

MATEMATYKA DYSKRETNA

WYBRANE DOWODY

„Myślę, że 7 punktów na 20 to nie jest zły wynik”

POPEŁNIONE PRZEZ

DZIURAWY PONTON

ZAŁATANY PONTON

PUCHATY POMPON

ZATOPIONY PONTON

TONĄCY PONTON

NOTNOP

Kraków

Anno Domini 2023

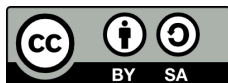
Spis treści

1	Kombinatoryka	1
1.1	Liczba sposobów umieszczenia n obiektów w k szufladach	1
1.2	Współczynnik dwumianowy i liczby Stirlinga	1
1.2.1	Współczynnik dwumianowy	1
1.2.2	Liczba Stirlinga II rodzaju	2
1.2.3	Liczba Stirlinga I rodzaju	2
1.3	Liczby Catalana	3
1.3.1	Wzór kombinatoryczny	3
1.3.2	Zależność rekurencyjna	5
2	Zasada włączeń i wyłączeń	6
2.1	Dowód zasady	6
2.2	Zliczanie cykli Hamiltona	7
2.3	Problem drzewa Steinera	8
3	Teoria liczb	12
3.1	Algorytm Euklidesa i tożsamość Bezouta	12
3.2	Fundamentalne twierdzenie arytmetyki	14
3.3	Chińskie twierdzenie o resztach	14
3.4	Funkcja φ Eulera	16
3.4.1	Definicja funkcji φ	16
3.4.2	Twierdzenie Eulera	16
3.4.3	Multiplikatywność funkcji φ	17
3.4.4	Wzór „jawny” na funkcję φ	17
3.5	Splot Dirichleta	18
3.6	Funkcja Möbiusa	21
3.6.1	Definicja i własności funkcji Möbiusa	21
3.6.2	Inwersja Möbiusa	22
3.6.3	Przykład zastosowania przy funkcji φ	22
4	Posety	24
4.1	Twierdzenie Dilwortha	24

4.2	Twierdzenie dualne do Dilwortha	27
4.3	Lemat Erdősa-Szekeresa o podciągach monotonicznych	28
4.4	Nierówność LYM	29
4.5	Twierdzenie Spernera	30
4.6	Nawiasowania i liczby Dedekinda	31
4.7	Cienie i twierdzenie Erdősa-Ko-Rado	33
4.8	Twierdzenie Kruskala-Katony/Lovása	34
5	Twierdzenie Ramseya i przyjaciele	38
5.1	Twierdzenie Ramsey'a	38
5.2	Ograniczenia dolne niektórych liczb Ramsey'a	40
5.3	Ograniczenie górne niektórych liczb Ramsey'a	42
5.4	Twierdzenie Erdősa-Szekeresa	43
5.4.1	Dowód z twierdzenia Ramseya	43
5.4.2	Dowód z kubeczkami i czapeczkami	44
5.5	Twierdzenie Schura	45
5.6	Twierdzenie Halesa-Jewett'a	46
5.7	Twierdzenie van der Waerden'a	47
6	Funkcje tworzące	48
6.1	Rozwiązywanie rekurencji liniowych	48
6.1.1	Rozkład na ułamki proste	48
6.2	Ciąg Fibbonaciego	48
6.3	Ciąg Catalana	50
6.4	Zliczanie podziałów	52
7	Przepływy	57
7.1	Definicje	57
7.2	Własności przekrojów i przepływów	59
7.3	Twierdzenie Forda-Fulkersona	60
8	Skojarzenia	62
8.1	Twierdzenie Halla	62
8.2	Macierz symboliczna Tutte'a	64
9	Kolorowanie grafów	70
9.1	Liczba kolorująca	70
9.1.1	Co to w ogóle jest	70
9.1.2	Relacja z liczbą chromatyczną	71
9.1.3	Algorytm obliczania liczby kolorującej	71
9.2	Kolorowanie krawędziowe grafów dwudzielnych	72
9.3	Twierdzenie Vizinga	73

9.4	Twierdzenie Brooksa	78
9.5	Grafy bez trójkątów o dużej liczbie chromatycznej	81
9.5.1	Czemu interesują nas takie konstrukcje?	81
9.5.2	Co będziemy konstruować?	81
9.5.3	Konstrukcja Mycielskiego	82
9.5.4	Konstrukcja Tutte'a	84
9.5.5	Konstrukcja Zyкова	86
9.6	Shift grafy	87
9.7	Grafy przecięć kwadratów	88
9.8	Grafy przecięć prostokątów	88
9.8.1	Liczba kolorująca	88
9.8.2	Liczba chromatyczna	89
9.9	Grafy planarne	91
9.9.1	Wzór Eulera	91
9.9.2	Liczba kolorująca	91
9.9.3	5-kolorowość	93
9.9.4	5-wybieralność	94
10	Grafy, ale nie kolorowanie	98
10.1	Sekwencja stopni w grafie	98
10.2	Twierdzenie Turana	101
10.2.1	Graf Turana	101
10.2.2	Twierdzenie Turana	101

Licencja



Ten utwór jest dostępny na licencji Creative Commons Uznanie autorstwa na tych samych warunkach 4.0 Międzynarodowe.

Rozdział 1

Kombinatoryka

1.1 Liczba sposobów umieszczenia n obiektów w k szufladach

Rozróżnialność obiektów	Rozróżnialność szuflad	Iniektywnie	Surjektywnie	Dowolnie
Tak	Tak	k^n	$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} \cdot k!$	k^n
Tak	Nie	$\begin{cases} 0, n > k \\ 1 \leq k \end{cases}$	$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$	$\sum_{i=1}^k \left\{ \begin{smallmatrix} n \\ i \end{smallmatrix} \right\}$
Nie	Tak	$\binom{k}{n}$	$\binom{n-1}{k-1}$	$\binom{n+k-1}{k-1}$
Nie	Nie	$\begin{cases} 0, n > k \\ 1, n \leq k \end{cases}$	$p(n, k)$	$\sum_{i=1}^k p(n, i)$

Jako $p(n, k)$ definiujemy liczbę podziałów liczby n na k niezerowych składników.

1.2 Współczynnik dwumianowy i liczby Stirlinga

1.2.1 Współczynnik dwumianowy

Twierdzenie 1.2.1 (Wzór rekurencyjny na dwumian Newtona).

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad (1.1)$$

Dowód. Moc zbioru zawierającego wszystkie podzbiory k -elementowe zbioru n -elementowego wynosi właśnie $\binom{n}{k}$. Bierzemy sobie ten zbiór i nazywamy go F . Wybieramy jakikolwiek element ze zbioru n -elementowego którego zbiór podzbiorów rozważamy i nazywamy go x . Tworzymy dwa zbiory, A i B : A zawiera wszystkie zbiory z F których elementem jest x , B zawiera wszystkie zbiory z F do których x nie należy. Z oczywistych względów zachodzi:

$$A \cup B = F$$

$$A \cap B = \emptyset$$

Zatem jeśli zliczymy ile jest elementów w A , a ile w B , to suma tych liczb jest mocą zbioru F . Zbiorów w A jest $\binom{n-1}{k-1}$, bo dla każdego zbioru wiemy już, że jest tam x , a pozostałe elementy możemy wziąć jak chcemy. Zbiorów w B jest $\binom{n-1}{k}$, bo po prostu wybieramy k elementów z elementów które są różne od x (a których jest właśnie $n-1$). \square

1.2.2 Liczba Stirlinga II rodzaju

Twierdzenie 1.2.2 (Wzór rekurencyjny na liczbę Stirlinga II rodzaju).

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} + k \cdot \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\} \quad (1.2)$$

Dowód. Rozpatrujemy zbiór wszystkich podziałów zbioru n -elementowego na k niepustych podzbiorów (mający moc równą $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$) i nazwijmy go F . Bierzemy sobie jakiś x z naszego zbioru n -elementowego i wykonujemy podział zbioru F na zbiory A i B . Zbiór A zawiera wszystkie elementy F takie, że zawierają $\{x\}$, a więc, innymi słowy, jeden z „bloków” danego podziału musi być taki, że tylko x do niego należy. Zbiór B to zbiór pozostałych podziałów, a więc wszystkie podziały z F w których x występuje w swoim „bloku” razem z jakimiś innymi elementami. Z oczywistych względów zachodzi:

$$A \cup B = F$$

$$A \cap B = \emptyset$$

Łatwo zauważyć, że $A = \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\}$, bo mamy zawsze jeden „segment” w którym znajduje się sam x , więc moc zbioru A jest równa liczbie możliwych podziałów całej reszty elementów, czyli właśnie $n-1$ elementów na $k-1$ „bloków”. Moc zbioru B wynosi zaś $k \cdot \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\}$, bo dzielimy sobie wszystkie elementy poza x na k „bloków”, a potem „dorzucamy” x do któregoś z powstałych już „bloków” (oczywiście „bloki” przy podziale generowanym przez liczbę Stirlinga II rodzaju są niepuste). Ponieważ bloków do których możemy „dorzucić” x jest k , otrzymujemy $k \cdot \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\}$. To prowadzi nas już do postulowanej równości. \square

1.2.3 Liczba Stirlinga I rodzaju

Twierdzenie 1.2.3 (Wzór rekurencyjny na liczbę Stirlinga I rodzaju).

$$\left[\begin{matrix} n \\ k \end{matrix} \right] = \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right] + (n-1) \cdot \left[\begin{matrix} n-1 \\ k \end{matrix} \right] \quad (1.3)$$

Dowód. Stosujemy motyw podobny dla powyższych dowodów. F to zbiór zawierający wszystkie permutacje na n elementach które „rozbijają się” na k cykli. Bierzemy sobie jakiś element x i rozpatrujemy dwa zbiory, A , B takie że do A należą wszystkie permutacje gdzie x przechodzi na siebie samego, a do B należą wszystkie permutacje gdzie x nie przechodzi na siebie samego. Moc zbioru A to $\left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right]$, bo x przechodzący na siebie samego stanowi jeden cykl (więc

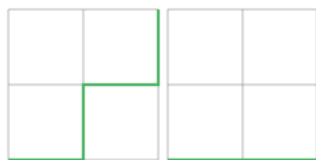
„pozostałość” permutacji trzeba rozbić na $k - 1$ cykli). Obliczenie mocy zbioru B jest nieco śmieszniejsze, ale okazuje się że jest równe $(n - 1) \cdot \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right]$. Wynika to z faktu, że bierzemy sobie wszystkie elementy poza x i robimy na nich permutacje, które da się podzielić na k cykli; następnie ten element x „dopychamy” w jakieś miejsce w jakimś cyklu. Przez „dopchnięcie” mam na myśli sytuację, gdy jakiś element y przechodził na element z , ale x „dopychamy” w miejsce z ; wtedy y przechodzi na x , a x na z . Operacja „dopchnięcia” nie psuje liczby cykli, a x możemy „dopchnąć” zawsze na $n - 1$ miejsc, co daje nam postulowaną równość. \square

1.3 Liczby Catalana

Liczba Catalana jest to liczba ścieżek długości $2n$ w kwadracie $n \times n$ „poniżej” przekątnej (lub na jej poziomie), idących za każdym razem jednostkę do góry lub jednostkę w prawo. Ścieżki takie nazywamy ścieżkami Dycka. Niezwykle formalna definicja. To jest jedna z tych rzeczy, które chyba po prostu trzeba narysować.



Rysunek 1.1: Ścieżki Dycka długości 2; $c_1 = 1$



Rysunek 1.2: Ścieżki Dycka długości 4; $c_2 = 2$



Rysunek 1.3: Ścieżki Dycka długości 6; $c_3 = 5$

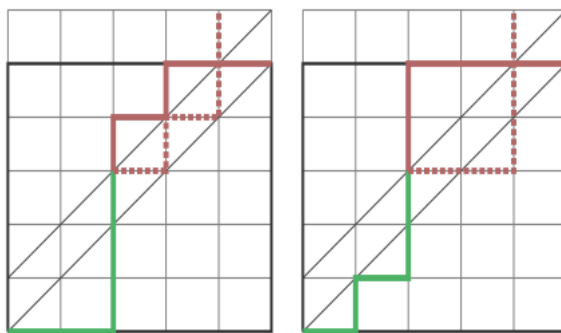
1.3.1 Wzór kombinatoryczny

Twierdzenie 1.3.1 (Wzór kombinatoryczny na liczby Catalana).

$$c_n = \frac{1}{n+1} \cdot \binom{2n}{n} \quad (1.4)$$

Mamy sobie nasz kwadrat $n \times n$. Przekątną możemy opisać tak jakby wzorem $y = x$ (tak intuicyjnie, bo nie działamy w żadnym układzie współrzędnych, bla bla bla). Robimy sobie

teraz prostą $y = x + 1$, idącą jakby „o jednostkę wyżej”. Zauważamy, że jeśli jakaś ścieżka przekracza linię naszej przekątnej, to musi „dotknąć” linii $y = x + 1$. *To widać.* Teraz wpadamy na świetny pomysł; jeśli jakaś ścieżka idąca po tym kwadracie „spotyka się” z $y = x + 1$, to od tego momentu odbijamy ją symetrycznie względem $y = x + 1$. Zauważamy, że ścieżka ta (po odbiciu) skończy się w punkcie $(n - 1, n + 1)$ zamiast w (n, n) . Fakt ten dowodzimy stosując dowód przez rysowanie.



Rysunek 1.4: Przykłady odbicia niepoprawnej ścieżki

Zauważamy fascynujący fakt, mianowicie dwie różne ścieżki będą mieć 2 różne odbicia, a więc nasze przekształcenie jest iniektywne. Ponadto, jak sobie zobaczymy jakąkolwiek ścieżkę zaczynającą się w $(0, 0)$, ale kończącą się w $(n - 1, n + 1)$, to jesteśmy w stanie zobaczyć gdzie pierwszy raz przecina się z $y = x + 1$, a następnie ją odbić, otrzymując ścieżkę idącą do (n, n) i niebędącą ścieżką Dycka, której odbicie daje wyjściową ścieżkę. Zatem odbijanie jest suriektywne. A to oznacza tylko jedną rzecz: bijekcję między ścieżkami które „nie są catalanowe”, a ścieżkami „odbitymi”.

Wszystkich możliwych ścieżek od $(0, 0)$ do (n, n) mamy $\binom{2n}{n}$, bo długość naszej drogi ma $2n$ i wybieramy sobie n miejsc gdzie idziemy w prawo. Wszystkich możliwych ścieżek od $(0, 0)$ do $(n - 1, n + 1)$ (czyli tych które są „złe”) mamy $\binom{2n}{n-1}$, bo, analogicznie, ścieżka jest długości $2n$ ale w prawo idziemy $n - 1$ razy. To prowadzi nas do wyniku:

$$\begin{aligned}
 c_n &= \binom{2n}{n} - \binom{2n}{n-1} \\
 &= \frac{(2n)!}{n! \cdot n!} - \frac{(2n)!}{(n-1)! \cdot (n+1)!} \\
 &= \frac{(n+1) \cdot (2n)!}{n! \cdot (n+1)!} - \frac{n \cdot (2n)!}{n! \cdot (n+1)!} \\
 &= \frac{(2n)!}{n! \cdot (n+1)!} \\
 &= \frac{1}{n+1} \cdot \frac{(2n)!}{n! \cdot n!} \\
 &= \frac{1}{n+1} \cdot \binom{2n}{n}
 \end{aligned}$$

1.3.2 Zależność rekurencyjna

Twierdzenie 1.3.2 (Wzór rekurencyjny na liczby Catalana).

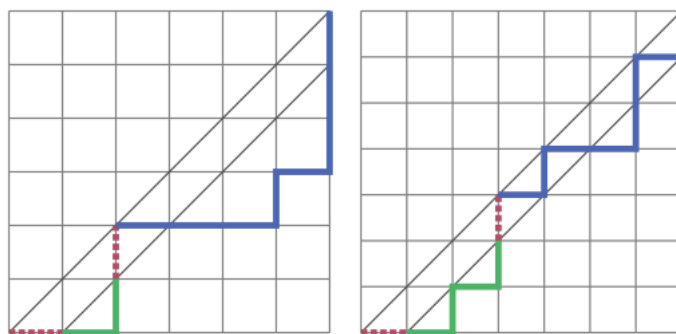
$$c_n = c_0 \cdot c_{n-1} + c_1 \cdot c_{n-2} + \cdots + c_{n-1} \cdot c_0 \quad (1.5)$$

Dowód. Znowuż mamy kwadrat $n \times n$, ale tym razem dorysowujemy sobie prostą $y = x - 1$. Każda ścieżka przetnie kiedyś tę linię i każda ścieżka dotknie kiedyś przekątnej $y = x$ (można to udowodnić machając i pokazując na rysunek). Rzecz teraz ma się tak, że jeśli po „spotkaniu się” z $y = x - 1$ idziesz do góry, to potem musisz odbić w prawo (lub w skrajnym przypadku skończyłeś poprawną ścieżkę). Jednocześnie pierwszy wybór kierunku (tzn. ten w punkcie $(0, 0)$ zawsze jest „w prawo”, bo jeśli ktoś pójdzie „do góry” to znajdzie się w $(0, 1)$, powyżej przekątnej $y = x$).

Bierzemy sobie zatem pierwsze miejsce gdzie spotkałeś się z $y = x$ i zauważamy, że jeśli dane jest ono jakimiś współrzędnymi (i, i) to przecięliśmy $y = x - 1$ w $(i, i - 1)$. Ponadto, ścieżka którą szliśmy od punktu $(1, 0)$ do $(i, i - 1)$ tak naprawdę jest ścieżką Dycka w kwadracie od punktów $(1, 0)$, $(i, i - 1)$ (kwadrat ten ma długość $i - 1$). Ależ plot twist! Ścieżka którą idziemy od punktu (i, i) do (n, n) jest zaś już po prostu ścieżką Dycka w kwadracie o długości boku $n - i$. Ścieżki te są od siebie niezależne i w ogóle, a długości tych „kwadratów catalanowych” sumują się do $i - 1 + n - i = n - 1$, więc teraz możemy zmaistrować wzór (w zależności od długości boków kwadratów, które z kolei są dyktowane tym kiedy się „spotkamy” z $y = x$):

$$c_n = \sum_{i=0}^{n-1} c_i \cdot c_{n-1-i}$$

Co już można odwinąć do postaci która była w twierdzeniu.



Rysunek 1.5: Przykłady „podzielenia” poprawnej ścieżki Dycka na podścieżki

□

Rozdział 2

Zasada włączeń i wyłączeń

2.1 Dowód zasady

Twierdzenie 2.1.1 (Zasada włączeń i wyłączeń).

$$\left| \bigcup_{i \in [n]} A_i \right| = \sum_{\emptyset \neq X \subset [n]} (-1)^{|X|-1} \cdot \left| \bigcap_{i \in X} A_i \right| \quad (2.1)$$

Dowód. Weźmy sobie jakieś $x \in \bigcup A_i$ należące dokładnie do k zbiorów (gdzie $k \leq n$). Bez straty ogólności można założyć, że $x \in A_1, A_2, A_3, \dots, A_k$ oraz $x \notin A_{k+1}, A_{k+2}, A_{k+3}, \dots, A_n$. Zauważamy, że x w sumie występującej po lewej stronie postulowanej równości zostanie zliczone raz (oczywiste), a po prawej:

1. Sumując $A_1, A_2, A_3, \dots, A_k$ zliczone zostanie k razy,
2. Sumując $A_1 \cap A_2, \dots$ zliczone zostanie $\binom{k}{2}$ razy i odjęte od wcześniejszej wartości
3. Sumując l -elementowe przecięcia zbiorów A_1, A_2, \dots, A_k zostanie odjęte/dodane $\binom{k}{l}$ razy.

Mamy więc, że x jest zliczone $\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} \dots$ razy. Powołujemy się wtedy na magiczny wzór, który wygląda następująco:

$$\sum_{i=0}^k (-1)^{i+1} \binom{k}{i} = -(1-1)^k = 0$$

Skąd mamy

$$\sum_{i=1}^k (-1)^{i+1} \binom{k}{i} = 1$$

bo $\binom{k}{0} = 1$. To prowadzi nas do konkluzji, że x po prawej stronie również został zliczony 1 raz, czyli wszystko działa tak jak powinno.

□

2.2 Zliczanie cykli Hamiltona

Zanim przejdziemy do twierdzenia, musimy wprowadzić niestety parę definicji. Przez U oznaczamy zbiór wszystkich **spacerów** długości $n + 1$ w grafie w którym usiłujemy zliczyć liczbę cykli Hamiltona (pod względem liczby wierzchołków; przez n oznaczamy oczywiście liczbę wierzchołków w grafie), zaczynających się w jakimś wierzchołku v_0 i również w nim kończących. Przez A_i oznaczamy zbiór wszystkich spacerów z U , które przechodzą przez wierzchołek o numerze i . Ponadto zakładamy, że

$$U = \bigcap_{i \in \emptyset} B$$

gdzie B jest czymkolwiek (w sensie serio czymkolwiek). Dlaczego tak zakładamy? Nie mam pojęcia, ale inaczej dowód by nie zadziałał. Formaliści mogą spojrzeć na definicję czapeczkowania jeśli czapeczkujemy jedynie po elementach zbioru pustego, but, honestly, I don't care. Ważna obserwacja zanim jeszcze przejdziemy do dowodu:

$$2 \cdot |H| = \left| \bigcap_{i \in [n]} A_i \right|$$

Gdzie H jest to zbiór zawierający wszystkie cykle Hamiltona. Ta obserwacja w sumie ma sens, bo jeśli jakiś spacer ma długość $n + 1$ zaczyna się i kończy w v_0 i jednocześnie przechodzi przez każdy wierzchołek, to musi być cyklem Hamiltona (no bo dwa razy był w v_0 , najpierw z niego wychodząc a potem do niego wchodząc, a w pozostałych $n - 1$ wierzchołkach musiał być dokładnie raz bo cały spacer ma długość $n - 1 + 2 = n + 1$). Należy zauważyć że cykle Hamiltona w ten sposób zliczamy zawsze podwójnie, bo cykle w grafach nieskierowanych mają to do siebie że można je obejść na 2 różne sposoby wychodząc z tego samego punktu, idąc „na prawo” lub „na lewo”.

Twierdzenie 2.2.1 (O liczbie cykli Hamiltona w grafie).

$$\left| \bigcap_{i \in [n]} A_i \right| = \sum_{X \subset [n]} (-1)^{|X|} \cdot \left| \bigcap_{i \in X} (U \setminus A_i) \right| \quad (2.2)$$

Dowód. Po pierwsze należy zauważyć, że

$$\left| \bigcap_{i \in [n]} A_i \right| = |U| - \left| \bigcup_{i \in [n]} (U \setminus A_i) \right|$$

W sumie jak się to pokontempluje to zaczyna się to robić oczywiste. Jest to obserwacja czysto teoriomnogościowa; jeśli jakiś spacer znajduje się w przecięciu, to znaczy że jest w każdym zbiorze A_i dla dowolnego i , a więc po prawej stronie nie zostanie „usunięty” z uniwersum (tj. zbioru U) bo za każdym razem zostanie usunięty ze zbioru elementów „do wywalenia”, a jeśli nie należy do przecięcia to znaczy że spacer ten nie należy do jakiegoś A_k , a więc $U \setminus A_k$ będzie go zawierać, a więc przy sumowaniu elementów „do wywalenia” zostanie on wliczony.

Pamiętacie nasze śmieszne założenie o tym, że U jest równe przecięciu po elementach zbioru pustego? Teraz go użyjemy, bo

$$|U| - \left| \bigcup_{i \in [n]} (U \setminus A_i) \right| = \left| \bigcap_{i \in \emptyset} (U \setminus A_i) \right| + \sum_{\emptyset \neq X \subset [n]} (-1)^{|X|} \cdot \left| \bigcap_{i \in X} (U \setminus A_i) \right|$$

To przejście może wyglądać przerażająco, ale w sumie nic ciekawego się tu nie stało; pierwszy element po lewej stronie (tj. U) rozpisaliśmy korzystając właśnie z założenia, że $U = \bigcap_{i \in \emptyset} B$, gdzie B jest czymkolwiek, a więc w szczególności $U \setminus A_i$. Drugi element z lewej strony rozpisaliśmy stosując po prostu zasadę włączeń i wyłączeń (aczkolwiek zmieniliśmy znak, by żyło się prościej, a więc i skorygowaliśmy potęgę przy (-1) by wszystko się zgadzało).

Teraz możemy sobie popatrzeć na to co nam wyszło, i uświadomić sobie, że teraz to już możemy sobie po prostu radośnie dodać pierwszy i drugi składnik z prawej strony:

$$\left| \bigcap_{i \in \emptyset} (U \setminus A_i) \right| + \sum_{\emptyset \neq X \subset [n]} (-1)^{|X|} \cdot \left| \bigcap_{i \in X} (U \setminus A_i) \right| = \sum_{X \subset [n]} (-1)^{|X|} \cdot \left| \bigcap_{i \in X} (U \setminus A_i) \right|$$

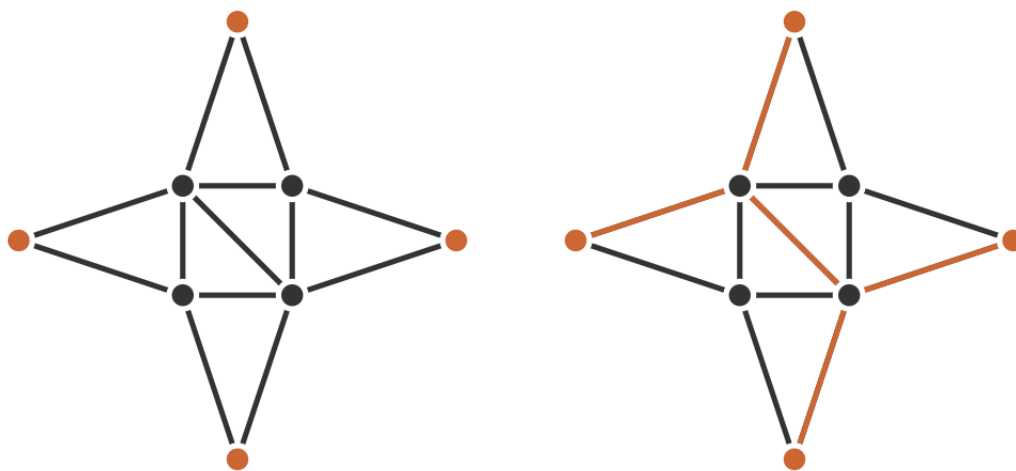
Co prowadzi nas do otrzymania postulowanej równości. □

A jak chcemy zastosować tę równość do zliczania ścieżek Hamiltona? Otóż jak sobie podumamy i oznaczymy $S_i = U \setminus A_i$ (czyli S_i to zbiór spacerów z uniwersum takich, że nie przechodzą przez wierzchołek i), to $\left| \bigcap_{i \in X} S_i \right|$ to są wszystkie spacery spełniające warunki bycia w uniwersum, ale na podgrafie indukowanym bez wierzchołków należących do X . A liczbę spacerów w grafie mających długość $n + 1$ między dwoma wierzchołkami możemy policzyć, robiąc macierz incydencji wierzchołków i podnosząc ją do potęgi $n + 1$. No i fajnie.

2.3 Problem drzewa Steinera

To nie jest przyjemny dowód i jest absolutnie koszmarny do sformalizowania. Mimo wszystko spróbuję. W sumie to nawet nie jest dowód, to jest bardziej algorytm postępowania.

Zacznijmy na początku od zdefiniowania problemu. Mamy graf G oraz zbiór wierzchołków, które z jakiegoś powodu nazywamy *terminalami*. Bardzo chcielibyśmy znaleźć najmniejszy (krawędziowo) podgraf, który łączy wszystkie terminale. Oczywiście widzimy, że musi być to drzewo (stąd nazwa), gdyż w przeciwnym razie moglibyśmy pozbyć się jakiejś krawędzi bez naruszania spójności.



Rysunek 2.1: Przykładowy graf z terminalami oraz minimalne drzewo je łączące

Spacerem rozgałęziającym się będziemy nazywać ukorzenione oraz uporządkowane (tzn. dzieci każdego wierzchołka są ponumerowane) drzewo, które „przerzucimy” w dosyć dziwny sposób na graf w którym szukamy drzewa Steinera. Generalnie wierzchołki drzewa mapujemy dowolnie na wierzchołki grafu, z tym że jeśli 2 wierzchołki w drzewie są połączone krawędzią, to po przemapowaniu również muszą być połączone krawędzią. Co ważne, **wiele wierzchołków drzewa może zostać przemapowane na ten sam wierzchołek naszego grafu**. Intuicyjnie odpowiada to wielu równoległym spacerom z tego samego punktu.

Formalniej można o tym myśleć jak o krotce

$$(T, \pi, \varphi)$$

gdzie T jest jakimś drzewem, π permutacją dzięki której mamy porządek dzieci, a φ funkcją mapującą wierzchołki tego drzewa na nasz graf, zgodnie z warunkiem który został tu opisany.

Bardzo chcielibyśmy umieć liczyć sobie, ile jest spacerów rozgałęziających się o danej długości, „zaczynających” się w danym wierzchołku. Okazuje się, że możemy to liczyć z pomocą programowania dynamicznego. Przed $dp[v][i]$ będziemy oznaczać liczbę spacerów rozgałęziających się „wychodzących” z wierzchołka v mających i krawędzi. Mamy, że:

$$dp[v][0] = 1$$

co jest dosyć oczywiste, bo skoro jest 0 krawędzi to ten spacer rozgałęziający się ma po prostu jeden wierzchołek i taki jest jeden. Dosyć prosto też zaobserwować, że

$$dp[v][1] = \deg(v)$$

Bo drzewo które będziemy chcieli zmapować na nasz graf będzie mieć 1 krawędź; tym samym jesteśmy w stanie zmapować jeden wierzchołek zawsze na wierzchołek v , a drugi na któregoś

z jego sąsiadów. Mało odkrywczą obserwacją i w sumie to bezużyteczną, bo wprost będzie wynikać ze wzoru który zostanie zaraz podany.

Twierdzenie 2.3.1 (Straszny wzór).

$$dp[u][i] = \sum_{v \in N(u)} \sum_{a+b=i-1} dp[u][a] \cdot dp[v][b] \quad (2.3)$$

Dowód. Tu trzeba by chyba było zacząć rysować, żeby to sensownie dowieść, ale generalnie chodzi o to że jak mamy drzewo i mapujemy je na nasz graf, to dziecko naszego korzenia (najbardziej na „lewo” jak rozpiszemy graficznie) w swoim poddrzewie ma jakieś a krawędzi, a cała reszta drzewa ma jakieś b krawędzi. Jak się to narysuje to widać, że $a + b = n - 1$, bo krawędź łącząca korzeń z lewym dzieckiem łączyła 2 rozpatrywane przez nas poddrzewa, które teraz rozpatrujemy osobno. Teraz liczba spacerów rozgałęziających się to po prostu suma po wszystkich możliwych wierzchołkach na które mapujemy tamto dziecko i możliwych wartościach a, b i iloczynach spacerów $dp[u][a]$ i $dp[v][b]$ czyli liczbach spacerów rozgałęziających się długości a z tego dziecka i długości b z całej reszty. Wartości te już mamy policzone, więc to jest poprawnie zdefiniowane. Obliczenie wszystkich możliwych tych wartości działa jakoś wielomianowo.



Rysunek 2.2: Przykłady podziału spaceru na dwie części.
Po lewej $a = 2, b = 5$, po prawej $a = 7, b = 0$

□

Z tego wzoru istotnie wynika wcześniejsza obserwacja, bo

$$dp[u][1] = \sum_{v \in N(u)} \sum_{a+b=0} dp[u][a] \cdot dp[v][b] = \sum_{v \in N(u)} dp[u][0] \cdot dp[v][0] = \sum_{v \in N(u)} 1 \cdot 1 = \deg(u)$$

Teraz zaczniemy używać motywów bardzo podobnych do tych występujących w problemie

zliczania liczby cykli Hamiltona w grafie. Mianowicie, przez U oznaczę sobie zbiór wszystkich spacerów rozgałęziających się, wychodzących z jakiegoś terminala t oraz mapujących dokładnie l krawędzi (innymi słowy, drzewo musi mieć l krawędzi, a funkcja przesyłająca musi przesyłać jego korzeń na t). Poza tym, zakładam że w grafie mam jakieś terminale t_1, t_2, \dots, t_k (gdy terminal jest tylko jeden, problem znalezienia drzewa Steinera jest dosyć trywialny). Przez A_i oznaczam zbiór wszystkich spacerów rozgałęziających się z U , które mapują jakiś wierzchołek drzewa na terminal t_i .

Zauważmy, że $\bigcap_{i \in [k]} A_i$ da nam zbiór wszystkich spacerów rozgałęziających się, które można „przerobić” do postaci drzewa łączącego wszystkie terminale, a więc jeśli jest niepusty to znaczy to, że istnieje drzewo łączące wszystkie terminale mające l krawędzi (lub mniej, ale to nam w tym problemie nie przeszkadza; chcemy wiedzieć czy istnieje drzewo łączące wszystkie terminale, mające maksymalnie l krawędzi).

Ponadto, żeby żyło się prościej, wprowadzam oznaczenie $S_i = U - A_i$. Innymi słowy, S_i to zbiór wszystkich spacerów rozgałęziających się z U , które nie mapują niczego na t_i . Wykonuję teraz przekształcenia podobne do tych, które robiliśmy przy cyklach Hamiltona:

$$\left| \bigcap_{i \in [k]} A_i \right| = |U| - \left| \bigcup_{i \in [k]} U \setminus A_i \right| = |U| - \left| \bigcup_{i \in [k]} S_i \right|$$

$$|U| - \left| \bigcup_{i \in [k]} S_i \right| = |U| - \sum_{\emptyset \neq X \subset [k]} (-1)^{|X|-1} \cdot \left| \bigcap_{i \in X} S_i \right|$$

Zasadniczo teraz mamy już skończony algorytm obliczania, bo:

1. $|U|$ jesteśmy w stanie obliczyć w czasie wielomianowym, bo to po prostu $dp[t][l]$
2. $\left| \bigcap_{i \in X} S_i \right|$ dla danego X również obliczamy w czasie wielomianowym, bo to jest $dp[t][l]$ ale policzone dla grafu indukowanego bez wierzchołków, po których iterujemy się idąc przez X . Innymi słowy, zbiór $S_{i_1} \cap S_{i_2} \cap \dots \cap S_{i_j}$ jest to zbiór wszystkich spacerów rozgałęziających się w grafie $G[V \setminus \{t_{i_1}, t_{i_2}, \dots, t_{i_j}\}]$.

Rozdział 3

Teoria liczb

3.1 Algorytm Euklidesa i tożsamość Bezouta

Definicja 3.1.1 (Notacja). Niech $a, b \in \mathbb{Z}$. Mówimy, że:

1. a jest podzielne przez b jeżeli istnieje $k \in \mathbb{Z}$ spełniające $a \cdot k = b$. Równoważnie mówimy, że b jest dzielnikiem a , i oznaczamy tę relację jako $a \mid b$, a jej negację przez $a \nmid b$.
2. liczba c jest *wspólnym dzielnikiem* a, b jeżeli $c \mid a$ oraz $c \mid b$. Przez $\gcd(a, b)$ oznaczamy *największy wspólny dzielnik* liczb a, b , tj. największe $k \in \mathbb{N}$ spełniające $k \mid a$ oraz $k \mid b$.
3. a jest *względnie pierwsze* z b jeżeli $\gcd(a, b) = 1$. Oznaczamy to równoważnie przez $a \perp b$.

Fakt 3.1.1. Niech $a, b, c, d \in \mathbb{N}$ i $d \mid a, d \mid b$. Zachodzi:

1. $d \mid -a$
2. $d \mid a + b$
3. $d \mid a \cdot c$
4. $d \mid \gcd(a, b)$
5. $a \mid c \implies d \mid c$
6. $c \mid \gcd(a, b) \iff c \mid a \wedge c \mid b$

Twierdzenie 3.1.1 (Algorytm Euklidesa). Niech $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{N}$ będzie funkcją zdefiniowaną rekurencyjnie jako:

$$f(a, b) = \begin{cases} a & \text{gdy } b = 0 \\ f(b, a \bmod b) & \text{wpp.} \end{cases}$$

Zachodzi $f = \gcd$.¹

¹Na liczby całkowite \gcd rozszerzamy biorąc $\gcd(a, b) = \gcd(|a|, |b|)$.

Dowód. Zauważmy, że $\gcd(a, 0) = a$ ponieważ dla każdego a istnieje $k = 0$ spełniające $a \cdot k = 0$, czyli 0 jest podzielne przez wszystkie liczby naturalne. Dowodzi to przypadkowi bazowemu rekurencji. Wiemy, że $a \bmod b = a - k \cdot b$ dla pewnego $k \in \mathbb{N}$ – ale z poprzednich faktów możemy wywnioskować, że d jest wspólnym dzielnikiem a, b wtedy i tylko wtedy, gdy jest wspólnym dzielnikiem $b, a \bmod b$, co kończy dowód. \square

Twierdzenie 3.1.2 (Tożsamość Bezouta). Niech $a, b \in \mathbb{Z}$ i $d = \gcd(a, b)$. Istnieje nieskończenie wiele par liczb $x, y \in \mathbb{Z}$ takich, że $a \cdot x + b \cdot y = d$. Liczby x, y nazywa się *współczynnikami Bezouta*.

