§1. Algorytmy przepływowe

Podstawowe pojęcia

Definicja.

Grafem nazywamy każdą parę $G = (V, E)$ taką, że V jest zbiorem skończonym, nazywanym *zbiorem wierzchołków grafu* G, oraz E jest podzbiorem zbioru $V \times V$, nazywanym *zbiorem krawędzi grafu* G.

Oznaczenie.

Jeśli G jest grafem, to przez V_G oznaczamy zbiór jego wierzchołków, zaś przez E_G zbiór jego krawędzi. Ponadto

$$E_G^* := E_G \cup \{(u, v) : (v, u) \in E_G\}.$$

Definicja.

Wierzchołkiem grafu G nazywamy każdy element zbioru V_G.

Definicja.

Krawędzią grafu G nazywamy każdy element zbioru E_G.

Definicja.

Siecią (*przepływową*) nazywamy każdą czwórkę $\Gamma = (G, c, s, t)$ taką, że G jest grafem, $c : E_G^* \to \mathbb{R}_+$ funkcją taką, że $c(a) > 0$ dla wszystkich $a \in E_G$ oraz $c(a) = 0$ dla wszystkich $a \in E_G^* \setminus E_G$, oraz s i t wierzchołkami grafu G, nazywanymi *źródłem* i *ujściem sieci* Γ, odpowiednio, przy czym $s \neq t$.

Definicja.

Niech $\Gamma = (G, c, s, t)$ będzie siecią oraz $a \in E_G$. *Przepustowością krawędzi* a *w sieci* Γ nazywamy liczbę $c(a)$.

Oznaczenie.

Niech V będzie zbiorem skończonym oraz $E \subset V \times V$. Jeśli $f : E \to \mathbb{R}$ oraz $X, Y \subset V$, to

$$f(X, Y) := \sum_{\substack{x \in X, y \in Y \\ (x,y) \in E}} f(x, y).$$

Definicja.

Przepływem w sieci (G, c, s, t) nazywamy każdą funkcję $f : E_G^* \to \mathbb{R}$ taką, że spełnione są następujące warunki:

(1) *warunek ograniczenia przepustowości*, tzn. $f(a) \leq c(a)$ dla wszystkich $a \in E_G^*$;

(2) *warunek skośnej symetrii*, tzn. $f(u,v) + f(v,u) = 0$ dla wszystkich $(u,v) \in E_G^*$;

(3) *warunek zachowania przepływu*, tzn. $f(u, V_G) = 0$ dla wszystkich $u \in V_G \setminus \{s,t\}$.

DEFINICJA.

Niech f będzie przepływem w sieci (G,c,s,t). *Wartością* $|f|$ *przepływu* f nazywamy liczbę $f(s, V_G)$.

DEFINICJA.

Przepływ f w sieci Γ nazywamy *maksymalnym*, jeśli

$$|f| = \max\{|f'| : f' \text{ jest przepływem w sieci } \Gamma\}.$$

PROBLEM (PROBLEM MAKSYMALNEGO PRZEPŁYWU).

Dla danej sieci przepływowej Γ znaleźć przepływ maksymalny.

LEMAT 1.1.

Niech f będzie przepływem w sieci (G,c,s,t). Wtedy:

(1) $f(X,X) = 0$ dla wszystkich $X \subset V_G$,

(2) $f(X,Y) + f(Y,X) = 0$ dla wszystkich $X, Y \subset V_G$,

(3) $f(X \cup Y, Z) = f(X,Z) + f(Y,Z) - f(X \cap Y, Z)$ oraz $f(X, Y \cup Z) = f(X,Y) + f(X,Z) - f(X, Y \cap Z)$ dla wszystkich $X, Y, Z \subset V_G$,

(4) $|f| = f(V_G, t)$.

DOWÓD.

Ćwiczenie. □

SIECI REZYDUALNE

OZNACZENIE.

Dla grafu G oraz funkcji $h : E_G^* \to \mathbb{R}_+$ definiujemy graf G_h wzorem

$$G_h := (V_G, E_h),$$

gdzie

$$E_h := \{a \in E_G^* : h(a) > 0\}.$$

DEFINICJA.

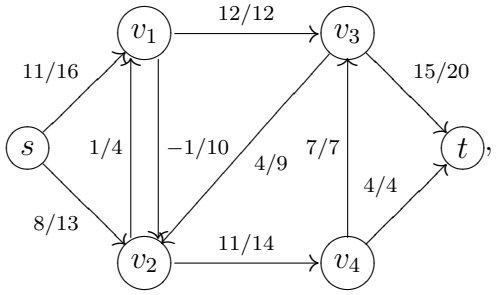
Siecią rezydualną Γ_f *przepływu* f *w sieci* $\Gamma = (G,c,s,t)$ nazywamy czwórkę $(G_{c-f}, c-f, s, t)$.

Uwaga.

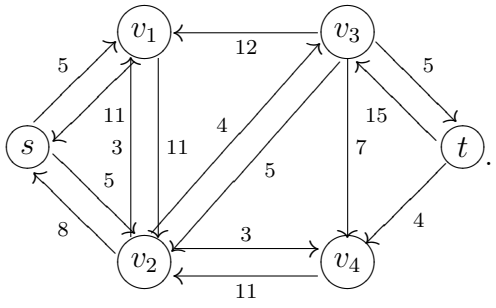
Sieć rezydualna jest siecią przepływową.

Przykład.

Jeśli sieć oraz przepływ są opisane następująco



to sieć rezydualna ma postać



Lemat 1.2.

Niech f będzie przepływem w sieci Γ. Jeśli f' jest przepływem w sieci Γ_f, to funkcja $f + f'$ jest przepływem w sieci Γ oraz $|f + f'| = |f| + |f'|$.

Dowód.

Ćwiczenie. □

Uwaga.

Niech f będzie przepływem w sieci Γ. Jeśli f' jest przepływem w sieci Γ_f, to $(\Gamma_f)_{f'} = \Gamma_{f+f'}$.

Ścieżki powiększające

Definicja.

Drogą (prostą) w grafie G nazywamy każdy ciąg $(u_0, \ldots, u_n)$, $n \in \mathbb{N}$, wierzchołków grafu G taki, że $(u_{i-i}, u_i) \in E_G$ dla wszystkich $i \in [1, n]$ (oraz $u_i \neq u_j$ dla wszystkich $i, j \in [0, n]$, $i \neq j$, odpowiednio).

DEFINICJA.
Niech $p = (u_0, \ldots, u_n)$ będzie drogą w grafie. *Początkiem σp drogi p* nazywamy wierzchołek u_0, zaś *końcem τp drogi p* nazywamy wierzchołek u_n.

DEFINICJA.
Niech G będzie grafem oraz $p = (u_0, \ldots, u_n)$ będzie drogą w grafie G. Mówimy, że *krawędź (u, v) leży na drodze p*, jeśli istnieje indeks $i \in [1, n]$ taki, że $(u_{i-1}, u_i) = (u, v)$.

DEFINICJA.
Ścieżką w sieci (G, c, s, t) nazywamy każdą drogę prostą p w grafie G taką, że $\sigma p = s$ oraz $\tau p = t$.

DEFINICJA.
Niech f będzie przepływem w sieci Γ. *Ścieżką powiększającą dla przepływu f* nazywamy każdą ścieżkę w sieci Γ_f.

DEFINICJA.
Przepustowością ścieżki p w sieci (G, c, s, t) nazywamy liczbę

$$c(p) := \min\{c(a) : \text{krawędź } a \text{ leży na drodze } p\}.$$

PRZYKŁAD.
Ciągi (s, v_1, v_2, v_3, t) oraz (s, v_2, v_3, t) są jednymi ścieżkami powiększającymi w poprzednim przykładzie. Przepustowość obu ścieżek w sieci rezydualnej jest równa 4.

UWAGA.
Ścieżkę w sieci (G, c, s, t) można znaleźć w czasie $O(|E_G|)$ (stosując przeszukiwanie wgłąb/wszerz).

DEFINICJA.
Niech p będzie ścieżką w sieci $\Gamma = (G, c, s, t)$. *Przepływem δ^p_Γ w sieci Γ związanym ze ścieżką p* nazywamy funkcję $E^*_G \to \mathbb{R}$ zdefiniowaną wzorem

$$\delta^p_\Gamma(u, v) := \begin{cases} c(p) & \text{krawędź } (u, v) \text{ leży na ścieżce } p, \\ -c(p) & \text{krawędź } (v, u) \text{ leży na ścieżce } p, \\ 0 & \text{w przeciwnym wypadku,} \end{cases} \qquad (u, v) \in E^*_G.$$

UWAGA.
Jeśli p jest ścieżką w sieci Γ, to funkcja δ^p_Γ jest przepływem w sieci Γ takim, że $|\delta^p_\Gamma| = c(p)$.

Definicja.
Zmianą f^p_Γ przepływu f w sieci Γ związaną ze ścieżką powiększającą p nazywamy funkcję $f + \delta^p_{\Gamma_f}$.

Wniosek 1.3.
Jeśli p jest ścieżką powiększającą dla przepływu f w sieci Γ, to f^p_Γ jest przepływem w sieci Γ takim, że $|f^p_\Gamma| > |f|$.

Przekroje w sieci

Definicja.
Przekrojem sieci (G, c, s, t) nazywamy każdą parę (S, T) taką, że $S, T \subset V_G$, $S \cup T = V_G$, $S \cap T = \varnothing$, $s \in S$ i $t \in T$.

Definicja.
Niech (S, T) będzie przekrojem sieci (G, c, s, t). *Przepustowością przekroju* (S, T) nazywamy liczbę $c(S, T)$.

Definicja.
Przekrój (S, T) sieci $\Gamma = (G, c, s, t)$ nazywamy *minimalnym*, jeśli

$$c(S, T) = \min\{c(S', T') : (S', T') \text{ jest przekrojem sieci } \Gamma\}.$$

Definicja.
Niech $\Gamma = (G, c, s, t)$ będzie siecią przepływową, f przepływem w sieci Γ, oraz (S, T) przekrojem sieci Γ. *Przepływem netto przekroju* (S, T) nazywamy liczbę $f(S, T)$.

Przykład.
W poprzednim przykładzie dla przekroju $(\{s, v_1, v_2\}, \{v_3, v_4, t\})$ przepustowości wynosi 26, zaś przepływ netto 19.

Lemat 1.4.
Niech (G, c, s, t) będzie siecią przepływową, f przepływem w sieci Γ, oraz (S, T) przekrojem sieci Γ. Wtedy $f(S, T) = |f|$.

Dowód.
Wiemy, że $f(S, S) = 0$ na mocy Lematu 1.1 (1), zatem

$$\begin{aligned} f(S, T) = f(S, V_G) - f(S, S) &= f(S, V_G) \\ &= f(s, V_G) + f(S \setminus s, V_G) = |f| + f(S \setminus s, V_G). \end{aligned}$$

Ponieważ $t \notin S$ na mocy definicji przekroju, więc warunek zachowania przepływu implikuje, że $f(S \setminus s, V_G) = 0$, co kończy dowód. □

Wniosek 1.5.

Jeśli f jest przepływem w sieci (G, c, s, t), to $|f| \leq c(S, T)$ dla dowolnego przekroju (S, T) sieci (G, c, s, t).

Twierdzenie 1.6 (o maksymalnym przepływie i minimalnym przekroju).

Dla przepływu f w sieci $\Gamma = (G, c, s, t)$ następujące warunki są równoważne.

(1) Przepływ f jest maksymalny.

(2) Nie istnieją ścieżki powiększające dla przepływu f.

(3) Istnieje przekrój (S, T) sieci Γ taki, że $|f| = c(S, T)$.

Dowód.

(1) ⇒ (2): Wynika natychmiast z Wniosku 1.3.

(2) ⇒ (3): Przypuśćmy, że nie istnieją ścieżki powiększające dla przepływu f oraz zdefiniujmy zbiory S i T wzorami

$$S := \{u \in V_G : \text{istnieje droga (prosta) } p \text{ w grafie } G_{c-f} \text{ taka, że } \sigma p = s \text{ i } \tau p = u\}$$

oraz $T := V_G \setminus S$. Oczywiście $s \in S$. Ponadto z założeń wynika, że $t \in T$, zatem para (S, T) jest przekrojem sieci Γ. Zauważmy, że z definicji zbioru S wynika, że $f(u, v) = c(u, v)$ dla wszystkich $u \in S$ i $v \in T$ takich, że $(u, v) \in E_G^*$. Wykorzystując Lemat 1.4 otrzymujemy zatem, że

$$|f| = f(S, T) = c(S, T).$$

(3) ⇒ (1): Wynika natychmiast z Wniosku 1.5. □

Algorytm Forda–Fulkersona

Algorytm (Algorytm Forda–Fulkersona).

```
Dane: Sieć przepływowa (G, c, s, t).
Wynik: Przepływ maksymalny f w sieci (G, c, s, t).

f := 0;
while istnieje ścieżka powiększająca p dla przepływu f do
begin
```

```
    m := min {c (a) - f (a) | krawędź a leży na ścieżce p};
    for każda krawędź (u, v) leżąca na ścieżce p do
    begin
      f (u, v) := f (u, v) + m;
      f (v, u) := f (v, u) - m;
    end;
  end;
```

Uwaga.

Jeśli $\Gamma = (G, c, s, t)$ jest siecią przepływową taką, że $c(a) \in \mathbb{N}$ dla wszystkich $a \in E_G$, to złożoność algorytmu Forda–Fulkersona wynosi $O(|E_G| \cdot |f|)$, gdzie f jest przepływem maksymalnym w sieci Γ.

Ćwiczenie.

Czy algorytm Forda–Fulkersona ma własność stopu?

Algorytm Edmondsa–Karpa

Definicja.

Niech $p = (u_0, \ldots, u_n)$ będzie drogą w grafie G. *Długością* $d(p)$ *drogi* p nazywamy liczbę n.

Definicja.

Niech u i v będą wierzchołkami grafu G. *Odległością między wierzchołkami* u *i* v nazywamy liczbę $d_G(u, v)$ zdefiniowaną wzorem

$$d_G(u, v) := \min\{d(p) \in \mathbb{N} : p \text{ jest drogą (prostą) grafie } G \text{ taką, że } \sigma p = u \text{ oraz } \tau p = v\}.$$

Uwaga.

W powyższej definicji stosujemy umowę $\min \varnothing := \infty$.

