Title: Hierarchiczność wielodzielnych struktur dostępu

Author: Renata Kawa

Citation style: Kawa Renata. (2015). Hierarchiczność wielodzielnych struktur dostępu. Praca doktorska. Katowice : Uniwersytet Śląski

Instytut Matematyki Uniwersytetu Śląskiego w Katowicach

Hierarchiczność wielodzielnych struktur dostępu

Renata Kawa

Rozprawa doktorska napisana pod kierunkiem
dr. hab. Mieczysława Kuli

Katowice 2015

Podziękowania

Chciałabym złożyć podziękowania promotorowi dr. hab. Mieczysławowi Kuli za poświęcenie mi swojego czasu i uwagi, oraz wkład wniesiony w powstanie tej pracy.

Spis treści

Wstęp

Pojęcie schematu podziału sekretu zostało wprowadzone niezależnie przez Blakleya [3] i Shamira [21] w 1979 roku. Pomysł, który leży u podstaw tego pojęcia, polega na podzieleniu informacji, zwanej sekretem, na części, które następnie są przesyłane do uczestników. Kluczowe jest, że tylko pewne, z góry ustalone zbiory uczestników mogą odzyskać sekret. Takie zbiory nazywamy zbiorami autoryzowanymi, natomiast rodzinę zbiorów autoryzowanych nazywamy strukturą dostępu. Równie istotne jest, aby zbiory uczestników nie należące do struktury dostępu nie mogły odzyskać sekretu.

Schematy podziału sekretu znajdują zastosowanie w pewnych dziedzinach związanych z systemami zabezpieczeń. Przykładowo, sejf w banku może otwierać się po podaniu klucza, który przyjmujemy jako sekret. Aby otworzyć sejf, pewna z góry ustalona liczba pracowników banku musi wyrazić na to zgodę podając swoje udziały pozwalające na wyznaczenie sekretu, czyli klucza otwierającego sejf. Podobnie można zastosować schemat podziału sekretu w środowisku wojskowym, gdzie wystrzelenie pocisku balistycznego powinno być możliwe tylko wtedy, gdy pewna liczba upoważnionych osób wyrazi na to zgodę i poda swoje udziały umożliwiające obliczenie sekretu, czyli kodu uruchamiającego pocisk. Te dwa przykłady ilustrują jak schematy podziału sekretu pozwalają dzielić kontrolę nad decyzjami o znaczących konsekwencjach. Drugim obszarem zastosowania schematów podziału sekretu jest uwierzytelnianie. W takim przypadku nie jest istotna sama wartość sekretu, natomiast liczy się fakt wyznaczenia jego poprawnej wartości. W ten sposób można wykorzystać schemat podziału sekretu do potwierdzania tożsamości, na przykład osób uczestniczących w pewnym spotkaniu. Jeśli uczestnicy spotkania ujawnią swoje udziały, które prowadzą do wyznaczenia wartości nie będącej sekretem, oznacza to, że wśród nich znajduje się osoba, która podała niewłaściwą wartość udziału. Pomijając możliwość pomyłki lub celowego działania, świadczy to o przybyciu na spotkanie osoby nieuprawnionej, podszywająca się pod kogoś innego.

Konstrukcje Blakleya i Shamira, pomimo, iż reprezentowały tę samą koncepcję, były istotnie różne. Propozycja Shamira zyskała dużą popularność i zapo-

czątkowała rozwój nowego nurtu badań w kryptologii. Wiele schematów podziału sekretu opisanych w literaturze to uogólnienia schematu Shamira. Warto wyróżnić kilka prac, które wniosły istotny wkład w rozwój pojęcia schematu podziału sekretu. W dwóch, powstałych niezależnie, pracach: Benaloha i Leichtera [2] oraz Ito, Saito i Nishizeki [12], zostały przedstawione konstrukcje schematów podziału sekretu dla dowolnej rodziny monotonicznej podzbiorów zbioru uczestników. Niestety skonstruowane w tych pracach schematy (dwa różne), pomimo że uniwersalne, mają poważną wadę: możliwe wartości sekretu są elementami ustalonego ciała, podczas gdy udziały są wektorami o współrzędnych z tego ciała, a liczba tych współrzędnych rośnie wykładniczo wraz ze wzrostem liczby uczestników.

