo, że ciąg wartości $\langle X_1 = r_1, \ldots, X_n = r_n\rangle$ jest ciągiem typowym, bowiem zachodzą równości $\lg \mathsf{P}[r] = \lg \prod_{1\leq i\leq n} \mathsf{P}[X_i = r_i] = \sum_{1\leq i\leq n} \lg p_{X_i}(r_i)$ oraz $p(X)(\omega) = p_X(a)$ o ile $X(\omega) = a$. To kończy dowód szacowania $\mathsf{P}[r \text{ jest } \epsilon\text{-typowy}] > 1-\epsilon$.

Pokażemy teraz jak efektywnie kodować ciągi wartości n prób Bernoulliego. Podzielmy ciągi $r \in \{0,1\}^n$ na ϵ-typowe A i pozostałe B. Ustawmy elementy A i B w dwie listy. Kod $c(r)$ ciągu r zaczyna się od 0 lub 1 w zależności od tego czy r należy do A czy B. Potem następuje numer pozycji r na odpowiedniej liście zapisany binarnie, przy czym wszystkie elementy A mają numery takiej samej długości, podobnie z B, dopisujemy na początku zera w razie potrzeby. Jeżeli $r \in A$ to $|c(r)| \leq 2 + \lg|A|$. Oszacujemy liczność A. Mamy

$$1 = \sum_{r\in\{0,1\}^*} \mathsf{P}[r] \geq \sum_{r\in A} \mathsf{P}[r] \geq \sum_{r\in A} 2^{-n(\mathrm{H}(p)+\epsilon)} = |A|\cdot 2^{-n(\mathrm{H}(p)+\epsilon)} .$$

Zatem $|c(r)| \leq 2 + n(\mathrm{H}(p)+\epsilon)$ dla $r \in A$. Natomiast $|c(r)| \leq 1+n$ dla $r \in B$. Niech n tak duże, że $\mathsf{P}[B] < \epsilon$. Oszacujemy średnią długość otrzymanego kodu C:

$$\mathrm{L}(C) = \sum_{r\in A} \mathsf{P}[r]\cdot|c(r)| + \sum_{r\in B}\mathsf{P}[r]\cdot|c(r)| \leq \sum_{r\in A}\mathsf{P}[r]\cdot(2+n(\mathrm{H}(p)+\epsilon)) + \sum_{r\in B}\mathsf{P}[r]\cdot(1+n)$$
$$\leq \mathsf{P}[A]\cdot(2+n(\mathrm{H}(p)+\epsilon)) + \mathsf{P}[B]\cdot(1+n) \leq n(\mathrm{H}(p)+\epsilon+3/n) \leq n(\mathrm{H}(p)+2\epsilon) ,$$

dla $3/n < \epsilon$. Zatem dostatecznie długi ciąg wyników prób Bernoulliego z prawdopodobieństwem sukcesu p można skompresować średnio o czynnik dowolnie bliski $\mathrm{H}(p)$.

Pokażemy teraz, że takiej kompresji nie można polepszyć, dla kodów prefiksowych. Zaczniemy od technicznych przygotowań. Niech ciągi $\langle a_1, \ldots, a_n\rangle$ i $\langle b_1, \ldots, b_n\rangle$ określają rozkłady prawdopodobieństwa, to znaczy $0 \le a_i, b_i \le 1$ oraz $\sum_i a_i = \sum_i b_i = 1$. Korzystając z nierówności $\ln x \le x - 1$ mamy

$$\sum_i a_i \lg \frac{b_i}{a_i} = \frac{1}{\ln 2} \sum_i a_i \ln \frac{b_i}{a_i} \le \frac{1}{\ln 2} \sum_i a_i \Big(\frac{b_i}{a_i} - 1\Big) = \frac{1}{\ln 2} \big(\sum_i b_i - \sum_i a_i\big) = 0 \ .$$

Stąd dostajemy nierówność

$$\sum_{i=1}^{n} a_i \lg \frac{1}{a_i} \le \sum_{i=1}^{n} a_i \lg \frac{1}{b_i} \ . \tag{1}$$

Potrzebujemy także pewnej własności kodów prefiksowych znanej jako nierówność Krafta. Niech C kod prefiksowy nad alfabetem $\{0,1\}$. Niech $d_{\max} = \max_{c\in C} |c|$. Dla $c \in C$, niech P_c będzie zbiorem tych słów z $\{0,1\}^{d_{\max}}$ że c jest ich przedrostkiem. Mamy $|P_c| = 2^{d_{\max}-|c|}$. Zbiory P_c są rozłączne bowiem C prefiksowy. Stąd $\sum_{c\in C} 2^{d_{\max}-|c|} \le 2^{d_{\max}}$, czyli

$$\sum_{c\in C} 2^{-|c|} \le 1 \ ,$$

jest to własnie *nierówność Krafta*.

Używając nazwy nierówność Krafta trzeba pamiętać że tak na prawdę jest to równoważność, w tym sensie, że prawdziwe jest odwrotne wynikanie: niech $d_1, \ldots, d_k$ liczby naturalne takie, że zachodzi nierówność $\sum_{i=1}^{k} 2^{-d_i} \le 1$, wtedy istnieje kod prefiksowy $C = \{c_1, \ldots, c_k\}$ taki, że $|c_i| = d_i$. W celu jego pokazania, ustawmy elementy $\{0,1\}^d$ w listę, gdzie $d = \max_{1\le i\le k}\{d_i\}$. Niech c_1 będzie przedrostkiem długości d_1 pierwszego słowa na liście. Usuńmy wszystkie słowa, których c_1 jest przedrostkiem z listy. Niech c_2 przedrostek długości d_2 pierwszego słowa na pozostałej liście. Usuńmy słowa, których jest przedrostkiem z listy, i tak dalej. Łącznie usuniemy $\sum_{i=1}^{k} 2^{d-d_i} \le 2^d$ słów, czyli konstrukcja nie zatrzyma się przez wyczerpanie listy dla $i < k$.

Niech $\langle p_1, \ldots, p_n\rangle$ rozkład prawdopodobieństwa zmiennej X. Niech wartości X kodowane przez kod prefiksowy $C = \{c_1, \ldots, c_n\}$, wtedy $\mathrm{L}(C) = \sum_{i=1}^{n} p_i|c_i|$. Połóżmy $a_i = p_i$ oraz $b_i = 2^{-|c_i|} / \sum_{i=1}^{n} 2^{-|c_i|}$ w nierówności 1. Korzystając dodatkowo z nierówności Krafta dostajemy

$$\mathrm{H}(X) \le \sum_{i=1}^{n} p_i \lg(\sum_{i=1}^{n} 2^{-|c_i|}) - \sum_{i=1}^{n} p_i \lg 2^{-|c_i|} \le \sum_{i=1}^{n} p_i \lg 1 + \sum_{i=1}^{n} p_i|c_i| = \mathrm{L}(C) \ .$$

W powyższych rozważaniach założenie o tym że kod prefiksowy można opuścić (patrz zadanie 6). Fakt, że ciąg wartości niezależnych zmiennych losowych $X_1, X_2, \ldots$ o takim samym rozkładzie jak X można kodować ze średnią liczbą bitów $\mathrm{H}(X)$ na wartość i że jest to optymalne nazywa się *pierwszym twierdzeniem Shannona* lub *twierdzeniem o kodowaniu dla kanałów bez szumu.*

Pokażemy teraz jak znajdować dobry binarny kod dla rozkładu prawdopodobieństwa $p = \langle p_1, \ldots, p_k \rangle$. Podana metoda znajduje *kod Huffmana* mający najkrótszą średnią długość wśród takich kodów. Algorytm jest rekurencyjny. Niech p_{k-1} oraz p_k najmniejsze w rozkładzie p. Rozważmy rozkład prawdopodobieństwa $q = \langle q_1 = p_1, \ldots, q_{k-2} = p_{k-2}, q_{k-1} = p_{k-1} + p_k \rangle$. Algorytm znajduje rekurencyjnie kod $\tilde{C} = \{\tilde{c}_1, \ldots, \tilde{c}_{k-1}\}$ dla rozkładu q. Szukany kod określamy jako $\{\tilde{c}_1, \ldots, \tilde{c}_{k-2}, \tilde{c}_{k-1}0, \tilde{c}_{k-1}1\}$. Oto uzasadnienie optymalności. Niech $C = \{c_1, \ldots, c_k\}$ kod optymalny dla rozkładu p. Z nierówności Krafta można założyć, że C prefiksowy. Jeżeli $p_j < p_i$ to $|c_i| \leq |c_j|$ bowiem w przeciwnym przypadku zamieniając c_i z c_j rolami dostaniemy kod o krótszej średniej długości. Niech $c \in C$ najdłuższe słowo. Istnieje inne $c' \in C$ takie, że $|c| = |c'|$, w przeciwnym przypadku moglibyśmy usunąć ostatni bit c i dostać nadal dekodowalny kod, bowiem C prefiksowy. Istnieje takie c', które różni się z c tylko na ostatnim bicie, w przeciwnym przypadku znów moglibyśmy c skrócić o ostatni bit. Zatem możemy przyjąć, że dwa najmniejsze prawdopodobieństwa p_{k-1} i p_k odpowiadają słowom c_{k-1} i c_k, które różnią się tylko na ostatnim bicie. Przejdźmy do kodu C' w którym c_{k-1} i c_k zastąpiony jest ich wspólnym przedrostkiem, z prawdopodobieństwem $p_{k-1} + p_k$. Ponieważ $\mathrm{L}(C) = \mathrm{L}(C') + p_{k-1} + p_k$, jeżeli znajdziemy optymalny kod C' to z niego dostaniemy optymalny kod C zgodnie z metodą Huffmana. Cofając się w rekursji dochodzimy do przypadku tylko dwóch prawdopodobieństw, dla których optymalnym kodem jest $\{0, 1\}$. To kończy dowód optymalności.

Rozważymy teraz problem komunikacji z zakłóceniami. Niech dany będzie system, w którym można nadawać ciąg sygnałów wybieranych spośród $S = \{s_1, \ldots, s_k\}$, po każdym nadaniu odbierana jest jedna z wiadomości w $T = \{t_1, \ldots, t_m\}$. Powiemy, że jest to *kanał z szumem*, gdy prawdopodobieństwo odebrania wiadomości zależy tylko od nadanego sygnału, przy czym zdarzenia nadania i odebrania kolejnych sygnałów i odpowiadających im wiadomości są niezależne. Niech zmienne losowe X i Y oznaczają odpowiednio nadany sygnał i odebraną wiadomość. Będziemy używali oznaczeń $\mathsf{P}[t] = \mathsf{P}[Y = t]$, $\mathsf{P}[s] = \mathsf{P}[X = s]$, $\mathsf{P}[t \mid s] = \mathsf{P}[Y = t \mid X = s]$, $\mathsf{P}[s \mid t] = \mathsf{P}[X = s \mid Y = t]$, $\mathsf{P}[s, t] = \mathsf{P}[X = s \text{ oraz } Y = t]$. Tablica prawdopodobieństw warunkowych $\mathsf{P}[t_j \mid s_i]$ jednoznacznie określa kanał z szumem, nazywamy ją *tablicą kanału*. Natomiast prawdopodobieństwa warunkowe $\mathsf{P}[s_i \mid t_j]$ można wyznaczyć z rozkładu X i tablicy $\mathsf{P}[t_j \mid s_i]$ kanału zgodnie z wzorem Bayesa. Odebranie wiadomości $Y = t$ przekazuje informację o X. Jest ona równa

$$\sum_{s \in S} \mathsf{P}[s \mid t] \cdot \lg \frac{1}{\mathsf{P}[s \mid t]} = \mathrm{H}(X \mid t) \ .$$

Uśredniając po wiadomościach określamy *entropię warunkową*:

$$\mathrm{H}(X \mid Y) = \sum_{t \in T} \mathsf{P}[t] \cdot \mathrm{H}(X \mid t) \ .$$

Znajomość Y zmniejsza naszą niepewność o X średnio o $\mathrm{H}(X \mid Y)$. Określamy *wzajemną informację X i Y* jako $\mathrm{I}(X;Y) = \mathrm{H}(X) - \mathrm{H}(X \mid Y)$. *Przepustowość* kanału z szumem określamy jako $\max_{r(X)} \mathrm{I}(X;Y)$, gdzie bierzemy maksimum po rozkładach $r(X)$ zmiennej X. Moglibyśmy oczekiwać, że przepustowość to średnia ilość informacji jaką można przekazać wysyłając jeden sygnał przez kanał z szumem. Zauważmy, że jest to optymistyczne oczekiwanie, bowiem wzajemna informacja jest określona przez odwołanie

do liczb $\mathrm{H}(X \mid t)$, a one są równe entropii pod warunkiem otrzymania wiadomości t. Ale kodowanie sygnału o wydajności bliskiej entropii może zależeć od tego jaką wiadomość otrzyma odbiorca, czyli od wiedzy o przyszłości. Widzimy, że przepustowość kanału jest zdefiniowana konserwatywnie, tym ciekawszy jest fakt, że tyle informacji rzeczywiście można przekazywać przez kanał. Mówi o tym tak zwane drugie twierdzenie Shannona.

Entropia warunkowa $\mathrm{H}(X \mid Y)$ oraz informacja $\mathrm{I}(X;Y)$ są wyznaczone przez rozkłady zmiennych X i Y, a w ich definicji nie potrzebujemy odwoływać się do związków z kanałem. Niech zmienne X i Y mają rozkłady $p(x) = \mathsf{P}[X = x]$ i $p(y) = \mathsf{P}[Y = y]$, oraz *łączny rozkład* $p(x,y) = \mathsf{P}[X = x \text{ oraz } Y = y]$. Określmy *łączną entropię*:

$$\mathrm{H}(X,Y) = -\sum_x \sum_y p(x,y) \cdot \lg p(x,y) = \mathrm{H}(Y,X) \ .$$

Możemy sprawdzić równości $\mathrm{H}(X,Y) = \mathrm{H}(X) + \mathrm{H}(Y \mid X)$ oraz $\mathrm{I}(X;Y) = \mathrm{H}(X) + \mathrm{H}(Y) - \mathrm{H}(X,Y)$. Stąd wynika symetryczność informacji $\mathrm{I}(X;Y) = \mathrm{H}(Y) - \mathrm{H}(Y \mid X) = \mathrm{I}(Y;X)$.

Najprostszym kanałem z szumem jest *binarny kanał symetryczny* (BKS), w którym wysyłamy 0 lub 1, oraz odbieramy też 0 lub 1, przy czym $\mathsf{P}[0 \mid 1] = \mathsf{P}[1 \mid 0] = p$ oraz $\mathsf{P}[1 \mid 1] = \mathsf{P}[0 \mid 0] = 1 - p$, gdzie p to prawdopodobieństwo *przekłamania* lub *błędu*. Obliczymy przepustowość takiego BKS. Przy ustalonym sygnale, wiadomości mają rozkład Bernoulliego o entropii $\mathrm{H}(p)$. Stąd

$$\begin{aligned} \mathrm{I}(X;Y) &= \mathrm{H}(Y) - \mathrm{H}(Y \mid X) = \mathrm{H}(Y) - \sum_s \mathsf{P}[s] \cdot \mathrm{H}(Y \mid X = s) \\ &= \mathrm{H}(Y) - \sum_s \mathsf{P}[s] \cdot \mathrm{H}(p) = \mathrm{H}(Y) - \mathrm{H}(p). \end{aligned}$$

Z symetryczności wzajemnej informacji, przepustowość kanału jest równa maksymalnej wartości $\mathrm{H}(Y) - \mathrm{H}(p)$. Jeżeli X ma rozkład jednostajny, czyli wysyłamy każdy z sygnałów z prawdopodobieństwem $1/2$, to wtedy Y też ma taki rozkład i $\mathrm{H}(Y) = 1$, razem mamy $\mathrm{I}(X;Y) = 1 - H(p)$.

Zadania

1. Podaj przykład kodu $C = \{c_1, \ldots, c_k\}$ dekodowalnego, który nie jest prefiksowy. Niech $l = \langle |c_1|, \ldots, |c_k| \rangle$ ciąg długości słów z C. Znajdź kod prefiksowy C' dla którego l też jest jego ciągiem długości słów.

2. Pokaż, że jeżeli X zmienna losowa, a $f : \mathbb{R} \to \mathbb{R}$ funkcja różnowartościowa, to X i $f(X)$ mają taką samą entropię.

3. Znajdź kod Huffmana dla rozkładu prawdopodobieństw $\langle \frac{1}{24}, \frac{2}{24}, \frac{2}{24}, \frac{3}{24}, \frac{3}{24}, \frac{4}{24}, \frac{9}{24} \rangle$.

4. Dla jakich rozkładów prawdopodobieństwa p entropia zmiennej losowej o rozkładzie p jest równa średniej długości kodu Huffmana dla p?

5. Niech z każdym słowem $x \in \{0,1\}^n$ będzie związane prawdopodobieństwo $s_x = p^k \cdot (1-p)^{n-k}$, gdzie k to liczba wystąpień 1-ki w x. Niech C_n to kod Huffmana dla rozkładu $\langle s_x \rangle$. Pokaż, że $\mathrm{L}(C_n) \to \mathrm{H}(p)$ dla $n \to \infty$.

6. Pokaż, że nierówność Krafta jest prawdziwa dla wszystkich kodów z własnością dekodowania.

7. Wyznacz prawdopodobieństwa $\mathsf{P}[s_i \mid t_j]$ z tablicy prawdopodobieństw $\mathsf{P}[t_j \mid s_i]$ kanału z szumem oraz prawdopodobieństw $\mathsf{P}[s_i]$.

8. Pokaż równość $\mathrm{H}(X,Y) = \mathrm{H}(X) + \mathrm{H}(Y \mid X)$.

9. Pokaż równość $\mathrm{I}(X;Y) = \mathrm{H}(X) + \mathrm{H}(Y) - \mathrm{H}(X,Y)$.

10. Dany BKS z prawdopodobieństwem błędu 1/4. Nadajemy komunikat $x \in \{0,1\}^*$ powtarzając każdy bit 3 razy, to znaczy wysyłając $3 \cdot |x|$ sygnałów. Oszacuj ile średnio informacji przekazuje nadanie jednego sygnału.

11. Niech kanał z szumem ma zbiór sygnałów $\{0,1\}$ i zbiór wiadomości $\{0,1,b\}$. Niech tablica kanału zawiera $\mathsf{P}[0 \mid 0] = \mathsf{P}[1 \mid 1] = \frac{1}{2}$ oraz $\mathsf{P}[0 \mid 1] = \mathsf{P}[b \mid 1] = \mathsf{P}[1 \mid 0] = \mathsf{P}[b \mid 0] = \frac{1}{4}$. Pokaż, ze przepustowość tego kanału jest równa 0.

12. Niech kanał z szumem ma zbiór sygnałów $\{0,1\}$ i zbiór wiadomości $\{0,1,b\}$. Niech tablica kanału zawiera $\mathsf{P}[0 \mid 0] = \mathsf{P}[1 \mid 1] = \frac{2}{3}$ oraz $\mathsf{P}[0 \mid 1] = \mathsf{P}[b \mid 1] = \mathsf{P}[1 \mid 0] = \mathsf{P}[b \mid 0] = \frac{1}{6}$. Znajdź przepustowość tego kanału.

13. Podaj przykład kanału z szumem, który umożliwia transmisję danych z efektywnością dwa bity informacji na przesłany sygnał.

14. Podaj przykład kanału z szumem, w którym dla każdego sygnału s liczba wiadomości jakie można odebrać z prawdopodobieństwem większym od zera po nadaniu s jest większa niż jeden, a przy tym kanał ten umożliwia transmisję danych z efektywnością trzy bity informacji na nadany sygnał.

MMD Wykład 7.

Bogdan Chlebus

Kody poprawiające błędy I. Omówimy metody przesyłania informacji przez kanał z szumem. Nadawca chciałby przekazać odbiorcy pewien tekst, który traktujemy jak strumień symboli z ustalonego alfabetu A. Wysyłanymi sygnałami i odbieranymi wiadomościami są symbole A. Tablica kanału określa z jakim prawdopodobieństwem odbierzemy $a_1 \in A$ o ile wysłany został $a_2 \in A$. Jeżeli $a_1 \neq a_2$ to zaszło *przekłamanie.* Zakładamy że wysyłane symbole nigdy nie są gubione, co najwyżej przekłamywane. Zdarzenia przekłamań przy transmisji kolejnych symboli są niezależne. Rozważamy tylko takie kanały, dla których istnieje liczba $0 \leq p < 1/2$ taka, że prawdopodobieństwo przekłamania przy każdej transmisji symbolu jest nie większe niż p. Nadawany tekst dzielimy na kolejne słowa długości k. W celu przesłania słowa $w \in A^k$ budujemy słowo $w' = \mathrm{K}(w) \in A^n$, gdzie $n \geq k$. Funkcja K obliczana jest przez odpowiedni algorytm kodowania, i powinna mieć własność, że znając $\mathrm{K}(w)$ można jednoznacznie wyznaczyć w. W trakcie transmisji mogą być przekłamania, i odbiorca otrzyma jeszcze inne słowo $w'' \in A^n$. Mamy zatem następujący schemat:

Nadawca: koduje słowo $w \in A^k$ jako $w' = \mathrm{K}(w) \in A^n$ i wysyła symbol po symbolu.

Transmisja: w' przekazane kanałem z szumem, odebrane jako $w'' \in A^n$.

Odbiorca: stara się znaleźć w' na podstawie w'', a potem $w = \mathrm{K}^{-1}(w')$ na podstawie słowa w'.

Jeżeli $\mathrm{K} : A^k \to A^n$ jest sposobem kodowania, to obraz $\mathrm{K}(A^k) = \mathcal{C} \subseteq A^n$ nazywamy *kodem*, elementy kodu to jego *słowa kodowe.* $|\mathcal{C}|$ oznacza liczność kodu $\mathcal{C}$. Operację, która każdemu słowu $w'' \in A^n$ przyporządkowywuje pewne słowo kodowe $w' \in \mathcal{C}$, a potem słowo $w \in A^k$ takie, że $\mathrm{K}(w) = w'$, nazywamy *odkodowywaniem. Odległość Hamminga* pomiędzy dwoma słowami $x, y \in A^n$ oznaczamy przez $\mathrm{hd}(x, y)$, jest to liczba pozycji na których się różnią. Na przykład $\mathrm{hd}(10110, 11010) = 2$, ponieważ słowa różnią się na dwóch pozycjach: drugiej i trzeciej. Interesuje nas odkodowywanie, które na podstawie $w'' \in A^n$ znajduje takie $w' \in \mathcal{C}$, że prawdopodobieństwo otrzymania w'' jest największe, pod warunkiem że zostało wysłane w'. Jako w' należy wziąć słowo w $\mathcal{C}$, które jest najbliższe w'' w sensie odległości Hamminga, bowiem $p < 1/2$. Stąd widać, że im dalej słowa kodowe są odległe od siebie, tym mniejsze będzie prawdopodobieństwo błędu odkodowania. Określamy zbiór $\{t \in A^n : \mathrm{hd}(t, w) \leq r\}$ jako *kulę o środku w i promieniu r.* Powiemy, że *kod $\mathcal{C}$ poprawia r błędów,* jeżeli wszystkie kule o środkach w słowach kodowych i promieniach r są rozłączne. *Minimalna odległość kodu* $\mathcal{C}$ to minimalna wartość $\mathrm{hd}(x, y)$, dla $x, y \in \mathcal{C}$, $x \neq y$. Jeżeli jest ona równa $2 \cdot r + 1$ to kod poprawia r błędów. Jeżeli kod ma M słów kodowych długości n i ma minimalną odległośc d, to powiemy, że jest typu (n, M, d).

Przykład: Niech $A = \{0, 1\}$, i kod $\mathcal{C}$ składa się z tych ciągów w A^n, których suma wyrazów jest parzysta. Algorytm kodowania przyporządkowuje słowu $w \in A^{n-1}$ słowo $\mathrm{K}(w) \in A^n$ przez dodanie na końcu *bitu kontroli parzystości*, tak, by otrzymane słowo było w $\mathcal{C}$.

Minimalna odległość $\mathcal{C}$ jest równa 2. Kod $\mathcal{C}$ nie może poprawić nawet jednego błędu, ale odbiorca może rozpoznać, że nastąpił błąd, gdy była nieparzysta liczba przekłamań. $\Diamond$

Przykład: Niech $A = \{0, 1\}$, $k = 1$. Kodowanie polega na tym, że każdy symbol $a \in A$ powtarzamy trzy razy: $\mathrm{K}(a) = aaa$. Kodem jest $\mathcal{P}_3 = \{000, 111\}$. Otrzymaną przez kanał transmisyjny trójkę bitów $\langle a, b, c\rangle$ odkodowujemy jako $d = \lfloor (a + b + c)/2 \rfloor$. Taki kod nazywamy *powtarzającym*, w naszym przypadku 3 razy. Podobnie określamy kod $\mathcal{P}_s = \{0^s, 1^s\}$ powtarzający s razy. Minimalna odległość kodu $\mathcal{P}_3$ jest równa 3, poprawia on jeden błąd. $\Diamond$

Dla kodu $\mathcal{P}_s$, wraz ze wzrostem s maleje prawdopodobieństwo błędu odkodowania. Natomiast rośnie jego redundancja, w tym sensie, żekażdy bit słowa kodowego zawiera tylko $1/s$ bitów informacji, bo wszystkie razem opisują jeden wysłany bit. Ogólnie, dla kodu $\mathcal{C} \subseteq A^n$, liczbę $R = n^{-1} \cdot \log_2(|\mathcal{C}|)$ nazywamy *zawartością informacji kodu* $\mathcal{C}$. Shannon pokazał, że można zmniejszyć prawdopodobieństwo błedu odkodowania dowolnie blisko zera, jednocześnie mając zawartość informacji odgraniczoną od zera. Rozważmy binarny alfabet $\{0, 1\}$ oraz BSK z prawdopodobieństwem przekłamania p. *Drugie twierdzenie Shannona* mówi, że jeżeli stała $R > 0$ jest mniejsza niż przepustowość $1 - \mathrm{H}(p)$ tego kanału, to istnieje ciąg kodów $\langle \mathcal{C}_n \rangle_{n \geq 1}$, gdzie długość $\mathcal{C}_n$ równa n, takich, że $|\mathcal{C}_n| = 2^{\lfloor Rn \rfloor}$ i prawdopodobieństwo błędu odkodowania dla $\mathcal{C}_n$ zbiega do 0 wraz z $n \to \infty$. Oryginalny dowód Shannona używał metody probabilistycznej: pokazał on, że jako $\mathcal{C}_n$ wystarczy wybrać losowy podzbiór $\{0, 1\}^n$ liczności $2^{\lfloor Rn \rfloor}$, z prawdopodobieństwem większym od zera będzie to dobry kod.

Przykład: Rozważmy macierz

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

określającą *kod Hamminga* $\mathcal{H}_3$. Słowo $w \in \{0, 1\}^7$ jest w $\mathcal{H}_3$ gdy zachodzi $H \cdot w^T = 0$, gdzie działania w $\mathbb{F}_2$. Na przykład $0101010 \in \mathcal{H}_3$ oraz $1111110 \notin \mathcal{H}_3$. Zbiór rozwiązań równania $H \cdot w^T = 0$ jest przestrzenią liniową wymiaru 4, zatem ma $2^4 = 16$ elementów. Słowa kodowe możemy wzajemnie jednoznacznie przyporządkować wszystkim słowom z $\{0, 1\}^4$. Zauważmy, ze kolumny H to zapisy binarne kolejnych liczb w [1..7]. Niech $b = \langle b_1, \ldots, b_7 \rangle$ to *wektor błędów transmisji*, gdzie $b_i = 1$ gdy błędnie przesłano i-ty bit, $b_i = 0$ w przeciwnym przypadku. Wysyłajac $w \in \mathcal{H}_3$ dostajemy $z = w + b$. Ma miejsce równość:

$$Hz^T = Hw^T + Hb^T = Hb^T \ .$$

Jeżeli był tylko jeden błąd transmisji, na przykład $b_i = 1$, to $Hb^T = h_i$, gdzie ciąg h_i jest binarnym przedstawieniem liczby i. Zatem $\mathcal{H}_3$ poprawia jeden błąd. $\Diamond$

Kody liniowe. Porównując kody $\mathcal{P}_3$ i $\mathcal{H}_3$ widzimy, że kod powtarzający 3 razy wymaga $4 \cdot 3 = 12$ bitów a kod Hamminga $\mathcal{H}_3$ wymaga tylko 7, do zakodowania słowa długości 4, każdy z tych kodów poprawia 1 błąd. Kod Hamminga jest zatem istotnie lepszy, i zasługuje na to aby być dla nas inspiracją. $\mathcal{H}_3$ jest podprzestrzenią liniową $\mathbb{F}_2^7$, bo

jest opisany jednorodnym układem równań liniowych. Możemy przypuszczać, że bogata struktura algebraiczna kodu powinna ułatwić zrozumienie jego działania i być może także efektywne kodowanie i odkodowywanie. Podstawą jest możliwość wykonywania operacji algebraicznych na symbolach alfabetu. Jeżeli alfabet jest ciałem skończonym $\mathbb{F}$, natomiast kod $\mathcal{C}$ podprzestrzenią liniową $\mathbb{F}^n$, to takie kody nazywamy *liniowymi*. Jeżeli alfabetem jest $\mathbb{F}_2$ to kod nazywamy *binarnym*. Liczbę n, czyli długość słów kodowych, nazywamy *długością kodu*. *Wymiar kodu* to jego wymiar jako przestrzeni liniowej. Parę liczb $[n, k]$, gdzie n długość a k to wymiar kodu $\mathcal{C}$, nazywamy *typem* kodu liniowego. Słowo wejściowe $w = a_1 \dots a_k$ będziemy kodować w sposob liniowy jako pewne słowo $c = c_1 \dots c_n \in \mathcal{C}$. To znaczy, symbole c_j, dla $1 \leq j \leq n$ będą kombinacjami liniowymi symboli a_i, czyli $c = w \cdot G$, dla pewnej macierzy G określającej kodujące przekształcenie liniowe, którego obrazem jest kod $\mathcal{C}$. Macierz G nazywamy *macierzą tworzącą* $\mathcal{C}$. Taką macierzą może być każda macierz $k \times n$, której wiersze są bazą $\mathcal{C}$. Inny opis kodu $\mathcal{C}$ to zbiór równań liniowych, które są spełnione dokładnie przez słowa kodowe. To znaczy: $c \in \mathcal{C}$ w.t.w. gdy $H \cdot c^T = 0$, gdzie H jest pewną macierzą, nazywaną *macierzą kontroli parzystości kodu* $\mathcal{C}$. Istnieje takie k pozycji w słowach kodowych kodu $\mathcal{C}$ typu $[n, k]$, że tam ustalone wartości określają jednoznacznie słowo w $\mathcal{C}$. Po ustaleniu takich pozycji znajdujące się na nich symbole są nazywane *symbolami informacyjnymi*, one moga być przyjęte jako przekazywana informacja. Wygodnie jest mieć macierz G postaci $G = [I_k \mid A]$, gdzie I_k to macierz jednostkowa $k \times k$. W takim przypadku szczególnie łatwo jest odkodować słowa kodowe. Jeżeli $c = w \cdot [I_k \mid A]$, dla $w = a_1 \dots a_k$ oraz $c = c_1 \dots c_n$, to mamy $c_i = a_i$ dla $1 \leq i \leq k$ oraz $c_j = w \cdot A_{j-k}$ dla $k < j \leq n$, gdzie $A = [A_1 \dots A_{n-k}]$. To znaczy, że $c \in \mathcal{C}$ w.t.w. gdy $H \cdot c^T = 0$, gdzie $H = [-A^T \mid I_{n-k}]$. Rzeczywiscie, i-tym wyrazem ciągu Hc^T jest $-\langle c_1 \dots c_k \rangle \cdot A_i + c_{i+k}$, dla $1 \leq i \leq n-k$, gdzie kropka $\cdot$ oznacza mnożenie skalarne. Mówimy, że takie macierze G oraz H *są w postaci standardowej.*

Niech kod $\mathcal{C}$ typu $[n, k]$ ma macierz tworzącą G. Określmy *kod dualny* $\mathcal{C}^\perp$ jako zbiór słów g takich, że $g \cdot c = 0$ (iloczyn skalarny), dla każdego $c \in \mathcal{C}$. Kod $\mathcal{C}^\perp$ jest typu $[n, n-k]$, a jego macierz tworząca H jest macierzą kontroli parzystosci $\mathcal{C}$, bowiem $H \cdot G^T = 0$. Ogólnie, jeżeli H jest macierzą kontroli parzystości kodu $\mathcal{C}$, to $\mathcal{C}$ ma wymiar k w.t.w. gdy H ma rząd $n - k$.

Waga słowa w, oznaczana $\mathrm{wg}(w)$, to odległość w od słowa złożonego z samych zer: $\mathrm{wg}(w) = \mathrm{hd}(w, 0)$. *Minimalna waga kodu* $\mathcal{C}$ to $\min\{\mathrm{wg}(c) : c \in \mathcal{C}, c \neq 0\}$. Dla kodow liniowych, minimalna odległość i waga są sobie równe: $\mathrm{hd}(x, y) = \mathrm{hd}(x-y, 0) = \mathrm{wg}(x-y)$, ponieważ $\mathcal{C}$ jest zamkniety na różnice. Kod typu $[n, k]$ o minimalnej odległości d jest określany jako *typu* $[n, k, d]$. Dla H macierzy kontroli parzystości kodu $\mathcal{C}$ długości n zachodzi: $\mathcal{C}$ ma minimalną odległość d w.t.w. gdy *każde* $d-1$ kolumn H jest liniowo niezależnych i *pewne* d kolumn jest liniowo zależnych. Mianowicie, istnieje $c \in \mathcal{C}$ takie że $\mathrm{wg}(c) = f$ w.t.w. istnieje c taki, że $Hc^T = 0$ i $\mathrm{wg}(c) = f$ w.t.w. f kolumn H jest liniowo zależnych. Stąd wynika, że jeżeli istnieje liniowy kod typu $[n, k, d]$, to $n - k \geq d - 1$, jako że $n - k$ to rząd H.