Oznaczenie.

Dla grafu G oraz funkcji $h : E_G^* \to \mathbb{R}_+$ piszemy $d_h(u, v) := d_{G_h}(u, v)$.

Definicja.

Ścieżkę p w sieci (G, c, s, t) nazywamy *minimalną*, jeśli $d(p) = d_G(s, t)$.

Uwaga.

Minimalną ścieżkę w sieci (G, c, s, t) można znaleźć stosując przeszukiwanie wszerz. Złożoność tej metody postępowania wynosi $O(|E_G|)$.

Algorytm (Algorytm Edmondsa–Karpa).

```
Dane: Sieć przepływowa (G, c, s, t).
Wynik: Przepływ maksymalny f w sieci (G, c, s, t).

f := 0;
while istnieje minimalna ścieżka powiększająca p
  dla przepływu f do
begin
  m := min {c (a) - f (a) | krawedź a leży na ścieżce p};
  for każda krawędź (u, v) leżąca na ścieżce p do
  begin
    f (u, v) := f (u, v) + m;
    f (v, u) := f (v, u) - m;
  end;
end;
```

Lemat 1.7.

Niech p będzie ścieżką minimalną w sieci $\Gamma = (G, c, s, t)$ oraz $u \in V_G$. Wtedy $d_{c-\delta^p_\Gamma}(s, u) \geq d_G(s, u)$. Ponadto, jeśli istnieje wierzchołek $v \in V_G$ taki, że $(v, u) \in E_{c-\delta^p_\Gamma} \setminus E_G$ i $d_{c-\delta^p_\Gamma}(s, v) = d_{c-\delta^p_\Gamma}(s, u) - 1$, to $d_{c-\delta^p_\Gamma}(s, u) \geq d_G(s, u) + 2$.

Uwaga.

Powyższy lemat ma oczywiście wersję dualną (dla odległości do ujścia sieci), z której także będziemy korzystać.

Dowód.

Niech $h := c - \delta^p_\Gamma$. Oczywiście możemy założyć, że $d_h(s, u) < \infty$. Udowodnimy powyższy lemat przez indukcję ze względu na $d_h(s, u)$.

Jeśli $d_h(s, u) = 0$, to $u = s$ i teza jest oczywista.

Załóżmy teraz, że $d_h(s, u) > 0$ i ustalmy $v \in V_G$ taki, że $d_h(s, v) = d_h(s, u) - 1$ oraz $(v, u) \in E_h$. Z założenia indukcyjnego wiemy, że $d_h(s, v) \geq d_G(s, v)$.

Jeśli $(v, u) \in E_G$, to mamy ciąg nierówności

$$d_G(s, u) \leq d_G(s, v) + 1 \leq d_h(s, v) + 1 = d_h(s, u),$$

który kończy dowód w tym przypadku.

Załóżmy teraz, że $(v, u) \notin E_G$. Ponieważ $(v, u) \in E_h$ oznacza to, że krawędź (u, v) leży na ścieżce p. Z minimalności ścieżki p wynika zatem, że

$$d_G(s, u) = d_G(s, v) - 1 \leq d_h(s, v) - 1 = d_h(s, u) - 2,$$

co kończy dowód. □

Definicja.

Parę $((f_0, \ldots, f_n), (p_0, \ldots, p_{n-1}))$, $n \in \mathbb{N}$, złożoną z ciągu $(f_0, \ldots, f_n)$ przepływów w sieci Γ oraz ciągu $(p_0, \ldots, p_{n-1})$ ścieżek w sieci Γ nazywamy *dopuszczalną*, jeśli p_i jest minimalną ścieżką powiększającą dla przypływu f_i taką, że $f_{i+1} = (f_i)^{p_i}_{\Gamma}$.

Twierdzenie 1.8.

Jeśli $\Gamma = (G, c, s, t)$ jest siecią przepływową, to $n \leq |V_G| \cdot |E_G|$ dla każdej pary dopuszczalnej $((f_0, \ldots, f_n), (p_0, \ldots, p_{n-1}))$.

Dowód.

Dla każdego indeksu $i \in [0, n-1]$ ustalmy wierzchołki $u_i, v_i \in V_G$ takie, że krawędź (u_i, v_i) leży na ścieżce p_i oraz $(c - f_i)(u_i, v_j) = (c - f_i)(p_i)$. Wiemy, że $(u_i, v_i) \in E^*_G$ dla każdego indeksu $i \in [0, n-1]$. Dla dowodu twierdzenia wystarczy zatem pokazać, że

$$|\{i \in [0, n-1] : (u_i, v_i) = a\}| \leq \frac{|V_G|}{2}$$

dla każdej krawędzi $a \in E^*_G$.

Ustalmy krawędź $(u, v) \in E^*_G$ oraz niech

$$\{i \in [0, n-1] : (u_i, v_i) = (u, v)\} = \{i_0 < \cdots < i_m\}.$$

Przez indukcję, że względu na j pokażemy, że

$$d_{c-f_{i_j}}(s, u) \geq 2 \cdot j$$

dla wszystkich indeksów $j \in [0, m]$, co zakończy dowód, gdyż z minimalności ścieżki p_{i_m} wynika, że $u \neq t$, a więc $d_{c-f_{i_m}}(s, u) \leq |V_G| - 2$.

Dla $j = 0$ powyższa teza jest oczywista, załóżmy zatem, że $j > 0$. Dla uproszczenia notacji definiujemy $k := i_{j-1}$ oraz $l := i_j$. Z założenia indukcyjnego wiemy, że

$$d_{c-f_k}(s, u) \geq 2 \cdot j - 2.$$

Ponadto z założeń wynika, że $d_{c-f_k}(s, v) = d_{c-f_k}(s, u) + 1$. Zauważmy również, że $(u, v) \notin E_{c-f_{k+1}}$, zatem istnieje indeks $i \in [k+1, l-1]$ taki, że $(u, v) \in E_{c-f_{i+1}} \setminus E_{c-f_i}$. To oznacza, że krawędź (v, u) leży na na ścieżce p_i, zatem $d_{c-f_i}(s, u) = d_{c-f_i}(s, v) + 1$. Stosując teraz Lemat 1.7 oraz powyższe równości uzyskujemy, że

$$d_{c-f_l}(s,u) \geq d_{c-f_i}(s,u) = d_{c-f_i}(s,v) + 1 \geq d_{c-f_k}(s,v) + 1 = d_{c-f_k}(s,u) + 2 \geq 2 \cdot j,$$

co kończy dowód. □

Uwaga.

Niech $\Gamma = (G, c, s, t)$ będzie siecią przepływową. Powyższe twierdzenie implikuje, że złożoność obliczeniowa algorytmu Edmondsa–Karpa wynosi $O(|V_G| \cdot |E_G|^2)$.

Przepływy blokujące

Definicja.

Przepływem blokującym w sieci $\Gamma = (G, c, s, t)$ nazywamy każdy przepływ $b \neq 0$ w sieci Γ taki, że spełnione są następujące warunki:

(1) istnieje para dopuszczalna $((f_0, \ldots, f_n), (p_0, \ldots, p_{n-1}))$ taka, że $f_0 = 0$, $f_n = b$ oraz $d(p_i) = d_G(s,t)$ dla każdego indeksu $i \in [0, n-1]$,

(2) dla każdej ścieżki minimalnej p w sieci Γ istnieje krawędź a leżąca na ścieżce p taka, że $c(a) = b(a)$.

Algorytm (Dinica znajdowania maksymalnego przepływu).

```
Dane: Sieć przepływowa (G, c, s, t).
Wynik: Przepływ maksymalny f w sieci (G, c, s, t).

f := 0;
while istnieje ścieżka powiększająca dla przepływu f do
begin
  znajdź przepływ blokujący b w sieci rezydualnej;
  f := f + b;
end;
```

Lemat 1.9.

Jeśli b jest przepływem blokującym w sieci $\Gamma = (G, c, s, t)$, to $d_{c-b}(s,t) > d_G(s,t)$.

Dowód.

Jeśli $d_{c-b}(s,t) = \infty$, to teza jest oczywista (warunek $b \neq 0$ implikuje, że $d_G(s,t) < \infty$). Załóżmy zatem, że $d_{c-b}(s,t) < \infty$. Niech p będzie ścieżką minimalną w sieci Γ_b.

Załóżmy najpierw, że ścieżka p jest drogą w grafie G. Wtedy oczywiście

$d(p) \geq d_G(s,t)$. Gdyby $d(p) = d_G(s,t)$, to droga p byłaby ścieżką minimalną w sieci Γ, zatem istniałaby krawędź a leżąca na ścieżce p taka, że $c(a) = b(a)$. Wtedy jednak $a \notin E_{c-b}$, co prowadzi do sprzeczności.

Załóżmy teraz, że ścieżka p nie jest drogą w sieci Γ. Ustalmy także parę dopuszczalna $((f_0, \ldots, f_n), (p_0, \ldots, p_{n-1}))$ taką, że $f_0 = 0$, $f_n = b$ oraz $d(p_i) = d_G(s,t)$ dla każdego $i \in [0, n-1]$. Ponieważ ścieżka p jest drogą w grafie G_{c-f_n} oraz nie jest drogą w grafie G_{c-f_0}, więc istnieje indeks $i \in [1, n]$ taki, że ścieżka p jest drogą w grafie G_{c-f_i}, ale nie jest drogą w grafie $G_{c-f_{i-1}}$. Z Lematu 1.7 wiemy oczywiście, że $d(p) = d_{c-f_n}(s,t) \geq d_{c-f_i}(s,t)$.

Przypuśćmy najpierw, że $d(p) > d_{c-f_i}(s,t)$. Wtedy z Lematu 1.7 wynika, że

$$d_{c-b}(s,t) = d(p) > d_{c-f_i}(s,t) \geq d_{c-f_0}(s,t) = d_G(s,t),$$

co kończy dowód w tym przypadku.

Przypuśćmy teraz, że $d(p) = d_{c-f_i}(s,t)$. Wtedy droga p jest ścieżką minimalną w sieci Γ_{f_i}. Ustalmy krawędź (u,v) leżącą na ścieżce p taką, że $(u,v) \notin E_{c-f_{i-1}}$. Zauważmy, że $d_{c-f_i}(s,u) = d_{c-f_i}(s,v) - 1$. Korzystając zatem z Lematu 1.7 i jego dualnej wersji wiemy, że $d_{c-f_i}(s,v) \geq d_{c-f_{i-1}}(s,v) + 2$ oraz $d_{c-f_i}(v,t) \geq d_{c-f_{i-1}}(v,t)$. Stąd otrzymujemy, że

$$\begin{aligned} d_{c-b}(s,t) = d_{c-f_i}(s,t) &= d_{c-f_i}(s,v) + d_{c-f_i}(v,t) \\ &\geq d_{c-f_{i-1}}(s,v) + 2 + d_{c-f_{i-1}}(v,t) \geq d_{c-f_{i-1}}(s,t) + 2 \geq d_G(s,t), \end{aligned}$$

co kończy dowód. □

Wniosek 1.10.

Niech $(f_0, \ldots, f_n)$ będzie ciągiem przepływów w sieci $\Gamma = (G, c, s, t)$ takim, że dla każdego indeksu $i \in [1, n]$ istnieje przepływ blokujący b w sieci $\Gamma_{f_{i-1}}$ taki, że $f_i = f_{i-1} + b$. Wtedy $n \leq |V_G| - 1$.

Dowód.

Możliwe wartości $d_{c-f}(s,t)$ dla przepływu f w sieci Γ należą do zbioru $[1, |V_G| - 1] \cup \{\infty\}$. □

Znajdowanie przepływu blokującego

Definicja.

Grafem warstwowym dla sieci $\Gamma = (G, c, s, t)$ nazywamy graf $G_\Gamma := (V_G, E_\Gamma)$, gdzie

$$E_\Gamma := \{(u,v) \in E_G : d_G(u,t) = d_G(v,t) + 1\}.$$

Uwaga.

Niech $\Gamma = (G, c, s, t)$ będzie siecią taką, że $d_G(s, t) < \infty$. Jeśli $u \in V_G$, $u \neq s$, oraz istnieje droga z wierzchołka s do wierzchołka u w grafie G_Γ, to istnieje droga z wierzchołka u do wierzchołka t. Powyższa własność implikuje, że drogę z wierzchołka s do wierzchołka t w grafie warstwowym możemy znaleźć w czasie $O(|V_G|)$.

Uwaga.

Graf warstwowy dla sieci (G, c, s, t) można znaleźć stosując przeszukiwanie wszerz. Złożoność tej metody postępowania wynosi $O(|E_G|)$.

Definicja.

Przepustowością wierzchołka $u \in V_G$ w sieci (G, c, s, t) nazywamy liczbę $c(u)$ zdefiniowaną następująco

$$c(u) := \min\{c(V_G, u), c(u, V_G)\}.$$

Algorytm (Dinica znajdowania przepływu blokującego).

```
Dane: Sieć przepływowa (G, c, s, t).
Wynik: Przepływ blokujący b dla sieci (G, c, s, t).

b := 0;
V := zbiór krawędzi grafu G;
E := zbiór krawędzi grafu warstwowego dla sieci (G, c, s, t);
while istnieje droga p w grafie (V, E) z wierzchołka s do
  wierzchołka t do
begin
  m := min {c (a) | krawędź a leży na ścieżce p};
  for każda krawędź (u, v) leżąca na ścieżce p do
  begin
    b (u, v) := b (u, v) + m;
    b (v, u) := b (v, u) - m;
    c (u, v) := c (u, v) - m;
    c (v, u) := c (v, u) + m;
  end;
  for każda krawędź (u, v) leżąca na ścieżce p do
    if c (u, v) = 0 then
    begin
      usuń krawędź (u, v) ze zbioru E;
      if c (u) = 0 then
        usuń rekurencyjnie ze zbioru V wierzchołek v oraz
```

```
            wcześniejsze wierzchołki w, dla których c (w) = 0
            (usuwając też sąsiadujące krawędzie ze zbioru E);
    end;
end;
```

Uwaga.

Rekurencyjna procedura usuwania wierzchołków o zerowej przepustowości ma na celu zachowanie własności, o której mowa w uwadze po definicji grafu warstowego.

Uwaga.

