Nagroda Gödla - ćwiczenia

Ćwiczenia 1

Będziemy ćwiczyć algebrę, przyda się później do algorytmu AKS, a poza tym sama w sobie jest ciekawa. Pokażemy (z drobnymi lukami), że ciało skończone rzędu (czyli o liczbie elementów) n istnieje wtedy i tylko wtedy, gdy $n = p^k$ dla pewnej liczby pierwszej p i naturalnej k. Podaję def. ciała (grupa przemienna z dodawaniem, prawie grupa przemienna z mnożeniem - 0 nie ma odwrotności, rozdzielność).

1. Najpierw pokażmy, że dla liczby pierwszej p istnieje ciało rzędu p.

Po prostu $\mathbb{Z}_p$ działa.

2. Teraz pokażemy (prawie), że istnieje ciało rzędu p^k. Konstrukcja jest następująca. Bierzemy dowolny wielomian nieskracalny $h(x)$ stopnia k nad $\mathbb{Z}_p$. (nie jest jasne, że istnieje, to jest pewna luka) Definiujemy nasze ciało jako $F = \mathbb{Z}_p[x]/h(x)$, czyli dzielimy wielomiany modulo $h(x)$. Pokazać, że tu wszystko dobrze działa.

Tu warto zrobić sobie wszystko na spokojnie. Można rozważyć przykład np. dla $n = 9$, czyli wielomiany stopnia 2 nad $\mathbb{Z}_3$. Przykładowym wielomianem nieskracalnym jest $x^2 + 1$. Wszystkie rzeczy wychodzą w miarę prosto, przy czym istnienie odwrotności nie jest jasne. Najłatwiej chyba jest to pokazać z algorytmu Euklidesa.

3. Teraz pokażemy, że nie ma ciał o innych rzędach. Na początek: pokazać, że charakterystyka ciała jest liczbą pierwszą. Charakterystyka to najmniejsza liczba k taka, że $1 + 1 + \ldots + 1 = 0$, gdzie jedynek jest dokładnie k.

Załóżmy, że suma k jedynek to 0, ale $k = ab$ dla pewnych $a, b > 1$. Niech x_ℓ to suma ℓ jedynek. Mamy więc $x_a x_b = 0$. Pokażemy, że z tego wynika, że $x_a = 0$ lub $x_b = 0$, czyli sprzeczność - charakterystyka jest jednak mniejsza. Ogólnie, niech $xy = 0$, ale $x \neq 0 \neq y$. Wówczas istnieją x^{-1} oraz y^{-1}. Mamy więc $x^{-1}xyy^{-1} = (x^{-1}x)(yy^{-1}) = 1 \cdot 1 = 1$, a z drugiej strony $x^{-1}xyy^{-1} = x^{-1}(xy)y^{-1} = x^{-1}0y^{-1} = 0$. Sprzeczność.

4. Teraz pokażemy, że podzbiór złożony z sum $1 + \ldots + 1$ jest ciałem (to wychodzi łatwo, to po prostu jest ciało $\mathbb{Z}_p$).

5. Teraz pokażmy, że F jest przestrzenią liniową nad $\mathbb{Z}_p$.

To po prostu wychodzi jak zobaczymy co trzeba pokazać. Dodanie dwóch elementów z F oraz pomnożenie elementu z F przez element z $\mathbb{Z}_p$ ma być nadal w ciele. Poza tym musi zachodzić rozdzielność. Wszystkie te rzeczy wynikają natychmiast z własności ciała.

6. Pokażmy, że to już daje, że $n = p^k$.

Z algebry liniowej wynika, że istnieje pewna baza. Niech ma ona moc k i będzie to $\{\alpha_1, \ldots, \alpha_k\}$. Musi być skończona, bo F jest skończone. Wiemy też,

że każdy element F przedstawia się jednoznacznie w bazie. Współczynniki są z $\mathbb{Z}_p$, czyli możliwych elementów F jest p^k.

Ćwiczenia 2

Kontynuujemy algebrę, jako przygotowanie do AKS.

Niech ϵ_n to pierwiastek n-tego stopnia z n, ten o najmniejszym niezerowym kącie. Wtedy definiujemy n-ty wielomian cyklotoniczny

$$\phi_n(x) = \prod_{k|n}(x - \epsilon_n^k).$$

Przyjrzymy się pierwszym kilku. $\phi_1(x) = x-1$, $\phi_2(x) = x+1$, $\phi_3(x) = x^2+x+1$, $\phi_4(x) = x^2 + 1$, $\phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\phi_6(x) = x^2 + x + 1$. Ogólnie np. $\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ dla liczb pierwszych p.

1. Pokaż, że $\prod_{d|n} \phi_d(x) = x^n - 1$.

Po prostu wystarczy pokazać, że wszystkie $x - \epsilon_n^k$ występują tam.

Formułujemy teraz Lemat Gaussa (tak naprawdę jego część). Jeśli $p(x) \in \mathbb{Z}[x]$ jest prymitywny (ang. primitive, może po polsku inaczej, NWD współczynników to 1) i nierozkładalny w $\mathbb{Z}[x]$, to jest też nierozkładalny w $\mathbb{Q}[x]$.

2. Pokaż, że $\phi_n(x) \in \mathbb{Z}[x]$.

Rozwiązanie to indukcja. Trzeba założyć, że wszystkie $\phi_k(x) \in \mathbb{Z}[x]$ dla $k < n$ i skorzystać z zadania 1.

Teraz przechodzimy do **bisymulacji**. Pokażemy, że równoważność gramatyk prostych jest nierozstrzygalna. Gramatyki proste to deterministyczne gramatyki bezkonteksowe w postaci Greibach, w szczególności każdy nieterminal generuje co najwyżej (a po naturalnych założeniach dokładnie) jedno słowo.

Definiujemy normę nieterminala jako długość najkrótszego generowanego słowa.

3. Pokazać, że dla każdej gramatyki można założyć, że jest ona unormowana (gdy zależy nam tylko na języku).

4. Jak duża może być norma?

Mówimy o bisymulacji, grze bisymulacyjnej, przykłady.

5. Pokazać, że dla unormowanych gramatyk prostych bisymulacja i równość języków to to samo. Zauważmy w ogóle (potem), że to się tyczy każdego deterministycznego i unormowanego systemu.

Rozstrzygniemy teraz bisymulację dla ogólnych (nie koniecznie prostych) unormowanych gramatyk w postaci Greibach.

6. Pokazać, że $\alpha \sim \beta$ implikuje $||\alpha|| = ||\beta||$.

Ćwiczenia 3

Kontynuujemy bisymulację. Teraz mówimy o rozkładzie.

1. Pokaż, że dla każdego nie pierwszego X istnieje $\alpha \in P^*$ taka, że $X \sim \alpha$.

Możemy zatem zdefiniować bazę. Baza składa się z symboli pierwszych oraz dla każdego nie pierwszego z pary (X, α), gdzie $\alpha \in P^*$. Kluczowa jest następująca własność.

2. Pokaż jednoznaczność rozkładu, tj. że dla każdych $\alpha, \beta \in P^*$ jeśli $\alpha \sim \beta$, to $\alpha = \beta$. Zwróćmy uwagę przy okazji, że to oznacza, że dla dowolnych γ, δ zachodzi $\gamma \sim \delta \iff dec_B(\gamma) = dec_B(\delta)$.

Trzeba wziąć kontrprzykład, który jest najmniejszy jeśli chodzi o normę. Następnie należy wziąć jego ruch redukujący normę i odpowiedź. Wyjdzie z tego sprzeczność.

3. To jak teraz opracować algorytm? Zauważmy, że gdybyśmy mieli bazę dla $\sim$ to już łatwo. Trzeba po prostu spróbować zgadnąć bazę B taką, że $\equiv_B$ to bisymulacja i $\alpha \equiv_B \beta$.