Jak odkodowywać kody liniowe? Jeżeli b jest wektorem błędów, i wysyłamy słowo $c \in \mathcal{C}$, to otrzymamy $d = c + b$. Zatem $d - b \in \mathcal{C}$. Zbiór wektorów postaci $b + \mathcal{C} = \{b + c : c \in \mathcal{C}\}$ nazywamy *warstwą* $\mathcal{C}$. Dwa wektory x_1, x_2 są w tej samej warstwie gdy $x_1 - x_2 \in \mathcal{C}$. Oto

prosty algorytm odkodowywania: otrzymawszy c, znajdź wektor e o najmniejszej wadze w warstwie wyznaczonej przez c i odkoduj c jako $a = c - e$; takie słowo e nazywa się *liderem warstwy* c. Aby znaleźć warstwę wektora c, obliczamy $H \cdot c^T$, czyli jego *syndrom*, gdzie H macierz kontroli parzystości $\mathcal{C}$. Zauważmy, że x, y są w tej samej warstwie w.t.w. gdy $x - y \in \mathcal{C}$ w.t.w. gdy $H(x-y)^T = 0$ w.t.w. $Hx^T = Hy^T$. Liderów warstw najwygodniej jest stablicować posługując się wartościami syndromów warstw. Syndrom, dla kodów binarnych, jest równy sumie kolumn H wziętych z pozycji, w których wystąpił błąd: jeżeli $d = c + b$, dla $c \in \mathcal{C}$, to $H(d)^T = Hc^T + Hb^T = Hb^T$.

Naszym kolejnym celem jest uogólnienie kodu Hamminga $\mathcal{H}_3$ tak, by otrzymać podobnie dobry kod poprawiający więcej niż jeden błąd. Kody różniące się tylko kolejnością symboli określamy jako *równoważne*. Permutując kolumny macierzy parzystości dostajemy takie kody. Rozważymy teraz dwa kody równoważne $\mathcal{H}_3$.

Przykład: Interpretujemy kolumny macierzy kontroli parzystości H kodu $\mathcal{H}_3$ jako elementy $\mathrm{GF}(2^3)$. Niech α element pierwotny, wtedy w H można poprzestawiać kolumny tak, by otrzymac $H' = [1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6]$. Na przykład, jeżeli ciało wyznaczone przez wielomian nierozkładalny $x^3 + x + 1 \in \mathbb{F}_2[x]$, to możemy dostać

$$H' = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Niech $\mathcal{H}_3'$ to kod, którego macierzą kontroli parzystości jest H'. Wektor $a = \langle a_0, \ldots, a_6 \rangle \in \mathcal{H}_3'$ gdy $H' \cdot a^T = 0$ w.t.w. $\sum_{i=0}^{6} a_i \alpha^i = 0$ w.t.w. $A(\alpha) = 0$, gdzie A wielomian $A(x) = a_0 + a_1 x + \cdots + a_6 x^6$. Odtąd będziemy interpretować słowa kodowe jak wielomiany. $\Diamond$

Przykład: Kolumny H można poprzestawiać jeszcze inaczej, do postaci:

$$H'' = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Drugi wiersz macierzy H'' jest cyklicznym przesunięciem wiersza pierwszego o jedną pozycję, a wiersz trzeci drugiego. Niech $\mathcal{H}_3''$ będzie kodem, którego macierzą kontroli parzystości jest H''. Sprawdzamy (ćwiczenie), że kod $\mathcal{H}_3''$ jest zamknięty na cykliczne przesunięcia słów kodowych, to znaczy: jeżeli $a = \langle a_0, \ldots, a_7 \rangle \in \mathcal{H}_3''$ to także $a = \langle a_7, a_0, a_1 \ldots, a_6 \rangle \in \mathcal{H}_3''$. To jest inspiracją do rozważenia kodów cyklicznych, mających podobne własności. $\Diamond$

Kody cykliczne. Utożsamiamy słowa kodowe z wielomianami. Jeżeli $A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}[x]$, to $a_n + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1}$ jest otrzymany z $A(x)$ przez pomnożenie przez x, jeżeli jednocześnie "utożsamimy" x^n z 1. Formalnie, utożsamiamy dwa wielomiany, gdy mają taką samą resztę z dzielenia przez $x^n - 1$ w $\mathbb{F}[x]$, czyli rozważamy pierścień $\mathbb{F}[x]/(x^n - 1)$ reszt modulo $x^n - 1$. Jeżeli kod byłby zamknięty na cykliczne przesunięcia słów kodowych, to przy interpretacji wielomianowej byłby zamknięty na mnożenie przez zmienną x w $\mathbb{F}[x]/(x^n - 1)$, czyli, z liniowości kodu, na mnożenie przez dowolny element pierścienia $\mathbb{F}[x]/(x^n - 1)$. To prowadzi do następującej

definicji. *Kod cykliczny* określamy jako ideał w pierścieniu $\mathbb{F}[x]/(x^n-1)$, gdzie $\mathbb{F}$ ciało skończone. Przykładem ideału pierścienia P jest zbiór elementów postaci $a \cdot r$, gdzie $a \in P$ ustalony oraz $r \in P$ przebiega elementy P. To jest ideał główny, czyli generowany przez jeden element, w tym przypadku a. Jak pamiętamy, w pierścieniach gdzie można jednoznacznie dzielić z resztą, jak w $\mathbb{Z}$, lub $\mathbb{F}[x]$, lub $\mathbb{F}[x]/A(x)$ gdzie $A(x) \in \mathbb{F}[x]$, dla $\mathbb{F}$ ciała, wszystkie ideały właściwe niezerowe są główne. Stąd każdy kod $\mathcal{C}$ cykliczny ma jednoznacznie wyznaczony generator $g(x)$, nazwiemy go *wielomianem tworzącym kodu*. Podzielmy x^n-1 przez taki wielomian w $\mathbb{F}[x]$. Mamy $x^n-1 = Q(x)\cdot g(x) + R(x)$, gdzie $\deg R(x) < \deg g(x)$. W pierścieniu $\mathbb{F}[x]/(x^n-1)$ zachodzi $R(x) = -Q(x)\cdot g(x)$, zatem $R(x) = 0$. Czyli $g(x)$ jest dzielnikiem x^n-1. Jeżeli $\deg g(x) = n-k$ to wielomiany $g(x), xg(x), x^2g(x), \ldots, x^{k-1}g(x)$ tworzą bazę kodu $\mathcal{C}$ typu $[n,k]$. Niech $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$, wtedy macierz tworząca kodu $\mathcal{C}$ jest następująca:

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

Wielomian $g(x)$ dzieli x^n-1, czyli $x^n-1 = g(x)\cdot h(x)$. Jeżeli $A(x)$ jest słowem kodowym, to $A(x) = g(x)\cdot D(x)$, zatem $h(x)\cdot A(x) = 0$ w $\mathbb{F}[x]/(x^n-1)$. Niech $h(x) = h_0 + h_1x + \cdots + h_kx^k$, wtedy $a_0h_i + a_1h_{i-1} + \cdots + a_{n-k}h_{i-n+k} = 0$, co oznacza, że macierz

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & h_k & \cdots & h_1 & h_0 \\ 0 & 0 & \cdots & h_k & h_{k-1} & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & h_{k-1} & \cdots & h_1 & h_0 & \cdots & 0 & 0 \end{bmatrix}$$

jest macierzą kontroli parzystości $\mathcal{C}$. Ponieważ generator $g(x)$ kodu $\mathcal{C}$ jest dzielnikiem x^n-1, jeżeli znamy rozkład $x^n-1 = P_1(x)\cdot\ldots\cdot P_r(x)$ na czynniki nad podciałem $\mathbb{F}$, którego elementy są symbolami alfabetu, to tym samym mamy określone wszystkie kody cykliczne w $\mathbb{F}[x]/(x^n-1)$. Dla prostoty rozważamy przypadek, gdy alfabetem jest podciało proste $\mathbb{F}$. Jeżeli $P_i(\beta) = 0$, dla $\beta \in \mathbb{F}$, to $P_i(x)$ jest dla β wielomianem minimalnym, a podzielność $Q(x)$ przez $P_i(x)$ w $\mathbb{F}[x]$ jest równoważna $Q(\beta) = 0$. W ten sposób możemy określić kod podając gdzie ma się zerować wielomian tworzący, czyli podając *zera kodu*. W terminach macierzy kontroli parzystości, każde takie β daje wiersz postaci $[1, \beta, \beta^2, \ldots]$.

Kody BCH. Niech $n = p^m - 1$, a β element pierwotny $\mathrm{GF}(p^m)$. Określmy kod przez wymaganie by elementy $\beta^s, \beta^{s+1}, \ldots, \beta^{s+d-2}$ były jego zerami. Alfabetem kodu jest $\mathbb{F}_p$. Macierz kontroli parzystości jest rozmiaru $(d-1)m \times n$ i ma następującą postać:

$$J = \begin{bmatrix} 1 & \beta^s & \beta^{2s} & \ldots \\ 1 & \beta^{s+1} & \beta^{2(s+1)} & \ldots \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \beta^{s+d-2} & \beta^{2(s+d-2)} & \ldots \end{bmatrix}$$

Pokażemy, że minimalna odległość tego kodu jest co najmniej d, w tym celu wystarczy pokazać, że każde $d-1$ kolumn J jest liniowo niezależnych. Weźmy taką podmacierz, i

podzielmy każdą kolumnę przez element z pierwszego wiersza. Dostaniemy macierz:

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ \gamma_1 & \gamma_2 & \cdots & \gamma_{d-1} \\ \gamma_1^2 & \gamma_2^2 & \cdots & \gamma_{d-1}^2 \\ \dots & \dots & \dots & \dots \\ \gamma_1^{d-2} & \gamma_2^{d-2} & \cdots & \gamma_{d-1}^{d-2} \end{bmatrix}$$

Jest to macierz Vandermonde'a o wyznaczniku $\prod_{1 \le j < i \le d-1}(\gamma_i - \gamma_j) \neq 0$.

Podamy przykład kodu BCH o minimalnej odległości 5, czyli poprawiającego dwa błędy. Niech $n = 2^4 - 1$, ciało $\mathbb{F} = \mathrm{GF}(2^4)$. Niech α element pierwotny ciała $\mathbb{F}$, i niech $\alpha, \alpha^2, \alpha^3, \alpha^4$ miejsca zerowe kodu. Nasz szukany kod będzie generowany przez najmniejszą wspólną wielokrotność wielomianów minimalnych tych miejsc zerowych kodu. Niech ciało $\mathrm{GF}(2^4)$ będzie reprezentowane jako ciało reszt modulo $x^4 + x + 1$. Oto wielomiany minimalne elementów ciała:

Elementy ciała:	Wielomian minimalny:
0	x
1	$x + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$x^4 + x + 1$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$x^4 + x^3 + 1$

Wielomianem tworzącym naszego kodu jest $(x^4+x+1)(x^4+x^3+x^2+x+1)$, a otrzymany kod jest binarny typu $[15, 7, 5]$.

Zadania

1. Przekazujemy 4 bity informacji za pomocą 12 bitów kodu powtarzającego 3 razy i za pomocą 7 bitów kodu Hamminga $\mathcal{H}_3$. Oblicz odpowiednie prawdopodobieństwa błędu odkodowania, gdy prawdopodobieństwo przekłamania dla BSK jest równe $p = \frac{1}{100}$.

2. Pokaż, że jeżeli istnieje kod typu (n, M, d) nad alfabetem A, to zachodzi nierówność $M \le |A|^{n-d+1}$. *Wskazówka*: przejdź do nowego kodu przez usunięcie symboli na pewnych $d-1$ pozycjach.

3. Niech $K_q(n, d)$ będzie licznością kuli o promieniu d w A^n, gdzie $|A| = q$. Pokaż, że $K_q(n, d) = \sum_{i=0}^{d} \binom{n}{i}(q-1)^i$.

4. Pokaż *ograniczenie Hamminga:* jeżeli istnieje kod nad alfabetem A, gdzie $|A| = q$, długości n, poprawiający b błędow i mający T słów kodowych, to zachodzi nierówność: $T \cdot \sum_{i=0}^{b} \binom{n}{i}(q-1)^i \le q^n$.

5. Pokaż, że kody powtarzające są kodami liniowymi. Znajdź macierz tworzącą i kontroli parzystości dla powtarzania trzy razy.

6. Kod typu $[n, n-k]$ nad $\mathbb{F}_q$, gdzie $n = (q^k - 1)/(q-1)$ wyznaczony przez macierz kontroli parzystości, w której kolumny są parami niezależne to *kod Hamminga*. Pokaż, że takie kody zawsze istnieją. Ile błędów poprawiają?

7. Kod długości n poprawiający b błędów jest *doskonały*, jezeli każde słowo długości n jest odległe o nie więcej niż b od nie więcej niż jednego słowa kodowego. Pokaż, że każdy kod Hamminga jest doskonały.

8. Oto macierz tworząca liniowego kodu binarnego $\mathcal{C}$:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

   Znajdź macierz kontroli parzystości $\mathcal{C}$. Ile błędów może poprawić ten kod? Otrzymaliśmy komunikat 0100111, o którym wiemy, że nastąpiło w nim nie więcej niż jedno przekłamanie. Znajdź oryginalny 4-bitowy komunikat, który został nadany.

9. Czy istnieje kod typu $[11, 8, 5]$?

10. Podaj przykład kodu, który sam jest swoim kodem dualnym.

11. Sprawdź, że kod $\mathcal{H}_3''$ jest zamknięty na cykliczne przesunięcia słów kodowych.

12. Ile jest binarnych kodów cyklicznych długości 7?

13. Dlaczego w definicji kodów BCH przyjęliśmy $n = p^m - 1$?

14. Znajdź macierze tworzącą i kontroli parzystości dla binarnego kodu BCH określonego przez wielomian tworzący $(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \in \mathbb{F}_{2^4}[x]$.

15. Znajdź wielomian tworzący binarnego kodu BCH typu $[15, 5, 7]$.

MMD Wykład 8.

Bogdan Chlebus

Kody poprawiające błędy II.

Niech $\mathbb{F}_q$ ciało, $n = q - 1$, oraz α element pierwotny $\mathbb{F}_q$. Rozważmy macierz nieosobliwą

$$A = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \ldots & \alpha^{(n-1)(n-1)} \end{bmatrix}$$

Przekształcenie, które dla argumentu $b \in \mathbb{F}_q^n$ daje wartość $A \cdot b = B = \langle B_0, \ldots, B_{n-1} \rangle$, nazywamy *dyskretną transformacją Fouriera*, i oznaczamy DTF. Mamy $B_i = \sum_{k=0}^{n-1} b_k \alpha^{ki}$. Innymi słowy: wykonanie DTF dla argumentu $b = \langle b_0, \ldots, b_{n-1} \rangle$ to obliczenie wartości wielomianu $b(x) = b_0 + b_1 \cdot x + \ldots + b_{n-1}x^{n-1}$ w kolejnych potęgach α. Wielomian $\hat{B}(z) = \sum_{i=0}^{n-1} B_i z^{n-i}$ w kontekście kodów nazywamy *wielomianem Mattsona-Solomona* (lub krócej *MS-wielomianem*) ciągu b. Znając $\hat{B}$ można obliczyć b następująco: $b_j = \frac{1}{n}\hat{B}(\alpha^j)$, dla $0 \leq j \leq n-1$. Sprawdzamy:

$$\begin{aligned} \hat{B}(\alpha^j) &= \sum_{i=0}^{n-1} B_i \cdot (\alpha^j)^{n-i} = \sum_{i=0}^{n-1} \sum_{k=0}^{n-1} b_k \cdot \alpha^{ki} \cdot (\alpha^j)^{n-i} \\ &= \sum_{k=0}^{n-1} b_k \sum_{i=0}^{n-1} \alpha^{ki+jn-ji} = \sum_{k=0}^{n-1} b_k \sum_{i=0}^{n-1} \alpha^{i(k-j)} \ , \end{aligned}$$

ponieważ $\alpha^n = 1$. Dla $k = j$ odpowiedni składnik jest równy $n \cdot b_j$. Dla $k \neq j$ mamy

$$\sum_{i=0}^{n-1} \alpha^{i(k-j)} = \frac{1 - (\alpha^{k-j})^n}{1 - \alpha^{k-j}} = 0 \ .$$

Stąd $\hat{B}(\alpha^j) = n \cdot b_j$. Jako wniosek zauważmy, że jeżeli t spośród potęg α jest zerami wielomianu $\hat{B}$, to waga ciągu b jest równa $n - t$.

Kody Reeda-Solomona. Określamy kod $\mathrm{RS}(n, k)$ jako zbiór ciągów $s \in \mathbb{F}_q^n$, $s = \langle s_0, \ldots, s_{n-1} \rangle$, takich, że $s_j = P(\alpha^j)$, dla $0 \leq j \leq n-1$, gdzie $P(x) \in \mathbb{F}_q[x]$ ma stopień nie większy niż $k - 1$. Wielomian $P(x)$ jest określony przez ciąg swoich współczynników P_i, wygodnie jest przyjąć, że $P(x) = P_0 + P_1 x + \ldots + P_{n-1}x^{n-1}$ i utożsamiać $P(x)$ z ciągiem $P = \langle P_0, \ldots, P_{n-1} \rangle$, gdzie $P_i = 0$ dla $i \geq n - k + 1$. Ciąg $s = \langle s_0, \ldots, s_{n-1} \rangle$ utożsamiamy także z wielomianem $s(x) = s_0 + s_1 x + \ldots + s_{n-1}x^{n-1}$. Zauważmy, że $P(x)$ jest MS-wielomianem ciągu $\langle s_j/n \rangle_{0 \leq j \leq n-1}$, czyli $n \cdot P(x)$ jest MS-wielomianem ciągu s. DTF jest przekształceniem liniowym różnowartościowym, które przekształca $\mathbb{F}_q^n$ w $\mathbb{F}_q^n$, kod $\mathrm{RS}(n, k)$ jest otrzymany jako przeciwobraz podprzestrzeni $\mathbb{F}_q^k$, zatem ma wymiar k, czyli jest typu $[n, k]$. Wielomian $P(x)$ stopnia nie większego niż $k - 1$ może mieć co najwyżej $k - 1$ pierwiastków, stąd każde słowo w kodzie $\mathrm{RS}(n, k)$ może mieć co najwyżej $k - 1$ zer, czyli jego waga jest co najmniej $n - k + 1$. Pamiętamy, że minimalna odległość kodu typu $[n, k]$ jest nie większa niż $n - k + 1$. Zatem minimalna odległość kodu $\mathrm{RS}(n, k)$

jest dokładnie równa $n-k+1$. Kody typu $[n,k,d]$ dla których $d=n-k+1$ nazywają się *optymalnymi*.

Z określenia MS wielomianu i DTF mamy:

$$n \cdot P_{n-i} = \sum_{k=0}^{n-1} s_k \cdot \alpha^{ki} = s(\alpha^i) \ .$$

Ponieważ $P_i = 0$ dla $i = k, k+1, \ldots, n$, dostajemy, że α^i jest pierwiastkiem $s(x)$ dla $i = 1, \ldots, n-k$. Stąd widzimy, że kody RS(n,k) to kody cykliczne, których wielomianem tworzącym jest $\prod_{i=1}^{k-1}(x-\alpha^i)$. Są to zatem kody BCH szczególnej postaci, ale zauważmy że ich alfabetem są "duże" ciała $\mathbb{F}_q$ a nie podciała proste $\mathbb{F}_q$. Taka interpretacja kodów RS(n,k) pozwala odwołać się do ogólnych zasad kodowania dla kodów BCH. Najprościej kodowanie dla kodów RS interpretować w następujący sposób: dana informacja $P = \langle P_0, \ldots, P_{k-1}\rangle$, zakoduj ją jako ciąg wartości wielomianu $P(x)$ w kolejnych potęgach α. Pamiętajmy, że P jest ciągiem elementów $\mathbb{F}_q$, jeżeli chcemy kodować informacje podane w postaci binarnej, musimy najpierw zapisać je w takiej postaci.

Mając kod $\mathcal{C}$ nad alfabetem GF(p^m) można przejść do kodu $\mathcal{C}'$ nad alfabetem $\mathbb{F}_p$ w następujący sposób. Symbol $a \in \mathrm{GF}(p^m)$ może być utożsamiony z ciągiem $\langle a_1, \ldots, a_m\rangle$, gdzie $a_i \in \mathbb{F}_p$, takim że $a = \sum_{i=1}^m a_i \cdot \beta_i$, gdzie $\beta_1, \ldots, \beta_m$ to baza GF(p^m) nad swoim podciałem prostym. Jeżeli zatem słowo $c \in \mathcal{C}$ jest ciągiem $\langle c_1, \ldots, c_n\rangle$ to możemy mu przyporządkować ciąg $c' = \langle c_{1,1}, c_{1,2}, \ldots, c_{1,m}, c_{2,1}, c_{2,2}, \ldots, c_{2,m}, \ldots, c_{n,1}, \ldots, c_{n,m}\rangle$, gdzie $c_i = \sum_{j=1}^m c_{i,j}\beta_j$. Słowo c' składa się z $n \cdot m$ symboli z $\mathbb{F}_p$. Przejście od c do c' nazwiemy *rzutowaniem* kodu, w tym przypadku na alfabet $\mathbb{F}_p$. Operacja rzutowania jest przekształceniem liniowym, zatem z kodów liniowych dostajemy liniowe. Jeżeli kod $\mathcal{C}$ jest typu $[n,k,d]$, to przez rzutowanie dostaniemy kod $\mathcal{C}'$ typu $[n\cdot m, k\cdot m, d']$, gdzie $d' \geq d$. Parametr d' czasem wzrasta w stosunku do d, i może zależeć od wyboru bazy $\mathbb{F}_q$ nad podciałem prostym.

Przykład: Rozważmy ciało $\mathbb{F} = \mathrm{GF}(2^2)$, niech będzie określone jako ciało reszt w $\mathbb{F}_2[x]$ modulo x^2+x+1. Zbudujemy kod RS$(3,2)$ nad $\mathbb{F}$. Ciało $\mathbb{F}$ składa się z elementów $0, 1, \alpha, \alpha^2$, które odpowiadają wielomianom $0, 1, x, x+1$, zatem mogą być przedstawione jako ciągi bitów $00, 01, 10, 11$. Mamy 4^2 wielomianów stopnia co najwyżej 1 nad $\mathbb{F}$, słowa kodowe to ciągi wartości tych wielomianów w punktach $1, \alpha, \alpha^2$. Na przykład weźmy wielomian $P(x) = \alpha^2 \cdot x + 1$, mamy $P(1) = \alpha$, $P(\alpha) = 0$, $P(\alpha^2) = \alpha^2$. Zatem dostaliśmy słowo kodowe $\langle \alpha, 0, \alpha^2\rangle$, a po zrzutowanie na alfabet binarny słowo $\langle 1,0,0,0,1,1\rangle$. Oto tablica wszystkich słow kodowych RS$(3,2)$:

000	111	$\alpha\alpha\alpha$	$\alpha^2\alpha^2\alpha^2$
$1\alpha\alpha^2$	$0\alpha^2\alpha$	$\alpha^2 01$	$\alpha 10$
$\alpha\alpha^2 1$	$\alpha^2\alpha 0$	$01\alpha^2$	10α
$\alpha^2 1\alpha$	$\alpha 0\alpha^2$	$1\alpha^2 0$	$0\alpha 1$

Jest to kod typu $[3,2,2]$ nad alfabetem $\mathbb{F}_4$, i jest optymalny. Po zrzutowaniu na alfabet

binarny dostajemy kod:

000000	010101	101010	111111
011011	001110	110001	100100
101101	111000	000111	010010
110110	100011	011100	001001

Ten kod jest typu $[6, 4]$. Jego minimalna odległość jest równa 2, ponieważ istnieją w nim słowa o wadze 2. Kod nadal jest cykliczny, ale nie jest już optymalny. $\Diamond$

Rozpraszanie informacji. Jest to metoda kodowania informacji pozwalająca odtworzyć dane na podstawie fragmentów zapisu, oparta o pomysł podobny jak w kodach RS. Niech l, m, k liczby naturalne, $m \geq k$. Chcielibyśmy każdy ciąg $f \in \{0,1\}^l$ zapisać w postaci m pakietów $s_1, \ldots, s_m$ takich, że każde k spośród nich wystarczy na odtworzenie f. W tym celu podzielmy f na k rozłącznych bloków $f = f_0 \ldots f_{k-1}$, gdzie $|f_i| \leq \lceil l/k \rceil$. Interpretujemy f_i jako elementy ciała $\mathbb{F} = \mathrm{GF}(2^a)$, gdzie a tak duże, że zachodzą nierówności $a \geq l/k$ i $2^a > m$ (w razie potrzeby do f_i dopisujemy zera). Niech α element pierwotny w $\mathbb{F}$. Ciąg f interpretujemy jako wielomian $P(x) = \sum_{i=0}^{k-1} f_i \cdot x^i \in \mathbb{F}[x]$. Niech $t_j = P(\alpha^{j-1})$, dla $1 \leq j \leq m$. Określamy pakiet s_j jako parę $\langle j, t_j \rangle$. Przypuśćmy, że znamy k różnych pakietów $\langle j_1, t_{j_1} \rangle, \ldots, \langle j_k, t_{j_k} \rangle$. Zatem znamy wartości wielomianu P stopnia $k-1$ w k punktach, co pozwala jednoznacznie odtworzyć P rozwiązując odpowiedni problem interpolacji. W tym celu wystarczy rozwiązać układ równań

$$\langle t_{j_1} \ldots, t_{j_k} \rangle^T = B \cdot \langle f_0, f_1, \ldots, f_{k-1} \rangle^T$$

względem zmiennych f_i, gdzie i-ty wiersz macierzy B jest postaci $\langle 1, \alpha^{j_i}, \alpha^{2 \cdot j_i}, \ldots, \alpha^{(k-1) \cdot j_i} \rangle$. Macierz B jest odwracalna jako macierz Vandermonde'a.

Kody asymptotycznie dobre. Przypomnijmy, że jeżeli $\mathrm{K} : \{0,1\}^k \to \{0,1\}^n$ jest różnowartościowym kodowaniem, to liczba $k/n = R$ nazywana jest zawartością informacji kodu $\mathrm{K}(\{0,1\}^k)$. Niech D będzie minimalną odległością kodu $\mathcal{C} \subseteq \{0,1\}^n$, wtedy liczba $\delta = D/n$ oznacza *minimalną względną odległość* $\mathcal{C}$. Jeżeli p jest prawdopodobieństwem błędu przesłania bitu przez BSK, a przesyłamy n bitów, to oczekiwana liczba błędów jest równa $p \cdot n$. Będziemy mogli poprawić te błędy, gdy $2 \cdot p \cdot n + 1 < D = n \cdot \delta$, zatem gdy $2p < \delta$. To uzasadnia, dlaczego dobrze jest mieć minimalne względne odległości kodów oddzielone od zera przez stałą. Długie słowa kodowe są dobre, ponieważ im większe n tym mniejsze prawdopodobieństwo, że liczba błędów będzie odchylona od oczekiwanej $p \cdot n$ o więcej niż $\epsilon \cdot n$, dla $\epsilon < \delta - 2p$. Chcemy mieć także kody z zawartością informacji odgraniczoną od zera, aby czas transmisji był proporcjonalny do długości tekstu, który chcemy przekazać.

Niech $\langle \mathcal{C}_n \rangle$, dla $n \geq 1$, będzie ciągiem kodów takim, że długości $\mathcal{C}_n$ rosną wraz z n. Niech R_n będzie zawartością informacji $\mathcal{C}_n$, a δ_n będzie minimalną względną odległością $\mathcal{C}_n$. Powiemy, że ciąg $\langle \mathcal{C}_n \rangle$ jest *asymptotycznie dobry* gdy istnieją takie stałe $R > 0$ i $\delta > 0$, że zachodzi $R_n \geq R$ i $\delta_n \geq \delta$, dla każdej liczby $n \geq 1$.

Pokażemy *ograniczenie Gilberta-Varshamova*, które mówi, że jeżeli $R < 1 - \mathrm{H}(\delta)$ to, dla każdego dostatecznie dużego n, istnieje binarny kod liniowy o długości słów n, zawartości informacji R i minimalnej względnej odległości δ, gdzie H to funkcja entropii.

Potrzebujemy mieć macierz tworzącą rozmiaru $Rn \times n$ i rzędu Rn dla kodu, w którym waga każdego słowa jest co najmniej δn. Dla ustalonej macierzy tworzącej G rozmiaru $Rn \times n$, słowa kodowe to liniowe kombinacje wierszy G, które w przypadku arytmetyki w $\mathbb{F}_2$ odpowiadają podzbiorom zbioru numerów wierszy $[1..Rn]$. Takich podzbiorów jest 2^{Rn}. Słów długości n o wadze nie większej niż δn jest

$$\sum_{0 \le i \le \delta n} \binom{n}{i} \le 2^{n\mathrm{H}(\delta)} \ .$$

Stąd jest nie więcej niż $2^{n\mathrm{H}(\delta)}$ kodów, w których takie słowa istnieją. Razem jest nie więcej niż $2^{Rn} \cdot 2^{n\mathrm{H}(\delta)}$ słów w takich kodach. Pozostaje zbiór słów X liczności

$$2^n - 2^{Rn+\mathrm{H}(\delta)n} = 2^n - 2^{\alpha n} \ ,$$

gdzie $\alpha = 1 - \mathrm{H}(\delta) - R$. W zbiorze słów X istnieje Rn słów liniowo niezależnych, bowiem zbiór liniowych kombinacji $Rn - 1$ wektorów ma liczność 2^{Rn-1}, co jest mniejsze od $2^n - 2^{\alpha n}$, dla dostatecznie dużego n. Kod, którego bazą jest owe Rn liniowo niezależnych słów, nie zawiera żadnego słowa o wadze mniejszej lub równej δn.

Ograniczenie Gilberta-Varshamova implikuje istnienie ciągu asymptotycznie dobrych kodów binarnych. Opiszemy teraz metodę zbudowania takich kodów. Niech $\mathcal{C}$ będzie kodem $\mathrm{RS}(n,k)$ nad $\mathbb{F}_q$, gdzie $q = 2^m$. Niech α ustalony element pierwotny $\mathbb{F}_q$. Słowo kodowe $c \in \mathcal{C}$ jest ciągiem $\langle c_1, \ldots, c_n \rangle$, gdzie $c_i \in \mathbb{F}_q$. Słowu c przyporządkujemy inne słowo $g = \langle g_1, \ldots, g_{2i} \rangle$, w którym $g_{2i-1} = c_i$ oraz $g_{2i} = \alpha^i \cdot c_i$, dla $1 \le i \le n$. Następnie g przekształcamy na słowo binarne h przez rzutowanie, takie h ma długość $2 \cdot m \cdot n$. Słowa h tej postaci tworzą *kod Justesena* $J(n,k)$, dla odpowiedniego m. Długość $J(n,k)$ jest równa $2 \cdot m \cdot n$. Jest to kod liniowy wymiaru $m \cdot k$. Niech R będzie stałą taką, że $0 < R < 1/2$. Dla każdego m określamy kod $\mathcal{C}_n$ jako kod Justesena $J(n,k)$ otrzymany z kodu $\mathrm{RS}(n,k)$ nad $\mathbb{F}_{2^m}$ o parametrach $n = 2^m - 1$ i $k = \lceil 2 \cdot R \cdot n \rceil$. Niech R_n to zawartość informacji $\mathcal{C}_n$. Mamy

$$R_n = \frac{m \cdot k}{2 \cdot m \cdot n} = \frac{k}{2 \cdot n} = \frac{\lceil 2 \cdot R \cdot n \rceil}{2 \cdot n} \ge R \ .$$

Oszacujemy teraz δ_n równe minimalnej względnej odległości $\mathcal{C}_n$. Słowo $c \in \mathcal{C}_n$, $c \neq 0$, zawiera co najmniej $n - k + 1$ niezerowych rozłącznych podsłów binarnych długości $2m$ (*podsłowem* słowa w jest ciąg kolejnych symboli w) otrzymanych z rzutowania par $\langle g_{2i-1}, g_{2i} \rangle$. Zauważmy, że są one różne między sobą, bowiem $\alpha^i = g_{2i}/g_{2i-1}$. Niech T oznacza zbiór takich słów długości $2m$ dla ustalonego c. Niech $l = 2m$. Podzbiór T złożony ze słów wagi nie większej niż ϵl liczy nie więcej niż $\sum_{i=1}^{\epsilon l} \binom{l}{i} \le 2^{l\mathrm{H}(\epsilon)}$ elementów, dla $0 < \epsilon < 1$. Zatem suma wag słów w T jest równa co najmniej $\epsilon \cdot l\big(|T| - 2^{l\mathrm{H}(\epsilon)}\big)$. Mamy

$$|T| \ge n - k + 1 = n - \lceil 2 \cdot r \cdot n \rceil + 1 \ge n \cdot (1 - 2R) \ .$$

Waga c jest równa sumie wag słów w T i wynosi co najmniej

$$\epsilon 2m(n(1-2R) - 2^{2m\mathrm{H}(\epsilon)}) = \epsilon 2m(n(1-2R) - (n+1)^{2\mathrm{H}(\epsilon)}) \ .$$

Wybierzmy ϵ takie, żeby $2\mathrm{H}(\epsilon) < 1$. Wtedy mamy

$$\delta_n \geq \frac{\epsilon 2m(n(1-2R) - (n+1)^{2\mathrm{H}(\epsilon)})}{2mn} \geq \epsilon_0(1-2R) \ ,$$

gdzie stała ϵ_0 nie zależy od m. To wszystko razem pokazuje, że ciąg $\langle \mathcal{C}_n \rangle$ jest asymptotycznie dobry.