Uczestnicy biorący udział w schemacie podziału sekretu nie muszą być równorzędni, lecz podobnie jak w życiu codziennym, na przykład w przedsiębiorstwach czy wojsku, znajdują się w różnego rodzajach hierarchiach, a ich pozycja zależy od zajmowanego stanowiska czy stopnia wojskowego. Naturalne jest zatem, aby schemat podziału sekretu uwzględniał miejsce uczestnika w zajmowanej hierarchii. Struktury dostępu, w których uczestnicy podzieleni są na rozłączne bloki, odpowiadające grupom osób o tej samej pozycji w hierarchii, nazywamy strukturami hierarchicznymi. W zbiorze autoryzowanym hierarchicznej struktury dostępu dowolny uczestnik może być zastąpiony przez uczestnika znajdującego się w tym samym bloku lub bloku będącym wyżej w hierarchii, i nadal będzie to zbiór autoryzowany.

Hierarchię w zbiorze bloków można zapisać za pomocą relacji częściowego porządku, co zostanie pokazane w niniejszej pracy. Pierwsze struktury hierarchiczne były rozważane przez Shamira [21] i dotyczyły hierarchii, która odpowiada porządkowi liniowemu w zbiorze bloków. Takie struktury nazywamy ściśle hierarchicznymi. Shamir zaproponował rozwiązanie, w którym uczestnik stojący wyżej w hierarchii otrzymuje więcej udziałów. Nie jest to cecha pożądana dla schematu podziału sekretu, ponieważ możliwe wartości sekretu oraz potencjalne wartości udziałów powinny należeć do tego samego zbioru. Schematy podziału sekretu spełniające ten warunek nazywamy idealnymi. Schemat zaproponowany przez Shamira dla struktur ściśle hierarchicznych nie jest idealny, co sprawiło, iż prace nad ściśle hierarchicznymi strukturami dostępu kontynuowało wielu autorów, m.in. Simmons [22], Tassa [24] oraz Farràs i Padró [10]. Ci ostatni zasługują na szczególną uwagę, ponieważ w swojej pracy podali warunki konieczne i wystarczające na to, aby struktura ściśle hierarchiczna była idealna, czyli istniał schemat idealny, dla którego ta struktura byłaby strukturą dostępu.

Kolejną interesującą klasą struktur dostępu rozważaną w literaturze są struktury oddziałowe, czyli takie, które odpowiadają porządkowi antyliniowemu w zbiorze bloków. Pisząc wprost, w takiej strukturze nie ma żadnej hierarchii pomiędzy blokami. W literaturze można spotkać wiele przykładów oddziałowych struktur dostępu, które są idealne, jednakże do tej pory nie zostały podane warunki ko-

nieczne na to, aby oddziałowa struktura dostępu była idealna. Pewien postęp do rozwoju tego zagadnienia wnieśli Simmons [22], Brickell [4], Tassa i Dyn [25] oraz Farràs [7]. Jak dotąd, najszerszą klasę takich struktur podał Farràs. Wykażemy w podrozdziale 4.6, że warunki podane przez Farràsa nie są warunkami koniecznymi, aby oddziałowa struktura dostępu była idealna.

Powstaje pytanie, czy istnieją hierarchiczne struktury dostępu, dla których częściowy porządek pomiędzy blokami uczestników jest inny niż liniowy i antyliniowy. Niniejsza praca zawiera pozytywną odpowiedź na to pytanie. Ponadto wykazujemy, że wśród tych struktur są także struktury idealne.

Pracę rozpoczynamy od wprowadzenia podstawowych definicji i faktów dotyczących schematów podziału sekretu oraz struktur dostępu. Ponadto badane są własności spójnych i idealnych schematów podziału sekretu. W szczególności pokazujemy związek pomiędzy mocami zbiorów niezależnych i maksymalnych zbiorów nieautoryzowanych schematu podziału sekretu (wniosek 1.25), mający zastosowanie w rozdziale trzecim.