4. Jak sprawdzić, czy dla danej bazy B relacja $\equiv_B$ jest bisymulacją?

Wystarczy sprawdzić, że każda para w B przetrwa jeden krok. Załóżmy, że to sprawdziliśmy. Wystarczy pokazać teraz, że w ogóle każda para w $\equiv_B$ przetrwa jeden krok. No a wtedy każda para przetrwa dowolnie wiele kroków.

Teraz będziemy się zajmować **aproksymacjami dla TSP**.

5. Pokazać, że TSP nie da się aproksymować ze stałym czynnikiem (tu załóżmy czynnik 2).

To się robi poprzez redukcję z cyklu Hamiltona. W instancji TSP wstawiamy tam gdzie była krawędź w oryginalnym grafie krawędź z wagą 1, a tam gdzie nie było krawędź z wagą $3n$.

6. Teraz robimy metryczny TSP, czyli zakładamy, że odległości spełniają nierówność trójkąta. Pokazać, że da się w tej sytuacji zrobić algorytm wielomianowy ze stałą aproksymacji 2.

Robi się minimalne drzewo rozpinające, które ma koszt oczywiście mniejszy niż minimalny cykl. Obchodzi się je dwa razy. Jak chce się dojść na wierzchołka, w którym się już było to robi pomija się go i idzie bezpośrednio do następnego nieodwiedzonego. Ten skrót dzięki nierówności trójkąta nie wydłuża całej drogi.

7. A teraz zrobić algorytm wielomianowy ze stałą aproksymacji $\frac{3}{2}$ (hipoteza jest, że $\frac{4}{3}$ to optimum).

Rozważmy wierzchołki, które mają w minimalnym drzewie rozpinającym stopień nieparzysty. Robimy na nich minimalne skojarzenie doskonałe. Łatwo pokazać, że istnieje skojarzenie doskonałe o koszcie mniejszym niż połowa minimalnego cyklu komiwojażera. Teraz to skojarzenie razem z drzewem rozpinającym dają graf w każdym stopniu parzystym. Robimy na nim cykl Eulera, on przechodzi przez wszystkie wierzchołki. Koszt tego nie przekracza $\frac{3}{2}$ minimalnego cyklu komiwojażera. Teraz robimy to samo co poprzednio, czyli jeśli

chcemy jakiś wierzchołek odwiedzić drugi raz, to dodajemy skrót, który dzięki nierówności trójkąta niczego nie psuje.

Ćwiczenia 4

Robimy na ćwiczeniach rzeczy, które zostały z AKSu.

1. Pokaż, że krok 1 w algorytmie (sprawdzanie, czy $n = a^b$ dla pewnego $b > 1$) jest wielomianowy.

2. Pokaż, że krok 5 w algorytmie (sprawdzenia tej równości modulo $x^r - 1, n$) jest wielomianowy.

3. Liczymy czas działania algorytmu AKS (szacujemy z góry, żeby wyszło około $n^{21/2}$).

4. Udowodnić Lemat 4.3.

Wypisuję jak definiujemy r (najmniejsza liczba nie dzieląca iloczynu) i chcemy pokazać trzy rzeczy:

1. $r \leqslant B$,
2. $r \perp n$ (bo $\frac{r}{NWD(r,n)}$ też nie dzieli iloczynu),
3. $o_r(n) > \log^2(n)$.

5. Udowodnić, że jeśli n oraz p są introspektywne dla $(x + a)$, to $\frac{n}{p}$ też (to może).

To się robi dość skomplikowanie, najpierw łatwo, a potem trzeba pokazać, że $f^p = g^p$ implikuje $f = g$ w naszym przypadku.

6. Udowodnić Lemat 4.9 (może).

To zrobię na wykładzie jednak.

Ćwiczenia 5

To były pierwsze ćwiczenia z algorytmów kwantowych.

1. Znaleźć obwód mapujący $|00\rangle$ na $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Najpierw przykładamy Hadamarda do pierwszego kubitu, a potem controlled not do obu.

2. Pokazać, że macierze unitarne to te same co zachowujące długość.

Niech $v_1, \ldots, v_n$ to kolumny macierzy A. Z unitarności wynika, że $v_i \bar{v}_i = 1$ oraz $v_i \bar{v}_j = 0$ dla $i \neq j$. Niech $v = (a_1, \ldots, a_n)$. Mamy $Av = \sum_{i=1}^n a_i v_i$. Zatem

$$|Av| = (\sum_{i=1}^n a_i v_i)(\overline{\sum_{j=1}^n a_j v_j}) = \sum_{1 \leqslant i,j \leqslant n} a_i \bar{a}_j v_i \bar{v}_j = \sum_{i=1}^n a_i \bar{a}_i = |v|.$$

No to pokazaliśmy w jedną stronę. W drugą stronę jest chyba nieco trudniej, ale nie bardzo.

3. Analizujemy macierze kwantowej transformaty Fouriera. Pokazać, że są one unitarne.

4. Zobaczyć, że obwód, który realizuje kwantową transformatę Fouriera faktycznie ją realizuje. (Tego nie zrobiliśmy, ale to można by zrobić na tych ćwiczeniach. Jest za to napisane na wykładzie.)

Ćwiczenia 6

To są drugie ćwiczenia z algorytmów kwantowych. Oprócz tego pokazaliśmy też twierdzenie Immermana-Szelepcsenyiego o tym, że NL = coNL.

1. Pokaż, że grupa $\mathbb{Z}_p^*$ jest cykliczna. (to nie jest proste, ale da się zrobić, są w Internecie różne rozwiązania)

2. Pokaż, że jeśli umiemy rozwiązać problem rzędu elementu modulo w P, to też rozwiązać faktoryzację w P.

Teraz pokazujemy, że NL = coNL. Pokazujemy to na kroki. Robiliśmy coś w stylu opisu poniżej.

3. Pokaż, że jeśli umielibyśmy policzyć ile elementów jest osiągalnych z s w n krokach, to umielibyśmy niedeterministycznie sprawdzić, czy t jest osiągalny z s.

Po prostu przeglądamy wszystkie elementy, zgadujemy ścieżkę do nich i liczymy ile zgadliśmy. Jeśli zgadliśmy, że t nie jest osiągalny oraz licznik zgadniętych, że są osiągalne wyszedł taki jaki powinien być wynik, to t nie jest osiągalny.

4. Powiedzmy, że mamy liczbę osiągalnych w k krokach. Jak sprawdzić, czy v jest osiągalny w $k+1$ krokach?

Przebiegamy wszystkie (tu używamy liczby osiągalnych w k krokach) wierzchołki osiągalne w k krokach i z każdego robimy jeszcze jeden krok.

5. A teraz pokazać jak z liczby osiągalnych w k krokach policzyć liczbę osiągalnych w $k+1$ krokach.

Po prostu przechodzimy po wszystkich v i sprawdzamy, czy jest osiągalny w $k+1$ krokach tak jak w zadaniu 4. Jak złożymy wszystkie te rzeczy plus to, że nieosiągalność jest coNL-zupełna, to mamy, że NL = coNL.

Można dla poprawienia zrozumienia zapytać co tu jest świadkiem (tym zgadniętym). Odpowiedź jest taka, że to jest ciąg zbiorów wierzchołków osiągalnych w coraz większych odległościach.

Ćwiczenia 7

Będziemy się zajmowali błądzeniem losowym w grafach nieskierowanych. Na te ćwiczenia n to liczba wierzchołków w grafie, a m to liczba krawędzi. Pokażemy ogólnie rzecz biorąc, że w grafach nieskierowanych istnieje takie C, że jeśli zrobimy Cn^3 kroków błądzenia losowego i v jest osiągalne z u, to z dużym prawdopodobieństwem jeśli startujemy z u, to odwiedzimy v podczas tego błądzenia.

Błądzenie losowe polega na tym, że jeśli jesteśmy w jakimś wierzchołku o stopniu d, to wychodzimy z prawdopodobieństwem $\frac{1}{d}$ każdą z krawędzi.