Kody ekspanderowe. Dla wszystkich dotychczas przedstawionych kodów nie są znane algorytmy kodowania lub odkodowywania, których czas działania byłby proporcjonalny do długości słowa kodowego. Przedstawimy teraz kody i algorytm odkodowywania działający w czasie liniowym.

Niech $G = \langle V, E \rangle$ graf prosty. Zbiór sąsiadów wierzchołków z $A \subseteq V$ oznaczamy przez $\mathrm{S}(A)$. Powiemy, że *każdy podzbiór o co najwyżej m wierzchołkach rozszerza sią o czynnik* $\beta > 1$, gdy $|\mathrm{S}(A)| > \beta \cdot |A|$ dla każdego $A \subseteq V$ takiego, że $|A| \leq m$. Grafy, które mają własność rozszerzania nazywa sie *ekspanderami*. Graf dwudzielny $\langle V_1 \cup V_2, E \rangle$ jest (f,g)-*regularny* gdy wierzchołki V_1 są stopnia f, a V_2 są stopnia g. Stąd, jeżeli $|V_1| = k$ to $|V_2| = \frac{f}{g} \cdot k$. Wierzchołki stopnia f nazywamy *zmiennymi* a stopnia g *warunkami*. Niech G będzie grafem (f,g)-regularnym o n zmiennych. Powiemy, że jest on (f,g,ϵ,β)-*ekspanderem* gdy każdy zbiór co najwyżej $\epsilon \cdot n$ zmiennych rozszerza się o czynnik β.

Opiszemy kody binarne $\mathcal{C}(G,\mathcal{B})$ gdzie G jest (f,g)-regularny a $\mathcal{B}$ jest binarnym liniowym kodem o długości g. Długość n kodu $\mathcal{C}(G,\mathcal{B})$ jest równa liczności zbioru zmiennych G. Oto definicja: $c = c_1, \ldots, c_n \in \mathcal{C}(G,\mathcal{B})$ w.t.w. gdy dla każdego warunku t, jeżeli $v_{i_1}, \ldots, v_{i_g}$ są zmiennymi sąsiadującymi z t to $c_{i_1}, \ldots, c_{i_g} \in \mathcal{B}$. Zauważmy, że kod $\mathcal{C}(G,\mathcal{B})$ też jest kodem liniowym, bowiem jest zdefiniowany przez koniunkcję liniowych warunków.

Niech G będzie $(f,g,\epsilon,\frac{f}{g\delta})$-ekspanderem, $\mathcal{B}$ kodem długości g, zawartości informacji $R > (f-1)/f$ i minimalnej względnej odległości δ. Pokażemy, że wtedy kod $\mathcal{C}(G,\mathcal{B})$ ma zawartość informacji co najmniej $f \cdot R - f + 1$ i minimalną względną odległość co najmniej ϵ. Każdy warunek daje $(1-R)g$ wierszy do macierzy kontroli parzystości, która razem ma ich $n \cdot \frac{f}{g}(1-R) \cdot g = f(1-R)$. Stąd wymiar $\mathcal{C}(G,\mathcal{B})$ równy co najmniej $n - fn(1-R) = n(fR - f + 1)$. Oszacujemy minimalną odległość $\mathcal{C}(G,\mathcal{B})$. Niech $c \neq 0$ słowo kodowe o wadze nie większej niż $\epsilon \cdot n$. Niech J to zbiór zmiennych w c o wartościach równych 1. Zbiór J ma więcej niż $\frac{f}{g \cdot \delta} \cdot |J|$ sąsiadów z własności rozszerzania ekspandera. Istnieje warunek sąsiadujący z mniej niż $g \cdot \delta$ zmiennymi z J, ponieważ $f \cdot |J|$ krawędzi jest incydentnych z J. To jest sprzeczne z założeniem, że δ to minimalna względna odległość $\mathcal{B}$. Zatem każde niezerowe słowo kodowe ma wagę większą niż $\epsilon \cdot n$.

Niech $\mathcal{E}$ będzie kodem kontroli parzystości, to znaczy słowa kodowe mają parzystą sumę bitów. Rozważymy kody postaci $\mathcal{C}(G,\mathcal{E})$. Powiemy, że warunek G jest *spełniony* przez wartościowanie zmiennych gdy suma wartości zmiennych sąsiadujących z warunkiem jest parzysta. Oto algorytm odkodowywania dla $\mathcal{C}(G,\mathcal{E})$: Jeżeli istnieje zmienna, która sąsiaduje z większa liczbą nie spełnionych niż spełnionych warunków to zamień wartość tej zmiennej; powtarzaj aż nie będzie takiej zmiennej.

Pokażemy, że jeżeli G jest $(f,g,\epsilon,\frac{3}{4}f)$-ekspanderem to algorytm poprawnie odkoduje słowo, w którym nie więcej niż $\epsilon n/2$ błędów. Weźmy słowo odległe o nie więcej niż $\epsilon n/2$

od słowa kodowego. Powiemy, że zmienne o nieprawidłowych wartościach są *zepsute*. Niech z oznacza liczbę takich zmiennych, s liczbę spełnionych warunków sąsiadujących z co najmniej jedną zepsutą zmienną. Niech u oznacza liczbę niespełnionych warunków. Własność rozszerzania daje $u + s > \frac{3}{4} \cdot z$. Każdy spełniony warunek sąsiadujący z zepsutą zmienną musi sąsiadować z jeszcze inną taką, stąd mamy $u + 2s \leq f \cdot z$. Razem te nierówności dają

$$\frac{f \cdot z}{2} < u \ . \tag{1}$$

Każdy niespełniony warunek sąsiaduje z zepsutą zmienną. Zatem istnieje zepsuta zmienna, której więcej niż połowa sąsiadujących warunków nie jest spełnionych. To wszystko zachodzi o ile $z \leq \epsilon \cdot n$. Pokażemy, że ten warunek jest zawsze spełniony. Mianowicie: na początku $u \leq f\epsilon n/2$, a gdyby z osiągnęła kiedykolwiek wartość ϵn to nierówność (1) dałaby $u > f\epsilon n/2$, co jest sprzeczne z tym, że u się zmniejsza.

Załóżmy, że mamy rodzinę grafów G_n, które są $(f, g, \epsilon, \frac{3}{4}f)$-ekspanderami, i G_n ma n zmiennych. Odpowiada jej rodzina kodów $\mathcal{C}_n = \mathcal{C}(G_n, \mathcal{E})$. Algorytm odkodowywania zastosowany do $\mathcal{C}_n$ można zaimplementować tak, by działał w czasie $\mathcal{O}(n)$. Istnieją takie grafy G_n, ale nie są znane ich deterministyczne konstrukcje. Podobny efekt można otrzymać konstruktywnie biorąc gorsze ekspandery, które wiadomo jak zbudować, za to kody lepsze niż $\mathcal{E}$.

Zadania

1. Pokaż, że jeżeli $M \cdot K_q(n, d-1) \leq q^n$ to istnieje kod typu (n, M, d) nad alfabetem A o q symbolach.
   Wskazówka: Niech $\mathcal{C}$ maksymalny kod typu (n, M', d). Każde słowo z A^n jest w odległości mniejszej niż d od pewnego słowa z $\mathcal{C}$.

2. Pokaż, że jeżeli $K_q(n, d-1) < q^{n-k+1}$ to istnieje kod typu $[n, k, d]$ nad alfabetem o q symbolach. *Wskazówka:* Kod typu $[n, k-1, d]$ ma liczność q^{k-1}, o ile istnieje.

3. Niech α element pierwotny ciała $\mathrm{GF}(2^k)$ i $n = 2^k - 1$. Niech H będzie macierzą binarną rozmiaru $2k \times n$, w której i-tą kolumną jest $\langle \alpha^i, \alpha^{3i} \rangle^T$. Jakiego typu jest binarny kod, którego H jest macierzą kontroli parzystości? Czy jest to kod BCH?

4. Pokaż, że kody Hamminga są kodami BCH.

5. Rozważmy operację zmiany kodu binarnego $\mathcal{C}$ na inny przez dopisanie bitu parzystości na końcu każdego słowa kodowego w $\mathcal{C}$. Czy ta operacja zachowuje liniowość i cykliczność? Jak wpływa na minimalną odległość kodu?

6. Znajdź macierz odwrotną do A określającej DTF.

7. Pokaż, że DTF i przekształcenie odwrotne można wykonać za pomocą $\mathcal{O}(q \log q)$ operacji ciała $\mathbb{F}_q$. Załóż, że $q = 2^i$.
   Wskazówka: sprowadź problem rekurencyjnie do obliczania wartości wielomianu w parzystych potęgach α.

8. Znajdź macierz tworzącą dla kodu RS(n,k).

9. Pokaż jak kodować kody RS(n,k) za pomocą $\mathcal{O}(n \log n)$ operacji ciała.

10. Znajdź macierz kontroli parzystości dla kodu RS$(3,2)$ nad $\mathbb{F}_4$.

11. Przekształćmy kod RS(n,k) przez dodanie na końcu każdego słowa kodowego symbolu tak, by suma wszystkich symboli w otrzymanym słowie była równa 0. Pokaż, że minimalna odległość zwiększy się i dostaniemy kod typu $[n+1, k, n-k+2]$.

12. Czy rzutowanie zawsze przekształca kody cykliczne na cykliczne?

13. Czy ideał w $\mathbb{F}[x]$ ograniczony do wielomianów stopnia $\leq n$ jest kodem cyklicznym?

14. Uzasadnij dlaczego kody RS są cykliczne.

15. Rozważmy metodę rozpraszania informacji kodującą dane rozmiaru l jako $m = 10$ pakietów, gdzie każde $k = 5$ z nich pozwala odtworzyć dane. Oszacuj łączny rozmiar takich 10 pakietów względem l.

16. Rozważmy metode rozpraszania informacji przy ustalonych l, m, k. Plik długości n dzielimy na słowa długości l i każde kodujemy jako m pakietów. Wszystkie pakiety wysyłamy siecią, odbiorca dostaje je w dowolnej kolejności, niektóre być może są tracone. Jaką dodatkową informację powinne nieść pakiety? Oszacuj łączny rozmiar użytych pakietów względem n.

17. Niech H macierz kontroli parzystości kodu $\mathcal{C}$ typu $[n,k]$. Pokaż równoważność: $\mathcal{C}$ jest optymalny w.t.w. gdy każde $n-k$ kolumny H są liniowo niezależne.

18. Niech grafy G_n będą $(f, g, \epsilon, \frac{3}{4}f)$-ekspanderami i G_n ma n zmiennych. Odpowiada jej rodzina kodów $\mathcal{C}_n = \mathcal{C}(G_n, \mathcal{E})$. Pokaż, że algorytm odkodowywania kodów $\mathcal{C}_n$ można zaimplementować tak, aby działał w czasie liniowym. Oszacuj zawartośc informacji i minimalną odległość kodów $\mathcal{C}_n$. Czy te kody są asymptotycznie dobre?

MMD Wykład 9.

Bogdan Chlebus

Funkcje tworzące i prawdopodobieństwo. Niech X zmienna losowa o wartościach całkowitych nieujemnych. Funkcję tworzącą ciągu $\langle \mathsf{P}[X=i] \rangle_{i \geq 0}$, to znaczy

$$\sum_{i=o}^{\infty} t^i \cdot \mathsf{P}[X=i] = \mathsf{E}\,[t^X] \ ,$$

oznaczamy przez $F_X(t)$ i nazywamy *funkcją tworzącą prawdopodobieństwa zmiennej* X. Szereg potegowy określający F_X ma promien zbieżności co najmniej 1. Jak wiadomo z analizy, funkcja rozwijalna w szereg potęgowy ma jedno rozwinięcie, stąd funkcja tworząca prawdopodobieństwa X wyznacza jednoznacznie rozkład X. Różniczkując k razy $F_X(t)$ dostajemy:

$$F_X^{(k)} = \sum_{i=0}^{\infty} t^{i-k} \cdot i(i-1) \cdot \ldots \cdot (i-k+1) \cdot \mathsf{P}[X=i] \ . \tag{1}$$

Szereg (1), czyli $\mathsf{E}\,[t^{X-k} X(X-1)\cdots(X-k+1)]$, może być rozbieżny dla $t=1$, ale na mocy twierdzenia Abela zawsze zachodzi równość $\lim_{t \uparrow 1} F_X^{(k)}(t) = \mathsf{E}\,[X(X-1)\cdots(X-k+1)]$, gdzie $\lim_{t \uparrow a}$ oznacza granicę lewostronną w punkcie a. Przyjmujemy, że odtąd $F_X^{(k)}(1)$ jest skrótem $\lim_{t \uparrow 1} F_X^{(k)}(t)$, co obejmuje przypadek, gdy ta wielkość jest nieskończona.

Zachodzą nastęoujące dwa użyteczne wzory, gdzie $F = F_X$:

$$\mathsf{E}\,X = \sum_{i=0}^{\infty} i \cdot \mathsf{P}[X=i] = F'(1) \ , \tag{2}$$

$$\mathrm{Var}\,X = \mathsf{E}\,X^2 - (\mathsf{E}\,X)^2 = \mathsf{E}\,[X(X-1)+X] - (\mathsf{E}\,X)^2 = F''(1) + F'(1) - (F'(1))^2. \tag{3}$$

Przykład. Rozważmy nieskończony ciąg prób Bernoulli'ego. Niech $X=k$ gdy przy k-tej próbie dostajemy pierwszy sukces. Rozkład X dany wzorem

$$\mathsf{P}[X=k] = p(1-p)^{k-1} \ ,$$

dla $k = 1, 2, \ldots$ oraz $0 < p < 1$, nazywamy *rozkładem geometrycznym*. Obliczymy wartość oczekiwaną i wariancję dla takiej zmiennej X. Oznaczmy $q = 1-p$. Najpierw znajdziemy funkcję tworzącą $F = F_X$:

$$F(t) = \sum_{k=1}^{\infty} t^k p q^{k-1} = pt + pqt^2 + pq^2t^3 + \cdots = pt(1 + qt + q^2t^2 + \cdots) = \frac{pt}{1-qt} \ ,$$

dla $|qt| < 1$. Stąd

$$F'(t) = \frac{p(1-qt)+qpt}{(1-qt)^2} = \frac{p}{(1-qt)^2} \ ,$$

i dostajemy $\mathsf{E}\,X = F'(1) = p(1-q)^{-2} = 1/p$. Podobnie $F''(t) = 2pq(1-qt)^{-3}$ oraz $F''(1) = 2qp^{-2}$. Podstawiamy:

$$\mathrm{Var}\,X = F''(1) + F'(1) - (F'(1))^2 = 2qp^{-2} + p^{-1} - p^{-2} = qp^{-2} \ .$$

$\Diamond$

Przykład: Rozważmy rozkład zmiennej X_n równej sumie n niezależnych zmiennych o takim samym rozkładzie geometrycznym, czyli rozkład czasu oczekiwania na n-ty sukces w nieskończonym ciągu prób Bernoulli'ego. Rozkład jest dany wzorem

$$\mathsf{P}[X_n = k] = \binom{k-1}{n-1} p^n (1-p)^{k-n} \ ,$$

dla $k = n, n+1, \ldots$. Zmienna Y_n ma rozkład *ujemny dwumianowy*, jeżeli $\mathsf{P}[Y_n = k] = \mathsf{P}[X_n = n+k]$, dla k calkowitej nieujemnej. To prawdopodobieństwo można przekształcić przez negowanie górnego wskaźnika:

$$\begin{aligned} \binom{n+k-1}{n-1} p^n (1-p)^k &= \binom{n+k-1}{k} p^n (1-p)^k \\ &= \binom{-n}{k} p^n (-q)^k = \binom{-n}{k} \left(\frac{-q}{p}\right)^k \left(\frac{1}{p}\right)^{-n-k} \ , \end{aligned}$$

gdzie $q = 1-p$, co formalnie przypomina postać wzoru na k sukcesów w *ujemnej* liczbie $-n$ prób Bernoulli'ego, z *ujemną* liczbą $-q/p$ jako prawdopodobieństwem sukcesu. Co więcej: $\mathsf{E}\, Y_n = (-n)(-q/p)$ oraz $\operatorname{Var} Y = (-n)(-q/p)(1/p)$ – ćwiczenie. $\Diamond$

Jeżeli X i Y są niezależne, to zachodzi

$$F_{X+Y}(t) = \mathsf{E}\,[t^{X+Y}] = \mathsf{E}\,[t^X \cdot t^Y] = \mathsf{E}\, t^X \cdot \mathsf{E}\, t^Y = F_X \cdot F_Y \ , \tag{4}$$

ponieważ t^X i t^Y są niezależne. Niech $X_0, X_1, \ldots$ ciag niezaleznych zmiennych losowych o wartościach całkowitych nieujemnych i takim samym rozkladzie jak pewna zmienna X, oraz Y zmienna losowa o wartościach całkowitych nieujemnych niezależna od kazdego X_i. Niech zmienna losowa Z będzie *losową sumą* $X_0 + X_1 + \ldots$ *o długości wyznaczonej przez zmienną* Y, to znaczy $Z = X_0 + X_1 + \cdots X_Y$. Pokażemy, że $F_Z = F_Y(F_X)$. Zacznijmy od

$$\mathsf{P}[Z = k] = \sum_{i=0}^{\infty} \mathsf{P}[Y = i] \cdot \mathsf{P}[X_1 + \cdots X_i = k] \ ,$$

co wynika ze wzoru na prawdopodobieństwo całkowite i niezależności. Funkcja tworząca:

$$\begin{aligned} F_Z &= \sum_{k=0}^{\infty} t^k \cdot \mathsf{P}[Z = k] = \sum_{k=0}^{\infty} t^k \cdot \sum_{i=0}^{\infty} \mathsf{P}[Y = i] \cdot \mathsf{P}[X_0 + \cdots + X_i = k] \\ &= \sum_{i=0}^{\infty} \mathsf{P}[Y = i] \cdot \sum_{k=0}^{\infty} t^k \cdot \mathsf{P}[X_0 + \cdots + X_i = k] = \sum_{i=0}^{\infty} \mathsf{P}[Y = i] \cdot F_X^i(t) = F_Y(F_X(t)) \ , \end{aligned}$$

gdzie skorzystaliśmy z (4). To pozwala obliczyć wartość oczekiwaną Z. Mianowicie:

$$\mathsf{E}\, Z = F_Z'(1) = F_X'(1) \cdot F_Y'(F_X(1)) = F_X'(1) \cdot F_Y'(1) = \mathsf{E}\, X \cdot \mathsf{E}\, Y \ ,$$

o ile $\mathsf{E}\, X$ i $\mathsf{E}\, Y$ istnieją. Jeżeli $Z = X_1 + \ldots + X_Y$ oraz wszystkie X_i mają taki sam rozkład jak pewna X, to równość $\mathsf{E}\, Z = \mathsf{E}\, X \cdot \mathsf{E}\, Y$ nazywamy *równaniem Walda*. Można ją pokazać osłabiając założenie, że Y jest niezależna od zmiennych X_i. Powiemy, że zmienna

Y o wartościach całkowitych dodatnich jest *czasem zatrzymania dla ciągu zmiennych losowych* $\langle X_i\rangle_{i\geq 1}$, gdy każde zdarzenie $Y = n$ jest wyznaczone przez wartości $X_1, \ldots, X_n$, to znaczy gdy możemy określić czy $Y = n$ zachodzi czy nie znając $X_1, \ldots, X_n$. (Na przykład: rzucamy monetą symetryczną aż do chwili wyrzucenia dziesiątego orła; niech X_i mają rozkłady Bernoulli'ego, $X_i = 1$ gdy wynikiem i-tego rzutu jest orzeł, Y równy najmniejszemu n takiemu, że $X_1 + \ldots + X_n = 10$.) Niech $\langle X_i\rangle_{i\geq 1}$ ciąg niezależnych zmiennych losowych i Y czas zatrzymania dla tego ciągu. Rozważmy zmienną losową o wartościach 0 lub 1 równą $[Y = n]$, gdzie nawiasy kwadratowe w takim kontekście oznaczają notację Iversona. Wtedy jest ona niezależna od ciągu zmiennych $X_{n+1}, X_{n+2}, \ldots$. Rzeczywiście: $[Y = n]$ jest wyznaczona przez $X_1, \ldots, X_n$, które są niezależne od X_i dla $i > n$. Pokażemy, że jeżeli $\langle X_i\rangle_{i\geq 1}$ jest ciągiem niezależnych zmiennych losowych o takim samym rozkładzie jak X i skończonej wartości oczekiwanej, oraz Y jest czasem zatrzymania dla $\langle X_i\rangle_{i\geq 1}$, gdzie istnieje wartość oczekiwana Y, to zachodzi równanie Walda dla losowej sumy $Z = X_1 + \ldots + X_Y$. Dla dowodu przekształćmy równanie Walda:

$$\begin{aligned}\mathsf{E}\,X \cdot \mathsf{E}\,Y &= \mathsf{E}\,X \cdot \sum_{i\geq 1} \mathsf{P}[Y \geq i] = \mathsf{E}\,X \cdot \sum_{i\geq 1} \mathsf{E}\,[Y \geq i] = \sum_{i\geq 1} \mathsf{E}\,X \cdot \mathsf{E}\,[Y \geq i] \\ &= \sum_{i\geq 1} \mathsf{E}\,X_i \cdot \mathsf{E}\,[Y \geq i] = \sum_{i\geq 1} \mathsf{E}\,X_i \cdot [Y \geq i]\ ,\end{aligned}$$

gdzie ostatnia równość na mocy niezależności X_i od $[Y \geq i] = \prod_{k=1}^{i-1}(1 - [Y = k])$, co jest prawdą jako że X_i niezależna od $[Y = k]$ dla $k < i$. Teraz zmieniamy kolejność sumowania:

$$\sum_{i\geq 1} \mathsf{E}\,X_i \cdot [Y \geq i] = \mathsf{E} \sum_{i\geq 1} X_i \cdot [Y \geq i] = \mathsf{E}\,Z\ ,$$

co jest poprawne na mocy bezwzględnej zbieżności szeregów $\mathsf{E}\,X_i \cdot [Y \geq i]$.

Nierówności. Niech X zmienna losowa i niech f niemalejąca funkcja o wartościach dodatnich. Zachodzą nierówności:

$$\mathsf{E}\,f(X)\ \geq\ \mathsf{P}[f(X) \geq f(a)] \cdot f(a)\ \geq\ \mathsf{P}[X \geq a] \cdot f(a)\ .$$

Stąd dostajemy *nierówność Markowa:*

$$\mathsf{P}[X \geq a] \leq \frac{\mathsf{E}\,f(X)}{f(a)}\ .$$

Jeżeli X jest nieujemna a f jest identycznością, to dostajemy następujący szczególny przypadek tej nierówności: $\mathsf{P}[X \geq a] \leq \frac{\mathsf{E}\,X}{a}$. Niech $\mathsf{E}\,X = \mu$ oraz $\operatorname{Var} X > 0$. Niech $\sigma \geq 0$ *odchylenie standardowe* X, to znaczy $\sigma^2 = \operatorname{Var} X$. Stosując nierówność Markowa do zmiennej $(X - \mu)^2$ dostajemy nierówność

$$\mathsf{P}[|X - \mu| \geq t\sigma] = \mathsf{P}[(X - \mu)^2 \geq t^2\sigma^2] \leq \mathsf{E}\,(X - \mu)^2/t^2\sigma^2 = 1/t^2\ ,$$

zwaną *nierównością Czebyszewa.*

Przykład: Niech $S_n = \sum_{i=1}^n X_i$ będzie sumą zmiennych niezależnych X_i, z których każda ma wartość oczekiwaną μ oraz wariancję σ^2. Wtedy $\mathsf{E}\,S_n/n = \mu$ oraz $\operatorname{Var}(S_n/n) = \sigma^2/n$.

Z nierówności Czebyszewa mamy

$$\mathsf{P}\Big[\Big|\frac{S_n}{n} - \mu\Big| \geq a\Big] \leq \frac{\mathrm{Var}\,(S_n/n)}{a^2} = \frac{\sigma^2}{n \cdot a^2} \ .$$

Dostajemy, że $\lim_{n\to\infty} \mathsf{P}[|\frac{S_n}{n} - \mu| \geq a] = 0$, co nazywa się *słabym prawem wielkich liczb*. *Mocne prawo wielkich liczb*, które otrzymujemy ze słabego zamieniając miejscami P i $\lim_{n\to\infty}$ też jest prawdziwe, ale nie będziemy tego pokazywać. $\Diamond$

Niech X zmienna losowa, rozważmy szereg $M_X(t)$ określony następująco:

$$M_X(t) = \mathsf{E}\, e^{tX} = \sum_{\omega\in\Omega} \mathsf{P}[\omega] \cdot e^{t\cdot X(\omega)} = \sum_{\omega\in\Omega} \mathsf{P}[\omega] \cdot \sum_{k\geq 0} \frac{t^k X^k(\omega)}{k!} \ .$$

Załóżmy, że powyższy szereg iterowany jest zbieżny bezwzględnie, wtedy możemy zmienić kolejność sumowania i dostajemy:

$$M_X(t) = \sum_{k\geq 0} \frac{1}{k!} \sum_{\omega\in\Omega} \mathsf{P}[\omega] \cdot (t \cdot X(\omega))^k = \sum_{k\geq 0} \frac{t^k}{k!} \cdot \mathsf{E}\, X^k \ .$$

Liczbę $\mathsf{E}\, X^k$ nazywamy *k-tym momentem* zmiennej losowej X, stąd $M_X(t)$ jest wykładniczą funkcją tworzącą ciągu momentów X, nazywaną *funkcją tworzącą momentów* X. Jeżeli $M_X(t)$ ma niezerowy promień zbieżności, to różniczkując dostajemy $\mathsf{E}\, X^k = M_X^{(k)}(0)$. Jeżeli $X = X_1 + X_2$ gdzie X_1 i X_2 niezależne, to

$$M_X(t) = \mathsf{E}\, e^{tX} = \mathsf{E}\, e^{tX_1 + tX_2} = \mathsf{E}\,(e^{tX_1} \cdot e^{tX_2}) = \mathsf{E}\, e^{tX_1} \cdot \mathsf{E}\, e^{tX_2} = M_{X_1}(t) \cdot M_{X_2}(t) \ . \quad (5)$$

Zastosujemy nierówność Markowa do funkcji tworzącej momentów kładąc $f(x) = e^{s\cdot x}$, dla parametru $s \geq 0$. Dostajemy $\mathsf{P}[X \geq a] \leq e^{-sa} \cdot M_X(s)$. Biorąc kres dolny prawej strony dostajemy *nierówność Chernoffa*:

$$\mathsf{P}[X \geq a] \leq \inf_{s\geq 0} e^{-sa} \cdot M_X(s) \ . \quad (6)$$

Staje się ona użyteczna, gdy prawą stronę przekształcimy do zamkniętej postaci, to znaczy oszacujemy przez liczbę niezależną od s. Zauważmy, że każdy wybór wartości s daje szacowanie lewej strony.

Przykład: Niech $X_1, \ldots, X_n$ będą niezależnymi zmiennymi o takim samym rozkładzie $\mathsf{P}[X_i = 1] = \mathsf{P}[X_i = -1] = 1/2$. Rozważamy $X = X_1 + \ldots + X_n$. Mamy

$$M_{X_i}(s) = \mathsf{E}\,[e^{sX_i}] = \frac{1}{2}e^s + \frac{1}{2}e^{-s} \leq e^{s^2/2} \ ,$$

gdzie nierówność można sprawdzić na przykład z rozwinięcia w szereg. Stąd $M_X(t) = \prod_{i=1}^n M_{X_i}(t) \leq e^{s^2 n/2}$, gdzie skorzystaliśmy z (5). Z nierówności Chernoffa mamy

$$\mathsf{P}[X \geq a] \leq e^{-sa + s^2 n/2} \leq e^{-a^2/2n} \ ,$$

gdzie położyliśmy $s = a/n$. Dla $a = n^{3/4}$ dostajemy $\mathsf{P}[X \geq n^{3/4}] \leq e^{-\sqrt{n}/2}$, co jest silnym wykładniczym szacowaniem. Porównajmy, co dałaby nam w tej sytuacji nierówność

Czebyszewa. Mamy $\mathsf{E}\,X = 0$ i $\mathrm{Var}\,X = n$, co daje $\mathsf{P}[|X| > t \cdot \sqrt{n}] \leq t^{-2}$. Dla $t = n^{1/4}$ dostajemy $\mathsf{P}[|X| \geq n^{3/4}] \leq 1/\sqrt{n}$, co jest znacznie słabszym wielomianowym szacowaniem. Możemy także zastosować nierówność Markowa bezpośrednio, w tym celu rozważmy zmienne $Y_i = X_i + 1$ o rozkładzie Bernoulli'ego. Niech $Y = \sum_{1 \leq i \leq n} Y_i$, mamy $\mathsf{E}\,Y = n$. Korzystając z nierówności Markowa dostajemy

$$\mathsf{P}[X \geq a] = \mathsf{P}[Y \geq n + a] \leq \frac{\mathsf{E}\,Y}{n + a} = \frac{n}{n + a} \ .$$

Dla $a = n^{3/4}$ dostajemy ograniczenie $\frac{1}{1+n^{-1/4}}$, które zbiega do 1, i jest jeszcze słabsze. $\Diamond$

Wyprowadzimy nierówność Chernoffa dla *ciągu prób Poissona*, czyli dla zmiennej $X = \sum_{i=1}^{n} X_i$, gdzie $X_1, \ldots, X_n$ są niezależne, oraz $\mathsf{P}[X_i = 1] = p_i$, $\mathsf{P}[X_i = 0] = 1 - p_i$. Niech $Y = \sum_{i=1}^{n} Y_i$, gdzie Y_i niezależne, $\mathsf{P}[Y_i = 1 - p_i] = p_i$, $\mathsf{P}[Y_i = -p_i] = 1 - p_i$. Zachodzi $\mathsf{E}\,Y = 0$ bowiem $Y = X - \mu$, gdzie $\mu = \mathsf{E}\,X = \sum_{i=1}^{n} p_i$. Niech $a > 0$.

$$\mathsf{P}[Y \geq a] \leq e^{-sa}\,\mathsf{E}\,[e^{sY}] = e^{-sa}\,\mathsf{E}\,[\prod_{i=1}^{n} e^{sY_i}] = e^{-sa} \prod_{i=1}^{n} \mathsf{E}\,[e^{sY_i}] \ . \tag{7}$$

Oszacujemy wartość oczekiwaną e^{sY_i}:

$$\begin{aligned} \mathsf{E}\,e^{sY_i} &= p_i e^{s(1-p_i)} + (1 - p_i)e^{-sp_i} = e^{-sp_i}(1 + p_i(e^s - 1)) \\ &\leq e^{-sp_i} \exp(p_i(e^s - 1)) = \exp(p_i(e^s - s - 1)) \ , \end{aligned}$$

co razem daje

$$\prod_{i=1}^{n} \mathsf{E}\,e^{sY_i} \leq \exp(\sum_{i=1}^{n} p_i(e^s - s - 1)) = \exp(\mu(e^s - s - 1)) \ .$$

Podstawiamy do (7) i dostajemy

$$\mathsf{P}[Y \geq a] \leq \exp(-sa + \mu(e^s - s - 1)) \leq \exp(-(a + \mu)\ln\Big(1 + \frac{a}{\mu}\Big) + a) \ ,$$

gdzie przyjęliśmy $s = \ln\big(1 + \frac{a}{\mu}\big)$. Niech $a = \epsilon\mu$ i $b = 1 + \epsilon$. Podstawiając dostajemy:

$$\mathsf{P}[X \geq b \cdot \mu] = \mathsf{P}[Y \geq a] \leq \exp(-\mu(1 - b + b\ln b) \ . \tag{8}$$

Jeżeli $0 < \epsilon < 1$ to możemy skorzystać z nierówności $-\epsilon + (1 + \epsilon)\ln(1 + \epsilon) > \epsilon^2/3$, którą można sprawdzić na przykład z rozwinięcia w szereg $\ln(1 + \epsilon)$, wtedy dostajemy:

$$\mathsf{P}[X \geq (1 + \epsilon)\mu] \leq e^{-\epsilon^2\mu/3} \ . \tag{9}$$

Teraz oszacujemy w drugą stronę. Początek jest podobny:

$$\mathsf{P}[Y \leq -a] = \mathsf{P}[-Y \geq a] \leq e^{-sa}\,\mathsf{E}\,[e^{-sY}] = e^{-sa}\,\mathsf{E}\,\Big[\prod_{i=1}^{n} e^{-sY_i}\Big] = e^{-sa} \prod_{i=1}^{n} \mathsf{E}\,[e^{-sY_i}] \ . \tag{10}$$

Zachodzi

$$\mathsf{E}\,e^{-sY_i} = p_i e^{-s(1-p_i)} + (1 - p_i)e^{sp_i} = e^{sp_i}(1 + p_i(e^{-s} - 1))$$

$$\leq e^{sp_i} \exp(p_i(e^{-s} - 1)) = \exp(p_i(e^{-s} + s - 1)) \ ,$$

gdzie skorzystaliśmy z nierówności $1 + x \leq e^x$. To prowadzi do szacowania

$$\prod_{i=1}^{n} \mathsf{E}\, e^{-sY_i} \leq \prod_{i=1}^{n} \exp(p_i(e^{-s} + s - 1)) = \exp(\sum_{i=1}^{n} p_i(e^{-s} + s - 1))$$
$$= \exp(\mu(e^{-s} + s - 1)) \leq e^{s^2\mu/2} \ ,$$

gdzie skorzystaliśmy z nierówności $e^{-x} + x - 1 \leq x^2/2$. Kładąc $s = a/\mu$ i podstawiając do (10) dostajemy

$$\mathsf{P}[X - \mu \leq -a] = \mathsf{P}[Y \leq -a] \leq e^{-sa+s^2\mu/2} \leq e^{-a^2/2\mu} \ .$$

Dla $a = \epsilon\mu$ dostajemy

$$\mathsf{P}[X \leq (1 - \epsilon)\mu] \leq e^{-\epsilon^2\mu/2} \ . \tag{11}$$

Szacowania (9) i (11) są wygodne do stosowania gdy X ma rozkład dwumianowy.