Niech (G, c, s, t) będzie siecią przepływową. Złożoność obliczeniowa powyższego algorytmu wynosi $O(|V_G| \cdot |E_G|)$. Stąd złożoność algorytmu Dinica znajdowania maksymalnego przepływu wynosi $O(|V_G|^2 \cdot |E_G|)$.

Algorytm trzech Hindusów

Uwaga.

Tytułowymi trzema Hindusami są Malhort, Kumar i Maheshwari.

Algorytm (MKM znajdowania przepływu blokującego).

```
Dane: Sieć przepływowa (G, c, s, t).
Wynik: Przepływ blokujący b dla sieci (G, c, s, t).

b := 0;
V := zbiór wierzchołków grafu G;
E := zbiór krawędzi grafu warstwowego dla sieci (G, c, s, t);
for każda krawędź (u, v) grafu G do
  if (u, v) nie należy do zbioru E then
    c (u, v) := 0;
while zbiór V jest niepusty do
begin
  znajdź wierzchołek u o minimalnej przepustowości;
  prześlij c (u) jednostek z wierzchołka u do wierzchołka t
    nasycając kolejne krawędzie w zbiorze E;
  cofnij c (u) jednostek z wierzchołka u do wierzchołka s
    nasycając kolejne krawędzie w zbiorze E;
  usuń wierzchołek u ze zbioru V;
  usuń krawędzie sąsiadujące z wierzchołkiem u ze zbioru E;
end;
```

Uwaga.

Niech (G, c, s, t) będzie siecią przepływową. Złożoność obliczeniowa powyższego algorytmu wynosi $O(|V_G|^2)$. Zatem złożoność algorytmu Dinica znajdowania maksymalnego przepływu wykorzystującego algorytm trzech Hindusów do znajdowania przepływu blokującego wynosi $O(|V_G|^3)$.

§2. Więcej kombinatoryki

Więcej o szeregach formalnych

Założenie.

Wszystkie rozważane szeregi są szeregami o wyrazach zespolonych.

Definicja.

Mówimy, że *szereg* $\mathcal{A} = \sum_{n\in\mathbb{N}} a_n T^n$ *jest granicą ciągu* $(\mathcal{A}_m)_{m\in\mathbb{N}}$ *szeregów* $\mathcal{A}_m = \sum_{n\in\mathbb{N}} a_{m,n} T^n$, $m \in \mathbb{N}$ (piszemy $\lim_{m\to\infty} \mathcal{A}_m = \mathcal{A}$), jeśli dla każdego indeksu $n \in \mathbb{N}$ istnieje indeks $M \in \mathbb{N}$ taki, że $a_{m,n} = a_n$ dla wszystkich indeksów $m \geq M$.

Przykład.

Dla każdego szeregu $\mathcal{A} = \sum_{n\in\mathbb{N}} a_n T^n$ mamy $\mathcal{A} = \lim_{m\to\infty} A_m$, gdzie $A_m := \sum_{n\in[0,m]} a_n T^n$, $m \in \mathbb{N}$.

Lemat 2.1.

Jeśli $\mathcal{A} := \lim_{m\to\infty} \mathcal{A}_m$ oraz $\mathcal{B} := \lim_{m\to\infty} \mathcal{B}_m$ dla $\mathcal{A}_m, \mathcal{B}_m \in \mathbb{C}[[T]]$, $m \in \mathbb{N}$, to

$$\lim_{m\to\infty} (\mathcal{A}_m + \mathcal{B}_m) = \mathcal{A} + \mathcal{B} \quad \text{oraz} \quad \lim_{m\to\infty} (\mathcal{A}_m \cdot \mathcal{B}_m) = \mathcal{A} \cdot \mathcal{B}.$$

Dowód.

Ćwiczenie. □

Przypomnienie.

Niech $\varphi : R \to S$ będzie homomorfizmem pierścieni oraz $s \in S$. Wtedy istnieje jedyny homomorfizm pierścieni $\psi : R[T] \to S$ taki, że $\psi|_R = \varphi$ oraz $\psi(T) = s$. Piszemy $h(s) := \psi(h)$ dla każdego wielomianu $h \in R[T]$.

Oznaczenie.

Jeśli $\mathcal{A} = \sum_{n\in\mathbb{N}} a_n T^n$, to $\mathcal{A}(0) := a_0$.

Lemat 2.2.

Niech $\mathcal{A} = \sum_{n\in\mathbb{N}} a_n T^n$ oraz $\mathcal{A}_m := \sum_{n\in[0,m]} a_n T^n$, $m \in \mathbb{N}$. Jeśli $\mathcal{B}(0) = 0$ dla $\mathcal{B} \in \mathbb{C}[[T]]$, to istnieje $\lim_{m\to\infty} \mathcal{A}_m(\mathcal{B})$.

Dowód.

Ćwiczenie. □

Oznaczenie.

Niech $\mathcal{A} = \sum_{n\in\mathbb{N}} a_n T^n$ oraz $\mathcal{A}_m := \sum_{n\in[0,m]} a_n T^n$, $m \in \mathbb{N}$. Jeśli $\mathcal{B}(0) = 0$ dla $\mathcal{B} \in \mathbb{C}[[T]]$, to

$$\mathcal{A}(\mathcal{B}) := \lim_{m\to\infty} \mathcal{A}_m(\mathcal{B}).$$

OZNACZENIE.

Jeśli $\mathcal{A} = \sum_{n\in\mathbb{N}} a_n T^n$, to

$$\operatorname{ldeg} \mathcal{A} := \min\{n \in \mathbb{N} : a_n \neq 0\}.$$

LEMAT 2.3.

Jeśli $\mathcal{A}_m \in \mathbb{C}[[T]]$, $m \in \mathbb{N}$, są takie, że $\lim_{m\to\infty} \operatorname{ldeg} \mathcal{A}_m = \infty$, to istnieje $\lim_{m\to\infty} \sum_{i\in[0,m]} \mathcal{A}_i$.

DOWÓD.

Ćwiczenie. □

OZNACZENIE.

Jeśli $\mathcal{A}_m \in \mathbb{C}[[T]]$, $m \in \mathbb{N}$, są takie, że $\lim_{m\to\infty} \operatorname{ldeg} \mathcal{A}_m = \infty$, to

$$\sum_{m\in\mathbb{N}} \mathcal{A}_m := \lim_{m\to\infty} \sum_{i\in[0,m]} \mathcal{A}_i.$$

LEMAT 2.4.

Jeśli $\mathcal{A}_m \in \mathbb{C}[[T]]$, $m \in \mathbb{N}$, są takie, że $\lim_{m\to\infty} \operatorname{ldeg}(\mathcal{A}_m - 1) = \infty$, to istnieje $\lim_{m\to\infty} \prod_{i\in[0,m]} \mathcal{A}_i$.

DOWÓD.

Ćwiczenie. □

OZNACZENIE.

Jeśli $\mathcal{A}_m \in \mathbb{C}[[T]]$, $m \in \mathbb{N}$, są takie, że $\lim_{m\to\infty} \operatorname{ldeg}(\mathcal{A}_m - 1) = \infty$, to

$$\prod_{m\in\mathbb{N}} \mathcal{A}_m := \lim_{m\to\infty} \prod_{i\in[0,m]} \mathcal{A}_i.$$

DEFINICJA.

Pochodną szeregu $\mathcal{A} = \sum_{n\in\mathbb{N}} a_n T^n$ nazywamy szereg $\mathcal{A}'$ zdefiniowany wzorem

$$\mathcal{A}' := \sum_{n\in\mathbb{N}_+} n \cdot a_n \cdot T^{n-1}.$$

Lemat 2.5.
Jeśli $\mathcal{A} = \lim_{m\to\infty} \mathcal{A}_m$ dla $\mathcal{A}_m \in \mathbb{C}[[T]]$, $m \in \mathbb{N}$, to $\mathcal{A}' = \lim_{m\to\infty} \mathcal{A}'_m$.

Dowód.
Ćwiczenie. □

Wniosek 2.6.
Niech $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[T]]$.

(1) Jeśli $\mathcal{C} := \mathcal{A} + \mathcal{B}$, to $\mathcal{C}' = \mathcal{A}' + \mathcal{B}'$.

(2) Jeśli $\mathcal{C} := \mathcal{A} \cdot \mathcal{B}$, to $\mathcal{C}' = \mathcal{A}' \cdot \mathcal{B} + \mathcal{A} \cdot \mathcal{B}'$.

(3) Jeśli $\mathcal{B}(0) = 0$ oraz $\mathcal{C} := \mathcal{A}(\mathcal{B})$, to $\mathcal{C}' = \mathcal{A}'(\mathcal{B}) \cdot \mathcal{B}'$.

Dowód.
Ćwiczenie. □

Wniosek 2.7.
Niech $\mathcal{A}_m \in \mathbb{C}[T]$, $m \in \mathbb{N}$, będą takie, że $\lim_{m\to\infty} \operatorname{ldeg} \mathcal{A}_m = \infty$. Jeśli $\mathcal{A} := \sum_{m\in\mathbb{N}} \mathcal{A}_m$, to $\mathcal{A}' = \sum_{m\in\mathbb{N}} \mathcal{A}'_m$.

Oznaczenie.
Jeśli $\mathcal{A}(0) = 1$ dla $\mathcal{A} \in \mathbb{C}[[T]]$, to

$$\ln \mathcal{A} := \mathcal{L}(\mathcal{A} - 1),$$

gdzie

$$\mathcal{L} := \sum_{n\in\mathbb{N}_+} \frac{(-1)^{n-1}}{n} \cdot T^n.$$

Lemat 2.8.

(1) Jeśli $\mathcal{A}(0) = 1 = \mathcal{B}(0)$ dla $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[T]]$, to

$$\ln(\mathcal{A} \cdot \mathcal{B}) = \ln \mathcal{A} + \ln \mathcal{B}.$$

(2) Jeśli $\mathcal{A}(0) = 1$ oraz $\mathcal{B} := \ln \mathcal{A}$ dla $\mathcal{A} \in \mathbb{C}[[T]]$, to

$$\mathcal{B}' = \frac{\mathcal{A}'}{\mathcal{A}}.$$

(3) Niech $\mathcal{A}_m \in \mathbb{C}[T]$, $m \in \mathbb{N}$, będą takie, że $\mathcal{A}_m(0) = 1$ dla każdego $m \in \mathbb{N}$. Jeśli $\mathcal{A} = \lim_{m\to\infty} \mathcal{A}_m$, to

$$\ln \mathcal{A} = \lim_{m\to\infty} \ln \mathcal{A}_m.$$

Dowód.
Ćwiczenie. □

Podziały

Definicja.
Podziałem liczby $n \in \mathbb{N}$ nazywamy każdy ciąg $\lambda = (\lambda_1, \lambda_2, \ldots)$ liczb całkowitych nieujemnych taki, że $\sum_{i \in \mathbb{N}_+} \lambda_i = n$ oraz $\lambda_i \geq \lambda_{i+1}$ dla każdego indeksu $i \in \mathbb{N}_+$.

Oznaczenie.
Jeśli λ jest podziałem liczby $n \in \mathbb{N}$, to piszemy $\lambda \vdash n$.

Definicja.
Wysokością podziału λ nazywamy liczbę $h(\lambda)$ zdefiniowaną wzorem

$$h(\lambda) := \max\{i \in \mathbb{N} : \lambda_i > 0\}.$$

Definicja.
Jeśli λ jest podziałem, to liczby $\lambda_1, \ldots, \lambda_{h(\lambda)}$ nazywamy *częściami podziału* λ.

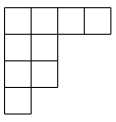
Uwaga.
Każdy ciąg $(\lambda_1, \ldots, \lambda_h)$ liczb całkowitych nieujemnych takich, że $\lambda_1 \geq \cdots \geq \lambda_h$ utożsamiamy z podziałem

$$(\lambda_1, \ldots, \lambda_h, 0, 0, \ldots).$$

Definicja.
Podziałem dualnym do podziału λ nazywamy ciąg $\tilde{\lambda}$ zdefiniowany wzorem

$$\tilde{\lambda}_i := |\{j \in \mathbb{N}_+ : \lambda_j \geq i\}|, \qquad i \in \mathbb{N}_+.$$

Uwaga.
Podziały przedstawia się często graficznie w postaci tzw. diagramów Younga. Diagram Younga podziału λ składa się lewostronnie wyrównanych wierszy złożonych z kwadratów jednostkowych, przy czym w wierszu i znajduje się λ_i kwadratów. Np. diagram Younga podziału $(4, 2, 2, 1)$ ma postać



W tej interpretacji podział dualny zlicza ilość kwadratów w poszczególnych kolumnach diagramu Younga. Stąd widać, że podziałem dualnym do podziału $(4, 2, 2, 1)$ jest podział $(4, 3, 1, 1)$.

Uwaga.
Niech $n \in \mathbb{N}$. Jeśli $\lambda \vdash n$, to

$$\tilde{\lambda}_i - \tilde{\lambda}_{i+1} = |\{j \in \mathbb{N} : \lambda_j = i\}|$$

dla każdego indeksu $i \in \mathbb{N}_+$.

Lemat 2.9.
Niech $n \in \mathbb{N}$. Jeśli $\lambda \vdash n$, to

$$\sum_{i \in \mathbb{N}_+} i \cdot (\tilde{\lambda}_i - \tilde{\lambda}_{i+1}) = n.$$

Dowód.
Korzystając z poprzedniej uwagi otrzymujemy, że

$$\sum_{i \in \mathbb{N}_+} i \cdot (\tilde{\lambda}_i - \tilde{\lambda}_{i+1}) = \sum_{i \in \mathbb{N}_+} i \cdot |\{j \in \mathbb{N}_+ : \lambda_j = i\}| = \sum_{j \in \mathbb{N}_+} \lambda_j = n,$$

co kończy dowód.

Wniosek 2.10.
Niech $n \in \mathbb{N}$. Jeśli $\lambda \vdash n$, to $\tilde{\lambda} \vdash n$.