1. Niech $H_{u,v}$ będzie oczekiwaną liczbą kroków, po których startując z u odwiedzimy błądząc losowo wierzchołek v. Pokaż, że jeśli $H_{u,v} = O(n^3)$, to istnieje C takie, że $\mathbb{P}(\text{odwiedzę } v \text{ po } Cn^3 \text{ krokach}) \geqslant \frac{1}{2}$.

Będziemy korzystali z nierówności Markowa, która mówi, że w szczególności dla zmiennej losowej X, która przyjmuje tylko nieujemne wartości zachodzi

$$\mathbb{P}(X \geqslant k\,\mathbb{E}X) \leqslant \frac{1}{k}.$$

Niech X to pierwszy czas dotarcia z u do v. Wtedy $\mathbb{E}X = H_{u,v}$. A zatem jeśli $H_{u,v} \leqslant Dn^3$, to $\mathbb{P}(X \geqslant 2Dn^3) \leqslant \frac{1}{2}$.

2. W dalszej części ćwiczeń skupimy się więc na pokazaniu, że $H_{u,v} = O(n^3)$ dla grafów nieskierowanych. Pokazać przykład, że dla grafów skierowanych może być to wykładnicze.

Rozważmy graf o wierzchołkach $0, 1, \ldots, n-1, n$. Niech krawędzie będą następujące: $(i, i+1)$ dla $i < n$ oraz $(i, 0)$ dla $0 < i < n$. Wówczas żeby dotrzeć z 0 do n trzeba $n-1$ razy pójść krawędzią $(i, i+1)$. Widać się, że oczekiwany czas dotarcia do n jest wykładniczy. Można to precyzyjniej pokazać tak, że prawdopodobieństwo dotarcia tam w jednym spacerze zaczynającym się z 0 wynosi $2^{-(n-1)}$. Jeśli to się nie uda, to wracamy z powrotem do 0. A więc oczekiwana liczba spacerów jest wykładnicza (chyba), można to pewnie łatwo pokazać.

3. Rozważmy graf będący linią, tzn. składający się z wierzchołków $0, 1, \ldots, n$ i krawędzi $(i, i+1)$ dla $i < n$. Obliczmy $H_{0,n}$.

Dla uproszczenia oznaczeń niech $H_i = H_{i,n}$. Można napisać równania rekurencyjne:

$$H_0 = 1 + H_1, \qquad H_n = 0,$$

oraz

$$H_i = 1 + \frac{H_{i-1} + H_{i+1}}{2}$$

dla $0 < i < n$. Wiemy, że te równania mają tylko jedno rozwiązanie. Można pokazać, że rozwiązanie $H_i = n^2 - i^2$ spełnia powyższe warunki, więc to jest odpowiedź. Zachodzi więc $H_{0,n} = n^2$.

4. Teraz będziemy dążyli do pokazania, że dla każdych u, v zachodzi $H_{u,v} + H_{v,u} = O(n^3)$. W tym celu użyjemy nietypowego sposobu: analizy przepływu prądu przez obwód. Pewnie można to zrobić samymi przepływami, nie odwołując się do prądu, ale tak jest chyba bardziej intuicyjnie. Rozważmy nasz graf, w

którym w każdą krawędź wstawiliśmy opornik o oporze równym 1. Naszym ogólnym celem będzie pokazanie, że

$$H_{u,v} + H_{v,u} = 2m \cdot R_{u,v},$$

gdzie m, dla przypomnienia, to liczba krawędzie w grafie, a $R_{u,v}$ to opór pomiędzy wierzchołkami u a v w naszym grafie. Oczywiście $m = O(n^2)$. Nietrudno pokazać, że $R_{u,v} = O(n)$ o ile istnieje ścieżka z u do v. Istotnie, jeśli usuniemy wszystkie oporniki w grafie spoza tej ścieżki, to opór nie zmaleje (pewnie wzrośnie). No a ścieżka ma opór taki jak jej długość, czyli maksymalnie liniowy. To by zatem pokazało, że istotnie $R_{u,v} + R_{v,u} = O(n^3)$.

Robimy tak. Przykładamy potencjały do różnych wierzchołków tak, że

- dla każdego wierzchołka w wpływa do niego prąd o natężeniu $d(w)$, czyli jego stopniu
- dodatkowo z wierzchołka v wypływa prąd o natężeniu $2m$.

Suma stopni wierzchołków w grafie to dwa razy liczba krawędzi, więc jest ok, tyle samo prądu wpływa, co wypływa. Niech $\phi_{u,v}$ to różnica potencjałów w tej sytuacji pomiędzy wierzchołkiem u a v. Zadanie brzmi: pokaż, że $\phi_{u,v} = H_{u,v}$. Można dać wskazówkę, żeby napisać równania rekurencyjne i zobaczyć, że są one takie same.

Wierzchołek v jest ustalony. Oznaczmy więc $H_u = H_{u,v}$ oraz $\phi_u = \phi_{u,v}$. Oczywiście dla $u = v$ zachodzi $H_v = 0 = \phi_v$. W dalszej części zakładamy, że $u \neq v$. Niech $d(u)$ to stopień u, a $S(u)$ to zbiór wszystkich sąsiadów u. Dla dowolnego u równanie na H_u jest następujące:

$$H_u = 1 + \frac{1}{d(u)} \sum_{w \in S(u)} H_w.$$

Niech $I_{s,t}$ to natężenie prądu pomiędzy s a t, gdy ci są sąsiadami. Dla dowolnego u do u wpływa $d(u)$ prądu, z definicji sytuacji. Musi więc tyle samo wypływać. Mamy więc

$$d(u) = \sum_{w \in S(u)} I_{u,w} = \sum_{w \in S(u)} \phi_{u,w} = \sum_{w \in S(u)} \phi_u - \phi_w = \sum_{w \in S(u))} \phi_u - \sum_{w \in S(u)} \phi_w = d(u)\phi_u - \sum_{w \in S(u)} \phi_w.$$

Po prostym przekształceniu otrzymujemy

$$\phi_u = 1 + \frac{1}{d(u)} \sum_{w \in S(u)} \phi_w.$$

Czyli istotnie $H_w = \phi_w$.

5. Nazwijmy powyższy scenariusz literą A. Teraz opiszmy scenariusz B. Jest on analogiczny, tyle, że to z wierzchołka u wypuszczamy prąd o natężeniu $2m$. Niech teraz napięcia to $\phi'_{s,t}$. Pokaż, że $\phi'_{v,u} = H_{v,u}$.

To jest oczywiste, dokładnie tak jak poprzednio.

6. Teraz robimy scenariusz C. Z każdego wierzchołka w wypuszczamy teraz prąd o natężeniu $d(w)$, a do wierzchołka u wpuszczamy prąd o natężeniu $2m$. Oblicz ile teraz wynosi $\phi''_{u,v}$.

Wszystko jest w odwrotną stronę niż w scenariuszu B. A zatem

$$\phi''_{u,v} = \phi'_{v,u} = H_{v,u}.$$

7. Pokazać teraz, że $H_{u,v} + H_{v,u} = 2m \cdot R_{u,v}$.

Sumujemy scenariusze A i C. Niech napięcie będzie oznaczane teraz $\phi'''_{s,t}$. Mamy więc prąd o natężeniu $2m$, który wpływa do u i prąd o natężeniu $2m$, który wypływa z v. A więc

$$\phi'''_{u,v} = 2m \cdot R_{u,v}.$$

Z drugiej jednak strony to są zsumowane scenariusze A i C, więc

$$\phi'''_{u,v} = \phi_{u,v} + \phi''_{u,v} = H_{u,v} + H_{v,u},$$

co kończy dowód.