Dowód. Zauważmy, że mając jedno rozwiązanie x, y możemy otrzymać ich nieskończenie wiele – wystarczy wziąć zbiór $\{(x + bk, y - ak) : k \in \mathbb{Z}\}$. Pokażemy więc istnienie jednego rozwiązania – co więcej, pokażemy efektywny algorytm jego otrzymywania.

Zmodyfikujemy nieco w tym celu algorytm Euklidesa – zamiast zwracać jednej liczby będzie zwracał ich trójkę. Wynikiem $f(a, b)$ będzie trójka (d, s, t) spełniająca warunki $d = \gcd(a, b)$ oraz $a \cdot s + b \cdot t = d$. Dla przypadku bazowego $b = 0$ łatwo zauważyć, że działa trójka $(a, 1, 0)$, bo $d = a = a \cdot 1 + b \cdot 0$. Odrobinę trudniej jest dla przypadku rekurencyjnego. Niech (d', s', t') to wartości wywołania funkcji $f(b, a \bmod b)$. Oczywiście $d = d'$, ale ciężiej podejść do wartości s, t . Aby to zrobić potrzebujemy skorzystać z pomocy brata operacji modulo – dzielenia bez reszty². Niech $q = \lfloor \frac{a}{b} \rfloor$. Z definicji wiemy, że $q \cdot b + a \bmod b = a$. Ale to oznacza, że:

$$\begin{aligned} d &= b \cdot s' + (a \bmod b) \cdot t' \\ &= b \cdot s' + (a - q \cdot b) \cdot t' \\ &= a \cdot t' + b \cdot (s' - q \cdot t'), \end{aligned}$$

co daje nam wzór na $s = t'$ i $t = s - q \cdot t'$.

Nasza końcowa funkcja wygląda więc następująco:

$$f(a, b) = \begin{cases} (a, 1, 0) & \text{gdy } b = 0 \\ (d, t, s - t * q) & \text{wpp, gdzie } q = \lfloor \frac{a}{b} \rfloor, (d, s, t) = f(b, a \bmod b) \end{cases}$$

Powyższy algorytm obliczania współczynników Bezouta nazywa się *rozszerzonym algorytmem Euklidesa*. \square

Wniosek 3.1.1. Dla dowolnego $a, b \in \mathbb{N}$, $d = \gcd(a, b)$ zachodzi:

$$\{a \cdot x + b \cdot y : x, y \in \mathbb{Z}\} = \{d \cdot k : k \in \mathbb{Z}\}.$$

²Zwykle idą w parze jako dzielenie z resztą, lecz dla uproszczenia nie wprowadziliśmy go przy podstawowym algorytmie Euklidesa

3.2 Fundamentalne twierdzenie arytmetyki

Definicja 3.2.1 (Liczby pierwsze). Mówimy, że liczba $p \in \mathbb{N}$ jest *pierwsza*, jeżeli $|\{k \in \mathbb{N} : k \mid p\}| = 2$. Równoważnie, liczba p jest pierwsza jeżeli $p \neq 1$ oraz $\{k \in \mathbb{N} : k \mid p\} = \{1, p\}$. Zbiór wszystkich liczb pierwszych oznaczamy \mathbb{P} .

Twierdzenie 3.2.1 (Fundamentalne twierdzenie arytmetyki). Niech $n \in \mathbb{N}_1$. Istnieje dokładnie jeden multizbiór liczb pierwszych $\mathcal{S} \subset \mathbb{P}$ spełniający $\prod \mathcal{S} = n$. Ten multizbiór nazywamy *rozkładem* n na czynniki pierwsze.

Dowód istnienia. Najpierw udowodnimy istnienie, przez indukcję po n . Dla $n = 1$ możemy wziąć $\mathcal{S} = \emptyset$, więc bazę indukcji mamy załatwioną. Jeżeli $n \in \mathbb{P}$ możemy wziąć $\mathcal{S} = \{n\}$ i analogicznie dostać odpowiedź. Niech $n \notin \mathbb{P}$. Z definicji liczb pierwszych istnieją a, k spełniające $a \cdot k = n$ i $a \notin \{1, p\}$. Ale to oznacza, że $a, k < p$, czyli z indukcji istnieją multizbiory A, K spełniające $a = \prod A, k = \prod K \implies n = \prod(A \cup K)$, co kończy dowód. \square

Aby wykazać unikalność takiego rozkładu udowodnimy najpierw pomocniczy lemat:

Lemat 3.2.1 (Lemat Euklidesa). Niech $p \in \mathbb{P}$ i $a, b \in \mathbb{N}_1$, oraz $p \mid ab$. Wtedy $p \mid a$ lub $p \mid b$.

Dowód lematu. Jeżeli $p \mid a$ to oczywiście mamy spełnioną tezę. Załóżmy więc, że $p \nmid a$. Ale to oznacza, że $\gcd(p, a) = 1$ (jest to jedyny inny dzielnik p). Z tożsamości Bezouta istnieją x, y spełniające $ax + py = 1$. Mnożąc stronami przez b otrzymujemy $axb + pyb = b$. Ale $p \mid ab \implies p \mid axb \implies p \mid axb + pyb$, co dowodzi $p \mid b$ i kończy dowód. \square

Dowód unikalności. Mając ten lemat możemy przystąpić do dowodu nie wprost. Załóżmy, że istnieje liczba o dwóch różnych rozkładach na czynniki pierwsze. Niech n będzie najmniejszą taką liczbą, a \mathcal{S}, \mathcal{T} będą jej rozkładami. Oczywiście $n \neq 1 \implies \mathcal{S}, \mathcal{T} \neq \emptyset$. Niech $p \in \mathcal{S}$ będzie dowolną liczbą pierwszą z \mathcal{S} . Z lematu Euklidesa i równości $\prod \mathcal{S} = \prod \mathcal{T}$ wiemy, że istnieje $q \in \mathcal{T}$ takie, że $p \mid q$. Ale ponieważ $p, q \in \mathbb{P}$ musi zachodzić $p = q$. Oznacza to, że zachodzi $\prod(\mathcal{S} \setminus p) = \prod(\mathcal{T} \setminus p)$, co wraz z faktem, że $p \geq 2$ pokazuje istnienie mniejszego n o nieunikalnym rozkładzie, co jest sprzeczne z założeniem o minimalności i kończy dowód. \square

3.3 Chińskie twierdzenie o resztach

Twierdzenie 3.3.1 (Chińskie twierdzenie o resztach). Niech $n, m \in \mathbb{N}_1, n \perp m, a \in [n]_0, b \in [m]_0$. Wtedy istnieje dokładnie jedno $x \in [nm]_0$ spełniające układ kongruencji:

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

Dowód unikalności. Załóżmy, że istnieją $x, y \in [nm]_0$ obydwa spełniające układ równań. Niech $z = x - y$. Zachodzi:

$$\begin{cases} x - y \equiv a - a \equiv 0 \pmod{n}, \\ x - y \equiv b - b \equiv 0 \pmod{m}, \end{cases}$$

czyli $n \mid z, m \mid z \implies nm \mid z$. Ale to oznacza, że $z = 0$, bo analizując możliwe wartości otrzymujemy, że $z \in \{-nm + 1, \dots, nm - 1\}$, a 0 jest jedyną liczbą podzielną przez nm w tym przedziale. Czyli $x - y = 0 \implies x = y$. \square

Dowód istnienia „ala MFT”. Niech $f : [nm]_0 \ni x \mapsto (x \bmod n, x \bmod m) \in [n]_0 \times [m]_0$. Z dowodu unikalności wiemy, że ta funkcja jest injekcją – ale ponieważ $|[nm]_0| = nm = |[n]_0 \times [m]_0|$, funkcja f musi być również surjektywna (inaczej moc by się nie zgadzała). \square

Dowód istnienia przez konstrukcję. Wiemy, że $n \perp m$, czyli z tożsamości Bezouta istnieją k, l spełniające $n \cdot k + m \cdot l = 1$. Niech $x = m \cdot l \cdot a + n \cdot k \cdot b \pmod{nm}$. Wtedy zachodzi:

$$\begin{aligned} x &= m \cdot l \cdot a + n \cdot k \cdot b && \pmod{n} \\ &\equiv (1 - n \cdot k) \cdot a + 0 && \pmod{n} \\ &\equiv 1 \cdot a \equiv a && \pmod{n}; \\ x &= m \cdot l \cdot a + n \cdot k \cdot b && \pmod{m} \\ &\equiv 0 + (1 - m \cdot l) \cdot b && \pmod{m} \\ &\equiv 1 \cdot b \equiv b && \pmod{m}, \end{aligned}$$

czyli x jest poprawnym rozwiązaniem układu równań, co kończy dowód. \square

Wniosek 3.3.1. Niech $n_1, n_2, \dots, n_k \in \mathbb{N}_k$ będą parami względnie pierwsze, a $a_i \in [n_i]$ dla każdego i . Wtedy istnieje dokładnie jedno $x \in [\prod_{i=1}^k n_i]$ spełniające układ kongruencji:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Dowód. Aplikujemy chińskie twierdzenie o resztach $k - 1$ razy, najpierw dla n_1 i n_2 , potem dla $n_1 n_2$ i n_3 , itd. \square

3.4 Funkcja φ Eulera

3.4.1 Definicja funkcji φ

Definicja 3.4.1. Niech $n \in \mathbb{N}_1$. Przez \mathbb{Z}_n^* oznaczamy zbiór $\{x \in \mathbb{Z} : 1 \leq x \leq n, x \perp n\}$.

Funkcję φ (czasami nazywaną funkcją „tocjent” Eulera) definiujemy jako $\varphi(n) = |\mathbb{Z}_n^*|$, czyli ilość liczb naturalnych mniejszych i względnie pierwszych z n .

Twierdzenie 3.4.1. Zbiór \mathbb{Z}_n^* z mnożeniem modulo n jest grupą.

Dowód. Dla przejrzystości, mnożenie modulo n oznaczmy przez \circ , a mnożenie w pierścieniu liczb całkowitych przez \cdot .

Aksjomat łączności przechodzi bezpośrednio z pierścienia liczb całkowitych (branie reszty z dzielenia przez n nie zmienia tej własności).

Oczywiście 1 jest elementem neutralnym mnożenia oraz należy do \mathbb{Z}_n^* dla każdego n .

Grupa jest również zamknięta na mnożenie – założmy nie wprost, że $a, b \in \mathbb{Z}_n^*$, ale $a \circ b \notin \mathbb{Z}_n^*$. Oznacza to, że istnieje jakiś dzielnik pierwszy p , że $p \mid n$ oraz $p \mid a \circ b$. Z definicji mnożenia modulo wiemy, że $a \circ b = a \cdot b - n \cdot k$ dla pewnego $k \in \mathbb{N}$, czyli $a \circ b + n \cdot k = a \cdot b$. Ale ponieważ p dzieli lewą stronę równania, musi również dzielić prawą. Z lematu Euklidesa (patrz. fundamentalne twierdzenie arytmetyki) wynika, że $p \mid a$ lub $p \mid b$, a ponieważ $p \mid n$ jest to sprzeczne z założeniem $a, b \in \mathbb{Z}_n^*$.

Pozostało wykazać jedynie istnienie odwrotności. Niech $a \in \mathbb{Z}_n^*$. Ponieważ $\gcd(a, n) = 1$, z tożsamości Bezouta istnieją x, y spełniające:

$$a \cdot x + n \cdot y = 1.$$

Jak przyjrzymy się wystarczająco długo, to widzimy, że z definicji mnożenia modulo wynika $x \equiv a^{-1} \pmod{n}$. Oczywiście $x \perp n$ bo dla dowolnej liczby d dzielącej x oraz n zachodzi $d \mid 1 \implies d = 1$ (możemy wyjąć d przed nawias w tożsamości). \square

3.4.2 Twierdzenie Eulera

Twierdzenie 3.4.2. Dla dowolnego $a \perp n$ zachodzi $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Niech $a = n \cdot k + b$, i $b \in \{0, 1, \dots, n-1\}$. Oczywiście zachodzi $a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{n}$ oraz $a \perp n \implies b \perp n$. W takim razie zachodzi $b \in \mathbb{Z}_n^*$. Niech r będzie rzędem b w tej grupie. Z twierdzenia Lagrange’a wynika, że $r \mid \varphi(n)$, ponieważ $\varphi(n)$ to z definicji $|\mathbb{Z}_n^*|$, czyli $b^{\varphi(n)} \equiv (b^r)^d \equiv 1^d \equiv 1 \pmod{n}$, co kończy dowód. \square

3.4.3 Multiplikatywność funkcji φ

Definicja 3.4.2 (Funkcje multiplikatywne). Funkcję $f : \mathbb{N}_1 \rightarrow \mathbb{R}$ nazywamy *multiplikatywną*, jeżeli $f(1) = 1$ i dla dowolnych $n, m \in \mathbb{N}_1$ zachodzi:

$$n \perp m \implies f(n \cdot m) = f(n) \cdot f(m).$$

Twierdzenie 3.4.3. φ jest funkcją multiplikatywną.

Dowód. Oczywiście $\varphi(1) = |\{1\}| = 1$. Niech $n, m \in \mathbb{N}_1$ i $n \perp m$. Z definicji φ wiemy, że aby pokazać oczekiwaną równość wystarczy wykazać bijekcję z \mathbb{Z}_{nm}^* w $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Postawimy hipotezę, że funkcja $f : \mathbb{Z}_{nm}^* \ni x \mapsto (x \bmod n, x \bmod m) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ jest dobrze zdefiniowaną bijekcją. Dobra definicja wynika prosto z własności dzielenia – jeżeli $k \mid n$ to $k \mid nm$, czyli $\gcd(a, n) \neq 1 \implies \gcd(a, nm) \neq 1$. Z kontrapozycji dostajemy, że $\gcd(a, nm) = 1 \implies \gcd(a, n) = 1$, co wystarcza aby dowieść dobrze zdefiniowaną operację. Natomiast injektywność i surjektywność wynika bezpośrednio z chińskiego twierdzenia o resztach. Jeżeli istniałoby $x \neq y$ spełniające $(x \bmod n, x \bmod m) = (y \bmod n, y \bmod m)$, to otrzymujemy sprzeczność z (istniałyby dwa rozwiązania chińskiego twierdzenia o resztach w przedziale $[nm]_0$). Analogicznie, jeżeli mamy parę (a, b) to rozwiązując układ kongruencji znajdziemy odpowiedni element $x \in [nm]_0$ spełniający $(a, b) = (x \bmod n, x \bmod m)$ oraz $x \perp nm$.³ \square

Więcej o funkcjach multiplikatywnych opowiemy w sekcji *Splot Dirichleta*.

3.4.4 Wzór „jawny” na funkcję φ

Twierdzenie 3.4.4. Niech f będzie funkcją arytmetyczną, a $n \in \mathbb{N}_1$. Niech $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, gdzie $p_i \in \mathbb{P}$ oraz $i \neq j \implies p_i \neq p_j$ (wiemy, że taki rozkład zawsze istnieje z fundamentalnego twierdzenia arytmetyki). f jest multiplikatywna wtedy i tylko wtedy, gdy zachodzi:

$$f(n) = \prod_{i=1}^k f(p_i^{\alpha_i}).$$

Dowód. Obie implikacje są w miarę łatwe do zauważenia, poniżej udowodnimy mniej trywialną z nich.⁴ Załóżmy, że f jest multiplikatywna. Wykonamy indukcję po k . Dla $k = 0$ zachodzi $n = 1 \implies f(1) = \prod_{k=1}^0 = 1$. Inaczej niech $P = \prod_{i=1}^{k-1} p_i^{\alpha_i}$ – oczywiście $P \perp p_k^{\alpha_k}$. Z indukcji wiemy, że $f(P) = \prod_{i=1}^{k-1} f(p_i^{\alpha_i})$, a z multiplikatywności otrzymujemy $f(n) = f(P) \cdot f(p_k^{\alpha_k})$, co dowodzi oczekiwanej równości. \square

³Jeżeli istniałby nietrywialny wspólny dzielnik x, nm to z lematu Euklidesa musiałby dzielić n lub m , co byłoby sprzeczne z wyborem a, b

⁴Drugą implikację w sposób klasyczny dla podręczników matematycznych pozostawiamy czytelnikowi.

Wniosek 3.4.1. Niech $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, gdzie $p_i \in \mathbb{P}$ oraz $i \neq j \implies p_i \neq p_j$. Zachodzi:

$$\varphi(n) = \prod_{i=1}^k p_i^{\alpha_i-1} \cdot (p_i - 1) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

Dowód. Oczywiście $\varphi(1) = 1 = \prod_{i=1}^0 \dots$. Z poprzedniego twierdzenia wiemy, że wystarczy udowodnić równość $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ dla każdego $p \in \mathbb{P}$ – wtedy twierdzenie otrzymamy bezpośrednio z multiplikatywności φ .

Indukujemy się po α – dla $\alpha = 1$ zachodzi $\varphi(p) = p - 1$, ponieważ wszystkie mniejsze liczby naturalne są względnie pierwsze z p . Niech $\alpha \geq 2$: wtedy $\varphi(p^\alpha) = p \cdot \varphi(p^{\alpha-1})$, ponieważ wiemy, że tylko liczby postaci $x + kp^{\alpha-1}$, gdzie $k \in \{0, 1, \dots, p-1\}$ a $x \in \mathbb{Z}_{p^{\alpha-1}}^*$ będą względnie pierwsze z p . Jest tak ze względu na następujące równoważności:

$$x \perp p^{\alpha-1} \iff p \mid x \iff p \mid (x + p^{\alpha-1}).$$

Ale to oznacza, że $\varphi(p^\alpha) = p \cdot \varphi(p^{\alpha-1}) \stackrel{ind.}{=} p \cdot p^{\alpha-2}(p-1) = (p-1)p^{\alpha-1}$. □

3.5 Splot Dirichleta

Definicja 3.5.1 (Funkcje arytmetyczne). Mówimy, że funkcja f jest *arytmetyczna* jeżeli należy ona do zbioru $\mathbb{R}^{\mathbb{N}_1}$ (innymi słowy jest ona typu $\mathbb{N}_1 \rightarrow \mathbb{R}$).⁵

Definicja 3.5.2 (Splot Dirichleta). Niech f, g będą funkcjami arytmetycznymi. *Splotem Dirichleta* (oznaczanym $f * g$) nazywamy funkcję $h : \mathbb{N}_1 \rightarrow \mathbb{R}$ zdefiniowaną w następujący sposób:

$$h(n) = \sum_{d \mid n} f(d)g\left(\frac{n}{d}\right) = \sum_{\substack{ab=n \\ a>0}} f(a)g(b).⁶$$

Symbol $* : \mathbb{R}^{\mathbb{N}_1} \times \mathbb{R}^{\mathbb{N}_1} \rightarrow \mathbb{R}^{\mathbb{N}_1}$ nazywamy operatorem splotu Dirichleta.

Twierdzenie 3.5.1. Zbiór funkcji arytmetycznych $\mathbb{R}^{\mathbb{N}_1}$ wraz z operatorem $*$ splotu Dirichleta tworzy monoid przemienny (tj. półgrupę przemienną z el. neutralnym / grupę przemienną bez odwrotności). Monoid ten oznaczmy przez \mathbb{D} .⁷

Dowód. Zamknięcie na działania oraz przemienność są oczywiste z definicji $*$, więc wystarczy udowodnić łączność i istnienie elementu neutralnego.

⁵W literaturze definicja ta często zawiera zbiór liczb zespolonych jako przeciwdziedzinę (zamiast rzeczywistych), jednakże dla naszych celów jest to trochę przesada i pozwolimy sobie zawęzić tę definicję dla przejrzystości.

⁶Dla ułatwienia zapisu będę pomijał warunek $a > 0$ w dolnym indeksie (w tym kontekście operujemy na sumach liczb naturalnych, a nie całkowitych)

⁷Nie znaleźliśmy standardowego oznaczenia tej struktury, więc pozwolimy sobie na trochę dowolności w jego wprowadzeniu. Dla ciekawych warto zaznaczyć, że ten monoid można rozszerzyć do pierścienia jeżeli dodamy do niego operator dodawania funkcji po współrzędnych.

Najpierw udowodnimy łączność: niestety nie ma tutaj ładnego dowodu, jedynie dużo obliczeń:

$$\begin{aligned}
(f * (g * h))(n) &= \sum_{ab=n} f(a)(g * h)(b) \\
&= \sum_{ab=n} f(a) \left(\sum_{cd=b} g(c)h(d) \right) \\
&= \sum_{acd=n} f(a)g(c)h(d) \\
&= \sum_{ed=n} \left(\sum_{e=ac} f(a)g(c) \right) h(d) \\
&= \sum_{ed=n} (f * g)(e)h(d) \\
&= ((f * g) * h)(n)
\end{aligned}$$

Jak przeanalizujemy dokładnie własności sum i rozdzielność mnożenia względem dodawania, to otrzymamy że wszystkie powyższe przekształcenia były dozwolone.

Pozostało pokazać element neutralny, jednak po chwili zastanowienia możemy dojść do jego definicji – będzie to funkcja postaci $\mathcal{I}(n) = [n \stackrel{?}{=} 1]$ (tj. funkcja charakterystyczna jedynek). Aby to udowodnić wystarczy rozpisać definicję spłotu dla dowolnej funkcji f :

$$\begin{aligned}
(f * \mathcal{I})(n) &= \sum_{ab=n} f(a)\mathcal{I}(b) \\
&= f(n)\mathcal{I}(1) + \sum_{\substack{ab=n \\ b \neq 1}} f(a)\mathcal{I}(b) \\
&= f(n) \cdot 1 + \sum_{\substack{ab=n \\ b \neq 1}} f(a) \cdot 0 \\
&= f(n)
\end{aligned}$$

□

Twierdzenie 3.5.2 (Odwrotność Dirichleta). Niech $f \in \mathbb{R}^{\mathbb{N}_1}$. Zachodzi $f(1) \neq 0$ wtedy, i tylko wtedy, gdy istnieje $g \in \mathbb{R}^{\mathbb{N}_1}$ spełniające: $f * g = \mathcal{I}$. Funkcję g nazywamy *odwrotnością* f względem spłotu Dirichleta.

Dowód. Zauważmy, że jeżeli istnieje takie g to $(f * g)(1) \stackrel{\text{def.}}{=} f(1)g(1) = \mathcal{I}(1) = 1$, czyli musi zachodzić $g(1) = f(1)^{-1}$ oraz oczekiwana przez nas własność $f(1) \neq 0$.

Implikację w drugą stronę dowodzimy konstruując funkcję g indukcyjnie – jak ustaliliśmy zachodzi $g(1) = \frac{1}{f(1)}$. Rozważmy wartość g w punkcie $n \neq 1$ – wiemy, że:

$$(f * g)(n) = 0 = \sum_{ab=n} f(a)g(b) = g(n)f(1) + \sum_{\substack{ab=n \\ b \neq n}} f(a)g(b),$$

czyli:

$$g(n) = -\frac{\sum_{\substack{ab=n \\ b \neq n}} f(a)g(b)}{f(1)}.$$

Wartość ta jest dobrze zdefiniowana z indukcji, co dowodzi istnieniu g .

□

Wniosek 3.5.1. $\mathbb{D}_1 = \{f \in \mathbb{D} : f(1) \neq 0\}$ jest grupą przemenną.

Definicja 3.5.3 (Funkcje multiplikatywne; bis). Funkcję $f : \mathbb{N}_1 \rightarrow \mathbb{R}$ nazywamy *multiplikatywną*, jeżeli $f(1) = 1$ i dla dowolnych $n, m \in \mathbb{N}_1$ zachodzi:

$$n \perp m \implies f(n \cdot m) = f(n) \cdot f(m).$$

Zbiór wszystkich grup multiplikatywnych oznaczymy przez \mathbb{D}_* .

Twierdzenie 3.5.3. \mathbb{D}_* jest podgrupą⁸ grupy \mathbb{D}_1 . Równoważnie, jeżeli a, b są funkcjami multiplikatywnymi to $f * g$ oraz f^{-1} również są multiplikatywne.

Dowód. Najpierw udowodnimy multiplikatywność spłotu – niech f, g będą funkcjami multiplikatywnymi. Oczywiście $(f * g)(1) = f(1)g(1) = 1$. Niech $n, m \in \mathbb{N}_1, n \perp m$. Wtedy:

$$\begin{aligned} (f * g)(nm) & \quad \text{(definicja *)} \\ &= \sum_{xy=nm} f(x)g(y) \quad \text{(rozkład } x, y \text{ na dzielniki } n, m) \\ &= \sum_{\substack{ab=n \\ cd=m}} f(ac)g(bd) \quad \text{(multiplikatywność } f, g) \\ &= \sum_{\substack{ab=n \\ cd=m}} f(a)f(c)g(b)g(d) \quad \text{(zamiana kolejności)} \\ &= \sum_{\substack{ab=n \\ cd=m}} f(a)g(b)f(c)g(d) \quad \text{(własności sum)} \\ &= \sum_{ab=n} f(a)g(b) \cdot \sum_{cd=m} f(c)g(d) \quad \text{(definicja *)} \\ &= (f * g)(n) \cdot (f * g)(m) \end{aligned}$$

Multiplikatywność odwrotności dowodzimy analogicznie, lecz korzystając dodatkowo z indukcji i definicji odwrotności Dirichleta. Niech f będzie funkcją multiplikatywną, a $g = f^{-1}$. Z definicji odwrotności zachodzi $g(1) = 1$, oraz $g(k) = \sum_{\substack{ab=k \\ b \neq k}} f(a)g(b)$ dla $k \in \mathbb{N}_2$. Niech

⁸nawet normalną!

$n, m \in \mathbb{N}_1, n \perp m$ i $n, m \neq 1$. Wtedy:

$$\begin{aligned}
-g(nm) &= \sum_{\substack{xy=n \\ y \neq nm}} f(x)g(y) && \text{(definicja } f^{-1}) \\
&= \sum_{\substack{ab=n \\ cd=m \\ bd \neq nm}} f(ac)g(bd) && \text{(rozkład } x, y \text{ na dzielniki } n, m) \\
&= \sum_{\substack{ab=n \\ cd=m \\ bd \neq nm}} f(a)f(c)g(b)g(d) && \text{(multiplikatywność } f \text{ i } g \text{ z indukcji)} \\
&= \sum_{\substack{ab=n \\ cd=m \\ bd \neq nm}} f(a)g(b)f(c)g(d) && \text{(zamiana kolejności)} \\
&= \sum_{ab=n} f(a)g(b) \cdot \sum_{cd=m} f(c)g(d) - g(n)g(m) && \text{(zabawa sumami)} \\
&= (f * g)(n) \cdot (f * g)(m) - g(n)g(m) && \text{(definicja } *) \\
&= \mathcal{I}(n) \cdot \mathcal{I}(m) - g(n)g(m) && \text{(definicja } g = f^{-1}) \\
&= -g(n)g(m) && \text{(definicja } \mathcal{I})
\end{aligned}$$

□

3.6 Funkcja Möbiusa

3.6.1 Definicja i własności funkcji Möbiusa

Definicja 3.6.1 (Funkcja Möbiusa). Funkcją Möbiusa (oznaczaną μ) nazywamy funkcję zdefiniowaną w następujący sposób:

$$\mu(n) = \begin{cases} 1 & \text{gdy } n = 1 \\ 0 & \text{gdy istnieje } p \in \mathbb{P} : p^2 \mid n \\ (-1)^{|S|} & \text{wpp, gdzie } S \text{ to zbiór czynników pierwszych } n \end{cases}$$

Fakt 3.6.1. Funkcja μ jest multiplikatywna.

Dowód. Zauważmy, że z definicji wynika, że dla $p \in \mathbb{P}$ zachodzi $\mu(p^\alpha) = -[\alpha \stackrel{?}{=} 1]$. Z twierdzenia 3.4.4 wiemy, że aby f było multiplikatywne wystarczy wykazać, że $\mu(\prod_{i=1}^k p_i^{\alpha_i}) = \prod \mu(p_i^{\alpha_i})$ dla parami różnych liczb pierwszych p_i .

Niech $n = p_1^{\alpha_1} p_2^{\alpha_2} p_k^{\alpha_k}$. Jeżeli istnieje x takie, że $\alpha_x \geq 2$, to zachodzi

$$\mu(n) = 0 = \mu(p_x^{\alpha_x}) \cdot \prod_{\substack{i=1 \\ i \neq x}}^k p_i^{\alpha_i} = \prod_{i=1}^k \mu(p_i^{\alpha_i}).$$

Inaczej zachodzi

$$\mu(n) = (-1)^k = \prod_{i=1}^k (-1) = \prod_{i=1}^k \mu(p_i^{\alpha_i}).$$

Czyli zachodzi oczekiwana własność, co kończy dowód. \square

Twierdzenie 3.6.1. Niech funkcja K_1 będzie zdefiniowana jako $K_1(n) = 1$ (funkcja stała równa 1). Zachodzi $K_1 * \mu = \mathcal{I}$ (tj. μ jest odwrotnością Dirichleta funkcji K_1).

Dowód. Z twierdzenia 3.5.3 wiemy, że $K_1 * \mu$ jest multiplikatywne (K_1 jest trywialnie multiplikatywne). Wystarczy więc pokazać, że $(K_1 * \mu)(p^\alpha) = 0$ dla $\alpha > 1$, wtedy z 3.4.4 otrzymamy równość z \mathcal{I} . Co defakto kończy dowód, bo z definicji splotu otrzymujemy:

$$(K_1 * \mu)(p^\alpha) = \sum_{ab=p^\alpha} 1 \cdot \mu(b) = \mu(1) + \mu(p) = 1 - 1 = 0.$$

\square

3.6.2 Inwersja Möbiusa

Twierdzenie 3.6.2 (Inwersja Möbiusa). Niech f, g będą funkcjami arytmetycznymi. $g = \sum_{d|n} f(d) = (f * K_1)$ wtedy i tylko wtedy, gdy $f = (g * \mu)$.

Dowód.

$$\begin{aligned} f * K_1 &= g && \Longleftrightarrow \\ f * K_1 * \mu &= g * \mu && \Longleftrightarrow \\ f * \mathcal{I} &= g * \mu && \Longleftrightarrow \\ f &= g * \mu \end{aligned}$$

\square

3.6.3 Przykład zastosowania przy funkcji φ

Twierdzenie 3.6.3. Zachodzi $\varphi = \text{id} * \mu$, gdzie $\text{id}(x) = x$.

Dowód. W tym dowodzie założymy, że nie wiemy nic o multiplikatywności ani wzorze jawnym φ , jedynie o jego definicji jako moc zbioru liczb mniejszych i względnie pierwszych z n .

Niech $n \in \mathbb{N}_1$. Zauważmy, że definicja funkcji φ jest równoważna następującej funkcji:

$$\begin{aligned}
 \varphi(n) &= \sum_{a=1}^n \mathcal{I}(\gcd(a, n)) && \text{(Interpretacja definicji)} \\
 &= \sum_{a=1}^n \sum_{d|\gcd(a, n)} \mu(d) && \mathcal{I} = (K_1 * \mu) \\
 &= \sum_{a=1}^n \sum_{\substack{d|a \\ d|n}} \mu(d) && \text{(Własność gcd)} \\
 &= \sum_{d|n} \left(\mu(d) \cdot \sum_{\substack{a \in [n] \\ d|a}} 1 \right) && \text{(Zamiana kolejności)} \\
 &= \sum_{d|n} \mu(d) \cdot \frac{n}{d} && \text{(Interpretacja sumy)} \\
 &= (\mu * \text{id})(n) && \text{(Definicja *)}
 \end{aligned}$$

□

Wniosek 3.6.1. Zachodzi $n = K_1 * \varphi = \sum_{d|n} \phi(d)$ (z inwersji Möbiusa). Ponadto φ jest multiplikatywne (bo jest splotem dwóch funkcji multiplikatywnych).

Rozdział 4

Posety

Dla przypomnienia z MFI, posetem nazywamy parę (X, \preceq) , gdzie $\preceq \subset X \times X$ jest relacją zwrotną, przechodnią i antysymetryczną. Przez \mathbb{B}_n oznaczamy poset $(\mathcal{P}([n]), \subseteq)$.

4.1 Twierdzenie Dilwortha

Twierdzenie 4.1.1 (Twierdzenie Dilwortha). Długość maksymalnego antyłańcucha w posecie jest równa ilości łańcuchów w najmniejszym pokryciu łańcuchowym (tj. rozkładzie posetu na podzbiory będące łańcuchami). Długość tą dla danego posetu nazywamy szerokością i oznaczamy przez $\text{width}(P)$.

Dowód. Robimy indukcję po liczbie elementów posetu; gdy poset P składa się z jednego elementu, twierdzenie zachodzi w trywialny sposób. W dalszej części dowodu, pisząc P będziemy mieli na myśli zbiór, na którym zdefiniowany jest nasz poset (bo formalne poset to tupla).

Założmy teraz, że mamy poset zdefiniowany na n elementach. Wiemy, że jego antyłańcuch maksymalny ma długość k . Antyłańcuchów maksymalnych spełniających ten warunek nie musi być jeden; oznaczmy zbiór wszystkich antyłańcuchów maksymalnych w tym posecie jako A .

Zdefiniujmy teraz (dla danego antyłańcucha maksymalnego $\alpha \in A$) zbiory U_α i D_α , które będziemy określać odpowiednio jako *upset* i *downset* antyłańcucha α . Do zbioru U_α należą wszystkie elementy P , takie że są (ostro) większe od jakiegokolwiek elementu z α . Do zbioru D_α należą zaś wszystkie elementy P , takie że są mniejsze (ostro) od jakiegokolwiek elementu z α . Bardziej formalnie:

$$U_\alpha = \{x \in P \mid \exists_{y \in \alpha} y \leq x\} \setminus \alpha$$

$$D_\alpha = \{x \in P \mid \exists_{y \in \alpha} y \geq x\} \setminus \alpha$$

Pierwsza obserwacja którą należy wykonać, to taka że dla dowolnego $\alpha \in A$ jest tak, że $U_\alpha \cup D_\alpha \cup \alpha = P$. Jest to oczywiste; jeśli istniałby jakiś element z P który nie należałby ani do downsetu α , ani do upsetu α , ani do antyłańcucha maksymalnego α , to z faktu że nie należy ani

do downsetu ani do upsetu wynikałoby, że musiałby należeć do antylańcucha maksymalnego α (bo nie jest porównywalny z żadnym jego elementem).

Drua obserwacja: dla dowolnego $\alpha \in A$ nie istnieje element, który należy jednocześnie do U_α i D_α . Aby dowieść tę obserwację, załóżmy nie wprost, że istnieją jakieś $x, y, z \in P$ takie, że:

1. $y, z \in \alpha$
2. $x \geq y$
3. $x \leq z$

Wówczas otrzymujemy, że $y \leq x \leq z$, a więc z tranzytywności w posetach dostalibyśmy, że $y \leq z$. To prowadziło do sprzeczności, bo założyliśmy że $y, z \in \alpha$, a więc znajdują się w jednym antylańcuchu (i nie mogą być porównywalne).

Udowodnimy teraz szybki lemacik.

Lemat 4.1.1. Następujące warunki są równoważne:

1. Antylańcuch maksymalny α jest taki, że $D_\alpha = \emptyset$;
2. Antylańcuch maksymalny α składa się **jedynie** ze wszystkich elementów minimalnych posetu P .

Dowód. 1. (1) \implies (2); stosujemy dowód nie wprost. Załóżmy, że istnieje taki antylańcuch maksymalny α , że $D_\alpha = \emptyset$, ale do α nie należy jakiś element minimalny z P^1 . Nazwijmy go x . Rozważmy zbiór $\alpha' = \alpha \cup \{x\}$. Jeśli α' jest antylańcuchem, to znaczy że α nie był antylańcuchem maksymalnym i otrzymujemy sprzeczność z założeniami. Jeśli α' nie jest antylańcuchem, to oznacza że istnieje jakieś $y \in \alpha$ takie, że $y \leq x$ lub $y \geq x$.

Nie może być tak, że $y \leq x$, bo x jest elementem minimalnym w P . Jeśli $y \geq x$, to z kolei mamy, że $x \in D_\alpha$, skąd otrzymujemy sprzeczność.

Należy tutaj dodać, że ten dowód nie wprost pokazał jedynie, że α w takim przypadku zawiera wszystkie elementy minimalne z P , ale nie pokazaliśmy że *nie należą do niego* inne elementy z P . Na szczęście, wiedząc że wszystkie elementy minimalne z P znajdują się w α , wiemy że jakkolwiek inny element nie może się tam znaleźć (bo skoro nie jest minimalny to jest porównywalny z jakimś minimum, a więc nie należy do antylańcucha). To już kończy dowód.

2. (2) \implies (1); element minimalny to taki, że nie istnieje element który byłby od niego mniejszy. Z definicji D_α musi zatem być tak, że $D_\alpha = \emptyset$.

□

¹Należy również uważać na to, że nie możemy w tym dowodzie założyć *czegokolwiek* o elementach w α – w szczególności *a priori* możliwe jest, że α zawiera jakieś elementy które nie są minimalne w P .

Niemal identycznym dowodem można posłużyć się, by dowieść następujący lemat:

Lemat 4.1.2. Następujące warunki są równoważne:

1. Antyłańcuch maksymalny α jest taki, że $U_\alpha = \emptyset$;
2. Antyłańcuch maksymalny α składa się **jedynie** ze wszystkich elementów maksymalnych posetu P .