Zadania

1. Rzucamy kostką do gry aż do otrzymania dziesiątej szóstki. Oblicz oczekiwaną liczbę rzutów na dwa sposoby: (a) przez rozkład geometryczny; (b) z równania Walda.

2. Znajdź funkcje tworzące prawdopodobienstwa zmiennych o rozkładzie dwumianowym i ujemnym dwumianowym. Wyznacz ich wartosci oczekiwane i wariancje stosując wzory (2) i (3).

3. Urna zawiera b białych i c czarnych kul. Losujemy kule ze zwracaniem (odpowiednio: bez zwracania), aż do wyciągnięcia pierwszej czarnej. Oblicz wartość oczekiwaną liczby wyciągniętych kul.

4. Znajdź rozkład sumy dwóch niezależnych zmiennych losowych o rozkładach Poissona, z parametrami λ_1 i λ_2, odpowiednio.

5. Niech $Z = X_0 + \cdots + X_Y$, gdzie Y i X_i niezalezne, Y ma rozklad Poisson'a a X_i maja ten sam rozklad Bernoulli'ego. Znajdz rozklad Z.

6. Niech zmienna losowa X o wartościach całkowitych dodatnich ma funkcję tworzącą rozkładu prawdopodobieństwa równą $F_X(t) = \sum_{n=0}^{\infty} t^n \cdot \mathsf{P}[X = n]$. Wyraź funkcję tworzącą $G_X(t)$ ciągu $\langle \mathsf{P}[X \geq n] \rangle_n$ przez $F_X(t)$.

7. Znajdź funkcję tworzącą momentów i k-ty moment dla zmiennych o rozkładach: a) Bernoulli'ego; b) dwumianowym; c) geometrycznym; d) Poissona.

8. Czy jeżeli $\mathsf{E}\, X^k$ istnieje, dla $k > 1$, to istnieje także $\mathsf{E}\, X^{k-1}$?

9. Dlaczego w nierówności Chernoffa (6) bierzemy infimum tylko po nieujemnych wartościach s?

10. Niech X zmienna losowa, pokaż równość $\operatorname{Var}(a \cdot X + b) = a^2 \cdot \operatorname{Var} X$.

11. Niech X bedzie sumą n niezależnych zmiennych losowych X_i, gdzie X_i ma rozkład, w którym każda spośród wartości $0, 1, 2, \ldots, m$ jest przyjmowana z takim samym prawdopodobieństwem. Wyprowadź dla X zamkniętą postać nierówności Chernoffa.

12. Wyprowadź zamkniętą postać nierówności Chernoffa dla sumy niezależnych zmiennych losowych, każda o takim samym rozkładzie geometrycznym, odpowiednio Poissona. Porównaj z nierównością Czebyszewa.

13. Dla każdej spośród n kul wybieramy losowo i niezależnie jedną spośród n urn i tam umieszczamy kulę. Pokaż, dla dowolnej stałej $a > 1$, że w każdej urnie jest $\mathcal{O}(\log n / \log \log n)$ kul z prawdopodobieństwem nie mniejszym niż $1 - n^{-a}$.
Wskazówka: skorzystaj z nierówności (8).

14. Funkcja $f : \mathbb{R} \to \mathbb{R}$ jest *wypukła* gdy dla każdej $x \in \mathbb{R}$ istnieje liczba $a(x) \in \mathbb{R}$ taka, że $f(t) \geq f(x) + a(x) \cdot (t - x)$. Pokaż, że jeżeli f jest wypukła i X zmienna losowa to ma miejsce *nierówność Jensena*: $\mathsf{E}\, f(X) \geq f(\mathsf{E}\, X)$.

15. Czy któraś z następujących nierówności $\mathsf{E}\, X^2 \geq (\mathsf{E}\, X)^2$ lub $\mathsf{E}\, X^2 \leq (\mathsf{E}\, X)^2$ jest zawsze prawdziwa?

MMD Wykład 10.

Bogdan Chlebus

Więcej o nierównościach probabilistycznych. Zaczniemy od przykładów.

Przykład: Niech $\mathcal{C}$ kod binarny długości n o minimalnej względnej odległości $\delta < 1$. Zatem każde dwa różne słowa kodowe są odległe o co najmniej $\delta \cdot n$. Niech p będzie prawdopodobieństwem przekłamania przy transmisji bitu. Niech zmienna losowa $X = X_1 + \ldots + X_n$ określona w ten sposób, że X_i równe 1 gdy ma miejsce przekłamanie przy transmisji i-tego bitu słowa kodowego, oraz $X_i = 0$ w przeciwnym przypadku. Oczekiwana liczba przekłamań przy transmisji jednego słowa kodowego równa $\mathsf{E}\, X = p \cdot n$. Załóżmy, że $p < \delta$, niech $\epsilon = \delta - p$. Prawdopodobieństwo błedu odkodowania jest nie większe od prawdopodobieństwa tego, że liczba przekłamań będzie większa od oczekiwanej $p \cdot n$ o $\epsilon \cdot n$. Szacujemy z nierówności Chernoffa:

$$\mathsf{P}[X \geq \mathsf{E}\, X + \epsilon \cdot p \cdot n] \leq e^{-\epsilon^2 \cdot p \cdot n} \leq e^{-(\delta - p)^2 \cdot p \cdot n} \ .$$

Przypuśćmy, że $R < 1 - \mathrm{H}(p)$. Ponieważ $p < \delta$, więc także $1 - \mathrm{H}(p) < 1 - \mathrm{H}(\delta)$. Na mocy ograniczenia Gilberta-Varshamova istnieje (liniowy) binarny kod $\mathcal{C}$ o długości n, zawartości informacji R i minimalnej względnej odległości δ. Dla niego prawdopodobieństwo błędu odkodowania jest nie większe niż $e^{-(\delta - p)^2 \cdot p \cdot n}$, zatem zbiega do 0 przy $n \to \infty$. To razem daje twierdzenie Shannona. Przy okazji widzimy dlaczego asymptotycznie dobre kody są użyteczne: zwiększając długości kodów zmniejszamy do zera (wykładniczo względem długości) prawdopodobieństwo błędu odkodowania, nie schodząc poniżej pewnej ustalonej wielkości transmisji informacji na przesłany bit. $\Diamond$

Przykład: Wrzucamy losowo n kul do $2n$ urn. Interesuje nas liczba urn, które zawierają dokładnie jedną kulę. Rzuty interpretujemy jako wykonywane kolejno próby. Moglibyśmy za sukces uznać trafienie w pustą urnę, wtedy liczba sukcesów to liczba zajętych urn, jeżeli jest ona większa niż $n/2$ to muszą być urny z pojedyńczymi kulami. Niech Y to zmienna mówiąca ile było sukcesów. Pojawia się techniczny problem, że prawdopodobieństwo sukcesu w i-tej próbie zależy od wyników $i - 1$ poprzednich prób. Oto obejście tego problemu: szacujemy przez wprowadzenie innej zmiennej losowej X, która majoryzuje powyżej opisany model prób, w tym sensie, że zachodzi $\mathsf{P}[X \leq k] \leq \mathsf{P}[Y \leq k]$, dla każdego k naturalnego. Robimy to w dwóch etapach. Najpierw określamy rzut jako zakończony sukcesem, gdy już $\frac{3}{4}$-te urn zajętych lub trafiamy w pustą urnę. Niech teraz X będzie ciągiem n prób Bernoulliego, każda z prawdopodobieństwem sukcesu równym $\frac{\frac{1}{4}+1}{2} = \frac{5}{8}$, który daje nie lepszą liczbę sukcesów. Oczekiwana liczba sukcesów dla X jest równa $\mu = \frac{5}{8}n$. Zmienna X ma rozkład dwumianowy, odpowiednia zamknięta postać nierówności Chernoffa to $\mathsf{P}[X - \mu \leq -\epsilon\mu] < e^{-\epsilon^2\mu/2}$. Weźmy $\epsilon = 1/10$. Zdarzenie A równe $X - \mu > -\epsilon\mu$ oznacza w tym przypadku, że zachodzi $X > (1-\epsilon)\mu = \frac{9}{10}\mu = \frac{9}{10} \cdot \frac{5}{8}n = \frac{9}{16}n$. Ponumerujmy urny w kolejności od zawierających najwięcej do najmniej kul. Dla każdej niepustej urny o numerze większym od $n/2$, która musi zawierać dokładnie jedną kulę, istnieje odpowiednia urna o numerze mniejszym od $n/2$ też zawierająca dokładnie jedną kulę. Jeżeli zdarzenie A zachodzi to liczba urn z jedną kulą jest większa niż $2(X - \frac{n}{2}) = \frac{n}{8}$. Prawdopodobieństwo, że tak jest wynosi co najmniej

$$1 - e^{-\epsilon^2\mu/2} = 1 - e^{-n \cdot \frac{1}{100} \cdot \frac{5}{8} \cdot \frac{1}{2}} = 1 - e^{-n/320} \ .$$

Pokazaliśmy, że liczba urn zawierających dokładnie po jednej kuli jest co najmniej $n/8$ z prawdopodobieństwem wykładniczo bliskim 1. $\Diamond$

Martyngały. Rodzinę $\mathcal{F}$ podzbiorów Ω nazywamy *σ-ciałem* gdy spełnia warunki:

1. $\emptyset \in \mathcal{F}$;
2. Jeżeli $E \in \mathcal{F}$ to $\Omega - E \in \mathcal{F}$;
3. Jeżeli $E_1, E_2, \ldots$ jest przeliczalną rodziną elementów $\mathcal{F}$ to $E_1 \cup E_2 \cup \ldots \in \mathcal{F}$.

Każde σ-ciało jest zamknięte na skończone operacje mnogościowe $\cap$ i $\cup$. Zmienna losowa X jest *mierzalna względem* $\mathcal{F}$ lub *$\mathcal{F}$-mierzalna* gdy $\{\omega \in \Omega : X(\omega) \leq x\} \in \mathcal{F}$, dla każdego x rzeczywistego. Każda zmienna losowa X wyznacza najmniejsze σ-ciało $\mathcal{F}(X)$ względem którego jest mierzalna. Mianowicie X wyznacza podział Ω na bloki, na których ma stałą wartość, zbiór przeliczalnych sum tych bloków tworzy σ-ciało. Podobnie określamy najmniejsze σ-ciało $\mathcal{F}(X_1, \ldots, X_n)$ względem którego wszystkie zmienne losowe $X_1, \ldots, X_n$ są mierzalne. Odwrotnie, każde σ-ciało wyznacza podział Ω na bloki; są to klasy abstrakcji relacji, która zachodzi między dwoma zdarzeniami ω_1 i ω_2 gdy nie istnieje zdarzenie $A \in \mathcal{F}$ takie, że $\omega_1 \in A$ oraz $\omega_2 \notin A$. Zmienna losowa X jest mierzalna względem σ-ciała $\mathcal{F}$ w.t.w. gdy jest stała na każdym bloku wyznaczonym przez $\mathcal{F}$ (patrz zadanie 2).

Jeżeli A jest zdarzeniem takim, że $P[A] > 0$, a X to zmienna losowa, to określamy *wartość oczekiwaną X pod warunkiem A*, oznaczaną przez $\mathsf{E}[X \mid A]$, jako $\sum_x x \cdot \mathsf{P}[X = x \mid A]$. Dla $\mathcal{F}$, które jest σ-ciałem, określamy funkcję $\mathsf{E}[X \mid \mathcal{F}]$ w ten sposób, że jej wartość w punkcie $\omega \in \Omega$ to $\mathsf{E}[X \mid A]$, gdzie A to blok $\mathcal{F}$ do którego należy ω (zakładamy, że nie ma bloków o zerowym prawdopodobieństwie). Jeżeli σ-ciała są wyznaczone przez zmienne losowe, to piszemy $\mathsf{E}[X \mid Y]$ zamiast $\mathsf{E}[X \mid \mathcal{F}(Y)]$, i odpowiednio $\mathsf{E}[X \mid Y_1, \ldots, Y_n]$ zamiast $\mathsf{E}[X \mid \mathcal{F}(Y_1, \ldots, Y_n)]$. Jeżeli X jest mierzalna względem $\mathcal{F}$ to $\mathsf{E}[X \mid \mathcal{F}] = X$. Zauważmy, że $\mathsf{E}[X \mid \mathcal{F}]$ czy $\mathsf{E}[X \mid Y]$ są *zmiennymi losowymi*, a nie liczbami jak wartość oczekiwana $\mathsf{E}\,X$.

Filtracją nazywamy ciąg σ-ciał $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \ldots$. Wyznaczają one coraz drobniejsze podziały Ω na bloki. Niech $\langle \mathcal{F}_i \rangle$ filtracja oraz $\langle X_i \rangle$ ciąg zmiennych losowych (jeżeli skończone, to takiej samej długości). Jest to *martyngał* gdy $\mathsf{E}[X_{i+1} \mid \mathcal{F}_i] = X_i$. Czasem podajemy tylko ciąg zmiennych losowych, wtedy mamy na myśli $\mathcal{F}_i = \mathcal{F}(X_1, \ldots, X_i)$; to znaczy: stwierdzenie, że ciąg $\langle X_0, X_1, X_2, \ldots \rangle$ jest martyngałem, bez podania dodatkowo filtracji, oznacza, że zachodzi $\mathsf{E}[X_{i+1} \mid X_1, \ldots, X_i] = X_i$.

Przykład: Niech $X_0, X_1, X_2, \ldots$ niezależne zmienne losowe, takie, że $\mathsf{E}[X_i] = 0$. Oznaczmy $S_i = X_0 + \cdots + X_i$. Wtedy $\langle S_n \rangle_{n \geq 0}$ jest martyngałem. Rzeczywiście:

$$\mathsf{E}[S_{n+1} \mid X_0, \ldots, X_n] = \mathsf{E}[S_n + X_{n+1} \mid X_0, \ldots, X_n] = S_n + \mathsf{E}[X_{n+1} \mid X_0, \ldots, X_n] = S_n \ ,$$

gdzie skorzystaliśmy z mierzalności S_n względem $\mathcal{F}(X_1, \ldots, X_n)$ oraz z niezależności (patrz zadanie 3). $\Diamond$

Przykład: Niech $\langle \mathcal{F}_i \rangle$ filtracja, oraz X zmienna losowa. Wtedy ciąg $X_i = \mathsf{E}[X \mid \mathcal{F}_i]$ jest martyngałem. Wynika to z tego, że jeżeli mamy dwa σ-ciała $\mathcal{G}_1 \subseteq \mathcal{G}_2$ to ma miejsce równość $\mathsf{E}[\mathsf{E}[X \mid \mathcal{G}_2] \mid \mathcal{G}_1] = \mathsf{E}[X \mid \mathcal{G}_1]$ (ćwiczenie). Tak otrzymany martyngał nazywamy *martyngałem Dooba.* $\Diamond$

Przykład: Słowo *martyngał* ma także inne znaczenie. Rozważmy grę sprawiedliwą (to znaczy $p = 1/2$), w której możemy stawiać dowolne wielokrotności stawki minimalnej, i gdy stawiamy x to z prawdopodobieństwem $1/2$ wygrywamy $2x$ i tak samo z prawdopodobieństwem $1/2$ tracimy x. Stosujemy taką strategię: zaczynamy od stawki x, podwajamy stawkę do pierwszej wygranej, potem wychodzimy z gry. Ta strategia nazywa się właśnie martyngałem. Z prawdopodobieństwem 1 gwarantuje ona wygraną równą x, o ile oczywiście mamy nieograniczony kapitał. $\Diamond$

Wszystkie zmienne losowe występujące w martyngale mają taką samą wartość oczekiwaną (ćwiczenie). Prawdopodobieństwo odchylenia od niej można oszacować podobnie jak w nierówności Chernoffa, o ile tylko kolejne elementy martyngału niewiele się różnią. Niech $\langle X_0, X_1, X_2, \ldots \rangle$ będzie martyngałem, oraz $|X_n - X_{n-1}| \leq b_n$, dla ciągu b_n. Wtedy, dla $a > 0$, zachodzi *nierówność Azumy:*

$$\mathsf{P}[X_n - X_0 \geq a] \leq \exp\Big(\frac{-a^2}{2\sum_{1\leq i\leq n} b_i^2}\Big) \ . \tag{1}$$

Dowód zaczynamy podobnie jak dla nierówności Chernoffa:

$$\mathsf{P}[X_n - X_0 \geq a] \leq e^{-sa} \cdot \mathsf{E}[\exp(s(X_n - X_0))] \ , \tag{2}$$

gdzie $s \geq 0$ jest parametrem. Niech $\mathcal{F}_i = \mathcal{F}(X_0, \ldots, X_i)$. Zachodzi

$$\mathsf{E}[\exp(s(X_n - X_0)) \mid \mathcal{F}_{n-1}] = \exp(s(X_{n-1} - X_0)) \cdot \mathsf{E}[\exp(s(X_n - X_{n-1})) \mid \mathcal{F}_{n-1}] \ , \tag{3}$$

ponieważ X_{n-1} jest $\mathcal{F}_{n-1}$-mierzalna (patrz zadanie 7). Jeżeli zmienna losowa Y spełnia warunki $|Y| \leq 1$ oraz $\mathsf{E}[Y \mid \mathcal{F}] = 0$ to zachodzi $\mathsf{E}[e^{cY} \mid \mathcal{F}] \leq e^{c^2/2}$ dla $c > 0$ (patrz zadanie 8). Weźmy $Y = (X_n - X_{n-1})/b_n$ oraz $\mathcal{F} = \mathcal{F}_{n-1}$. Sprawdzamy:

$$\mathsf{E}[Y \mid \mathcal{F}] = (\mathsf{E}[X_n \mid \mathcal{F}_{n-1}] - \mathsf{E}[X_{n-1} \mid \mathcal{F}_{n-1}])/b_n = (X_{n-1} - X_{n-1})/b_n = 0 \ ,$$

co wynika z określenia martyngału i mierzalności X_{n-1} względem $\mathcal{F}_{n-1}$. Stąd dostajemy nierówność $\mathsf{E}[\exp(sb_nY \mid \mathcal{F}_{n-1})] \leq \exp(s^2b_n^2/2)$, co podstawiamy do (3) i dostajemy

$$\mathsf{E}[\exp(s(X_n - X_0)) \mid \mathcal{F}_{n-1}] \leq \exp(s(X_{n-1} - X_0)) \cdot \exp(s^2 \cdot b_n^2) \ . \tag{4}$$

Bierzemy wartość oczekiwaną obu stron (4) i mamy nierówność: $\mathsf{E}[\exp(s(X_n - X_0))] \leq \exp(s^2b_n^2/2) \cdot \mathsf{E}[\exp(s(X_{n-1} - X_0))]$. Powtarzamy rekurencyjnie i dostajemy $\mathsf{E}[e^{s(X_n - X_0)}] \leq \exp\Big(\frac{s^2}{2}\sum_{1\leq i\leq n} b_i^2\Big)$. Zatem, na podstawie (2), mamy:

$$\mathsf{P}[X_n - X_0 \geq a] \leq \exp\Big(-as + \frac{s^2}{2}\sum_{1\leq i\leq n} b_i^2\Big) \ .$$

Kładąc $s = a/\sum_{1\le i\le n} b_i^2$ dostajemy nierówność Azumy (1). Podobne szacowanie zachodzi dla $\mathsf{P}[X_n - X_0 \le -a]$ (ćwiczenie), razem mamy inną postać:

$$\mathsf{P}[|X_n - X_0| \ge a] \le 2\exp\Big(\frac{-a^2}{2\sum_{1\le i\le n} b_i^2}\Big) \ .$$

Przykład: Niech $X_1, \ldots, X_n$ niezależne zmienne losowe takie, że $X_i \in [0,1]$ oraz istnieją $\mu_i = \mathsf{E}\, X_i$. Niech $X = X_1 + \ldots + X_n$, wtedy $\mathsf{E}\, X = \sum_{1\le i\le n} \mu_i$, oznaczamy $\mathsf{E}\, X = \mu$. Rozważmy zmienne losowe $Y_i = X_i - \mu_i$. Niech $S_0 = 0$ oraz $S_k = Y_1 + \ldots + Y_k$, dla $1 \le k \le n$. Ciąg $S_0, S_1, \ldots, S_n$ jest martyngałem oraz $|S_i - S_{i-1}| \le 2$, dla $1 \le i \le n$. Z nierówności Azumy dostajemy jako wniosek nierówność

$$\mathsf{P}[|X - \mu| \ge \epsilon n] \le 2 \cdot \exp\Big(\frac{-\epsilon^2 \cdot n^2}{2\sum_{1\le i\le n} 2^2}\Big) = 2e^{-\epsilon^2 n/8} \ ,$$

którą nazywa się *nierównością Hoeffdinga*. $\Diamond$

Stosowanie nierówności Azumy nazywa się często *metodą ograniczonych różnic*. Opiszemy teraz użyteczny wariant tej metody. Niech h będzie funkcją n zmiennych. Powiemy, że $x = \langle x_1, \ldots, x_n\rangle$ i $y = \langle y_1, \ldots, y_n\rangle$ *różnią się na jednej współrzędnej* gdy $x_i = y_i$ dla $1 \le i \le n$ oprócz być może jednej wartości i. Jeżeli spełniona jest nierówność $|h(x) - h(y)| \le b$ dla x i y różniących się na jednej współrzędnej, to h *spełnia warunek Lipschitza ze stałą* b. Rozważmy sytuację, gdy zmienna losowa jest postaci $X = h(X_1, \ldots, X_n)$, gdzie h spełnia warunek Lipschitza ze stała b, a $X_1, \ldots, X_n$ są zmiennymi losowymi. Rozważmy martyngał Dooba $\langle Y_i\rangle_{0\le i\le n}$, gdzie $Y_i = \mathsf{E}[X \mid \mathcal{F}_i]$ oraz filtracja $\langle \mathcal{F}_i\rangle$ określona jest przez $\mathcal{F}_0 = \{\emptyset, \Omega\}$, $\mathcal{F}_i = \mathcal{F}(X_1, \ldots, X_i)$. Innymi słowy: $Y_0 = \mathsf{E}\, X$ oraz, dla $1 \le i \le n$, Y_i to oczekiwana wartość X pod warunkiem, że znamy wartości $X_1, \ldots, X_i$. Pokażemy, że gdy poznajemy kolejną wartość X_{i+1}, to warunkowa wartość oczekiwana nie zmienia się więcej niż o b. Niech $\omega \in \Omega$ dowolne zdarzenie elementarne, dla którego chcemy to pokazać. Niech $A = \{\omega' : X_j(\omega') = X_j(\omega) \text{ dla } 1 \le j \le i\}$. A rozpada się na bloki B_j na których X_{i+1} ma takie same wartości, niech $\omega \in B_0$. Z kolei każde B_j rozpada się na rozłączne podzbiory $C_{j,k}$, niektóre być może puste, na których X jest stała. Numeracja po k jest dobrana tak, że jeżeli $\omega_1 \in C_{j_1,k}$ i $\omega_2 \in C_{j_2,k}$ to zachodzi $X_j(\omega_1) = X_j(\omega_2)$ dla wszystkich $j > i+1$. Korzystając z określenia martyngału mamy

$$Y_i = \sum_j Y_{i+1}(B_j)\mathsf{P}[B_j \mid A] \quad \text{oraz} \quad Y_{i+1} = \sum_k X(C_{j,k})\mathsf{P}[C_{j,k} \mid B_j] \ .$$

Stąd

$$\begin{aligned}
|Y_{i+1}(B_0) - Y_i| &= |Y_{i+1}(B_0) - \sum_j Y_{i+1}(B_j)\mathsf{P}[B_j \mid A]| \\
&= \Big|\sum_k X(C_{0,k})\mathsf{P}[C_{0,k} \mid B_0] - \sum_j \sum_k X(C_{j,k})\mathsf{P}[C_{j,k} \mid B_j]\mathsf{P}[B_j \mid A]\Big| \\
&= \Big|\sum_k \Big(X(C_{0,k})\mathsf{P}[C_{0,k} \mid B_0] - \sum_j X(C_{j,k})\mathsf{P}[C_{j,k} \mid A]\Big)\Big|
\end{aligned}$$

$$\leq b \cdot \left| \sum_k \mathsf{P}[C_{0,k} \mid B_0] - \sum_k \sum_j \mathsf{P}[C_{j,k} \mid A] \right| ,$$

ponieważ X_j dają te same wartości na elementach z $C_{0,k}$ oraz $C_{j,k}$, za wyjątkiem być może $j = i+1$. Moduł różnicy sum szacuje sie przez 1 ponieważ $0 \leq \sum_k \mathsf{P}[C_{0,k} \mid B_0] \leq 1$ i $0 \leq \sum_j \sum_k \mathsf{P}[C_{j,k} \mid A] \leq 1$, skąd wynika $|Y_{i+1} - Y_i| \leq b$. Z nierówności Azumy mamy $\mathsf{P}[|X - \mathsf{E}\, X| \geq a] \leq 2\exp(-a^2/2nb^2)$. Podstawiając $a = c\sqrt{n}$ dostajemy

$$\mathsf{P}[|X - \mathsf{E}\, X| \geq c\sqrt{n}] \leq 2\exp\Big(\frac{-c^2}{2b^2}\Big) , \tag{5}$$

co też nazywamy nierównością Azumy. Zauważmy, że wartość oczekiwana nie występuje w oszacowaniu danym przez nierówność Azumy, zatem można oszacować odchylenie od wartości oczekiwanej nie wiedząc wiele na temat wartości oczekiwanej.

Przykład: Wrzucamy losowo n kul do n urn. Chcielibyśmy oszacować liczbę urn do których trafiło dokładnie po jednej kuli. Rozumowania przez nierówność Chernoffa, jak dla przypadku $2n$ kul, nie można powtórzyć bez istotnych zmian. Oto inny sposób: Dla każdej urny, prawdopodobieństwo, że będzie tam kula jest równe

$$p = 1 - \Big(\frac{n-1}{n}\Big)^n = 1 - \Big(1 - \frac{1}{n}\Big)^n \longrightarrow_{n\to\infty} 1 - \frac{1}{e} > \frac{1}{2} .$$

Niech $0 < \epsilon < 1 - \frac{1}{2} - \frac{1}{e}$, wtedy oczekiwana liczba zajętych urn równa $pn > \big(\frac{1}{2} + \epsilon\big)n$, dla dostatecznie dużych n. Niech X_i to miejsce i-tej kuli, natomiast $h(X_1, \ldots, X_n)$ to liczba zajętych urn. Jeżeli zmienimy wartość jednej spośród X_i to liczba zajętych urn zmieni się co najwyżej o 1, zatem spełniony jest warunek Lipschitza ze stałą 1. Z nierówności Azumy (5) prawdopodobieństwo odchylenia liczby pustych komórek od wartości oczekiwanej o więcej niż $c\sqrt{n}$ jest nie większe niż $2e^{-c^2/2}$. Biorąc wartość c równą $\frac{\epsilon}{2}\sqrt{n}$ dostajemy, że liczba urn zawierających dokładnie jedną kulę jest równa co najmniej ϵn z prawdopodobieństwem co najmniej $1 - e^{-\epsilon^2 n/8}$. $\Diamond$

Przykład: Niech G będzie dwudzielnym (f, g)-regularnym grafem o n wierzchołkach stopnia f. Dla $0 < \epsilon < 1$, wybierzmy losowy zbiór A liczności ϵn spośród wierzchołków stopnia f. Każdy wierzchołek stopnia f jest w A z prawdopodobieństwem ϵ. Dany wierzchołek stopnia g nie ma sąsiada w A z prawdopodobieństwem

$$\begin{aligned} &\frac{n-\epsilon n}{n} \cdot \frac{n-\epsilon n-1}{n-1} \cdot \ldots \cdot \frac{n-\epsilon n-(g-1)}{n-(g-1)} \\ &= (1-\epsilon) \cdot \frac{n-\epsilon n-\frac{1}{n}}{n-\frac{1}{n}} \cdot \ldots \cdot \frac{n-\epsilon n-\frac{g-1}{n}}{n-\frac{g-1}{n}} \leq (1-\epsilon)^g , \end{aligned}$$

które także zbiega do $(1-\epsilon)^g$. To pozwala oszacować wartość oczekiwaną liczności zbioru sąsiadów A (patrz zadanie 13). Możemy postąpić trochę inaczej: dla $0 < \epsilon < 1$, ustalmy zbiór A liczności ϵn spośród wierzchołków stopnia f natomiast krawędzie G ustalmy w sposób losowy. Podobnie jek wyżej, prawdopodobieństwo tego, że dany wierzchołek stopnia g jest sąsiadem A jest co najmniej $1-(1-\epsilon)^g$. Niech Y liczność zbioru sąsiadów A, widzimy, że $\mathsf{E}\, Y$ wynosi co najmniej $n \cdot \frac{f}{g} \cdot (1-(1-\epsilon)^g)$. Ponumerujmy krawędzie

wychodzące ze zbioru A, niech X_i to wierzchołek stopnia g incydentny z i-tą krawędzią. Spełniony jest warunek Lipschitza ze stałą 1, bowiem zmiana jednej spośród X_i zmienia liczność zbioru sąsiadów A o co najwyżej 1. Z nierówności Azumy mamy szcowanie

$$\mathsf{P}[Y - \mathsf{E}\,Y \leq -c \cdot \sqrt{\epsilon f n}] \leq e^{-c^2/2} \ .$$

Zbiór A można wybrać na $\binom{n}{\epsilon n}$ sposobów. Jeżeli ma miejsce nierówność

$$\binom{n}{n\epsilon} \cdot e^{-c^2/2} < 1 \ , \tag{6}$$

to istnieje graf G dla którego liczność zbioru sąsiadów każdego zbioru wierzchołków liczności ϵn, składającego się z wierzchołków stopnia n, będzie co najmniej $\mathsf{E}\,Y - c\sqrt{\epsilon f n}$. Skorzystamy z szacowania $\binom{n}{\epsilon n} < 2^{n\mathrm{H}(\epsilon)}$, stąd (6) zachodzi gdy ma miejsce $2^{n\mathrm{H}(\epsilon)} \cdot e^{-c^2/2} = 2^{n\mathrm{H}(\epsilon) - (\log_2 e)c^2/2} < 1$, a zatem gdy $n\mathrm{H}(\epsilon) - \log_2 e \cdot \frac{c^2}{2} < 0$, czyli $c \geq \left(\frac{2n\mathrm{H}(\epsilon)}{\log_2 e}\right)^{1/2}$. Podstawiamy $c = \left(\frac{2n\mathrm{H}(\epsilon)}{\log_2 e}\right)^{1/2}$ do $\mathsf{E}\,Y - c\sqrt{\epsilon f n}$. Nierówność (6) zachodzi, zatem pokazaliśmy, że istnieje graf (f, g)-regularny G o n wierzchołkach stopnia f, który jest (f, g, ϵ, β)-ekspanderem dla wartości β równej $\frac{f}{g \cdot \epsilon} \cdot (1 - (1 - \epsilon)^g) - \left(\frac{2f\mathrm{H}(\epsilon)}{\epsilon \log_2 e}\right)^{1/2}$. $\Diamond$

Zadania

1. Jaki przepływ informacji przez BKS daje stosowanie kodów, których użyliśmy w dowodzie twierdzenia Shannona?

2. Pokaż, że jeżeli zmienna X mierzalna względem $\mathcal{F}$ to X stała na każdym bloku $\mathcal{F}$.

3. Pokaż, że jeżeli zmienne X i Y są niezależne to $\mathsf{E}\,[X \mid Y] = \mathsf{E}\,[X]$.

4. Pokaż następujące własności warunkowej wartości oczekiwanej:

   (a) $\mathsf{E}\,[\mathsf{E}\,[X \mid Y]] = \mathsf{E}\,[X]$;

   (b) $\mathsf{E}\,[Y\,\mathsf{E}\,[X \mid Y]] = \mathsf{E}\,[XY]$;

   (c) Jeżeli $\mathcal{G}_1 \subseteq \mathcal{G}_2$ dwa σ-ciała to $\mathsf{E}\,[\mathsf{E}\,[X \mid \mathcal{G}_2] \mid \mathcal{G}_1] = \mathsf{E}\,[X \mid \mathcal{G}_1]$.