8. Pokazać przykład grafu i wierzchołków u, v takich, że $H_{u,v} = \Theta(n^3)$.

Bierzemy długą ścieżkę, o długości N, niech u będzie na jej prawym końcu, a v na jej lewym końcu. Na prawym końcu, w u dołączamy klikę K_N. Liczba wierzchołków n to $n = 2N$. Mamy więc $m = N + \binom{N}{2} = \Theta(n^2)$. Mamy też $R_{u,v} = n = \Theta(n)$ A więc $H_{u,v} + H_{v,u} = \Theta(n^3)$. Z drugiej strony wiemy z zadania 3, że $H_{v,u} = N^2$. Zatem $H_{u,v} = \Theta(n^3) - N^2 = \Theta(n^3)$.

Ćwiczenia 8

Zajmujemy się ułamkami łańcuchowymi. Pretekstem do tego było to, że pod koniec algorytmu Shora ta metoda jest wykorzystywana do znalezienia dobrego przybliżenia jakiejś liczby przez ułamek. Prawdziwym powodem jest to, że to ciekawy kawałek matematyki.

Ogólnie ułamek łańcuchowy to przedstawienie pewnej liczby x w postaci

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{1}{a_3 + \cdots}}},$$

gdzie wszystkie $a_i \in \mathbb{Z}^+$. Bierzemy zawsze największe możliwe a_i, tak, że np. $x - a_0 < 1$. Oznaczymy wtedy $x = [a_0; a_1, a_2, \ldots]$. Przykładowo mamy $\sqrt{2} = [1; 2, 2, 2, \ldots]$. Oznaczmy $R_n = [a_0; a_1, a_2, \ldots, a_n]$, czyli np. $R_0 = a_0$, $R_1 = a_0 + \frac{1}{a_1}$. Oznaczmy też $x_n = [a_n; a_{n+1}, a_{n+2}, \ldots]$. Czyli np. $x = x_0$. Okazuje się, że R_n jest dobrym przybliżeniem x. Łatwo zobaczyć też, że jest liczbą wymierną. Twierdzenie, które będziemy dowodzić to:

Twierdzenie Jeśli $R_n = \frac{p}{q}$ oraz $|x - \frac{p'}{q'}| < |x - R_n|$, to wówczas $q' > q$.

Innymi słowy liczby R_n są najlepszymi przybliżeniami liczby x.

1. Pokaż, że rozwinięcie x w ułamek łańcuchowy jest skończone wtedy i tylko wtedy, gdy x jest liczbą wymierną.

Jasne jest, że skończone rozwinięcie jest liczbą wymierną, więc liczba niewymierna ma zawsze nieskończone rozwinięcie. Nieco trudniejsze jest pokazanie, że liczba wymierna ma skończone. Pokażemy jednak, że mianownik x_{k+1} jest zawsze mniejszy niż mianownik x_k, więc w końcu zejdzie on do 1 i rozwijanie się skończy. Niech $x_k = \frac{p}{q}$. Mamy $x_k = a_k + \frac{1}{x_{k+1}}$. A więc $\frac{1}{x_{k+1}} = x_k - a_k = \frac{p-a_k q}{q} = \frac{p'}{q}$, gdzie $p' < q$, bo a_k jest największe możliwe. A zatem $x_{k+1} = \frac{q}{p'}$, no i mamy $p' < q$, czyli to, co chcemy.

2. Zdefiniujmy ciąg $P_0 = a_0$, $Q_0 = 1$, $P_1 = a_0 a_1 + 1$, $Q_1 = a_1$ oraz $P_k = a_k P_{k-1} + P_{k-2}$, $Q_k = a_k Q_{k-1} + Q_{k-2}$ dla $k \geqslant 2$. Mamy $R_0 = a_0 = \frac{P_0}{Q_0}$ oraz $R_1 = a_0 + \frac{1}{a_1} = \frac{P_1}{Q_1}$. Pokaż, że $R_n = \frac{P_n}{Q_n}$.

Pokazujemy przez indukcję. Załóżmy, że $R_m = \frac{P_m}{Q_m}$. Zatem

$$R_m = \frac{P_m}{Q_m} = \frac{a_m P_{m-1} + P_{m-2}}{a_m Q_{m-1} + Q_{m-2}}.$$

Zauważmy, że jeśli podstawimy $a_m + \frac{1}{a_{m+1}}$ zamiast a_m w R_m to dostaniemy R_{m+1}. A więc tak samo jest z prawej strony. Mamy więc

$$R_{m+1} = \frac{P_{m-1}(a_m + \frac{1}{a_{m+1}}) + P_{m-2}}{Q_{m-1}(a_m + \frac{1}{a_{m+1}}) + Q_{m-2}} = \frac{a_{m+1}(a_m P_{m-1} + P_{m-2}) + P_{m-1}}{a_{m+1}(a_m Q_{m-1} + Q_{m-2}) + Q_{m-1}} = \frac{a_{m+1} P_m + P_{m-1}}{a_{m+1} Q_m + Q_{m-1}} = \frac{P_{m+1}}{Q_{m+1}}.$$

3. Pokaż, że $P_{k-1} Q_k - Q_{k-1} P_k = (-1)^k$.

To idzie łatwo przez indukcję.

4. Pokaż, że $R_0 < R_2 < R_4 < \ldots < R_5 < R_3 < R_1$ (dla x, dla którego one się nie zrównują, tzn. a_5 istnieje, np. dla x niewymiernego).

To łatwo widać z poprzedniego zadania na przykład.

5. Oblicz $R_n - R_{n-1}$.

Wychodzi

$$R_n - R_{n-1} = \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{P_n Q_{n-1} - Q_n P_{n-1}}{Q_n Q_{n-1}} = \frac{(-1)^{n-1}}{Q_n Q_{n-1}}.$$

6. Pokaż, że $|x - R_{n+1}| < |x - R_n|$. (to jest dość trudne, ja to pokazałem na tablicy)

Mamy

$$x_0 = \frac{P_n x_{n+1} + P_{n+1}}{Q_n x_{n+1} + Q_{n+1}}.$$

A zatem

$$x_0 - R_n = \frac{P_n x_{n+1} + P_{n+1}}{Q_n x_{n+1} + Q_{n+1}} - \frac{P_n}{Q_n} = \frac{Q_n P_{n-1} - P_n Q_{n-1}}{Q_n (Q_n x_{n+1} + Q_{n-1}} = \frac{(-1)^n}{Q_n (Q_n x_{n+1} + Q_{n-1})}.$$

Ponieważ $x_{n+1} < a_{n+1} + 1$ to

$$|x_0 - R_n| > \frac{1}{Q_n(Q_n(a_{n+1}+1) + Q_{n-1})} = \frac{1}{Q_n(Q_{n+1} + Q_n)}.$$

Z drugiej strony $x_{n+2} > 1$, więc

$$|x_0 - R_{n+1}| < \frac{1}{Q_{n+1}(Q_n + Q_{n+1})} < |x_0 - R_n|.$$

7. Niech $\frac{r}{s}$ takie, że $s \leqslant Q_n$. Pokaż, że wówczas $|x - \frac{r}{s}| \geqslant |x - \frac{P_n}{Q_n}|$.

Załóżmy, że $|x - \frac{r}{s}| < |x - \frac{P_n}{Q_n}|$. Pokażemy, że wówczas $s > Q_n$. Mamy $R_{n-1} < \frac{r}{s} < R_n$ lub $R_n < \frac{r}{s} < R_{n-1}$, to dość łatwo pokazać z ćw. 6 i ćw. 5. Zatem

$$|\frac{r}{s} - R_{n-1}| < |R_n - R_{n-1}| = \frac{1}{Q_n Q_{n-1}}.$$

Mamy więc

$$\frac{1}{Q_n Q_{n-1}} > |\frac{r}{s} - R_{n-1}| = |\frac{r}{s} - \frac{P_{n-1}}{Q_{n-1}}| = \frac{|rQ_{n-1} - sP_{n-1}|}{sQ_{n-1}} \geqslant \frac{1}{sQ_{n-1}},$$

skąd $s > Q_n$.