Dowód.
Z poprzedniej uwagi wiemy, że $\tilde{\lambda}_i \geq \tilde{\lambda}_{i+1}$ dla każdego $i \in \mathbb{N}_+$. Ponadto wykorzystując poprzedni lemat dostajemy, że

$$\begin{aligned}\sum_{i \in \mathbb{N}_+} \tilde{\lambda}_i &= \sum_{i \in \mathbb{N}_+} \sum_{j \in [i, \infty)} (\tilde{\lambda}_j - \tilde{\lambda}_{j+1}) = \sum_{j \in \mathbb{N}_+} \sum_{i \in [1, j]} (\tilde{\lambda}_j - \tilde{\lambda}_{j+1}) \\ &= \sum_{j \in \mathbb{N}_+} j \cdot (\tilde{\lambda}_j - \tilde{\lambda}_{j+1}) = n. \quad \square\end{aligned}$$

Lemat 2.11.
Niech $n \in \mathbb{N}$, $\lambda \vdash n$, $i, j \in \mathbb{N}$. Wtedy $\lambda_i \geq j$ wtedy i tylko wtedy, gdy $\tilde{\lambda}_j \geq i$.

Dowód.
Ćwiczenie.

WNIOSEK 2.12.
Jeśli $n \in \mathbb{N}$ i $\lambda \vdash n$, to $\tilde{\tilde{\lambda}} = \lambda$.

DOWÓD.
Ustalmy $i \in \mathbb{N}$. Wtedy

$$\tilde{\tilde{\lambda}}_i = |\{j \in \mathbb{N} : \tilde{\lambda}_j \geq i\}| = |\{j \in \mathbb{N} : \lambda_i \geq j\}| = \lambda_i,$$

co kończy dowód. □

OZNACZENIE.
Niech $X \subset \mathbb{N}_+$. Wtedy

$$\mathcal{P}_X := \sum_{n \in \mathbb{N}} p_{n,X} \cdot T^n,$$

gdzie dla liczby $n \in \mathbb{N}$ definiujemy

$$p_{n,X} := |P_{n,X}|$$

i

$$P_{n,X} := \{\lambda \vdash n : \lambda_i \in X \text{ dla wszystkich } i \in [1, h(\lambda)]\}.$$

Ponadto $\mathcal{P} := \mathcal{P}_{\mathbb{N}_+}$ oraz $p_n := p_{n,\mathbb{N}_+}$ i $P_n := P_{n,\mathbb{N}_+}$ dla $n \in \mathbb{N}$.

UWAGA.
Powyższy wniosek oznacza w szczególności, że dla każdego $n \in \mathbb{N}$ funkcja $P_n \to P_n$, $\lambda \mapsto \tilde{\lambda}$, jest bijekcją.

LEMAT 2.13.
Niech $n \in \mathbb{N}_+$ i $X \subset \mathbb{N}_+$, oraz

$$P'_{n,X} := \{(l_i)_{i \in X} : l_i \in \mathbb{N} \text{ dla każdego indeksu } i \in X \text{ oraz } \sum_{i \in X} i \cdot l_i = n\}.$$

Wtedy $|P'_{n,X}| = p_{n,X}$.

DOWÓD.
Zauważmy najpierw, że zbiór $P'_{n,X}$ jest równoliczny ze zbiorem

$$P''_{n,X} := \{(l_i)_{i \in \mathbb{N}} : l_i \in \mathbb{N} \text{ dla każdego indeksu } i \in \mathbb{N},$$
$$l_i = 0 \text{ dla każdego indeksu } i \in \mathbb{N} \setminus X \text{ oraz } \sum_{i \in X} i \cdot l_i = n\}.$$

Ponadto $\tilde{\lambda}_i = \tilde{\lambda}_{i+1}$ dla każdego indeksu $i \in \mathbb{N}_+ \setminus X$ oraz każdego podziału $\lambda \in P_{n,X}$. Stąd funkcja $P_{n,X} \to P''_{n,X}$ dana wzorem

$$\lambda \mapsto (\tilde{\lambda}_i - \tilde{\lambda}_{i+1})_{i\in\mathbb{N}}$$

jest dobrze określona bijekcją, co kończy dowód. □

Stwierdzenie 2.14.
Jeśli $X \subset \mathbb{N}_+$, to

$$\mathcal{P}_X = \prod_{m\in X} \frac{1}{1-T^m}.$$

Dowód.
Ponieważ

$$\frac{1}{1-T^m} = \sum_{n\in\mathbb{N}} T^{n\cdot m},$$

więc współczynnik przy T^n w szeregu $\prod_{m\in X} \frac{1}{1-T^m}$ jest równy mocy zbioru $|P'_{n,X}|$ z poprzedniego lematu, co kończy dowód. □

Oznaczenie.
Dla liczby $n \in \mathbb{N}_+$ piszemy

$$\sigma(n) := \sum_{\substack{d\in[1,n]\\ d|n}} d.$$

Wniosek 2.15.
Dla każdego $n \in \mathbb{N}_+$ mamy

$$p_n = \frac{1}{n} \sum_{i\in[1,n]} \sigma(i) \cdot p_{n-i}.$$

Dowód.
Z poprzedniego stwierdzenia wynika, że

$$\ln \mathcal{P} = -\sum_{m\in\mathbb{N}_+} \ln(1-T^m),$$

skąd

$$\frac{\mathcal{P}'}{\mathcal{P}} = \sum_{m\in\mathbb{N}_+} \frac{m\cdot T^{m-1}}{1-T^m} = \sum_{m\in\mathbb{N}_+} \sum_{j\in\mathbb{N}} m \cdot T^{m-1+m\cdot j}.$$

Ostatecznie

$$T \cdot \mathcal{P}' = \mathcal{P} \cdot \sum_{m \in \mathbb{N}_+} \sum_{j \in \mathbb{N}_+} m \cdot T^{mj} = \mathcal{P} \cdot \sum_{n \in \mathbb{N}_+} \sigma(n) \cdot T^n.$$

Porównując współczynniki powyższych szeregów otrzymujemy tezę. □

Oznaczenie.

Dla liczby $n \in \mathbb{N}$ definiujemy

$$Q_n := \{\lambda \vdash n : \lambda_i > \lambda_{i+1} \text{ dla wszystkich } i \in [1, h(\lambda) - 1]\},$$

i $q_n := |Q_n|$. Ponadto

$$\mathcal{Q} := \sum_{n \in \mathbb{N}} q_n \cdot T^n.$$

Uwaga.

Zauważmy, że

$$\mathcal{Q} = \prod_{m \in \mathbb{N}_+} (1 + T^m).$$

Twierdzenie 2.16.

Jeśli $X := 2 \cdot \mathbb{N} + 1$, to $p_{n,X} = q_n$ dla każdej liczby $n \in \mathbb{N}$.

Dowód.

Wystarczy pokazać, że $\mathcal{Q} = \mathcal{P}_X$. Zauważmy jednak, że

$$\mathcal{Q} = \prod_{m \in \mathbb{N}_+} (1 + T^m) = \prod_{m \in \mathbb{N}_+} \frac{1 - T^{2 \cdot m}}{1 - T^m} = \prod_{m \in X} \frac{1}{1 - T^m} = \mathcal{P}_X,$$

co kończy dowód. □

Uwaga.

W powyższym dowodzie wykorzystujemy równość

$$\lim_{m \to \infty} \prod_{\substack{i \in [1,m] \\ 2 \cdot i > m}} (1 - T^{2 \cdot i}) = 1,$$

będąca konsekwencją równości

$$\lim_{m \to \infty} \operatorname{ldeg} \left(\prod_{\substack{i \in [1,m] \\ 2 \cdot i > m}} (1 - T^{2 \cdot i}) - 1 \right) = \infty.$$

Oznaczenie.
Jeśli $n \in \mathbb{N}$, to $(T)_n := \prod_{i\in[1,n]}(1-T^i)$.

Definicja.
Wielomianem Gaussa dla liczb $m \in \mathbb{N}$ *i* $n \in \mathbb{Z}$ nazywamy szereg $\begin{bmatrix} m \\ n \end{bmatrix}$ zdefiniowany wzorem

$$\begin{bmatrix} m \\ n \end{bmatrix} := \begin{cases} \frac{(T)_m}{(T)_n \cdot (T)_{m-n}} & n \in [0,m], \\ 0 & \text{w przeciwnym wypadku.} \end{cases}$$

Lemat 2.17.
Niech $m \in \mathbb{N}$ i $n \in \mathbb{Z}$.
(1) $\begin{bmatrix} m \\ 0 \end{bmatrix} = 1 = \begin{bmatrix} m \\ m \end{bmatrix}$.
(2) $\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} m \\ m-n \end{bmatrix}$.
(3) Jeśli $m > 0$ i $n \geq 0$, to $\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} m-1 \\ n-1 \end{bmatrix} + T^n \cdot \begin{bmatrix} m-1 \\ n \end{bmatrix}$.
(4) Jeśli $n \in [0,m]$, to $\begin{bmatrix} m \\ n \end{bmatrix} \in \mathbb{C}[T]$ oraz $\deg \begin{bmatrix} m \\ n \end{bmatrix} = n \cdot (m-n)$.
(5) $\begin{bmatrix} m \\ n \end{bmatrix}(1) = \binom{m}{n}$.

Dowód.
Ćwiczenie. □

Oznaczenie.
Niech $k, l \in \mathbb{N}$. Jeśli $n \in \mathbb{N}$, to

$$P_n(k,l) := \{\lambda \vdash n : \lambda_1 \leq k \text{ i } h(\lambda) \leq l\}$$

i $p_n(k,l) := |P_n(k,l)|$. Ponadto

$$\mathcal{G}(k,l) := \sum_{n\in\mathbb{N}} p_n(k,l) \cdot T^n.$$

Twierdzenie 2.18.
Jeśli $k, l \in \mathbb{N}$, to $\mathcal{G}(k,l) = \begin{bmatrix} k+l \\ k \end{bmatrix}$.

Dowód.
Dla dowodu powyższego twierdzenia wystarczy pokazać, że $\mathcal{G}(k,l) = 1$ jeśli $k = 0$ lub $l = 0$ oraz $\mathcal{G}(k,l) = \mathcal{G}(k-1,l) + T^k \cdot \mathcal{G}(k,l-1)$ jeśli $k,l > 0$. Zauważmy, że jeśli $k = 0$ lub $l = 0$, to

$$P_n(k,l) = \begin{cases} \{(0,0,\ldots)\} & n = 0, \\ \varnothing & n > 0, \end{cases}$$

co dowodzi pierwszej części. Druga cześć równoważna jest temu, że dla każdej liczby $n \in \mathbb{N}$ mamy równość

$$p_n(k,l) = p_n(k-1,l) + p_{n-k}(k,l-1),$$

gdzie $p_{n-k}(k,l-1) := 0$ dla $n \in [0,k-1]$. W celu dowodu powyższej równości rozważmy funkcję $f : P_n(k-1,l) \cup P_{n-k}(k,l-1) \to P_n(k,l)$ daną wzorem

$$f(\lambda) := \begin{cases} \lambda & \lambda \in P_n(k-1,l), \\ (k,\lambda_1,\lambda_2,\ldots) & \lambda \in P_{n-k}(k,l-1), \end{cases}$$

gdzie podobnie jak poprzednio $P_{n-k}(k,l-1) = \varnothing$ dla $n \in [0,k-1]$. Zauważmy, że funkcja f jest bijekcją – funkcja odwrotna $g : P_n(k,l) \to P_n(k-1,l) \cup P_{n-k}(k,l-1)$ dana jest wzorem

$$g(\lambda) := \begin{cases} \lambda & \lambda_1 \leq k-1, \\ (\lambda_2,\lambda_3,\ldots) & \lambda_1 = k, \end{cases} \quad \lambda \in P_n(k,l),$$

co kończy dowód. □

Oznaczenie.
Dla liczby $m \in \mathbb{Z}$ definujemy

$$\omega(m) := \frac{1}{2} \cdot m \cdot (3 \cdot m - 1).$$

Uwaga.
Jeśli $m \in \mathbb{N}_+$, to

$$\omega(-m) := \frac{1}{2} \cdot m \cdot (3 \cdot m + 1).$$

Uwaga.
Liczby $\omega(m)$, $m \in \mathbb{Z}$, są parami różne.

Oznaczenie.
Dla liczby $n \in \mathbb{N}$ definiujemy

$$Q'_n := \{\lambda \in Q_n : 2 \mid h(\lambda)\} \qquad \text{i} \qquad Q''_n := \{\lambda \in Q_n : 2 \nmid h(\lambda)\},$$

oraz $q'_n := |Q'_n|$ i $q''_n := |Q''_n|$.

Twierdzenie 2.19.
Niech $n \in \mathbb{N}$.

(1) Jeśli $n \notin \{\omega(m) : m \in \mathbb{Z}\}$, to $q'_n = q''_n$.

(2) Jeśli $n = \omega(m)$ dla pewnej liczby $m \in \mathbb{Z}$, to $q'_n = q''_n + (-1)^m$.

DOWÓD.

Dla $n = 0$ teza wynika z bezpośredniego sprawdzenia, załóżmy zatem, że $n > 0$. Dla liczby $m \in \mathbb{N}_+$ definiujemy

$$\lambda'^{(m)} := (2m-1, \ldots, m) \qquad \text{i} \qquad \lambda''^{(m)} := (2m, \ldots, m+1).$$

Zauważmy, że

- $\lambda'^{(m)} \in Q'_n$ wtedy i tylko wtedy, gdy $2 \mid m$ oraz $n = \omega(m)$,
- $\lambda'^{(m)} \in Q''_n$ wtedy i tylko wtedy, gdy $2 \nmid m$ oraz $n = \omega(m)$,
- $\lambda''^{(m)} \in Q'_n$ wtedy i tylko wtedy, gdy $2 \mid m$ oraz $n = \omega(-m)$,
- $\lambda''^{(m)} \in Q''_n$ wtedy i tylko wtedy, gdy $2 \nmid m$ oraz $n = \omega(-m)$.

Niech $L := \{\lambda'^{(m)}, \lambda''^{(m)} : m \in \mathbb{N}_+\}$. Dla podziału $\lambda \in Q_n$ definiujemy

$$b(\lambda) := \max\{i \in [1, h(\lambda)] : \lambda_i = \lambda_1 - i + 1\}$$

i

$$d(\lambda) := \lambda_{h(\lambda)}.$$

Definiujemy funkcję $f : Q_n \setminus L \to Q_n \setminus L$ wzorem

$$f(\lambda) := \begin{cases} (\lambda_1 - 1, \ldots, \lambda_{b(\lambda)} - 1, \lambda_{b(\lambda)+1}, \ldots, \lambda_{h(\lambda)}, b(\lambda)) & \lambda_{h(\lambda)} > b(\lambda), \\ (\lambda_1 + 1, \ldots, \lambda_{d(\lambda)} + 1, \lambda_{d(\lambda)+1}, \ldots, \lambda_{h(\lambda)-1}) & \lambda_{h(\lambda)} \leq b(\lambda). \end{cases}$$

Zauważmy, że $(f \circ f)(\lambda) = \lambda$ dla wszystkich podziałów $\lambda \in Q_n \setminus L$, zatem funkcja f jest bijekcją. Ponadto $f(Q'_n \setminus L) = Q''_n \setminus L$, co kończy dowód. □

WNIOSEK 2.20.