5. Niech Y zmienna losowa o wartościach całkowitych nieujemnych. Niech $X_0, X_1, X_2, \ldots$ ciąg zmiennych losowych, wszystkie określone na tej samej przestrzeni. Czy prawdziwa jest równość $\mathsf{E}\,X_Y = \sum_{i \geq 0} \mathsf{E}\,[X_i \mid Y = i] \cdot \mathsf{P}[Y = i]$?

6. Pokaż, że jeżeli ciąg $X_0, X_1, X_2, \ldots$ jest martyngałem, to $\mathsf{E}\,[X_i] = \mathsf{E}\,[X_0]$.

7. Pokaż, że jeżeli X jest $\mathcal{F}$-mierzalna, to zachodzi $\mathsf{E}\,[X \cdot Y \mid \mathcal{F}]] = X \cdot \mathsf{E}\,[Y \mid \mathcal{F}]$.

8. Pokaż, że jeżeli $|Y| \leq 1$, $\mathsf{E}\,[Y] = 0$, oraz $c > 0$, to $\mathsf{E}\,e^{cY} \leq \frac{1}{2}e^{-c} + \frac{1}{2}e^{c} < e^{c^2/2}$. Wskazówka: wypukłość funkcji wykładniczej.

9. Niech ciąg $X_0, X_1, X_2, \ldots$ będzie przyrostem kapitału po kolejnych krokach stosowania martyngału (jako strategii gry). Pokaż, że jest to martyngał w sensie warunkowych wartości oczekiwanych. Pokaż że oczekiwany kapitał który stracimy, stosując martyngał do czasu aż wyjdziemy na swoje, jest nieskończony.

10. Wrzucamy losowo $2n$ kul do n urn. Pokaż, że jest $\Omega(n)$ urn zawierających dokładnie po jednej kuli, z prawdopodobieństwem wykładniczo zbiegającym do 1 wraz z $n \to \infty$.

11. Niech tablica prostokątna ma rozmiary $n \times n$. Na początku miejsca $\langle 1, i\rangle$ zawierają jedynki a pozostałe zera. W każdym miejscu $\langle x, y\rangle$ tablicy wstawiamy jedynkę, czas trwania tej operacji $\xi_{x,y}$ jest liczony od kroku pojawienia się jedynki w $\langle x-1, y\rangle$. Zmienne losowe $\xi_{x,y}$ mają ten sam rozkład geometryczny i są niezależne. Oszacuj wartość oczekiwaną liczby kroków po których wszystkie zera znikną.

12. W jednym kroku wrzucamy losowo n kul do zbioru urn, zostawiamy puste urny, pozostale usuwamy. Zaczynamy od n urn, powtarzamy kroki aż nie pozostanie żadna urna. Pokaż że oczekiwana liczba kroków jest $\mathcal{O}(n \log^* n)$, gdzie $\log^{(1)} x = \log x$, $\log^{(k+1)} x = \log(\log^{(k)} x)$, and $\log^* x = \min_k[\log^{(k)} x \leq 1]$.

13. Niech G będzie (f, g)-regularnym grafem dwudzielnym o n wierzchołkach stopnia f, i niech $0 < \epsilon < 1$. Pokaż, że istnieje zbiór A wierzchołków stopnia f i liczności $\epsilon \cdot n$ taki, że A ma co najwyżej $n \cdot \epsilon \cdot \frac{f}{g} \cdot (1 - (1-\epsilon)^g) + \mathcal{O}(1)$ sąsiadów.

14. Pokaż, że dla każdej pary liczb całkowitych $f, g \geq 1$ istnieje $0 < \epsilon < 1$ takie, że dla każdego $n \geq 1$ o własności $g \mid (f \cdot n)$ istnieje $(f, g, \epsilon, \frac{3}{4} \cdot f)$-ekspander o n wierzchołkach stopnia f.

MMD Wykład 11.

Bogdan Chlebus

Losowe błądzenie na prostej. Cząstka znajduje się na prostej, początkowo w punkcie o współrzędnej 0. W każdym kroku zmienia współrzedną położenia o $+1$ lub -1, z prawdopodobieństwem p lub $q = 1 - p$ odpowiednio, gdzie kolejne kierunki ruchów niezależne. Formalnie, niech X_i ma rozkład $\mathsf{P}[X_i = 1] = p$, $\mathsf{P}[X_i = -1] = 1 - p = q$, gdzie X_i niezależne. Wtedy pozycja cząstki po n-tym kroku równa $S_n = X_1 + \cdots + X_n$. Niech $f_0(n)$ będzie prawdopodobieństwem, że cząstka wraca do punktu 0 po n krokach po raz pierwszy, ma to miejsce dla $n > 0$, w szczególnośći $f_0(0) = 0$. Podobnie, $g_0(n)$ to prawdopodobieństwo, że jesteśmy w punkcie 0 po n krokach, w szczególnośći $g_0(0) = 1$, $g_0(k) = 0$ dla k nieparzystego.

Niech $F_0(t) = \sum_n f_0(n) \cdot t^n$, $G_0(t) = \sum_n g_0(n) \cdot t^n$ odpowiednie funkcje tworzące. Jeżeli n parzyste, to $g_0(n) = \binom{n}{n/2}(pq)^{n/2}$, poniewaz wykonujemy tyle samo ruchow w lewo i w prawo. Stąd

$$\begin{aligned} G_0(t) &= \sum_{n=0}^{\infty} \binom{n}{n/2} (pq)^{n/2} \cdot [2 \mid n] \cdot t^n = \sum_{n=0}^{\infty} \binom{2n}{n} \cdot (pq)^n \cdot t^{2n} \\ &= \sum_{n=0}^{\infty} \binom{-1/2}{n} (-4pqt^2)^n = (1 - 4pqt^2)^{-1/2} \ . \end{aligned}$$

Z drugiej strony zachodzi wzór $g_0(n) = \sum_{i=0}^{n} f_0(i) g_0(n-i)$, dla $n \geq 1$, zatem mamy

$$G_0(t) = 1 + \sum_{k=1}^{\infty} t^k g_0(k) = 1 + F_0(t) G_0(t) \ ,$$

z własności splotu i tego, że wyraz wolny $F_0(t) \cdot G_0(t)$ równy 0. Stąd także

$$F_0(t) = (G_0(t) - 1)/G_0(t) = [(1 - 4pqt^2)^{-1/2} - 1](1 - 4pqt^2)^{1/2} = 1 - (1 - 4pqt^2)^{1/2} \ . \quad (1)$$

Możemy obliczyć prawdopodobieństwo zdarzenia, że cząstka wróci do punktu startu, czyli $\sum_{i=0}^{\infty} f_0(i) = F_0(1)$, mimo, że nie znamy explicite $f_0(k)$. Podstawiamy $t = 1$ w (1) i dostajemy $F_0(1) = 1 - \sqrt{1 - 4pq} = 1 - |p - q|$. Widzimy, że powrót do 0 jest zdarzeniem pewnym tylko dla *błądzenia symetrycznego*, czyli gdy $p = q$. Ale nawet w tym przypadku czas oczekiwania na pierwszy powrót wynosi

$$\lim_{t \to 1} F_0'(t) = \lim_{t \to 1} (1 - (1 - t^2)^{1/2})' = \lim_{t \to 1} \frac{t}{\sqrt{1 - t^2}} = \infty \ .$$

Niech $f_k(n)$ bedzie prawdopodobieństwem tego, że pierwszy raz (po starcie) cząstka odwiedza punkt o wspolrzednej k w kroku n, i $F_k(t) = \sum_{i=0}^{\infty} f_k(i) t^i$ funkcja tworząca. Podobnie jak poprzednio $f_k(n) = \sum_{i=1}^{n-1} f_1(i) f_{k-1}(n-i)$. Stąd wynika

$$F_k(t) = F_{k-1}(t) \cdot F_1(t) = (F_1(t))^k \ .$$

Wystarczy obliczyć $F_1(t)$. Mamy $F_1(t) = pt + qtF_2(t) = pt + qtF_1^2(t)$, jako że $f_1(1) = p$ i $f_1(n) = qf_2(n-1)$, dla $n > 1$. Rozwiązujemy względem $F_1(t)$ i dostajemy

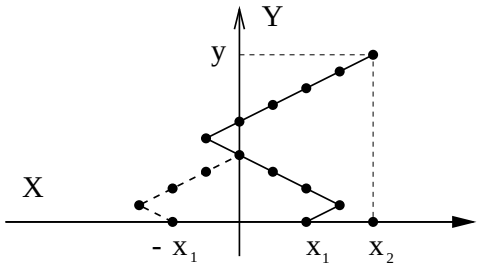
$$F_1(t) = \frac{1 - (1 - 4pqt^2)^{1/2}}{2qt} \ ,$$

gdyż drugie rozwiązanie jest nieograniczone przy $t \to 0$. Podstawiając $t = 1$ otrzymujemy

$$F_1(1) = \frac{1 - |p - q|}{2q} = \min\Big\{1, \frac{p}{q}\Big\} .$$

Z takim prawdopodobieństwem cząstka kiedykolwiek osiągnie współrzędną większą od 0.

Przedstawmy trajektorię cząstki na płaszczyźnie: w przestrzeni (oś X) i w czasie (oś Y). *Zasada odbicia* mówi: liczba dróg z punktu (x_1, y_1) do (x_2, y_2), gdzie $x_1, x_2 \geq 0$ i $y_2 > y_1$, które przecinają oś Y, jest równa liczbie dróg z $(-x_1, y_1)$ do (x_2, y_2). Dla dowodu, niech T część drogi aż do pierwszego punktu przecięcia z Y, zamieniamy tę drogę odbijając T na drugą stronę osi Y, patrz Rysunek 1. Inny wariant: liczba dróg z (x_1, y_1) do (x_2, y_2) i przecinających oś taka sama jak liczba dróg z (x_1, y_1) do $(-x_2, y_2)$: odbijamy począwszy od ostatniego punktu przecięcia z osią Y.



Rysunek 1: Zasada odbicia: niech $y_1 = 0$, drodze z $(x_1, 0)$ do (x_2, y) przyporządkowujemy drogę z $(-x_1, 0)$ do (x_2, y).

Przykład: Niech Max_n maksymalna odległość na prawo od startu w czasie pierwszych n kroków błądzenia symetrycznego na prostej. Pokażemy, że $\mathsf{E}\,\mathrm{Max}_n = \Theta(\sqrt{n})$.

Położenie cząstki po n krokach ma wartość $S_n = X_1 + \ldots + X_n$, gdzie $X_1, X_2, \ldots$ to ciąg niezależnych zmiennych losowych takich, że $\mathsf{P}[X_i = \pm 1] = 1/2$. Zdarzenie $\mathrm{Max}_n \geq a$ jest sumą trzech rozłącznych zdarzeń: zdarzenia A równego $S_n = a$, zdarzenia B równego $S_n > a$, i zdarzenia C, które zachodzi gdy $S_n < a$ ale jednocześnie istnieje $k < n$ takie, że $S_k = a$. Zauważmy, że $\mathsf{P}[B] = \mathsf{P}[C]$: mianowicie, każdej trajektorii cząstki z B możemy jednoznacznie przyporządkować trajektorię z C w ten sposób, że gdy cząstka opuszcza współrzędną a po raz ostatni, to raz idzie na lewo a raz na prawo, tak jak w zasadzie odbicia. Dostajemy zatem $\mathsf{P}[\mathrm{Max}_a \geq n] = \mathsf{P}[S_n = a] + 2\mathsf{P}[S_n > a]$, a stąd

$$2\mathsf{P}[S_n > a] \leq \mathsf{P}[\mathrm{Max}_n \geq a] \leq 2\mathsf{P}[S_n \geq a] . \tag{2}$$

Oprzemy się na wzorze $\mathsf{E}\,\mathrm{Max}_n = \sum_{a=1}^{n} \mathsf{P}[\mathrm{Max}_n \geq a]$. Z niego i (2) mamy:

$$2\sum_{a=2}^{n} \mathsf{P}[S_n \geq a] \leq \mathsf{E}\,\mathrm{Max}_n \leq 2\sum_{a=1}^{n} \mathsf{P}[S_n \geq a] . \tag{3}$$

Oznaczmy $S_n^+ = \max[0, S_n]$. Z (3) dostajemy $2\mathsf{E}\,(S_n^+ - 1) \leq \mathsf{E}\,\mathrm{Max}_n \leq 2\mathsf{E}\,S_n^+$.
Ale $\mathsf{E}\,S_n^+ = \frac{1}{2}\mathsf{E}\,|S_n|$. Stąd $\mathsf{E}\,\mathrm{Max}_n = \mathsf{E}\,|S_n| + O(1)$. Obliczymy:

$$\mathsf{E}\,|S_n| = \sum_{a=0}^{n} |n - 2a| \binom{n}{a} 2^{-n} . \tag{4}$$

Dla prostoty, niech n parzyste. Sumę (4), bez czynnika 2^{-n}, dzielimy na cztery części:

$$\sum_{a=0}^{n} |n-2a| \binom{n}{a} = \sum_{a=0}^{\frac{n}{2}-1} (n-2a)\binom{n}{a} + \sum_{a=\frac{n}{2}+1}^{n} (2a-n)\binom{n}{a}$$

$$= n \underbrace{\sum_{a=0}^{\frac{n}{2}-1} \binom{n}{a}}_{S_1} - 2 \underbrace{\sum_{a=0}^{\frac{n}{2}-1} a\binom{n}{a}}_{S_2} + 2 \underbrace{\sum_{a=\frac{n}{2}+1}^{n} a\binom{n}{a}}_{S_3} - n \underbrace{\sum_{a=\frac{n}{2}+1}^{n} \binom{n}{a}}_{S_4} . \qquad (5)$$

Obliczamy kolejno: $S_1 = \sum_{a=0}^{\frac{n}{2}-1} \binom{n}{a} = 2^{n-1} - \frac{1}{2}\binom{n}{n/2}$.
Skorzystaliśmy z $2^n = (1+1)^n = \sum_{a=0}^{\frac{n}{2}-1} \binom{n}{a} + \binom{n}{n/2} + \sum_{a=\frac{n}{2}+1}^{n} \binom{n}{a}$ oraz $\binom{n}{a} = \binom{n}{n-a}$. Z nich wynika $\sum_{a=0}^{\frac{n}{2}-1} \binom{n}{a} = \sum_{a=\frac{n}{2}+1}^{n} \binom{n}{a} = \frac{1}{2}\left(2^n - \binom{n}{n/2}\right)$. Następne podobnie:

$S_2 = \sum_{a=0}^{\frac{n}{2}-1} a\binom{n}{a} = \sum_{a=1}^{\frac{n}{2}-1} a \cdot \frac{n}{a}\binom{n-1}{a-1} = n \sum_{a=1}^{\frac{n}{2}-1} \binom{n-1}{a-1} = n\left(2^{n-2} - \binom{n-1}{\frac{n}{2}-1}\right)$.

$S_3 = \sum_{a=\frac{n}{2}+1}^{n} a\binom{n}{a} = \sum_{a=\frac{n}{2}+1}^{n} a\frac{n}{a}\binom{n-1}{a-1} = n \sum_{a=\frac{n}{2}}^{n-1} \binom{n-1}{a} = n2^{n-2}$.

$S_4 = \sum_{a=\frac{n}{2}+1}^{n} \binom{n}{a} = 2^{n-1} - \frac{1}{2}\binom{n}{n/2}$.

Podstawiając do równania (5) dostajemy następujące wyrażenie:

$$\left[n\left(2^{n-1} - \frac{1}{2}\binom{n}{n/2}\right) - 2n\left(2^{n-2} - \binom{n-1}{\frac{n}{2}-1}\right) + 2n \cdot 2^{n-2} - n\left(2^{n-1} - \frac{1}{2}\binom{n}{n/2}\right)\right] \cdot 2^{-n} .$$

Po uproszczeniu otrzymujemy: $\mathsf{E}\,|S_n| = 2n \cdot \binom{n-1}{\frac{n}{2}-1} \cdot 2^{-n}$. Ze wzoru Stirling'a:

$$\binom{n-1}{\frac{n}{2}-1} = \frac{1}{2}\binom{n}{n/2} = \frac{n!}{2\left(\frac{n}{2}!\right)^2} = \Theta\left(\frac{1}{2} \cdot \left(\frac{n}{e}\right)^n \cdot \sqrt{n} \cdot \left(\left(\frac{e}{n/2}\right)^{n/2} \frac{1}{\sqrt{n}}\right)^2\right) = \Theta\left(2^n \cdot n^{-1/2}\right) .$$

Stąd wynika $\mathsf{E}\,\mathrm{Max}_n = \Theta(\sqrt{n})$. $\Diamond$

Niech $L_y(x_1, x_2)$ oznacza liczbę dróg z $(x_1, 0)$ do (x_2, y). W każdej z nich jest pewne a ruchów w prawo i b w lewo, gdzie $a + b = y$, $a - b = x_2 - x_1$. Stąd $a = \frac{y+x_2-x_1}{2}$, i mamy $L_y(x_1, x_2) = \binom{y}{(y+x_2-x_1)/2}$. Niech $M_y(x_1, x_2)$ oznacza liczbę takich dróg przecinających oś Y.

Lemat o głosowaniu mówi, że liczba dróg z $(0, 0)$ do (x, y), które nie wracają do osi Y, jest równa $\frac{x}{y} \cdot L_y(0, x)$. (Zadanie 6 pokazuje skąd wzięła się nazwa.) Dla dowodu zauważmy, że pierwszy ruch musi byc w kierunku dodatnim, czyli zaczynamy od $(1, 1)$. Z zasady odbicia szukana liczba to

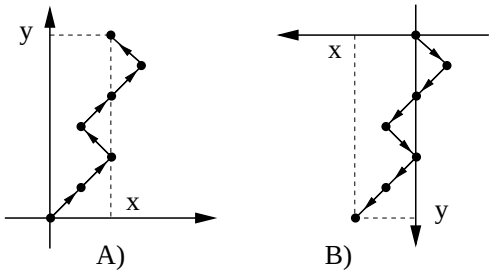
$$L_{y-1}(1,x) - M_{y-1}(1,x) = L_{y-1}(1,x) - L_{y-1}(-1,x) = \binom{y-1}{\frac{y+x}{2}-1} - \binom{y-1}{\frac{y+x}{2}} = \frac{x}{y} \cdot \binom{y}{\frac{y+x}{2}} ,$$

gdzie ostatnią równość sprawdzmy przez rozwinięcie w silnie.

Z lematu o glosowaniu jest $\frac{x}{n} \cdot L_n(0, x)$ sposobów dotarcia do punktu (x, n) bez odwiedzania zera, każde z prawdopodobieństwem $p^{(n+x)/2} q^{(n-x)/2}$. Stąd

$$\mathsf{P}[S_1 \cdots S_n \neq 0, S_n = x] = \frac{x}{n} \cdot L_n(0, x) \cdot p^{(n+x)/2} q^{(n-x)/2} = \frac{x}{n} \cdot \mathsf{P}[S_n = x] . \qquad (6)$$

Odwróćmy błądzenie: zamiast sum $0, X_1, X_1+X_2, \ldots, \sum_{i=1}^n X_i$ rozważmy sumy $0, X_n, X_n+X_{n-1}, \ldots, \sum_{i=1}^n X_i$. Wykres odwróconego błądzenia otrzymujemy odwracając kierunki osi współrzędnych i przesuwając początek układu do $\langle \sum_{i=1}^n X_i, n\rangle$, patrz Rysunek 2.



Rysunek 2: A) Wykres przykładowego błądzenia. B) To błądzenie po odwróceniu.

Błądzenie dociera do $x > 0$ stale przez wartości dodatnie (oprócz chwili startu) w.t.w. gdy odwrócone błądzenie dociera do $x > 0$ po raz pierwszy. Przypomnijmy oznaczenie $f_x(n)$ na prawdopodobieństwo zdarzenia, że cząstka odwiedza punkt o współrzędnej x po raz pierwszy w n-tym kroku po starcie. Dostajemy

$$f_x(n) = \frac{x}{n} \cdot \mathsf{P}[S_n = x] \ .$$

Liczba $P_x = \sum_{n=1}^{\infty} f_x(n)$ to prawdopodobieństwo, że cząstka odwiedzi kiedyś x. Jeżeli $p = q$ to $P_x = 1$. Z drugiej strony, na mocy wzoru (6), P_x to oczekiwana liczba odwiedzin x przed powrotem do zera. Dla $p = q$ ta oczekiwana wartość równa 1, niezależnie od x, co jest raczej nieoczekiwane.

Ruina gracza. Błądzenie losowe często interpretuje sie w języku gier hazardowych: ruch w prawo to wygrana, a w lewo to przegrana, w razie wygranej zyskujemy podstawową stawkę, równą 1, w razie przegranej ją tracimy. Położenie cząstki S_n to przyrost kapitalu po n grach. Jeżeli chcemy grać do chwili powiększenia kapitalu o stawkę podstawową, to $F_1(1)$ jest równe prawdopodobieństwu tego, że gra się kiedyś skończy, o ile dysponujemy kapitalem nieograniczonym. (Jeżeli kapital jest ograniczony to skończenie się gry jest zdarzeniem pewnym.) Rozważmy następujący wariant gry: zaczynamy z kapitałem $a > 0$, gra kończy się, gdy osiągniemy kapitał $b > a$, lub stracimy wszystko. Wyznaczymy prawdopodobieństwo R_a ruiny gracza. Liczby R_a spełniają równanie liniowe $R_a = p \cdot R_{a+1} + q \cdot R_{a-1}$, dla $0 < a < b$, przy warunkach brzegowych $R_0 = 1$ i $R_b = 0$. W równoważnej postaci:

$$p \cdot R_a - R_{a-1} + q \cdot R_{a-2} = 0 \ .$$

Stąd funkcja tworząca ciagu $\langle R_a\rangle$ jest postaci $\frac{w(x)}{p-x+qx^2}$, dla pewnego wielomianu $w(x)$. Zachodzi $p - x + qx^2 = p(1-\alpha x)(1-\beta x)$, gdzie α i β spełniają równanie $py^2 - y + q = 0$. Rozwiązujemy to równanie względem y i dostajemy:

$$\alpha, \beta = \frac{1 \pm \sqrt{1-4pq}}{2q} = 1, \frac{p}{q} \ .$$

Jeżeli $p = q$ to rozwiązanie jest postaci $R_a = Aa + B$, z warunków brzegowych dostajemy $R_a = 1 - \frac{a}{b}$. Jezeli $p \neq q$ to rozwiązanie postaci $R_a = A + B\left(\frac{p}{q}\right)^a$, z warunków brzegowych

dostajemy

$$R_a = \frac{\left(\frac{p}{q}\right)^a - \left(\frac{p}{q}\right)^b}{1 - \left(\frac{p}{q}\right)^b} \ .$$

Jeżeli gramy w ruletkę obstawiając kolor, to $p = 18/38 = 9/19$. Przypuśćmy, że zawsze stawiamy stawkę podstawową 1. Wtedy, jeżeli zaczynamy od kapitalu 2-ch stawek a chcemy go powiększyć do 16-tu, to prawdopodobieństwo sukcesu jest równe około 0.053. Ale możemy grać inaczej, na przykład stawiając zawsze cały kapitał. Wtedy wystarczy wygrać trzy razy pod rząd, czyli z prawdopodobieństwem $(9/19)^3 \approx 0.106 \gg 0.053$. Pokażemy optymalnosc strategi "stawiania wszystkiego" dla takiego zadania. Dla uproszczenia oznaczeń załóżymy że b jest postaci $b = 2^n$. Formalnie, określamy *śmiałą strategię* następująco: niech c bieżący kapitał, jeżeli $c \le b - c$ to stawiamy c, jeżeli $b > c > b - c$ to stawiamy $b - c$. Niech $B(a)$ prawdopodobieństwo ostatecznego sukcesu. Liczby $B(a)$ spelniają równanie

$$B(a) = pB(2a) \cdot [a \le b/2] + (p + qB(2a - b)) \cdot [a > b/2] \ ,$$

przy warunkach brzegowych $B(0) = 0$ i $B(b) = 1$, gdzie nawiasy kwadratowe to notacja Iversona. Uzasadnienie: jeżeli $a \le b - a$ to z prawdopodobieństwem p kontynuujemy grę z podwojonym kapitałem, a jeżeli $b > a > b - a$ to gra kończy się natychmiastowym sukcesem z prawdopodobieństwem p lub kontynuujemy ją z kapitałem $a - (b - a) = 2a - b$ w razie chwilowej porażki. Pokażemy, że zachodzi nierówność

$$B(a) \ge pB(a + d) + qB(a - d) \ , \tag{7}$$

dla $0 \le a - d \le a \le a + d \le b$, o ile $p \le q$. Jest ona równoważna nierówności

$$C(l, r) = B(s) - pB(r) - qB(l) \ge 0 \ ,$$

gdzie $s = (l + r)/2$. Dowód przez odwrotną indukcję po maksymalnej i takiej, że $2^i \mid l$ oraz $2^i \mid r$. Poczatek indukcji: $i = n$. Jest to możliwe tylko gdy $l = 0$ i $r = b = 2^n$. Wtedy $C(0, b) = B(b/2) - p = 0$. Krok indukcyjny: rozważamy 4 przypadki, w zależności od położenia $b/2$ względem liczb $l \le s \le r$. Na przykład dla $r \le b/2$ mamy $C(l, r) = pC(2l, 2r) \ge 0$. Trudniejszy przypadek: $l \le s \le b/2 \le r$. Wtedy

$$C(l, r) = pB(2s) - p(p + qB(2r - b)) - pqB(2l) \ .$$

Korzystając z $B(2s) = p + qB(4s - b)$ i $B(2s - \frac{b}{2}) = pB(4s - b)$ dostajemy $pB(2s) = p^2 + qpB(4s - b) = p^2 + qB(2s - \frac{b}{2})$, a stąd

$$\begin{aligned} C(l, r) &= p^2 + qB\Big(2s - \frac{b}{2}\Big) - p^2 - pqB(2r - b) - pqB(2l) \\ &= q[B\Big(2s - \frac{b}{2}\Big) - pB(2r - b) - pB(2l)] \ . \end{aligned}$$

Przypuśćmy, że $2r - b \ge 2l$, odwrotna nierówność podobnie. Wtedy $C(l, r) \ge qC(2l, 2r - b) \ge 0$, ponieważ $q \ge p$. Pozostałe przypadki podobnie, co kończy dowod (7).

Rozważmy dowolną strategię T. Niech T_k otrzymana z T w ten sposób, że przez pierwsze k kroków stosujemy T a potem strategię śmiałą. Z nierówności (7) przez indukcję wynika, że prawdopodobieństwo ostatecznego sukcesu przy T_k jest nie lepsze niż przy strategii śmiałej cały czas. Niech $\mathcal{S}$ oznacza strategię śmiałą. Niech D_k zdarzenie, że gra kończy się dokładnie po k krokach, gdy stosujemy strategię T. Szacujemy:

$$\begin{aligned}\mathsf{P}[\text{ sukces } T] &= \sum_k \mathsf{P}[\text{ sukces } T \mid D_k] \cdot \mathsf{P}[D_k] = \sum_k \mathsf{P}[\text{ sukces } T_k \mid D_k] \cdot \mathsf{P}[D_k] \\ &\leq \sum_k \mathsf{P}[\text{ sukces } \mathcal{S} \mid D_k] \cdot \mathsf{P}[D_k] = \mathsf{P}[\text{ sukces } \mathcal{S}] \ ,\end{aligned}$$

co kończy dowód optymalności śmiałej strategii.

Zadania

1. Pokaż z równania Walda, że oczekiwany czas pierwszego powrotu do punktu startu przy symetrycznym błądzeniu jest nieskończony.

2. Jakie jest prawdopodobieństwo, że cząstka błądząca po prostej odwiedzi kiedykolwiek punkt o współrzędnej x?

3. Rozważmy błądzenie losowe z barierami, które pochłaniają cząstkę przy pierwszym zetknięciu, i są ustawione w punktach o współrzędnych całkowitych $-x$ i y, dla nieujemnych x i y. Oblicz prawdopodobieństwo pochłonięcia cząstki przez każdą z barier. Jaka jest oczekiwana pozycja cząstki w chwili pochłonięcia? Jaki jest oczekiwany czas błądzenia?

4. Jaka jest oczekiwana liczba odwiedzin zera w n krokach błądzenia symetrycznego?

5. Niech X_n oznacza liczbę punktów odwiedzonych dokładnie jeden raz w n krokach symetrycznego błądzenia na prostej. Pokaż, że $\mathsf{E}\, X_n = 2$.

6. Jest a zwolenników i b przeciwników sprawy, która ma być rozstrzygnięta przez głosowanie, gdzie $a > b$. Głosujący oddają swoje głosy w losowej kolejności. Jakie jest prawdopodobieństwo, że zwolennicy prowadzą przez cały czas głosowania?

7. Niech $\mathrm{Max}_n = \max(0, S_1, \ldots, S_n)$ dla błądzenia gdzie $p \neq 1 - p$. Oszacuj $\mathsf{E}\, \mathrm{Max}_n$.

8. Pokaż, że dla błądzenia symetrycznego zachodzi $\mathsf{P}[S_1 \cdot \ldots \cdot S_{2n} \neq 0] = \mathsf{P}[S_{2n} = 0]$.

9. Dla błądzenia symetrycznego po prostej, niech Y_{2n} oznacza czas ostatniej wizyty w zerze w ciagu $2n$ krokow błądzenia. Pokaż $\mathsf{P}[Y_{2n} = 2k] = \mathsf{P}[S_{2k} = 0] \cdot \mathsf{P}[S_{2n-2k} = 0]$. Wskazówka: Skorzystaj z (6).

10. Niech Y_{2n} jak w zadaniu 9. Pokaż *prawo arcusa sinusa*, które mówi, że prawdopodobieństwa $\mathsf{P}[\frac{Y_{2n}}{2n} \leq a]$ zbiegają do liczby $\frac{2}{\pi} \arcsin(\sqrt{a})$, przy $n \to \infty$.
Wskazówka: Oblicz przybliżenie $\mathsf{P}[S_{2i} = 0]$ ze wzoru Stirlinga, a następnie skorzystaj ze wzoru $\int_0^a \frac{dt}{\sqrt{t(1-t)}} = 2 \arcsin(\sqrt{a})$.

11. Gracz zaczyna grę z kapitałem $a > 0$, gra do ruiny lub osiągniecia kapitału $b > a$. Jaka jest jego optymalna strategia dla $p > q$? Jaka strategia maksymalizuje oczekiwany czas trwania gry, w zależności od p?

12. Niech zmienna X przyjmuje wartości dodatnie całkowite, $\mathsf{E}\,X < \infty$, oraz $\mathsf{P}[X = i] \geq \mathsf{P}[X = j]$ dla $i \leq j$. Pokaż $\mathsf{P}[X = n] \leq 2\mathsf{E}\,X/n^2$.

13. Niech $\mathsf{E}\,X = \mu$ oraz $\mathrm{Var}\,X = \sigma^2$. Pokaż nierówność $\mathsf{P}[X \geq \mu + a] \leq \frac{\sigma^2}{\sigma^2+a^2}$.
Wskazówka: Nierówność Markowa. Jeżeli $\mathsf{E}\,Y = 0$ to $\mathrm{Var}\,Y = \mathsf{E}\,Y^2$.

14. *Problem zbieracza kuponów:* Każde pudełko płatków śniadaniowych zawiera jeden spośrod n rodzajów kuponów. Rodzaj kuponu w i-tym kupionym pudełku to wartość zmiennej X_i, zakładamy, że $\langle X_i \rangle_{i \geq 1}$ są niezależne i mają taki sam *rozkład jednostajny*, to znaczy przyjmują każdą z możliwych wartości rodzaju kuponu z takim samym prawdopobieństwem. Kupujemy pudełka do chwili gdy zbierzemy wszystkie kupony. Pokaż, że oczekiwana liczba kupionych pudełek jest $\mathcal{O}(n \log n)$.

MMD Wykład 12.

Bogdan Chlebus

Łańcuchy Markowa. Rozważamy nieskończony ciąg kolejnych prób lub eksperymentów. Niech zajście zdarzenia E po kolejnej próbie zależy tylko od wyników tej i poprzednich prób. Jeżeli ciąg czasów oczekiwania na kolejne wystąpienia E jest ciągiem niezależnych zmiennych losowych o takim samym rozkładzie, to zdarzenie E nazywamy *rekurencyjnym*.