Rozdział drugi poświęcony jest matroidom i polimatroidom, ponieważ istnieje silny związek pomiędzy tymi pojęciami, a schematami podziału sekretu i strukturami dostępu. Związek schematów podziału sekretu z matroidami zauważyli Brickell i Davenport [5]. Farràs, Martí-Farré i Padró [8], [9] wykazali związek wielodzielnych struktur dostępu z polimatroidami, co okazuje się być bardzo przydatnym narzędziem do ich badania. W rozprawie skupiamy się głównie na strukturach dostępu, które są wyznaczane przez polimatroidy jednorodne, dlatego też rozdział ten zawiera wyniki opisujące własności tej klasy polimatroidów. Pokazujemy między innymi, że istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy rodziną polimatroidów jednorodnych zdefiniowanych na zbiorze J_m i rodziną m-elementowych nierosnących ciągów nieujemnych liczb całkowitych (stwierdzenia 2.25 i 2.26). Ponadto podajemy warunek konieczny i wystarczający na to, aby polimatroid jednorodny był polimatroidem boolowskim (twierdzenie 2.49).

W rozdziale trzecim prezentujemy definicję struktury hierarchicznej, uogólniającej pojęcia struktur ściśle hierarchicznych i oddziałowych. Przedstawiamy także wygodną wektorową reprezentację zbiorów uczestników wprowadzoną przez Farràsa, Martí-Farré i Padró [8], [9]. Ponadto przybliżamy nieco historię struktur ściśle hierarchicznych i oddziałowych. Na zakończenie tego rozdziału podajemy odpowiedź (negatywną) na pewne pytanie postawione przez Tassę w pracy [24], dotyczące idealności pewnej klasy struktur ściśle hierarchicznych. Pomimo, iż Farràs i Padró [10] również odpowiedzieli na to pytanie, dowód zawarty w rozprawie jest przeprowadzony za pomocą innych narzędzi i jest prostszy (twierdzenie 3.32).

Rozdział czwarty jest poświęcony badaniom hierarchicznych struktur dostępu, w szczególności tych, dla których porządek pomiędzy blokami uczestników jest

inny niż liniowy i antyliniowy. Rozpoczynamy go od zacytowania twierdzenia 4.1 Farràsa, Martí-Farré i Padró [8], [9], które służy nam w dalszym ciągu do konstruowania wielodzielnych struktur dostępu za pomocą polimatroidów jednorodnych. Otrzymane struktury dostępu badamy w podrozdziale 4.3 pod względem hierarchii w rodzinie bloków uczestników, także pod względem idealności i spójności. Uzyskane wyniki prezentujemy w formie tabel na przykładach struktur z dwoma, trzema i czterema blokami. Podrozdział 4.5 poświęcamy na zbadanie wielodzielnych struktur dostępu wyznaczonych przez jednorodne polimatroidy boolowskie. Ponadto, na zakończenie, wykazujemy, że warunki podane przez Farràsa nie są warunkami koniecznymi, aby oddziałowa struktura dostępu była idealna.

Rozdział piąty ma nieco inny charakter. Farràs i Padró [10] w swojej pracy wskazali jak porównać w ściśle hierarchicznej strukturze dostępu dwa zbiory uczestników badając ich reprezentacje wektorowe. W tym rozdziale uogólniamy ten wynik wskazując sposób na porównanie dwóch zbiorów uczestników w dowolnej wielodzielnej strukturze dostępu dysponując ich reprezentacjami wektorowymi (twierdzenie 5.12). Metoda wykorzystana w tym rozdziale nawiązuje do znanego z teorii badań operacyjnych zadania transportowego, które zostanie dla naszych potrzeb nieco zmodyfikowane.

Na zakończenie podamy pewne hipotezy, które nasunęły się podczas pracy nad wynikami zawartymi w niniejszej rozprawie.

Oznaczenia

W pracy będziemy używać następujących oznaczeń:
$\mathbb{N}$ – zbiór liczb naturalnych.
$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ – zbiór liczb naturalnych razem z 0.
$\mathbb{Z}$ – zbiór liczb całkowitych.
$\mathbb{R}$ – zbiór liczb rzeczywistych.
$\mathbb{N}_0^m = \underbrace{\mathbb{N}_0 \times \cdots \times \mathbb{N}_0}_{m \text{ razy}}$ – iloczyn kartezjański k kopii zbioru $\mathbb{N}_0$.
$\mathcal{P}(A)$ – rodzina wszystkich podzbiorów zbioru A.
$\mathcal{P}_k(A)$ – rodzina wszystkich podzbiorów k-elementowych zbioru A.