Teraz musimy rozpatrzyć trzy przypadki:

1. $\exists_{\alpha \in A} U_\alpha = D_\alpha = \emptyset$

W tym przypadku istnieje antyłańcuch maksymalny, którego upset i downset są puste. Nietrudno pokazać, że jest to jedyny antyłańcuch maksymalny (ale to nie ma znaczenia dla dowodu). Co ma znaczenie dla dowodu to to, że wystarczy z każdego elementu tego antyłańcucha utworzyć jednoelementowy łańcuch zawierający tylko siebie samego. Jako że α ma k elementów, dostajemy podział P na k antyłańcuchów.

2. $\exists_{\alpha \in A} U_\alpha \neq \emptyset \wedge D_\alpha \neq \emptyset$

Rozpatruję sobie posety na zbiorach $B = A \cup U_\alpha$ i $C = A \cup D_\alpha$. Jako, że $U_\alpha \neq \emptyset$ i $D_\alpha \neq \emptyset$, to z pewnością $|B| < |P|$ i $|C| < |P|$. W takim razie, B i C z założenia indukcyjnego da się podzielić na k łańcuchów.

Ponadto, każdy element α (zarówno w pokryciu łańcuchowym zbioru B , jak i C) należy do łańcucha innego niż jakikolwiek inny element α , jako że 2 elementy z jednego antyłańcucha nie mogą znaleźć się w jednym łańcuchu. W dodatku, z definicji zbiorów U_α i D_α bezpośrednio wynika, że każdy element α jest elementem najmniejszym w odpowiednim łańcuchu z pokrycia łańcuchowego zbioru B , i elementem największym w odpowiednim łańcuchu ze zbioru C . W takim razie po prostu „sklejam” łańcuchy z B i C w danym elemencie z α i mam poprawne pokrycie łańcuchowe całego posetu P .

3. Przypadek przeciwny do dwóch wcześniejszych, tj. $\forall_{\alpha \in A} U_\alpha = \emptyset$ **ALBO** $D_\alpha = \emptyset$

Korzystając z lematów 4.1.1 i 4.1.2, wiemy, że dla każdego $\alpha \in A$ jest tak, że składa się (jedynie) ze wszystkich elementów maksymalnych lub ze wszystkich elementów minimalnych w P . Nawiasem mówiąc, to bezpośrednio implikuje, że w tym przypadku $|A| \leq 2$, ale nie jest to specjalnie ważne.

Weźmy z P takie x, y , że x jest elementem maksymalnym, a y jest elementem minimalnym w P , przy czym chcemy, by te dwa elementy były porównywalne (tzn. $x \geq y$). Taka para dwóch elementów szczęśliwie zawsze istnieje – jeśli w A istnieje antyłańcuch bez downsetu, to parę tę stanowi dowolne maksimum i jego świadek bycia w upsecie; analogicznie w dualnym przypadku. Rozważmy więc poset $P' = P \setminus \{x, y\}$. Zauważmy, że:

- $|P'| = |P| - 2$, co pozwala nam zastosować założenie indukcyjne;

- jako, że każde $\alpha \in A$ zawierało zbiór wszystkich elementów maksymalnych lub minimalnych P , wiemy że długość **wszystkich** antyłańcuchów maksymalnych zmniejszyła się o 1, a więc długość najdłuższego antyłańcucha wynosi $k - 1$.

To oznacza, że z założenia indukcyjnego P' możemy podzielić na $k - 1$ łańcuchów. Tak więc dodając do P' łańcuch $\{x, y\}$ otrzymujemy podział P na k łańcuchów, a to kończy dowód.

□

Alternatywny dowód. Ten dowód opiera się na twierdzeniu Kőniga. Niech (P, \preceq) będzie posetem. Łatwo zauważyć, że rozmiar największego antyłańcucha jest większy lub równy od najmniejszego rozkładu P na łańcuchy – elementy tego największego antyłańcucha muszą znaleźć się w parami różnych łańcuchach. Wystarczy więc udowodnić nierówność w drugą stronę – że jeżeli mamy *najmniejsze* pokrycie łańcuchowe, to rozmiar największego antyłańcucha jest większy lub równy od mocy tego pokrycia. Skonstruujmy graf dwudzielny $G = (P, P', E)$, gdzie P' to kopia elementów P (innymi słowy chcemy aby $V = P \sqcup P$, gdzie V to zbiór wszystkich wierzchołków grafu), a para $(u, v') \in E$ wtedy, i tylko wtedy, gdy $u \prec v$. Przez M oznaczmy pewne skojarzenie tego grafu. Zauważmy następujący fakt – istnieje „naturalna” bijekcja pomiędzy podziałami P na łańcuchy, a skojarzeniami w G . Mając podział R na łańcuchy możemy zdefiniować skojarzenie przez równoważność $(a, b') \in M$ wtw. a jest bezpośrednio przed b w jednym łańcuchu. Odwracając ten proces, mając pewne skojarzenie możemy uzyskać rozkład na łańcuchy ustalając, zaczynając podziału na jednoelementowe łańcuchy, a następnie dla każdego $(a, b') \in M$ łącząc łańcuchy (\dots, a) i (b, \dots) w (\dots, a, b, \dots) – łatwo wykazać, że zawsze a, b będą na końcach, tj. ta operacja jest poprawnie zdefiniowana. Co ciekawsze, z konstrukcji bijekcji łatwo zauważyć, że zachodzi równość $|R| = |P| - |M|$, bo dla każdej krawędzi skojarzenia „łączymy” dokładnie dwa łańcuchy (zmniejszając moc początkową $|P|$ o 1). Niech R będzie najmniejszym pokryciem łańcuchowym P , a M odpowiadającym mu skojarzeniem. Weźmy teraz najmniejsze pokrycie wierzchołkowe C grafu G , które z tw. Kőniga ma moc $|M|$. Definiujemy zbiór pomocniczy $D = \{x \in P : x \in C \text{ lub } x' \in C\}$ – z tej definicji wynika nierówność $|D| \leq |C|$. Ale zbiór $P \setminus D$ jest antyłańcuchem naszego posetu – ponieważ C było pokryciem wierzchołkowym, każde dwa elementy spoza D muszą nie mieć krawędzi między sobą w zdefiniowanym wcześniej grafie dwudzielnym, czyli przechodząc na posety są one parami nieporównywalne. Znaleźliśmy więc antyłańcuch o mocy $|P| - |D| \geq |P| - |C| = |P| - |M| = |R|$, co kończy dowód.

□

4.2 Twierdzenie dualne do Dilwortha

Twierdzenie 4.2.1 (Twierdzenie dualne do twierdzenia Dilwortha). Długość maksymalnego łańcucha w posecie wynosi Długość maksymalnego łańcucha w posecie jest równa ilości antyłańcuchów w najmniejszym pokryciu antyłańcuchowym (tj. rozkładzie posetu na podzbiory

będące antylańcuchami). Długość tę dla danego posetu nazywamy szerokością i oznaczamy $\text{height}(P)$.

Dowód. W jedną stronę nierówność jest trywialna – mając łańcuch o długości k , każdy z jego elementów musi trafić do innego antylańcucha. Dowodzimy więc nierówność w drugą stronę. Niech (P, \leq) będzie posetem – zdefiniujmy sobie funkcję φ idącą z elementów P w liczby naturalne, taką że $\varphi(x)$ jest to moc najdłuższego łańcucha w P , którego maksimum wynosi x . Zauważmy, że φ może przyjmować jedynie wartości w zakresie $1 \dots k$, bo k to długość najdłuższego łańcucha w ogóle. Zauważamy, że wszystkie elementy P które przechodzą na jakąś liczbę m muszą być ze sobą nieporównywalne, a więc formować antylańcuch. Gdyby tak nie było i istniałyby jakieś elementy x, y , takie że, bez straty ogólności, $x \leq y$ i $\varphi(x) = \varphi(y) = z$, to łańcuch w którym x jest elementem maksymalnym i który ma długość z możemy „rozszerzyć” dodając do niego y , które stałoby się nowym elementem maksymalnym; tym samym maksymalna długość łańcucha w którym y byłoby elementem maksymalnym wynosiłaby nie z , a $z+1$, co prowadziłoby do sprzeczności. W takim razie dla każdej liczby naturalnej w zakresie $1 \dots k$ mamy jakiś antylańcuch i wiemy, że te antylańcuchy w sumie muszą pokrywać cały poset P , co kończy dowód. \square

4.3 Lemat Erdősa-Szekeresa o podciągach monotonicznych

Twierdzenie 4.3.1 (Lemat Erdősa-Szekeresa o podciągach monotonicznych). W ciągu składającym się z $n \cdot m + 1$ liczb naturalnych ($n, m \leq 1$) znajduje się podciąg niemalejący długości co najmniej $n + 1$ lub nierosnący długości co najmniej $m + 1$.

Dowód. Zdefiniujmy sobie porządek częściowy na elementach ciągu. Mówimy, że $a \preceq b$, gdy b występuje później niż a w ciągu oraz $a \geq b$. Zauważmy, że łańcuch w tak zdefiniowanym posecie jest podciągiem nierosnącym naszego ciągu, zaś antylańcuch musi być podciągiem niemalejącym. Z twierdzenia dualnego do twierdzenia Dilwortha wnioskujemy, że w dowolnym posecie zachodzi $\text{width}(P) \cdot \text{height}(P) \geq |P|$. Prowadzi to nas już zasadniczo do tezy, którą możemy teraz dowieść nie wprost: założmy, że istnieje taki ciąg długości $n \cdot m + 1$, w którym każdy podciąg niemalejący ma długość maksymalnie n , a nierosnący ma długość maksymalnie m . Oznacza to, że najdłuższy łańcuch w naszym wcześniej zdefiniowanym posecie ma długość m , a antylańcuch długość n , skąd otrzymujemy że $n \cdot m \geq n \cdot m + 1$, co prowadzi nas do sprzeczności. \square

4.4 Nierówność LYM

Twierdzenie 4.4.1 (Nierówność LYM (Lubella, Yamamoto, Meshalkina)). Niech \mathcal{D} będzie antyłańcuchem kraty \mathbb{B}_n . Wtedy zachodzi:

$$\sum_{X \in \mathcal{D}} \frac{1}{\binom{n}{|X|}} \leq 1. \quad (4.1)$$

Alternatywnie, jeżeli f_n to liczba zbiorów o mocy n w \mathcal{D} , to twierdzenie można zapisać jako:

$$\sum_{i=0}^n \frac{f_n}{\binom{n}{i}} \leq 1. \quad (4.2)$$

Dowód. Dowód opierać się będzie na pewnej „dziwnej” funkcji $\nu : \mathbb{B}_n \rightarrow \mathcal{P}(S_n)$, gdzie S_n to zbiór wszystkich permutacji n -elementowych.² Naszą funkcję definiujemy w następujący sposób:

$$\nu(X) = \{\pi \in S_n : \{\pi(1), \pi(2), \dots, \pi(|X|)\} = X\},$$

czyli innymi słowy jest to zbiór wszystkich permutacji, których pierwsze $|X|$ elementów należy do X . Zauważmy teraz dwa ciekawe fakty:

1. $|\nu(X)| = |X| \cdot (n - |X|)$

Fakt ten wynika z prostego zliczania – łatwo zauważyć, że wszystkie permutacje w $\nu(X)$ są postaci

$$\pi = (\sigma(1), \sigma(2), \dots, \sigma_{|X|}, \rho(1), \rho(2), \dots, \rho(n - |X|)),$$

gdzie σ jest „permutacją” X (tj. bijekcją z $[|X|]$ na X), a ρ jest analogicznym ustawieniem elementów z $[n] \setminus X$. Z reguły mnożenia otrzymujemy więc moc zbioru $\nu(X)$.

2. $X \neq Y, \nu(X) \cap \nu(Y) \neq \emptyset \implies X, Y$ – porównywalne

Załóżmy BSO, że $|X| \leq |Y|$, i niech π będzie elementem świadczącym niepustości przecięcia, tj. $\pi \in \nu(X)$ oraz $\pi \in \nu(Y)$. Z definicji ν wiemy, że $X = \{\pi(1), \pi(2), \dots, \pi(|X|)\}$ oraz $Y = \{\pi(1), \pi(2), \dots, \pi(|Y|)\}$ – ale z tego oczywiście wynika, że $X \subset Y$. Z tej obserwacji możemy wywnioskować, że dla dowolnego antyłańcucha $\mathcal{D} \subset \mathbb{B}_n$ i $X, Y \in \mathcal{D}$, $X \neq Y$ zachodzi $\nu(X) \cap \nu(Y) = \emptyset$.

Czyli z drugiej obserwacji wynika, że $\bigsqcup_{X \in \mathcal{D}} \nu(X) \subset S_n$, bo każdej permutacji odpowiada co

²Dla fanów algebry jest to zbiór podkładowy grupy symetrycznej na zbiorze $[n]$.

najwyżej jeden zbiór z antylańcucha \mathcal{D} – wykonamy więc kilka transformacji:

$$\begin{aligned}
\bigcup_{X \in \mathcal{D}} \nu(X) &\subset S_n && \implies \\
\sum_{X \in \mathcal{D}} |\nu(X)| &\leq |S_n| && \iff \\
\sum_{X \in \mathcal{D}} |X| \cdot (n - |X|) &\leq n! && \iff \\
\sum_{X \in \mathcal{D}} \frac{|X| \cdot (n - |X|)}{n!} &\leq 1 && \iff \\
\sum_{X \in \mathcal{D}} \frac{1}{\binom{n}{|X|}} &\leq 1
\end{aligned}$$

□

4.5 Twierdzenie Spernera

Twierdzenie 4.5.1 (Twierdzenie Spernera). Najdłuższy antylańcuch \mathcal{D} w kracie zbiorów \mathbb{B}_n ma moc $\binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil}$.

Dowód przez nierówność LYM. Przedstawimy dowody dla $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ – dla sufitu są one analogiczne. Jesteśmy w stanie wskazać antylańcuch takiej długości – $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. Wystarczy pokazać więc, że nie istnieje dłuższy antylańcuch. Niech \mathcal{D} będzie antylańcuchem, wtedy:

$$\begin{aligned}
\forall_{0 \leq k \leq n} : \binom{n}{k} &\leq \binom{n}{\lfloor \frac{n}{2} \rfloor} && \implies \text{(tr. obserwacja)} \\
1 \geq \sum_{X \in \mathcal{D}} \frac{1}{\binom{n}{|X|}} &\geq \frac{|\mathcal{D}|}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} && \implies \text{(nier. LYM)} \\
\binom{n}{\lfloor \frac{n}{2} \rfloor} &\geq |\mathcal{D}| && \text{(mnożenie stronami)}
\end{aligned}$$

□

Definicja 4.5.1 (Łańcuchy symetryczne). Łańcuch C w \mathbb{B}_n nazywamy symetrycznym, jeśli $C = \{X_k, X_{k+1}, \dots, X_{n-k}\}$, gdzie $X_k \subset X_{k+1} \subset \dots \subset X_{n-k}$ oraz $|X_i| = i$ dla pewnego k . Taki łańcuch narysowany na kracie jest symetryczny względem środkowego poziomu.

Dowód tw. Spernera przez łańcuchy symetryczne. Rozważmy podział \mathbb{B}_n na łańcuchy symetryczne. Każdy taki łańcuch zawiera dokładnie jeden element ze środkowego poziomu (rozmiaru $\lfloor \frac{n}{2} \rfloor$), a więc podział ma $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ elementów. Z twierdzenia Dilwortha antylańcuch nie może mieć więcej niż tyle elementów. □

Niestety powyższy dowód nie jest jeszcze kompletny, bo nie wiemy jeszcze czy taki podział na łańcuchy symetryczne wogóle istnieje. Na szczęście właśnie to pokażemy

Definicja 4.6.1. Liczba Dedekinda D_n to liczba antylańcuchów w \mathbb{B}_n .

Twierdzenie 4.6.2 (Ograniczenie na liczby Dedekinda). Liczba Dedekinda D_n ograniczona jest nierównościami

$$2^{\lfloor \frac{n}{2} \rfloor} \leq D_n \leq 3^{\lfloor \frac{n}{2} \rfloor}.$$

Dowód. Dolne ograniczenie wynika z tego, że największy antylańcuch ma $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ elementów, a dowolny jego podzbiór jest antylańcuchem.

Pozostało wykazać ograniczenie górne. Wykorzystamy obserwację, że antylańcuchy można utożsamiać z ich stożkami dolnymi (zbiorami elementów, które są mniejsze lub równe elementom antylańcucha) – antylańcuch zadaje swój stożek dolny i można go odzyskać biorąc elementy maksymalne. Natomiast stożki dolne można utożsamiać z monotonicznymi funkcjami $\mathbb{B}_n \rightarrow \{0, 1\}$, które są dopełnieniami funkcji charakterystycznych tych zbiorów. Będziemy zliczać funkcje monotoniczne.

Rozważmy podział na łańcuchy symetryczne \mathcal{C} zadany przez konstrukcję z nawiasowaniem. Każdy łańcuch $C \in \mathcal{C}$ ma ustalone elementy sparowane, a zmieniają się elementy niesparowane. Dla $\{A_0, \dots, A_k\} \in \mathcal{C}$, gdzie $A_0 \subset \dots \subset A_k$ i $k \geq 2$, w zbiorze A_i i -ty niesparowany nawias jest ostatnim domkniętym. Dla $0 < i < k$ istnieje za nim nawias otwarty. Możemy obrócić te nawiasy i sparować je, tworząc zbiór B_i , który należy do pewnego krótszego łańcucha w \mathcal{C} (są w nim dwa nowe sparowane nawiasy). Zauważmy, że $A_{i-1} \subset B_i \subset A_{i+1}$ (do A_{i-1} nie należą oba elementy, które obróciliśmy, tworząc B_i , a do A_{i+1} należą).

Będziemy definiować funkcję monotoniczną f , zaczynając od najkrótszych łańcuchów w \mathcal{C} . Na tych długości co najwyżej 2 (istnieją, bo środkowe poziomy są większe od nieśrodkowych, więc łańcuchy zawierające coś z nieśrodkowych poziomów nie pokrywają środkowych) mamy maksymalnie 3 opcje (oba elementy dostają tę samą lub różne wartości). Rozważmy łańcuch $\{A_0, \dots, A_k\}$ i zbiór $\{B_1, \dots, B_{k-1}\}$ zbiorów otrzymanych z elementów łańcucha przez opisane wyżej przekształcenie. Funkcja f jest już na nich zdefiniowana. Jeśli $f(B_1) = 1$, to $f(A_2) = 1$ z monotoniczności i pozostaje nam wybór wartości na dwóch zbiorach z rozważanego łańcucha. Jeśli $f(B_{k-1}) = 0$, to $f(A_{k-2}) = 0$ z monotoniczności i ponownie pozostaje nam wybór wartości na dwóch zbiorach. Jeśli $f(B_1) = 0$ i $f(B_{k-1}) = 1$, to istnieje takie $i \in [k-2]$, że $f(B_i) = 0$ i $f(B_{i+1}) = 1$. Wtedy z monotoniczności $f(A_{i-1}) = 0$ i $f(A_{i+1}) = 1$, więc również zostały nam do wybrania dwie wartości. Zatem dla każdego z $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ łańcuchów mamy możliwość dokonania co najwyżej⁵ 3 wyborów, czyli razem mamy $3^{\lfloor \frac{n}{2} \rfloor}$ możliwości. \square

⁵Podczas konstrukcji może okazać się, że próbując ustalić dany łańcuch sprzeczne ze sobą ograniczenia – może się tak zdarzyć jeżeli istnieje kilka miejsc gdzie $B_i = 0, B_{i+1} = 1$. W takiej sytuacji wiemy, że taka funkcja nie istnieje, ale nie psuje to ograniczenia górnego.

4.7 Cienie i twierdzenie Erdősa-Ko-Rado

Definicja 4.7.1. Dla zbioru $\mathcal{B} \subset \binom{[n]}{k}$ jego cieniem dolnym nazywamy zbiór

$$\Delta\mathcal{B} = \{A : \exists B \in \mathcal{B}, x \in B \ A = B \setminus \{x\}\},$$

a cieniem górnym nazywamy zbiór

$$\nabla\mathcal{B} = \{A : \exists B \in \mathcal{B}, x \in [n] \setminus B \ A = B \cup \{x\}\}.$$

Elementy cienia odpowiednio tracą lub zyskują jeden element – cień jest obcięciem stożka do najbliższego poziomu.

Twierdzenie 4.7.1 (O rozmiarze cienia). Dla $\mathcal{B} \subset \binom{[n]}{k}$ zachodzą następujące nierówności:

$$\begin{aligned} |\Delta\mathcal{B}| &\geq \frac{k}{n-k+1} |\mathcal{B}|, \\ |\nabla\mathcal{B}| &\geq \frac{n-k}{k+1} |\mathcal{B}|. \end{aligned}$$

Z powyższego twierdzenia wynika, że $|\Delta\mathcal{B}| \geq |\mathcal{B}|$ dla $k \geq \frac{n+1}{2}$ oraz $|\nabla\mathcal{B}| \geq |\mathcal{B}|$ dla $k \leq \frac{n-1}{2}$.

Dowód. Zliczamy moc zbioru $W = \{(A, B) : B \in \mathcal{B}, A \in \Delta\mathcal{B}, A \subset B\}$. Jest ona równa $k|\mathcal{B}|$, bo każdy element \mathcal{B} ma dokładnie k swoich elementów cienia. Jednocześnie każdy element cienia może mieć co najwyżej $n - (k - 1)$ swoich nadzbiorów w \mathcal{B} , więc $|W| \leq |\Delta\mathcal{B}|(n - k + 1)$, co dowodzi pierwszej nierówności. Analogiczne zliczenie dla górnego cienia (każdy element \mathcal{B} ma $n - k$ swoich elementów cienia, element cienia ma co najwyżej $k + 1$ elementów \mathcal{B}) daje drugą nierówność. \square

Twierdzenie 4.7.2 (Twierdzenie Spernera, bis). Największy antyłańcuch w \mathbb{B}_n ma rozmiar $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Dowód przez cienie. Niech \mathcal{A} będzie antyłańcuchem w \mathbb{B}_n i niech $\mathcal{A}_j = \mathcal{A} \cap \binom{[n]}{j}$. Jeśli $i = \min\{j : \mathcal{A}_j \neq \emptyset\}$, to dla $i \leq \frac{n-1}{2}$ zbiór $\mathcal{A}' = (\mathcal{A} \setminus \mathcal{A}_i) \cup \nabla\mathcal{A}_i$ ma większą moc od \mathcal{A} oraz dalej jest antyłańcuchem – jeśli coś jest nad cieniem górnym \mathcal{A}_i , to jest też nad \mathcal{A}_i , więc \mathcal{A} nie byłby antyłańcuchem. Podobnie, jeśli weźmiemy $k = \max\{j : \mathcal{A}_j \neq \emptyset\}$ i będzie $k \geq \frac{n+1}{2}$. Możemy więc po kolei przesuwając kolejne poziomy bliżej środka kraty. Jeśli $2 \nmid n$, to możemy wybrać dowolny ze środkowych poziomów, bo nierówności z cieniami na to pozwalają. \square

Definicja 4.7.2. Rodzina zbiorów \mathcal{F} jest przecinająca się, jeśli $\forall X, Y \in \mathcal{F} \ X \cap Y \neq \emptyset$.

Twierdzenie 4.7.3. Największa rodzina przecinająca się w \mathbb{B}_n ma rozmiar 2^{n-1} .

Dowód. Zauważmy, że dla rodziny przecinającej \mathcal{F} nie może jednocześnie zachodzić $X \in \mathcal{F}$ i $\bar{X} \in \mathcal{F}$. Zatem jest $|\mathcal{F}| \leq 2^{n-1}$. Przykładem takiej rodziny mogą być wszystkie podzbiory \mathbb{B}_n zawierające 1. \square

Twierdzenie 4.7.4 (Erdős-Ko-Rado). Niech $\mathcal{F} \subseteq \binom{[n]}{k}$ będzie przecinająca się i niech $2k \leq n$. Maksymalny rozmiar \mathcal{F} to $\binom{n-1}{k-1}$.

Dowód. Najpierw zauważmy, że dla $2k > n$ można wziąć $\mathcal{F} = \binom{[n]}{k}$, bo wszystkie takie zbiory muszą się przecinać.

Faktyczny dowód zaczniemy, rozważając cykl σ elementów $[n]$ (tj. permutację o jednym cyklu). Przedziałem k -elementowym w σ nazwiemy ciąg k elementów występujących kolejno w σ , być może zapętłając się modulo n . Pokażemy, że do \mathcal{F} może należeć co najwyżej k przedziałów dla każdego takiego cyklu σ . Załóżmy, że $X = \{x_1, \dots, x_k\} \in \mathcal{F}$ jest przedziałem w σ . Zauważmy, że pary przedziałów, z których jeden ma prawy koniec w x_i , a drugi ma lewy koniec w x_{i+1} dla $i \in [k]$ są jedynymi przedziałami, które mogą należeć do \mathcal{F} i co najwyżej jeden z każdej pary należy do \mathcal{F} (bo muszą się wzajemnie przecinać i przecinać X , a warunek $2k \leq n$ zapewnia, że nie przetną się „z drugiej strony”). Zatem zbiór $W = \{(X, \sigma) : X \in \mathcal{F}, \sigma \text{ cyklem w } [n], X \text{ przedziałem w } \sigma\}$ ma co najwyżej $k(n-1)!$ elementów (po k na każdy cykl, a cykliów jest $(n-1)!$). Jednocześnie każdy zbiór z \mathcal{F} można dopełnić do cyklu, stawiając go na początku cyklu i permutując jego elementy i pozostałe elementy, co daje nam $|W| = |\mathcal{F}|k!(n-k)!$, zatem $|\mathcal{F}| \leq \frac{k(n-1)!}{k!(n-k)!} = \binom{n-1}{k-1}$.

Aby znaleźć rodzinę spełniającą to ograniczenie, można wziąć wszystkie elementy z $\binom{[n-1]}{k-1}$ z dorzuconym elementem n . \square

4.8 Twierdzenie Kruskala-Katony/Lovása

Twierdzenie 4.8.1 (k -kaskadowa reprezentacja liczb naturalnych). Niech $m, k \in \mathbb{N}_1$. Istnieją takie liczby $a_k > a_{k-1} > \dots > a_s \geq s \geq 1$, że

$$m = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \dots + \binom{a_s}{s},$$

a ponadto taka reprezentacja jest jedyna.

Dowód. Istnienie dowodzimy indukując się po (k, m) , dla $k = 1$ mamy $m = \binom{m}{1}$, dla $m = 1$ mamy $m = \binom{k}{k}$. W kroku indukcyjnym niech $a_k = \max\{a : \binom{a}{k} \leq m\}$, mamy $m = \binom{a_k}{k} + m'$, a m' z indukcji ma $(k-1)$ -kaskadową reprezentację (lub jest równe 0, co kończy konstrukcję), w której jest $a_{k-1} < a_k$, bo inaczej $m \geq \binom{a_k}{k} + \binom{a_k}{k-1} = \binom{a_k+1}{k}$ wbrew definicji a_k .

Założmy nie wprost, że taka reprezentacja nie jest jedyna, a m jest minimalnym przykładem tego. Wtedy $m = \binom{a_k}{k} + \dots + \binom{a_s}{s} = \binom{a'_k}{k} + \dots + \binom{a'_{s'}}{s'}$ i $a_k \neq a'_k$ (inaczej można odjąć te same

czynniki i otrzymać mniejszy kontrprzykład). Bez straty ogólności $a_k > a'_k$. Wtedy jednak $\binom{a'_k}{k} + \dots + \binom{a'_{s'}}{s'} \leq \binom{a_k-1}{k} + \binom{a_k-2}{k-1} + \dots + \binom{a_k-k}{1} < \binom{a_k}{k} \leq m$, co daje sprzeczność (druga nierówność wynika z tożsamości dwumianów $\sum_{i=0}^k \binom{n-1+i}{i} = \binom{n+k}{k}$). \square

Definicja 4.8.1 (Porządek „colex”). Na zbiorze $\binom{\mathbb{N}}{k}$ definiujemy porządek koleksykograficzny: dla $A, B \in \binom{\mathbb{N}}{k}$ jest $A <_{\text{col}} B$ wtedy i tylko wtedy, gdy $\max(A \div B) \in B$. Oznacza to, że o porządku „colex” decyduje ostatni (największy) różniący się element (a nie jak w porządku leksykograficznym najmniejszy, stąd nazwa).

Twierdzenie 4.8.2 (Twierdzenie Kruskala-Katony). Niech $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ i $|\mathcal{F}| = m = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \dots + \binom{a_s}{s}$. Wtedy

$$|\Delta\mathcal{F}| \geq \binom{a_k}{k-1} + \binom{a_{k-1}}{k-2} + \dots + \binom{a_s}{s-1}.$$

Co więcej, takie ograniczenie jest najlepsze możliwe.

Dowód. Najpierw pokażemy, że istnieje rodzina spełniająca to ograniczenie. Weźmy rodzinę $\mathcal{C}(m, k)$ pierwszych m elementów z $\binom{\mathbb{N}}{k}$ w porządku koleksykograficznym. Mając zadaną k -kaskadową reprezentację m widzimy, że $\mathcal{C}(m, k)$ składa się z $\binom{[a_k]}{k}$, zbiorów powstałych przez dodanie $\{a_k + 1\}$ do $\binom{[a_k-1]}{k-1}$, dodanie $\{a_k + 1, a_{k-1} + 1\}$ do $\binom{[a_k-2]}{k-2}$ i tak dalej, aż do zbiorów powstałych przez dodanie $\{a_k + 1, \dots, a_{s+1} + 1\}$ do $\binom{[a_s]}{s}$ – bierzemy tyle ile się da na najmniejszym możliwym zbiorze, potem zostają nam zbiory, w których jest liczba o jeden większa i rekurencyjnie bierzemy mniejsze zbiory. Cień takiej rodziny składa się z $\binom{[a_k]}{k-1}$, zbiorów powstałych przez dodanie $\{a_k + 1\}$ do $\binom{[a_k-1]}{k-2}$, dodanie $\{a_k + 1, a_{k-1} + 1\}$ do $\binom{[a_k-2]}{k-3}$ i tak dalej, aż do zbiorów powstałych przez dodanie $\{a_k + 1, \dots, a_{s+1} + 1\}$ do $\binom{[a_s]}{s-1}$ – biorąc cień kolejnych z tych zbiorów usunięcie któregoś z wyróżnionych elementów da nam jeden z otrzymanych wcześniej zbiorów, wszystkie inne dadzą coś nowego. To daje nam poszukiwaną wielkość cienia.

Pokazanie, że osiągnięta wartość jest faktycznie najmniejsza, przebiega identycznie jak dowód twierdzenia Lovásza (który zaraz pokażemy), z tym, że trzeba wielokrotnie stosować rekurencyjny wzór na współczynniki dwumianowe. \square

Definicja 4.8.2. Niech $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ dla pewnego $k \geq 1$ oraz ustalmy $i \geq 2$. Operator przesunięcia S_i tworzy nową rodzinę $S_i(\mathcal{F}) = \{S_i(F) : F \in \mathcal{F}\}$, gdzie

$$S_i(F) = \begin{cases} F \setminus \{i\} \cup \{1\} & \text{jeśli } i \in F, 1 \notin F \text{ oraz } F \setminus \{i\} \cup \{1\} \notin \mathcal{F}, \\ F & \text{w przeciwnym przypadku.} \end{cases}$$

Jeśli $S_i(F) = F$ z powodu istnienia już przesuniętego zbioru w rodzinie, to mówimy, że F został zablokowany.

Lemat 4.8.1. Dla każdego skończonego $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ i $i \geq 2$ jest $|S_i(\mathcal{F})| = |\mathcal{F}|$.

Dowód. Różne zbiory są przesuwane w różne zbiory, a zbiór nie zostanie przesunięty, jeśli jego przesunięcie już jest w rodzinie. \square

Lemat 4.8.2. Dla dowolnego skończonego $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ i dowolnego $i \geq 2$ jest $\Delta S_i(\mathcal{F}) \subseteq S_i(\Delta \mathcal{F})$.

Dowód. Dowód wymaga rozważenia czterech przypadków. Przypuśćmy, że $E \in \Delta S_i(\mathcal{F})$, więc $E = S_i(F) \setminus \{x\}$ dla pewnego $F \in \mathcal{F}$ i $x \in S_i(F)$.

Najpierw założymy, że $1, i \notin S_i(F)$. Ponieważ $1 \notin S_i(F)$, musimy mieć $S_i(F) = F$, a zatem $E \subset F$. Zatem $E \in \Delta \mathcal{F}$, a ponieważ $i \notin E$, to $S_i(E) = E$. W związku z tym $E \in S_i(\Delta \mathcal{F})$.

Teraz przypuśćmy, że $1, i \in S_i(F)$. Ponieważ $i \in S_i(F)$, mamy $S_i(F) = F$, a zatem $E \in \Delta \mathcal{F}$, jak wcześniej. Jeśli $x \neq 1$, to $1 \in E$, i zatem $E = S_i(E) \in S_i(\Delta \mathcal{F})$. Jeśli $x = 1$, to $E' = E \setminus \{i\} \cup \{1\} \subset F$, a zatem $E' \in \Delta \mathcal{F}$. To oznacza, że E jest zablokowane i $S_i(E) = E$, co implikuje $E \in S_i(\Delta \mathcal{F})$.

W trzecim przypadku przypuśćmy, że $S_i(F) \cap \{1, i\} = \{i\}$. Ponieważ $i \in S_i(F)$, musimy mieć $S_i(F) = F$. Jednakże, jako że $i \in F$ i $1 \notin F$, F musiało być zablokowane przez $F' = F \setminus \{i\} \cup \{1\} \in \mathcal{F}$. Ponieważ $E \subset S_i(F) = F$, $E \in \Delta \mathcal{F}$. Jeśli $x = i$, to $i \notin E$, i zatem $E = S_i(E) \in S_i(\Delta \mathcal{F})$. Jeśli $x \neq i$, to E byłoby zablokowane przez $E' = F' \setminus \{x\} \in \Delta \mathcal{F}$, i zatem $E = S_i(E) \in S_i(\Delta \mathcal{F})$ również w tym przypadku.

Ostatni przypadek to gdy $S_i(F) \cap \{1, i\} = \{1\}$. Zauważmy, że $i \notin E$ i zatem $S_i(E) = E$. W związku z tym, jeśli $E \in \Delta \mathcal{F}$, to $E = S_i(E) \in S_i(\Delta \mathcal{F})$. Jeśli F nie przesunął się, to $F = S_i(F)$ i $E \in \Delta \mathcal{F}$. Jeśli F przesunął się, to $S_i(F) = F \setminus \{i\} \cup \{1\}$. Jeśli $x = 1$, to $E \subset F$ i zatem jak wcześniej $E \in \Delta \mathcal{F}$. Jeśli $x \neq 1$, niech $E' = E \setminus \{1\} \cup \{i\}$ i zauważmy, że $E' \subset F$, i zatem $E' \in \Delta \mathcal{F}$. Wtedy albo $E \in \Delta \mathcal{F}$, albo E' nie jest zablokowane przed przesunięciem, i $E = S_i(E') \in S_i(\Delta \mathcal{F})$. To kończy analizę przypadków. \square

Definicja 4.8.3. Rodzinę $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ nazywamy stabilną, jeśli $S_i(\mathcal{F}) = \mathcal{F}$ dla każdego $i \geq 2$.

Lemat 4.8.3. Dla każdej skończonej rodziny $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ istnieje rodzina stabilna $\mathcal{G} \subset \binom{\mathbb{N}}{k}$ taka, że $|\mathcal{G}| = |\mathcal{F}|$ i $|\Delta \mathcal{G}| \leq |\Delta \mathcal{F}|$.

Dowód. Dla stabilnej \mathcal{F} można wziąć $\mathcal{G} = \mathcal{F}$, a inaczej można wziąć $\mathcal{F}' = S_i(\mathcal{F}) \neq \mathcal{F}$ dla pewnego $i \geq 2$ – Lematy 4.8.1 i 4.8.2 dają pożądane wielkości odpowiednich zbiorów. Możemy w ten sposób przesuwać rodzinę, póki się da. Ten proces się zakończy, bo każde przesunięcie zwiększa liczbę zbiorów zawierających 1. \square

Lemat 4.8.4. Dla każdej stabilnej rodziny $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ zachodzi $\Delta \mathcal{F}_0 \subseteq \mathcal{F}'_1$, gdzie $\mathcal{F} = \mathcal{F}_0 \sqcup \mathcal{F}_1$ i $\mathcal{F}_0 = \{F \in \mathcal{F} : 1 \notin F\}$ oraz $\mathcal{F}_1 = \{F \in \mathcal{F} : 1 \in F\}$ i $\mathcal{F}'_1 = \{F \setminus \{1\} : F \in \mathcal{F}_1\}$.