Przykład: Niech próbą będzie próba Bernoulliego, na przykład rzut monetą. Niech zdarzenie E zachodzi w n-tym kroku, gdy liczby wyrzucanych orłów i reszek są sobie równe. Odpowiada to powrotowi do zera przy błądzeniu losowym na prostej. Zauważmy, że pozycja cząstki na prostej w kroku n zależy od pozycji w kroku $n-1$, ale gdy E zajdzie, to czas oczekiwania na następne wystąpienie E ma taki sam rozkład jak na samym początku eksperymentu, oraz jest niezależny od wszystkich takich czasów. $\Diamond$

Niech f_n oznacza prawdopodobieństwo pierwszego wystąpienia E w kroku n, a g_n prawdopodobieństwo, że E ma miejsce w kroku n, gdzie ustalamy dodatkowo, że $g_0 = 1$ i $f_0 = 0$. Definicję zdarzenia rekurencyjnego można wyrazić inaczej następująco:

$$g_n = f_1 g_{n-1} + f_2 g_{n-2} + \ldots + f_n g_0 \ , \tag{1}$$

dla $n \geq 1$. Ponieważ $f_0 = 0$, widzimy, że ciąg $\langle g_n \rangle$ jest splotem ciągów $\langle f_n \rangle$ i $\langle g_n \rangle$, dla $n \geq 1$. Niech

$$F(z) = \sum_{n \geq 0} f_n z^n \qquad \text{i} \qquad G(z) = \sum_{n \geq 0} g_n z^n$$

będą odpowiednimi funkcjami tworzącymi. Z własności splotu $G(z) - 1 = F(z)G(z)$, czyli

$$G(z) = \frac{1}{1 - F(z)} \ . \tag{2}$$

Liczba $f = \sum_{n \geq 0} f_n$ to prawdopodobieństwo, że E kiedyś zajdzie. Jeżeli $f = 1$ to E nazywamy *powracającym*. Wtedy ciąg $\langle f_n \rangle$ jest rozkładem prawdopodobieństwa czasu oczekiwania na pierwsze wystąpienie zdarzenia E, a liczba $\mu = \sum_{n \geq 0} n f_n$ jest jego wartością oczekiwaną, zwaną *średnim czasem powrotu*. Jeżeli $f < 1$ to E nazywamy *chwilowym* i przyjmujemy $\mu = \infty$. Podobnie liczba $g - 1$, gdzie $g = \sum_{n \geq 0} g_n$, to oczekiwana liczba wystąpień E. Ma miejsce użyteczne kryterium: E jest powracające w.t.w. gdy $g = \infty$. W dowodzie korzystamy z twierdzenia Abela. Jeżeli E jest powracające, to $\lim_{z \uparrow 1} F(z) = f = 1$ i z wzoru (2) mamy $g = \lim_{z \uparrow 1} G(z) = \infty$. Jeżeli E jest chwilowe, to podobnie $g = \lim_{z \uparrow 1} G(z) = \frac{1}{1-f} < \infty$. Zdarzenie rekurencyjne E ma *okres* $t > 1$, jeżeli $g_n = 0$ dla n nie będących wielokrotnością t, oraz t jest najmniejsza dodatnią liczbą całkowitą o tej własności. Zdarzenie E jest *okresowe* gdy ma okres większy od 1.

Przykład: Niech E to zdarzenie powrotu do zera w błądzeniu na prostej. Ma ono okres 2, bowiem cząstka nie może wrócić w kroku nieparzystym. E jest zdarzeniem powracającym tylko w przypadku błądzenia symetrycznego. Rozważmy błądzenie z odbijającymi barierami: jeżeli cząstka osiąga barierę, to w następnym kroku wraca do poprzedniej pozycji. Przypuśćmy, że są dwie takie bariery a cząstka jest pomiędzy nimi. Cząstka zaczyna na lewej barierze. Zdarzenie powrotu do lewej bariery jest zawsze powracające, jeżeli tylko prawdopodobieństwa ruchów w prawo i lewo są niezerowe poza barierami (ćwiczenie). $\Diamond$

Niech $X = \langle X_0, X_1, X_2, \ldots \rangle$ ciąg zmiennych losowych o wartościach całkowitych dodatnich. W kontekście łańcuchów Markowa stosujemy następującą terminologię: Jeżeli $X_i = j$ to powiemy, że X *jest w stanie* j *w chwili* i. Jeżeli $X_{n-1} = k$ oraz $X_n = j$ to X *w kroku* n *przechodzi ze stanu* k *do* j. Oto główna definicja: X jest (jednorodnym) *łańcuchem Markowa* gdy prawdopodobieństwo przejścia do stanu j w kroku n zależy tylko od tego, w jakim stanie X jest po kroku $n-1$. Formalnie

$$\begin{aligned}&\mathsf{P}[X_n = j \mid X_{n-1} = k, X_{n-2} = k_{n-2}, \ldots, X_0 = k_0] \\ &= \mathsf{P}[X_n = j \mid X_{n-1} = k] = \mathsf{P}[X_1 = j \mid X_0 = k] \ .\end{aligned}$$

Własność, że liczby $\mathsf{P}[X_n = j \mid X_{n-1} = k]$ nie zależą od n nazywamy *jednorodnością*. Używamy ustalonych oznaczeń na pewne prawdopodobieństwa:

(1) $p_k(n) = \mathsf{P}[X_n = k]$, a rozkład $p_k(0)$ nazywamy *początkowym*;

(2) $p_{kj} = \mathsf{P}[X_n = j \mid X_{n-1} = k]$, macierz $P = [p_{kj}]$ nazywamy *macierzą przejścia* X. Jest ona *stochastyczna*, to znaczy, że ma wartości nieujemne, które sumują sie do 1 w każdym wierszu.

(3) $p_{ij}(n) = \mathsf{P}[X_{k+n} = j \mid X_k = i]$, macierz $P_n = [p_{ij}(n)]$ to *macierz przejścia w* n *krokach*.

Zachodzą *równania Chapmana-Kołmogorowa:*

$$p_{ij}(s+u) = \sum_k p_{ik}(s) \cdot p_{kj}(u) \ ,$$

co wynika z wzoru na prawdopodobieństwo całkowite:

$$\mathsf{P}[X_{s+u} = j \mid X_0 = i] = \sum_k \mathsf{P}[X_{s+u} = j \mid X_s = k] \cdot \mathsf{P}[X_s = k \mid X_0 = i] \ .$$

W notacji macierzowej: $P_{s+u} = P_s \cdot P_u$, w szczególności $P_n = P^n$. Rozkład dowolnej zmiennej Y o wartościach całkowitych nieujemnych to ciąg $\langle \mathsf{P}[Y = i] \rangle_{i \geq 0}$. Jeżeli $a = \langle a_1, a_2, \ldots \rangle$ jest rozkładem początkowym łańcucha Markowa X, czyli rozkładem X_0, to rozkład X_n dany jest wzorem $a \cdot P^n$.

Przykład: Rozważmy błądzenie na dodatniej półprostej z odbijającą barierą w punkcie o współrzędnej 0. Niech X_n to pozycja cząstki w kroku n. Bez względu na to w jaki sposób cząstka osiągnęła pozycję $X_{n-1} = k$, następna pozycja X_n zależy tylko od wartości k, oraz liczby $\mathsf{P}[X_n = j \mid X_{n-1} = k]$ są takie same dla wszystkich n. Zatem mamy łańcuch Markowa, którego stanami są współrzędne cząstki. Oto nieskończona macierz przejścia P:

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & \ldots \\ q & 0 & p & 0 & 0 & \ldots \\ 0 & q & 0 & p & 0 & \ldots \\ 0 & 0 & q & 0 & p & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{bmatrix}$$

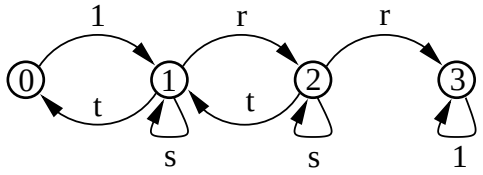
gdzie p to prawdopodobieństwo ruchu w prawo, i $q = p - 1$. $\Diamond$

Jeżeli $X_0 = i$ to powrót do stanu i jest zdarzeniem rekurencyjnym. Zamiast o własnościach tego zdarzenia mówimy krócej o własnościach stanu i, na przykład, że stan i jest okresowy. W szczególności i jest stanem powracającym gdy $\sum_n p_{ii}(n) = \infty$ a chwilowym gdy $\sum_n p_{ii}(n) < \infty$. Jeżeli i chwilowy to $\lim_{n\to\infty} p_{ii}(n) = 0$. Niech $f_{ij}(n)$ to prawdopodobieństwo pierwszego dojścia do stanu j w kroku n, po starcie w stanie i. Liczba $f_{ij} = \sum_n f_{ij}(n)$ to prawdopodobieństwo zdarzenia, że stan j może być osiągnięty ze stanu i. Stan i jest powracający gdy $f_{ii} = 1$.

Przykład: Rozważmy błądzenie cząstki z lewą barierą odbijającą w punkcie 0 i prawą barierą pochłaniającą w punkcie 3, gdzie poza barierami prawdopodobieństwo ruchu w prawo równe r, w lewo t, a pozostania na miejscu równe s. Jest to skończony łańcuch Markowa o czterech stanach $0, 1, 2, 3$. Oto jego macierz przejścia:

$$Q = \begin{bmatrix} 0 & 1 & 0 & 0 \\ t & s & r & 0 \\ 0 & t & s & r \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Taki łańcuch można też przedstawić jako etykietowany graf skierowany, w którym wierzchołki odpowiadają stanom, krawędzie przejściom ze stanu do stanu z niezerowym prawdopodobieństwem, etykiety to odpowiednie prawdopodobieństwa, patrz rysunek 1.



Rysunek 1: Łańcuch Markowa z macierzą przejścia Q przedstawiony jako skierowany graf etykietowany.

Dla tego łańcucha obliczymy prawdopodobieństwo $f_{1,0}$. Rozważmy pierwszy ruch cząstki ze stanu 1, z wzoru na prawdopodobieństwo całkowite mamy

$$f_{1,0} = t \cdot 1 + s \cdot f_{1,0} + r \cdot f_{2,0} \ . \tag{3}$$

Podobnie $f_{2,0} = t \cdot f_{1,0} + s \cdot f_{2,0} + r \cdot 0$. Obliczamy $f_{2,0}(1-s) = t \cdot f_{1,0}$ i po podstawieniu do wzoru (3) dostajemy $f_{1,0} = t \cdot (r + t - \frac{rt}{r+t})^{-1}$. Podobnie można obliczyć każda liczbę f_{ij}, w szczególności, że $f_{i,3} = 1$ (ćwiczenie). Przypuśćmy, że cząstka zaczyna błądzenie w stanie X_0, gdzie zmienna X_0 ma jakiś rozkład $a = \langle a_0, a_1, a_2, a_3 \rangle$. Jeżeli cząstka startuje w stanie i to jest pochłaniana przez stan 3 po oczekiwanym czasie $m_i = \sum_{n\geq 0} n \cdot f_{i,3}(n)$. Początkowa pozycja dana przez a, zatem oczekiwany czas pochłonięcia równy $m = \sum_{0\leq i\leq 3} a_i \cdot m_i$. Obliczymy m bez konieczności sumowania szeregów $\sum_n f_{ij}(n)$. Mianowicie, następujący układ równań

$$\begin{aligned} m_0 &= m_1 + 1 \\ m_1 &= tm_0 + sm_1 + rm_2 + 1 \\ m_2 &= tm_1 + sm_2 + rm_3 + 1 \end{aligned}$$

$$m_3 = 0$$

określa wartości m_i. Intuicyjnie wynika to z tego, że po jednym kroku cząstka znajdzie się w jednym z sąsiednich stanów z odpowiednim prawdopodobieństwem, ale to kosztuje jednostkę czasu, jest to rodzaj odpowiednika wzoru na prawdopodobieństwo całkowite. Oto formalny dowód: Z wzoru na prawdopodobieństwo całkowite, następujące równania

$$f_{1,3}(n+1) = tf_{0,3}(n) + sf_{1,3}(n) + rf_{2,3}(n)$$

są prawdziwe dla każdego $n \geq 0$. Stąd

$$t \cdot m_0 + s \cdot m_1 + r \cdot m_2 = \sum_{n\geq 0} n f_{1,3}(n+1)$$

$$= \sum_{n\geq 0}(n+1)f_{1,3}(n+1) - \sum_{n\geq 0} f_{1,3}(n+1) = m_1 - f_{1,3} = m_1 - 1 \ ,$$

ponieważ $f_{1,3}(0) = 0$. Podobnie uzasadniamy pozostałe równania. $\Diamond$

Zachodzi następujące równanie analogiczne do (1):

$$p_{ik}(n) = \sum_{j=1}^{n} f_{ik}(j)p_{kk}(n-j) \tag{4}$$

dla $n \geq 1$, czyli $\langle p_{ik}(n)\rangle_n$ jest splotem ciągów $\langle f_{ik}(n)\rangle_n$ oraz $\langle p_{kk}(n)\rangle_n$ dla $n \geq 1$. Określmy funkcje tworzące:

$$F_{ik}(z) = \sum_{n\geq 0} f_{ik}(n)z^n \qquad \text{i} \qquad P_{ik}(z) = \sum_{n\geq 0} p_{ik}(n)z^n.$$

Z równania (4) wynika równość $P_{ik}(z) = [i = k] + F_{ik}(z)P_{kk}(z)$. Korzystając z twierdzenia Abela widzimy, że jeżeli k jest powracający, czyli $\lim_{z\uparrow 1} P_{kk}(z) = \infty$, to także $\sum_{n\geq 0} p_{ik}(n) = \infty$, o ile $f_{ik} > 0$. Podobnie, jeżeli k jest chwilowy, to $\sum_{n\geq 0} p_{ik}(n) < \infty$, w szczególności $\lim_{n\to\infty} p_{ik}(n) = 0$.

Stan j jest *osiągalny* ze stanu i gdy $f_{ij} > 0$. Stany i oraz j sa *wzajemnie osiągalne* gdy $f_{ij} \cdot f_{ji} > 0$. Wzajemna osiągalność jest relacją równoważności. Jej klasy abstrakcji nazywamy *nieprzywiedlnymi* zbiorami stanów, a gdy jest tylko jedna klasa to cały łańcuch nazywamy nieprzywiedlnym (to ogólna reguła: gdy wszystkie stany mają jakąś własność to tak nazywamy łańcuch). Rozważmy dwa stany i oraz j wzajemnie osiągalne. Niech s i u liczby takie, że $p_{ij}(s) > 0$ i $p_{ji}(u) > 0$. Z równania Chapmana-Kołmogorowa wynika, że dla każdego $n \geq 0$ całkowitego zachodzi $p_{ii}(s+n+u) \geq p_{ij}(s) \cdot p_{jj}(n) \cdot p_{ji}(u)$. Czyli prawdziwa jest nierówność

$$p_{ii}(n+s+u) \geq c \cdot p_{jj}(n) \ , \tag{5}$$

dla pewnej $c > 0$. Podobnie

$$p_{jj}(n+s+u) \geq c \cdot p_{ii}(n) \ . \tag{6}$$

Te nierówności implikują następujące równoważności:

$$\lim_{n\to\infty} p_{jj}(n) = 0 \qquad \text{w.t.w.} \qquad \lim_{n\to\infty} p_{ii}(n) = 0 \ ; \tag{7}$$

$$\sum_{n\geq 0} p_{jj}(n) = \infty \qquad \text{w.t.w.} \qquad \sum_{n\geq 0} p_{ii}(n) = \infty \ . \tag{8}$$

Z (8) wynika, że jeżeli dwa stany są wzajemnie osiągalne to są albo oba chwilowe albo oba powracające. Także mają ten sam okres: mianowicie, niech t_i oraz t_j okresy stanów i oraz j odpowiednio. Z (5) oraz (6) wynika, że $t_i \mid (s+u)$ oraz $t_j \mid (s+u)$, a stąd dalej, że $t_i \mid t_j$ oraz $t_j \mid t_i$, czyli $t_i = t_j$.

Zbiór stanów C jest *zamknięty* gdy $p_{ij} = 0$ dla każdej pary stanów $i \in C$ oraz $j \notin C$. Ma miejsce *twierdzenie o rozkładzie:* zbiór wszystkich stanów rozkłada się jednoznacznie na rozłączne podzbiory $T \cup C_1 \cup C_2 \cup \ldots$, gdzie T jest zbiorem stanów chwilowych a każdy C_i jest nieprzywiedlnym i zamkniętym zbiorem stanów powracających. Rzeczywiście, niech $C_1 \cup C_2 \cup \ldots$ będzie podziałem stanów powracających na klasy abstrakcji relacji wzajemnej osiągalności. Przypuśćmy, że istnieją dwa stany i oraz j z różnych klas, dla których $p_{ij} > 0$. Oczywiście wtedy $f_{ji} = 0$. Stan i nie może być powracający bowiem

$$f_{ii} = \sum_k p_{ik} f_{ki} \leq \sum_{k\neq j} p_{ik} < 1$$

ponieważ $p_{ij} > 0$ – sprzeczność. Ten fakt wyjaśnia w pewnym stopniu zachowanie się łańcucha wraz z upływem czasu: Jeżeli zaczyna w stanie chwilowym, to albo zawsze jest w takich stanach albo kiedyś przechodzi do stanu powracającego, i wtedy na zawsze pozostaje w odpowiednim zbiorze nieprzywiedlnym. Gdy łańcuch jest w zbiorze nieprzywiedlnym to pozostale stany tak jakby nie istniały, to motywuje rozważanie łańcuchów nieprzywiedlnych.

Średni czas powrotu stanu k określamy jako $\mu_k = \sum_{n\geq 0} n f_{kk}(n)$, gdy k jest powracający, i $\mu_k = \infty$ gdy k jest chwilowy. Stan powracający jest *zerowy* gdy $\lim_{n\to\infty} p_{kk}(n) = 0$, w przeciwnym przypadku jest *niezerowy* lub *dodatni*. Jeżeli dwa stany powracające są wzajemnie osiągalne to albo oba są zerowe albo oba dodatnie, co wynika z równoważności (7).

W nieprzywiedlnym łańcuchu Markowa wszystkie stany są albo chwilowe albo powracające zerowe albo powracające dodatnie. Skończony łańcuch nieprzywiedlny musi zawierać stan dodatni, a zatem cały być dodatni. Rzeczywiście, gdyby wszystkie stany były chwilowe lub zerowe to $\lim_{n\to\infty} p_{ij}(n) = 0$, dla każdego i oraz j (zadanie 9). Macierz P^n ma skończoną liczbę kolumn, wiersz nie może mieć sumy wyrazów równej 1 i zbiegać do zera.

Przykład: Błądzenie cząstki na prostej pomiędzy dwoma odbijającymi barierami to skończony nieprzywiedlny łańcuch Markowa, o ile poza barierami można iść w każdym kierunku z niezerowym prawdopodobieństwem. Stąd wszystkie stany nie dość, że powracające, to także dodatnie. Gdy jedną z barier zamienimy na pochłaniająca, łańcuch przestaje być nieprzywiedlny: wszystkie stany oprócz pochłaniającego są chwilowe, a stan pochłaniający stanowi jednoelementowy zamknięty nieprzywiedlny zbiór stanów. $\Diamond$

Przykład: Rozważamy błądzenie symetryczne w d wymiarowej przestrzeni Euklidesowej E^d. Cząstka porusza się wśród punktów o wszystkich d współrzędnych całkowitych. W każdym kroku cząstka zmienia wartość każdej ze swych d współrzędnych o ± 1 z prawdopodobieństwem $1/2$ niezależnie. Jest to łańcuch Markowa, gdzie stany to punkty przestrzeni o wszystkich współrzędnych całkowitych. Pokażemy, że dla $d \leq 2$ wszystkie stany są powracające zerowe, a dla $d \geq 3$ wszystkie stany są chwilowe. Niech $d = 1$: błądzenie po prostej. Oznaczmy przez g_n prawdopodobieństwo, że cząstka po n krokach znów jest w punkcie startu:

$$g_{2n} = \binom{2n}{n} 2^{-2n} = \frac{(2n)!}{(n!)^2} \cdot 2^{-2n} \ .$$

Ze wzoru Stirlinga, $n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n (1 + o(1))$. Stąd dostajemy

$$g_{2n} = \frac{\sqrt{4\pi n}\left(\frac{2n}{e}\right)^{2n}}{2\pi n \left(\frac{n}{e}\right)^{2n}} \cdot 2^{-2n} \cdot (1 + o(1)) = (\pi n)^{-\frac{1}{2}}(1 + o(1)) \ .$$

Jeżeli $g_n^{(d)}$ oznacza prawdopodobieństwo powrotu w n-tym kroku do punktu startu dla d wymiarów, to $g_{2n}^{(d)} = (g_{2n})^d = \Theta(n^{-d/2})$. Dla $d \leq 2$, mamy $\sum_n g_{2n}^{(d)} = \infty$, stąd stany są powracające, a zerowość wynika z tego, że $g_{2n}^{(d)} \to 0$ dla $n \to \infty$. Dla $d \geq 3$ mamy $\sum_n g_{2n}^{(d)} < \infty$, wtedy stany są chwilowe. Zatem prawdopodobieństwo powrotu cząstki do punktu startu jest równe 1 dla $d \leq 2$ oraz mniejsze niż 1 dla $d \geq 3$. $\Diamond$

Zadania

1. Pokaż, że dla łańcucha Markowa z rysunku 1 zachodzi $f_{i,3} = 1$ dla $0 \leq i \leq 3$. Znajdź podział stanów tego łańcucha na chwilowe, powracające zerowe i powracające dodatnie.

2. Łańcuch skończony ma macierz przejścia P jak niżej. Podaj rozkład na stany chwilowe i nieprzywiedlne zamknięte zbiory stanów powracających.

$$P = \begin{bmatrix} 1/3 & 1/3 & 0 & 1/3 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 1/3 & 2/3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

3. Łańcuch skończony ma stany $\{0, 1, 2\}$ i macierz przejścia $P = \begin{bmatrix} 1/2 & 1/4 & 1/4 \\ 1/3 & 1/3 & 1/3 \\ 0 & 0 & 1 \end{bmatrix}$ Oblicz prawdopodobieństwa $f_{i,j}$ dla każdych $0 \leq i \leq 2$ oraz $0 \leq j \leq 2$.

4. Pokaż, że jeżeli łańcuch jest nieprzywiedlny i powracający to $f_{ij} = 1$ dla każdych i, j.

5. Niech łańcuch Markowa ma macierz przejścia $P = \begin{bmatrix} 1/4 & 3/4 \\ 2/3 & 1/3 \end{bmatrix}$. Oblicz średnie czasy powrotu stanów $\mu_i = \sum_{n \geq 0} n f_{ii}(n)$ bezpośrednio z tej formuły.

6. W nieskończonym ciągu prób Bernoulli'ego sukces zachodzi z prawdopodobieństwem p. Oznaczmy zajście sukcesu przez $\mathcal{S}$ a porażki przez $\mathcal{P}$. Jaka jest oczekiwana liczba prób do chwili pojawienia się schematu $\mathcal{SPPS}$?

7. Rozważmy nieskończony ciąg rzutów monetą symetryczną, których wynikiem jest orzeł $\mathcal{O}$ lub reszka $\mathcal{R}$. Jeden z graczy stawia na to, że ciąg $\mathcal{OOR}$ pojawi się pierwszy, a drugi, że XYZ. Rozważ dwa przypadki: a) XYZ=$\mathcal{ORR}$, oraz b) XYZ=$\mathcal{RRO}$. Dla każdej z tych gier oblicz prawdopodobieństwo wygranej każdego z graczy, oraz oczekiwany czas trwania gry.

8. Niech ciąg $\langle c_n \rangle$ będzie splotem ciągów $\langle a_n \rangle$ i $\langle b_n \rangle$, gdzie $\sum_{n\geq 0} a_n < \infty$ oraz $b_n \to 0$. Pokaż, że $c_n \to 0$.

9. Pokaż, że jeżeli stan k jest chwilowy lub powracający zerowy, natomiast i jest dowolnym stanem, to zachodzi $\lim_{n\to\infty} p_{ik}(n) = 0$.
Wskazówka: Skorzystaj z (4) oraz zadania 8.

10. Rozważmy błądzenie losowe w d-wymiarowej przestrzeni Euklidesowej, w którym cząstka zmienia tylko jedną współrzędną, w każdym kroku niezależnie i losowo wybraną, o 1 lub -1 z prawdopodobieństwem $\frac{1}{2}$. Pokaż, że dla $d \leq 2$ wszystkie stany są powracające zerowe, a dla $d \geq 3$ wszystkie stany są chwilowe.

11. Podaj przykład nieskończonego nieprzywiedlnego łańcucha Markowa, w którym wszystkie stany są powracające dodatnie.

12. Oszacuj prawdopodobieństwo powrotu do początku układu współrzędnych dla błądzenia symetrycznego w E^3.

13. Jaki jest oczekiwany czas powrotu dla błądzenia symetrycznego w E^2?

MMD Wykład 13.

Bogdan Chlebus

Rozkłady stacjonarne łańcuchów Markowa.

Rozkład prawdopodobieństwa $a = \langle a_1, a_2, \ldots \rangle$ na stanach łańcucha Markowa $\langle X_0, X_1, \ldots \rangle$ o macierzy przejścia P nazywamy *stacjonarnym* jeżeli $aP = a$. Nazwa bierze się stąd, że jeżeli a jest rozkładem początkowym X_0, to potem każde X_n ma taki rozkład. Łańcuch nieprzywiedlny, który jest bądź chwilowy bądź zerowy, nie ma rozkładu stacjonarnego. Rzeczywiście, przypuśćmy, że a jest takim rozkładem stacjonarnym. Zachodzi szacowanie

$$\sum_{i \geq 1} a_i p_{ij}(n) \leq \sum_{i=1}^{m} a_i p_{ij}(n) + \sum_{i>m} a_i \rightarrow_{n \rightarrow \infty} 0 \ ,$$

ponieważ składnik $\sum_{i>m} a_i$ może być dowolnie mały dla dostateczne dużego m, po jego ustaleniu bierzemy dostatecznie duże n. Ten rodzaj argumentu nazywamy *przez zbieżność ograniczoną*. Kontynuując: ponieważ dla każdego j zachodzi $a_j = \sum_{i \geq 1} a_i p_{ij}(n)$, dostajemy że $a_j = 0$, co jest w sprzeczności z $\sum_j a_j = 1$.

Jeżeli istnieje rozwiązanie $x = \langle x_1, x_2, \ldots \rangle$ równania $xP = x$ takie, że $x_i \geq 0$ oraz $0 < \sum_n x_n < \infty$ to ciąg $\langle x_i / \sum_n x_n \rangle_i$ jest rozkładem stacjonarnym. Pokażemy, że jeżeli łańcuch jest nieprzywiedlny to istnieje dodatnie rozwiązanie x równania $xP = x$, to znaczy o wszystkich wyrazach $x_i > 0$. Niech s będzie dowolnym stanem. Określmy x_i jako średnią liczbę odwiedzin stanu i od startu w s do czasu pierwszego powrotu do s. Niech $h_i(n)$ to prawdopodobieństwo, że łańcuch w n-tym kroku po opuszczeniu s jest w stanie i, bez powrotów do s w międzyczasie. Stąd $f_{ss}(k+l) \geq h_i(k) f_{is}(l)$. Niech $f_{is}(l) > 0$ dla pewnej liczby l, która istnieje z nieprzywiedlności. Wtedy $h_i(k) \leq f_{ss}(k+l)/f_{is}(l)$, czyli

$$x_i = \sum_{k \geq 1} h_i(k) \leq \frac{1}{f_{is}(l)} \sum_{k \geq 1} f_{ss}(k+l) \leq f_{is}(l)^{-1} < \infty \ ,$$

zatem x_i jest dobrze określony. Mamy $h_i(1) = p_{si}$ oraz $h_i(k) = \sum_{j \neq s} h_j(k-1) p_{ji}$, dla $k > 1$. Stąd

$$\begin{aligned} x_i = \sum_{k \geq 1} h_i(k) &= p_{si} + \sum_{k \geq 2} h_i(k) = p_{si} + \sum_{k \geq 2} \sum_{j \neq s} h_j(k-1) p_{ji} \\ &= p_{si} + \sum_{j \neq s} p_{ji} \sum_{k \geq 1} h_j(k) = x_s p_{si} + \sum_{j \neq s} x_j p_{ji} \ , \end{aligned}$$

czyli $xP = x$. Przypuśćmy, że $x_j = 0$ dla pewnego j. Pokażemy, że wtedy $x_i = 0$ dla każdego i. Zachodzi szacowanie:

$$0 = x_j = \sum_i x_i \cdot p_{ij}(n) \geq x_i \cdot p_{ij}(n).$$

Ponieważ łańcuch jest nieprzywiedlny, więc dla pewnego n mamy $p_{ij}(n) > 0$, czyli rzeczywiście $x_i = 0$. Wszystko to jest to w sprzeczności z $\sum_i x_i = \mu_s$, gdzie $\mu_s > 0$ oznacza średni czas powrotu do s. Razem widzimy, że $\langle x_i \rangle$ jest dodatni. Jeżeli dodatkowo $\mu_s < \infty$ to ciąg $\langle x_i / \mu_s \rangle_i$ jest rozkładem prawdopodobieństwa i jest to rozkład stacjonarny.

Podsumujmy:

1. Jeżeli w łańcuchu nieprzywiedlnym istnieje choć jeden stan o skończonym średnim czasie powrotu, to istnieje rozkład stacjonarny.

2. W łańcuchu nieprzywiedlnym powracającym zerowym wszystkie stany mają nieskończone średnie czasy powrotu, bo wiemy, że w takich łańcuchach nie ma rozkładu stacjonarnego.

3. Czy może być tak, że łańcuch jest nieprzywiedlny powracający dodatni oraz nie ma rozkładu stacjonarnego, czyli ma wszystkie średnie czasy powrotu nieskończone? Nie jest to możliwe; uzasadnimy to później.

Pokazaliśmy, że nieprzywiedlny łańcuch powracający ma rozkład stacjonarny, o ile istnieje stan s taki, że $\mu_s < \infty$. Pokażemy, że wtedy $\mu_i < \infty$ dla *każdego* stanu i. Niech r_i to czas pierwszego dojścia do i po starcie. W szczególności $r_i > 0$. Niech rozkład początkowy będzie równy rozkładowi stacjonarnemu a, czyli $\mathsf{P}[X_0 = k] = a_k$. Zbadamy wielkość

$$a_i\mu_i = a_i \sum_{j\geq 0} \mathsf{P}[r_i > j \mid X_0 = i] = \sum_{j\geq 0} \mathsf{P}[r_i > j, X_0 = i].$$

Rozważmy ciąg $b_k = \mathsf{P}[X_n \neq i \text{ dla } m \leq n < m+k]$. Jest to prawdopodobieństwo zdarzenia, że przez k kolejnych kroków łańcuch jest w stanie różnym od i, które jest niezależne od numeru początkowego kroku, bowiem każde X_n ma ten sam rozkład. Wyraźmy składniki $\mathsf{P}[r_i > j, X_0 = i]$ przez liczby b_k. Dla $j = 0$ mamy

$$\mathsf{P}[r_i > 0, X_0 = i] = \mathsf{P}[X_0 = i] = \mathsf{P}[X_1 = i] = 1 - b_1 \ .$$

Natomiast dla $j > 0$:

$$\begin{aligned}\mathsf{P}[r_i > j, X_0 = i] &= \mathsf{P}[X_n \neq i \text{ dla } 1 \leq n \leq j, X_0 = i] \\ = \mathsf{P}[X_n \neq i \text{ dla } 1 \leq n \leq j] - \mathsf{P}[X_n \neq i \text{ dla } 0 \leq n \leq j] &= b_j - b_{j+1} \ .\end{aligned}$$

Stąd $a_i\mu_i = 1 - b_1 + b_1 - \lim_{j\to\infty} b_j = 1 - \lim_{j\to\infty} b_j$. Pokażemy, że $b_j \to 0$. Skorzystamy z tego że jest to łańcuch nieprzywiedlny powracający, zatem $f_{ki} = 1$.

$$\begin{aligned}\lim_{j\to\infty} b_j &= \lim_{j\to\infty} \mathsf{P}[X_n \neq i \text{ dla } 1 \leq i \leq j] = \lim_{j\to\infty} \sum_{k\geq 1} a_k \cdot \mathsf{P}[X_n \neq i \text{ dla } 1 \leq i \leq j \mid X_0 = k] \\ &= \lim_{j\to\infty} \sum_{k\geq 1} a_k \cdot (1 - \sum_{1\leq n\leq j} f_{ki}(n)) = 1 - \lim_{j\to\infty} \sum_{k\geq 1} a_k \cdot \sum_{1\leq n\leq j} f_{ki}(n) \\ &= 1 - \sum_{k\geq 1} a_k \lim_{j\to\infty} \sum_{1\leq n\leq j} f_{ki}(n) = 1 - \sum_{k\geq 1} a_k f_{ki} = 0 \ ,\end{aligned}$$

gdzie zamiana sumy z przejściem granicznym jest ze zbieżności ograniczonej (zadania 11 i 12). Stąd $a_i\mu_i = 1$. Pokazaliśmy zatem, że jeżeli w nieprzywiedlnym łańcuchu Markowa istnieje stan s taki, że $\mu_s < \infty$, to istnieje rozkład stacjonarny a, oraz $\mu_i = a_i^{-1} < \infty$ dla każdego stanu i. Teraz zajmiemy się pytaniem czy prawdziwe jest odwrotne wynikanie.

Rozważmy zbiór V wszystkich rozwiązań równania $xP = x$, gdzie P to macierz przejścia nieprzywiedlnego łańcucha. V jest przestrzenią liniową, jako zbiór rozwiązań

układu równań liniowych. Wiemy, że istnieje co najmniej jedno rozwiązanie dodatnie $x = \langle x_i \rangle$, to znaczy takie, że $x_i > 0$. Wiemy także, że jeżeli choć jedno $x_i = 0$ to $x = 0$. Pokażemy, że wymiar V jest równy 1. Niech $y = \langle y_i \rangle \in V$ dowolne rozwiązanie niezerowe. Jeżeli $z = \langle z_i \rangle \in V$ rozwiązanie to $y \cdot z_1 y_1 = \langle y_1 z_1 / y_1, y_2 z_1 / y_1, \dots \rangle$ ma taki sam pierwszy wyraz jak z, zatem $z - y\frac{z_1}{y_1}$ ma pierwszy wyraz równy 0, czyli $z = y \cdot \frac{z_1}{y_1}$. To pokazuje, że zbiór złożony z y tworzy bazę, zatem każde niezerowe rozwiązanie $xP = x$ jest bazą.