Na końcu Damian Orlef pokazywał geometryczną interpretację ułamków łańcuchowych. Pokazuje się, że jeśli dla każdej liczby wymiernej $\frac{p}{q}$ narysuje się okrąg o środku w punkcie $(\frac{p}{q}, \frac{1}{2q^2})$ i promieniu $\frac{1}{2q^2}$, to takie okręgi są albo rozłączne albo styczne. Teraz ułamki łańcuchowe są jakoś powiązane z wpisywaniem okręgów pomiędzy dwa styczne i prostą $y = 0$.

Ćwiczenia 9

Na ćwiczeniach zrobiliśmy jedno zadanie oraz zaczęliśmy drugie. Oba były inspirowane przez algorytmy strumieniowe. Pierwsze wzięło się stąd, że przy pokazywaniu algorytmu randomizowanego, aproksymującego F_2 skorzystaliśmy z faktu, że mając $\Theta(\log(n))$ bitów losowych możemy stworzyć liniową rodzinę zmiennych Rademachera (jakby rzut monetą), które są czwórkami niezależne. To zadanie tak naprawdę można rozdzielić na kilka, co zrobiliśmy.

Drugie zadanie natomiast wzięło się stąd, że przy pokazywaniu, że algorytm deterministyczny, który aproksymuje F_k dla $k \neq 1$ musi używać $\Theta(n)$ pamięci wykorzystaliśmy fakt, że postulowana rodzina zbiorów $\mathcal{F}$ istnieje.

Mówimy, że zmienne $X_1, \ldots, X_k$, przyjmujące wartości ze skończonego zbioru S są *niezależne* jeśli dla dowolnych $a_1, \ldots, a_k \in S$ zachodzi:

$$\mathbb{P}(X_1 = a_1 \wedge X_2 = a_2 \wedge \ldots X_k \wedge a_k) = \mathbb{P}(X_1 = a_1)\mathbb{P}(X_2 = a_2) \cdots \mathbb{P}(X_k = a_k).$$

Zmienne $X_1, \ldots, X_k$ są *r-niezależne*, jeśli dla każdego zbioru $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$ zmienne $X_{i_1}, \ldots, X_{i_r}$ są niezależne. Dla $r = 2$ nazywamy to też parami niezależnością, dla $r = 3$ trójkami niezależnością itd.

1. Pokaż, że mając $\log(n)$ bitów losowych możemy realizować następujący algorytm: ktoś nam daje $i \in \{1, \ldots, n\}$, a my zwracamy zmienną X_i. Zmienne X_i mają spełniać: $\mathbb{P}(X_i = 1) = \mathbb{P}(X_i = -1) = \frac{1}{2}$ oraz być parami niezależne.

Niech te bity losowe to $b_1, \ldots, b_k$. Robimy tak, że dla każdego niepustego zbioru $S \subseteq \{1, \ldots, k\}$ definiujemy zmienną $X_S = \bigoplus_{i \in S} b_i$. Wówczas wszystkie X_S są parami niezależne i jest ich $2^k - 1$.

2. Teraz pokazać, że podobnie możemy zrobić, by zmienne X_i były trójkami niezależne.

Robimy tak jak poprzednio bity $b_1, \ldots, b_k$ oraz specjalny bit b. Dla dowolnego (nawet pustego) zbioru $S \subseteq \{1, \ldots, k\}$ definiujemy $X_S = (\bigoplus_{i \in S} b_i) \oplus b$. Łatwo sprawdzić, że dla dowolnych S_1, S_2, S_3 zmienne X_{S_i} i X_{S_j} są niezależne oraz $S_1 \oplus S_2 \neq S_3$. Ten ostatni warunek implikuje, że zmienne X_{S_1}, X_{S_2} oraz X_{S_3} są niezależne. Agitowaliśmy to na ćwiczeniach, ale nie pokazaliśmy tego.

3. Teraz pokazać to samo dla czwórkami niezależnych zmiennych oraz ogólnie r-niezależnych dla ustalonego r.

Najpierw dla czwórkami niezależnych. Weźmy bity $b_1, \ldots, b_k$. Będziemy chcieli wybierać niektóre podzbiory $S \subseteq \{1, \ldots, k\}$. Powinno być tak, że $S_{i_1} \neq \emptyset$, $S_{i_1} \neq S_{i_2}$, $S_{i_1} \oplus S_{i_2} \neq S_{i_3}$ oraz $S_{i_1} \oplus S_{i_2} \oplus S_{i_3} \neq S_{i_4}$. Ładniej to wygląda napisane tak:

$$S_{i_1} \neq \emptyset$$
$$S_{i_1} \oplus S_{i_2} \neq \emptyset$$
$$S_{i_1} \oplus S_{i_2} \oplus S_{i_3} \neq \emptyset$$
$$S_{i_1} \oplus S_{i_2} \oplus S_{i_3} \oplus S_{i_4} \neq \emptyset.$$

Powiedzmy, że wybieramy te zbiory. Powiedzmy, że mamy już wybranych m z nich. Wtedy: pierwszy warunek zabrania nam 1 zbioru, drugi m zbiorów, trzeci $\binom{m}{2}$, a czwarty $\binom{m}{3}$ zbiorów. W sumie rzędu m^3 zbiorów. A więc, z grubsza, dopóki $m^3 < 2^k$ to możemy jeszcze dobrać jakiś zbiór. A więc wybierzemy rzędu $2^{k/3}$ zbiorów, czyli możemy zrobić rzędu $2^{k/3}$ zmiennych 4-niezależnych. Analogicznie możemy zrobić rzędu $2^{k/(r-1)}$ zmiennych r-niezależnych.

4. Pokaż, że istnieje rodzina $\mathcal{F}$ podzbiorów zbioru $\{1, \ldots, n\}$ takich, że

1. dla każdego $S \in \mathcal{F}$ zachodzi $|S| = n/4$,
2. dla każdych $S, T \in \mathcal{F}$ zachodzi $|S \cap T| \leqslant n/8$,
3. rodzina $\mathcal{F}$ jest wykładnicza, czyli $|\mathcal{F}| = 2^{\Theta(n)}$.

Nie rozwiązaliśmy tego, ale zostawiliśmy do pomyślenia w domu. Powiedzieliśmy o dwóch sposobach, które znam, które można do tego stosować. Jedno to metoda probabilistyczna. Drugie to interpretacja grafowa. Dla każdego zbioru mocy $n/4$ robimy wierzchołek, łączymy krawędzią zbiory, które mają przecięcie co najmniej mocy $n/8$. Wystarczy teraz pokazać, że istnieje wykładniczej wielkości zbiór niezależny.

Ewentualnie można tu zrobić zadania z algorytmów strumieniowych (których nie robiliśmy, ale miałem w planie):

- pokaż, że algorytm randomizowany dokładny obliczający F_k musi używać $\Omega(n)$ pamięci dla $k \neq 1$,
- pokaż, że algorytm randomizowany aproksymujący F_1 musi używać $\Omega(\log \log m)$ pamięci,
- pokaż, że algorytm randomizowany aproksymujący F_2 musi używać $\Omega(\log n + \log \log m)$ pamięci,
- zaprojektuj algorytm przybliżający $\sum_{i=1}^{n} \log(m_i!)$ w sensownej pamięci (ten sposób co dla F_k).

Ćwiczenia 10

Będziemy zajmować się metodą probabilistyczną. Została wprowadzona mniej więcej w latach 40-tych XX wieku, jej pionierem był Erdös, który wymyślił wiele dowodów, przy jej użyciu (choć nie on ją wymyślił). Polega na tym, że pokazuje się istnienie obiektu spełniającego pewne wymagania poprzez fakt, że losowy obiekt spełnia te wymagania. Często też pokazuje się tak, że istnieje obiekt o pewnej własności $\geqslant k$ tak, że wartość oczekiwana tej własności jest $\geqslant k$. Metoda ta okazała się niesłychanie skuteczna, nieraz też wtedy, gdy ciężko skonstruować konkretny obiekt. Stosowana jest w wielu działach matematyki. W informatyce teoretycznej często w teorii grafów, buduje się graf losowy (jakiegoś rodzaju) i stosuje metodę.