Rozdział 1

Schematy podziału sekretu

1.1 Wiadomości wstępne

Rozdział ten rozpoczniemy od podstawowych oznaczeń, definicji i twierdzeń dotyczących schematów podziału sekretu. Niech $P = \{p_1, \ldots, p_n\}$ będzie skończonym zbiorem uczestników oraz niech s będzie pewną informacją, nazywaną sekretem. Ponadto p_0 oznaczać będzie dealera, czyli osobę, która realizuje schemat podziału sekretu, oraz niech $P' := P \cup \{p_0\}$. Schematem podziału sekretu określa się protokół kryptograficzny generujący informacje zwane udziałami, które następnie zostają rozdzielone pomiędzy uczestników w taki sposób, że tylko pewne ustalone grupy uczestników mogą odzyskać sekret, a pozostałe zbiory osób nie są w stanie tego zrobić. Zakładamy, że dla każdego schematu podziału sekretu zbiór możliwych wartości sekretu oraz zbiory możliwych wartości udziałów są skończone. Tymczasowo przyjmiemy następujące, nieformalne określenia, które sprecyzujemy w kolejnym podrozdziale.

Definicja 1.1. *Zbiorem autoryzowanym schematu podziału sekretu* nazywamy taki podzbiór uczestników, którzy łącząc swoje udziały mogą odtworzyć sekret. W przeciwnym przypadku podzbiór uczestników nazywamy *zbiorem nieautoryzowanym schematu podziału sekretu. Strukturą dostępu schematu podziału sekretu* nazywamy rodzinę jego zbiorów autoryzowanych.

Następujący przykład, pochodzący od Shamira [21], jest pierwszym historycznie oraz najbardziej znanym schematem podziału sekretu.

Przykład 1.2. Na początku przeprowadzane są pewne czynności przygotowawcze. Dealer ustala q-elementowe ciało skończone $\mathbb{F}_q$, gdzie $q > n$. Następnie wybiera n różnych, niezerowych elementów $x_i \in \mathbb{F}_q$, $i \in \{1, \ldots, n\}$, zwanych identyfikatorami i przypisuje je uczestnikom, w ten sposób, że uczestnik p_i otrzymuje

identyfikator x_i. Ponadto dealer ustala próg schematu $t \leqslant n$ oraz sekret $s \in \mathbb{F}_q$. Poza sekretem, wszystkie powyższe informacje są jawne.

Chcąc rozdzielić sekret wśród uczestników, dealer wykonuje następujące kroki:

1. losuje $t-1$ elementów z ciała $\mathbb{F}_q$: $a_1, a_2, \ldots, a_{t-1}$;
2. dla każdego uczestnika p_i, $i \in \{1, \ldots, n\}$, oblicza jego udział $u_i = f(x_i)$, gdzie
$$f(x) = a_{t-1}x^{t-1} + \cdots + a_2x^2 + a_1x + s;$$
3. wysyła udziały do uczestników, używając bezpiecznego kanału komunikacji.

Dowolny zbiór $A \subseteq P$, $|A| \geqslant t$, jest autoryzowany: jego uczestnicy chcąc odzyskać sekret s stosują interpolację Lagrange'a, aby wyznaczyć wielomian f, a dokładniej jego wartość w punkcie 0. Jeśli $|A| < t$, to zbiór A jest nieautoryzowany: uczestnicy takiego zbioru A nie mają możliwości odtworzenia wielomianu f, a w szczególności sekretu s. Ponadto uczestnicy takiego zbioru A nie mogą uzyskać nawet częściowej informacji o sekrecie, to znaczy wykluczyć pewnych jego możliwych wartości.

Opisany powyżej schemat Shamira jest przykładem tak zwanego schematu progowego.

Definicja 1.3. *Schematem progowym* (n, t), gdzie $t \leqslant n$, nazywamy schemat podziału sekretu, w którym każdy zbiór uczestników zawierający co najmniej t elementów jest autoryzowany. Rodzinę

$$\Gamma = \{A \subseteq P \colon |A| \geqslant t\},$$

nazywamy *progową strukturą dostępu z progiem* t.

Naturalne jest założenie, iż jeśli pewien zbiór uczestników potrafi odzyskać sekret, to każdy jego nadzbiór również ma taką możliwość, a zatem struktura dostępu Γ dowolnego schematu podziału sekretu ma własność monotoniczności:

$$A \subseteq B, A \in \Gamma \Longrightarrow B \in \Gamma.$$

Definicja 1.4. Rodzinę podzbiorów dowolnego zbioru, która ma własność monotoniczności będziemy nazywać *rodziną monotoniczną*.