Dowód. Przypuśćmy, że $E \in \Delta \mathcal{F}_0$. Wówczas musimy mieć $E = F \setminus \{x\}$ dla pewnego $F \in \mathcal{F}_0$ oraz $x \in F$. Ponieważ $F \in \mathcal{F}_0$, $x \geq 2$. Ponieważ \mathcal{F} jest stabilna, to $S_x(\mathcal{F}) = \mathcal{F}$, a zatem

$S_x(F) = F$. To oznacza, że F był zablokowany, więc $F' = F \setminus \{x\} \cup \{1\} \in \mathcal{F}$ i w szczególności jest w \mathcal{F}_1 . Zatem $E = (F \setminus \{x\} \cup \{1\}) \setminus \{1\} \in \mathcal{F}'_1$. \square

Lemat 4.8.5. Dla każdej stabilnej rodziny $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ zachodzi $|\Delta\mathcal{F}| = |\mathcal{F}'_1| + |\Delta\mathcal{F}'_1|$, gdzie $\mathcal{F} = \mathcal{F}_0 \sqcup \mathcal{F}_1$ i $\mathcal{F}_0 = \{F \in \mathcal{F} : 1 \notin F\}$ oraz $\mathcal{F}_1 = \{F \in \mathcal{F} : 1 \in F\}$ i $\mathcal{F}'_1 = \{F \setminus \{1\} : F \in \mathcal{F}_1\}$.

Dowód. Oczywiście mamy $\Delta\mathcal{F} = \Delta\mathcal{F}_0 \cup \Delta\mathcal{F}_1$. W Lemacie 4.8.4 pokazaliśmy, że $\Delta\mathcal{F}_0 \subseteq \mathcal{F}'_1$. Niech $\mathcal{F}'' = \{F \cup \{1\} : F \in \Delta\mathcal{F}'_1\}$. Pokażemy, że $\Delta\mathcal{F}_1 = \mathcal{F}'_1 \cup \mathcal{F}''$. Te dwa zbiory są rozłączne (elementy tylko jednego zawierają 1), a w pierwszym z nich zawiera się \mathcal{F}_0 , więc da nam to żadaną równość.

To, że $\mathcal{F}'_1 \subseteq \Delta\mathcal{F}_1$, wynika z jego definicji, ponieważ dla każdego $F' \in \mathcal{F}'_1$ mamy $F' = F \setminus \{1\}$ dla pewnego $F \in \mathcal{F}_1$. Usunięcie elementu i dodanie 1 do elementu \mathcal{F}'_1 (przy definiowaniu \mathcal{F}'') można zrobić w odwrotnej kolejności, więc $\mathcal{F}'' \subseteq \Delta\mathcal{F}_1$. Jednocześnie w tych dwóch zbiorach znajdują się wszystkie elementy cienia \mathcal{F}_1 – jedne z nich powstają przez usunięcie 1, a drugie przez usunięcie czegośkolwiek innego. To dowodzi zawierania w drugą stronę i kończy dowód. \square

Twierdzenie 4.8.3 (Lovász). Niech $\mathcal{F} \subset \binom{\mathbb{N}}{k}$ i $|\mathcal{F}| = m = \binom{x}{k}$, gdzie $x \in \mathbb{R}$. (dla przypomnienia, definiujemy $\binom{x}{k} = \frac{x^{\underline{k}}}{k!}$). Wtedy

$$|\Delta\mathcal{F}| \geq \binom{x}{k-1}.$$

Dowód. Przeprowadzimy indukcję po (k, m) . Dla $k = 1$ cień zawiera zbiór pusty i wymagamy od niego rozmiaru 1. Dla $m = 1 = \binom{k}{k}$ cień składa się z $k = \binom{k}{k-1}$ elementów. Dalej zakładamy, że $k, m \geq 2$. Z Lematu 4.8.3 możemy założyć, że \mathcal{F} jest stabilna. Niech $\mathcal{F} = \mathcal{F}_0 \sqcup \mathcal{F}_1$ i $\mathcal{F}_0 = \{F \in \mathcal{F} : 1 \notin F\}$ oraz $\mathcal{F}_1 = \{F \in \mathcal{F} : 1 \in F\}$ i $\mathcal{F}'_1 = \{F \setminus \{1\} : F \in \mathcal{F}_1\}$. Pokażemy, że $|\mathcal{F}'_1| \geq \binom{x-1}{k-1}$.

Założmy, że tak nie jest. Mamy $m = |\mathcal{F}| = |\mathcal{F}_0| + |\mathcal{F}_1|$ oraz $|\mathcal{F}'_1| = |\mathcal{F}_1|$, zatem $|\mathcal{F}_0| > \binom{x}{k} - \binom{x-1}{k-1} = \binom{x-1}{k}$. Dla stabilnej rodziny \mathcal{F} rodzina \mathcal{F}_1 jest niepusta i $|\mathcal{F}_0| < m$, więc z indukcji i Lematu 4.8.4 jest $|\mathcal{F}'_1| \geq |\Delta\mathcal{F}_0| \geq \binom{x-1}{k-1}$, co daje sprzeczność z założeniem nie wprost.

Z indukcji mamy teraz $|\Delta\mathcal{F}'_1| \geq \binom{x-1}{k-2}$. Z Lematu 4.8.5 mamy więc $|\Delta\mathcal{F}| = |\mathcal{F}'_1| + |\Delta\mathcal{F}'_1| \geq \binom{x-1}{k-1} + \binom{x-1}{k-2} = \binom{x}{k-1}$, co kończy dowód. \square

Rozdział 5

Twierdzenie Ramseya i przyjaciele

5.1 Twierdzenie Ramsey’a

W twierdzeniach ramseyowych nie chodzi o jakieś liczby, a o granice Twojej wyobraźni

Student TCSu który uwalit egzamin

Definicja 5.1.1 (Liczby Ramseya). Liczbą Ramseya $R^{(p)}(k; \ell_1, \ell_2, \dots, \ell_k)$ dla $p, k, \ell_i \in \mathbb{N}_1$, nazywamy najmniejszą taką liczbę N , że dla każdej funkcji $c : \binom{[N]}{p} \rightarrow [k]$ (zwanej „kolorowaniem”) istnieje kolor $\alpha \in [k]$ oraz zbiór $S \subseteq [N]$ spełniający: $|S| = \ell_\alpha$ oraz $\binom{S}{p} \subseteq c^{-1}(\alpha)$ – dowolny zbiór spełniający drugą z tych własności (dla dowolnego α) nazywamy „monochromatycznym”.

Twierdzenie 5.1.1. Liczby

$$R^{(p)}(k; \ell_1, \ell_2, \ell_3, \dots, \ell_k)$$

są zdefiniowane poprawnie.

Dowód. Prowadzimy indukcję po p, k i $\sum_{i \in [k]} \ell_i$. Sprawdzamy przypadki bazowe:

1. Gdy $p = 1$ poprawność wynika z zasady szufladkowej, $N = (\sum_{i \in [k]} \ell_i - 1) + 1$;
2. Gdy $k = 1$ trywialnie $R^{(p)}(1; \ell) = \min(p, \ell)$;
3. Trzeci przypadek bazowy polega na tym, że jeżeli dla jakiegoś j , $\ell_j = p$ (p jest to minimalna wartość którą w ogóle może przyjąć jakiejkolwiek ℓ_i , inaczej to by nie miało sensu). Wtedy zachodzi $R^{(p)}(k; \ell_1, \ell_2, \ell_3, \dots, \ell_j, \dots, \ell_k) = R^{(p)}(k-1; \ell_1, \ell_2, \ell_3, \dots, \ell_{j-1}, \ell_{j+1}, \dots, \ell_k)$. Wynika to z prostej obserwacji – jeżeli istnieje jakikolwiek element $x \subset \binom{[N]}{p}$ dla którego $c(x) = j$, to z definicji możemy przyjąć $\alpha = j, S = x$ aby otrzymać „świadka” dla danego kolorowania – oznacza to, że jedyne kolorowania, które mogą dowodzić fałszywości tw. Ramseya dla danego N nie przypisują żadnemu podzbirowi koloru j , a co za tym idzie możemy rozważać kolorowanie mniejszą ilością kolorów.

Zostaje przypadek, gdzie $p, k \geq 2$ i dla każdego i zachodzi $\ell_i > p$. Wprowadźmy oznaczenie:

$$L_i = R^{(p)}(k; \ell_1, \ell_2, \dots, \ell_{i-1}, \ell_i - 1, \ell_{i+1}, \dots, \ell_k)$$

Z założenia indukcyjnego L_i jest zdefiniowane poprawnie (bo zredukowaliśmy sumę ℓ_i ; formalisci mogą sobie podumać nad indukcją po wielu zmiennych i jak działa). Teraz definiujemy sobie pewną *potężną* liczbę służącą jako ograniczenie górne:

$$N = R^{(p-1)}(k; L_1, L_2, L_3, \dots, L_k) + 1$$

Ponownie, jest ona poprawnie zdefiniowana z założenia indukcyjnego (bo kolorujemy teraz podzbiory $p - 1$ -elementowe). Po co ta jedynka na końcu? Zaraz się okaże. Niech c będzie dowolnym kolorowaniem zbioru $\binom{[N]}{p}$ na k kolorów – zdefiniujmy sobie teraz kolorowanie c' , które koloruje $\binom{[N-1]}{p-1}$ również na k kolorów. c' definiujemy sobie w oparciu o c w niezwykle fascynujący sposób – $c'(S) = c(S \cup \{N\})$. Pomocne może być tutaj narysowanie tej sytuacji.

Z definicji N wiemy, że mamy jakieś j oraz jakiś zbiór $S \subset [N - 1]$ o mocy $|S| = L_j$, który jest monochromatyczny względem kolorowania c' .

Ale z definicji L_j wiemy, że istnieje tu podzbiór l_1 lub l_2 lub \dots lub $l_j - 1$ lub \dots lub l_s elementów taki, że każdy ich k -elementowy podzbiór ma ten sam kolor (w kolorowaniu c). Jeśli własność ta zachodzi dla jakiegokolwiek ℓ_i gdzie $i \neq j$, to ta własność nam się przez przypadek właśnie udowodniła (i nawet nie użyliśmy naszego śmiesznego kolorowania). Pozostaje nam ciekawszy przypadek, gdy mamy $l_j - 1$ punktów takich, że ich każdy k -elementowy podzbiór jest pokolorowany na kolor j .

Ale w tym przypadku z definicji c' otrzymujemy fajną własność – dowolny zbiór $M \in \binom{S}{p-1}$ ma z definicji ten sam kolor co $S \cup \{N\}$ w kolorowaniu c . Czyli skoro w S istnieje podzbiór M o mocy $l_j - 1$ taki, że wszystkie elementy $\binom{M}{p}$ są koloru j , to po dodaniu N do tego podzbioru otrzymujemy zbiór l_j -elementowy spełniający założenia o kolorowaniu. Sparse'owanie tego co się stało może trochę zająć, ale w sumie to udowodniliśmy twierdzenie Ramsey'a. Fajnie. \square

Alternatywny szkic dowodu. Można ułatwić odrobinę powyższy dowód nie indukując się po liczbie kolorów k . Najpierw dowodzimy przypadek dla $p = k = 2$ – dowód opisany jest w sekcji o ograniczeniu górnym liczby $R(s, t)$ przez Erdősa-Szekeresa. Następnie rozszerzamy dowód dla wszystkich p w sposób analogiczny do tego powyżej. Aby rozszerzyć dowód dla wszystkich k wystarczy zauważyć, że

$$R^{(p)}(k; \ell_1, \ell_2, \dots, \ell_k) \leq R^{(p)}(2; \ell_1, R^{(p)}(k - 1, \ell_2, \ell_3, \dots, \ell_k))$$

Aby to udowodnić, przyjmując prawą stronę nierówności jako N i mając kolorowanie $c : \binom{[N]}{p} \rightarrow [k]$, definiujemy kolorowanie na dwóch kolorach $c'(x) = \min(c(x), 2)$. Z definicji N musi istnieć poprawne kolorowanie ℓ_1 elementów na kolor 1, które dowodzi poprawności N , lub kolorowanie

zbioru o mocy $R^{(p)}(k-1; \ell_2, \ell_3, \dots, \ell_k)$ składające się wyłącznie z kolorów innych od 1 – wtedy kontynuujemy rozumowanie rekurencyjnie na mniejszej ilości kolorów, co dowodzi poprawności N . Dowód ten jest na tyle fajny na egzaminie, że pracując tylko na dwóch kolorach tracimy trochę „boilerplate'u” z poprzedniego dowodu, a ponadto nie musimy się powtarzać przy dowodzie ograniczenia Erdősa-Szekeres'a. \square

5.2 Ograniczenia dolne niektórych liczb Ramsey'a

Twierdzenie 5.2.1 (Ograniczenie dolne na symetryczną liczbę Ramsey'a $R(k, k)$).

$$(\sqrt{2})^k < R(k, k) \quad (5.1)$$

Dowód. Oznaczmy jako B zbiór wszystkich kolorowań, w których istnieje monochromatyczna (czerwona lub niebieska) klika rozmiaru k . Jako, że zbiór wszystkich kolorowań krawędzi grafu na N wierzchołkach ma moc $2^{\binom{N}{2}}$, to jeśli pokażemy że $|B| < 2^{\binom{N}{2}}$, pokażemy że istnieje takie kolorowanie krawędzi grafu, że nie istnieje monochromatyczna klika rozmiaru k , a więc $|N| < R(k, k)$.

Zauważmy, że $B = \bigcup_{x \in \binom{[N]}{k}} B_x$, gdzie jako B_x rozumiemy zbiór wszystkich takich kolorowań, że zbiór x (stanowiącym k wierzchołków z $[N]$) stanowi monochromatyczną klikę (tzn. dla dowolnej pary krawędzi z x krawędzie te mają ten sam kolor).

Możemy to teraz bardzo brutalnie przeszacować:

$$|B| \leq \sum_{x \in \binom{[N]}{k}} |B_x|$$

Będziemy tutaj zliczać wielokrotnie mnóstwo rzeczy, ale to nam wystarczy. To zaś przeszacujemy jeszcze brutalniej:

$$\sum_{x \in \binom{[N]}{k}} |B_x| \leq \binom{N}{k} \cdot 2 \cdot 2^{\binom{N}{2} - \binom{k}{2}}$$

Co tutaj zrobiliśmy? Cóż, mówimy że bierzemy k punktów z N punktów, ustawiamy wszystkim krawędziom między nimi jeden z dwóch kolorów, po czym mówimy że wszystkie pozostałe krawędzie mogą mieć absolutnie jakikolwiek kolor. Niewątpliwie będziemy podwójnie zliczać wiele kolorowań, ale niespecjalnie nas to tutaj obchodzi.

Chcielibyśmy teraz pokazać, że

$$\binom{N}{k} \cdot 2 \cdot 2^{\binom{N}{2} - \binom{k}{2}} < 2^{\binom{N}{2}}$$

równoważnie:

$$\binom{N}{k} < 2^{\binom{k}{2} - 1}$$

Jednocześnie usiłujemy pokazać ograniczenie dolne, więc

$$N \leq (\sqrt{2})^k$$

Jeśli podniesiemy tę nierówność do k -tej potęgi

$$N^k \leq 2^{\frac{k^2}{2}}$$

Przeszacujmy zatem $\binom{N}{k}$:

$$\binom{N}{k} = \frac{N!}{k! \cdot (N-k)!} \leq \frac{N^k}{k!}$$

Takie przeszacowanie w sumie ma sens, skracamy $N!$ z $(n-k)!$ i szacujemy potęgę kroczącą przez potęgę. Teraz jeszcze fajnie byłoby zauważyć, że $k! > 2^{\frac{k}{2}+1}$, skąd mamy:

$$\frac{N!}{k! \cdot (N-k)!} \leq \frac{N^k}{k!} < \frac{N^k}{2^{\frac{k}{2}+1}} \leq \frac{2^{\frac{k^2}{2}}}{2^{\frac{k}{2}+1}} = 2^{\frac{k \cdot (k-1)}{2}-1} = 2^{\binom{k}{2}-1}$$

czyli wyszło to co chcieliśmy żeby wyszło. □

Alternatywny dowód probabilistyczny. Niech $N = (\sqrt{2})^k$ – będziemy kolorować zbiór $\binom{N}{2}$ w sposób jednorodnie losowy. Aby to zrobić, kolorujemy każdy element z równym prawdopodobieństwem $\frac{1}{2}$ na kolor 1 lub 2 – wtedy zbiorem zdarzeń jest $2^{\binom{N}{2}}$ (zbiór wszystkich kolorowań), a każde z nich możemy otrzymać z równym prawdopodobieństwem.

Zastanówmy się teraz, jaka jest szansa, że ustalając dowolny podzbiór $S \subset [N]$ o mocy k , a następnie losując kolorowanie, zbiór S będzie monochromatyczny. Łatwo zauważyć, że prawdopodobieństwo wyniesie $2 \cdot 2^{-\binom{k}{2}}$ (zawężamy zbiór zdarzeń do kolorowania zbioru S , aby otrzymać zbiór zdarzeń o mocy $2^{\binom{k}{2}}$, a istnieją w nim 2 zbiory monochromatyczne).

Możemy teraz oszacować prawdopodobieństwo (oznaczone p), że istnieje jakakolwiek zbiór jest monochromatyczny:

$$\begin{aligned} p &\leq 2 \cdot 2^{-\binom{k}{2}} \cdot \binom{N}{k} \\ &= 2 \cdot 2^{-\frac{1}{2}k(k-1)} \cdot \frac{(2^{\frac{k}{2}})^k}{k!} \\ &< 2 \cdot 2^{-\frac{k^2}{2}} \cdot 2^{\frac{k}{2}} \cdot 2^{\frac{k^2}{2}} \cdot \frac{1}{k!} \\ &= \frac{2^{\frac{k}{2}+1}}{k!} \leq 1 \end{aligned}$$

Ale ponieważ $p < 1$ w zbiorze zdarzeń musi istnieć świadek, że N nie zawiera monochromatycznego zbioru wielkości k , co kończy dowód. □

5.3 Ograniczenie górne niektórych liczb Ramsey'a

Twierdzenie 5.3.1 (Erdős).

$$R(k, k) \leq 2^{2k} \quad (5.2)$$

Dowód. Mamy sobie klikę na $N = 2^{2k}$ punktach. Weźmy sobie jakiś przypadkowy, v_1 . Wychodzą z niego jakieś czerwone lub niebieskie krawędzie do wszystkich innych punktów. Dosyć oczywistym jest, że przynajmniej połowa wychodzących z niego krawędzi musi być czerwona lub niebieska (bo są tylko 2 dostępne kolory, zasada szufladkowa czy coś). To oznacza, że mamy jakoś co najmniej 2^{2k-1} punktów łączących się z v_1 tym samym kolorem. Zbiór tych wszystkich punktów oznaczmy jako C_1 . Bierzemy jakiś wierzchołek v_2 ze zbioru C_1 i tworzymy analogicznie zbiór C_2 . Bardzo ważne jest by zauważyć, że v_2 z punktami z C_2 nie musi się łączyć na ten sam kolor, na który v_1 łączy się z punktami z C_1 . W każdym razie, ponawiając tę procedurę otrzymamy ciąg $2k$ punktów v_1, v_2, \dots, v_{2k} . Dla każdego punktu v_i z tego ciągu prawdą jest, że punkty v_{i+1}, \dots, v_{2k} łączą się z nim w tym samym kolorze (bo wszystkie są elementami zbioru C_i). To w sumie już prowadzi nas do rozwiązania, bo skoro punktów w tym ciągu jest $2k$, to musi być co najmniej k takich że łączą się ze wszystkimi „późniejszymi” na czerwono lub na niebiesko, a więc otrzymujemy klikę monochromatyczną rozmiaru co najmniej k . Fajnie. \square

Twierdzenie 5.3.2 (Erdős-Szekeres).

$$R(k, k) \leq \binom{s+t-2}{s-1} \quad (5.3)$$

Dowód. Zastosujemy indukcję po $s+t$. Dla $s=t=2$ jest $R^{(2)}(2,2)=2$. Niech $N = R^{(2)}(s-1, t) + R^{(2)}(s, t-1)$. Pokażemy, że $R(s, t) \leq N$, co indukcyjnie udowodni tezę (patrz: własności dwumianów). Niech $c : \binom{[N]}{2} \rightarrow [2]$ i $v \in [N]$. Przez A oznaczmy zbiór tych elementów $[N]$, które w parze z v są pokolorowane kolorem 1. Analogicznie definiujemy B dla koloru 2. Mamy $|A| + |B| + 1 = N$. Jeśli $|A| \geq R^{(2)}(s-1, t)$ lub $|B| \geq R^{(2)}(s, t-1)$, to istnieją odpowiednie zbiory – albo wewnątrz A lub B , albo po dodaniu do znalezionych zbiorów v . Któraś z tych nierówności musi zachodzić, bo inaczej suma ich mocy jest za mała (Dirichlet się kłania). \square

Warto zaznaczyć, że powyższy dowód można łatwo przerobić na dowód pierwszego ograniczenia – możemy ograniczyć $R(s, t)$ przez 2^{s+t} zamiast dwumianu, przez co powtarzając dowód otrzymujemy ograniczenie z tw. Erdősa.

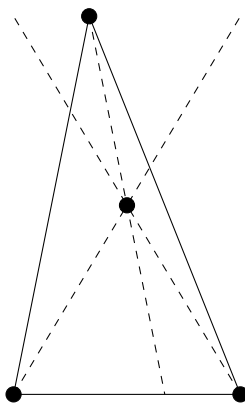
5.4 Twierdzenie Erdősa-Szekeresa

5.4.1 Dowód z twierdzenia Ramseya

Definicja 5.4.1. Mówimy, że zbiór punktów na płaszczyźnie jest w pozycji ogólnej, jeśli żadne trzy nie są współliniowe.

Twierdzenie 5.4.1 (Happy Ending Problem; Esther Klein). W dowolnym zbiorze 5 punktów na płaszczyźnie w pozycji ogólnej pewne 4 tworzą czworokąt wypukły.

Dowód. Jeśli otoczka wypukła tych pięciu punktów ma 5 albo 4 punkty, to teza jest oczywista. Rozważmy sytuację, gdy otoczka wypukła jest trójkątem.



Umieszczając piąty punkt w dowolnym z powstałych trójkątów otrzymujemy czworokąt wypukły powstały z punktu w środku trójkąta i odpowiednich wierzchołków trójkąta. \square

Twierdzenie 5.4.2 (Erdős-Szekeres; przez Happy Ending Problem). Dla dowolnego n istnieje takie N , że jeśli N punktów na płaszczyźnie znajduje się w pozycji ogólnej to jakieś n z nich znajduje się w pozycji wypukłej.

Dowód. Na początek zauważmy, że jeśli dowolne 4 z n punktów w pozycji ogólnej tworzą czworokąt wypukły, to wszystkie n punktów tworzy wielokąt wypukły. Załóżmy nie wprost, że jakiś punkt leży we wnętrzu otoczki wypukłej takiego zbioru. Po striangulowaniu otoczki ten punkt leży w którymś z trójkątów. Czworokąt złożony z tego trójkąta i punktu w nim nie jest wypukły, a więc nie wszystkie czwórki są wypukłe – sprzeczność.

Niech $N = R^{(4)}(2; n, 5)$ i niech X będzie dowolny zbiorem N punktów w pozycji ogólnej.

Definiujemy kolorowanie $c : \binom{X}{4} \rightarrow [2]$ zadane przez $c(Y) = \begin{cases} 1 & Y \text{ wypukły} \\ 2 & Y \text{ wklęsły} \end{cases}$. Teraz albo

mamy zbiór n punktów, gdzie każda czwórka tworzy czworokąt wypukły (a więc całość tworzy wielokąt wypukły), albo 5 punktów, gdzie każda czwórka tworzy wielokąt wklęsły – to jednak nie może zajść na mocy Happy Ending Problem. \square

5.4.2 Dowód z kubeczkami i czapeczkami

Definicja 5.4.2. Zbiór k punktów na płaszczyźnie w pozycji ogólnej takich, że żadnym dwóm nie powtarza się żadna współrzędna nazwiemy k -kubkiem, jeśli dla każdej pary tych punktów wszystkie punkty pomiędzy nimi (to znaczy dla punktów o współrzędnych x_1, x_2 wszystkie punkty o współrzędnej $x_j : x_1 < x_j < x_2$) leżą poniżej linii prostej puszczanej przez te dwa punkty. k -kubek jest k -kątem wypukłym (dowód przez „bo widać”).

Definicja 5.4.3. Zbiór k punktów na płaszczyźnie w pozycji ogólnej takich, że żadnym dwóm nie powtarza się żadna współrzędna nazwiemy k -czapką, jeśli dla każdej pary tych punktów wszystkie punkty pomiędzy nimi (to znaczy dla punktów o współrzędnych x_1, x_2 wszystkie punkty o współrzędnej $x_j : x_1 < x_j < x_2$) leżą powyżej linii prostej puszczanej przez te dwa punkty. k -czapka jest k -kątem wypukłym (dowód jak wyżej).

Jako $f(k, c)$ będziemy oznaczać minimalną taką liczbę, że jeśli mamy $f(k, c)$ punktów o różnych współrzędnych x na płaszczyźnie (i w pozycji ogólnej) to znajdziemy tam k -kubek lub c -czapeczkę. Wtedy też

Twierdzenie 5.4.3 (O kubkach i czapkach). Liczba $f(k, c)$ określona jest poprawnie.

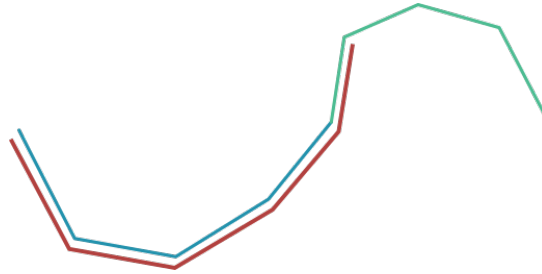
Dowód. Indukcja po k, c . Widać trywialnie, że $f(2, c) = 2$ oraz $f(k, 2) = 2$. Pokażemy teraz ograniczenie górne na $f(k, c)$:

$$f(k, c) \leq f(k-1, c) + f(k, c-1) - 1$$

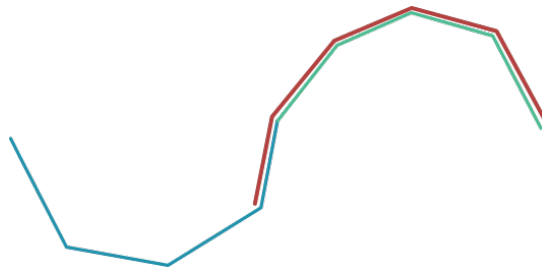
Rozważmy zbiór X punktów w pozycji ogólnej o parami różnych współrzędnych x oraz y mający $f(k-1, c) + f(k, c-1) - 1$ punktów. Nazwiemy go P . Z założenia indukcyjnego (biorąc pod uwagę pierwszy składnik) znajduje się w nim $k-1$ -kubek lub c -czapeczka. Jeśli znajduje się tam c -czapeczka to od razu mamy sprawę załatwioną; zakładamy więc że jest tam $k-1$ -kubek. Robimy teraz sobie zbiór E , taki że zawiera wszystkie końce $k-1$ -kubków z P . Na pewno jest taki jeden (bo na pewno mamy k -kubek). Okazuje się jednak, że moc E jest całkiem spora. Pokazujemy to za pomocą bardzo ciekawego fikołka; wywalamy ten koniec $k-1$ -kubka o którym wiemy, że on istnieje ze zbioru P (tak na chwilę). Plot twist polega na tym, że nadal mamy dostatecznie dużo punktów by zmaistrować $k-1$ kubek (być może zupełnie gdzie indziej, ale na pewno gdzieś on jest), bo punktów teraz jest $f(k-1, c) - 1 + f(k, c-1) - 1 \geq f(k-1, c)$. Procedurę tę powtarzamy póki możemy i wychodzi nam, że zbiór E ma moc co najmniej $f(k, c-1)$. Fajnie. Teraz jeśli zbiór E zawiera k -kubek to mamy tezę udowodnioną, więc założmy że zawiera $c-1$ -czapeczkę. Biorąc sobie teraz tę $c-1$ -czapeczkę; jej pierwszy punkt jest równocześnie końcem jakiegoś $k-1$ -kubka.

Jesteśmy już blisko końca dowodu. Weźmy sobie punkt który stanowił koniec $k-1$ -kubka i początek $c-1$ -czapeczki – nazwijmy go y . Punkt „na lewo” od niego, przedostatni w kubku, nazwijmy x . Punkt „na prawo” od niego, drugi w czapeczce, nazwijmy z . Rozpatrzmy prostą

która idzie między punktami x i z . Można dokonać szokującego odkrycia, że y leży albo nad nią, albo pod nią (jeśli leży na niej to punkty nie znajdowały się w pozycji ogólnej, co przeczyłoby założeniom twierdzenia). Teraz jeśli y leży pod nią, możemy rozszerzyć nasz $k-1$ -kubek na k -kubek, dorzucając do niego z . Analogicznie, jeśli leży on nad nią, możemy rozszerzyć czapeczkę (oczywiście z pozycji ogólnej wiemy, że nie są one współliniowe). To kończy dowód.



Rysunek 5.1: Rozszerzanie kubka



Rysunek 5.2: Rozszerzanie czapki

□

Z powyższego faktu wynika udowodnione wcześniej twierdzenie Erdősa-Szekeresa (biorąc $N = f(n, n)$) – o ile możemy pozbyć się założenia, że wszystkie punkty mają różne współrzędne. Wykorzystamy trick (i zdrową dawkę machania rękami), że możemy bezstratnie założyć fakt o różnych współrzędnych. Aby naprawić złą konfigurację, możemy obrócić o „odrobinę” punkty wokół pewnego punktu odniesienia – zmieni to współrzędne na tyle, aby były parami różne, ale jednocześnie zachowa wklęsłość znalezionej kubka/czapki.

5.5 Twierdzenie Schura

Twierdzenie 5.5.1 (Schur). Dla dowolnego $k \in \mathbb{N}$ istnieje N takie, że dla każdego kolorowania $c : [N] \rightarrow [k]$ istnieją $x, y, z \in [N]$ spełniające $x + y = z$ oraz $c(x) = c(y) = c(z)$.

Dowód. Dla $k \leq 1$ twierdzenie jest trywialne. Ustalmy $k \geq 2$ i weźmy $N = R^{(2)}(k; 3, 3, \dots, 3)$. Dla dowolnego kolorowania $c : [N] \rightarrow [k]$ definiujemy kolorowanie $c' : \binom{[N]}{2} \rightarrow [k]$ zadane przez $c'(\{x, y\}) = c(|x - y|)$. Z definicji N istnieje monochromatyczna trójka i, j, k . Niech bez straty ogólności niech $i \leq j \leq k$. Mamy $c(j - i) = c(k - i) = c(k - j)$, więc kładąc $x = j - i$, $y = k - j$, $x + y = k - i$ otrzymujemy tezę. □

5.6 Twierdzenie Halesa-Jewett'a

Definicja 5.6.1. d -wymiarową kostką o boku m nazywamy zbiór $[m]^d = \{(x_1, \dots, x_d) : \forall_i x_i \in [m]\}$.

Definicja 5.6.2. $L \subset [m]^d$ nazywamy linią kombinatoryczną, jeśli istnieje niepusty zbiór $I \subset [d]$ oraz $\{y_i\}_{i \in [d] \setminus I}$ takie, że L jest postaci $\{(x_1^\alpha, \dots, x_d^\alpha) : \alpha \in [m]\}$, gdzie

$$x_i^\alpha = \begin{cases} \alpha & i \in I \\ y_i & i \in [d] \setminus I \end{cases},$$

czyli istnieje zbiór wymiarów, na których współrzędne rosną od 1 do m , a na pozostałych są ustalone. Zbiór I nazywamy aktywnym zbiorem.

Definicja 5.6.3 (Alternatywna definicja). Dla niektórych bardziej intuicyjna może być równoważna definicja linii kombinatorycznej poprzez funkcje. Linią kombinatoryczną w $[m]^d$ nazywamy zbiór postaci $\{(f_1(i), f_2(i), \dots, f_n(i)) : i \in [m]\}$, gdzie każda z funkcji $f_i : [m] \rightarrow [m]$ jest równa $I : [m] \ni x \mapsto x \in [m]$ lub $K_v : [m] \ni x \mapsto v \in [m]$ dla pewnego v , oraz istnieje indeks j spełniający $f_j = I$. Zbiorem aktywnym jest wtedy zbiór $\mathcal{I} = \{i \in [m] : f_i = I\}$, a przez x_i^α oznaczamy $f_\alpha(i)$ (aby zachować notację z poprzedniej definicji).

Twierdzenie 5.6.1 (Hales-Jewett). Dla dowolnych $m, k \in \mathbb{N}_1$ istnieje $N \in \mathbb{N}$ o tej własności, że dla każdego kolorowania $c : [m]^N \rightarrow [k]$ istnieje monochromatyczna linia kombinatoryczna. Najmniejszą liczbę N spełniającą powyższe nazywamy $\text{HJ}(m, k)$.

Dowód. Dla linii kombinatorycznej L niech L^- i L^+ oznaczają jej pierwszy i ostatni punkt. Mówimy, że linie L_1, \dots, L_s są zogniskowane w f , jeśli $L_i^+ = f$ dla każdego $i \in [s]$. Dodatkowo mówimy, że są kolorowo zogniskowane, gdy wszystkie linie $L_i \setminus \{f\}$ są monochromatyczne i w innym kolorze. Przeprowadzimy dowód indukcyjny po m . Baza $m = 1$ jest oczywista (istnieje tylko jeden punkt kostki).

Zdefiniujmy $T = \text{FHJ}(k, s, m)$ jako najmniejszą taką liczbę, że każde k -kolorowanie $[m]^T$ albo zawiera monochromatyczną linię kombinatoryczną, albo zawiera s kolorowo zogniskowanych linii. Zauważmy, że podstawienie $s = k$ daje nam naszą tezę, bo co najmniej jedna ze zogniskowanych linii ma wtedy taki sam kolor, jak punkt zogniskowania. Dowodzimy istnienie tej rodziny liczb indukując się po s . Dla $s = 1$ wystarczy postawić $\text{FHJ}(k, 1, m) = \text{HJ}(k, m - 1)$ (istnieje krótsza monochromatyczna linia). Niech $n = \text{FHJ}(k, s - 1, m)$ i $n' = \text{HJ}(k^{m^n}, m - 1)$. Pokażemy, że $\text{FHJ}(k, s, m) \leq n + n'$.

Weźmy dowolne k -kolorowanie ϕ kostki $[m]^{n+n'}$. Można dla niego zdefiniować (k^{m^n}) -kolorowanie ϕ' kostki $[m]^{n'}$ jako kolorowanie produktowe wszystkich punktów o ustalonych pierwszych n' współrzędnych w $[m]^{n+n'}$ (zatem każda kostka $[m]^n$ jest osobnym kolorem). Z definicji n' w ϕ' istnieje linia L w $[m]^{n'}$ o aktywnym zbiorze I taka, że skrócona linia $L \setminus \{L^+\}$ jest monochromatyczna. To znaczy, że dla $a \in [m]^n$ i $b, b' \in L \setminus \{L^+\}$ zachodzi $\phi((b, a)) = \phi((b', a))$. Można więc zdefiniować kolorowanie ϕ'' kostki $[m]^n$ jako $\phi''(a) = \phi((b, a))$ dla dowolnego $b \in L \setminus \{L^+\}$.

Monochromatyczna linia w ϕ'' jest też monochromatyczną linią w ϕ (ten sam zbiór aktywny, w n' pierwszych wymiarach same nieaktywne leżące na L). Załóżmy więc, że w ϕ'' nie ma monochromatycznej linii. Z definicji n mamy w ϕ'' zbiór $s - 1$ kolorowo zogniskowanych linii L_1, \dots, L_{s-1} o aktywnych zbiorach I_1, \dots, I_{s-1} i ognisku f . Dla każdego i zdefiniujemy L'_i jako linię w $[m]^{n+n'}$ o pierwszym punkcie (L^-, L_i^-) i aktywnym zbiorze $I \cup I_i$, a L'_s jako linię o pierwszym punkcie (L^-, f) i aktywnym zbiorze I . O ile w ϕ nie ma monochromatycznej linii, to właśnie zdefiniowaliśmy s kolorowo zogniskowanych linii o ognisku (L^+, f) , bo jeśli f był innego koloru niż wszystkie zogniskowane w nim linie, to L'_s będzie miała całkiem nowy kolor. To kończy dowód. \square

5.7 Twierdzenie van der Waerden'a

Twierdzenie 5.7.1 (van der Waerden). Dla każdego $m, k \geq 1$ istnieje N o tej własności, że dla każdego kolorowania $c : [N] \rightarrow [k]$ istnieje monochromatyczny ciąg arytmetyczny długości m zawarty w $[N]$.