Oprócz tego rozwiążemy też zadanie 4 z ćwiczeń 9.

Rozważmy przykład, podany zresztą przez Erdösa. Kolorujemy K_n na dwa kolory. Pokazać, że da się tak pokolorować, by nie było monochromatycznej kliki K_r. Pokażmy to dla $n = 25$, $r = 7$. Ustalmy konkretną klikę. Ona ma $\binom{7}{2} = 21$ krawędzi. Prawdopodobieństwo, że wszystkie będą tego samego koloru to $2^{-(21-1)} = 2^{-20}$. Takich klik jest $\binom{25}{7} = 480700$. Zatem prawdopodobieństwo, że któraś z nich będzie monochromatyczna jest mniejsze lub równe $\frac{480700}{2^{20}} < 1$. Zatem istnieje kolorowanie takie, że żadna z klik wielkości 7 nie jest monochromatyczna.

1. Pokaż, że w grafie jest cięcie o mocy $\geqslant \frac{m}{2}$.

Rozważmy konkretną krawędź. Wybierzmy losowo wierzchołki do zbioru S, będziemy rozważać cięcie pomiędzy S a $V \setminus S$. Prawdopodobieństwo, że nasza krawędź należy do cięcia to $\frac{1}{2}$. A więc wartość oczekiwana $\mathbb{E}X_i$, gdzie X_i to należenie krawędzi do cięcia to $\frac{1}{2}$. Zatem $\mathbb{E}X$, gdzie X to liczba krawędzi w cięciu to $\mathbb{E}X = \frac{m}{2}$. Zatem istnieje cięcie o minimum $\frac{m}{2}$ krawędziach. To jest też przykład wykorzystania wartości oczekiwanej.

2. Pokaż, że można pokolorować każdy element zbioru $\{1, 2, \ldots, 2015\}$ na jeden z czterech kolorów tak, by nie było żadnego 10 wyrazowego ciągu arytmetycznego w jednym kolorze.

Kolorujemy losowo elementy. Konkretny ciąg długości 10 jest monochromatyczny z prawdopodobieństwem 4^{-9}. Oszacujmy z góry liczbę ciągów. Nie działa takie najprostsze, tzn., że pierwszy wyraz może być od 1 do 2006, a skok może

być od 1 do $\lfloor \frac{2014}{9} \rfloor = 223$, bo $2006 \cdot 223 = 447338 > 4^9$. Zatem szacujemy dokładniej. Jak pierwszy wyraz to a, to skok może być od 1 do $\lfloor \frac{2015-a}{9} \rfloor$. Zatem ciągów jest nie więcej niż

$$\sum_{a=1}^{2006} \frac{2015-a}{9} \leqslant \frac{\sum_{a=1}^{2014} a}{9} = \frac{2014 \cdot 2015}{18} < \frac{2^{11} \cdot 2^{11}}{16} = 2^{18} = 4^9.$$

Czyli prawdopodobieństwo, że pewien ciąg jest monochromatyczny jest mniejsze niż 1. Zatem istnieje pokolorowanie takie, że nie ma ciągu monochromatycznego.

3. Rozwiązujemy teraz zadanie 4 z ćwiczeń 9.

Ta metoda została zaproponowana przez Marcina Pilipczuka. Najpierw zróbmy to metodą grafową. Zróbmy graf, w którym jest $\binom{n}{n/4}$ wierzchołków, każdy to pewien podzbiór S mocy $n/4$. Robimy krawędź między wierzchołkami gdy przecięcie odpowiadających zbiorów jest większe niż $n/8$. Zobaczmy, że każdy zbiór niezależny w tym grafie spełnia dwa pierwsze warunki z zadania. A więc wystarczy pokazać, że istnieje zbiór niezależny wykładniczego rozmiaru.

Wierzchołków jest $\binom{n}{n/4}$. Oszacujemy z góry stopień wierzchołka. Powiedzmy, że przecięcie jest wielkości k. Takich k możliwych jest około $n/8$ (od $n/8$ do $n/4$). Policzmy teraz dla konkretnego k. Wyborów jest $\binom{n}{k}$, więc nie więcej niż $2^{n/4}$. Poza tym z pozostałych $3n/4$ wierzchołków musimy dobrać ileś, nie więcej niż $n/8$. To to jest nie więcej niż $\binom{3n/4}{n/8}$.

Policzmy ile jest mniej więcej wierzchołków w terminach c^n. Najpierw może $\binom{n}{n/4}$. Ze wzoru Stirlinga $n! \approx (n/e)^n$. Ogólnie

$$\binom{an}{bn} = \frac{(an)!}{(bn)!(an-bn)!} \approx \frac{(an/e)^{an}}{(bn/e)^b n \cdot (an-bn/e)^{an-bn}}$$

$$= \frac{a^{an} n^{an} e^{bn} e^{an-bn}}{e^{an} b^{bn} n^{bn} (a-b)^{an-bn} n^{an-bn}} = \frac{a^{an}}{b^{bn}(a-b)^{(a-b)n}} = \Big(\frac{a^a}{b^b (a-b)^{a-b}}\Big)^n.$$

A więc

$$\binom{n}{n/4} \approx \Big(\frac{1}{(1/4)^{(}1/4)(3/4)^{3/4}}\Big)^n = \Big(\frac{4}{3^{3/4}}\Big)^n \approx 1,75^n.$$

Teraz

$$\binom{3n/4}{n/8} \approx \Big(\frac{(3/4)^{(}3/4)}{(1/8)^{(}1/8)(5/8)^{(}5/8)}\Big)^n \approx 1,40203^n.$$

A więc

$$n/8 \cdot 2^{n/4} \cdot \binom{3n/4}{n/8} \approx 1,1892^n \cdot 1,40203^n \approx 1,667^n.$$

W grafie w n wierzchołkach i maksymalnym stopniu d istnieje zbiór niezależny o mocy przynajmniej $n/(d+1)$. A więc tu istnieje zbiór niezależny o mocy przynajmniej

$$\Big(\frac{1,75}{1,667}\Big)^n \approx 1,049^n,$$

co jest wykładnicze.

Teraz drugie rozwiązanie, ta technika została zaproponowana przez Tomka Czajkę. Robimy metodą probabilistyczną. Wylosujmy K zbiorów $S_1, \ldots, S_K$ w

ten sposób, że każdy z n elementów wrzucamy do zbioru S_i z prawdopodobieństwem $1/3$. Wtedy wartość oczekiwana wielkości zbioru to $n/3 > n/4$, a wartość oczekiwana przecięcia to $n/9 < n/8$. Teraz korzystamy z pewnej wersji nierówności Chernoffa, która mówi, że dla konkretnego zbioru S_i prawdopodobieństwo tego, że wielkość S_i jest poniżej $n/4$ lub dla konkretnych S_i, S_j wielkość przecięcia jest powyżej $n/8$ jest wykładniczo małe w stosunku do n. Zaraz tu dopracujemy szczegóły. A zatem alternatywa tych dwóch zdarzeń jest wykładniczo mała w stosunku do n, a zatem możemy wziąć wykładniczo duże K takie, że suma tych możliwości jest mniejsza niż 1 i będzie na pewno wciąż istniało niezerowe prawdopodobieństwo, że wszystkie zbiory są duże, a przecięcia małe. Oczywiście jak zbiory są większe niż $n/4$, to możemy je obciąć nieco, wtedy przecięcia nie wzrosną i nadal będzie ok.