W świetle twierdzenia 1.17 uzasadniona jest następująca definicja.

Definicja 1.5. *Strukturą dostępu* nazywamy dowolną rodzinę monotoniczną podzbiorów zbioru P. *Zbiorami autoryzowanymi* nazywamy zbiory należące do struktury dostępu, a *zbiorami nieautoryzowanymi* wszystkie pozostałe podzbiory zbioru P.

Rodzinę wszystkich zbiorów należących do struktury dostępu Γ, minimalnych w sensie inkluzji, oznaczamy jako $\min \Gamma$. Zauważmy, że elementy zbioru $\min \Gamma$ są minimalnymi zbiorami autoryzowanymi. Należy zwrócić uwagę na fakt, że rodzina $\min \Gamma$ wraz z własnością monotoniczności wyznaczają w sposób jednoznaczny rodzinę Γ.

Pożądaną cechą schematów podziału sekretu i struktur dostępu jest ich spójność.

Definicja 1.6. Strukturę dostępu $\Gamma \subseteq \mathcal{P}(P)$ nazywamy *spójną*, jeśli każdy uczestnik $p \in P$ należy do pewnego minimalnego zbioru autoryzowanego, to znaczy

$$\bigcup_{A \in \min \Gamma} A = P.$$

Schemat podziału sekretu nazywamy *spójnym*, jeśli jego struktura dostępu jest spójna.

Łatwo można zauważyć, że jeśli schemat podziału sekretu nie jest spójny, to udział pewnego uczestnika jest zbędny i zawsze można go pominąć w procesie odzyskiwania sekretu. Schematy progowe, w szczególności schemat Shamira, są schematami spójnymi dla $t > 0$.

W niniejszej pracy nie będziemy rozważać schematów podziału sekretu, których struktura dostępu $\Gamma = \mathcal{P}(P)$ lub $\Gamma = \emptyset$. W pierwszym przypadku mamy $\min \Gamma = \{\emptyset\}$, co można interpretować w ten sposób, że sekret jest publicznie znany, czyli każda osoba, nawet spoza zbioru P, może go wyznaczyć. W drugim przypadku stosowanie schematu jest bezzasadne, ponieważ nikt nie jest w stanie wyznaczyć sekretu.

1.2 Schemat podziału sekretu jako macierz

Brickell oraz Davenport zaproponowali w [5] bardzo ogólną i jednocześnie precyzyjną definicję schematu podziału sekretu.

Definicja 1.7. *Schematem podziału sekretu* z n uczestnikami nazywamy taką macierz $\mathbf{M}$ z $n+1$ kolumnami oraz elementami z pewnego skończonego zbioru, że każde dwa jej wiersze są różne.

Kolejne kolumny macierzy $\mathbf{M}$ są przypisane kolejnym uczestnikom i zawierają możliwe wartości ich udziałów. Pierwsza kolumna jest szczególna, ponieważ jest przypisana dealerowi i zawiera potencjalne wartości sekretu. Dlatego też przyjmuje się, że sekret to inaczej udział dealera. Macierz $\mathbf{M}$ jest publicznie znana i każdy uczestnik wie, która kolumna jest z nim utożsamiana.

Nawiązując do przykładu 1.2, reprezentacja macierzowa schematu Shamira jest następująca. Należy rozważyć wszystkie wielomiany f stopnia co najwyżej $t-1$ nad ciałem $\mathbb{F}_q$. Następnie, posługując się identyfikatorami uczestników

$x_i, i \in \{1, \ldots, n\}$, tworzymy kolejne wiersze macierzy $\mathbf{M}$ obliczając dla każdego wielomianu f wartości:

$$f(0), f(x_1), \ldots, f(x_n).$$

W ten sposób w pierwszej kolumnie pojawią się wszystkie możliwe wartości sekretu s, zaś w kolejnych kolumnach wszystkie możliwe wartości udziałów odpowiednich uczestników.