Dowód. Niech $n = \text{HJ}(m, k)$ (najmniejsza taka liczba, że $[m]^{\text{HJ}(m, k)}$ ma monochromatyczną linię kombinatoryczną w dowolnym k -kolorowaniu) oraz $N = n \cdot m$. Dla dowolnego kolorowania $c : [N] \rightarrow [k]$ definiujemy $c' : [m]^n \rightarrow [k]$ jako $c'(x_1, \dots, x_n) = c(x_1 + \dots + x_n)$. Z definicji n dla kolorowania c' istnieje monochromatyczna linia kombinatoryczna $L \subset [m]^n$. Niech $S = \{\sum_{i=1}^m x_i : (x_1, x_2, x_3, \dots, x_m) \in L\}$ – łatwo zauważyć, że po ustawieniu tego zbioru w kolejności rosnącej otrzymamy ciąg arytmetyczny o różnicy $|I|$, gdzie I to aktywny zbiór linii L . Ale co więcej, z definicji c' wynika, że otrzymany zbiór S jest również monochromatyczny – otrzymujemy więc oczekiwaną tezę. \square

Rozdział 6

Funkcje tworzące

6.1 Rozwiązywanie rekurencji liniowych

I can elaborate: zrobiłam zadanka,
zobaczyłam tworzące, stwierdziłam, że
chce mi się spać, poszłam sobie

*Studentka TCSu o zadaniach z funkcji
tworzących na kolokwium*

6.1.1 Rozkład na ułamki proste

To nie jest formalny dowód ani formalna własność ani nic, bardziej schemat postępowania przy rozkładzie na ułamki proste. Sam dowód tego, że rozkład na ułamki proste istnieje, to *sprowadź do wspólnego mianownika i zobacz co Ci wyszło*. Jeżeli $\deg(P(x)) < \deg(Q(x))$ i $Q(x) = (x - a)^n \cdot (x - b)^k$ to:

$$\frac{P(x)}{Q(x)} = \frac{P(x)}{(x - a)^n \cdot (x - b)^k} = \frac{A_1}{x - a} + \frac{A_2}{(x - a)^2} + \dots + \frac{A_n}{(x - a)^n} + \frac{B_1}{x - b} + \frac{B_2}{(x - b)^2} + \dots + \frac{B_k}{(x - b)^k}$$

Oczywiście ten schemat można rozszerzać na więcej śmiesznych rzeczy w mianowniku, ale chyba widać o co chodzi.

6.2 Ciąg Fibbonaciego

Twierdzenie 6.2.1 (Wzór Bineta).

$$f_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right) \quad (6.1)$$

Dowód. Rozpisujemy sobie funkcję tworzącą ciągu f_n :

$$\begin{aligned}
F(x) &= f_0 + f_1 \cdot x + f_2 \cdot x^2 + f_3 \cdot x^3 \dots = \\
&= f_0 + f_1 \cdot x + (f_0 + f_1) \cdot x^2 + (f_1 + f_2) \cdot x^3 + \dots = \\
&= f_0 + f_1 \cdot x + f_0 \cdot x^2 + f_1 \cdot x^2 + f_1 \cdot x^3 + f_2 \cdot x^3 + \dots = \\
&= f_0 + f_1 \cdot x + f_0 \cdot x^2 + f_1 \cdot x^3 + \dots + f_1 \cdot x^2 + f_2 \cdot x^3 + \dots = \\
&= f_0 + f_1 \cdot x + x^2 \cdot (f_0 + f_1 \cdot x + \dots) + x \cdot (f_1 \cdot x + f_2 \cdot x^2 + \dots) = \\
&= f_0 + f_1 \cdot x + x^2 \cdot F(x) + x \cdot (F(x) - f_0) = \\
&= 0 + 1 \cdot x + x^2 \cdot F(x) + x \cdot (F(x) - 0) = \\
&= x + x^2 \cdot F(x) + x \cdot F(x)
\end{aligned}$$

W takim razie mamy, że:

$$F(x) = x + x^2 \cdot F(x) + x \cdot F(x)$$

$$F(x) - x^2 \cdot F(x) - x \cdot F(x) = x$$

$$F(x) \cdot (1 - x^2 - x) = x$$

$$F(x) = \frac{x}{-x^2 - x + 1}$$

Mianownik możemy rozbić (za pomocą liczenia jakichś delt czy coś):

$$F(x) = \frac{x}{(-1) \cdot \left(x - \left(-\frac{1+\sqrt{5}}{2}\right)\right) \cdot \left(x - \left(-\frac{1-\sqrt{5}}{2}\right)\right)}$$

Nie no, serio, jeśli ktoś myśli że będę TeXować te przekształcenia to się myli. Powinno wyjść po przekształceniach że:

$$F(x) = \frac{x}{(1 - ax) \cdot (1 - bx)}$$

gdzie $a = \frac{1+\sqrt{5}}{2}$, $b = \frac{1-\sqrt{5}}{2}$

Dalej rozbijamy na ułamki proste:

$$F(x) = \frac{A}{1 - ax} + \frac{B}{1 - bx}$$

A powinno wyjść $\frac{1}{\sqrt{5}}$, B powinno wyjść $-\frac{1}{\sqrt{5}}$.

Odwijamy każdą z tych funkcji tworzącą z osobna, korzystając ze wzoru podanego we wcześniejszym rozdziale i otrzymujemy wzór. □

6.3 Ciąg Catalana

Tak naprawdę jest to bezużyteczne, bo wzór który nam wyjdzie możemy również pokazać kombinatorycznie, no ale dobra. Korzystamy z faktu, że:

$$c_n = \sum_{i=0}^{n-1} c_i \cdot c_{n-1-i}$$

Rozpisujemy funkcję tworzącą c_n :

$$\begin{aligned} C(x) &= c_0 + c_1 \cdot x + c_2 \cdot x^2 + \dots = \\ &= c_0 + (c_0 \cdot c_0) \cdot x + (c_0 \cdot c_1 + c_1 \cdot c_0) \cdot x^2 + \dots = \\ &= c_0 + c_0 c_0 \cdot x + c_0 c_1 \cdot x^2 + c_1 c_0 \cdot x^2 + \dots = \\ &= c_0 + x \cdot (c_0 \cdot c_0 + c_0 c_1 \cdot x + c_1 c_0 \cdot x + \dots) = \\ &= c_0 + x \cdot C(x) \cdot C(x) \end{aligned}$$

Jeśli ktoś nie wie skąd wytrzasnąłem ostatnie przekształcenie to może sobie wymnożyć $C(x) \cdot C(x)$ żeby zobaczyć że to faktycznie tak wychodzi. Teraz, podobnie jak przy Fibonaccim, wyznaczam wzór na $C(x)$ (tylko że tym razem będą zabawy z równaniami kwadratowymi):

$$1 - C(x) + x(C(x))^2 = 0$$

Żeby żyło się łatwiej, podstawiam $a = C(x)$:

$$a^2 \cdot x - a + 1 = 0$$

Wyjdą nam 2 rozwiązania. Co teraz? Patrzymy na to, które na pewno ucieknie do nieskończoności dla $x = 0$ (bo funkcja tworząca ma być określona dla zera czy coś tam). Tej, która ucieka do nieskończoności nie bierzemy (bierzemy tę, w której dla $x = 0$ wyjdzie zero nad zero).

$$C(x) = \frac{1 - \sqrt{1 - 4x}}{2x}$$

Ten pierwiastek w funkcji tworzącej trochę boli w mózg, ale możemy zrobić fikołka poprzez zmajszrowanie funkcji tworzącej $G(x)$:

$$G(x) = \sqrt{1 - 4x}$$

Wtedy mamy, że:

$$C(x) = \frac{1 - G(x)}{2x} = \frac{1 - G(x)}{x} \cdot \frac{1}{2} = (-1) \cdot \frac{G(x) - 1}{x} \cdot \frac{1}{2}$$

Teraz zaczyna się robić śmiesznie, bo zauważmy że jeśli $G(x)$ było funkcją tworzącą jakiegoś ciągu g_n , to $\frac{G(x)-1}{x}$ jest tworzącą ciągu g_{n+1} (bo odjęliśmy jedynkę od $G(x)$ a potem przedzieliliśmy przez x – warto zauważyć, że $g_0 = 1$, bo $G(0) = 1$; tak działa „przesunięcie” ciągu o ileś elementów, że wywalamy k pierwszych elementów a potem dzielimy przez x^k).

Stąd mamy już, że:

$$c_n = (-1) \cdot g_{n+1} \cdot \frac{1}{2} = \frac{-g_{n+1}}{2}$$

No fajnie, ale skąd mamy wiedzieć ile to jest g_{n+1} ? Tutaj nadciąga z pomocą *śmieszny wzór*, który mówi że:

$$g_{n+1} = \frac{G^{(n+1)}(0)}{(n+1)!}$$

W sumie ten wzór ma sens, bo jak weźmiemy $n+1$ -szą pochodną to „skasujemy” wszystkie elementy które były wcześniej (robienie pochodnych po wielomianach jest fajne). Następnie dzielimy przez $(n+1)!$ by pozbyć się rzeczy, które „dołożyły” się do współczynnika w trakcie liczenia pochodnych, a potem ewaluujemy na zerze by zostało tylko to co nas interesuje (w sensie bo chcemy uzyskać tylko współczynnik przy x^{n+1}). Mnie takie wytłumaczenie przekonuje, formalisci zaś pewnie jeszcze nie ogarnęli co się dzieje przy zliczaniu ścieżek Hamiltona w grafie.

Teraz nasz problem redukuje się do problemu znajdowania pochodnej nieprzyjemnej funkcji. Trochę to będzie boleć, ale dosyć szybko znajdziemy pattern:

$$G(x)' = \sqrt{1-4x}' = ((1-4x)^{\frac{1}{2}})' = \frac{1}{2} \cdot (1-4x)^{-\frac{1}{2}} \cdot (-4)$$

$$G(x)'' = \frac{1}{2} \cdot \frac{-1}{2} \cdot (1-4x)^{-\frac{3}{2}} \cdot (-4)^2$$

$$G(x)''' = \frac{1}{2} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdot (1-4x)^{-\frac{5}{2}} \cdot (-4)^3$$

$$G(x)^{(n)} = \frac{1}{2} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdot \dots \cdot \frac{-(2n-3)}{2} \cdot (1-4x)^{-\frac{(2n-1)}{2}} \cdot (-4)^n$$

Skąd mamy, że:

$$G(0)^{(n+1)} = \frac{1}{2} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdot \dots \cdot \frac{-(2n-1)}{2} \cdot (1-0)^{-\frac{(2n+1)}{2}} \cdot (-4)^{n+1}$$

$$G(0)^{(n+1)} = \frac{1}{2} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdot \dots \cdot \frac{-(2n-1)}{2} \cdot (-4)^{n+1}$$

$$G(0)^{(n+1)} = \frac{1}{2^{n+1}} \cdot ((-1) \cdot (-3) \cdot (-5) \dots (-(2n-1))) \cdot (-4)^{n+1}$$

Minusów jest nieparzyście wiele jak się nad tym poduma, więc:

$$G(0)^{(n+1)} = -\frac{1}{2^{n+1}} \cdot (1 \cdot 3 \cdot 5 \dots (2n-1)) \cdot 4^{n+1}$$

$$G(0)^{(n+1)} = -2^{n+1} \cdot (1 \cdot 3 \cdot 5 \dots (2n-1))$$

Teraz dzielimy przez $(n+1)!$:

$$g_{n+1} = -\frac{2^{n+1} \cdot (1 \cdot 3 \cdot 5 \dots (2n-1))}{(n+1)!}$$

Wstawiamy do wzoru na c_n :

$$c_n = \frac{2^n \cdot (1 \cdot 3 \cdot 5 \dots (2n-1))}{(n+1)!}$$

Mnożymy licznik i mianownik przez $n!$:

$$c_n = \frac{n! \cdot 2^n \cdot (1 \cdot 3 \cdot 5 \dots (2n-1))}{(n+1)! \cdot n!}$$

Każdy z elementów iloczynu $n!$ mnożymy razy 2 (z elementem 2^n):

$$c_n = \frac{(2 \cdot 4 \cdot 6 \dots 2n) \cdot (1 \cdot 3 \cdot 5 \dots (2n-1))}{(n+1)! \cdot n!}$$

Teraz zauważamy że jak wymnożymy licznik to już mamy po prostu $(2n)!$

$$c_n = \frac{(2n)!}{(n+1)! \cdot n!}$$

I ostatecznie

$$c_n = \frac{1}{n+1} \cdot \frac{(2n)!}{n! \cdot n!} = \frac{1}{n+1} \cdot \binom{2n}{n}$$

Kurczę szlaczek, skądś kojarzę ten wzór.

6.4 Zliczanie podziałów

Chcemy pokazać fajny algorytm zliczania wszystkich podziałów liczby n .

Oznaczmy liczbę wszystkich podziałów liczby n jako $p(n)$. Jako „podziały liczby n ” mam na myśli liczbę sposobów na podzielenie liczby n na ileś składników (niezerowych), np. liczbę 2

mogę rozłożyć na $1 + 1$ albo po prostu na 2 (i w sumie to tyle). Funkcja tworząca ciągu p_n to:

$$P(x) = (1 + x + x^2 + x^3 + \dots) \cdot (1 + x^2 + x^4 + x^6 + \dots) \cdot (1 + x^3 + x^6 + x^9 + \dots) \dots$$

Pierwszy nawias odpowiada wybraniu jedynki do podziału (i temu ile razy ją bierzemy), drugi dwójki, trzeci trójki, etc.

Oczywiście przy x^n będziemy mieli p_n , jak to działa w funkcjach tworzących (i mam nadzieję, że widać dlaczego). Zapisujemy $P(x)$ w fajniejszej postaci:

$$P(x) = \frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \dots$$

Definiuję sobie $Q(x) = (1-x) \cdot (1-x^2) \cdot (1-x^3) \dots$. Zauważam, że $P(x) \cdot Q(x) = 1$, czyli $Q(x)$ jest funkcją odwrotną do $P(x)$. Okazuje się teraz, że $Q(x)$ jest funkcją tworzącą pewnego śmiesznego ciągu, który sobie zaraz pokażemy.

Póki co musimy wprowadzić oznaczenia:

1. e_n jest to liczba podziałów liczby n na parzystą liczbę składników parami różnych,
2. o_n jest to liczba podziałów liczby n na nieparzystą liczbę składników parami różnych.

Jak wszyscy powinniśmy już wiedzieć, funkcja tworząca ciągu $e_n + o_n$ (czyli po prostu wszystkich podziałów n ze składnikami parami różnymi) wygląda tak:

$$(1+x) \cdot (1+x^2) \cdot (1+x^3) \dots$$

Ten fakt do niczego nam się w sumie nie przyda, ale może pomóc zrozumieć co zaraz się stanie.

Możemy sobie teraz podumać, jaka jest funkcja tworząca ciągu $e_n - o_n$. Otóż pojawia się tu plot twist, bo funkcja tworząca tego ciągu to po prostu $Q(x)$:

$$(1-x) \cdot (1-x^2) \cdot (1-x^3) \dots$$

Działa to tak jak w powyższym przykładzie, z tym że jeśli wybraliśmy nieparzyście wiele składników to będzie nieparzyście wiele minusów i się „odejmie” od współczynnika przy x^n , a jeśli będzie parzyście wiele to się „doda”. Innymi słowy, do współczynnika przy x^n doda się 1 za każdy możliwy podział na parzyście wiele parami różnych składników, a odejmie się 1 za każdy możliwy podział na nieparzyście wiele parami różnych składników, czyli to co chcemy. Nie do końca mam pomysł jak to formalnie wytłumaczyć, więc proszę użyć swojej intuicji™.

Po co to wszystko? Okazuje się, że ciąg $q_n = e_n - o_n$ ma pewne śmieszne własności (które niestety będzie trzeba udowodnić, brace yourselves).

Twierdzenie 6.4.1 (Eulera).

$$q_n = \begin{cases} 0, & \text{gdy } n \neq \frac{(3 \cdot k \pm 1) \cdot k}{2} \\ (-1)^k & \text{wpp.} \end{cases} \quad (6.2)$$

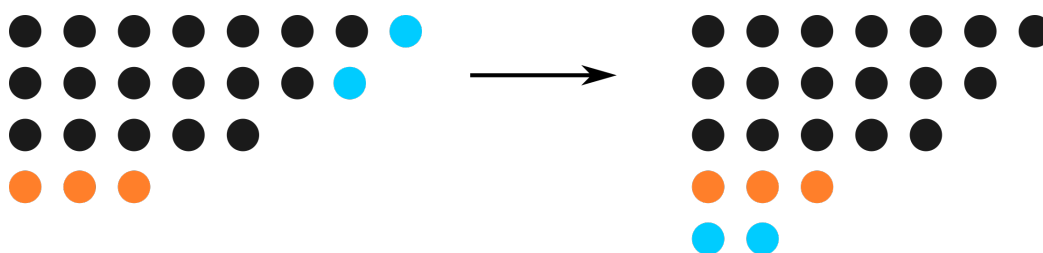
Dowód. Zrobimy sobie przekształcenie f , które przesyła prawie (dlaczego prawie to dojdziemy do tego za chwilę) każdy podział na n składników parami różnych na inny podział na n składników parami różnych (bijektywnie). Ktoś powie że sobie zrobiłem świetną bijekcję idącą z pewnego zbioru w samego siebie, but hear me out: ta bijekcja będzie mieć tę śmieszną własność, że jeśli podział był na parzyście wiele składników to będzie przesłany na nieparzyście wiele, a jeśli na nieparzyście wiele to będzie przesłany na parzyście wiele składników. To będzie fajne, bo pokażemy sobie że jest ich tyle samo (poza przypadkami gdzie definicja tej funkcji się popsuje, ale o tym za chwilę).

Generalnie to oznaczmy sobie najmniejszy składnik w podziale P jako a . Ponadto, zdefiniujmy sobie zbiór X , taki że zawiera on największe składniki podziału P , takie że każde dwa sąsiednie różnią się o jeden. Innymi słowy, jeśli podział $P = (\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_k)$, to $X = \{\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_d\}$, gdzie d jest największą liczbą taką, że kolejne składniki różnią się o 1 (zakładamy, że $\lambda_1 > \lambda_2 > \dots > \lambda_k$).

Teraz jak mamy te zbiory zdefiniowane to możemy robić śmieszne rzeczy. Jeśli $|X| < a - 1$, to możemy przerobić nasz podział, odejmując od każdego elementu z X 1, i dorzucając nowy element do podziału, taki że równy jest on moc $|X|$. Otrzymaliśmy oczywiście poprawny podział (niektórym może pomóc dowód przez rysowanie).

Dlaczego $|X| < a - 1$, a nie po prostu $|X| < a$? Otóż przychodzi tutaj pewien śmieszny problem, mianowicie może być tak, że składnik podziału o wartości a „wpadł” do X . W takim przypadku bijekcja nam się kompletnie popsuje i wtedy jej definiujemy (ale jeszcze do tego wrócimy). Natomiast jeśli a nie należy do $|X|$ to nasza bijekcja nadal działa. Fajnie.

Czyli reasumując: jeśli $|X| < a - 1$ lub ($|X| = a - 1$ i $a \notin X$) od każdego składnika z $|X|$ odejmujemy 1 i majstrujemy nowy składnik, który wrzucamy pod składnik o wartości a , który uprzednio był najmniejszy.

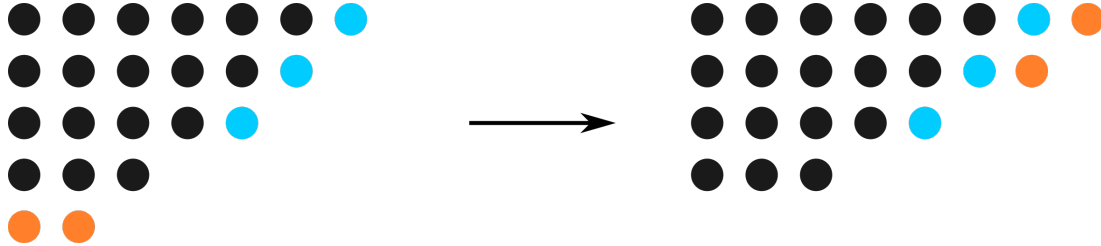


Rysunek 6.1: Wizualizacja przekształcenia (diagram Ferrersa). 2 „górne” składniki różnią się o 1, trzeci już różni się od nich o 2; $|X| = 2$, $a = 3$.

Zasadniczo to samo będziemy czynić (ale w drugą stronę), gdy okaże się że $a < |X|$. Ordynarnie

wywalam składnik a i do odpowiedniej liczby elementów z X „dodaję” 1, tak by się wyrównało. Należy zauważyć, że być może nie wszystkie elementy z X będą mieć coś do siebie dodane, ale to mi nic nie psuje. W sumie też fajnie byłoby dodać, że dodaję te jedynki najpierw największym składnikom; inaczej mogłoby to się popsuć.

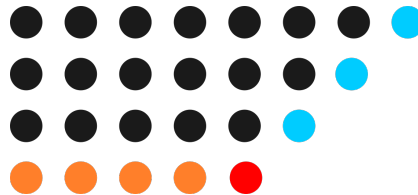
Co dzieje się, gdy $a = |X|$? Jeśli $a \in X$ to jest mi smutno, w przeciwnym razie mogę zrobić to samo co robiłem wcześniej i wszystko działa jak powinno.



Rysunek 6.2: Wizualizacja przekształcenia (diagram Ferrersa). 3 „górne” składniki różnią się o 1 więc należą do X . $|X| = 3$, $a = 2$, więc dwóm największym elementom dodajemy 1, a składnik a usuwamy.

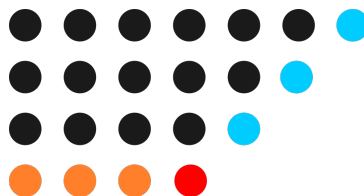
Zostają więc 2 przypadki, gdy coś może się popsuć:

1. $|X| = a - 1$, $a \in X$



Rysunek 6.3: Gdy $|X| = a - 1$ i składnik a jest w X ; widać, że nic nie możemy z tym zrobić.

2. $|X| = a$, $a \in x$



Rysunek 6.4: Gdy $|X| = a$ i składnik a jest w X ; również widać, że nasze przekształcenie nie zadziała.

Zauważmy, że sytuacja gdy składnik a jest w X jest bardzo dziwną sytuacją generalnie, bo jest to najmniejszy składnik; z definicji X mamy wtedy, że wszystkie kolejne składniki w P różnią się o dokładnie 1. Na podstawie tej obserwacji możemy już dokładnie powiedzieć, jakiej postaci musi być n , by miało taki „złośliwy” podział:

1. Gdy $|X| = a - 1$, $a \in X$, to n musi dla jakiegoś k być postaci $(k+1) + (k+2) + \dots + 2k$ ($|X| = k$, $a = k+1$, wszystko się zgadza)
2. Gdy $|X| = a$, $a \in x$, to n musi dla jakiegoś k być postaci $k + (k+1) + (k+2) + \dots + (2k-1)$ ($|X| = k$, $a = k$, ponownie wszystko gra)

Jak zastosujemy matematykę mniej dyskretną by wysumować te nawiasy, dostaniemy że n aby miało irytujący podział to musi być postaci $\frac{k \cdot (3k+1)}{2}$ lub $k \cdot (3k-1)2$. Jednocześnie nie ma takiego naturalnego k , że wartości te są sobie równe, więc jeśli n ma irytujący podział, to ma go tylko jednego. Wtedy nie możemy przerzucić tylko jednego podziału na inny (inne są ze sobą w bijekcji) więc $e_n - o_n = (-1)^k$ (jeśli k jest parzyste to irytujący podział ma parzyście wiele składników, a w przeciwnym razie nieparzyście wiele). Jeśli irytujący podział nie występuje, $e_n = o_n$ z bijekcji którą pokazaliśmy. Fajnie. \square

Dobra, ale wróćmy do tego cośmy chcieli udowodnić na samym początku. Co w ogóle wynika z tego twierdzenia Eulera? No w sumie to bardzo dużo, bo jak mamy $q_n = e_n - o_n$ i $Q(x)$ jest jego funkcją tworzącą:

$$Q(x) = q_0 + q_1 \cdot x + q_2 \cdot x^2 + q_3 \cdot x^3 + \dots$$

Ale znamy wartości współczynników q_i z twierdzenia Eulera:

$$Q(x) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} + \dots$$

Zauważmy, że współczynników które nie są zerowe jest tylko jakoś $O(\sqrt{n})$, czyli dosyć mało.

Pamiętajmy, że $P(x) \cdot Q(x) = 1$, czyli że ciąg który wyjdzie po ich wymnożeniu będzie wyglądać tak: $(1, 0, 0, 0, \dots)$ Ponieważ mnożenie w funkcjach tworzących działa jakoś tak, że w wynikowym ciągu (nazwijmy go r) element r_n można obliczyć w ten sposób:

$$r_n = \sum_{i=0}^n p_i \cdot q_{n-i}$$

I wiemy że w naszym przypadku $r_n = 0$ dla $n > 1$, to mamy że:

$$0 = p_n - p_{n-1} - p_{n-2} + p_{n-5} + p_{n-7} - p_{n-12} - \dots$$

To teraz p_n przerzucamy na drugą stronę i mnożymy stronami razy -1 i mamy wzór na p_n , które możemy obliczyć w $O(\sqrt{n})$. No i fajnie.

Rozdział 7

Przepływy

7.1 Definicje

Na egzaminie nie będzie przepływów,
prawda?

Student TCSu na dzień przed katastrofą

Zazwyczaj nie zajmuję się definiowaniem bo zakładam, że definicje są już znane, ale w przypadku sieci przepływowych zrobię wyjątek, bo na egzaminach pojawiają się pytania proszące o zdefiniowanie wszystkich pojęć z przepływów.

Źródło to wyróżniony wierzchołek, z którego krawędzie mogą jedynie „wychodzić” (graf jest skierowany).

Ujście to wyróżniony wierzchołek, do którego krawędzie mogą jedynie „wchodzić”.

c jest to funkcja przepustowości, idąca ze zbioru krawędzi w liczby naturalne > 0 (tak po ludzku to mówiona jaką przepustowość ma dana krawędź).

Przepływem całkowitoliczbowym nazywamy funkcję f przyporządkowującą każdej krawędzi jakąś liczbę naturalną mniejszą lub równą jej przepustowości. Dla każdego wierzchołka który nie jest źródłem lub przepływem jest tak, że suma po funkcjach przepływów krawędzi do niego wchodzących jest równa sumie po funkcjach przepływów do niej wchodzących (co w sumie jest dosyć oczywiste, studenci zafiksowani na fizyce gadają tam o jakichś prawach kirchoffa i nie wiem o co im chodzi; studiuje TCS, nie prawo).

Przekrojem sieci przepływowej S nazywamy jej „podział” na 2 zbiory wierzchołków jej grafu (S, T) , taki, że:

1. $S \cup T = V$

2. $S \cap T = \emptyset$

3. Źródło jest w S

4. Ujście jest w T

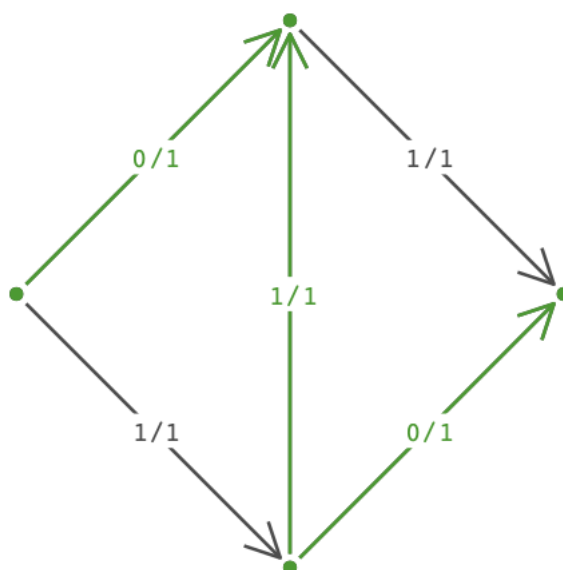
Przepustowością przekroju, również oznaczaną przez c (co generuje bałagan w oznaczeniach, ale to nie ja je wymyślałem) nazywamy sumę po przepustowościach wszystkich krawędzi wychodzących z S .

Przepływem przez przekrój nazywamy sumę po wartości funkcji f dla wszystkich krawędzi które „wychodzą” z S pomniejszoną o sumę po wartości funkcji f dla wszystkich krawędzi, które „wchodzą” do S (co jest dosyć intuicyjne, po prostu to co wypływa z S minus to co wpływa).

Przekrojem minimalnym nazywamy przekrój o minimalnej przepustowości. Od razu można też zauważyć, że przepustowość sieci (w sensie to ile maksymalnie może wpłynąć do ujścia) jest mniejsza lub równa od przepustowości przekroju minimalnego. Dowodzi się to za pomocą dowodu *to widać*. Formaliści mogą sobie nad tym podumać.

Ścieżką powiększającą w przepływie nazywamy zbiór krawędzi który będzie stanowić ścieżkę jeśli pominiemy ich skierowanie; generalnie to działa tak że musi ona iść od jakiegoś wierzchołka v do innego wierzchołka u ; zazwyczaj idzie ona od źródła do ujścia. Jeśli dana krawędź idzie „do przodu” to przepływ na niej nie może być równy przepustowości; jeśli idzie „do tyłu” musi być niezerowy. Dlaczego to tak nazywamy? Bo jak do wszystkich krawędzi idących „do przodu” dodamy 1 a od wszystkich idących „do tyłu” odejmiemy 1 (a ścieżka szła od źródła do ujścia) to nadal mamy poprawny przepływ, w którym dodatku do ujścia wchodzi jedna jednostka więcej.

Przez $val(f)$ czasem będziemy oznaczać to, ile w danym przepływie wpływa do ujścia (i będziemy starali się maksymalizować tę wartość).



Rysunek 7.1: Przykład ścieżki powiększającej w sieci przepływowej

7.2 Własności przekrojów i przepływów

Twierdzenie 7.2.1 (Oczywiste twierdzenie o przekrojach). Dla dowolnego przepływu w sieci przepływowej f i dla dowolnego jej przekroju (S, T) jest tak, że przepływ przez przekrój jest słabo mniejszy niż jego przepustowość (tzn. $f(S, T) \leq c(S, T)$).

Dowód. To widać. W sensie serio, gdyby suma po przepływach krawędzi wychodzących z S była większa niż suma po ich przepustowościach, to znaczyłoby że coś gdzieś poszło bardzo mocno nie tak. \square

Twierdzenie 7.2.2 (Mniej oczywiste twierdzenie o przekrojach). Przepływ przez każdy przekrój sieci jest taki sam i wynosi $val(f)$.

Dowód. Indukcja po liczbie wierzchołków w części S przekroju (tej do której należy źródło). Przypadek bazowy gdy $|S| = 1$ trywialny. W przypadku ogólnym mamy sobie jakiś przekrój (S, T) . Weźmy teraz jakiś $x \in S$ (różny od źródła, na pewno taki jest bo dla przypadku gdzie jest tylko jeden wierzchołek w S mamy to już udowodnione) i wrzucmy go do T , otrzymując alternatywny przekrój (S', T') . Teraz jest śmiesznie, bo wiemy z założenia indukcyjnego że przepływ przez $(S', T') = val(f)$, bo S' ma mniejszą moc od S . Rozpiszmy sobie teraz $f(S', T')$ oraz $f(S, T)$ (przez v_s etc. oznaczam wierzchołek należący do S lub innych zbiorów):

$$f(S, T) = \sum_{(v_s, v_t) \in E, v_s \neq x} f(v_s, v_t) + \sum_{(x, v_t) \in E} f(x, v_t) - \sum_{(v_t, v_s) \in E, v_s \neq x} f(v_t, v_s) - \sum_{(v_t, x) \in E} f(v_t, x)$$

Jako że jeśli punkt $v \in S$ oraz $v \neq x$, to $v \in S'$, możemy to uprościć i zapisać jako:

$$f(S, T) = \sum_{(v_{s'}, v_t) \in E} f(v_{s'}, v_t) + \sum_{(x, v_t) \in E} f(x, v_t) - \sum_{(v_t, v_{s'}) \in E} f(v_t, v_{s'}) - \sum_{(v_t, x) \in E} f(v_t, x)$$

$$f(S', T') = \sum_{(v_{s'}, v_{t'}) \in E, v_{t'} \neq x} f(v_{s'}, v_{t'}) + \sum_{(v_{s'}, x) \in E} f(v_{s'}, x) - \sum_{(v_{t'}, v_{s'}) \in E, v_{t'} \neq x} f(v_{t'}, v_{s'}) - \sum_{(x, v_{s'}) \in E} f(x, v_{s'})$$

Jako, że jeśli punkt $v \in T'$ oraz $v \neq x$, to wiemy że $v \in T$:

$$f(S', T') = \sum_{(v_{s'}, v_t) \in E} f(v_{s'}, v_t) + \sum_{(v_{s'}, x) \in E} f(v_{s'}, x) - \sum_{(v_t, v_{s'}) \in E} f(v_t, v_{s'}) - \sum_{(x, v_{s'}) \in E} f(x, v_{s'})$$

To wygląda przerażająco, ale w sumie wynika wprost z definicji przepływu, po prostu dodajemy te wszystkie krawędzie do siebie. Zasadniczo nic ciekawego. Co teraz jest fajne to to, że możemy policzyć $f(S, T) = f(S', T')$ (zwróćmy uwagę, że pierwszy i trzeci składnik się uproszcza (co w sumie ma sens, bo jedyne co zmienialiśmy to pozycja x , więc to co przepływa w reszcie grafu się nie zmieniło – ależ plot twist), zostawiając tylko składniki z x).

$$f(S, T) - f(S', T') = \sum_{(x, v_t) \in E} f(x, v_t) - \sum_{(v_{s'}, x) \in E} f(v_{s'}, x) - \sum_{(v_t, x) \in E} f(v_t, x) + \sum_{(x, v_{s'}) \in E} f(x, v_{s'})$$

Jako, że do x wpływa tyle samo co wypływa:

$$\begin{aligned} f(S, T) - f(S', T') &= \sum_{(x, v_t) \in E} f(x, v_t) - \sum_{(v_t, x) \in E} f(v_t, x) + \sum_{(x, v_{s'}) \in E} f(x, v_{s'}) - \sum_{(v_{s'}, x) \in E} f(v_{s'}, x) \\ &= 0 + 0 = 0 \end{aligned}$$

Skąd mamy szokujące odkrycie, że $f(S, T) = f(S', T')$. Ale przecież $f(S', T')$ było równe $val(f)$, czyli wszystko się zgadza. \square

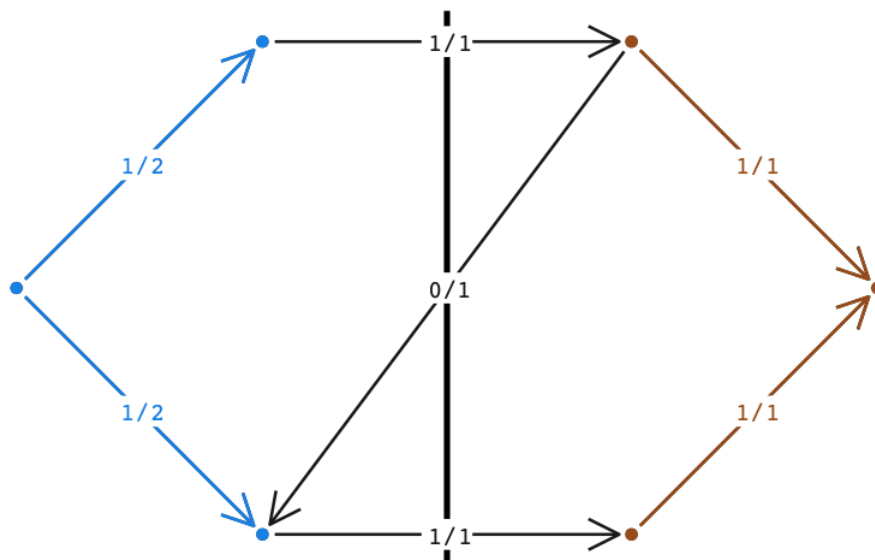
7.3 Twierdzenie Forda-Fulkersona

Twierdzenie 7.3.1. Następujące warunki są równoważne:

1. f jest przepływem maksymalnym
2. W sieci przepływowej nie istnieje ścieżka powiększająca od źródła do ujścia
3. Przekrój (S, T) taki, że S zawiera wszystkie wierzchołki do których istnieje ścieżka powiększająca od źródła, jest poprawnie zdefiniowanym przekrojem, spełniającym warunek $f(S, T) = c(S, T)$

Dowód. Trzeci warunek brzmi strasznie, ale tak naprawdę taki nie jest. Zajmijmy się poszczególnymi implikacjami celem udowodnienia równoważności:

1. (1) \implies (2): Trywialne do udowodnienia, gdyby f było przepływem maksymalnym a istniałaby ścieżka powiększająca od źródła do ujścia to mógłbym zwiększyć wartość przepływu o 1 za jej pomocą, a więc przepływ ten nie byłby maksymalny.
2. (2) \implies (3): Ładnie się to dowodzi, stosując dowód przez rysowanie. Idea generalnie jest taka, że poprawność przekroju podanego w (3) wynika nam z tego, że z (2) mamy że nie istnieje ścieżka powiększająca od źródła do ujścia, a więc ujście na pewno będzie T . Źródło na pewno będzie w S , oczywiście. Pozostałe warunki dla przekroju oczywiście będą spełnione, więc mamy że (S, T) to poprawnie zdefiniowany przekrój. Jak teraz sobie spojrzymy na wszystkie krawędzie wchodzące i wychodzące z S to odkrywamy, że skoro nie ma ścieżki powiększającej która wychodziłaby poza S , to wszystkie krawędzie wychodzące muszą być w pełni wysyczone, a wszystkie wchodzące wyzerowane (inaczej moglibyśmy dorzucić wierzchołek z T do S , zgodnie z definicją naszego przekroju). No a skoro tak jest, to mamy że $f(S, T) = c(S, T)$; innymi słowy przepływ przez przekrój jest równy jego przepustowości.