Wersja nierówności Chernoffa, z której możemy skorzystać jest taka. Niech $X_1, \ldots, X_k$ to niezależne zmienne losowe o wartościach w $\{0, 1\}$. Niech $X = \sum_{i=1}^{k} X_i$, $\mu = \mathbb{E}X$. Wtedy dla każdego $\delta > 0$ zachodzi

$$\mathbb{P}(X > (1+\delta)\mu) < \Big(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\Big)^{\mu}.$$

Niech teraz S, T to moje zbiory. Kładę $X_i = 1$ gdy $i \in S$. Mam $X = \sum_{i=1}^{n} X_i$ to wielkość $S \cap T$. Zachodzi $\mathbb{E}X = n/9$. Z Chernoffa mam

$$\mathbb{P}(X > (1 + 1/8) \cdot n/9) < \Big(\frac{e^{1/8}}{(9/8)^{9/8}}\Big)^{n/9} \approx (0.9925)^{n/9},$$

co jest wykładniczo małe. Podobnie skorzystam z Chernoffa w drugą stronę. To jest techniczne, ale idea Chernoffa jest zasadniczo jasna.

4. Niech $n \in \mathbb{Z}^+$. Niech A będzie zbiorem n reszt z dzielenia przez n^2. Pokaż, że istnieje zbiór B złożony z n reszt z dzielenia przez n^2 który spełnia warunek: przynajmniej połowa reszt z dzielenia przez n^2 przystaje do $a + b$ dla pewnego $a \in A$, $b \in B$.

Losujemy liczby z B. Prawdopodobieństwo, że konkretna liczba k nie jest postaci $a + b$ to jest

$$(1 - \frac{n}{n^2})^n = (1 - 1/n)^n < 1/e < 1/2.$$

Zatem prawdopodobieństwo, że ustalona liczba jest postaci $a + b$ jest większe lub równe $1/2$, czyli wartość oczekiwana jest większa lub równa $n^2/2$, czyli jest pewien wybór B taki, że wychodzi więcej lub równo $n^2/2$.

Można dać jeszcze więcej zadań na metodę probabilistyczną. Jest tego sporo w sieci, jest np. artykuł Tomka Kobosa z Delty o metodzie probabilistycznej albo zadania braci Kotowskich (z polskich źródeł).

Ćwiczenia 11

Dzisiaj kontynuujemy metodę probabilistyczną, nieco bardziej zaawansowane rzeczy, ale nie bardzo.

1. Pokaż, że istnieje turniej, w którym jest przynajmniej $\frac{n!}{2^{n-1}}$ cykli Hamiltona.

Po prostu losujemy skierowanie krawędzi. Konkretny cykl Hamiltona ma 2 opcje za 2^n, żeby cały był skierowany w tę samą stronę. Potencjalnych cykli Hamiltona jest $n!$. A zatem wartość oczekiwana cykli Hamiltona to $\frac{n!}{2^{n-1}}$, a więc istnieje turniej, który ma przynajmniej tyle.

2. Niech liczba $n = n(k, \ell)$ będzie maksymalnym n takim, że istnieją zbiory $A_1, \ldots, A_n$ oraz $B_1, \ldots, B_n$ (powiedzmy liczb naturalnych, ale to nieistotne) takie, że:

- dla każdego $i \in \{1, \ldots, n\}$ zachodzi $|A_i| = k$, $|B_i| = \ell$,
- dla każdego $i \in \{1, \ldots, n\}$ zachodzi $A_i \cap B_i = \emptyset$,
- dla każdych $i, j \in \{1, \ldots, n\}$, $i \neq j$ zachodzi $A_i \cap B_j \neq \emptyset$.

Pokazać, że $n(k, l) = \binom{k+\ell}{k}$.

Wskazówka: uporządkować losowo dziedzinę i rozważyć zdarzenia U_i.

Najpierw pokażmy, że $n(k, l) \geqslant \binom{k+\ell}{k}$. Po spełniają: A_i - podzbiory $\{1, \ldots, k+\ell\}$ wielkości k, B_i podzbiory wielkości ℓ, gdzie $B_i = \{1, \ldots, k+\ell\} \setminus A_i$.

Teraz pokażemy super argument za tym, że lepiej się nie da. Przypuśćmy, że mamy jakąś lepszą rodzinę, dziedziną jest $X = \bigcup_{1 \leqslant i \leqslant n} A_i \cup B_i$. Uporządkujmy X liniowo w losowy sposób. Prawdopodobieństwo zdarzenia U_i: wszystkie elementy A_i są przed B_i wynosi $\frac{1}{\binom{k+\ell}{k}}$. Zauważmy, że zdarzenia U_i są rozłączne. A zatem

$$1 \geqslant \mathbb{P}\Big(\bigcup_{1 \leqslant i \leqslant n} U_i\Big) = n\mathbb{P}(U_i) = \frac{n}{\binom{k+\ell}{k}},$$

z czego wynika, że $n \leqslant \binom{k+\ell}{k}$.

3. Pokaż lemat Spernera: dla rodziny podzbiorów $\mathcal{F}$ zbioru $\{1, \ldots, 2n\}$ takiej, że dla $S, T \in \mathcal{F}$ zachodzi $S \not\subseteq T$ spełnione jest $|\mathcal{F}| \leqslant \binom{2n}{n}$.

Wskazówka: zrobić tak jak w poprzednim zadaniu, tylko A_i nie mają ustalonej wielkości.

Powiedzmy, że jest taka rodzina, to są zbiory A_i. Kładziemy $B_i = \{1, \ldots, 2n\} \setminus A_i$. Niech $|\mathcal{F}| = K$. Wówczas używając argumenty z poprzedniego zadania dostajemy, że

$$1 \geqslant \sum_{i=1}^{K} \frac{1}{\binom{2n}{|A_i|}} \geqslant \sum_{i=1}^{K} \frac{1}{\binom{2n}{n}} = \frac{K}{\binom{2n}{n}},$$

zatem $K \leqslant \binom{2n}{n}$.

4. Pokaż słabe twierdzenie Turana: niech d to średni stopień wierzchołka w grafie, czyli $d = \frac{2m}{n}$. Pokaż, że wówczas wielkość zbioru niezależnego spełnia $\alpha(G) \geqslant \frac{n}{2d}$. Uwaga: twierdzenie Turana mówi o $\frac{n}{d+1}$, czego nie da się już poprawić (graf będący sumą K_{d+1}).

Zauważmy, że w grafie, który ma n wierzchołków i m krawędzi istnieje co najmniej $n - m$ spójnych składowych, więc istnieje też zbiór niezależny o mocy

$n-m$. Skupmy się na pokazaniu, że istnieje taki podzbiór S wierzchołków grafu, że $n_S - m_S \geqslant \frac{n}{2d}$, gdzie n_S i m_S to odpowiednio liczba wierzchołków i krawędzi w tym zbiorze.

Zróbmy tak: wylosujmy zbiór S, każdy wierzchołek wrzucamy do S z prawdopodobieństwem p. Niech X to liczba wierzchołków, a Y to liczba krawędzi w S. Wówczas $\mathbb{E}X = np$, $\mathbb{E}Y = mp^2 = \frac{nd}{2}p^2$. Zatem $\mathbb{E}(X - Y) = np(1 - pd/2)$. Jeśli weźmiemy $p = \frac{1}{d}$, to mamy $\mathbb{E}(X - Y) = \frac{n}{2d}$. A zatem istnieje przynajmniej jeden zbiór S taki, że $n_S - m_S \geqslant \frac{n}{2d}$.

5. Pokaż, że $\binom{2n}{n} \geqslant \frac{2^{2n}}{2n+1}$.

To jest na rozgrzewkę. Po prostu pokazuje się, że $\binom{2n}{n}$ jest największy spośród $\binom{2n}{i}$ dla $0 \leqslant i \leqslant 2n$.