Jeśli $n \in \mathbb{N}_+$, to

$$p_n = \sum_{m \in \mathbb{N}_+} (-1)^{m+1} \cdot (p_{n-\omega(m)} + p_{n-\omega(-m)}),$$

gdzie $p_{-k} := 0$ dla $k \in \mathbb{N}_+$.

Dowód.

Zauważmy, że

$$\sum_{n\in\mathbb{N}}(q'_n - q''_n)\cdot T^n = \prod_{m\in\mathbb{N}_+}(1-T^i),$$

zatem korzystając ze Stwierdzenia 2.14 otrzymujemy, że

$$\mathcal{P}\cdot\sum_{n\in\mathbb{N}}(q'_n - q''_n)\cdot T^n = 1.$$

Z drugiej strony poprzednie twierdzenie oznacza, że

$$\sum_{n\in\mathbb{N}}(q'_n - q''_n)\cdot T^n = 1 + \sum_{m\in\mathbb{N}_+}(-1)^m\cdot(T^{\omega(m)} + T^{\omega(-m)}).$$

Ostatecznie

$$\mathcal{P}\cdot\Big(1 + \sum_{m\in\mathbb{N}_+}(-1)^m\cdot(T^{\omega(m)} + T^{\omega(-m)})\Big) = 1.$$

Porównując współczynniki przy T^n dla $n\in\mathbb{N}_+$ otrzymujemy tezę. □

Zagadnienia minimaksowe

Definicja.

Łańcuchem w zbiorze uporządkowanym P nazywamy każdy podzbiór L zbioru P taki, że $a\le b$ lub $b\le a$ dla wszystkich elementów $a,b\in L$.

Definicja.

Łańcuch L w zbiorze uporządkowanym P nazywamy *maksymalnym*, jeśli $L = L'$ dla każdego łańcucha L' w zbiorze P takiego, że $L\subset L'$.

Definicja.

Antyłańcuchem w zbiorze uporządkowanym P nazywamy każdy podzbiór A zbioru P taki, że $a\not\le b$ i $b\not\le a$ dla wszystkich elementów $a,b\in A$, $a\neq b$.

Oznaczenie.

Dla zbioru częściowo uporządkowanego P definiujemy

$$M_P := \max\{|A| : A \text{ jest antyłańcuchem w zbiorze } P\}.$$

Twierdzenie 2.21 (Dilworth).

Jeśli P jest skończonym zbiorem częściowo uporządkowanym, to

$$M_P = \min\Big\{m \in \mathbb{N} : \text{istnieją łańcuchy } L_1, \ldots, L_m \text{w zbiorze } P \text{ takie, że } P = \bigcup_{i\in[1,m]} L_i\Big\}.$$

Dowód.

Zauważmy najpierw, że jeśli $P = \bigcup_{i\in[1,m]} L_i$ dla łańcuchów $L_1, \ldots, L_m$ w zbiorze P oraz A jest antyłańcuchem w zbiorze P, to $|A \cap L_i| \leq 1$ dla każdego indeksu $i \in [1, m]$, więc $|A| \leq m$. Dla dowodu twierdzenia wystarczy zatem pokazać, że istnieją łańcuchy $L_1, \ldots, L_{M_P}$ w zbiorze P takie, że $P = \bigcup_{i\in[1,M_P]} L_i$. Fakt ten udowodnimy przez indukcję ze względu na $|P|$. Teza jest oczywiście prawdziwa, gdy $|P| = 0$, załóżmy zatem, że $|P| > 0$.

Niech L będzie łańcuchem maksymalnym w zbiorze P i $M := M_{P\setminus L}$. Jeśli $M \leq M_P - 1$, to teza wynika bezpośrednio z założenia indukcyjnego, załóżmy zatem, że $M = M_P$. Ustalmy antyłańcuch A w zbiorze $P\setminus L$ taki, że $|A| = M$. Niech

$$S^+ := \{x \in P : \text{istnieje element } a \in A \text{ taki, że } a \leq x\}$$

i

$$S^- := \{x \in P : \text{istnieje element } a \in A \text{ taki, że } x \leq a\}.$$

Ponieważ $|A| = M_P$, więc $S^+ \cup S^- = P$. Ponadto $\max S^- = A$ i $\min S^+ = A$. Z maksymalności łańcucha L wynika, że $\max L \notin S^-$ oraz $\min L \notin S^+$, a więc w szczególności $|S^-|, |S^+| < |P|$. Istotnie, gdyby $\max L \in S^-$, to istniałby element $a \in A$ taki, że $\max L \leq a$. Ponieważ $L \cap A = \varnothing$, więc zbiór $L \cup \{a\}$ byłby łańcuchem takim, że $L \subsetneq L \cup \{a\}$, co jest niemożliwe.

Z założenia indukcyjnego istnieją łańcuchy $L_1^-, \ldots, L_M^-$ i $L_1^+, \ldots, L_M^+$ takie, że $S^- = \bigcup_{i\in[1,M]} L_i^-$ i $S^+ = \bigcup_{i\in[1,M]} L_i^+$. Ponieważ $|L_i^- \cap A| = 1 = |L_i^+ \cap A|$ dla każdego indeksu $i \in [1, M]$, więc możemy bez straty ogólności założyć, że $L_i^- \cap A = L_i^+ \cap A$ dla każdego indeksu $i \in [1, M]$. Wtedy jednak

$$\max L_i^- = L_i^- \cap A = L_i^+ \cap A = \min L_i^+,$$

a więc zbiór $L_i := L_i^- \cup L_i^+$ jest łańcuchem, dla każdego indeksu $i \in [1, M]$. Ponadto $P = \bigcup_{i\in[1,M]} L_i$, co kończy dowód. □

Twierdzenie 2.22 (Erdős–Szerkes).

Niech $r, s \in \mathbb{N}$ oraz $a = (a_1, \ldots, a_{r\cdot s+1})$ będzie ciągiem liczb rzeczywistych. Wtedy albo istnieje słabo rosnący podciąg ciągu a długości $r + 1$ lub istnieje ściśle malejący podciąg ciągu a długości $s + 1$.

Dowód.

W zbiorze $P := [1, r \cdot s + 1]$ definiujemy relację $\preceq$ wzorem: $i \preceq j$ wtedy i tylko wtedy, gdy $i \leq j$ i $a_i \leq a_j$. Wtedy łańcuchy w zbiorze P odpowiadają podciągom słabo rosnącym ciągu a, podczas gdy antyłańcuchy w zbiorze P odpowiadają podciągom malejącym. Jeśli w ciągu a nie ma podciągu malejącego długości $s+1$, to z poprzedniego twierdzenia wynika, że zbiór P może być pokryty s łańcuchami. Jeden z tych łańcuchów musi mieć co najmniej $r + 1$ elementów, co kończy dowód. □

Oznaczenie.

Dla zbioru częściowo uporządkowanego P definiujemy

$$M'_P := \max\{|L| : L \text{ jest łańcuchem w zbiorze } P\}.$$

Twierdzenie 2.23.

Jeśli P jest skończonym zbiorem częściowo uporządkowanym, to

$$M'_P = \min\Big\{m \in \mathbb{N} : \text{istnieją antyłańcuchy } A_1, \ldots, A_m \text{ w zbiorze } P \text{ takie, że } P = \bigcup_{i\in[1,m]} A_i\Big\}.$$

Dowód.

Podobnie jak w dowodzie twierdzenia Dilwortha zauważmy, że jeśli $P = \bigcup_{i\in[1,m]} A_i$ dla antyłańcuchów $A_1, \ldots, A_m$ w zbiorze P oraz L jest łańcuchem w zbiorze P, to $|L \cap A_i| \leq 1$ dla każdego indeksu $i \in [1, m]$, więc $|L| \leq m$. Dla dowodu twierdzenia wystarczy zatem pokazać, że istnieją antyłańcuchy A_1, $\ldots$, $A_{M'_P}$ takie, że $P = \bigcup_{i\in[1,M'_P]} A_i$. Fakt ten udowodnimy przez indukcję ze względu na M'_P.

Teza jest w oczywisty sposób prawdziwa, gdy $M'_P = 0$, załóżmy zatem, że $M'_P > 0$ oraz niech $A := \max P$. Oczywiście zbiór A jest antyłańcuchem. Ponadto $M'_{P\setminus A} = M'_P - 1$, więc teza wynika z założenia indukcyjnego. □

Oznaczenie.

Dla zbioru skończonego X definiujemy

$$\mathcal{P}(X) := \{Y : Y \subset X\}.$$

Uwaga.

Jeśli X jest zbiorem skończonym, to zbiór $\mathcal{P}(X)$ jest częściowo uporządkowany przez relację inkluzji.

Definicja.

Rodziną Spernera podzbiorów zbioru skończonego X nazywamy każdy antyłańcuch w zbiorze $\mathcal{P}(X)$.

Oznaczenie.

Dla zbioru skończonego X definiujemy

$$\mathcal{S}(X) := \{\sigma : [1, n] \to X : \text{funkcja } \sigma \text{ jest bijekcją}\},$$

gdzie $n := |X|$.

Uwaga.

Niech X będzie zbiorem skończonym. Funkcja $F : \mathcal{S}(X) \to \mathcal{P}(X)^{n+1}$, gdzie $n := |X|$, dana dla $\sigma \in \mathcal{S}(X)$ wzorem

$$F(\sigma) := (C_0^\sigma, \ldots, C_n^\sigma),$$

gdzie

$$C_i^\sigma := \{\sigma(1), \ldots, \sigma(i)\}$$

dla $i \in [0, n]$, ustala bijekcję pomiędzy zbiorem $\mathcal{S}(X)$ oraz zbiorem łańcuchów maksymalnych w zbiorze $\mathcal{P}(X)$. W szczególności, jeśli $A \subset X$, to

$$|\{\mathcal{L} : \mathcal{L} \text{ jest łańcuchem maksymalnym w zbiorze } \mathcal{P}(X) \text{ i } A \in \mathcal{L}\}| = |A|! \cdot (|X| - |A|)!.$$

Twierdzenie 2.24.

Jeśli $\mathcal{A}$ jest rodziną Spernera podzbiorów zbioru skończonego X, to

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{|X|}{|A|}} \leq 1.$$

Dowód.

Niech

$$\mathcal{B}_A := \{\mathcal{L} : \mathcal{L} \text{ jest łańcuchem maksymalnym w zbiorze } \mathcal{P}(X) \text{ i } A \in \mathcal{L}\}$$

dla $A \in \mathcal{A}$. Zauważmy, że $\mathcal{B}_A \cap \mathcal{B}_B = \varnothing$ dla wszystkich zbiorów $A, B \in \mathcal{A}$ takich, że $A \neq B$. Stąd na mocy poprzedniej uwagi

$$\left| \bigcup_{A \in \mathcal{A}} \mathcal{B}_A \right| = \sum_{A \in \mathcal{A}} |A|! \cdot (|X| - |A|)!.$$

Z drugiej strony poprzednia uwaga implikuje również, że

$$\left|\bigcup_{A\in\mathcal{A}} \mathcal{B}_A\right| \leq |X|!,$$

co kończy dowód. □

Wniosek 2.25.
Jeśli $\mathcal{A}$ jest rodziną Spernera podzbiorów zbioru skończonego X, to

$$|\mathcal{A}| \leq \binom{|X|}{\lfloor |X|/2 \rfloor}.$$

Dowód.
Wystarczy zauważyć, że $\binom{|X|}{|A|} \leq \binom{|X|}{\lfloor |X|/2 \rfloor}$ dla każdego zbioru $A \in \mathcal{P}(X)$. □

Teoria Ramseya

Oznaczenie.
Dla zbioru skończonego X oraz liczby $r \in \mathbb{N}_+$ definiujemy

$$\mathcal{P}_r(X) := \{A \in \mathcal{P}(X) : |A| = r\}.$$

Definicja.
Niech X będzie zbiorem skończonym oraz $r, t \in \mathbb{N}_+$. *t-kolorowaniem r-elementowych podzbiorów zbioru X* nazywamy każdą funkcję $\mathcal{P}_r(X) \to [1, t]$.

Definicja.
Niech $r, t, q_1, \ldots, q_t \in \mathbb{N}_+$. *Liczbą Ramseya* $R(q_1, \ldots, q_t; r)$ nazywamy najmniejszą liczbę $N \in \mathbb{N}_+$ taką, że dla każdego zbioru skończonego X takiego, że $|X| \geq N$, oraz dla każdego kolorowania $f : \mathcal{P}_r(X) \to [1, t]$ istnieją indeks $i \in [1, t]$ oraz podzbiór $Y \subset X$ takie, że $|Y| \geq q_i$ oraz $f(Z) = i$ dla każdego zbioru $Z \in \mathcal{P}_r(Y)$.

Lemat 2.26.
Jeśli $t, q_1, \ldots, q_t \in \mathbb{N}_+$, to

$$R(q_1, \ldots, q_t; 1) = q_1 + \cdots + q_t - t + 1.$$

Dowód.
Zauważmy, że

$$q_1 + \cdots + q_t - t + 1 = (q_1 - 1) + \cdots + (q_t - 1) + 1,$$

co natychmiast implikuje tezę. □

Lemat 2.27.

Jeśli $r, t, q_1, \ldots, q_t \in \mathbb{N}_+$ są takie, że $r > 1$ i istnieje indeks $i \in [1, t]$ taki, że $q_i = 1$, to

$$R(q_1, \ldots, q_t; r) = 1.$$

Dowód.

Oczywiste. □

Stwierdzenie 2.28.

Niech $r, t, q_1, \ldots, q_t \in \mathbb{N}_+$ będą takie, że $r > 1$ oraz $q_i > 1$ dla wszystkich $i \in [1, t]$. Jeśli

$$Q_i := R(q_1, \ldots, q_{i-1}, q_i - 1, q_{i+1}, \ldots, q_t; r) < \infty$$

dla wszystkich indeksów $i \in [1, t]$, to

$$R(q_1, \ldots, q_t; r) \leq R(Q_1, \ldots, Q_t; r - 1) + 1.$$

Dowód.