Rysunek 7.2: Przekrój (S, T) taki, że do S należą wszystkie wierzchołki, do których idzie ścieżka powiększająca (zaznaczone na niebiesko). Nie jest możliwe poprowadzenie ścieżki powiększającej dalej, a więc krawędzie albo są maksymalnie wysycane (jeśli idą z S do T) albo wyzerowane (jeśli idą z T do S) (zaznaczone na czarno).

3. (3) \implies (1): Ponieważ $val(f)$ musi być mniejsze niż przepustowość dowolnego przekroju, co zauważyliśmy już przy etapie definicji pojęć (a formalisci mam nadzieję że już dowiedli, o ile nadal nie zastanawiają się co to jest liczba parzysta), a z (3) mamy, że przekrój (S, T) spełnia $f(S, T) = c(S, T)$ to mamy że przepływ ten jest maksymalny (no w sensie większego przepływu nam się nie uda zrobić, skoro właśnie osiągnęliśmy limit).

Z powyższego dowodu oczywiście również wynika, że przepustowość minimalnego przekroju jest równa $val(f)$. \square

Rozdział 8

Skojarzenia

8.1 Twierdzenie Halla

Dlaczego wysoki odsetek pracowników służby drogowej ma rodziny? Bo dużo Hall'ują.

Niezwykłe suchy żart pewnego studenta

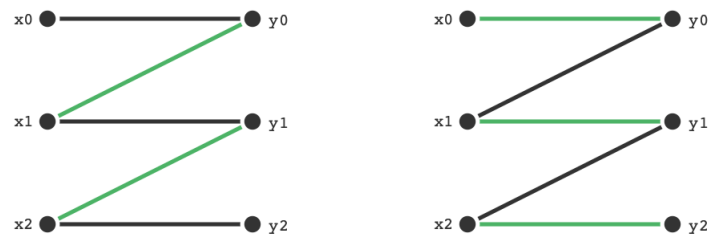
Twierdzenie 8.1.1 (Halla). Graf dwudzielny $G = (X, Y, E)$, gdzie $|X| = |Y|$ ma dopasowanie doskonałe wtedy i tylko wtedy, gdy dla dowolnego $A \subset X$ zachodzi:

$$|A| \leq |N(A)| \quad (8.1)$$

Dowód. Ponieważ twierdzenie mówi *wtedy i tylko wtedy*, musimy udowadniać w dwie strony. Zaczniemy od tej prostszej strony, czyli pokażemy że gdy graf dwudzielny w którym $|X| = |Y|$ ma dopasowanie doskonałe to $|A| \leq |N(A)|$. Zasadniczo od razu to widać, bo skoro dopasowanie doskonałe istnieje to wystarczy sobie je wziąć. Każdy wierzchołek z $|X|$ ma wówczas jakąś krawędź do wierzchołka z $|Y|$. Zauważamy, że siłą rzeczy w samym dopasowaniu (czyli jakimś podgrafe oryginalnego grafu dwudzielnego, z którego być może „wywalono” jakieś krawędzie) jest tak, że $|A| = |N(A)|$, z czego w szczególności wynika teza. To chyba widać.

W drugą stronę jest ciekawiej, bo po pierwsze musimy sobie wprowadzić instytucję *ścieżki powiększającej*. Nie należy tego mylić ze ścieżką powiększającą z przepływów, bo one mówią o innych rzeczach (ale idea jest ta sama). Generalnie to założmy sobie, że mam jakieś dopasowanie M które nie jest doskonałe. Oznacza to, że w X jest jakiś wierzchołek x_0 poza dopasowaniem. Jeśli x_0 łączy się z jakimś wierzchołkiem $y_0 \in Y$ i $y_0 \in M$. y łączy się z jakimś $x_1 \in M$ (bo są razem w dopasowaniu). Teraz jeśli x_1 łączy się z jakimś $y_1 \in Y$ takim, że $y_1 \notin M$ to ja to dopasowanie mogę przerobić: „połączyć” x z y i x_1 z y_1 , dorzucając dodatkowy wierzchołek do dopasowania. To jest przykład bardzo krótkiej ścieżki powiększającej, ale generalna idea to jest taki „zygzak” którego można przerobić, żeby dopasowanie powiększyło się

o jeden wierzchołek. At this point wszyscy już chyba wiedzą, że zamiłowania do formalizmu to ja nie mam.



Rysunek 8.1: Ścieżka powiększająca przed i po zamianie krawędzi

No dobra, ale co ma ścieżka powiększająca do twierdzenia Halla? Okazuje się że jest ona bardzo wygodnym narzędziem.

Założmy sobie nie wprost, że mamy jakiś graf dwudzielny $G = (X, Y, E)$, w którym zachodzi warunek Halla ale nie ma dopasowania doskonałego. W takim razie weźmy dopasowanie maksymalne M . Istnieje jakiś x , który nie należy do tego dopasowania (bo nie jest doskonałe). Z warunku Halla ($|A| \leq |N(A)|$ dla dowolnego $A \subset X$) mam, że x musi mieć jakiegoś sąsiada w Y . Zbiór wszystkich wierzchołków, z którymi połączony jest x (być może jest ich więcej, być może tylko jeden) oznaczam jako B_0 . Każdy wierzchołek z B_0 musi należeć do dopasowania M (bo inaczej mógłbym je rozszerzyć, biorąc krawędź między tym wierzchołkiem a x). Wszystkie wierzchołki z X które są razem w dopasowaniu z wierzchołkami z B_0 oznaczam jako A_1 . Oczywiście $|A_1| = |B_0|$. Zauważmy, że $|A_1 \cup \{x\}| \geq |B_0|$, a zatem musi istnieć jakiś zbiór wierzchołków B_1 który ma krawędzie do wierzchołków zbioru A_1 . Ponownie, wszystkie krawędzie z B_1 muszą być w dopasowaniu, bo inaczej mielibyśmy ścieżkę powiększającą (aha!) od x do jakiegoś wierzchołka z B_1 . W takim razie mamy jakiś zbiór A_2 wierzchołków które są w dopasowaniu z wierzchołkami z B_1 , ponownie $|A_2| = |B_1|$. $|A_2| + |A_1| + 1 \geq |B_0| + |B_1|$, skąd wierzchołki z A_2 łączą się jeszcze z jakimiś innymi wierzchołkami z Y , ich zbiór nazwiemy B_2 . I ponownie, wierzchołki z B_2 muszą być w dopasowaniu, bo inaczej mielibyśmy ścieżkę powiększającą. Korzystamy teraz z faktu który zawsze zakładamy, tj. faktu że grafy są skończone.

I tak dalej, aż do wyczerpania zasobów

Stefan „Siara” Siarzewski do senatora

Ferdynanda Lipskiego, „Kilerów-ów

2-óch”

Nietrudno bowiem zauważyć, że w końcu wierzchołki się skończą i albo dostaniemy sprzeczność z założeniem że warunek Halla zachodzi, albo wyjdzie nam ścieżka powiększająca (a dopasowanie miało być maksymalne). Tym samym kończymy dowód. \square

8.2 Macierz symboliczna Tutte’a

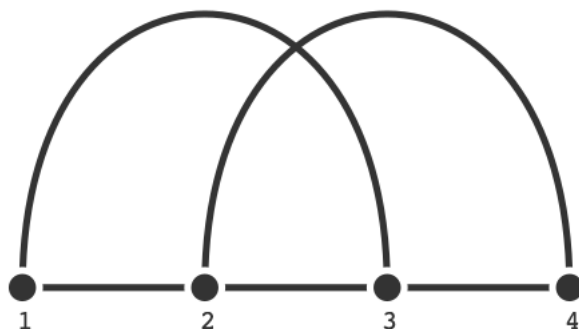
Twierdzenie Hall’a jest fajne, ale niestety działa tylko w grafach dwudzielnych. Przydałby się nam jakiś warunek, który mówi o istnieniu dopasowania doskonałego w *dowolnym* grafie.

Powiedzmy, że mamy graf G o n wierzchołkach. Dla uproszczenia będziemy te wierzchołki traktować jako liczby ze zbioru $[n]$, bo wyjdzie na to samo. Dla każdej krawędzi $\{i, j\}$, gdzie $i < j$, zrobimy sobie pewną zmienną, którą będziemy oznaczać x_{ij} . Za chwilę wyjaśni się, co to dokładnie znaczy. Następnie zdefiniujemy sobie tzw. *macierz symboliczną Tutte’a*. Jest to

macierz $n \times n$, a wypełniamy ją zgodnie z poniższą regułą:

$$M_G[i, j] = \begin{cases} 0 & \iff \{i, j\} \notin E(G) \\ x_{ij} & \iff \{i, j\} \in E(G) \wedge i < j \\ -x_{ij} & \iff \{i, j\} \in E(G) \wedge i > j \end{cases}$$

Przykładowo, dla takiego grafu:



będzie

$$M_G = \begin{bmatrix} 0 & x_{12} & x_{13} & 0 \\ -x_{12} & 0 & x_{23} & x_{24} \\ -x_{13} & -x_{23} & 0 & x_{34} \\ 0 & -x_{24} & -x_{34} & 0 \end{bmatrix}$$

Zwróćmy uwagę, że jest to macierz skośnie symetryczna.

Prawdziwe okazuje się:

Twierdzenie 8.2.1. Graf G ma dopasowanie doskonałe wtedy i tylko wtedy, gdy wyznacznik symboliczny macierzy M_G jest niezerowy.

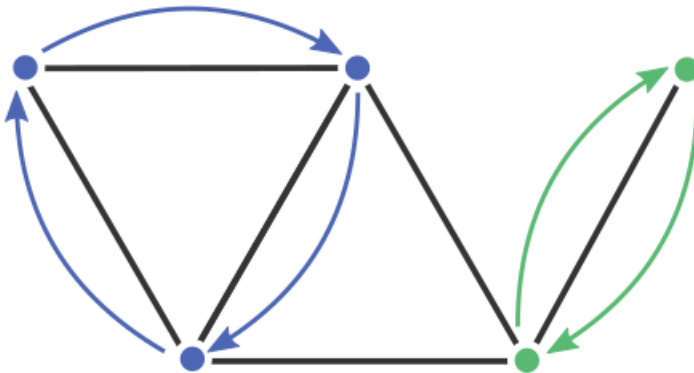
Spokojnie, powoli... Wyjaśnijmy sobie najpierw, czym jest ten wyznacznik symboliczny. Wyznacznik macierzy będzie (z definicji) czymś takim:

$$\det(M_G) = \sum_{\pi \in S_n} \text{sgn}(\pi) \cdot \left(\prod_{i=1}^n M_G[i, \pi(i)] \right)$$

Gdyby w naszej macierzy M_G były konkretne liczby, to wyznacznik byłby po prostu wartością

tego wyrażenia. Ale w naszej macierzy są bliżej nieokreślone (na razie) zmienne, więc będziemy to wyrażenie traktować jako wielomian tych wszystkich zmiennych x_{ij} odpowiadających krawędziom i nazwać *wyznacznikiem symbolicznym*. Przez jego „niezerowość” rozumiemy, że ten wielomian nie jest tożsamościowo równy zero. Skoro wyjaśniliśmy już, o czym mówi to (na pierwszy rzut oka losowe) twierdzenie, to możemy przystąpić do jego dowodzenia.

Dowód. Najpierw zaobserwujmy, o czym mówi nam wyznacznik symboliczny. Iterujemy się tam po wszystkich permutacjach $\pi \in S_n$. Wiadomo, że każda permutacja rozkłada się na rozłączne cykle. Okazuje się, że każda permutacja, dla której wyrażenie pod sumą się nie zeruje, odpowiada pewnemu skierowanemu pokryciu cyklowemu G . Co to jest pokrycie cyklowe? Najprościej mówiąc: bierzemy sobie kilka rozłącznych wierzchołkowo cykli w G w taki sposób, żeby każdy wierzchołek G należał do jakiegoś wybranego cyklu. Ponieważ mówimy o *skierowanym* pokryciu cyklowym, to jedna krawędź nieskierowana może się liczyć jako cykl długości 2, z krawędziami skierowanymi w obydwie strony. Poniżej przykładowy graf i pewne jego pokrycie cyklowe:

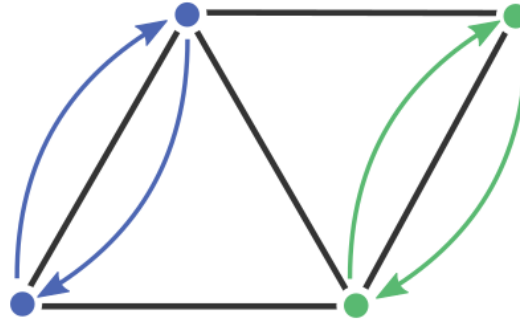


Rysunek 8.2: Przykładowe pokrycie cyklowe

Mając tę intuicję, faktycznie widzimy, że permutacja π , dla której wyrażenie pod sumą się nie zeruje, odpowiada pokryciu cyklowemu. Gdyby bowiem nie było to pokrycie cyklowe, to nie istniałaby w G któraś krawędź postaci $(i, \pi(i))$. Ale wtedy, z definicji M_G , byłoby $M_G[i, \pi(i)] = 0$, czyli jednak składnik odpowiadający π zerowałby się. Zatem tak naprawdę:

$$\det(M_G) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot \left(\prod_{i=1}^n M_G[i, \pi(i)] \right) = \sum_{\substack{\pi \in S_n \\ \pi \text{ — pokr. cykl. } G}} \operatorname{sgn}(\pi) \cdot \left(\prod_{i=1}^n M_G[i, \pi(i)] \right)$$

Z tego od razu możemy wyprowadzić dowód w jedną stronę. Załóżmy, że istnieje skojarzenie doskonałe w G i, bez straty ogólności, składa się ono z krawędzi $\{1, 2\}, \{3, 4\}, \dots, \{2k-1, 2k\}$, gdzie $2k = n$. Skoro to skojarzenie doskonałe, to te krawędzie nie dotykają się wierzchołkami, zatem możemy zrobić pokrycie wierzchołkowe transpozycjami $(1, 2), (3, 4), \dots, (2k-1, 2k)$, jak na poniższym rysunku:



Rysunek 8.3: Pokrycie cyklowe zrealizowane za pomocą transpozycji

W wyznaczniku symbolicznym składnik odpowiadający permutacji opisującej to pokrycie cyklowe będzie wyglądał następująco:

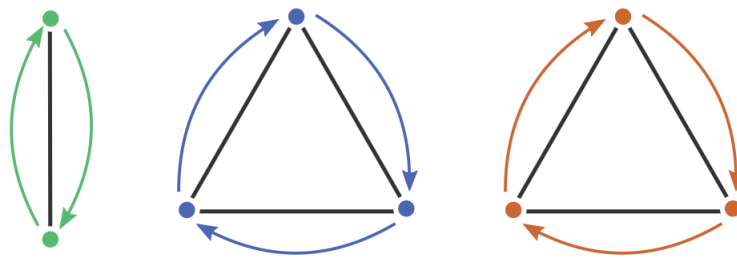
$$x_{12} \cdot (-x_{12}) \cdot x_{34} \cdot (-x_{34}) \cdot \dots \cdot x_{2k-1 \ 2k} \cdot (-x_{2k-1 \ 2k})$$

i po prostu widać, że nic się z tym nie zredukuje, bo są tu tylko transpozycje, więc jeśli nawet je odwrócimy to nic się nie zmieni — w szczególności znak tego wyrażenia. Zatem faktycznie wyznacznik symboliczny nie będzie tożsamościowo równy zero.

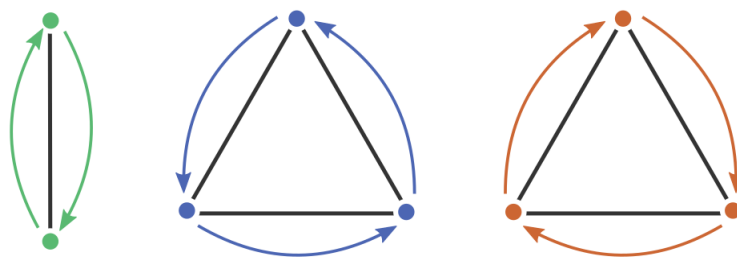
Dowód w drugą stronę, tzn.: jeśli wyznacznik symboliczny nie jest tożsamościowo równy zero, to mamy skojarzenie doskonałe, jest nieco bardziej skomplikowany, ale opiera się na naturalnej obserwacji:

$$\begin{aligned} \det(M_G) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot \left(\prod_{i=1}^n M_G[i, \pi(i)] \right) = \sum_{\substack{\pi \in S_n \\ \pi \text{ — pokr. cykl. } G}} \operatorname{sgn}(\pi) \cdot \left(\prod_{i=1}^n M_G[i, \pi(i)] \right) \\ &= \left(\sum_{\substack{\pi \in S_n \\ \pi \text{ — pokr. cykl. } G \\ \pi \text{ bez niep. cykli}}} \operatorname{sgn}(\pi) \left(\prod_{i=1}^n M_G[i, \pi(i)] \right) \right) + \left(\sum_{\substack{\pi \in S_n \\ \pi \text{ — pokr. cykl. } G \\ \pi \text{ ma niep. cykle}}} \operatorname{sgn}(\pi) \left(\prod_{i=1}^n M_G[i, \pi(i)] \right) \right) \end{aligned}$$

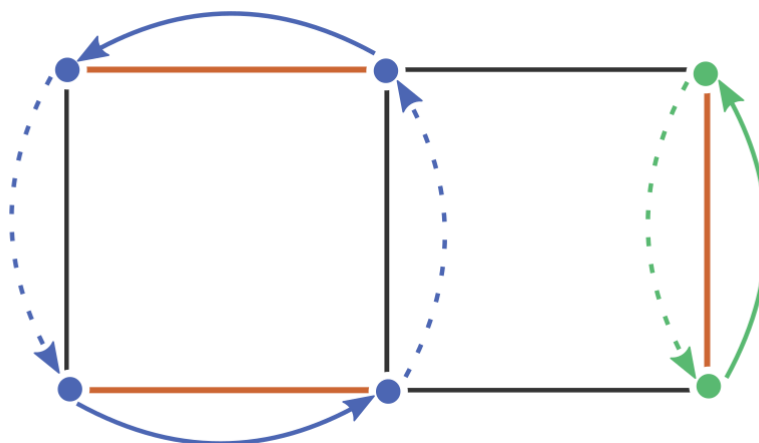
Jak nam to pomaga? Zauważmy, że druga suma się zeruje. Dlaczego? Otóż dla każdej permutacji, w której istnieje nieparzysty cykl, możemy wziąć nieparzysty cykl zawierający najmniejszą liczbą i go odwrócić. Np. z poniższej permutacji π :

Rysunek 8.4: Permutacja $\pi = (1, 2)(3, 4, 5)(6, 7, 8)$

powstanie permutacja π' :

Rysunek 8.5: Permutacja $\pi' = (1, 2)(5, 4, 3)(6, 7, 8)$

To przekształcenie jest oczywiście bijekcją (i dodatkowo inwolucją). Zauważmy też, że składnik sumy odpowiadający π' różni się tylko znakiem od składnika sumy odpowiadającego π — końce krawędzi przecież się nie zmieniły, jedynie dla każdej zmiennej odpowiadającej krawędzi zmienił się znak, bo krawędź zmieniła kierunek. A cykl był nieparzystej długości, co oznacza, że zmieniło się nieparzyste wiele znaków. Zatem składnik dla π zredukuje się ze składnikiem dla π' dla dowolnej permutacji π , w której istnieje nieparzysty cykl, czyli rzeczywiście cała druga suma się wyzeruje. Ale założyliśmy, że wyznacznik symboliczny jest niezerowy, czyli pierwsza suma jest niezerowa. Oznacza to, że istnieje pokrycie cyklowe G , w którym nie ma nieparzystych cykli — innymi słowy, są same parzyste. Zauważmy teraz, że ponieważ są to rozłączne cykle parzystej długości pokrywające G , to, biorąc co drugą krawędź z każdego takiego cyklu, otrzymamy dopasowanie doskonałe:



Rysunek 8.6: Pokrycie cyklowe oraz skojarzenie doskonałe; linia ciągła oznacza krawędź cyklu, którą bierzemy do skojarzenia

A to właśnie chcieliśmy pokazać!

□

Rozdział 9

Kolorowanie grafów

9.1 Liczba kolorująca

9.1.1 Co to w ogóle jest

Liczba kolorująca jest źródłem konfuzji dla niezliczonych studentów. Co ona w ogóle robi, po co jest i dlaczego nie ma jej w żadnej literaturze? Na to ostatnie pytanie nie odpowiem, ale liczba kolorująca, oznaczana również jako $col(G)$ jest użyteczna, bo, jak za niedługo pokażemy, ogranicza od góry $\chi(G)$ oraz da się ją obliczyć w czasie wielomianowym (na wypadek gdyby ktoś się jeszcze nie zorientował, kolorowanie grafów jest problemem klasy NP-przykrej). Poza tym jestem zdania, że nazwanie tego *liczba kolorująca* to fatalna decyzja, bo dosyć ładnie kamufluje co to w ogóle jest; w tym momencie chciałbym napisać coś śmiesznego o matematykach i dziwnych decyzjach, ale nic śmiesznego nie przychodzi mi do głowy.

9.1.1.1 Definicja

Rozpatrzmy wszystkie permutacje wierzchołków grafu G . Zdefiniujmy funkcję f , która dla każdego wierzchołka w obrębie danej permutacji przypisuje liczbę jego sąsiadów, którzy wystąpili „przed nim” w permutacji. Zdefiniujmy funkcję g , która dla danej permutacji wynosi maksymalnej wartości funkcji f policzonej dla wszystkich wierzchołków z tej permutacji i dodaje do tego jeden. Skąd wytrzasnęła się ta jedynka zaraz się dowiemy, obiecuję że to nie jest kolejny arbitralny wymysł matematyków którzy wypili za dużo kawy (tak jak nazwa tego bytu).

Fajnie teraz zauważyć, że g dla danej permutacji oszacowuje z góry jak bardzo może „sko-pać” kolorowanie algorytm First-Fit, jeśli pokoloruje wierzchołki zgodnie z tą permutacją; w najgorszym przypadku, gdy istnieje jakiś wierzchołek mający d sąsiadów „na lewo” i wszyscy mają różne kolory, to FF da mu kolor $d + 1$. Stąd maksymalna liczba sąsiadów na lewo wśród wierzchołków (+1) daje nam górne oszacowanie na to, jak First-Fit może popsuć kolorowanie *jeśli będzie kolorować według tej permutacji*.

Nikogo teraz chyba nie zdziwi fakt, że $col(G)$ to jest po prostu minimum po funkcjach g dla

wszystkich permutacji wierzchołków grafu G .

9.1.2 Relacja z liczbą chromatyczną

9.1.2.1 Ograniczenie liczby chromatycznej przez liczbę kolorującą

Twierdzenie 9.1.1 (Relacja liczby kolorującej z liczbą chromatyczną).

$$\chi(G) \leq col(G) \quad (9.1)$$

Dowód. Gdy tak nie było, to istniałaby taka permutacja wierzchołków grafu że First-Fit pokolorowałby graf lepiej niż $\chi(G)$ mówi, że da się pokolorować. Koniec dowodu. Serio. \square

9.1.2.2 Ograniczenie liczby kolorującej przez jakąś funkcję liczby chromatycznej

Nie da się. Znaczący da się, ale tylko w pewnych klasach grafów. W ogólnej klasie grafów istnieją takie grafy, że liczba kolorująca leci do nieskończoności, a $\chi(G) = 2$. Grafem takim jest na przykład klika dwudzielna $K_{n,n}$. Swoją drogą to jest protip: jeśli potrzebujesz udowodnić że $col(G)$ nie da się ograniczyć w jakiejś klasie grafów przez funkcję $\chi(G)$, spróbuj pokazać że da się tam skonstruować klikę dwudzielną. Nie ma za co.

9.1.3 Algorytm obliczania liczby kolorującej

Twierdzenie 9.1.2 (Magiczny wzór na liczbę kolorującą).

$$col(G) = \max\{\delta(H) : H \subset_{ind.} G\} + 1 \quad (9.2)$$

Dowód. Ten wzór wygląda na początku dziwnie, ale w sumie ma sens. Dowodzić to będziemy trochę dziwnie, bo zamiast pokazywać od razu równość, pokażemy ograniczenie z góry i z dołu (skąd będziemy mieć, że istotnie zachodzi równość).

Pokażmy zatem nierówność w pierwszą stronę:

$$col(G) \geq \max\{\delta(H) : H \subset_{ind.} G\} + 1$$

Dowód jest dosyć prosty; jeśli $col(G) = k$ dla jakiegoś k , to znaczy to że istnieje jakaś permutacja wierzchołków G taka, że każdy wierzchołek „na lewo” ma co najwyżej $k - 1$ sąsiadów. Teraz dla każdego podgrafu indukowanego H jest tak, że gdzieś w tej permutacji jest „ostatni” wierzchołek należący do tego podgrafu indukowanego. Nie ma on w ogóle krawędzi „na prawo” i ma same krawędzie „na lewo”. Minimalnie może ich mieć $\delta(H)$, czyli w takim razie $\delta(H) \leq k - 1$, skąd mamy że $k \geq \delta(H) + 1$ dla dowolnego podgrafu indukowanego (skąd mamy już tezę).

W drugą stronę dowód przy okazji pokazuje nam wielomianowy algorytm obliczania $col(G)$. Nie ukrywam że jest on bardzo fajny.

$$\text{col}(G) \leq \max\{\delta(H) : H \subset_{\text{ind.}} G\} + 1$$

Konstruujemy sobie permutację wierzchołków grafu G . W jaki sposób? Bierzymy wierzchołek o najmniejszym stopniu i wrzucamy go *na koniec* permutacji. Następnie rozpatrujemy podgraf indukowany H , bez tamtego wierzchołka o najmniejszym stopniu. H znowu ma jakiś wierzchołek o minimalnym stopniu, więc dorzucam go na koniec permutacji (przed wcześniejszym wierzchołkiem o minimalnym stopniu) i kontynuuję „obgryzanie”. Nietrudno zauważyć, że każdy wierzchołek ma „na lewo” od siebie jakieś $\delta(H)$ sąsiadów (gdzie H jest jakimś podgrafem indukowanym). Tym samym col jest z pewnością mniejszy lub równy niż maksymalny minimalny stopień wierzchołka w jakimś podgrafie indukowanym (+1).

Pokazaliśmy więc, że nasz „algorytm” generuje optymalną permutację, bo pokazaliśmy wcześniej że lepiej się nie da (pokazując ograniczenie dolne na $\text{col}(G)$). Jednocześnie dowodzi to równości.

□

9.2 Kolorowanie krawędziowe grafów dwudzielnych

Twierdzenie 9.2.1. Graf dwudzielny G można pokolorować krawędziowo przy użyciu $\Delta(G)$ wierzchołków.

Dowód. Dowód przez indukcję po liczbie krawędzi; przypadek bazowy trywialny. Do poprawnie pokolorowanego grafu dwudzielnego $G = (X, Y, E)$ dokładamy krawędź między jakimiś x i y i pokażemy, że taki graf również da się poprawnie pokolorować krawędziowo stosując $\Delta(G)$ kolorów.

Zauważam, że jako że krawędź między $x \in X$ i $y \in Y$ nie ma jeszcze koloru, to zarówno x jak i y muszą mieć jakiś kolor „wolny”, tzn. odpowiednio dla x jak i y muszą istnieć jakieś kolory α, β takie, że krawędź o kolorze α nie „wchodzi” do x , a krawędź o kolorze β nie „wchodzi” do y . Jeśli $\alpha = \beta$ to kolorujemy krawędź między x i y na kolor α no i mamy poprawne kolorowanie. Trochę nudne.

Ciekawszy przypadek jest, gdy $\alpha \neq \beta$: wtedy musimy jakoś sprytnie przekolorować G , by móc pokolorować krawędź między x i y na jakiś kolor. Załóżmy że do x wchodzi krawędź o kolorze β , a do y o kolorze α (bo inaczej byśmy to trywialnie pokolorowali). Spójrzmy na wierzchołek z którym łączy się x krawędzią o kolorze β ; nazwijmy go y_1 . Zauważmy, że z y_1 musi wychodzić krawędź o kolorze α , bo gdyby krawędź α była wolna dla y_1 , to krawędź koloru β mógłbym przekolorować na kolor α , a więc kolor β w x by się „zwolnił” i mógłbym przekolorować naszą oryginalną krawędź na β , otrzymując poprawne kolorowanie spełniające tezę zadania.

Wierzchołek z którym łączy się y_1 za pomocą koloru α nazwijmy zatem x_1 . Chyba już widzimy kierunek w którym to zmierza. x_1 łączy się kolorem β z jakimś y_2 , bo jeśli nie to kolor β

jest „wolny” i możemy wcześniejszą krawędź przekolorować na niego, zwalniając jej kolor w wierzchołku y_1 i umożliwiając dalsze przekolorowanie.

Sekwencję takich wierzchołków, opisaną w ten sposób nazwiemy $\beta\alpha$ –ścieżką. Zauważam że ścieżka ta nigdy nie może się „zacyklić” w grafie dwudzielnym (w tym wrócić do x lub y) bo wygenerowałoby to sprzeczność z założeniami dotyczącymi kolorowania. Jednocześnie jako że graf jest skończony, musi ona gdzieś się skończyć. Znaczy to że dojdziemy w pewnym momencie do jakiegoś punktu, od którego będziemy mogli przekolorować całą tę ścieżkę i uzyskać poprawne kolorowanie całego grafu G . \square

9.3 Twierdzenie Vizinga

Jest to dowód, który najłatwiej zrozumieć samemu rozrysowując sobie proces na kartce. Niemniej, z pomocą rysunków spróbuję go Wam przybliżyć.

Twierdzenie 9.3.1 (Vizing).

$$\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$$

Dowód. Ograniczenie dolne widzimy od razu – Δ krawędzi spotykających się w jednym wierzchołku musi dostać różne kolory.

Ograniczenie górne pokazujemy indukcją po liczbie pokolorowanych krawędzi. Jedną krawędź umiemy pokolorować bez problemu. Weźmy zatem częściowe kolorowanie i powiedzmy, że chcemy pokolorować krawędź (x, y) .

Skoro mamy do dyspozycji $\Delta + 1$ kolorów to znaczy, że każdy wierzchołek ma jakiś kolor wolny (nie wychodzi z niego krawędź w tym kolorze).

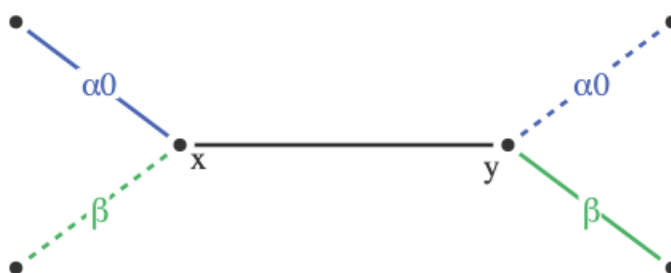
Obserwacja, z której będziemy dużo korzystać: jeśli dowolne wierzchołki x, y połączone krawędzią mają wolny ten sam kolor β to krawędź między nimi możemy pokolorować na tenże kolor. Kolory wolne dla danego wierzchołka będziemy oznaczać linią przerywaną, dotykającą tego wierzchołka.

Założmy więc, że mamy pecha i wierzchołki x, y nie mają wspólnych wolnych kolorów tj. jeśli x ma wolny kolor β to y ma ten kolor zajęty i vice versa. Dodatkowo niech α_0 będzie wolnym kolorem wierzchołka y .

Od tego momentu będziemy tak kombinować, żeby x zwolnić α_0 , być może zajmując przy tym β .



Rysunek 9.1: prosty przypadek; x i y mają wolny ten sam kolor β

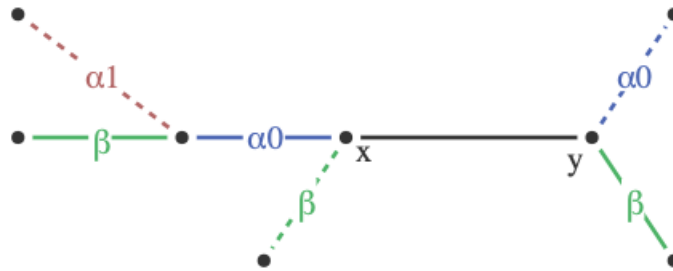


Rysunek 9.2: x i y nie mają wspólnych wolnych kolorów

Niech x_0 będzie taki, że krawędź (x, x_0) ma kolor α_0 . Jeśli x_0 ma wolny kolor β to krawędź

(x, x_0) możemy przekolorować na kolor β , tym samym sprawiając, że x ma wolne α_0 . Ale w takiej sytuacji możemy pokolorować (x, y) na kolor α_0 .

Zatem sytuacja ma się teraz tak:



Rysunek 9.3: x i y mają wolne różne kolory, x_0 ma zajętą β i wolne α_0

Jeżeli teraz x ma wolny kolor α_1 to krawędź (x, x_0) możemy przekolorować na α_1 , a krawędź (x, y) na α_0 . Niech więc (x, x_1) będzie w kolorze α_1 .

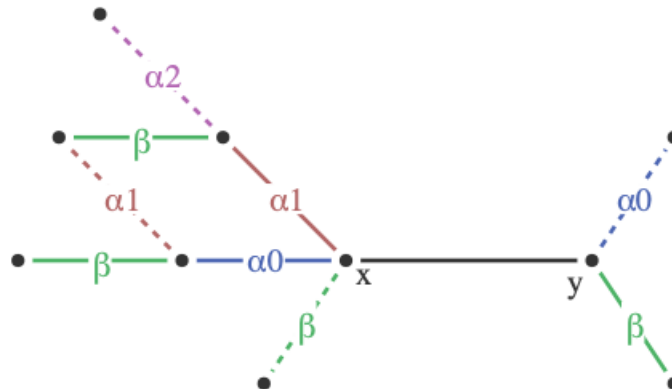
Jeśli x_1 miałby wolny kolor β to możemy przekolorować (x, x_1) na β , wtedy x zwalnia się α_1 a z tym wiemy co robić. No to niech w x_1 β będzie zajęta, a wolny będzie kolor α_2 . Poniżej ilustracja:

Podobnie jak wcześniej stwierdzamy, że z x wychodzi krawędź w kolorze α_2 , bo inaczej przekolorujemy (x, x_1) na α_2 . Kontynuujemy to rozumowanie aż napotkamy wierzchołek x_k o wolnym kolorze α_j , który już znajduje się wśród kolorów $\alpha_0, \dots, \alpha_{k-1}$

Niestety nie możemy wykonać tej samej sztuczki z przekolorowaniem co wcześniej, ale to nic nie szkodzi bo zrobimy co innego. Otóż wyjdźmy z wierzchołka x_k i pójdźmy ścieżką w kolorach na przemian β i α_j . Oczywiście kiedyś skończą nam się krawędzie i wylądujemy w jakimś wierzchołku v .

Rozważmy sobie teraz przypadki czym ten wierzchołek v jest.

1. $v \notin \{x, x_0, x_1, \dots, x_k\}$ Najfajniejszy przypadek - ścieżka kończy się w niezbyt istotnym miejscu. Zamieniamy kolory na ścieżce miejscami. Możemy tak zrobić, bo wewnętrznym

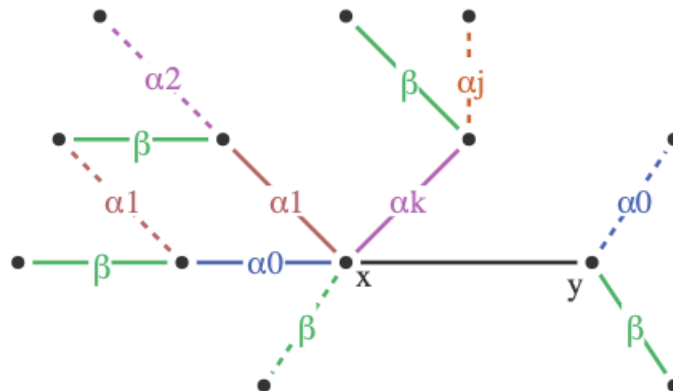


Rysunek 9.4: x_1 ma zajęta β a wolne α_2

wierzchołkom się nic nie zmienia, a na końcach odpowiedni kolor jest wolny.

Teraz, począwszy od krawędzi (x, x_k) przekolorujemy wachlarz. Dzięki przekolorowaniu, x_k ma teraz wolną β tak jak x , zatem (x, x_k) możemy dać kolor β . W takim razie x ma teraz wolny kolor α_k tak jak x_{k-1} , zatem (x, x_{k-1}) dostanie kolor α_k . Podobnie (x, x_{k-2}) dostanie kolor α_{k-1} .

W końcu dojdziemy do (x, x_0) , które dostanie kolor α_1 . Sprawiliśmy, że x ma wolne α_0 , więc z czystym sumieniem kolorujemy (x, y) na α_0 .



Rysunek 9.5: x_k ma wolny kolor α_j , który już widzieliśmy.