Przypomnimy teraz twierdzenie Czebyszewa z rachunku prawdopodobieństwa:

$$\mathbb{P}(|X - \mathbb{E}X| \geqslant t) \leqslant \frac{VarX}{t^2}.$$

To się dowodzi bardzo prosto. Rozważmy zmienną Y, która nie przyjmuje wartości ujemnych. Wówczas

$$\mathbb{E}Y \geqslant s \cdot \mathbb{P}(X \geqslant s),$$

co się nazywa nierównością Markowa. Niech teraz $Y = |X - \mathbb{E}X|^2$. Mamy więc

$$VarX = E(|X - \mathbb{E}X|^2) \geqslant t^2\mathbb{P}(|X - \mathbb{E}X|^2 \geqslant t^2) = t^2\mathbb{P}(|X - \mathbb{E}X| \geqslant t),$$

co jest równoważnie nierówności Czebyszewa.

6. Pokaż, że $\binom{2n}{n} \geqslant \frac{2^n}{4\sqrt{n}+2}$.

Wskazówka: rozważyć zmienną losową $Y = X_1 + \ldots + X_{2n}$, gdzie X_i są niezależne oraz $\mathbb{P}(X_i = 0) = \mathbb{P}(X_i = 1) = \frac{1}{2}$. Skorzystać też z twierdzenia Czebyszewa.

Zobaczmy, że $\mathbb{P}(Y = k) = \frac{\binom{2n}{k}}{2^{2n}}$. Mamy $\mathbb{E}Y = n$, $VarY = 2n \cdot VarX_i = \frac{n}{2}$. Zatem z Czebyszewa mamy:

$$\mathbb{P}(|Y - n| \geqslant \sqrt{n}) \leqslant \frac{n}{2(\sqrt{n}^2)} = \frac{1}{2},$$

czyli $\mathbb{P}(|Y-n| \leqslant \sqrt{n}) \geqslant \frac{1}{2}$. Mamy jednak $\mathbb{P}(Y = n) > \mathbb{P}(Y = k)$ dla $0 \leqslant k \leqslant 2n$, $k \neq n$. A więc

$$\mathbb{P}(Y = n) \geqslant \frac{\mathbb{P}(|Y - n| \leqslant \sqrt{n})}{2\sqrt{n} + 1} \geqslant \frac{1}{4\sqrt{n} + 2}.$$

Często w metodzie probabilistycznej chcemy pokazać, że prawdopodobieństwo wystąpienia jednego z niesprzyjających wydarzeń (np. monochromatycznej kliki) jest mniejsze niż 1. To oznacza, że prawdopodobieństwo tego, że żadne z nich nie wystąpi jest większe niż 0, czyli istnieje obiekt, w którym żadnego z nich nie ma. Często prawdopodobieństwo sumy wydarzeń szacujemy przez sumę prawdopodobieństw. Jednak czasem suma prawdopodobieństw jest większa niż

1, a nadal prawdopodobieństwo sumy wydarzeń jest mniejsze niż 1. Jeśli zdarzenia są niezależne, to wtedy

$$\mathbb{P}(\bigcup_{1\leqslant i\leqslant n} A_i) = 1 - \prod_{1\leqslant i\leqslant n} (1-\mathbb{P}(A_i)),$$

czyli wystarczy, by $\mathbb{P}(A_i) < 1$ dla każdego $1 \leqslant i \leqslant n$. Czasem jednak nie wszystkie zdarzenia są niezależne, ale nadal można zrobić coś w tym stylu. Z pomocą przychodzi lokalny lemat Lovasza (wersja symetryczna i niesymetryczna).

Lemat 1 (Symetryczny lokalny lemat Lovasza)**.** *Niech $A_1, \ldots, A_n$ będą zdarzeniami takimi, że $\mathbb{P}(A_i) \leqslant p$ dla $1 \leqslant i \leqslant n$ oraz każde z nich jest zależne od co najwyżej d pozostałych. Jeśli $p \leqslant \frac{1}{e(d+1)}$, to wówczas $\mathbb{P}(\bigcap_{1\leqslant i\leqslant n} \bar{A}_i) > 0$.*

Czyli jakby tu sytuacja dla $d = n-1$ pogarsza się e razy, to znaczy bez lematu, dla $d = n-1$ potrzeba byłoby $p < \frac{1}{n}$. No ale mamy za to uogólnienie na dowolne d.

Teraz za to niesymetryczny lemat, gdy różne zdarzenia mają potencjalnie różną liczbę zdarzeń od siebie zależnych. Symetryczna wersja dowodzi się łatwo z ogólnej.

Lemat 2 (Lokalny lemat Lovasza)**.** *Niech $A_1, \ldots, A_n$ będą zdarzeniami, $G = (V, E)$ będzie ich grafem zależności (wierzchołki to zdarzenia, krawędź gdy są zależne). Niech $x_i \in [0, 1)$ dla $1 \leqslant i \leqslant n$ takie, że dla $1 \leqslant i \leqslant n$ zachodzi*

$$\mathbb{P}(A_i) \leqslant x_i \prod_{(i,j)\in E} (1-x_j).$$

Wówczas

$$\mathbb{P}(\bigcap_{1\leqslant i\leqslant n} \bar{A}_i) \geqslant \prod_{1\leqslant i\leqslant n} (1-x_i) > 0.$$

7. Mamy $11n$ punktów na okręgu pokolorowanych na n kolorów, w każdym kolorze jest 11. Pokazać, że możemy wybrać zbiór n punktów, każdy w innych kolorze, tak, że żadne dwa sąsiednie nie będą wybrane.

Losujemy po jednym punkt z każdego koloru, każdy punkt z prawdopodobieństwem $\frac{1}{11}$. Niech A_i to zdarzenie: wybrane zostały punkty i oraz $i+1$ na okręgu (modulo $11n$). Mamy $\mathbb{P}(A_i) = p = \frac{1}{121}$. Policzymy od ilu zdarzeń jest ono zależne. Niech punkty i oraz $i+1$ będą w kolorach C_1 i C_2. Jest 11 punktów w C_1, więc oprócz A_i jest maksymalnie 21 innych zdarzeń z tymi punktami. Podobnie z C_2, w sumie są maksymalnie 42 zależne zdarzenia. Liczymy, że $e \cdot (42+1) \approx 116,89 < 121$, więc z symetrycznego lokalnego lematu Lovasza mamy, że $\mathbb{P}(\bigcap_{1\leqslant i\leqslant n} \bar{A}_i) > 0$, co kończy dowód.

8. Pokaż symetryczny lemat Lovasza z ogólnego.

Kładziemy $x_i = \frac{1}{d+1}$. Mamy wówczas dla każdego $1 \leqslant i \leqslant n$

$$x_i \prod_{(i,j)\in E} (1-x_j) = \frac{1}{d+1}(1-\frac{1}{d+1})^d \geqslant \frac{1}{d+1}(e^{-\frac{1}{d+1}})^d \geqslant \frac{1}{e(d+1)} \geqslant p.$$

9. Pokaż, że dowolna instancja k-SATa, w której każda zmienna występuje w co najwyżej $\frac{2^{k-2}}{k}$ klauzulach jest spełnialna. Załóżmy $k \geqslant 4$, dla mniejszych to nie ma sensu.

Wybierzmy losowo zmienne. Niech A_i oznacza: klauzula i-ta nie jest spełniona. Chcemy pokazać, że $\mathbb{P}(\bigcap_{1 \leqslant i \leqslant n} \bar{A}_i) > 0$. Mamy $\mathbb{P}(A_i) = 2^{-k} = p$. Policzmy od ilu A_j zależny jest A_i. Żeby były zależne, to musi być przynajmniej jedna zmienne wspólna. A więc jest tego $d \leqslant k\frac{2^{k-2}}{k} = 2^{k-2}$. Mamy więc

$$p = 2^{-k} = \frac{1}{4}\frac{1}{d} < \frac{1}{e(d+1)},$$

bo dla $k \geqslant 4$, możemy ustalić $d = 2^{k-2} \geqslant 4$ i wtedy $(2^{k-2}+1)e < 2^k$, w szczególności $5e < 16$.