Bez straty ogólności możemy założyć, że $R(Q_1, \ldots, Q_t; r - 1) < \infty$. Niech X będzie zbiorem skończonym takim, że

$$|X| \geq R(Q_1, \ldots, Q_t; r - 1) + 1.$$

Ustalmy kolorowanie $f : \mathcal{P}_r(X) \to [1, t]$ oraz element $x \in X$. Niech $X' := X \setminus \{x\}$ i zdefiniujmy kolorowanie $f' : \mathcal{P}_{r-1}(X') \to [1, t]$ wzorem

$$f'(Z') := f(Z' \cup \{x\})$$

dla $Z' \in \mathcal{P}_{r-1}(X')$. Ponieważ $|X'| \geq R(Q_1, \ldots, Q_t; r - 1)$, więc istnieją podzbiór $Y' \subset X'$ oraz indeks $i \in [1, t]$ takie, że $|Y'| \geq Q_i$ oraz $f'(Z') = i$ dla wszystkich podzbiorów $Z' \in \mathcal{P}_{r-1}(Y')$. Korzystając z definicji liczby Q_i wiemy, że istnieją podzbiór $Y \subset Y'$ oraz indeks $j \in [1, t]$ takie, że $|Y| \geq q_j - \delta_{i,j}$ oraz $f(Z) = j$ dla wszystkich podzbiorów $Z \in \mathcal{P}_r(Y)$, gdzie

$$\delta_{i,j} := \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$$

Jeśli $i \neq j$, to dowód jest zakończony. Jeśli $i = j$, to dla zbioru $Y'' := Y \cup \{x\}$ mamy $|Y''| \geq q_i$ oraz $f(Z) = i$ dla wszystkich podzbiorów $Z \in \mathcal{P}_r(Y'')$. □

Twierdzenie 2.29.
Jeśli $r, t, q_1, \ldots, q_t \in \mathbb{N}_+$, to

$$R(q_1, \ldots, q_t; r) < \infty.$$

Dowód.
Wynika natychmiast przez indukcję z powyższego stwierdzenia i poprzedzających go lematów. □

Oznaczenie.
Dla $a, b \in \mathbb{N}_+$ definiujemy

$$R(a, b) := R(a, b; 2).$$

Twierdzenie 2.30.
Jeśli $a, b \in \mathbb{N}_+$, to

$$R(a, b) \leq \binom{a+b-2}{b-1}.$$

Dowód.
Jeśli $a = 1$ lub $b = 1$, to teza wynika natychmiast z Lematu 2.27, załóżmy zatem, że $a > 1$ i $b > 1$. Korzystając ze Stwierdzenia 2.28, Lematu 2.26 i założenia indukcyjnego otrzymujemy wtedy, że

$$\begin{aligned} R(a, b; 2) &\leq R(R(a-1, b), R(a, b-1); 1) + 1 = R(a-1, b) + R(a, b-1) \\ &\leq \binom{a+b-3}{b-1} + \binom{a+b-3}{b-2} = \binom{a+b-2}{b-1}, \end{aligned}$$

co kończy dowód. □

Twierdzenie 2.31.
Jeśli $a, b \in \mathbb{N}_+$, to $R(a, b) \geq (a-1) \cdot (b-1) + 1$.

Dowód.
Jeśli $a = 1$ lub $b = 1$, to teza jest oczywista, załóżmy zatem, że $a > 1$ i $b > 1$. Dla $X := [1, (a-1) \cdot (b-1)]$ definiujemy kolorowanie $f : \mathcal{P}_2(X) \to [1, 2]$ wzorem

$$f(\{x, y\}) := \begin{cases} 1 & \lfloor \frac{x}{a-1} \rfloor = \lfloor \frac{y}{a-1} \rfloor, \\ 2 & \text{w przeciwnym wypadku.} \end{cases}$$

Jeśli $Y \subset X$ i $|Y| \geq a$, to istnieją elementy $x, y \in Y$ takie, że $\lfloor \frac{x}{a-1} \rfloor \neq \lfloor \frac{y}{a-1} \rfloor$, a więc $f(\{x, y\}) = 2$. Podobnie, gdy $Y \subset X$ i $|Y| \geq b$, to istnieją elementy $x, y \in Y$ takie, że $x \neq y$ i $\lfloor \frac{x}{a-1} \rfloor = \lfloor \frac{y}{a-1} \rfloor$, a więc $f(\{x, y\}) = 1$. □

Twierdzenie 2.32.

Niech $n \in \mathbb{N}_+$, $n \geq 3$. Jeśli $N \geq R(n, n; 3)$, to dla każdego zbioru S punktów na płaszczyźnie, z których żadne trzy nie są współliniowe, takiego, że $|S| = N$, istnieje podzbiór $T \subset S$ taki, że $|T| = n$ i punkty należące do zbioru T są wierzchołkami wielokąta wypukłego.

Dowód.

Niech T będzie zbiorem punktów na płaszczyźnie, z których żadne trzy nie są współliniowe. Zauważmy, że punkty należące do zbioru T są wierzchołkami wielokąta wypukłego wtedy i tylko wtedy, gdy dla dowolnych parami różnych punktów $A, B, C, D \in T$ punkt D nie leży wewnątrz trójkąta ABC.

Ustalmy $N \geq R(n, n; 3)$ oraz zbiór S punktów na płaszczyźnie, z których żadne trzy nie są współliniowe, taki, że $|S| = N$. Ustalmy bijekcję $F : [1, N] \to S$ i rozważmy kolorowanie $f : \mathcal{P}_3([1, N]) \to [1, 2]$ dane wzorem

$$f(\{i, j, k\}) := \begin{cases} 1 & \text{trójkąt } F(i)F(j)F(k) \text{ jest dodatnio zorientowany,} \\ 2 & \text{w przeciwnym wypadku,} \end{cases}$$

dla $i, j, k \in [1, N]$, $i < j < k$. Z założenia wiemy, że istnieje podzbiór $Y \subset [1, N]$ oraz liczba $i \in [1, 2]$ takie, że $|Y| = n$ oraz $f(Z) = i$ dla każdego $Z \in \mathcal{P}_3(Y)$. Bez straty ogólności możemy założyć, że $i = 1$. Pokażemy, że punkty należące do zbioru $F(Y)$ są wierzchołkami wielokąta wypukłego.

Przypuśćmy, że istnieją parami różne liczby $i, j, k, l \in Y$ takie, że punkt $F(l)$ leży wewnątrz trójkąta $F(i)F(j)F(k)$, przy czym $i < j < k$. Ponieważ $f(\{i, j, l\}) = 1$, więc $l \notin [i, j]$. Podobnie, warunek $f(\{j, k, l\}) = 1$ implikuje, że $l \notin [j, k]$. Z drugiej strony, warunek $f(\{i, k, l\}) = 1$ oznacza, że $l \in [i, k]$, co prowadzi do sprzeczności. □

§3. Elementy teorii kodowania

Ciała skończone

Oznaczenie.
Jeśli $p \in \mathbb{P}$, to definiujemy $\mathbb{F}_p := \mathbb{Z}/p$.

Stwierdzenie 3.1.
Jeśli $\mathbb{F}$ jest ciałem skończonym, to istnieje wyznaczona jednoznacznie liczba pierwsza p taka, że istnieje homomorfizm $\mathbb{F}_p \to \mathbb{F}$.

Definicja.
Liczbę p z powyższego stwierdzenia nazywamy *charakterystyką ciała* $\mathbb{F}$.

Uwaga.
Jeśli $\varphi : \mathbb{F} \to \mathbb{F}'$ jest homomorfizmem ciał, to funkcja φ jest injekcją.

Dowód.
Istnieje jedyny homomorfizm pierścieni $\mathbb{Z} \to \mathbb{F}$. Liczba p jest generatorem jądra tego homomorfizmu. □

Wniosek 3.2.
Jeśli $\mathbb{F}$ jest ciałem skończonym charakterystyki p, to istnieje liczba $n \in \mathbb{N}_+$ taka, że $|\mathbb{F}| = p^n$.

Dowód.
Zauważmy, że ciało $\mathbb{F}$ jest przestrzenią liniową nad ciałem $\mathbb{F}_p$, zatem $|\mathbb{F}| = |\mathbb{F}_p|^{\dim_{\mathbb{F}_p} \mathbb{F}}$. □

Definicja.
Jeśli $f \in \mathbb{F}[X]$, $f \neq 0$, to definiujemy

$$\mathbb{F}[X]/f := \{g \in \mathbb{F}[X] : \deg g < \deg f\}.$$

W zbiorze $\mathbb{F}[X]/f$ wprowadzamy działania $+$ i $*$ następująco: działanie $+$ jest zwykłym dodawaniem wielomianów, natomiast działanie $*$ definiujemy wzorem

$$g * h := \text{reszta z dzielenia wielomianu } g \cdot h \text{ przez wielomian } f$$

dla wielomianów $g, h \in \mathbb{F}[X]/f$.

Uwaga.

Jeśli $\mathbb{F}$ jest ciałem skończonym i $f \in \mathbb{F}[X]$, $f \neq 0$, to zbiór $\mathbb{F}[X]/f$ ma $|\mathbb{F}|^{\deg f}$ elementów.

Lemat 3.3.
Jeśli $f \in \mathbb{F}[X]$, $f \neq 0$, to zbiór $\mathbb{F}[X]/f$ wraz z działaniami $+$ i $*$ zdefiniowanymi powyżej jest pierścieniem (przemiennym z jedynką).

Dowód.
Ćwiczenie. □

Stwierdzenie 3.4.
Niech $\mathbb{F}$ będzie ciałem. Jeśli wielomian $f \in \mathbb{F}[X]$ jest nierozkładalny, to pierścień $\mathbb{F}[X]/f$ jest ciałem.

Dowód.
Ustalmy wielomian $g \in \mathbb{F}[X]/f$, $g \neq 0$. Musimy pokazać, że istnieje wielomian $h \in \mathbb{F}[X]/f$ taki, że $g * h = 1$. W tym celu wystarczy uzasadnić, że funkcja $F : \mathbb{F}[X]/f \to \mathbb{F}[X]/f$ dana wzorem $F(h) := g * h$ dla wielomianu $h \in \mathbb{F}[X]/f$ jest surjekcją. Zauważmy jednak, że funkcja F jest endomorfizmem liniowym, więc równoważnie wystarczy pokazać, że funkcja F jest injekcją, tzn. $\operatorname{Ker} F = \{0\}$. Przypuśćmy zatem, że $g * h = 0$ dla wielomianu $h \in \mathbb{F}[X]/f$. Wtedy $f \mid g \cdot h$, więc $f \mid h$, zatem $h = 0$. □

Stwierdzenie 3.5.
Niech $p \in \mathbb{P}$, $m, n \in \mathbb{N}_+$ i $m \mid n$ Jeśli $\mathbb{F}$ jest ciałem skończonym o p^m elementach, to $\alpha^{p^n} = \alpha$ dla każdego elementu $\alpha \in \mathbb{F}$.

Dowód.
Dowód będzie indukcyjny ze względu na $k := \frac{n}{m}$.

Załóżmy najpierw, że $k = 1$, tzn. $n = m$. Jeśli $\alpha = 0$, to teza jest oczywista. Jeśli $\alpha \neq 0$, to z twierdzenia Lagrange'a zastosowanego dla grupy multiplikatywnej ciała $\mathbb{F}$ wynika, że $\alpha^{p^m - 1} = 1$, a więc $\alpha^{p^m} = \alpha$.

Załóżmy teraz, że $k > 1$. Wtedy korzystając z założenia indukcyjnego dla $k - 1$ oraz 1 otrzymujemy, że

$$\alpha^{p^n} = \alpha^{p^{m \cdot k}} = (\alpha^{p^{m \cdot (k-1)}})^{p^m} = \alpha^{p^m} = \alpha,$$

co kończy dowód. □

Wniosek 3.6.
Niech $p \in \mathbb{P}$ i $n \in \mathbb{N}_+$. Jeśli $f \in \mathbb{F}_p[X]$ jest wielomianem nierozkładalnym i

$\deg f \mid n$, to $f \mid X^{p^{\deg f}} - X$.

Dowód.

Niech $m := \deg f$. Przypomnijmy też, że $|\mathbb{F}_p[X]/f| = p^m$. Niech α będzie resztą z dzielenia wielomianu X przez wielomian f. Wtedy resztą z dzielenia wielomianu X^{p^n} jest α^{p^n}. Ze Stwierdzenia 3.4 wiemy, że pierścień $\mathbb{F}_p[X]/f$ jest ciałem, zatem poprzednie stwierdzenie implikuje, że $f \mid \alpha^{p^n} - \alpha$, co kończy dowód. □

Wniosek 3.7.

Jeśli $\mathbb{F}$ jest ciałem skończonym, to

$$X^{|\mathbb{F}|} - X = \prod_{\alpha \in \mathbb{F}} (X - \alpha).$$

Dowód.

Z poprzedniego stwierdzenia wiemy, że $X - \alpha \mid X^{|\mathbb{F}|} - X$ dla każdego elementu $\alpha \in \mathbb{F}$. Stąd

$$\prod_{\alpha \in \mathbb{F}} (X - \alpha) \mid X^{|\mathbb{F}|} - X.$$

Ponieważ oba wielomiany są unormowane i tego samego stopnia, więc otrzymujemy tezę. □

Lemat 3.8.

Niech G będzie skończoną grupą abelową. Jeśli

$$r := \max\{|\alpha| : \alpha \in G\},$$

to $\alpha^r = 1$ dla wszystkich elementów $\alpha \in G$.

Dowód.

Ćwiczenie. □

Wniosek 3.9.

Jeśli $\mathbb{F}$ jest ciałem skończonym, to grupa $\mathbb{F}^*$ jest cykliczna.

Dowód.

Niech

$$r := \max\{|\alpha| : \alpha \in \mathbb{F}_q^*\}.$$

Korzystając z poprzedniego lematu wiemy, że $\alpha^r = 1$ dla każdego elementu $\alpha \in \mathbb{F}^*$, zatem

$$\prod_{\alpha \in \mathbb{F}^*} (X - \alpha) \mid X^r - 1.$$

Stąd

$$|\mathbb{F}^*| = \deg\Big(\prod_{\alpha\in\mathbb{F}^*}(X-\alpha)\Big) \leq \deg(X^r-1) = r \leq |\mathbb{F}^*|$$

co kończy dowód. □

Lemat 3.10.