Rysunek 9.6: Przekolorowanie wachlarza gdy ścieżka z x_k kończy się w poza wierzchołkami x, x_0, \dots, x_k

2. $v = x_{j-1}$ Taka sytuacja niestety może zajść, bo x_{j-1} ma wolny kolor x_j i zajętą β . Zauważmy, że nie możemy zrobić tego co w przypadku pierwszym, bo przekolorowanie ścieżki sprawia, że x_{j-1} ma kolor α_j zajęty, a taki kolor by otrzymał przy poprawianiu wachlarza. Zrobimy zatem co innego.

Tak jak wcześniej przekolorujemy ścieżkę, ale zamiast przekolorowywać krawędź (x, x_k) na β przekolorujemy (x, x_{j-1}) na β . Dalej możemy kontynuować tak jak poprzednio: (x, x_{j-1}) dostanie kolor α_{j-2} itd. (Musielismy przyjść do v krawędzią o kolorze β bo inaczej nie byłby to koniec ścieżki)



Rysunek 9.7: Przekolorowanie gdy ścieżka z x_k kończy się w x_{j-1}

□

9.4 Twierdzenie Brooksa

Twierdzenie 9.4.1 (Brooks). Jeśli spójny graf G jest kliką lub cyklem nieparzystym to $\chi(G) = \Delta(G) + 1$. W przeciwnym razie $\chi(G) \leq \Delta(G)$

Dowód. Widzimy, że cykl nieparzysty wymaga użycia $3 = \Delta(G) + 1$ kolorów, a w przypadku klikli sąsiedzi każdego wierzchołka używają $\Delta(G)$ kolorów, a jeszcze jeden potrzebujemy na ten wierzchołek. Przyjmijmy zatem, że nasz graf G nie jest ani cyklem nieparzystym ani kliką.

Jeśli $\Delta(G) \leq 2$ to G jest ścieżką lub cyklem parzystym i widzimy, że G jest dwudzielny.

Niech $\Delta(G) \geq 3$.

Idea dowodu jest taka, że będziemy chcieli jakoś skonstruować kolorowanie używające co najwyżej $\Delta(G)$ kolorów. W związku z tym będziemy inkrementalnie odfiltrowywać grafy, dla których takie kolorowanie stworzymy. Przedstawiam zatem kolejne własności grafu, dla którego będzie się trzeba trochę bardziej namęczyć.

1. G jest Δ -regularny Pokażemy, że w przeciwnym razie $\chi(G) \leq \Delta$ Jeśli G nie jest Δ -regularny to w G istnieje wierzchołek v o stopniu mniejszym niż Δ . Postawmy ten wierzchołek na końcu permutacji i spójrzmy na graf $G - v$. v miał jakichś sąsiadów,

których stopień wynosił co najwyżej Δ . W takim razie po usunięciu v jego byli sąsiedzi na pewno mają teraz stopień mniejszy niż Δ i możemy powtórzyć całe to rozumowanie aż skończą nam się wierzchołki i wygenerujemy całą permutację. Zauważamy, że dzięki konstrukcji każdy wierzchołek ma na lewo mniej niż Δ sąsiadów i dostajemy $col(G) \leq \Delta$

Wyberzmy dowolny wierzchołek v i oznaczmy $H = G - v$. Sąsiadom v zmniejszyliśmy stopień, zatem z powyższego wywodu wynika, że H jest Δ -kolorowalny. Pokolorujmy zatem H i przejdźmy do kolejnej własności.

2. Sąsiedzi v dostają parami różne kolory w kolorowaniu grafu H W przeciwnym razie któryś z Δ kolorów jest wolny w v i możemy go użyć kończąc kolorowanie.

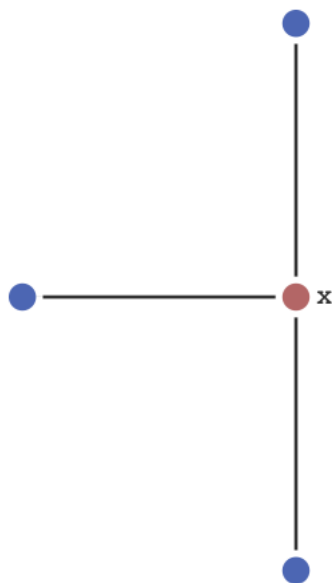
Nazwijmy sąsiadów v przez v_1, \dots, v_Δ i niech będą pokolorowani kolorami $1, \dots, \Delta$.

Oznaczmy $C_{ij} = H[\{v \in V \mid c(v) \in \{i, j\}\}]$ - podgraf indukowany grafu H , który zawiera wszystkie wierzchołki w kolorach i, j

3. Sąsiedzi v_i, v_j leżą w tym samym komponencie grafu C_{ij} W przeciwnym razie możemy wziąć komponent do którego należy v_i i przekolorować go tak, że wierzchołki o kolorze i dostają kolor j , a te o kolorze j dostają kolor i . Tym samym wierzchołki v_i, v_j otrzymują oba kolor j sprowadzając problem do poprzedniego podpunktu.
4. Każdy C_{ij} jest ścieżką. Załóżmy że tak nie jest i weźmy pierwszy licząc od v_i wierzchołek, który ma co najmniej trzech sąsiadów w C_{ij} i nazwijmy go x . Bez straty ogólności powiedzmy, że x ma kolor i . Rozważmy kolory jakie mają sąsiedzi x . Co najmniej trzech sąsiadów ma kolor j , a pozostałych jest $\Delta - 3$ W takim razie sąsiedzi x używają co najwyżej $\Delta - 2$ różnych kolorów. Oczywiście jeden z wolnych kolorów to i , ale możemy teraz przekolorować x na ten drugi. Ponieważ x był pierwszym rozgałęzieniem między v_i a v_j to po przekolorowaniu v_i oraz v_j muszą leżeć w różnych komponentach nowego C_{ij}
5. Każde dwa $C_{ij}, C_{ik}, k \neq j$ przecinają się tylko w v_i W przeciwnym razie istnieje wierzchołek x w kolorze i , który ma dwóch sąsiadów w kolorze j i dwóch sąsiadów w kolorze k . Jak się dobrze policzy to tak jak poprzednio wyjdzie nam, że jakiś kolor jest wolny i możemy zrobić ten sam myk z przekolorowaniem.
6. Istnieje para v_i, v_j , która nie jest połączoną krawędzią. W przeciwnym razie wierzchołki v, v_1, \dots, v_Δ tworzą klikę, co jest sprzeczne z założeniem.

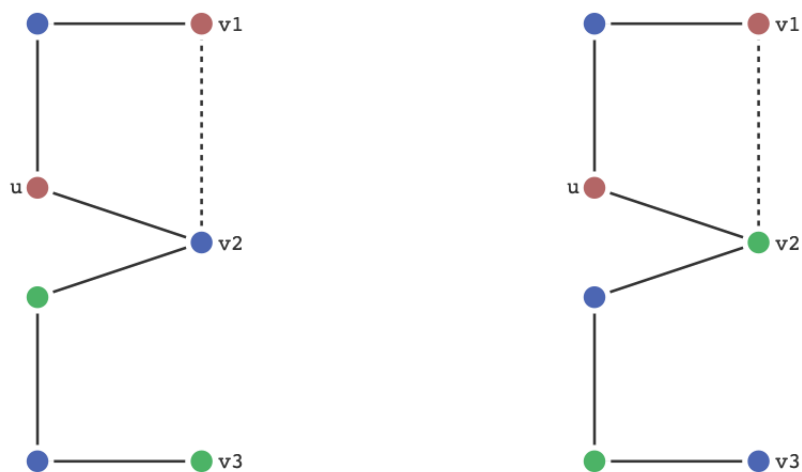
Bez straty ogólności powiedzmy, że v_1 i v_2 nie są połączone krawędzią. Jednak z własności (5) musi istnieć ścieżka między nimi. Niech więc u to będzie pierwszy wierzchołek w kolorze 1 na ścieżce od v_2 do v_1 .

Teraz dzieje się magia. W C_{23} zamieniamy kolory 2 i 3 i takie kolorowanie przepuszczamy przez warunki (2)–(5). Jeśli w którymś miejscu udało nam się stworzyć dobre kolorowanie to super, a jeśli nie to ups. Na szczęście zauważamy teraz fajną rzecz. Otóż wierzchołek u nadal jest połączony ścieżką w kolorach 1 i 2 z wierzchołkiem v_1 , zatem należy do



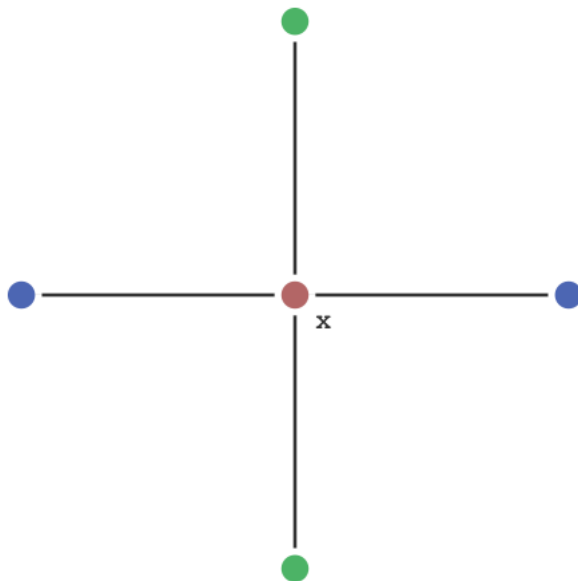
Rysunek 9.8: Wierzchołek x ma trzech sąsiadów w kolorze j

komponentu C_{12} , ale z drugiej strony jest połączony krawędzią z wierzchołkiem v_2 , który ma teraz kolor 3 zatem należy też do komponentu C_{13} . W takim razie nowe kolorowanie narusza warunek (5) co już umiemy rozwiązać.



Rysunek 9.10: Wierzchołki v_1 i v_2 przed i po przekolorowaniu komponentu C_{23}

To tyle, nie ma więcej warunków, które musimy rozważać. Fajnie.



Rysunek 9.9: Wierzchołek x ma dwóch sąsiadów w kolorze j i dwóch w kolorze k

9.5 Grafy bez trójkątów o dużej liczbie chromatycznej

9.5.1 Czemu interesują nas takie konstrukcje?

A komu to potrzebne? A dlaczego?

*Pani z Internetu, zapytana, czy należy
w Polsce zalegizować marihunaen*

Mogłoby się wydawać, że liczba chromatyczna jest w jakiś sposób własnością lokalną grafu. To znaczy, oczywiście widzimy, że jeśli graf ma liczbę klikową ω , to musimy użyć przynajmniej ω kolorów do jego pokolorowania. No dobra, ale może gdybyśmy lokalnie pokolorowali podgrafy będące dużymi klikami, to pozostałe części grafu już damy radę załatwić jakąś rozsądną liczbą dodatkowych kolorów? Prawda? Nieprawda. Okazuje się, że istnieją grafy, które nie zawierają nawet trójkątów, czyli mają $\omega < 3$, ale mają też dowolnie dużą liczbę chromatyczną. Czyli niestety życie (przynajmniej jeśli dla kogoś życie opiera się na optymalnym kolorowaniu grafów) nie jest takie proste...

9.5.2 Co będziemy konstruować?

Pokażemy trzy sposoby zrobienia ciągu grafów G_3, G_4, \dots (zaczynamy od 3 bo dla 0, 1 i 2 nie dzieje się nic ciekawego) takiego, że dla dowolnego $n \geq 3$ będą zachodzić dwie własności:

- $\omega(G_n) = 2$
- $\chi(G_n) \geq n$

Warto zwrócić uwagę, że n *nie będzie* liczbą wierzchołków w takim grafie. Pamiętajmy — ten ciąg grafów indeksujemy *liczbą chromatyczną*, która nas interesuje, nie liczbą wierzchołków. Liczba wierzchołków wyjdzie w praniu i będzie zupełnie inna.

W każdym z trzech sposobów zaczniemy od położenia $G_3 = C_5$. Wszystko się zgadza — C_5 nie zawiera trójkąta i ma $\chi = 3$, bo jest cyklem nieparzystej długości. Resztę ciągu konstruujemy rekurencyjnie.

9.5.3 Konstrukcja Mycielskiego

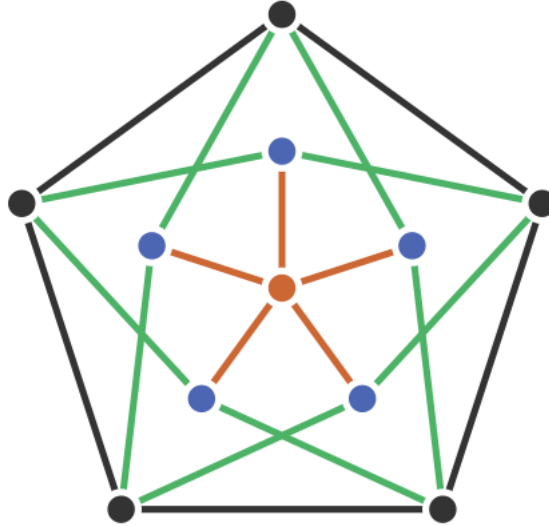
Założmy sobie, że mamy już G_n , które spełnia wszystkie własności, jakie chcieliśmy. Chcemy teraz zrobić G_{n+1} . W tym celu najpierw weźmiemy wierzchołki z G_n — nazwijmy je v_1, v_2, \dots, v_N , gdzie $N = |V(G_n)|$ (pamiętajmy tylko, że $N \neq n$). Doróbmy sobie jeszcze „kopie” tych wierzchołków, tzn. odpowiadające im nowe wierzchołki, które nazwiemy v'_1, v'_2, \dots, v'_N , i dorzućmy jeszcze specjalny wierzchołek v^* . Czyli, podsumowując, kładziemy

$$V(G_{n+1}) := \{v_1, v_2, \dots, v_N\} \cup \{v'_1, v'_2, \dots, v'_N\} \cup \{v^*\}$$

A jak będzie z krawędziami? Po pierwsze, krawędzie między oryginalnymi wierzchołkami grafu G_n zostają jak były. Po drugie, każdy wierzchołek będący kopią łączymy z wierzchołkiem specjalnym. Po trzecie, *nie łączymy* żadnych dwóch kopii. I po czwarte, każdą kopię łączymy z sąsiadami odpowiadającego jej oryginału (czyli zapewniamy, że kopia ma takie samo sąsiedztwo jak oryginał, poszerzone jedynie o v^*). Formalnie:

$$E(G_{n+1}) := E(G_n) \cup \{v_i v^* : i \in [N]\} \cup \{v'_i v_j : i, j \in [N] \wedge v_i v_j \in E(G_n)\}$$

Wyglądać to będzie mniej więcej tak:



Rysunek 9.11: Graf G_4 w konstrukcji Mycielskiego

Przekonajmy się teraz, że stworzony G_{n+1} posiada dwie cechy, których oczekiwaliśmy:

- $\omega(G_{n+1}) = 2$, czyli nie ma trójkątów. Zastanówmy się:
 - na pewno v^* nie jest w żadnym trójkącie, bo jego sąsiadami są tylko kopie, a żadne dwie kopie nie są połączone
 - z tego samego powodu żaden potencjalny trójkąt nie zawiera dwóch wierzchołków będących kopiami
 - trójkąt nie może składać się z samych oryginałów, bo założyliśmy, że w oryginalnym G_n nie było trójkątów

Zatem gdyby istniał trójkąt, to byłby on w postaci $v_i v'_j v_k$, dla pewnych $i, j, k \in [N]$.

Wtedy mielibyśmy oczywiście $v_i v_k \in E(G_{n+1})$, $v'_j v_i \in E(G_{n+1})$ oraz $v'_j v_k \in E(G_{n+1})$.

Ale pamiętajmy, że graf G_{n+1} skonstruowaliśmy tak, żeby oryginalny wierzchołek i jego kopia miały to samo sąsiedztwo (nie licząc v^*). Zatem skoro $v'_j v_i \in E(G_{n+1})$ oraz $v'_j v_k \in E(G_{n+1})$, to zachodzi $v_j v_i \in E(G_n)$ oraz $v_j v_k \in E(G_n)$. Krawędzi między oryginałami nie ruszaliśmy, więc skoro $v_i v_k \in E(G_{n+1})$ to również $v_i v_k \in E(G_n)$.

Ale z tego wszystkiego wychodzi, że w oryginalnym G_n istniał już trójkąt $v_i v_j v_k$, a przecież założyliśmy, że tak nie jest. Uzyskana sprzeczność dowodzi, że w G_{n+1} nie ma trójkątów. \square

- $\chi(G_{n+1}) \geq n + 1$. Załóżmy, że tak nie jest, tzn. $\chi(G_{n+1}) \leq n$. Weźmy zatem kolorowanie c , które o tym świadczy i poprawnie koloruje G_{n+1} używając nie więcej niż n kolorów. Przyjrzyjmy się teraz wierzchołkom-kopiom: widzimy na nich maksymalnie $n - 1$ kolorów. Dlaczego? Gdyby zużywały one n kolorów, to zabrakłoby wolnego koloru na v^* , który

przecież jest połączony ze wszystkimi kopiami.

Świetnie, to teraz stwórzmy sobie kolorowanie c' grafu G_n , które dla każdego $i \in [N]$ będzie działać bardzo prosto:

$$c'(v_i) = \begin{cases} c(v_i) & \iff c(v_i) \neq c(v^*) \\ c(v'_i) & \iff c(v_i) = c(v^*) \end{cases}$$

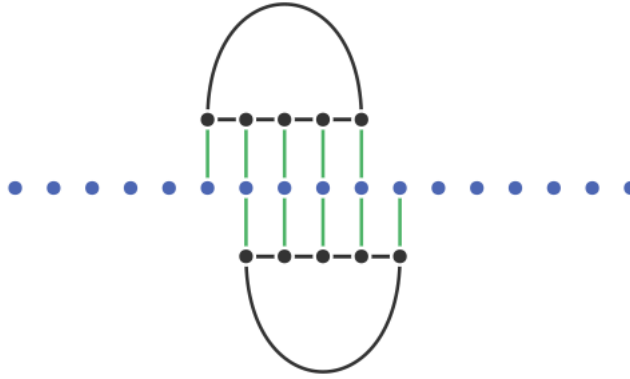
Innymi słowy: jeśli dany wierzchołek miał w kolorowaniu c taki kolor, jak specjalny wierzchołek v^* , to dajemy mu kolor jego kopii, a w przeciwnym przypadku zostawiamy taki kolor, jaki był. Zauważmy, że c' jest poprawnym kolorowaniem G_n . Dlaczego? Gdyby nie było, to znaczyłoby, że istnieje krawędź $v_i v_j$ taka, że $c'(v_i) = c'(v_j)$. Są trzy potencjalne wyjaśnienia tej sytuacji:

- w kolorowaniu c wierzchołki v_i i v_j już miały ten sam kolor i pozostał on niezmienny — ale to jest niemożliwe, bo kolorowanie c było poprawne
- w kolorowaniu c wierzchołki v_i i v_j miały ten sam kolor $c(v^*)$, i dla obydwu uległ on zmianie na ten sam kolor — niemożliwe, jak wyżej
- w kolorowaniu c wierzchołki wierzchołki miały różne kolory, przy czym dokładnie jeden z nich miał kolor $c(v^*)$. Przyjmijmy bez straty ogólności, że był to v_i . Skoro zatem $c'(v_i) = c'(v_j)$, a $c(v_i) = c(v^*)$, to mamy $c(v'_i) = c'(v_j) = c(v_j)$. Ale to jest niemożliwe, bo skoro jest krawędź $v_i v_j$, to jest też krawędź $v'_i v_j$, a w poprawnym kolorowaniu c nie mogło być dwóch sąsiednich wierzchołków w tym samym kolorze.

Uzyskane sprzeczności dowodzą, że c' rzeczywiście jest poprawnym kolorowaniem G_n przerobionym z kolorowania c , które używało nie więcej, niż n kolorów. Ale zauważmy, że w c' pozbyliśmy się jednego z kolorów, mianowicie $c(v^*)$. Zatem c' jest poprawnym $(n-1)$ -kolorowaniem grafu G_n , co jednak jest niemożliwe, bo przecież założyliśmy, że $\chi(G_n) \geq n$. Uzyskana sprzeczność dowodzi ostatecznie, że istotnie $\chi(G_{n+1}) \geq n+1$. \square

9.5.4 Konstrukcja Tutte'a

Ponownie zakładamy, że mamy działające G_n i chcemy zrobić G_{n+1} . Przyjmijmy $N = |V(G_n)|$. Ta konstrukcja jest bardzo prosta: najpierw tworzymy sobie $n \cdot (N-1) + 1$ zupełnie nowych wierzchołków — nazwijmy je *wierzchołkami głównymi*. Teraz przy każdym N -elementowym podzbiorze tych wierzchołków tworzymy kopię G_n i łączymy wierzchołki główne z odpowiadającymi im wierzchołkami z kopii G_n (w dowolnym porządku, byle każdy wierzchołek główny z podzbioru miał dokładnie jednego kolegę w odpowiadającej temu podzbiorowi kopii). Najłatwiej to zobaczyć na poniższym rysunku:



Rysunek 9.12: Fragment G_4 w konstrukcji Tutte'a

Między poszczególnymi kopiami G_n nie dajemy żadnych krawędzi. Podobnie nie dajemy żadnych krawędzi między wierzchołkami głównymi. I gotowe — mamy nasze G_{n+1} ! Przyjrzyjmy się, czemu taki graf spełnia nasze wymagania:

- brak trójkątów — oczywiście żadnego trójkąta nie ma:
 - w żadnej kopii G_n , bo założyliśmy, że G_n jest bez trójkątów
 - pomiędzy kopiami G_n , bo powiedzieliśmy, że różnych kopii w żaden sposób nie łączymy
 - wśród wierzchołków głównych, bo między nimi nie ma krawędzi

Zatem jedyny możliwy trójkąt musiałby mieć jeden wierzchołek główny i dwa wierzchołki z kopii. Ale te dwa z kopii nie mogą być w jednej kopii G_n , bo każdy wierzchołek główny ma dokładnie jednego kolegę w każdej kopii. Nie mogą też być w różnych kopiach G_n , bo aby domknąć trójkąt, musiałyby się łączyć, a między kopiami nie ma krawędzi. Zatem w G_{n+1} nie istnieją trójkąty. \square

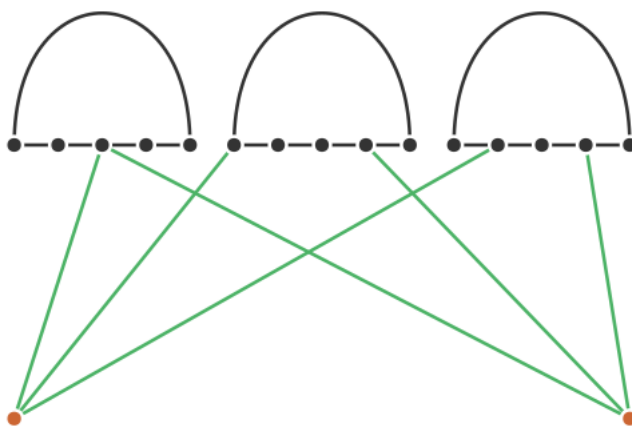
- $\chi(G_{n+1}) \geq n + 1$. Załóżmy, że tak nie jest, czyli $\chi(G_{n+1}) \leq n$. Weźmy zatem kolorowanie, które o tym świadczy. Ponieważ jest $n \cdot (N - 1) + 1$ głównych wierzchołków, to z zasady szufladkowej musi istnieć tam N wierzchołków, które mają taki sam kolor, powiedzmy k . Rozważmy teraz kopię skonstruowaną przy tym N -elementowym podzbiorze wierzchołków głównych. Żaden z wierzchołków w tej kopii nie może mieć koloru k , ponieważ jest połączony z odpowiadającym mu wierzchołkiem głównym. A to oznacza, że ta kopia G_n została pokolorowana nie więcej niż $n - 1$ kolorami. Ale to jest przecież niemożliwe, bo założyliśmy, że $\chi(G_n) \geq n$. Uzyskana sprzeczność pokazuje, że istotnie

$$\chi(G_{n+1}) \geq n + 1.$$

□

9.5.5 Konstrukcja Zykova

Również zakładamy, że mamy działające G_n . Będziemy tworzyć G_{n+1} . Na dobry początek zrobimy sobie n rozłącznych kopii grafu G_n . Teraz dla każdego możliwego wyboru, wyróżniającego po jednym wierzchołku z każdej kopii, dodajemy jeden wierzchołek „na dole” i łączymy go z tymi wyróżnionymi. Żadnych innych krawędzi nie dodajemy. Ponownie, najlepiej to zobaczyć na rysunku:



Rysunek 9.13: Fragment G_4 w konstrukcji Zykova

To będzie nasze G_{n+1} . Zbadajmy, czemu to działa:

- brak trójkątów — na pewno trójkąt nie znajdzie się:
 - w żadnej kopii G_n , bo z założenia nie ma tam trójkątów
 - pomiędzy różnymi kopiami G_n , bo nie są one wcale połączone
 - wśród wierzchołków „na dole”, bo nie ma między nimi żadnych krawędzi

Zatem jedyny potencjalny trójkąt musiałby mieć jeden wierzchołek na dole i dwa w kopiach G_n . Te dwa „górne” nie mogą być jednak w tej samej kopii G_n , bo każdy wierzchołek z dołu w danej kopii ma *dokładnie jednego* sąsiada. Nie mogą też być w różnych kopiach G_n , bo musiałyby być połączone, a przecież kopie się nie łączą. Czyli żaden trójkąt nie może się pojawić w G_{n+1} . □

- $\chi(G_{n+1}) \geq n + 1$. Pokażemy, że nie da się pokolorować G_{n+1} używając n -kolorów. Założymy do dowodu nie wprost, że jest to możliwe, i weźmy takie poprawne n -kolorowanie.

Powiedzmy, że te kolory to $1, 2, \dots, n$. Oczywiście każda kopia G_n używa wszystkich n kolorów, bo $\chi(G_n) \geq n$. Zatem z pierwszej kopii wybierzmy dowolny wierzchołek w kolorze 1, z drugiej kopii dowolny wierzchołek w kolorze 2, \dots , z n -tej kopii wierzchołek w kolorze n . To jest wybór po jednym wierzchołku z każdej kopii, więc na dole jest wierzchołek połączony z nimi wszystkimi. Ups... Ale to oznacza, że zabraknie na niego wolnego koloru, bo dla każdego z dostępnych n kolorów ten „dolny” wierzchołek jest połączony z wierzchołkiem w tym kolorze „na górze”. Uzyskana sprzeczność dowodzi nierówności $\chi(G_{n+1}) \geq n + 1$. \square

9.6 Shift grafy

Shift grafy są kolejnym przykładem rodziny grafów bez trójkątów ale o dowolnie dużej liczbie chromatycznej. Czemu są jako osobne wymaganie egzaminacyjne? Cytując Tadeusza Szuka, odpowiedź brzmi: nie wiem, choć się domyślam. Otóż konstrukcja shift grafów (znana też jako konstrukcja Erdősa–Hajnala) jest jawna, natomiast te poprzednie są rekurencyjne. Konkretniej: będziemy konstruować ciąg takich grafów $G_n = (V_n, E_n)$, że $\omega(G_n) = 2$ oraz $\chi(G_n) \geq \lceil \log_2 n \rceil$. Zrobimy to następująco:

$$V_n = \{[i, j] : 1 \leq i < j \leq n\}$$

$$\{[i, j], [k, l]\} \in E_n \iff j = k$$

Innymi słowy, wierzchołkami naszego grafu będą przedziały o końcach ze zbioru $[n]$, bez przedziałów będących pojedynczym punktem, natomiast dwa przedziały są połączone krawędzią wtedy, gdy koniec jednego dotyka początku drugiego. Nie ma tutaj trójkątów. Dlaczego? Trójkąt musiałby być w postaci $[i, j], [j, k], [k, i]$, a taka trójka przedziałów oczywiście nie może istnieć na prostej, bo wynikałoby z tego coś w stylu $i < j < k < i$.

Przyszedł czas udowodnić fakt o liczbie chromatycznej. Weźmy dowolne k -kolorowanie G_n i nazwijmy je c . Pokażemy, że $2^k \geq n$, czyli $k \geq \log_2 n$, a ponieważ pracujemy na liczbach całkowitych, to dostaniemy z tego $k \geq \lceil \log_2 n \rceil$. Zdefiniujmy zbiory C_1, C_2, \dots, C_n następująco:

$$C_i = \{b \in [k] : b = c([j, i]) \text{ dla } j < i\}$$

Mówiąc najprościej, w zbiorze C_i są kolory przedziałów kończących się na punkcie i . Teraz pokażemy, że $C_i \neq C_j$ dla $i \neq j$. W tym celu pokażemy, że dla każdej pary $j > i$ istnieje kolor należący do C_j i nienależący do C_i , czyli świadczący o różności tych zbiorów. Jak tego dokonamy? Okazuje się, że bardzo prosto. Weźmy przedział $[i, j]$. Ma on jakiś kolor $b \in [k]$. Żaden przedział kończący się na i nie może mieć koloru b , bo ma krawędź do $[i, j]$. Zatem $b \notin C_i$. Ale oczywiście przedział $[i, j]$ kończy się na j , a skoro ma kolor b , to $b \in C_j$.

Czyli, podsumowując, mamy zbiory C_1, C_2, \dots, C_n i wszystkie różne. Oczywiście wszystkie są też podzbiorami $[k]$. Z zasady szufladkowej wynika, że w takim razie $n \leq 2^k$, co kończy

dowód. □

9.7 Grafy przecięć kwadratów

Twierdzenie 9.7.1. Liczba kolorująca w grafach przecięć kwadratów na płaszczyźnie ograniczona jest przez $4\omega - 3$.

Dowód. Ustalmy sobie porządek na kwadratach taki, że jeśli dany kwadrat x ma krótszy bok niż kwadrat y , to y jest w permutacji przed x . Jeżeli ktoś nie wie jak działają permutacje wierzchołków dla liczby kolorującej to sugeruję poczytać najpierw jak to wszystko działa. W sumie to nie sugeruję tylko nakazuję.

Wracając, jako że im mniejszy jest kwadrat tym później jest w permutacji wierzchołków do cola, wszystkie kwadraty które są „na lewo” od niego i mają do niego krawędź (tj. przecinają się z nim) muszą „w sobie” mieć któryś z 4 wierzchołków tego kwadratu (przypominam że w grafie przecięć kwadratów na płaszczyźnie z definicji wszystkie kwadraty mają 2 krawędzie pionowo i 2 poziomo, nie dopuszczamy jakiegось obracania). Fakt ten wynika z dowodu *to widać*, ale serio – jeśli ktoś znalazł sposób na wstawianie kwadratu o większym boku w taki o mniejszym boku w grafie przecięć kwadratów **bez obracania** w taki sposób, że kwadrat o mniejszym boku nie ma żadnego wierzchołka w tym o większym boku, sugeruję kontakt z psychologiem.

No i fajnie, bo teraz ograniczam sobie liczbę kwadratów które mam „na lewo” przez $4\omega - 4$. Dlaczego? Bo wszystkie kwadraty które przecinają wierzchołek x mojego kwadratu (przypominam że kwadrat ma 4 wierzchołki, to zaraz będzie ważne) muszą formować jakąś klikę (no w sensie wszystkie mają punkt wspólny w postaci tego wierzchołka). Obecny kwadrat też wpada do tej kliky, więc wychodzi mi maksymalnie $\omega - 1$ sąsiadów na każdy wierzchołek. I w sumie to tyle, mamy ograniczenie liczby kolorującej więc mamy ograniczenie liczby chromatycznej. Fajnie. □

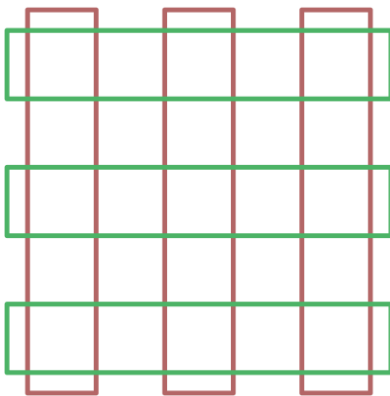
9.8 Grafy przecięć prostokątów

9.8.1 Liczba kolorująca

Czy jesteśmy w stanie ograniczyć liczbę kolorującą przez funkcję od liczby klikowej w grafie przecięć prostokątów na płaszczyźnie?

Twierdzenie 9.8.1. Nie.

Dowód. Możemy stworzyć klikę $K_{n,n}$ w tej klasie grafów. No i w sumie tyle.



Rysunek 9.14: $K_{3,3}$ jako przecięcia prostokątów

□

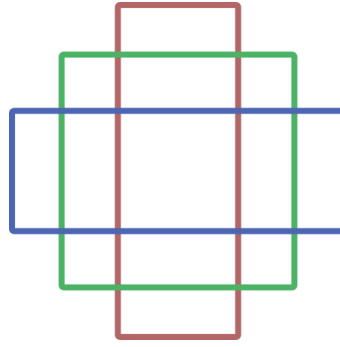
9.8.2 Liczba chromatyczna

Nie potrafimy ograniczyć liczby kolorującej to może chociaż chromatyczną umiemy? Okazuje się, że tak.

Twierdzenie 9.8.2. Liczba chromatyczna w grafach przecięć prostokątów na płaszczyźnie ograniczona jest przez $\omega \cdot (8\omega - 7)$.

Dowód. Kolorujemy prostokąty na płaszczyźnie w dość zabawny sposób, bo każdy kolor będzie składał się z pary liczb. Pierwsza współrzędna będzie przyjmowała wartości od 1 do ω , natomiast druga od 1 do $8\omega - 7$. Intuicyjnie będzie odpowiadało to podzieleniu prostokątów na ω warstw, z których każdą z osobna będziemy umieli pokolorować na $8\omega - 7$ kolorów.

Zacznijmy od pierwszej współrzędnej. Powiemy, że dwa prostokąty **krzyżują się** jeśli przecinają się, ale wewnątrz (bez brzegu) jednego nie zawiera wierzchołków drugiego. Jeżeli skierujemy relację krzyżowania w ten sposób, że $u \leq v$ gdy u jest węższy niż v to okazuje się, że dostaniemy częściowy porządek. Możemy zauważyć, że łańcuch w tym porządku to ciąg coraz węższych i dłuższych prostokątów o wspólnym „środku”, więc tworzą one klikę o maksymalnym rozmiarze ω .

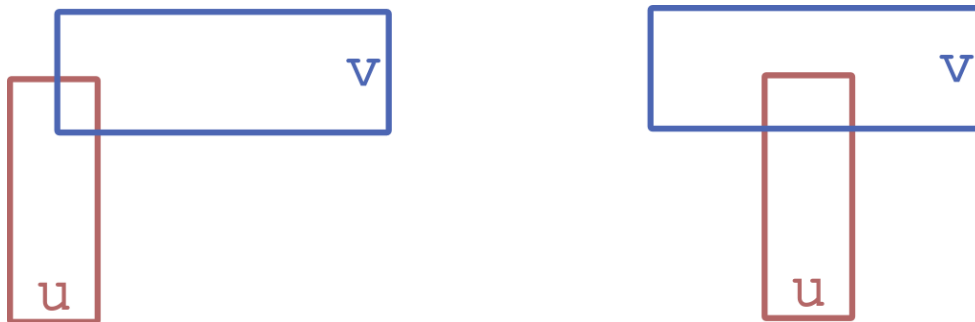


Rysunek 9.15: „Krzyżujące się” prostokąty tworzące klikę; każdy prostokąt dostaje inny kolor na pierwszej współrzędnej

Skoro rozmiar najdłuższego łańcucha to ω to możemy skorzystać z twierdzenia dualnego do Dilwortha i podzielić prostokąty na ω antyłańcuchów A_1, \dots, A_ω , które intuicyjnie będą odpowiadały grupom prostokątów, które się nie krzyżują parami. Następnie na pierwszej współrzędnej każdy prostokąt dostaje numer antyłańcucha do którego trafił.

Okazuje się, że dla prostokątów mających ten sam pierwszy kolor (a więc takich które się nie krzyżują) jesteśmy już w stanie ograniczyć liczbę kolorującą, a więc i liczbę chromatyczną. Robimy to w dosyć sprytny sposób. Mianowicie zauważamy, że skoro prostokąty się nie krzyżują, gdy przecinają się one to musi być tak że jakiś wierzchołek jednego jest w drugim (lub vice versa).

Co robimy z tym fascynującym faktem? Otóż majstrujemy sobie graf **skierowany** na prostokątach w taki sposób, że krawędź z prostokąta u do prostokąta v mamy, gdy u ma wierzchołek wewnątrz v .