Zanim opiszemy procedury dzielenia i odzyskiwania sekretu, wprowadźmy kilka oznaczeń:

- $\mathbf{M}(r, p)$ jest elementem macierzy $\mathbf{M}$ w wierszu r i kolumnie p.
- $\mathbf{M}(r, A)$ jest wierszem r ograniczonym do kolumn przypisanych uczestnikom ze zbioru A, $A \subseteq P'$.
- $S(p)$ jest zbiorem elementów w kolumnie p. W szczególności $S(p_0)$ jest zbiorem elementów w pierwszej kolumnie i jest to zbiór wszystkich możliwych wartości sekretu. W celu skrócenia zapisu, zamiast $S(p_0)$ piszemy S.
- $S(A) = \{\mathbf{M}(r, A) : r \text{ jest wierszem macierzy } \mathbf{M}\}$, $A \subseteq P'$.

Jeśli dealer chce rozdzielić sekret $s \in S$ wśród uczestników ze zbioru P, wykonuje następujące kroki:

1. wybiera taki wiersz $\hat{r}$, że $\mathbf{M}(\hat{r}, p_0) = s$;
2. dostarcza udział $\alpha_p := \mathbf{M}(\hat{r}, p)$ każdemu uczestnikowi $p \in P$ używając bezpiecznego kanału komunikacji.

Uczestnicy w zbiorze $A \subseteq P$ chcąc odzyskać sekret $s \in S$:

1. ujawniają wzajemnie swoje udziały;
2. szukają takiego wiersza $\tilde{r}$ w macierzy $\mathbf{M}$, że $\alpha_p = \mathbf{M}(\tilde{r}, p)$ dla każdego $p \in A$;
3. przyjmują, że sekretem jest element $s = \mathbf{M}(\tilde{r}, p_0)$.

Zazwyczaj uczestnicy pragnący odzyskać sekret odnajdą w macierzy $\mathbf{M}$ więcej niż jeden wiersz $\tilde{r}$ opisany w punkcie 2. Jednakże, jeśli stanowią oni zbiór autoryzowany, to wartość $\mathbf{M}(\tilde{r}, p_0)$ dla tych wierszy będzie taka sama, równa sekretowi wybranemu przez dealera. Z drugiej strony, jeśli uczestnicy tworzą zbiór nieautoryzowany, zgodnie z ideą podziału sekretu nie powinni oni mieć możliwości poznania sekretu, a więc opisana procedura odzyskiwania sekretu nie doprowadzi w takim przypadku do jednoznacznego wyniku. Wprowadzimy teraz kilka definicji usprawniających posługiwanie się macierzą $\mathbf{M}$.

Definicja 1.8. Niech $\mathbf{M}$ będzie schematem podziału sekretu. Mówimy, że uczestnicy ze zbioru $A \subseteq P$ *nie mają żadnej informacji* o udziale uczestnika $p \in P' \setminus A$, jeśli

$$\bigwedge_{r} \bigwedge_{\alpha \in S(p)} \bigvee_{\hat{r}} \quad \Big(\mathbf{M}(r, A) = \mathbf{M}(\hat{r}, A) \;\text{ i }\; \mathbf{M}(\hat{r}, p) = \alpha\Big),$$

albo równoważnie

$$\bigwedge_{\bar{w} \in S(A)} \bigwedge_{\alpha \in S(p)} \bigvee_{\hat{r}} \quad \Big(\mathbf{M}(\hat{r}, A) = \bar{w} \;\text{ i }\; \mathbf{M}(\hat{r}, p) = \alpha\Big).$$

Ujmując powyższą definicję w słowa, uczestnicy ze zbioru $A \subseteq P$ nie mają żadnej informacji o udziale uczestnika $p \in P' \setminus A$, jeśli dla dowolnego ciągu udziałów $\bar{w} \in S(A)$ i dowolnego udziału $\alpha \in S(p)$ istnieje taki wiersz, w którym $\bar{w}$ oraz α występują jednocześnie jako, odpowiednio, udziały uczestników ze zbioru A i uczestnika p. To oznacza, że próba odgadnięcia wartości udziału uczestnika p przez uczestników ze zbioru A prowadzi do wniosku, iż żadnej wartości tego udziału nie można wykluczyć.

Przeciwieństwem sytuacji opisanej powyżej jest posiadanie częściowej informacji o sekrecie pewnego uczestnika, o czym mówi następująca definicja.