Jeśli $\mathbb{F}$ jest ciałem skończonym charakterystyki p, to

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$$

dla wszystkich elementów $\alpha, \beta \in \mathbb{F}$ oraz liczb $n \in \mathbb{N}_+$.

Dowód.

Ćwiczenie. □

Lemat 3.11.

Jeśli $n \in \mathbb{N}_+$ i $k, l \in \mathbb{N}$, to

$$(n^k-1, n^l-1) = n^{(k,l)} - 1.$$

Dowód.

Ćwiczenie. □

Lemat 3.12.

Jeśli $\mathbb{F}$ jest ciałem i $k, l \in \mathbb{N}$, to

$$(X^k-1, X^l-1) = X^{(k,l)} - 1.$$

Dowód.

Ćwiczenie. □

Stwierdzenie 3.13.

Niech $p \in \mathbb{P}$ i $n \in \mathbb{N}_+$. Jeśli $f \in \mathbb{F}_p[X]$ jest wielomianem nierozkładalnym i $f \mid X^{p^n} - X$, to $\deg f \mid n$.

Dowód.

Niech $\mathbb{F} := \mathbb{F}_p[X]/f$. Ponieważ reszta z dzielenia wielomianu X^{p^n} przez wielomian f jest równa X, więc Stwierdzenie 3.5 i Lemat 3.10 implikują, że reszta z dzielenia wielomianu g^{p^n} przez wielomian f jest równa reszcie z dzielenia wielomianu g przez f dla każdego wielomianu $g \in \mathbb{F}_p[X]$. W konsekwencji $\alpha^{p^n} = \alpha$ dla każdego elementu $\alpha \in \mathbb{F}$, zatem Wniosek 3.7 implikuje, że

$$X^{p^{\deg f}} - X = \prod_{\alpha\in\mathbb{F}}(X-\alpha) \mid X^{p^n} - X.$$

Stąd

$$(X^{p^{\deg f}-1}-1, X^{p^n-1}-1) = X^{p^{\deg f}-1}-1.$$

Korzystając z Lematu 3.12 otrzymujemy więc, że

$$(p^{\deg f}-1, p^n-1) = p^{\deg f}-1,$$

a więc wykorzystując Lemat 3.11 mamy, że $(\deg f, n) = \deg f$, co kończy dowód. □

Twierdzenie 3.14.
Jeśli $p \in \mathbb{P}$ i $n \in \mathbb{N}_+$, to w pierścieniu $\mathbb{F}_p[X]$ mamy równość

$$X^{p^n} - X = \prod_{f \in \mathcal{F}} f,$$

gdzie $\mathcal{F}$ jest zbiorem nierozkładalnych wielomianów unormowanych w pierścieniu $\mathbb{F}_p[X]$, których stopnie dzielą n.

Dowód.
Z Wniosku 3.6 i powyższego stwierdzenia wynika, że istnieje funkcja $e : \mathcal{F} \to \mathbb{N}_+$ taka, że

$$X^{p^n} - X = \prod_{f \in \mathcal{F}} f^{e(f)}.$$

Gdyby istniał wielomian $f \in \mathcal{F}$ taki, że $e(f) > 1$, to $f \mid (X^{p^n} - X)' = -1$, co jest niemożliwe. □

Twierdzenie 3.15.
Jeśli $p \in \mathbb{P}$ i $n \in \mathbb{N}_+$, to istnieje wielomian nierozkładalny $f \in \mathbb{F}_p[X]$ stopnia n.

Dowód.
Dla każdej liczby $m \in \mathbb{N}_+$ niech k_m będzie liczbą unormowanych wielomianów nierozkładalnych stopnia m w pieścieniu $\mathbb{F}_p[X]$ oraz $K_m := m \cdot k_m$. Poprzednie twierdzenie implikuje, że

$$\sum_{l \mid m} K_l = p^m$$

dla każdej liczby $m \in \mathbb{N}_+$ .W szczególności

$$K_n = p^n - \sum_{\substack{l \mid n \\ l < n}} K_l$$

oraz $K_m \leq p^m$ dla każdej liczby $m \in \mathbb{N}_+$. W konsekwencji

$$K_n \geq p^n - \sum_{\substack{l|n \\ l<n}} p^l \geq p^n - \sum_{l\in[1,n-1]} p^l \geq p^n - (p^n - p) = p > 0,$$

co kończy dowód. □

Wniosek 3.16.

Jeśli $p \in \mathbb{P}$ i $n \in \mathbb{N}_+$, to istnieje ciało $\mathbb{F}$ takie, że $|K| = p^n$.

Dowód.

Wystarczy skorzystać z poprzedniego twierdzenia oraz Stwierdzenia 3.4. □

Twierdzenie 3.17.

Jeśli $\mathbb{F}$ i $\mathbb{F}'$ są ciałami skończonymi takimi, że $|\mathbb{F}| = |\mathbb{F}'|$, to ciała $\mathbb{F}$ i $\mathbb{F}'$ są izomorficzne.

Dowód.

Załóżmy, że $|\mathbb{F}| = p^n$ dla liczb $p \in \mathbb{P}$ oraz $n \in \mathbb{N}_+$. Wtedy ciała $\mathbb{F}$ i $\mathbb{F}'$ mają charakterystykę p. Korzystając ze Stwierdzenia 3.4 i Twierdzenia 3.15 bez straty ogólności możemy założyć, że $\mathbb{F} = \mathbb{F}_p[X]/f$, gdzie $f \in \mathbb{F}_p[X]$ jest unormowanym wielomianem nierozkładalnym. Korzystając z Wniosku 3.7 i Twierdzenia 3.14 wiemy, że w pierścieniu $\mathbb{F}'[X]$ ma miejsce równość

$$\prod_{g\in\mathcal{F}} g = X^{p^n} - X = \prod_{\alpha\in\mathbb{F}'} (X - \alpha),$$

gdzie $\mathcal{F}$ jest zbiorem unormowanych wielomianów nierozkładalnych w pierścieniu $\mathbb{F}_p[X]$, których stopień dzieli n. W szczególności, istnieje element $\alpha \in \mathbb{F}'$ taki, że $f(\alpha) = 0$. Wtedy funkcja $\mathbb{F} \to \mathbb{F}'$, $g \mapsto g(\alpha)$, jest homomorfizmem ciał. Ponieważ homomorfizmy ciał są injekcjami oraz $|\mathbb{F}| = |\mathbb{F}'| < \infty$, więc musi być ona bijekcją, co kończy dowód. □

Oznaczenie.

Dla liczby $q \in \mathbb{N}_+$ takiej, że $q = p^n$ dla pewnych liczb $p \in \mathbb{P}$ oraz $n \in \mathbb{N}_+$, przez $\mathbb{F}_q$ oznaczamy ustalone ciało o q elementach.

Kody liniowe

Założenie.

Do końca tego paragrafu $\mathbb{F}$ jest ciałem skończonym oraz $k \in \mathbb{N}_+$.

Definicja.

Kodem (liniowym) nad ciałem $\mathbb{F}$ nazywamy każdą podprzestrzeń liniową przestrzeni $\mathbb{F}^k$.

Przykład.

Jeśli

$$C := \{x \in \mathbb{F}_2^{k+1} : x_1 + \cdots + x_{k+1} = 0\},$$

to mówimy, że kod C powstaje z przestrzeni $\mathbb{F}_2^k$ przez dodanie bitu kontroli parzystości.

Przykład.

Kodem ISBN nazywamy kod

$$C := \{x \in \mathbb{F}_{11}^{10} : \sum_{i \in [1,10]} i \cdot x_i = 0\}.$$

W praktyce wykorzystujemy tylko te elementy $x \in C$, dla których $x_i \in [0, 9]$ dla wszystkich indeksów $i \in [1, 9]$.

Przykład.

Jeśli

$$C := \{x \in \mathbb{F}_2^k : x_1 = \cdots = x_k\},$$

to mówimy, że kod C powstaje przez k-krotne powtórzenie bitu.

Definicja.

Wagą słowa $x \in \mathbb{F}^k$ nazywamy

$$w(x) := |\{i \in [1, k] : x_i \neq 0\}|.$$

Definicja.

Odległością Hamminga nazywamy funkcję $d : \mathbb{F}^k \times \mathbb{F}^k \to \mathbb{N}$ zdefiniowaną wzorem

$$d(x, y) := w(x - y)$$

dla $x, y \in \mathbb{F}^k$.

Lemat 3.18.

Odległość Hamminga jest metryką.

Dowód.

Ćwiczenie. □

DEFINICJA.
Minimalną odległością kodu C nazywamy

$$d(C) := \min\{d(x,y) : x,y \in C,\ x \neq y\}.$$

LEMAT 3.19.
Jeśli C jest kodem, to

$$d(C) = \min\{w(x) : x \in C,\ x \neq 0\}.$$

DOWÓD.
Ćwiczenie. □

DEFINICJA.
Niech $t \in \mathbb{N}_+$. Mówimy, że *kod C wykrywa t błędów*, jeśli $d(C) > t$.

DEFINICJA.
Kulą o środku $x \in \mathbb{F}^k$ i promieniu $r \in \mathbb{N}$ nazywamy zbiór

$$K(x,r) := \{y \in \mathbb{F}^k : d(x,y) \leq r\}.$$

DEFINICJA.
Niech $t \in \mathbb{N}$. Mówimy, że *kod $C \subset \mathbb{F}^k$ koryguje t błędów*, jeśli $|K(x,t) \cap C| \leq 1$ dla każdego elementu $x \in \mathbb{F}^k$.

STWIERDZENIE 3.20.
Kod $C \subset \mathbb{F}^k$ koryguje $\lfloor \frac{d(C)-1}{2} \rfloor$ błędów.

DOWÓD.
Niech $r := \lfloor \frac{d(C)-1}{2} \rfloor$. Przypuśćmy, że istnieje element $x \in \mathbb{F}^k$ taki, że $|K(x,r) \cap C| > 1$ i ustalmy elementy $x', x'' \in C$ takie, że $x' \neq x''$ oraz $d(x,x') \leq r$ i $d(x,x'') \leq r$. Wtedy

$$d(x',x'') \leq d(x',x) + d(x,x'') \leq 2r < d(C),$$

co prowadzi do sprzeczności. □

DEFINICJA.
Zawartością informacyjną kodu $C \subset \mathbb{F}^k$ nazywamy

$$R_C := \frac{\dim_{\mathbb{F}} C}{k}.$$

Przykład.
Jeśli

$$C := \{x \in \mathbb{F}_2^9 : x_1 = x_2 = x_3,\ x_4 = x_5 = x_6,\ x_7 = x_8 = x_9\},$$

to $d(C) = 3$ oraz $R_C = \frac{1}{3}$. Z drugiej strony, $d(C') = 3$ i $R_{C'} = \frac{1}{2}$ dla

$$C' := \{x \in \mathbb{F}_2^6 : x_1 + x_2 + x_4 = 0,\ x_1 + x_3 + x_5 = 0,\ x_2 + x_3 + x_6 = 0\}.$$

Twierdzenie 3.21 (Ograniczenie Hamminga).
Jeśli $C \subset \mathbb{F}^k$ jest kodem korygującym t błędów, to

$$|C| \leq \frac{q^k}{\sum_{i\in[0,t]}(q-1)^i\binom{k}{i}},$$

gdzie $q := |\mathbb{F}|$.

Dowód.
Zauważmy, że

$$|K(x,t)| = \sum_{i\in[0,t]} (q-1)^i \binom{k}{i}$$

dla każdego elementu $x \in \mathbb{F}^k$. Ponieważ $K(x,t) \cap K(y,t) = \varnothing$ dla wszystkich elementów $x, y \in C$, $x \neq y$, więc to kończy dowód.

Twierdzenie 3.22.
Jeśli $C \subset \mathbb{F}^k$, to

$$|C| \leq q^{k-d(C)+1},$$

gdzie $q := |\mathbb{F}|$.

Dowód.
Wystarczy zauważyć, że funkcja $\alpha : C \to \mathbb{F}^{k-d(C)+1}$ dana wzorem

$$\alpha(x) := (x_1, \ldots, x_{k-d(C)+1})$$

dla $x \in C$, jest różnowartościowa.

Definicja.
Niech $C \subset \mathbb{F}^k$ będzie kodem i $l := \dim_{\mathbb{F}} C$. *Macierzą generującą kodu* C nazywamy każdą macierz $G \in \mathbb{M}_{l\times k}(\mathbb{F})$, której wiersze tworzą bazę kodu C jako przestrzeni liniowej nad ciałem $\mathbb{F}$.

DEFINICJA.

Niech $C \subset \mathbb{F}^k$ będzie kodem i $l := \dim_{\mathbb{F}} C$. *Macierzą kontroli parzystości kodu* C nazywamy każdą macierz $H \in \mathbb{M}_{(k-l)\times k}(\mathbb{F})$ taką, że

$$C := \{x \in \mathbb{F}^k : H \cdot x^{\mathrm{tr}} = 0\}.$$

UWAGA.

Jeśli G jest macierzą generatorów kodu $C \subset \mathbb{F}^k$ wymiaru l, to macierz $H \in \mathbb{M}_{(k-l)\times k}(\mathbb{F})$ jest macierzą kontroli parzystości kodu C wtedy i tylko wtedy, gdy $\operatorname{rk} H = k - l$ oraz $H \cdot G^{\mathrm{tr}} = 0$.

TWIERDZENIE 3.23.

Niech $l \in \mathbb{N}$ i $H \in \mathbb{M}_{l\times k}(\mathbb{F})$. Jeśli

$$C := \{x \in \mathbb{F}^k : H \cdot x^{\mathrm{tr}} = 0\},$$

to

$$d(C) := \min\{|I| : I \subset [1,k],\ I \neq \varnothing,\ \text{kolumny } H_i,\ i \in I,\ \text{macierzy } H \text{ są liniowo zależne}\}.$$

DOWÓD.