Rysunek 9.16: po lewej mamy krawędzie (u, v) oraz (v, u) , po prawej tylko (u, v)

Podobnie jak przy grafach przecięć kwadratów, zauważamy że z jednego prostokąta może wychodzić maksymalnie $4\omega - 4$ krawędzi (bo każdy wierzchołek może się zawierać w co najwyżej $\omega - 1$ prostokątów). W takim razie oszacowanie górne na liczbę krawędzi w grafie wynosi $|E| \leq |V| \cdot (4\omega - 4)$. Jednocześnie wiemy, że

$$\sum_{v \in V} \deg(v) = 2 \cdot |E|$$

Skąd

$$\sum_{v \in V} \deg(v) = 2 \cdot |E| \leq |V| \cdot (8\omega - 8)$$

$$\frac{\sum_{v \in V} \deg(v)}{|V|} \leq 8\omega - 8$$

Należy zauważyć, że po lewej stronie mam średnią arytmetyczną stopni wszystkich wierzchołków w tym grafie. Ponieważ jest ona mniejsza lub równa $8\omega - 8$, to wiem że istnieje na pewno wierzchołek który ma stopień mniejszy bądź równy $8\omega - 8$ (tak działa średnia arytmetyczna). To oczywiście tłumaczy się na to, że istnieje prostokąt o maksymalnym stopniu $8\omega - 8$ w grafie przecięć prostokątów. No a skoro tak, to prostokąt taki mogę sobie zawsze „wrzucić” zawsze na koniec permutacji do liczby kolorującej, „odgryźć” go od grafu i znowu wrzucić prostokąt o takim maksymalnym stopniu i tak dalej. Tym samym osiągnęliśmy ograniczenie na liczbę kolorującą w postaci $\text{col}(G) \leq 8\omega - 7$ (czyli również ograniczyliśmy liczbę możliwych kolorów „na drugiej współrzędnej” w ten sposób).

Podsumowując: skoro na pierwszej współrzędnej mamy ω możliwych wartości, a na drugiej $8\omega - 7$ to razem używamy $\omega \cdot (8\omega - 7)$ kolorów.

□

9.9 Grafy planarne

9.9.1 Wzór Eulera

Twierdzenie 9.9.1. Przez v oznaczmy liczbę wierzchołków, e liczbę krawędzi a f liczbę ścian spójnego grafu planarnego G . Mamy:

$$v - e + f = 2 \tag{9.3}$$

Dowód. Robimy sobie drzewo rozpinające naszego grafu G (ważne założenie, że jest on spójny). Drzewa to dosyć przyjemna klasa grafów, bo jeśli mają n wierzchołków to mają $n - 1$ krawędzi. Ponadto mają tylko jedną ścianę (zewnątrzną). Zatem $f = 1$, a $e = v - 1$. W takim razie dla drzewa rozpinającego naszego grafu planarnego zachodzi teza. Teraz zauważamy, że jak dodamy jakąś krawędź to to nadal zostaje równe 2, bo f zwiększa się o jeden i e zwiększa się o jeden. Dokładając zatem krawędź po krawędzi otrzymujemy wyjściowy graf planarny, w którym zachodzi teza. □

9.9.2 Liczba kolorująca

Pokażemy, że w dowolnym grafie planarnym G istnieje wierzchołek o stopniu równym co najwyżej 5. Wtedy w oczywisty sposób ograniczymy liczbę kolorującą od góry przez 6 (bo w takim razie $\delta(G) \leq 5$ dla dowolnego grafu planarnego, więc będziemy mogli zastosować fajny wzór na

liczbę kolorującą). Jeśli nie wiesz o jaki wzór mi chodzi, rekomenduję cofnięcie się do rozdziału o liczbie kolorującej, gdzie ten jest dowodzony. Do udowodnienia zostaje zatem pokazanie, że w każdym grafie planarnym istnieje wierzchołek o stopniu co najwyżej 5.

Twierdzenie 9.9.2. W każdym grafie planarnym istnieje wierzchołek o stopniu co najwyżej 5.

Dowód. Załóżmy nie wprost, że tak nie jest. Ponadto zakładamy że graf jest spójny (bo jak nie jest, to prowadzimy rozumowanie dla grafu spójnego dla jakiegoś jego komponentu spójnego). Ze wzoru eulera mamy, że $v - e + f = 2$. Jednocześnie z założenia nie wprost mamy, że każdy wierzchołek ma stopień co najmniej 6. Stosujemy lemat o uściskach dłoni:

$$\sum_{u \in V} \deg(u) = 2 \cdot |E|$$

Korzystając z założenia nie wprost, że dla dowolnego u jest tak, że $(\deg(u) \geq 6)$:

$$\sum_{u \in V} \deg(u) = 2 \cdot |E| \geq 6 \cdot v$$

czyli $e \geq 3v$. Teraz wykonuję fikołek, bo mówię że mój graf ma co najmniej 3 wierzchołki. Jeśli ma mniej, to w sumie teza jest oczywista. Jeśli ma co najmniej 3 wierzchołki zaś, to mogę wykonać bardzo ciekawą obserwację: mianowicie każda ściana „wydzielana” jest przez co najmniej 3 krawędzie. W dodatku każda krawędź ma „kontakt” z maksymalnie dwiema ścianami.

Teraz wykonuję bardzo śmieszłą czynność, bowiem robię coś niezwykle poetyckiego, co wręcz prosi się o rysunek; na każdej ścianie „kładę” 3 „monety”. Każda z tych monet idzie do różnych krawędzi. Jedna krawędź dostanie maksymalnie 2 monety, ale na każdej ścianie położono 3 monety. Stąd mam, że w grafie planarnym, który ma co najmniej 3 wierzchołki:

$$2e \geq 3f$$

Jest to najbardziej machany dowód przez rysowanie który znam, ale jest on prezentowany również na wykładach. I okazuje się, że jak podstawimy tę własność do wzoru Eulera otrzymamy coś bardzo ciekawego. Mianowicie:

$$v - e + f = 2$$

$$f = 2 - v + e$$

$$3f = 6 - 3v + 3e$$

$$6 - 3v + 3e = 3f \leq 2e$$

$$6 - 3v + 3e \leq 2e$$

$$6 - 3v + e \leq 0$$

$$e \leq 3v - 6$$

Zaraz chwilunia, ale z założenia nie wprost mieliśmy że $e \geq 3v$. Mielibyśmy wtedy, że $3v \leq 3v - 6$ skąd $0 \leq -6$. Brzmi trochę jak sprzeczność. \square

9.9.3 5-kolorowalność

Twierdzenie 9.9.3 (Ograniczenie górne na liczbę chromatyczną w grafach planarnych). W grafie planarnym G zachodzi:

$$\chi(G) \leq 5 \tag{9.4}$$

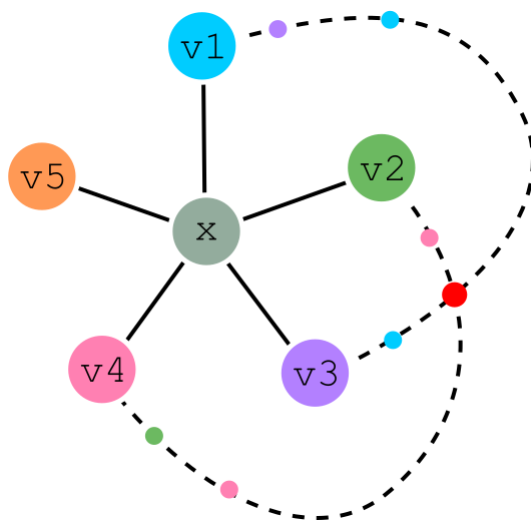
Dowód. Dowód przez indukcję. Zakładamy, że w każdym grafie planarnym jest tak, że istnieje wierzchołek o stopniu co najwyżej 5 (co zostało już udowodnione wcześniej).

Przypadek bazowy indukcji (graf planarny stanowiący po prostu jeden wierzchołek) jest trywialny.

Założmy teraz, że mam sobie graf planarny $G = (V, E)$. Biorę sobie wierzchołek x taki, że ma stopień mniejszy lub równy 5. Z założenia indukcyjnego graf indukowany na wierzchołkach $V \setminus \{x\}$ można pokolorować 5 kolorami (lub mniej). Zakładam, że x ma dokładnie 5 sąsiadów, bo jeśli ma ich mniej na pewno jest jakiś „wolny” z 5 kolorów na które mogę go pokolorować i otrzymać poprawne kolorowanie. Sąsiadów x oznaczam jako v_1, v_2, v_3, v_4 i v_5 . Bez straty ogólności zakładamy, że w tej kolejności zgodnie z ruchem wskazówek zegara. Zakładam że sąsiad v_i ma kolor i (czyli że każdy sąsiad ma inny kolor; jeśli tak nie jest, to od razu mam poprawne kolorowanie, bo znowu biorę sobie „wolny” kolor).

Zauważam teraz fajną rzecz: między dowolnymi dwoma sąsiadami v_i i v_j musi istnieć ścieżka z wierzchołkami o kolorach i, j, i, \dots, i, j . Wynika to z faktu, że gdyby takiej ścieżki nie było, to mógłbym wziąć sobie v_i i przekolorować go na kolor j . Jego sąsiada w kolorze j (o ile taki by istniał) na kolor i i tak dalej. Otrzymałbym poprawne kolorowanie, ale x miałby dwóch sąsiadów w kolorze j (jeśli v_i i v_j są połączone to taki zabieg nadal daje poprawne kolorowanie, ale v_j dostaje kolor i i w sumie to nic nie osiągnąłem) i mógłbym mu dać kolor i .

Skoro tak, to między v_1 i v_3 istnieje taka „ścieżka dwukolorowa”. Zauważam jednak, że wtedy nie może istnieć taka ścieżka między v_2 i v_4 (znaczy zależy jak je rozrysujemy, ale jak zobaczycie rysunek to się wyjaśni o co mi chodzi – pomysł jest taki, że v_2 jest poniekąd „odizolowany” przez ścieżkę między v_1 a v_3). To oznacza, że zgodnie z opisaną powyżej procedurą mogę sobie po prostu przekolorować v_2 na kolor 4, a wierzchołkowi x dać kolor 2, otrzymując poprawne kolorowanie. Nie mam pojęcia jak formalści chcieliby to sformalizować, ale ci pewnie nadal siedzą nad definicją spaceru rozgałęziającego się w drzewie Steinera.



Rysunek 9.17: Niemożliwe jest połączenie „ścieżką dwukolorową” wierzchołka v_2 z v_4 , jeśli takową już połączyliśmy wierzchołek v_1 z wierzchołkiem v_3 .

□

9.9.4 5-wybieralność

To było coś takiego?

Student TCSu o 5-wybieralności, na chwilę przed wejściem na egzamin

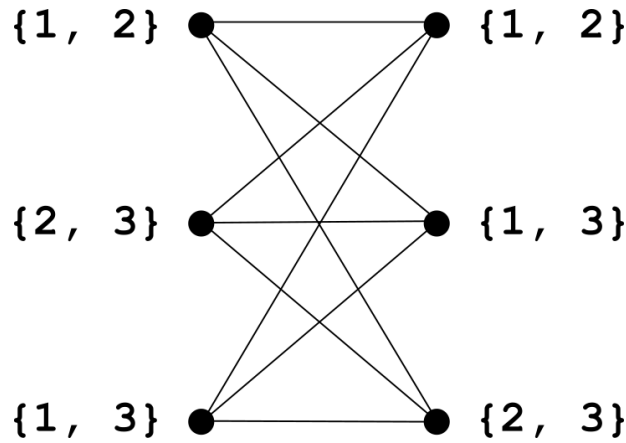
Jeśli myślisz że skoro tego nie ma w wymaganiach więc nie będzie na egzaminie, to się grubo mylisz. Byli już tacy, którzy na tym się przejechali. Nie wiem z czego wynika brak tego tematu w wymaganiach, ale czuję się zobowiązany go opisać.

9.9.4.1 Co to jest w ogóle 5-wybieralność?

Podejrzewam, że spora część czytających zaczęła wyświetlać obrazek *co.png* na twarzy gdy ujrzała frazę *5-wybieralność*. Z tego względu pozwolę sobie zdefiniować, o co w ogóle tutaj chodzi.

Mówimy, że graf G jest k -wybieralny, jeżeli po przydzieleniu każdemu wierzchołkowi jakiejś listy co najmniej k różnych kolorów na które można go pokolorować, możliwe jest jego pokolorowanie (dla dowolnego takiego przydziału list).

Przykład. Klika K_3 (znana wśród niektórych jako *trójkąt*) jest 3-wybieralna. Klika dwudzielna $K_{3,3}$ nie jest natomiast 2-wybieralna (mimo bycia 2-kolorowalną).



Rysunek 9.18: Klika dwudzielna $K_{3,3}$ z 2-elementowymi listami takimi, że grafu nie da się pokolorować poprawnie.

Zauważmy również, że jeśli graf G jest k -wybieralny, to $\chi(G) \leq k$; każdemu wierzchołkowi wystarczy dać listę k kolorów od 1 do k (bo da się go pokolorować dla dowolnego przydziału list, w szczególności również i do takiego).

Najmniejsze takie k , że graf G jest k -wybieralny, będziemy oznaczać jako $\chi_l(G)$.

9.9.4.2 5-wybieralność grafów planarnych

Niech G będzie grafem planarnym. Wtedy zachodzi:

Twierdzenie 9.9.4 (O 5-wybieralności grafów planarnych).

$$\chi_l(G) \leq 5 \quad (9.5)$$

Dowód. Dowód przeprowadzimy indukcją, do której będziemy potrzebowali nieco silniejszych założeń niż tylko, że G jest planarny i wszystkie listy są pięcioelementowe.

Założenia, które czynimy:

1. Każda wewnętrzna ściana jest trójkątem.
2. Do ściany zewnętrznej przyległe są dwa sąsiadujące wierzchołki u i v takie, że

$$|L(u)| = |L(v)| = 1, L(u) \neq L(v)$$

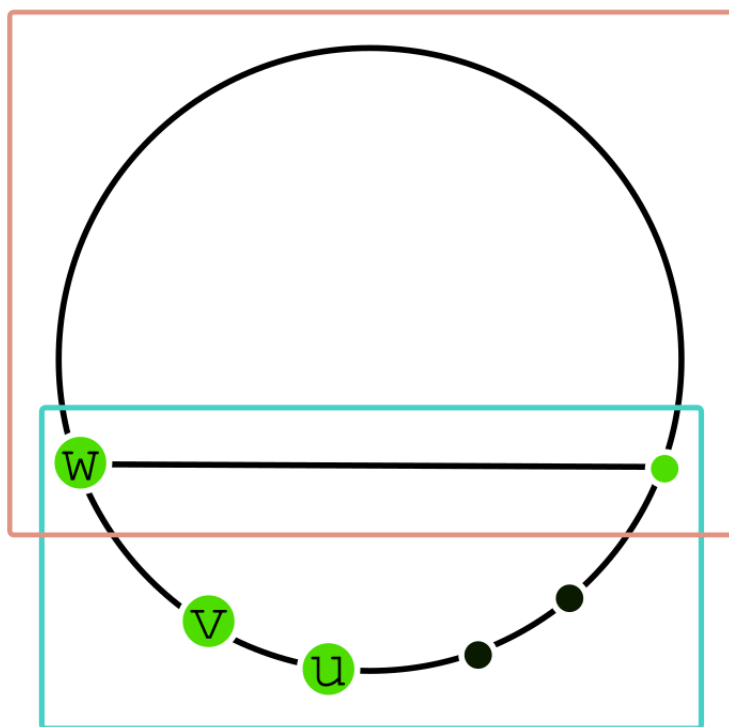
3. Pozostałe wierzchołki przyległe do ściany zewnętrznej mają listy długości 3
4. Wszystkie pozostałe wierzchołki grafu mają listy 5-elementowe

Zauważmy, że dowolny graf planarny wraz z listami 5-elementowymi jesteśmy w stanie przekształcić w graf spełniający powyższe warunki (dodając krawędzie i skracając odpowiednio listy), a uzyskane kolorowanie będzie poprawne w wyjściowym grafie.

Robimy indukcję po liczbie wierzchołków; Widzimy, że gdy G ma co najwyżej 3 wierzchołki to teza w trywialny sposób zachodzi.

Rozpatrzmy teraz graf G z jakimiś wierzchołkami v, u które są na ścianie zewnętrznej. Rozważmy sąsiada v ze ściany zewnętrznej (innego niż u). Nazwiemy go w . Rozpatrujemy teraz 2 przypadki:

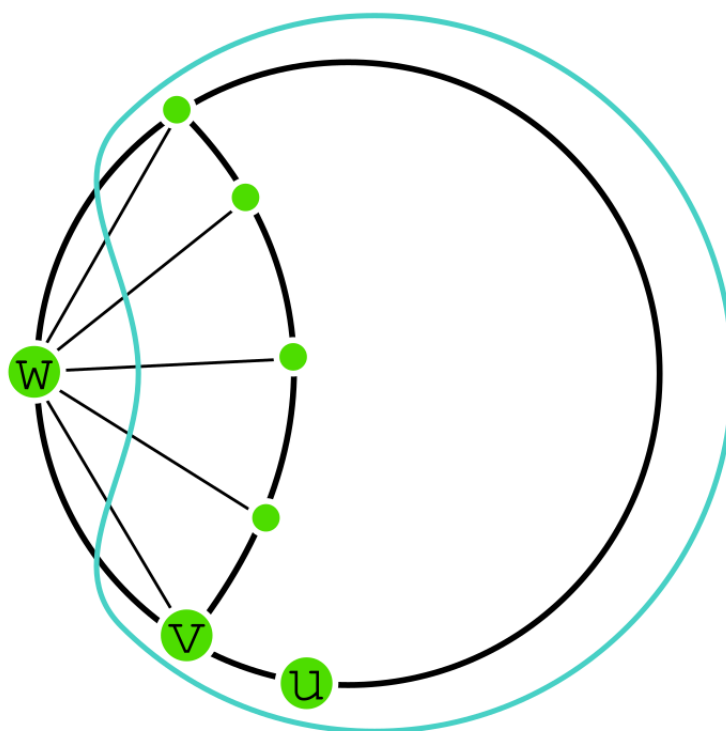
Gdy z w wychodzi jakaś „cięciwa”, tj. krawędź łącząca się z innym wierzchołkiem na ścianie zewnętrznej różnym od dwóch, z którymi w łączy się „normalnie”. Wtedy otrzymujemy „podział” grafu planarnego na 2 podgrafy. Z założenia indukcyjnego koloruję tę część, gdzie są wierzchołki v i u . Zauważamy, że po takim pokolorowaniu drugi podgraf również spełnia nasze założenia, by go indukcyjnie pokolorować (w i wierzchołek do którego prowadziła cięciwa mają już jakiś ustalony kolor; reszta wierzchołków na zewnątrz ma listy 3-elementowe a wewnątrz 5-elementowe; tu się nic nie zmieniło). Skoro tak, to go po prostu kolorujemy z założenia indukcyjnego i mamy poprawnie kolorowanie tą listą. Fajnie.



Rysunek 9.19: Z wierzchołka w wychodzi „cięciwa” która dzieli graf na 2 podgrafy; tę część, która zawiera v i u kolorujemy z założenia indukcyjnego. Wtedy w i wierzchołek którego on „dotyka” dostają już jakiś określony kolor, wobec czego dla drugiego podgrafu również możemy zastosować założenie indukcyjne.

W sytuacji, gdy z w nie ma takiej „cięciwy”, sytuacja robi się nieco śmieszniejsza, ale w sumie to nie bardzo. Oznacza to tyle, że jeśli w się łączy z jakimś wierzchołkiem, to ma on listę o 5 kolorach (chyba, że są to wierzchołki „na zewnątrz”, które będą maksymalnie 2). W takim

razie wykonujemy bardzo sprytny plan: tworzymy dwuelementowy podzbiór listy w , taki że nie ma on jedynego koloru na który możemy pokolorować v (zawsze możemy taki podzbiór utworzyć). Teraz każdemu sąsiadowi w z listą pięcioelementową przyporządkowujemy listę trójelementową, taką że nie ma ona żadnego z tamtych dwóch kolorów. Jak się to narysuje to się okaże, że graf zawierający wszystkie wierzchołki poza w , z tak zdefiniowanymi listami, możemy pokolorować z założenia indukcyjnego (rysunek powinien rozjaśnić dlaczego). Teraz dokładamy z powrotem w ; zauważamy, że musi mieć on co najmniej 1 taki kolor, że możemy go pokolorować (bo miał pułę 2 kolorów których nie współdzielił z nikim poza potencjalnie jednym wierzchołkiem, ale jak ten wierzchołek dostał kolor to na pewno zostanie nam 1 wolny). As you might've already guessed, nie mam bladego pojęcia jak to sformalizować. Whoopsie. Ale tak poza tym to właśnie dowiedliśmy co mieliśmy dowieść.



Rysunek 9.20: Z w nie wychodzi żadna „ciąciwa”, więc wszystkie wierzchołki z którymi się łączy mają listę długości 5 (poza v i jednym wierzchołkiem na okręgu). Modyfikujemy listy wierzchołkom których on dotyka i które mają 5 elementów, a potem go wywalamy; wtedy te z którymi się łączył będą na zewnątrz, i z założenia indukcyjnego możemy je pokolorować.

□

Rozdział 10

Grafy, ale nie kolorowanie

10.1 Sekwencja stopni w grafie

Twierdzenie 10.1.1 (O ciągu stopni w grafie). Niech liczby $(d_1, d_2, d_3, \dots, d_n)$ są takie, że $(d_1 \leq d_2 \leq d_3 \leq \dots d_n)$. Przez $(d'_1, d'_2, \dots, d'_{n-1})$ oznaczamy ciąg liczb taki, że:

$$d'_i = \begin{cases} d_i, & \text{gdy } i < n - d_n \\ d_i - 1, & \text{gdy } i \geq n - d_n \end{cases} \quad (10.1)$$

$(d_1 \leq d_2 \leq d_3 \leq \dots d_n)$ jest sekwencją grafową wtedy i tylko wtedy, gdy $(d'_1, d'_2, \dots, d'_{n-1})$ jest sekwencją grafową.

Dowód. To twierdzenie brzmi na początku totalnie randomowo, ale ma sens. Najlepiej chyba pokazać skąd to się wytrzasnęło, przeprowadzając dowód w drugą stronę (tzn. jeśli $(d'_1 \dots)$ to poprawny ciąg, to $(d_1 \dots)$ to również poprawna sekwencja grafowa).

No dobra, to powiedzmy że mamy poprawną sekwencję grafową (d'_1, \dots, d'_{n-1}) . Sekwencję z której ona powstała otrzymuję w ten sposób, że do grafu G który jest reprezentowany przez poprawną sekwencję po prostu dorzucam jeden wierzchołek i „podłączam” go do tylu ostatnich wierzchołków w sekwencji, żeby się „zgodziło” (czyli do d_n). Jak się spojrzy na definicję sekwencji to powinno się to robić oczywiste dlaczego to działa.

W drugą stronę jest to nieco mniej oczywiste.

Rozważmy najpierw prosty przypadek: $d_n = n - 1$. Oznacza to, że ostatni wierzchołek jest podłączony do wszystkich pozostałych wierzchołków. Zatem jeśli go usuniemy, to dostaniemy po prostu graf, którego sekwencją stopni jest $(d'_1, d'_2, \dots, d'_{n-1})$, co widać z definicji. Zatem w tym przypadku wszystko się zgadza.

Teraz rozważmy sytuację, w której $d_n < n - 1$. Chcemy pokazać, że istnieje graf, którego sekwencją stopni jest (d'_1, \dots, d'_{n-1}) . W tym celu pokażemy, że istnieje graf o sekwencji (d_1, \dots, d_n) taki, że ostatni wierzchołek jest podłączony do d_n wierzchołków bezpośrednio przed

nim. Wtedy zadziała identyczny trik z odrzuceniem tego wierzchołka i zmniejszeniem stopnia jego sąsiadom o 1, aby otrzymać elegancki graf o sekwencji (d'_1, \dots, d'_{n-1}) . Udowodnimy to nie wprost: założmy, że tak, nie jest. Sformalizujmy to założenie. Rozważmy zbiór wszystkich grafów, które mają taką sekwencję stopni, jak nasz wyjściowy graf:

$$\mathcal{G} = \{G : V(G) = \{v_1, \dots, v_n\} \wedge \forall_{i \in [n]} \deg_G(v_i) = d_i\}$$

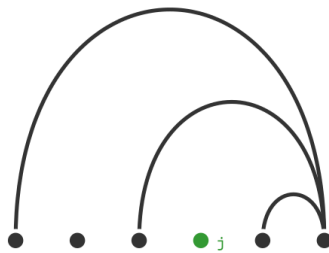
Zakładamy zatem, że dla każdego $G \in \mathcal{G}$ istnieje takie $i \in [n - d_n, n - 1]$, że $v_i v_n \notin E(G)$, tzn. każdy graf o interesującej nas sekwencji wierzchołków ma „dziurę” (nie-sąsiada) wśród d_n wierzchołków bezpośrednio poprzedzających v_n .

Możemy zatem zdefiniować fajną funkcję:

$$j: \mathcal{G} \mapsto [n - d_n, n - 1]$$

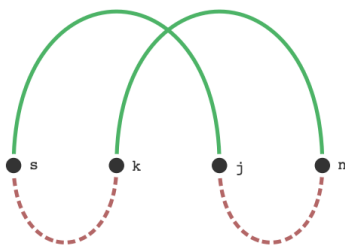
$$j(G) = \max \{i \in [n - d_n, n - 1] : v_i v_n \notin E(G)\}$$

Intuicyjnie, funkcja j wskazuje indeks najpóźniejszej „dziury” w danym grafie. Weźmy taki graf $G \in \mathcal{G}$, dla którego $j(G)$ jest *najmniejsze* możliwe (graf, który najpóźniejszą dziurę ma możliwie najwcześniej). Oczywiście wolno nam to zrobić, bo \mathcal{G} jest zbiorem skończonym. Aby uprościć zapis, przyjmijmy $j = j(G)$.



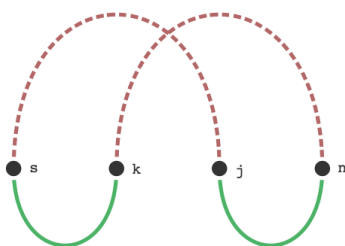
Rysunek 10.1: „Dziury” wśród d_n wierzchołków poprzedzających v_n

Wiemy, że istnieje takie $k < j$, że $v_k v_n \in E(G)$, bo inaczej wszyscy sąsiedzi v_n byłoby tuż przed nim i nie byłoby „dziury”. Wiemy też, że $d_k \leq d_j$, bo mamy do czynienia z sekwencją grafową. Ale to oznacza, że istnieje takie s , że $v_s v_j \in E(G)$, ale $v_s v_k \notin E(G)$. Dlaczego? Ponieważ, gdyby tak nie było, to v_k miałby krawędzie do wszystkich sąsiadów v_j oraz jeszcze do v_n , czyli byłoby $d_k > d_j$, co stanowi sprzeczność. Mamy więc sytuację jak poniżej:



Rysunek 10.2: Wyróżnione wierzchołki i krawędzie między nimi. Linia przerywana oznacza brak krawędzi.

Ale możemy teraz zmienić „status” wyróżnionych krawędzi, tzn. odrzucić krawędzie $v_s v_j$ i $v_k v_n$ oraz dodać krawędzie $v_s v_k$ i $v_j v_n$.



Rysunek 10.3: Wyróżnione wierzchołki po zamianie statusu krawędzi

Zauważmy, że każdy z wierzchołków, których dotknęła powyższa operacja, stracił jedną krawędź i zyskał jedną krawędź, więc sekwencja stopni nie uległa zmianie. Załataliśmy natomiast „dziurę” pod indeksem j . Mamy zatem graf G' , który ma następujące własności:

- $G' \in \mathcal{G}$, ponieważ zgadza się sekwencja grafowa. A zatem w G' jest „dziura” wśród d_n wierzchołków bezpośrednio poprzedzających v_n
- najpóźniejsza dziura znajduje się wcześniej niż pod indeksem j , bo tam była w G , a w G' została załatana

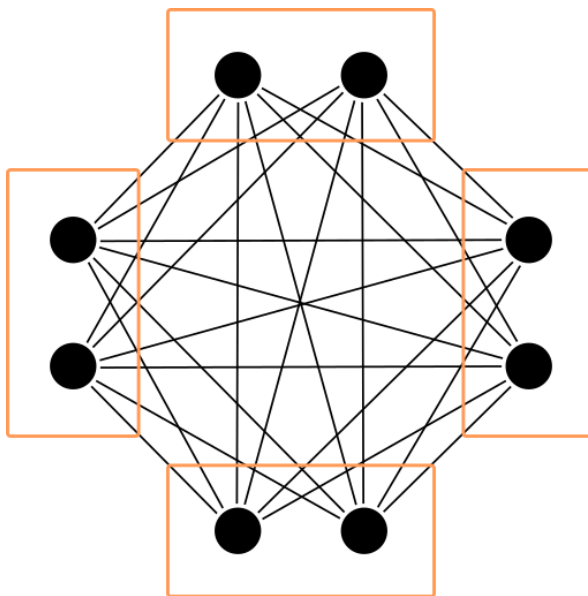
Ale przecież wybraliśmy j w taki sposób, aby było minimalne! Mamy zatem sprzeczność z wyjściowym założeniem i dowiedliśmy, że istnieje $G \in \mathcal{G}$ taki, że dla każdego $i \in [n - d_n, n - 1]$ mamy krawędź $v_i v_n$. Możemy zatem odrzucić wierzchołek v_n i uzyskać w ten sposób graf, którego sekwencją stopni jest (d'_1, \dots, d'_{n-1}) ! A to właśnie chcieliśmy udowodnić. \square

10.2 Twierdzenie Turana

Zastanawiałeś/aś się kiedyś w środku nocy, ile maksymalnie krawędzi może mieć graf na n wierzchołkach wolny od klikki rozmiaru r ? Nie? To dobrze świadczy o Twoim zdrowiu psychicznym, ale teraz niestety będziemy musieli sobie to porozwagać. Sorki.

10.2.1 Graf Turana

Na początku fajnie byłoby wiedzieć, czym jest graf Turana. Otóż graf Turana $T_{r-1}(n)$ jest to graf $r-1$ -dzielny na n wierzchołkach. Innymi słowy, dzielimy sobie a graf na $r-1$ grupiek (A_1, A_2, A_3, \dots) . Żądamy ponadto, by dla dowolnych i, j $|A_i - A_j| \leq 1$. Innymi słowy, chcemy by te „grupki” były zrównoważone. W obrębie danej grupki nie ma krawędzi między wierzchołkami, ale poza tym to wierzchołek z jakiejś grupki łączy się ze wszystkimi pozostałymi wierzchołkami z wszystkich innych grupiek. Można o tym myśleć trochę jak o bardziej ogólnej klicie dwudzielnej. W sumie to $T_2(2t)$ będzie izomorficzne z kliką dwudzielną $K_{t,t}$. Zauważmy, że $T_{r-1}(n)$ na pewno jest wolny od klikki na r wierzchołkach (to będzie ważne).



Rysunek 10.4: Graf $T_4(8)$

10.2.2 Twierdzenie Turana

Twierdzenie 10.2.1 (Turana). Dla dowolnego grafu G o n wierzchołkach, wolnego od klikki na r wierzchołkach zachodzi:

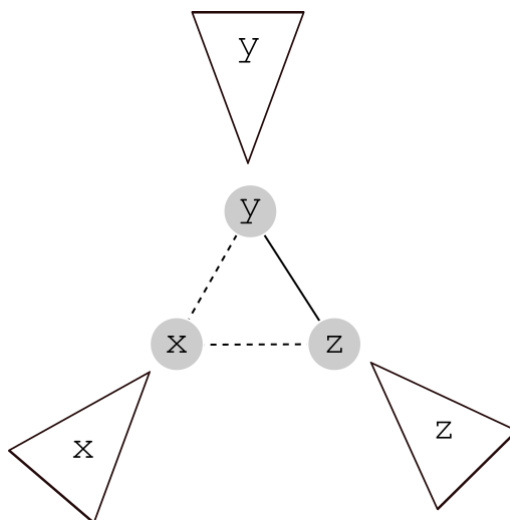
1. $|E(G)| \leq |E(T_{r-1}(n))|$
2. Jeśli $|E(G)| = |E(T_{r-1}(n))|$, to graf G jest izomorficzny z grafem $T_{r-1}(n)$.

Dowód. Uwaga, formalisci się ucieszą bo będę żonglować dziwnymi słowami. Zdefiniujemy sobie relację R , taką że para wierzchołków grafu G $(v_1, v_2) \in R$ jeżeli nie istnieje krawędź

między v_1 a v_2 . Po co nam ta relacja? Okazuje się, że w grafach Turana relacja ta jest relacją równoważności (co w sumie jest oczywiste; nie masz wierzchołka tylko do innych wierzchołków ze swojej „grupki” – innymi słowy, każda klasa równoważności stanowi oddzielną „grupkę” grafu Turana, mam nadzieję, że to widać).

No i jak sobie pomyślimy o tym to jeśli w grafie relacja ta jest relacją równoważności, to jest on prawie grafem Turana. Prawie w tym sensie, że może mieć niezrównoważoną liczbę elementów w grupkach. Jednak za pomocą dowodu *to widać* pokazujemy, że jeśli w grafie tym jest to relacja równoważności, to albo jest izomorficzny z grafem Turana albo można go „ulepszyć”, balansując grupki (a więc teza jest spełniona w tym przypadku). Nie, serio, to jest koniec dowodu w tym przypadku, nic formalniejsze nie było wyłożone.

Co robimy gdy w grafie G ta relacja nie jest relacją równoważności? Okazuje się, że możemy ją „naprawić”, tak, żeby się nią stała (jednocześnie zwiększając liczbę krawędzi, co doprowadzi nas do konkluzji że teza jest prawdziwa). Zauważmy, że jedyne co może się „popsuć” to tranzytywność (ta relacja zawsze będzie symetryczna i zwrotna). Weźmy sobie jakiś przykład wierzchołków, które w takim razie naruszają tranzytywność. Nazwijmy je x, y i z . Załóżmy, że między y i z jest krawędź, ale x nie ma krawędzi ani do y ani do z . Załóżmy też BSO, że $N(y) \geq N(z)$.

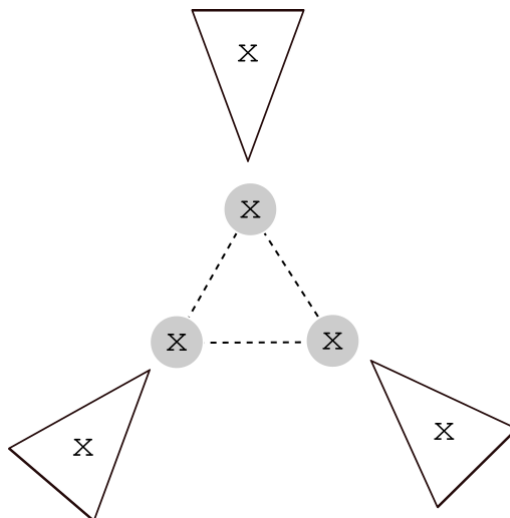


Rysunek 10.5: Przypadek przeczący tranzytywności naszej relacji: y jest w relacji z x i x w relacji z z , ale y nie jest w relacji z z (bo między y i z jest krawędź)

Rozważmy teraz 2 przypadki:

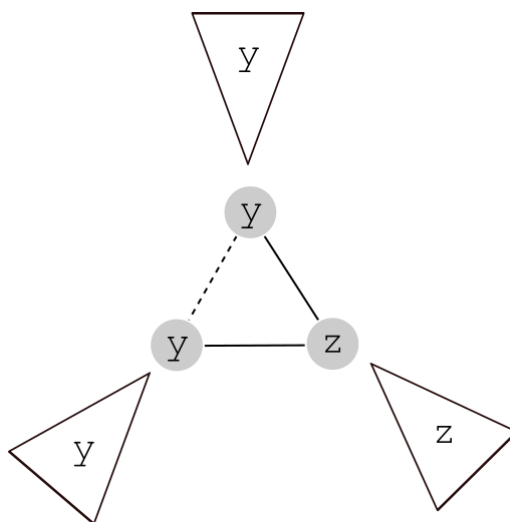
1. $|N(x)| > |N(y) \setminus \{z\}|$: Żeby „naprawić” relację, w miejsce y i z po prostu wstawiamy „kopie” x , tzn. wierzchołki które łączą się z tymi samymi wierzchołkami z którymi łączy się x . Między x a jego nowopowstałymi kopiami nie ma żadnych krawędzi. Jako, że $|N(x)| > |N(y) \setminus \{z\}| \geq |N(z) \setminus \{y\}|$ mamy, że w wyniku tego zabiegu do grafu zostały dodane co najmniej 2 krawędzie, a usunięta została jedna (ta, która łączyła y i z). Tym samym naprawiliśmy tranzytywność i zwiększyliśmy liczbę krawędzi, czyli wszystko jest

spoko (jednocześnie należy zauważyć, że na pewno nie zwiększyliśmy rozmiaru największej kliky w grafie, bo x i jego kopie nie są połączone).



Rysunek 10.6: Zamieniliśmy y i z na „kopie x ”. Jednocześnie usunęliśmy krawędź między y i z .

2. $|N(x)| \leq |N(y) \setminus \{z\}|$: Robimy tutaj podobnego fikołka jak powyżej, ale tym razem „zamieniamy” x na y oraz łączymy kopię y (czyli to co było wcześniej x) z z . W ten oto sposób tranzytywność dla tej trójki jest już okej i zwiększyliśmy liczbę krawędzi o co najmniej jedną. Jednocześnie nie zmieniliśmy rozmiaru największej kliky w grafie, bo między y a jego kopią nie ma krawędzi. *To widać.*



Rysunek 10.7: Zamieniliśmy x „kopię y ”. Jednocześnie dodaliśmy krawędź między x i z .

No i to jest koniec dowodu, bo pokazaliśmy że jak relacja równoważności nie zachodzi to możemy zwiększyć liczbę krawędzi, doprowadzając graf do grafu Turana. Ale fajne. \square