Przypuśćmy teraz, że istnieje rozkład stacjonarny a dla łańcucha nieprzywiedlnego. Zbiór $\{a\}$ jest bazą V. Każdy inny $y = \langle y_i \rangle \in V$ jest postaci $t \cdot a$, dla t rzeczywistego, zatem $\sum_i y_i = t < \infty$. Stąd wynika, że istnieje dokładnie jeden rozkład stacjonarny. Niech s dowolny stan. Rozważaliśmy ciąg $x = \langle x_i \rangle$, gdzie x_i to oczekiwana liczba odwiedzin stanu i pomiędzy dwiema kolejnymi wizytami w s, i pokazaliśmy, że $x \in V$ oraz $\sum x_i = \mu_s$. Stąd dostajemy, że jeżeli istnieje rozkład stacjonarny $a = \langle a_i \rangle$ dla nieprzywiedlnego łańcucha Markowa, to każdy stan i ma skończony średni czas powrotu μ_i równy a_i^{-1}.

Przykład: Błądzenie losowe po grafie. Rozważmy spójny graf prosty $G = \langle V, E \rangle$. Oznaczmy $m = |E|$. Cząstka umieszczona jest w jednym z wierzchołków i w kolejnych krokach przesuwa sie po krawędziach G. Jeżeli jest w wierzchołku v oraz $\{v, t\} \in E$ to prawdopodobieństwo przejścia z v do t jest równe $\frac{1}{\deg v}$. Otrzymujemy łańcuch Markowa, stan to wierzchołek G, w którym jest cząstka. Łańcuch jest nieprzywiedlny, ponieważ G jest spójny. Pokażemy, że rozkład stacjonarny $a = \langle a_v \rangle_{v \in V}$ jest określony przez $a_v = \frac{\deg v}{2m}$. Jest to rozkła prawdopodobieństwa z lematu o uściskach dłoni. Wystarczy zatem pokazać $aP = a$, gdzie P macierz przejścia. Sprawdzamy dla dowolnego wierzchołka t:

$$\sum_{v \in V} a_v \cdot P[v, t] = \sum_{\{v,t\} \in E} \frac{\deg v}{2m} \cdot \frac{1}{\deg v} = \frac{\deg t}{2m} = a_t \ .$$

Stąd oczekiwany czas powrotu do wierzchołka o stopniu d jest równy $2m/d$. $\Diamond$

Przykład: Kolejka. Rozważmy kolejkę obsługującą klientów pojawiających sie losowo, na starcie kolejka pusta. Wszystkie zdarzenia przybycia nowych i obsłużenia czekających klientów są niezależne. W każdym kroku:

(a) do kolejki dochodzi nowy klient z prawdopodobieństwem $\alpha > 0$;

(b) jeżeli już jest jakiś klient w kolejce, to z prawdopodobieństwem $\beta > 0$ najdłużej czekający opuszcza kolejkę.

Jest to łańcuch Markowa, którego stanami są liczby klientów w kolejce. Zbadamy dla jakich zależności między liczbami α i β łańcuch jest chwilowy a dla jakich powracający.

Zauważmy, że zachowanie kolejki można interpretować jak błądzenie dyskretne po nieujemnej części prostej z barierą w punkcie zero. Odpowiednie prawdopodobieństwa ruchu w lewo lub w prawo wyznaczamy następująco: Gdy kolejka pusta, to z prawdopodobieństwem α liczba klientów zwiększa się o 1, a z prawdopodobieństwem $1 - \alpha$ pozostaje równa 0. Gdy kolejka niepusta, to z prawdopodobieństwem $r = \alpha(1 - \beta)$ liczba klientów zwiększa się o 1, z prawdopodobieństwem $l = \beta(1 - \alpha)$ zmniejsza się o 1, z prawdopodo-

bieństwem $s = 1 - r - l$ pozostaje bez zmiany. Oto macierz przejścia:

$$P = \begin{bmatrix} 1-\alpha & \alpha & 0 & 0 & 0 & 0 & \cdots \\ l & s & r & 0 & 0 & 0 & \cdots \\ 0 & l & s & r & 0 & 0 & \cdots \\ 0 & 0 & l & s & r & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

Jest to łańcuch nieprzywiedlny. Sprawdzimy jak wyglądają ciągi $x = \langle x_0, x_1, x_2, \ldots \rangle$ takie, że $xP = x$. To równanie macierzowe jest równoważne ciągowi równań, którego pierwsze wyrazy wyglądają następująco:

$$\begin{aligned} x_0(1-\alpha) + x_1 l &= x_0 \\ x_0\alpha + x_1 s + x_2 l &= x_1 \\ x_1 r + x_2 s + x_3 l &= x_2 \quad \text{itd.} \end{aligned}$$

Możemy to zapisać jako równanie rekurencyjne zależne od x_0:

$$\begin{aligned} x_1 &= x_0 \frac{\alpha}{l} \ , \\ x_2 &= x_0 \frac{\alpha r}{l^2} \ , \\ x_{n+2} &= x_{n+1} \frac{r+l}{l} - x_n \frac{r}{l} \quad \text{dla } n \geq 1, \end{aligned}$$

lub bez warunków brzegowych w postaci

$$x_n l - x_{n-1}(r+l) + x_{n-2} r + a[n=0] + b[n=1] + c[n=2] = 0 \ , \tag{1}$$

gdzie $a = -x_0 l$, $b = x_0(r + l - \alpha)$, $c = x_0(\alpha - r)$, oraz $x_i = 0$ dla $i < 0$. Niech $F(t) = \sum_{n\geq 0} t^n x_n$ funkcja tworząca dla $\langle x_n \rangle$. Mnożąc (1) przez t^n i sumując po n dostajemy: $lF(t) - (r+l)tF(t) + rt^2F(t) = -a - bt - ct^2$, czyli

$$F(t) = \frac{-a - bt - ct^2}{rt^2 - (r+l)t + l} = x_0 \cdot \frac{(r-\alpha)t^2 + (\alpha - r - l)t + l}{rt^2 - (r+l)t + l} \ .$$

Przedstawmy mianownik w postaci $l(1 - d_1 t)(1 - d_2 t)$. Liczby d_1, d_2 są pierwiastkami równania $lt^2 - (r+l)t + r = 0$, czyli są równe $(r + l \pm \sqrt{\Delta})/2l$, gdzie $\Delta = (r+l)^2 - 4lr = (r-l)^2$. Stąd $d_1 = \frac{r}{l}$, $d_2 = 1$. Przedstawmy licznik w postaci $l(1 - c_1 t)(1 - c_2 t)$. Liczby c_1, c_2 są pierwiastkami równania $lt^2 + (\alpha - r - l)t + (r - \alpha) = 0$, skąd wyznaczamy ich wartości $c_1 = \frac{r-\alpha}{l}$, $c_2 = 1$. Czynnik $1 - t$ występuje w liczniku i mianowniku, po skróceniu dostajemy

$$\begin{aligned} F(t) &= x_0 \frac{1 - \frac{r-\alpha}{l} t}{1 - \frac{r}{l} t} = x_0 \Big(1 + \frac{\alpha t}{l} \cdot \frac{1}{1 - \frac{r}{l} t} \Big) \\ &= x_0 \Big(1 + \sum_{n\geq 0} \big(\frac{r}{l}\big)^n \frac{\alpha}{l} \cdot t^{n+1} \Big) = x_0 \Big(1 + \sum_{n \geq 1} \frac{r^{n-1}\alpha}{l^n} t^n \Big) \ . \end{aligned}$$

Stąd wyrazy ciągu $\langle x_n \rangle$ dla $n \geq 1$ są równe:

$$x_n = x_0 \cdot \frac{\alpha}{l} \cdot \left(\frac{r}{l}\right)^{n-1} .$$

Jeżeli $r < l$ to $\sum_{n\geq 0} x_n < \infty$. Przyjmując wartość x_0 taką, żeby $\sum_{n\geq 0} x_n = 1$, dostajemy rozkład stacjonarny. Wyznaczymy takie x_0. Ponieważ

$$1 = x_0\Big(1 + \sum_{n\geq 1} \big(\frac{r}{l}\big)^{n-1} \frac{\alpha}{l}\Big) = x_0\Big(1 + \frac{\alpha}{l} \cdot \frac{l}{l-r}\Big) = x_0 \frac{\beta}{\beta - \alpha} ,$$

więc $x_0 = \frac{\beta-\alpha}{\beta} = 1 - \frac{\alpha}{\beta}$. Razem pokazaliśmy, że średni czas czekania aż powtórzy się n klientów w kolejce jest równy $\frac{\beta}{\beta-\alpha}$ dla $n = 0$, oraz $\frac{\beta}{\beta-\alpha}\frac{l}{\alpha}(\frac{l}{r})^{n-1}$ dla $n > 0$, czyli rośnie wykładniczo wraz z n. Każdy stan jest powracający dodatni.

Rozważmy przypadek $r > l$. Niech f_{ij} prawdopodobieństwo, że będzie kiedyś j klientów po tym jak jest ich i. Z wzoru na prawdopodobieństwo całkowite $f_{1,1} = l f_{0,1} + s + r f_{2,1}$. Wznaczymy $f_{0,1}$ i $f_{2,1}$. Mamy $f_{0,1} = \alpha \sum_{i\geq 0}(1-\alpha)^i = 1$. Rozważmy błądzenie bez bariery, w którym l, s, r oznaczają prawdopodobieństwa odpowiednich ruchów, i niech f'_{ij} to prawdopodobieństwo osiągnięcia kiedyś pozycji j po starcie w i. Pokażemy, że $2r f_{2,1} = f'_{1,1} - s$. Zauważmy najpierw, że $f'_{1,1} - s$ to prawdopodobieństwo powrotu na start po ruchu w pierwszym kroku dla błądzenia bez bariery, natomiast $r f_{2,1}$ to prawdopodobieństwo powrotu przy ruchu w prawo w pierwszym kroku. Jeżeli nie ma bariery, to każda powracająca trajektoria zaczynająca się od ruchu w prawo ma odpowiadającą jej zaczynającą się od ruchu w lewo, o takim samym prawdopodobieństwie, co kończy uzasadnienie. Podstawiamy i szacujemy:

$$f_{1,1} = l + s + \frac{1}{2}(f'_{1,1} - s) \leq 1 - r + \frac{1}{2}(1 - s) = 1 - r + \frac{1}{2}(l + r) < 1 - r + r = 1 ,$$

ponieważ $l < r$. Zatem stan 1 nie jest powracający, czyli cały łańcuch jest chwilowy.

Dla $r = l$ to samo rozumowanie daje $f_{1,1} = 1$ o ile podstawimy wartość $f'_{1,1} = 1$ (ćwiczenie), czyli mamy łańcuch powracający. Ten łańcuch jest zerowy (zadanie 5), podobnie jak symetryczne błądzenie na prostej.

Podsumujmy: jeżeli $\alpha > \beta$ to łańcuch chwilowy; jeżeli $\alpha = \beta$ to łańcuch powracający zerowy; jeżeli $\alpha < \beta$, to łańcuch powracający dodatni. Tylko w ostatnim przypadku obsługa kolejki będzie w praktyce działać. $\Diamond$

Przykład: Szereg kolejek. Rozważmy kolejkę powracającą, to znaczy gdy $\beta > \alpha$. Przypuśćmy, że do jednej takiej kolejki przychodzi razem grupa n klientów. Zostaną oni obsłużeni w czasie $\mathcal{O}(n)$ z prawdopodobieństwem wykładniczo bliskim 1, co wynika z nierówności Chernoffa dla zmiennej o rozkładzie dwumianowym. Ustawmy n takich kolejek $Q_1, \ldots, Q_n$ szeregowo, to znaczy klient zaczyna od kolejki Q_1, i po obsłużeniu przez kolejkę Q_i, dla $i < n$, przechodzi do kolejki Q_{i+1}. Przypuśćmy, że grupa n nowych klientów przychodzi jednocześnie do szeregu kolejek $Q_1, \ldots, Q_n$. Pokażemy, że zostaną oni obsłużeni w czasie $\mathcal{O}(n)$ z prawdopodobieństwem wykładniczo bliskim 1.

Zauważmy, że jeżeli początkowa liczba klientów w jednej takiej kolejce ma rozkład taki sam jak wyznaczony wyżej rozkład stacjonarny $\langle x_k \rangle$, to prawdopodobieństwo zdarzenia,

że w pierwszym kroku zostanie obsłużony klient jest równe $(1-x_0)\cdot\beta = \frac{\alpha}{\beta}\beta = \alpha$. Niech w każdym kroku pojawia się nowy klient do kolejki Q_1 z prawdopodobieństwem α. Wtedy, dla każdej kolejki Q_i, jeżeli liczba klientów w pierwszym kroku ma rozkład $\langle x_k \rangle$ to będzie miała taki sam rozkład w przyszłości, oraz w każdym kroku z prawdopodobieństwem α pojawi się nowy klient dla Q_i, i z takim samym prawdopodobieństwem α kolejkę Q_i opuści obsłużony klient.

Wróćmy do sytuacji, gdy grupa n nowych klientów przychodzi do szeregu kolejek $Q_1, \ldots, Q_n$. Wstawmy ich do kolejki Q_0, skąd przechodzą do Q_1. Załóżmy, na potrzeby szacowania, że w kolejkach Q_i dla $i > 0$ są jeszcze starzy klienci, niech ich liczby mają rozkłady stacjonarne $\langle x_k \rangle$ w każdej z kolejek. Oszacujemy ilu jest razem starych klientów. Rozważmy zmienną Y o rozkładzie geometrycznym $\mathsf{P}[Y = k] = (1-q)q^{k-1}$, dla $k \geq 1$. Kładąc $q = \frac{r}{l}$ sprawdzamy, że $(1-q)q^{k-1} > x_k$, dla $k > 0$. Zmienna Y ma rozkład czasu oczekiwania na pierwszy sukces w ciągu prób Bernoulliego z prawdopodobieństwem sukcesu $1-q$. Zatem prawdopodobieństwo, że liczba starych klientów jest równa s jest mniejsze niż prawdopodobieństwo zdarzenia, że w s-tej takiej próbie Bernoulli'ego uzyskamy n-ty sukces. Odwołując się znów do nierówności Chernoffa dla rozkładu dwumianowego dostajemy, że z prawdopodobieństwem wykładniczo bliskim 1 względem n wystarczy wykonać $\mathcal{O}(n)$ prób by otrzymać n sukcesów. Zatem z takim prawdopodobieństwem jest $\mathcal{O}(n)$ starych klientów. Czekamy na obsłużenie $\mathcal{O}(n)$ wszystkich klientów, zatem n nowych klientów zostanie obsłużonych przez wszystkie kolejki w czasie $\mathcal{O}(n)$, z prawdopodobieństwem wykładniczo bliskim 1. $\Diamond$

Zadania

1. Niech łańcuch Markowa o dwóch stanach ma macierz przejścia $P = \begin{bmatrix} 1/4 & 3/4 \\ 2/3 & 1/3 \end{bmatrix}$. Oblicz średnie czasy powrotu każdego stanu znajdując rozkład stacjonarny.

2. Podaj przykład łańcucha Markowa, który ma dwa różne rozkłady stacjonarne.

3. Macierz przejścia łańcucha jest *podwójnie stochastyczna* gdy sumy kolum są równe 1. Pokaż, że jeżeli taki łańcuch jest skończony to jego rozkładem stacjonarnym jest rozkład jednostajny, to znaczy taki gdzie wszystkie prawdopodobieństwa są równe.

4. Rozważmy kolejkę z parametrami α i β, jak opisano w treści wykładu. Oszacuj rzędy wartości oczekiwanych: (a) liczby klientów w kroku n, i (b) maksymalnej liczby klientów w czasie pierwszych n kroków. W szczególności pokaż że, dla $\alpha > \beta$, po n krokach będzie $\Omega(n)$ klientów w kolejce z prawdopodobieństwem wykładniczo bliskim 1.

5. Rozważmy kolejkę, w której pojawia się nowy klient z prawdopodobieństwem α i pierwszy klient w niepustej kolejce jest obsługiwany z prawdopodobieństwem α. Pokaż, że jest to łańcuch powracający zerowy.

6. Rozważmy kolejkę powracającą, to znaczy taką, że jeżeli jest niepusta to prawdopodobieństwo jej zmniejszenia jest większe niż powiększenia. Pokaż z nierówności

Chernoffa, że jeżeli w kolejce jest $x > 0$ klientów, to z prawdopodobieństwem 1 kiedyś ich liczba będzie mniejsza niż x.

7. Znajdź nieprzywiedlny łańcuch Markowa o trzech stanach, którego rozkładem stacjonarnym jest ciąg $\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{6} \rangle$.

8. Niech $Q[i,j]$ symetryczna macierz stochastyczna. Niech $\langle \pi_i \rangle$ rozkład prawdopodobieństwa na tym samym zbiorze stanów, każde $\pi_i \neq 0$. Określmy $P[i,j] = Q[i,j] \min[1, \frac{\pi_j}{\pi_i}]$ dla $i \neq j$. Niech wartości $P[i,i]$ określone tak, by macierz P była macierzą stochastyczną. Pokaż, że rozkład $\langle \pi_i \rangle$ jest rozkładem stacjonarnym dla łańcucha Markowa o macierzy przejścia P.

9. Znajdź nieskończony nieprzywiedlny łańcuch Markowa, którego rozkładem stacjonarnym jest rozkład Poissona.

10. Do kolejki przychodzą klienci w krokach nieparzystych, ich liczby to niezależne zmienne losowe o takich samych rozkładach. W krokach parzystych klienci mogą opuścić kolejkę: każdy zgłasza niezależnie z prawdopodobieństwem p chęć opuszczenia kolejki, jeżeli jest tylko jeden chętny to opuszcza kolejkę, gdy więcej niż jeden to wszyscy pozostają w tym kroku. Niech s_i to prawdopodobieństwo, że w danym kroku nieparzystym zgłosi się i nowych klientów do kolejki. Pokaż, że jeżeli $s_0 + s_1 < 1$ to oczekiwana liczba klientów którzy kiedykolwiek opuszczą kolejkę jest $\mathcal{O}(1)$.

11. Jeżeli $b_n \to b$ i $\sum_{k \geq 0} a_k = a < \infty$ to $\lim_{n\to\infty} \sum_{k\geq 0} a_k b_n = \sum_{k \geq 0} \lim_{n\to\infty} a_k b_n$.

12. Jeżeli $\lim_{n\to\infty} c_{kn} = c_k$ oraz $|c_{kn}| \leq d_k$, gdzie $\sum_{k\geq 0} d_k < \infty$, to $\lim_{n\to\infty} \sum_{k\geq 0} c_{kn} = \sum_{k\geq 0} c_k$.

MMD Wykład 14.

Bogdan Chlebus

Ewolucja łańcuchów Markowa.

Łańcuch Markowa $X = \langle X_0, X_1, \dots \rangle$ nazywamy *ergodycznym* gdy jest nieprzywiedlny, nieokresowy, oraz każdy stan i ma skończony średni czas powrotu $\mu_i < \infty$.

Przykład: Rozważmy błądzenie losowe po grafie prostym $G = \langle V, E \rangle$, który jest spójny ale nie jest dwudzielny. Niech $m = |E|$ będzie liczbą krawędzi. Łańcuch jest nieprzywiedlny, ponieważ G jest spójny. Istnieje w grafie G cykl nieparzystej długości, ponieważ nie jest on dwudzielny. Istnieją zamknięte marszruty dowolnej parzystej długości, bowiem cząstka może oscylować między parą wierzchołków połączonych krawędzią. Zatem największym wspólnym dzielnikiem długości zamkniętej marszruty jest 1, czyli łańcuch jest nieokresowy. Wiemy, że każdy wierzchołek stopnia d ma średni czas powrotu $2m/d$. Wszystko to razem oznacza, że łańcuch jest ergodyczny. $\Diamond$

Jak wiemy, każdy łańcuch ergodyczny ma rozkład stacjonarny $\langle \mu_i^{-1} \rangle_i$. Teraz pokażemy, że rozkłady odwiedzenia stanów w kolejnych krokach zbiegają do rozkładu stacjonarnego, to znaczy zachodzi $\lim_{n\to\infty} p_k(n) = \mu_k^{-1}$. Zbieżność ciągów $p_{ij}(n)$ wraz z $n \to \infty$ ma miejsce także dla pewnych łańcuchów bez skończonych średnich czasów powrotu, mianowicie, jeżeli łańcuch jest tylko nieprzywiedlny i nieokresowy to ma miejsce równość

$$\lim_{n\to\infty} p_{ij}(n) = \frac{1}{\mu_j} \ , \tag{1}$$

co obejmuje także przypadek $\mu_j = \infty$, wtedy przyjmujemy $\mu_j^{-1} = 0$.

Zaczniemy od tej własności nieokresowych łańcuchów, ktora jest potrzebna jest w dowodzie równości 1. Pokażemy, że jeżeli X jest nieprzywiedlnym łańcuchem nieokresowym to dla każdej pary stanów i, j istnieje taka stała $c > 0$, że $p_{ij}(n) > 0$ dla $n > c$. Nieokresowość stanu j oznacza, że największą liczbą dzielącą wszystkie n takie, że $p_{jj}(n) > 0$ jest 1. Zatem istnieje skończony ciąg $n_1, \dots, n_s$ taki, że $\mathrm{NWD}(n_1, \dots, n_s) = 1$, oraz $p_{ij}(n_i) > 0$ dla $1 \le i \le s$. Istnieją także takie liczby całkowite b_i, że $\sum_{i=1}^{s} b_i n_i = 1$ (ćwiczenie). Niech $n_0 = n_1 + \cdots + n_s$. Każda liczba całkowita n jest postaci $n = an_0 + b$, gdzie $0 \le b < n_0$. Stąd

$$n = a \sum_{k=1}^{s} n_k + b \sum_{k=1}^{s} b_k n_k = \sum_{k=1}^{s} (a + b \cdot b_k) \cdot n_k \ .$$

Jeżeli $a \ge |n_0 b_k|$ dla $1 \le k \le s$, to $a + bb_k \ge 0$. Zatem istnieje $d_1 > 0$ taka, że każda liczba $n > d_1$ jest postaci $n = \sum c_k n_k$, gdzie $c_k \ge 0$. Niech $d_2 > 0$ takie, że $p_{ij}(d_2) > 0$, istnienie d_2 wynika z nieprzywiedlności. Wtedy, jeżeli $n > d_1$ to

$$p_{ij}(d_2 + n) \ge p_{ij}(d_2) \cdot \prod_{k=1}^{s} p_{jj}(c_k \cdot n_k) \ge p_{ij}(d) \cdot \prod_{k=1}^{s} (p_{jj}(n_k))^{c_k} > 0 \ .$$

Czyli możemy położyć $c = d_1 + d_2$. Stąd wynika, że jeżeli P jest macierzą przejścia skończonego nieprzywiedlnego nieokresowego łańcucha Markowa, to macierze P^n mają wszystkie wyrazy niezerowe dla dostatecznie dużych n.

W dowodzie zbieżności wykorzystamy *metodę couplingu*, która opiera się na następującej konstrukcji łączenia dwóch niezależnych kopii X i Y tego samego łańcucha Markowa. Niech $X = \langle X_0, X_1 \dots \rangle$ i $Y = \langle Y_0, Y_1 \dots \rangle$ ciągi zmiennych losowych, które są łańcuchami Markowa o tych samych stanach i macierzy przejścia, oraz każde X_i oraz Y_j są niezależne. Określamy $Z = \langle X, Y \rangle = \langle Z_0, Z_1, Z_2, \dots \rangle$, gdzie $Z_k = \langle X_k, Y_k \rangle$, oraz prawdopodobieństwo $p_{\langle a,b\rangle\langle c,d\rangle}$ przejścia ze stanu $\langle a, b\rangle$ do $\langle c, d\rangle$ jest równe $p_{a,c} \cdot p_{b,d}$. Jeżeli X i Y kopie nieprzywiedlnego i nieokresowego łańcucha, to także Z ma te własności. Mianowicie, wystarczy pokazać, że dla dowolnych $\langle a, b\rangle$ oraz $\langle c, d\rangle$ stanów Z liczby $p_{\langle a,b\rangle\langle c,d\rangle}(n)$ są większe od 0 dla wszystkich dostatecznie dużych n. Ten fakt wynika z określenia prawdopodobieństw przejść dla Z oraz z tego, że $p_{a,c}(n) > 0$ i $p_{b,d}(n) > 0$ dla dostatecznie dużych n.

Coupling stosujemy dla pokazania następującego faktu: jeżeli Z jest nieprzywiedlny oraz powracający, to zachodzi

$$\lim_{n\to\infty} (p_{ij}(n) - p_{kj}(n)) = 0 \ . \tag{2}$$

Ustalmy rozkład początkowy $Z_0 = \langle X_0, Y_0\rangle = \langle k, i\rangle$. Z prawdopodobieństwem 1 czas oczekiwania na dojście Z do stanu o obu współrzędnych równych sobie jest skończony, ponieważ Z jest powracający. Niech D zmienna losowa określająca ten czas. Rozkłady X_n i Y_n są takie same od momentu osiągnięcia stanu postaci $\langle u, u\rangle$. Szacujemy:

$$p_{kj}(n) = \mathsf{P}[X_n = j] = \mathsf{P}[X_n = j, D \le n] + \mathsf{P}[X_n = j, D > n]$$
$$= \mathsf{P}[Y_n = j, D \le n] + \mathsf{P}[X_n = j, D > n] \le \mathsf{P}[Y_n = j] + \mathsf{P}[D > n] = p_{ij}(n) + \mathsf{P}[D > n] \ .$$

Podobnie $p_{ij}(n) \le p_{kj}(n) + \mathsf{P}[D > n]$ czyli $|p_{ij}(n) - p_{kj}(n)| \le \mathsf{P}[D > n]$. Ale $\mathsf{P}[D < \infty] = 1$ czyli $\mathsf{P}[D > n] \to 0$, co pokazuje (2).

Przedstawimy teraz dowód równości (1). Niech X łańcuch nieprzywiedlny i nieokresowy.

1. Zaczniemy od przypadku gdy j jest powracający o skończonym średnim czasie powrotu $\mu_j < \infty$. Zatem istnieje rozkład stacjonarny $a = \langle a_i\rangle$ dla X, pokażemy że $\lim_{n\to\infty} p_{ij}(n) = a_j$. Łańcuch Z też jest nieprzywiedlny i ma rozkład stacjonarny (zadanie 1), a stąd jest powracający. Przekształcamy: $a_j - p_{ij}(n) = \sum_k a_k(p_{kj}(n) - p_{ij}(n))$, a to wyrażenie zbiega do zera, przez argument o zbieżności ograniczonej na mocy (2), co pokazuje (1).

2. Rozważmy przypadek, gdy j jest powracający o nieskończonym średnim czasie powrotu $\mu_j = \infty$. Gdyby Z był chwilowy to miałoby miejsce

$$p^2_{ij}(n) = p_{\langle i,i\rangle\langle j,j\rangle}(n) \to 0 \ ,$$

przy $n \to \infty$, zatem także $p_{ij} \to 0$, co dałoby (1). Zatem możemy założyć, że Z jest powracający, czyli zachodzi (2). Przypuśćmy, że $p_{ij}(n)$ nie zbiega do 0 przy $n \to \infty$. Ponieważ $p_{ij}(n)$ jest ograniczony, więc istnieje rosnący ciąg $\langle n_1, n_2 \dots \rangle$ taki, że $p_{ij}(n_l) \to b_j \neq 0$ przy $l \to \infty$. Z (2) wynika, że dla każdego stanu k zachodzi $p_{kj}(n_l) \to b_j \neq 0$ przy $l \to \infty$. Chcielibyśmy mieć taki ciąg$\langle n_1, n_2 \dots \rangle$, żeby $p_{ij}(n_l) \to b_j$ dla wszystkich j i odpowiednich b_j. Niech $\langle s_1, s_2 \dots \rangle$ lista wszystkich stanów. Wybieramy ciąg rosnący

$c_1 = \langle m_{1,1}, m_{1,2} \dots \rangle$ taki, że $p_{is_1}(m_{1,l}) \to b_{s_1} \neq 0$ przy $l \to \infty$. Następnie z ciągu c_1 wybieramy podciąg $c_2 = \langle m_{2,1}, m_{2,2} \dots \rangle$ taki, że $p_{is_2}(m_{2,l}) \to b_{s_2}$ przy $l \to \infty$; teraz b_{s_2} nie musi być różne od 0. Kontynuujemy ten proces dla wszystkich stanów, co daje ciąg ciągów $\langle c_1, c_2 \dots \rangle$. Jeżeli jest on skończony, to ostatni ciąg jest dobry, w przeciwnym przypadku ciąg $\langle n_k \rangle = \langle m_{kk} \rangle$ ma własność, że $p_{ij}(n_k) \to b_j$ dla wszystkich j, przy $k \to \infty$, gdzie ciąg $b = \langle b_j \rangle$ jest nieujemny niezerowy. Pokażemy, że mają wtedy miejsce dwa fakty: równość $b = Pb$, gdzie P to macierz przejścia, oraz $\sum_j b_j < \infty$. Razem dają one istnienie rozkładu stacjonarnego dla X, co jest w sprzeczności z $\mu_j = \infty$. Ograniczoność $\sum_i b_i$ wynika z tego, że $\sum_{j=1}^{m} b_j = \lim_{s\to\infty} \sum_{j=1}^{m} p_{ij}(n_s) \leq 1$ dla każdego $m \geq 1$. Ma miejsce także szacowanie

$$\sum_{1\leq k\leq m} p_{ik}(n_s) \cdot p_{kj} \leq p_{ij}(n_s + 1) = \sum_{k\geq 1} p_{ik} \cdot p_{kj}(n_s) \ .$$

Przechodząc z $n_s \to \infty$ widzimy, że $\sum_{1\leq k\leq m} b_k \cdot p_{kj} \leq \sum_{k\geq 1} p_{ik} \cdot b_j = b_j \sum_{k\geq 1} p_{ik} = b_j$. Stąd $\sum_{k\geq 1} b_k \cdot p_{kj} \leq b_j$. Zachodzi równość, czyli $\sum_{1\leq k\leq m} b_k \cdot p_{kj} = b_j$, ponieważ

$$\sum_{j\geq 1} \sum_{k\geq 1} b_k \cdot p_{kj} = \sum_{k\geq 1} b_k \sum_{j\geq 1} p_{kj} = \sum_{k\geq 1} b_k \ .$$

Zatem pokazaliśmy, że $\lim_{n\to\infty} p_{ij}(n) = 0 = \mu_j^{-1}$.

3. Ostatnim przypadkiem jest stan chwilowy j: wtedy $\lim_{n\to\infty} p_{ij}(n) = 0$ oraz $\mu_j = \infty$.

To kończy dowód równości (1) dla łańcuchów nieprzywiedlnych nieokresowych.

Łańcuchy ergodyczne mają niezerowy rozkład stacjonarny, i rozkłady prawdopodobieństw odwiedzenia stanów zbiegają z czasem do tego rozkładu. Ma to miejsce bez względu na rozkład początkowy, jeżeli bowiem $a = \langle a_1, a_2, \dots \rangle$ jest jakimś rozkładem początkowym, to

$$\lim_{n\to\infty} p_k(n) = \lim_{n\to\infty} \sum_{i\geq 1} a_i \cdot p_{ik}(n) = \sum_{i\geq 1} a_i \lim_{n\to\infty} p_{ik}(n) = \sum_{i\geq 1} a_i \cdot \mu_k^{-1} = \mu_k^{-1} \ ,$$

z ograniczonej zbieżności.

Zrewidujmy klasyfikację łańcuchów Markowa X w przypadku nieprzywiedlnym powracającym. Jeżeli X jest łańcuchem zerowym, to $\lim_{n\to\infty} p_{ij}(n) = 0$ oraz $\mu_j = \infty$, dla każdego stanu j. Jeżeli łańcuch X jest dodatni i nieokresowy, to $p_{ij}(n) \to \mu_j^{-1}$, ale ponieważ łańcuch nie jest zerowy, więc $\lim_{n\to\infty} p_{jj}(n) > 0$, zatem z równości (1) mamy, że $\mu_j < \infty$. Jeżeli łańcuch dodatni X ma okres t, to łańcuch $Y = \langle Y_n \rangle$ określony przez $Y_n = X_{nt}$ jest nieokresowy. Stąd mamy $\lim_{n\to\infty} p_{ij}(nt) = t \cdot \mu_j^{-1}$, gdzie μ_j to średni czas powrotu do j dla łańcucha Y, ponieważ średni czas powrotu stanu w Y jest t razy krótszy niż w X. Widzimy, że jeżeli Y ma skończone średnie czasy powrotów, to także łańcuch X ma tę własność. Zatem podział łańcuchów nieprzywiedlnych powracających na zerowe i dodatnie odpowiada podziałowi na takie łańcuchy, dla których średni czas powrotu stanów jest nieskończony i skończony, odpowiednio. Łańcuchy ergodyczne można zatem określić jako łańcuchy, które są nieprzywiedlne, dodatnie, i nieokresowe. Wiemy, że łańcuch nieprzywiedlny ma rozkład stacjonarny w.t.w. gdy średnie czasy powrotów

są skończone. Zatem każdy nieprzywiedlny łańcuch jest dodatni w.t.w. gdy ma rozkład stacjonarny.