Niech

$$d' := \min\{|I| : I \subset [1,k],\ I \neq \varnothing,\ \text{kolumny } H_i,\ i \in I,\ \text{macierzy } H \text{ są liniowo zależne}\}.$$

Przypomnijmy również, że

$$d(C) = \min\{w(x) : x \in C,\ x \neq 0\}.$$

Udowodnimy najpierw, że $d(C) \leq d'$. Ustalmy podzbiór $I \subset [1,k]$, $I \neq \varnothing$, taki, że kolumny H_i, $i \in I$, macierzy H są liniowo zależne oraz $|I| = d'$. Wtedy istnieje wektor $\lambda^I \in \mathbb{F}$, $\lambda \neq 0$, taki, że $H \cdot \lambda^{\mathrm{tr}} = 0$. Zdefiniujmy słowo $x \in \mathbb{F}^k$ wzorem

$$x_i := \begin{cases} \lambda_i & i \in I, \\ 0 & \text{w przeciwnym wypadku.} \end{cases}$$

Wtedy $H \cdot x^{\mathrm{tr}} = 0$, więc $x \in C$. Ponadto $x \neq 0$ oraz $w(x) = |I| = d'$, co kończy dowód nierówności $d(C) \leq d'$.

Pokażemy teraz, że $d(C) \geq d'$. Ustalmy słowo $x \in C$ takie, że $w(x) = d(C)$. Wtedy dla zbioru $I := \{i \in [1,k] : x_i \neq 0\}$ otrzymujemy, że $|I| = w(x) = d(C)$ oraz kolumny H_i, $i \in I$, macierzy H są liniowo zależne. □

Definicja.

Niech H będzie macierzą kontroli parzystości kodu $C \subset \mathbb{F}^k$. *Syndromem słowa* $y \in \mathbb{F}^k$ nazywamy element $S_H(y) \in \mathbb{F}^{k-l}$, gdzie $l := \dim_{\mathbb{F}} C$, zdefiniowany wzorem

$$S_H(y) := H \cdot y^{\mathrm{tr}}.$$

Lemat 3.24.

Niech $C \subset \mathbb{F}^k$ będzie kodem z macierzą kontroli parzystości H. Jeśli $y \in \mathbb{F}^k$ i $x \in C$, to

$$d(x, y) = \min\{d(z, y) : z \in C\}$$

wtedy i tylko wtedy, gdy $x = y - e$, gdzie element $e \in \mathbb{F}^k$ spełnia warunek

$$w(e) = \min\{w(f) : f \in \mathbb{F}^k,\ S_H(f) = S_H(y)\}.$$

Dowód.

Teza wynika z następującej obserwacji: jeśli $y \in \mathbb{F}^k$ oraz $z \in C$, to $S_C(y-z) = S_C(y)$ oraz $d(z, y) = w(y - z)$.

Algorytm (Dekodowania dla kodów liniowych).

I. Obliczenie wstępne.

```
Dane: kod C.

Dla każdego słowa x wyliczamy syndrom S (x).
Dla każdego syndromu s znajdujemy słowo e (s) takie, że
  w (e (s)) = min {w (x) : S (x) = s}.
```

II. Dekodowanie.

```
Dane: słowo x.

return x - e (S (x));
```

Kody cykliczne

Definicja.

Kod $C \subset \mathbb{F}^k$ nazywamy *cyklicznym*, jeśli dla każdego elementu $(x_1, \ldots, x_k) \in \mathbb{F}^k$ spełniony jest warunek:

$$(x_1, \ldots, x_k) \in C \text{ wtedy i tylko wtedy, gdy } (x_2, \ldots, x_k, x_1) \in C.$$

OZNACZENIE.

Definiujemy

$$R_k(\mathbb{F}) := \mathbb{F}[X]/(X^k - 1).$$

Przypomnijmy, że symbolem $*$ oznaczamy mnożenie w pierścieniu $R_k(\mathbb{F})$.

UWAGA.

Przestrzeń liniową $\mathbb{F}^k$ możemy utożsamić z pierścieniem $R_k(\mathbb{F})$ poprzez izomorfizm liniowy dany wzorem

$$(x_1, \ldots, x_k) \mapsto \sum_{i \in [1,k]} x_i \cdot X^{k-i}.$$

W dalszym ciągu będziemy badać kody będące podprzestrzeniami pierścienia $R_k(\mathbb{F})$. W szczególności, kod $C \subset R_k(\mathbb{F})$ nazywamy cyklicznym wtedy i tylko wtedy, gdy dla wielomianu $f \in R_k(\mathbb{F})$ spełniony jest warunek

$$f \in C \text{ wtedy i tylko wtedy, gdy } X * f \in C.$$

Istotnie, wystarczy zauważyć, że mamy równość

$$X * (a_1 X^{k-1} + \cdots + a_k) = a_2 X^{k-1} + \cdots + a_k X + a_1.$$

STWIERDZENIE 3.25.

Następujące warunki są równoważne dla kodu $C \subset R_k(\mathbb{F})$.

(1) Kod C jest cykliczny.

(2) Jeśli $f \in C$, to $X * f \in C$.

(3) Jeśli $f \in C$ i $g \in R_k(\mathbb{F})$, to $g * f \in C$.

DOWÓD.

Implikacja (1) $\Rightarrow$ (2) jest oczywista, natomiast implikacji (2) $\Rightarrow$ (3) dowodzi się przez prostą indukcję. Wreszcie, w dowodzie implikacji (3) $\Rightarrow$ (1) wystarczy uzasadnić, że jeśli $f \in R_k(\mathbb{F})$ oraz $X * f \in C$, to $f \in C$. Zauważmy jednak, że w powyższej sytuacji $f = X^{k-1} * (X * f)$, co kończy dowód. □

DEFINICJA.

Generatorem kodu cyklicznego C nazywamy każdy wielomian unormowany $g \in C$ taki, że

$$\deg g = \min\{\deg f : f \in C \text{ i } f \neq 0\}.$$

UWAGA.

Każdy niezerowy kod cykliczny posiada generator.

Twierdzenie 3.26.
Jeśli g jest generatorem kodu cyklicznego C, to $g \mid f$ dla każdego wielomianu $f \in C$.

Dowód.
Ustalmy wielomian $f \in C$. Wiemy, że istnieją wielomiany $q, r \in \mathbb{F}[X]$ takie, że

$$f = q \cdot g + r \qquad \text{i} \qquad \deg r < \deg g.$$

Zauważmy, że $r = f - q * g \in C$, co wobec definicji wielomianu g oznacza, że $r = 0$. □

Wniosek 3.27.
Jeśli g jest generatorem kodu cyklicznego $C \subset R_k(\mathbb{F})$, to

$$C = \{f \in R_k(\mathbb{F}) : g \mid f\}.$$

Dowód.
Oczywiste. □

Wniosek 3.28.
Jeśli g i g' są generatorami kodu cyklicznego, to $g = g'$.

Dowód.
Z poprzedniego stwierdzenia wiemy, że $g \mid g'$ i $g' \mid g$, zatem istnieje element $\lambda \in \mathbb{F}$ taki, że $g' = \lambda \cdot g$. Ponieważ wielomiany g i g' są unormowane, więc $\lambda = 1$, co kończy dowód. □

Wniosek 3.29.
Jeśli g jest generatorem kodu cyklicznego $C \subset R_k(\mathbb{F})$ wymiaru l, to $\deg g = k - l$.

Dowód.
Powyższe twierdzenie implikuje, że odwzorowanie

$$\{f \in \mathbb{F}[X] : \deg f < k - \deg g\} \to C,\ f \mapsto f \cdot g,$$

jest izomorfizmem przestrzeni liniowych. W szczególności

$$l = \dim_{\mathbb{F}} C = k - \deg g,$$

co kończy dowód. □

Wniosek 3.30.
Jeśli $g \in R_k(\mathbb{F})$ jest generatorem kodu cyklicznego $C \subset R_k(\mathbb{F})$, to $g \mid X^k - 1$.

Dowód.
Wiemy, że istnieją wielomiany $q, r \in \mathbb{F}[X]$ takie, że

$$X^k - 1 = q \cdot g + r \qquad \text{i} \qquad \deg r < \deg g.$$

Zauważmy, że $r = f * g \in C$, gdzie f jest resztą z dzielenia wielomianu $-q$ przez wielomian $X^k - 1$, co wobec definicji wielomianu g oznacza, że $r = 0$. □

Twierdzenie 3.31.
Niech $g \in R_k(\mathbb{F})$ będzie wielomianem unormowanym takim, że $g \mid X^k - 1$. Jeśli

$$C := \{f \in R_k(\mathbb{F}) : g \mid f\},$$

to zbiór C jest kodem cyklicznym oraz wielomian g jest generatorem kodu C.

Dowód.
Wystarczy sprawdzić, korzystając ze Stwierdzenia 3.25, że jeśli $f \in C$, to $X * f \in C$. Z definicji mnożenia w pierścieniu $R_k(\mathbb{F})$ wiemy, że istnieje wielomian $q \in \mathbb{F}[X]$ taki, że $X \cdot f = q \cdot (X^k - 1) + X * f$. Wtedy

$$g \mid X \cdot f - q \cdot (X^k - 1) = X * f,$$

co kończy dowód. □

Wniosek 3.32.
Funkcja

$$\{C \subset R_k(\mathbb{F}) : \text{zbiór } C \text{ jest niezerowym kodem cyklicznym}\} \\ \to \{g \in R_k(\mathbb{F}) : \text{wielomian } g \text{ jest unormowany i } g \mid X^k - 1\}$$

dana wzorem

$$C \mapsto \text{generator kodu } C$$

jest bijekcją. Funkcja odwrotna dana jest wzorem

$$g \mapsto \{f \in R_k(\mathbb{F}) : g \mid f\}.$$

Dowód.
Wynika natychmiast z powyższych rozważań. □

Lemat 3.33.
Niech $g = g_0 + \cdots + g_{k-l} \cdot X^{k-l}$ będzie generatorem kodu cyklicznego $C \subset R_k(\mathbb{F})$ wymiaru l. Jeśli

$$G := \begin{bmatrix} g_{k-l} & \cdots & g_0 & 0 & \cdots 0 & \\ 0 & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & g_{k-l} & \cdots & g_0 \end{bmatrix} \in \mathbb{M}_{l\times k}(\mathbb{F}),$$

to macierz G jest macierzą generatorów kodu C.

Dowód.
Zauważmy, że wiersze macierzy G należą do kodu C. Ponadto $\operatorname{rk} G = l$, gdyż $g_{k-l} = 1$, co kończy dowód. □

Twierdzenie 3.34.
Niech g będzie generatorem kodu cyklicznego $C \subset R_k(\mathbb{F})$ wymiaru l. Jeśli

$$h := \frac{X^k - 1}{g} = h_0 + \cdots + h_l \cdot X^l,$$

to macierz

$$H := \begin{bmatrix} h_0 & \cdots & h_l & 0 & \cdots & 0 \\ 0 & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & h_0 & \cdots & h_l \end{bmatrix} \in \mathbb{M}_{k-l\times k}(\mathbb{F})$$

jest macierzą kontroli parzystości kodu C.

Dowód.
Zauważmy, że $h_l = 1$, więc $\operatorname{rk} H = k - l$. Wystarczy zatem sprawdzić, że $H \cdot G^{\mathrm{tr}} = 0$, gdzie G jest macierzą generatorów kodu C opisaną w poprzednim lemacie. Zauważmy jednak, że jeśli $i \in [1, k-l]$ i $j \in [1, l]$, to współczynnik $(H \cdot G^{\mathrm{tr}})_{i,j}$ jest równy współczynnikowi przy $X^{(k-l)+(j-i)}$ w wielomianie $h \cdot g = X^k - 1$, co kończy dowód, gdyż $(k-l) + (j-i) \in [1, k-1]$. □

Definicja.
Jeśli $k = |\mathbb{F}| - 1$, $d \in [1, k]$ i β jest generatorem grupy $\mathbb{F}^*$, to definiujemy,

$$C(d, \beta) := \{f \in R_k(\mathbb{F}) : f(\beta^i) = 0 \text{ dla wszystkich liczb } i \in [1, d-1]\}.$$

Kody powyższej postaci nazywamy kodami *Reeda-Solomona*.

UWAGA.
Kody Reeda-Solomona są kodami cyklicznymi. Jeśli $k = |\mathbb{F}| - 1$, $d \in [1, k]$ i β jest generatorem grupy $\mathbb{F}^*$, to generatorem kodu $C(d, \beta)$ jest wielomian

$$\prod_{i \in [1, d-1]} (X - \beta^i).$$

TWIERDZENIE 3.35.
Jeśli $k = |\mathbb{F}| - 1$, $d \in [1, k]$ i β jest generatorem grupy $\mathbb{F}^*$, to

$$d(C(d, \beta)) = d.$$

DOWÓD.
Niech

$$H := \begin{bmatrix} \beta^{k-1} & \dots & \beta & 1 \\ \beta^{2\cdot(k-1)} & \dots & \beta^2 & 1 \\ \vdots & & \vdots & \vdots \\ \beta^{(d-1)\cdot(k-1)} & \dots & \beta^{d-1} & 1 \end{bmatrix}.$$

Zauważmy, że

$$C = \{x \in \mathbb{F}^k : H \cdot x^{\mathrm{tr}} = 0\}.$$

Jeśli $i_1, \dots, i_{d-1} \in [0, k-1]$ są parami różne, to macierz utworzona z kolumn $H_{k-i_1}, \dots, H_{k-i_{d-1}}$ macierzy H ma postać

$$\begin{bmatrix} \beta^{i_1} & \beta^{i_2} & \dots & \beta^{i_{d-1}} \\ \beta^{2\cdot i_1} & \beta^{2\cdot i_2} & \dots & \beta^{2\cdot i_{d-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{(d-1)\cdot i_1} & \beta^{(d-1)\cdot i_2} & \dots & \beta^{(d-1)\cdot i_{d-1}} \end{bmatrix},$$

więc jej wyznacznik jest równy

$$\beta^{\sum_{j \in [1, d-1]} (i_j - 1)} \cdot \prod_{\substack{p, q \in [1, d-1] \\ p < q}} (\beta^{i_q - 1} - \beta^{i_p - 1}) \neq 0.$$

Zatem kolumny $H_{i_1}, \dots, H_{i_{d-1}}$ są liniowo niezależne. Oczywiście, jeśli $I \subset [1, k]$ oraz $|I| = d$, to kolumny H_i, $i \in I$, są liniowo zależne, więc teza wynika z Twierdzenia 3.23. □