Definicja 1.9. Niech $\mathbf{M}$ będzie schematem podziału sekretu. Mówimy, że uczestnicy ze zbioru $A \subseteq P$ *mają częściową informację* o udziale uczestnika $p \in P' \setminus A$, jeśli

$$\bigvee_{\bar{w} \in S(A)} \bigvee_{\alpha \in S(p)} \bigwedge_{\hat{r}} \quad \Big(\mathbf{M}(\hat{r}, A) \neq \bar{w} \;\text{ lub }\; \mathbf{M}(\hat{r}, p) \neq \alpha\Big).$$

Możemy powiedzieć, że uczestnicy ze zbioru $A \subseteq P$ mają częściową informację o udziale uczestnika $p \in P' \setminus A$, jeśli istnieją taki ciąg udziałów $\bar{w} \in S(A)$ oraz taki udział $\alpha \in S(p)$, dla których nie znajdziemy wiersza, w którym $\bar{w}$ oraz α występowałyby jednocześnie jako, odpowiednio, udziały uczestników ze zbioru A i uczestnika p. W takiej sytuacji, jeśli uczestnicy ze zbioru A otrzymają udziały $\bar{w}$, to będą mogli wydedukować, że uczestnik p na pewno nie otrzymał udziału równego α, co stanowi już pewną informację o udziale uczestnika p.

Szczególnym przypadkiem posiadania częściowej informacji o sekrecie pewnego uczestnika jest znajomość jego udziału, co jest sprecyzowane w następującej definicji.

Definicja 1.10. Niech $\mathbf{M}$ będzie schematem podziału sekretu. Mówimy, że uczestnicy ze zbioru $A \subseteq P$ *znają* udział uczestnika $p \in P' \setminus A$, jeśli

$$\bigwedge_{r} \bigwedge_{\hat{r}} \quad \Big(\mathbf{M}(r, A) = \mathbf{M}(\hat{r}, A) \quad \Longrightarrow \quad \mathbf{M}(r, p) = \mathbf{M}(\hat{r}, p)\Big).$$

Mówimy, że uczestnicy ze zbioru $A \subseteq P$ znają udział uczestnika $p \in P' \setminus A$, jeśli we wszystkich wierszach, które są równe po ograniczeniu ich do udziałów uczestników ze zbioru A, występuje taka sama wartość udziału dla uczestnika p.

Teraz zaprezentujemy bardziej precyzyjne definicje pojęć wprowadzonych opisowo w poprzednim podrozdziale.

Definicja 1.11. Zbiór $A \subseteq P$ nazywamy *zbiorem autoryzowanym schematu podziału sekretu* $\mathbf{M}$, jeśli uczestnicy ze zbioru A znają (w sensie definicji 1.10) udział uczestnika p_0.

Definicja 1.12. *Strukturą dostępu Γ schematu podziału sekretu* $\mathbf{M}$ nazywamy rodzinę

$$\Gamma := \{A \subseteq P\colon \text{ uczestnicy ze zbioru } A \text{ znają udział uczestnika } p_0\}.$$

W praktyce od schematów podziału sekretu wymaga się, aby były one bezpieczne, to znaczy, aby zbiory nieautoryzowane nie mogły uzyskać żadnej informacji o udziale uczestnika p_0, czyli sekrecie. W związku z tym rozważa się tak zwane schematy doskonałe, które spełniają ten warunek.

Definicja 1.13. Schemat podziału sekretu $\mathbf{M}$ nazywamy *doskonałym*, jeśli dla dowolnego zbioru $A \subseteq P$, z tego, że uczestnicy ze zbioru A mają częściową informację o udziale uczestnika p_0, wynika, iż A jest zbiorem autoryzowanym.

Schemat Shamira jest doskonały: jeśli uczestnicy ze zbioru $A \subset P$, $|A| < t$, chcieliby wyznaczyć sekret, to byliby zmuszeni za brakujące udziały podstawiać wszystkie elementy ciała $\mathbb{F}_q$, co skutkowałoby otrzymaniem wszystkich możliwych wartości sekretu, a to jest równoznaczne z brakiem jakiejkolwiek informacji o nim.

Od schematów podziału sekretu wymaga się również, aby udziały były możliwie jak najbardziej zbliżone długością do długości sekretu. Pisząc długość, mamy na myśli liczbę bitów potrzebnych do zapisania elementu x pewnego zbioru skończonego X, która wynosi w przybliżeniu $\log_2 |X|$. Wymaganie to ma uzasadnienie praktyczne, z uwagi na sumaryczną ilość informacji o sekrecie, jaka musi być dystrybuowana między uczestników.