Zajmiemy się teraz szybkością zbieżności ergodycznych łańcuchów do rozkładu stacjonarnego. Pokażmy, że dla każdego skończonego i ergodycznego łańcucha Markowa zbieżność ta jest wykładnicza, to znaczy, istnieje stała $0 \le r < 1$ taka, że $|p_{ij}(n) - a_j| = \mathcal{O}(r^n)$, gdzie $\langle a_j \rangle$ to rozkład stacjonarny. Weźmy dwa stany g i h. Oszacujemy różnicę

$$\begin{aligned} p_{gj}(n+1) - p_{hj}(n+1) &= \sum_k (p_{gk} - p_{hk}) p_{kj}(n) \\ &\le l_j(n) \sum_{k \in C} (p_{gk} - p_{hk}) + s_j(n) \sum_{k \in D} (p_{gk} - p_{hk}) \ , \end{aligned} \tag{3}$$

gdzie określamy, że $k \in C$ o ile $p_{gk} \ge p_{hk}$, a w przeciwnym przypadku, że $k \in D$, oraz $s_j(n) = \min_k p_{kj}(n)$, $l_j(n) = \max_k p_{kj}(n)$. Zauważmy, że

$$\sum_{k \in C} (p_{gk} - p_{hk}) = -\sum_{k \in D} (p_{gk} - p_{hk}) \ .$$

Stąd (3) szacuje się przez $(l_j(n) - s_j(n)) \sum_{k \in C} (p_{gk} - p_{hk})$. Niech r oznacza maksymalną wartość $\sum_{k \in C} (p_{gk} - p_{hk})$ po wszystkich parach stanów g, h. Dostajemy zależność rekurencyjną

$$l_j(n+1) - s_j(n+1) \le r \cdot (l_j(n) - s_j(n)) \ ,$$

a stąd $l_j(n) - s_j(n) \le r^n$. To kończy dowód, o ile $r < 1$, bowiem $p_{ij}(n) \to a_j$, $s_j(n) \le p_{ij}(n) \le l_j(n)$, oraz ciąg $s_j(n)$ jest niemalejący, a ciąg $l_j(n)$ nierosnący (zadanie 5). Warunek $r < 1$ jest spełniony gdy macierz przejścia P ma wszystkie wyrazy różne od zera, bowiem

$$\sum_{k \in C} (p_{gk} - p_{hk}) = \sum_{k \in C} p_{gk} - \sum_{k \in C} p_{hk} = 1 - \sum_{k \in D} p_{gk} - \sum_{k \in C} p_{hk} = 1 - \sum_k \min[p_{gk}, p_{hk}] \ .$$

Jeżeli P ma zerowe wyrazy to nie ma ich macierz P^t dla pewnego całkowitego $t > 0$. Niech $r < 1$ będzie odpowiednią stałą dla łańcucha o macierzy przejścia P^t. Przedstawmy dowolną nieujemną liczbę całkowitą m jako $m = tn + u$, gdzie $0 \le u < t$. Wtedy

$$l_j(m) - s_j(m) = l_j(tn+u) - s_j(tn+u) \le l_j(tn) - s_j(tn) \le r^n \le r^{m/t - 1} \ .$$

Zatem dostajemy szukane szacowanie $|p_{ij}(m) - a_j| = O\left((r^{1/t})^m\right)$.

Przykład: Niech i będzie stanem skończonego ergodycznego łańcucha Markowa. Niech $a = \langle a_j \rangle$ rozkład stacjonarny, oraz $v_i(n)$ liczba odwiedzin stanu i w ciągu n kroków. Pokażemy, że zachodzi szacowanie

$$\mathsf{P}\left[\left|\frac{v_i(n)}{n} - a_i\right| = \mathcal{O}\left(n^{-3/4}\right)\right] = 1 - O\left(e^{-\sqrt{n}/2}\right) \ .$$

Zauważmy, że jeżeli E jest zdarzeniem rekurencyjnym, a $v(n)$ oraz $e(n)$ oznaczają, odpowiednio, liczbę zajść i oczekiwaną liczbę zajść E w ciągu n prób, to zmienna v spełnia warunek Lipschitza ze stałą 1. Stąd, z nierówności Azumy, mamy szacowanie:

$$\mathsf{P}[|v(n) - e(n)| \ge c\sqrt{n}] \le 2e^{-c^2/2} \ .$$

Rozważmy szczególny przypadek, gdy E to odwiedziny i w czasie pierwszych n kroków. Jeżeli zaczynamy od stanu k to $e(n) = \sum_{j=1}^{n} p_{ki}(j)$. Napiszmy $v_i(n) - e(n)$ w postaci:

$$v_i(n) - e(n) = (v_i(n) - a_i n) + (a_i n - \sum_{j=1}^{n} p_{ki}(j)) \ .$$

Szacujemy prawy składnik:

$$\left| a_i n - \sum_{j=1}^{n} p_{ki}(j) \right| = \left| \sum_{j=1}^{n} (a_i - p_{ki}(j)) \right| \leq \sum_{j=1}^{n} |a_i - p_{ki}(j)| \leq \sum_{j=1}^{n} b \cdot r^j = O(1) \ ,$$

gdzie b pewna stała. Stąd $v_i(n) - a_i \cdot n + \mathcal{O}(1) = v_i(n) - e(n)$. Zatem

$$\mathsf{P}\Big[\Big|\frac{v_i(n)}{n} - a_i\Big| \geq \frac{c}{\sqrt{n}} + \mathcal{O}\Big(\frac{1}{n}\Big)\Big] \leq \mathsf{P}\left[|v_i(n) - e(n)| \geq c\sqrt{n}\right] \leq 2e^{-c^2/2} \ ,$$

przez dobranie odpowiedniej stałej w $\mathcal{O}(1/n)$. Kładąc $c = n^{-1/4}$ dostajemy tezę. W szczególności zachodzi $\lim_{n\to\infty} = \frac{v_i(n)}{n} = a_i$ z prawdopodobieństwem 1 dla wszystkich stanów i. $\Diamond$

Zadania

1. Niech $Z = \langle Z_n \rangle = \langle X, Y \rangle$ będzie podwójnym łańcuchem Markowa $Z_n = \langle X_n, Y_n \rangle$, gdzie X i Y niezależne łańcuchy o takich samych stanach i macierzach przejścia. Pokaż:

   (a) Jeżeli X i Y mają rozkład stacjonarny a to rozkład b określony wzorem $b_{\langle i,j \rangle} = a_i \cdot a_j$ jest rozkładem stacjonarnym dla Z.

   (b) Jeżeli X i Y są nieprzywiedlne powracające to Z też jest taki.

2. Pokaż następujące *twierdzenie o odnowieniu:* Niech E będzie powracającym nieokresowym zdarzeniem rekurencyjnym, niech g_n i f_n to prawdopodobieństwa zajścia i pierwszego zajścia zdarzenia E w n-tym kroku, odpowiednio, i niech średni czas powrotu równy $\mu = \sum_{n\geq 0} n f_n$. Pokaż równość $\lim_{n\to\infty} g(n) = 1/\mu$.
   Wskazówka: Rozważ odpowiedni nieprzywiedlny i nieokresowy łańcuch Markowa.

3. Niech E bedzie zdarzeniem rekurencyjnym powracającym o okresie $t > 1$. Pokaż, że $g_{nt} \to t\mu^{-1}$.

4. Pokaż, że jeżeli k jest stanem nieokresowym to dla każdego stanu i ma miejsce równość: $\lim_{n\to\infty} p_{ik}(n) = f_{ik}\mu_k^{-1}$.

5. Dla łańcucha Markowa określamy ciągi $s_j(n) = \min_k p_{kj}(n)$ oraz $l_j(n) = \max_k p_{kj}(n)$. Pokaż, że $s_j(n+1) \geq s_j(n)$ oraz $l_j(n+1) \leq l_j(n)$.

6. Cząstka błądzi po wierzchołkach trójkąta, idąc zgodnie z ruchem wskazówek zegara z prawdopodobieństwem 2/3, oraz w przeciwnym kierunku z prawdopodobieństwem 1/3. Znajdź średnie czasy powrotów μ_j^{-1} do wierzchołków, i oszacuj $|p_{ij}(n) - \mu_j^{-1}|$ w zależności od n.

7. Pokazaliśmy oszacowanie $\mathsf{P}\left[\left|\frac{v_i(n)}{n} - a_i\right| = \mathcal{O}\left(n^{-3/4}\right)\right] = 1 - \mathcal{O}\left(e^{-\sqrt{n}/2}\right)$, dla skończonego ergodycznego łańcucha Markowa, w którym nic nie mówi się o liczbie stanów. Czy nie jest to sprzeczne z intuicją, że im większy łańcuch, tym rzadziej będziemy odwiedzać ustalony stan?

MMD Wykład 15.

Bogdan Chlebus

Metody probabilistyczne w teorii grafów. Niech wierzchołkami grafu o n wierzchołkach będą liczby naturalne z przedziału $[1..n]$. Dla takiego ustalonego grafu G i dla krawędzi $e = \{i, j\} \subseteq \{1, \ldots, n\}$, niech X_e oznacza *zmienną wzkaźnikową* krawędzi e, określoną jako $X_e = [e \text{ jest krawędzią } G]$, gdzie $[\ldots]$ to notacja Iversona. Jeżeli E to zbiór wszystkich podzbiorów dwuelementowych $\{1, \ldots, n\}$ to rodzina funkcji $\{X_e : e \in E\}$ określa jednoznacznie graf G. *Grafem losowym* $\mathcal{G}(n, p)$ nazywamy rodzinę zmiennych losowych $\{X_e : e \in E\}$ które są niezależne, oraz $\mathsf{P}[X_e = 1] = p$, dla każdej $e \in E$. Prawdopodobieństwo p może być funkcją $p = p(n)$ zależną od n. Grafy $\mathcal{G}(n, p)$ są wdzięcznym obiektem rozważań, bowiem można je interpretować jako ciąg $n(n+1)/2$ prób Bernoulli'ego.

Można rozważać inne modele grafów losowych. Niech W jakaś własność grafów. *Losowym grafem o własności* W nazywamy przestrzeń probabilistyczną, której zdarzeniami elementarnymi są wszystkie grafy (o n wierzchołkach), które mają własność W, każde zdarzenie elementarne ma takie samo prawdopodobieństwo. Badanie losowych grafów o jakiejś własności jest zwykle trudniejsze niż grafów $\mathcal{G}(n, p)$. Jeszcze inny model losowych grafów przedstawiony jest z zadaniach 2 oraz 3.

Powiemy, że własność grafów W jest *monotoniczna* gdy każdy graf otrzymany z grafu mającego własność W przez dodanie krawędzi także ma własność W. Dla ustalonego parametru n, jeżeli p rośnie od 0 do 1 to graf $\mathcal{G}(n, p)$ staje się coraz gęstszy, czyli rośnie prawdopodobieństwo zajścia monotonicznej własności. Dla wielu monotonicznych własności W istnieje wąski przedział wartości p taki, że poniżej niej graf zwykle nie ma własności W, a po jego przekroczeniu graf losowy ma własność W z dużym prawdopodobieństwem.

Funkcja $f(n)$ jest *funkcją progową* własności W gdy zachodzi:
(1) jeżeli $p(n) = o(f(n))$ oraz $0 \leq p(n) \leq 1$ to $\lim_{n\to\infty} \mathsf{P}[G(n, p(n)) \text{ ma własność } W] = 0$;
(2) jeżeli $f(n) = o(p(n))$ oraz $0 \leq p(n) \leq 1$ to $\lim_{n\to\infty} \mathsf{P}[G(n, p(n)) \text{ ma własność } W] = 1$.

Mówimy że ciąg zdarzeń $\langle A_n \rangle_n$ zachodzi *prawie zawsze* gdy $\lim_{n\to\infty} \mathsf{P}[A_n] = 1$. Zatem $f(n)$ jest funkcją progową gdy poniżej niej dana wlasność nie zachodzi prawie zawsze a powyżej zachodzi prawie zawsze.

Rozważmy następującą prostą własność W: "graf zawiera ścieżkę długości 2". Dla każdego ciągu wierzchołków S o 3 elementach, niech W_S oznacza, że S jest ścieżką, i niech Y_S będzie odpowiednią zmienną wskaźnikową, tzn. równą 1/0 gdy W_S odpowiednio zachodzi lub nie. Wtedy $\mathsf{E}[Y_S] = \mathsf{P}[W_S] = p^2$. Określmy $Y_n = \frac{1}{2}\sum Y_S$, po wszystkich takich ciągach S. Wtedy $\mathsf{E}\,Y_n$ jest oczekiwaną liczbą ścieżek długości 2. Obliczmy:

$$\mathsf{E}\,Y_n = \frac{1}{2}\sum \mathsf{E}\,Y_S = \frac{n(n-1)(n-2)}{2} \cdot p^2 = \frac{n^3 p^2}{2} \cdot (1 + o(1)).$$

Stąd $\mathsf{E}\,Y_n = \Theta(1)$ w.t.w. gdy $p = \Theta(n^{-3/2})$. Pokażemy, że $f(n) = n^{-3/2}$ jest funkcją progową własności W istnienia ścieżki długości 2. Z naszych rozważań wynika, że jeżeli $p(n) = o(n^{-3/2})$ to $\mathsf{E}\,Y_n = o(1)$.

Zastosujemy *metodę pierwszego momentu*, to znaczy skorzystamy z następującego faktu: Niech $\langle X_n \rangle$ ciąg zmiennych losowych przyjmujących wartości całkowite nieujemne, jeżeli $\mathsf{E}\, X_n = o(1)$ to $X_n = 0$ prawie zawsze. Dla dowodu, podstawiamy $a = 1$ w nierówności Markowa $\mathsf{P}[X \geq a] \leq \frac{\mathsf{E}\, X}{a}$ i dostajemy $\mathsf{P}[X \geq 1] \leq \mathsf{E}\, X$. Stąd $1 - \mathsf{P}[X_n = 0] = \mathsf{P}[X_n \geq 1] \leq \mathsf{E}\, X_n = o(1)$.

Wracając do naszej funkcji progowej, wystarczy podstawić X_n równe Y_n, co pokazuje pierwszą część definicji funkcji progowej.

Przypadek $n^{-3/2} = o(p(n))$ jest trochę bardziej skomplikowany. Zastosujemy *metodę drugiego momentu*, to znaczy skorzystamy z następującego faktu: Niech $\langle X_n \rangle$ ciąg zmiennych losowych przyjmujących wartości całkowite nieujemne, jeżeli $\mathsf{E}\, X_n > 0$ oraz $\operatorname{Var} X_n = o((\mathsf{E}\, X_n)^2)$ to $X_n > 0$ prawie zawsze. Dla dowodu, podstawiamy $a = \mathsf{E}\, X_n / \sqrt{\operatorname{Var} X_n}$ w nierówności Czebyszewa $\mathsf{P}[|X - \mathsf{E}\, X_n| \geq a \cdot \sqrt{\operatorname{Var} X_n}] \leq a^{-2}$. Dostajemy

$$\mathsf{P}[X_n = 0] \leq \mathsf{P}[|X_n - \mathsf{E}\, X_n| \geq \mathsf{E}\, X_n] \leq \operatorname{Var} X_n / (\mathsf{E}\, X_n)^2 = o(1) \ .$$

Wróćmy do badanej kandydatki na funkcję progową. Naszym założeniem jest $n^{-3/2} = o(p(n))$, to znaczy $n^{3/2} p(n) \to \infty$. Korzystając z $\operatorname{Var} Y_n = \mathsf{E}\, Y_n^2 - (\mathsf{E}\, Y_n)^2$ dostajemy

$$\frac{\operatorname{Var} Y_n}{(\mathsf{E}\, Y_n)^2} = \frac{\mathsf{E}\, Y_n^2}{(\mathsf{E}\, Y_n)^2} - 1 = \frac{\mathsf{E}\, Y_n^2}{\frac{1}{4} n^6 p^4 (1 + o(1))} - 1 \ .$$

Szacujemy:

$$\begin{aligned} \mathsf{E}\, Y_n^2 = \mathsf{E}\,(\frac{1}{2} \sum Y_S)^2 = \frac{1}{4}(\mathsf{E}\, Y_S^2 + \mathsf{E} \sum_{S_1 \neq S_2} Y_{S_1} Y_{S_2}) = \frac{1}{2} \mathsf{E}\, Y_n + \frac{1}{4} \mathsf{E} \sum_{S_1 \neq S_2} Y_{S_1} Y_{S_2}) \\ = \frac{1}{4} n^3 p^2 (1 + o(1)) + \frac{1}{4} \sum_{S_1 \neq S_2} Y_{S_1} Y_{S_2}) \ . \end{aligned}$$

Sumę $\sum_{S_1 \neq S_2} Y_{S_1} Y_{S_2}$ przedstawiamy jako $E_1 + E_2 + E_3$, gdzie E_1 odpowiada przypadkowi gdy S_1 i S_2 nie mają wspólnej krawędzi, E_2 gdy mają jedną, a E_3 gdy mają dwie wspólne krawędzie. Szacujemy: $E_1 = (2n^4 p^4 + 6n^5 p^4 + n^6 p^4)(1 + o(1)) = n^6 p^4 (1 + o(1))$, $E_2 = 8n^4 p^3 (1 + o(1))$, $E_3 = n^3 p^2 (1 + o(1))$. Razem:

$$\frac{\operatorname{Var} Y_n}{(\mathsf{E}\, Y_n)^2} = \frac{8n^4 p^3 + n^3 p^2}{\frac{1}{4} n^6 p^4} (1 + (1)) = \mathcal{O}\Big(\frac{(pn^{3/2})^3}{(pn^{3/2})^4}\Big) = \mathcal{O}\Big(\frac{1}{n^{3/2} p}\Big) = o(1) \ .$$

To pokazuje, że $Y_n > 0$ prawie zawsze, czyli w grafie o n wierzchołkach istnieje ścieżka długości 2 z prawdopodobieństwem zbiegającym do 1. Tym zakończyliśmy pokazanie że $n^{-3/2}$ jest funkcją progową dla własności posiadania drogi długości 2.

Zbadamy kilka parametrów grafów $\mathcal{G}(n, \frac{1}{2})$. Oznaczenia: $\alpha(G)$ to największa liczność zbioru niezależnego w G, $\omega(G)$ to największa liczność kliki w G, $\chi(G)$ to liczba chromatyczna G. Szacujemy:

$$\mathsf{P}[\alpha(G(n, \frac{1}{2})) \geq b] \leq \binom{n}{b} 2^{-\binom{b}{2}} \leq \Big(\frac{ne}{b}\Big)^b \cdot 2^{-\frac{b(b-1)}{2}} = \Big(\frac{ne\sqrt{2}}{b 2^{b/2}}\Big)^b \ .$$

Kładąc $b = c\log_2 n$ dla $c > 2$ dostajemy, że $\mathsf{P}[\alpha(\mathcal{G}(n,\frac{1}{2})) < b] = 1 - o(1)$ czyli prawie zawsze $\alpha(\mathcal{G}(n,\frac{1}{2})) = \mathcal{O}(\log n)$.

Dokładnie takie samo szacowanie pokazuje, że prawie zawsze $\omega(\mathcal{G}(n,\frac{1}{2})) = \mathcal{O}(\log n)$. Nic w tym dziwnego, bowiem $\mathcal{G}(n,\frac{1}{2}) = \overline{\mathcal{G}(n,\frac{1}{2})}$ oraz ogólnie $\omega(G) = \alpha(\overline{G})$, zatem tak na prawdę nie musimy nic szacować. (Graf $\overline{G}$ to uzupełnienie G, to znaczy ma te same wierzchołki co G ale każda para wierzchołków jest krawędzią G w.t.w. gdy nie jest krawędzią $\overline{G}$.)

Pokażemy teraz szacowanie tych parametrów grafów $G(n,\frac{1}{2})$ od dołu. Rozważmy następujący algorytm zachłanny znalezienia zbioru niezależnego $\{v_1, v_2, \ldots\}$. Jako v_1 wybieramy wierzchołek 1. Niech S_1 to zbiór wierzchołków, które nie są sąsiednie z v_1. Przypuśćmy, że wierzchołek v_i i zbiór $S_i \neq \emptyset$ są określone. Niech v_{i+1} to najmniejszy element S_i, oraz $S_{i+1} = \{v \in S_i : v \text{ nie jest sąsiedni z } v_{i+1}\}$. Ponieważ oczekiwany rozmiar S_{i+1} jest równy około połowie rozmiaru zbioru S_i, ten proces będzie kontynuowany średnio przez logarytmiczną liczbę kroków, i dostaniemy zbiór niezależny rozmiaru $\Theta(\log n)$.

Pokażemy to dokładnie stosując nierówność Chernoffa dla rozkładu dwumianowego. Ustalmy stałą $0 < \epsilon < 1$. Niech $\mathcal{A}_i$ to zdarzenie, które zachodzi gdy $|S_i| \geq n \cdot \left(\frac{1-\epsilon}{2}\right)^i$. Z nierówności Chernoffa

$$\mathsf{P}[-\mathcal{A}_1] = \mathsf{P}[|S_1| < n\cdot(1-\epsilon)/2] \leq \exp(-\epsilon^2 n/4)\ .$$

Podobnie

$$\mathsf{P}[-\mathcal{A}_2 \mid \mathcal{A}_1] = \mathsf{P}[|S_2| < n\cdot(1-\epsilon)^2/4 \mid \mathcal{A}_1] \leq \exp(-\epsilon^2(1-\epsilon)n/8)\ .$$

Ogólnie:

$$\mathsf{P}[-\mathcal{A}_i \mid \mathcal{A}_1 \cap \cdots \cap \mathcal{A}_{i-1}] \leq \exp\Big(-\frac{\epsilon^2(1-\epsilon)^{i-1}n}{2^{i+1}}\Big)\ .$$

Korzystamy z wzoru

$$\mathsf{P}[\bigcap_{i=1}^{k}\mathcal{A}_i] = \mathsf{P}[\mathcal{A}_1]\cdot\mathsf{P}[\mathcal{A}_2 \mid \mathcal{A}_1]\cdot\ldots\cdot\mathsf{P}[\mathcal{A}_k \mid \mathcal{A}_1\cap\ldots\cap\mathcal{A}_{i-1}]$$

Stąd otrzymujemy szacowanie

$$\begin{aligned}\mathsf{P}[\mathcal{A}_k] \geq \mathsf{P}[\bigcap_{i=1}^{k}\mathcal{A}_i] = \mathsf{P}[\mathcal{A}_1]\cdot\prod_{i=2}^{k}\mathsf{P}[\mathcal{A}_i \mid \mathcal{A}_1\cap\cdots\cap\mathcal{A}_{i-1}] &\geq \prod_{i=1}^{k}\Big(1-\exp\Big(-\frac{\epsilon^2(1-\epsilon)^{i-1}n}{2^{i+1}}\Big)\Big)\\ &\geq \Big(1-\exp\Big(-\frac{\epsilon^2(1-\epsilon)^{i-1}n}{2^{i+1}}\Big)\Big)^k \geq 1-k\exp\Big(-\frac{\epsilon^2(1-\epsilon)^{i-1}n}{2^{i+1}}\Big)\ .\end{aligned}$$

Oszacujemy k dla którego $\mathsf{P}[\mathcal{A}_k] \geq 1-\Theta(n^{-1})$. Jeżeli $k\exp\big(-\frac{\epsilon^2(1-\epsilon)^{i-1}n}{2^{i+1}}\big) \leq \frac{1}{n}$ to wtedy $\epsilon^2(1-\epsilon)^{k-1}n \geq \ln n$ a stąd $k = \Omega(\log n)$. Zatem prawie zawsze $\omega(\mathcal{G}(n,\frac{1}{2})) = \alpha(\mathcal{G}(n,\frac{1}{2})) = \Theta(\log n)$.

Jeżeli $G = \langle V, E\rangle$ to $\alpha(G)\cdot\chi(G) \geq |V|$. Stąd prawie zawsze $\chi(\mathcal{G}(n,\frac{1}{2})) = \Omega(n/\log n)$. Można pokazać, że prawie zawsze $\chi(\mathcal{G}(n,\frac{1}{2})) = \frac{n}{2\log_2 n}(1+o(n))$.

Błądzenie losowe po grafie.

Rozważmy graf prosty $G = \langle V, E\rangle$. Oznaczamy $n = |V|$, $m = |E|$. Cząstka umieszczona jest w jednym z wierzchołków i w kolejnych krokach przesuwa sie po krawędziach G. Jeżeli jest w wierzchołku v oraz $\{v,t\} \in E$ to prawdopodobieństwo przejścia z v do t jest równe $\frac{1}{\deg v}$. Otrzymujemy łańcuch Markowa, stan to wierzchołek G w którym jest cząstka. Zakładamy, że G jest spójny, zatem łańcuch jest nieprzywiedlny.

Oznaczmy przez $h(v,t)$ *czas przejścia* z v do t, to znaczy oczekiwany czas osiągnięcia t z wierzchołka v. *Czasem dojeżdżania* $c(v,t)$ nazywamy $h(v,t) + h(t,v)$. Jeżeli graf interpretujemy jak sieć elektryczną, to czasy dojeżdżania można wyrazić przez oporności. Mianowicie, niech każda krawędź ma opór jednostkowy, działają prawa Kirchhoff'a i Ohma. Przypomnijmy, że oporem efektywnym $r(v,t)$ między parą wierzchołków v i t nazywamy różnicę napięcia przyłożoną do v i t która spowoduje przepływ jednostkowy z v do t. Oto wspomniana zależność: $c(v,t) = 2m \cdot r(v,t)$. Dla dowodu, rozważmy eksperyment, w którym do każdego wierzchołka v wpływa prąd $\deg v$ a z wierzchołka t wypływa prąd $2m$. Uzyskujemy to przykładając napięcie $n(v,t)$ do każdego wierzchołka, mierzone względem t. Z praw Kirchhoff'a i Ohma mamy dla każdego v:

$$\deg v = \sum_{\{v,z\}\in E} n(v,t) - n(z,t) \ . \tag{1}$$

Dzieląc obie strony (1) przez $\deg v$ dostajemy

$$1 = n(v,t) - \sum_{\{v,z\}\in E} \frac{n(z,t)}{\deg v} \ .$$

Jednocześnie mamy także następującą zależności rekurencyjne na czasy przejścia, dla każdego wierzchołka v:

$$h(v,t) = \sum_{\{v,z\}\in E} \frac{1 + h(z,t)}{\deg v} = 1 + \sum_{\{v,z\}\in E} \frac{h(z,t)}{\deg v} \ . \tag{2}$$

Stąd widać, że równania (1) i (2) mają taki sam kształt, zatem $n(v,t) = h(v,t)$, z jednoznaczności rozwiązań.

Dodajmy do naszego prądu podobny, ale taki, że z każdego wierzchołka z *wypływa* prąd $\deg v$ a do wierzchołka v *wpływa* prąd $2m$. Te prądy znoszą się, oprócz v i t. Dostajemy, że napięcie $n(v,t) + n(t,v)$ pomiędzy v i t powoduje wpływanie do v i wypływanie z t prądu $2m$. Z prawa Ohma wynika $c(v,t) = 2m \cdot r(v,t)$.

Niech $P_v(G)$ będzie oczekiwanym czasem błądzenia cząstki, która zaczyna w v, aż do chwili gdy odwiedzi każdy wierzchołek. *Czas pokrycia* G, oznaczany $P(G)$, to maksimum z $P_v(G)$ po $v \in V$. Ma miejsce następujące ogólne szacowanie: $P(G) \leq 2m(n-1)$. Dla dowodu, weźmy dowolne drzewo T rozpinające G. Można nim obejść wierzchołki G przechodząc przez każdą krawędź T dwa razy. Stąd $P(G) \leq \sum_{\{v,t\}\in T}(h(v,t) + h(t,v))$. Wystarczy pokazać, że jeżeli $\{v,t\} \in E$ to $h(v,t) + h(t,v) \leq 2m$. Tu z kolei wystarczy pokazać, że oczekiwany czas od przejścia krawędzią w kierunku $v \to t$ do następnego

takiego przejścia jest nie większy niż $2m$. Rozważmy nowy łańcuch Markowa, którego stanami są zorientowane krawędzie G, dwa stany dla każdej krawędzi G. Jeżeli $x \to y$ i $y \to z$ są stanami, to prawdopodobieństwo przejścia z pierwszego do drugiego jest $1/\deg v$. Macierz przejścia w kolumnach sumuje się do 1 (ćwiczenie), czyli jest podwójnie stochastyczna. Zatem rozkład jednostajny jest stacjonarnym, a stąd oczekiwany czas powrotu to odwrotność prawdopodobieństwa rozkładu stacjonarnego, czyli $2m$.

Przykład: Problem czasu pokrycia kliki K_n jest tym samym co problem zbieracza n kuponów, jest zatem prawdziwe $P(K_n) = \mathcal{O}(n \log n)$. Niech G_1 będzie linią złożoną z n krawędzi, które tworzą drogę między końcami v i u. W G_1 mamy $r(u, v) = n$. Niech G_2 dowolny spójny graf o n wierzchołkach różnych od wierzchołków G_1 i o $\Theta(n^2)$ krawędziach. Niech G_3 ma wierzchołki z G_1 i G_2, podobnie krawędzie z G_1 i G_2, oraz dodatkowo wierzchołek v grafu G_1 połączony krawędzią z dowolnym wierzchołkiem G_2. Zauważmy że w sieci elektrycznej wyznaczonej przez G_3 także zachodzi $r(u, v) = n$, zatem w G_3 mamy $c(u, v) = \Theta(n^3)$. To pokazuje, że szacowanie $P(G) \leq 2m(n-1)$ jest asymptotycznie najlepsze możliwe. $\Diamond$

Zadania

1. Niech G_1 oznacza losowy graf mający n wierzchołków i $\lfloor n(n-1)/4 \rfloor$ krawędzi. Nech G_2 będzie grafem losowym $\mathcal{G}(n, 1/2)$. Który z grafów G_i ma większą oczekiwaną liczbę cykli Hamiltona?

2. Zaczynamy od n wierzchołków izolowanych i dodajemy w losowej kolejności wszystkie możliwe krawędzie między nimi, jedna po drugiej, zatrzymując się, gdy tylko otrzymany dotychczas graf G_n ma własność W. Oszacuj oczekiwaną liczbę krawędzi G_n, gdy jako W przyjmiemy:
   (a) brak wierzchołków izolowanych; (b) spójność; (c) istnienie cyklu.

3. Zaczynamy od kliki K_n, usuwamy jej krawędzie w losowej kolejności, jedna po drugiej, zatrzymując się, gdy tylko otrzymany dotychczas graf G_n przestaje mieć własność W. Oszacuj oczekiwaną liczbę krawędzi G_n, gdy jako W przyjmiemy:
   (a) brak wierzchołków izolowanych; (b) spójność; (c) istnienie cyklu.

4. Pokaż, że jeżeli $\operatorname{Var} X_n = o((\mathsf{E}\, X_n)^2)$ to $X_n = \mathsf{E}\, X_n(1 + o(1)$ prawie zawsze, o ile $\langle X_n \rangle$ ciąg zmiennych losowych o wartościach całkowitych nieujemnych.

5. Wrzucamy losowo m kul do n urn. Pokaż:
   (a) Jeżeli $m = an \ln n$, gdzie $a < 1$, to prawie zawsze jest pusta urna.
   (b) Jeżeli $m = an \ln n$, gdzie $a > 1$, to prawie zawsze wszystkie urny są niepuste.
   Wskazówka: metody pierwszego i drugiego momentu.

6. Pokaż, że prawie zawsze $\chi(\mathcal{G}(n, \frac{1}{2})) = \Theta(n/\log n)$.
   Wskazówka: Rozważ algorytm, który wybiera kolejne zbiory niezależne w sposób zachłanny i nadaje im kolejne kolory, aż pozostanie $\mathcal{O}(n/\log n)$ wierzchołków.

7. Pokaż przykład grafu H takiego, że oczekiwana wartość liczby podgrafów H w $\mathcal{G}(n,p)$ jest równa $n^\alpha p^\beta$, natomiast funkcją progową dla własności posiadania podgrafu H nie jest funkcja $n^{-\alpha/\beta}$.
Wskazówka: Niech H to K_4 z doczepionym wierzchołkiem wiszącym.

8. Pokaż następujące funkcje progowe:
   (a) $\ln n/n$ dla własności bycia spójnym;
   (b) $1/n$ dla własności nie bycia planarnym;
   (c) $\ln n/n$ dla własności zawierania ścieżki Hamiltona;
   (d) $n^{-2/(i-1)}$ dla własności zawierania kliki K_i.

9. Oszacuj czas pokrycia dla następujących grafów:
   (a) n wierzchołków połączonych krawędziami w linię;
   (b) kratownica $n \times n$.

10. Podaj przykład grafu G i jego dwóch wierzchołków x i y takich, że $h(x,y) = \Theta(n^2)$ ale $h(y,x) = \Theta(n^3)$.

11. Rozważmy graf prosty spójny o m krawędziach. Pokaż, że krawędź $\{x,y\}$ jest mostem w.t.w. gdy $h(x,y) + h(y,x) = 2m$.

12. Podaj przykłady ciągów grafów $\langle G_n \rangle_n$ i $\langle H_n \rangle_n$, takich, że H_n jest podgrafem G_n oraz zachodzą: (a) $P(H_n) = o(P(G_n))$; (b) $P(G_n) = o(P(H_n))$.

13. Czy istnieje ciąg grafów $\langle G_n \rangle$ taki, że G_n ma n wierzchołków oraz $P(G_n) = \mathcal{O}(n)$?