Definicja 1.14. *Złożonością schematu podziału sekretu* $\mathbf{M}$ nazywamy liczbę:

$$\rho(\mathbf{M}) := \max_{i \in \{1,\ldots,n\}} \frac{\log_2 |S(p_i)|}{\log_2 |S|}.$$

Definicja 1.15. Schemat podziału sekretu $\mathbf{M}$ nazywamy *idealnym*, jeśli jest doskonały i $\rho(\mathbf{M}) = 1$.

Schemat Shamira jest schematem idealnym, ponieważ jest doskonały oraz $S(p_i) = S = \mathbb{F}_q$ dla każdego $i \in \{1, \ldots, n\}$.

Lemat 1.16. *Jeśli schemat podziału sekretu $\boldsymbol{M}$ jest spójny i doskonały, to dla każdego $p \in P$ zachodzi nierówność $|S(p)| \geqslant |S|$. Jeśli, ponadto, schemat podziału sekretu $\boldsymbol{M}$ jest idealny, to $|S(p)| = |S|$ dla każdego $p \in P$.*

Dowód. Niech p będzie dowolnym uczestnikiem ze zbioru P. Wówczas ze spójności schematu $\mathbf{M}$ wynika, iż istnieje taki minimalny zbiór autoryzowany A, że $p \in A$. Zbiór $B = A \setminus \{p\}$ jest zbiorem nieautoryzowanym. Załóżmy nie wprost, że $|S(p)| < |S|$. Gdyby teraz uczestnicy ze zbioru B próbowali odgadnąć sekret sprawdzając wszystkie wartości ze zbioru $\alpha \in S(p)$, to istnieje co najmniej jedna wartość ze zbioru S, która nie może być w ten sposób uzyskana. To oznacza, że uczestnicy ze zbioru B mają częściową informację o sekrecie, więc na mocy założenia o doskonałości schematu $\mathbf{M}$ zbiór B jest autoryzowany. Stąd otrzymujemy sprzeczność.

W celu wykazania drugiej tezy załóżmy, że schemat $\mathbf{M}$ jest idealny. Z definicji idealności oraz pierwszej tezy otrzymujemy $|S(p)| = |S|$ dla każdego $p \in P$. □

Zgodnie z obowiązującym założeniem, że dla każdego schematu podziału sekretu zbiór możliwych wartości sekretu S oraz zbiory możliwych wartości udziałów $S(p)$, $p \in P$, są skończone, możemy przyjąć bez straty ogólności, że jeśli $|S(p)| = |S|$, to $S(p) = S$.

Zauważyliśmy już, że jeśli dany jest schemat podziału sekretu, to możemy jednoznacznie opisać jego strukturę dostępu Γ. W takiej sytuacji mówimy, że ten schemat realizuje Γ. Jednakże wiemy także, iż zgodnie z definicją 1.5, każdą rodzinę monotoniczną podzbiorów zbioru P nazywamy strukturą dostępu. Uzasadnieniem takiego postępowania jest następujące twierdzenie wykazane w dwóch, powstałych niezależnie, pracach: Benaloha i Leichtera [2] oraz Ito, Saito i Nishizeki [12].

Twierdzenie 1.17 ([2, Theorem 2], [12, Theorem 1])**.** *Dla każdej struktury dostępu $\Gamma \subsetneq \mathcal{P}(P)$ istnieje doskonały schemat podziału sekretu realizujący Γ.*

Niestety, doskonałe schematy skonstruowane dla dowolnej struktury dostępu $\Gamma \subsetneq \mathcal{P}(P)$ przez dwa niezależne zespoły autorów twierdzenia 1.17 nie są idealne, ponieważ sekret jest elementem ciała skończonego, podczas gdy każdy udział jest wektorem z wieloma współrzędnymi z tego ciała. Ponadto w obu zaproponowanych konstrukcjach liczba współrzędnych w udziałach rośnie wykładniczo wraz ze wzrostem liczby uczestników. Do tej pory nie udało się tego wyniku istotnie poprawić ani pokazać, że jest optymalny. Ponadto wiadomo, że istnieją struktury dostępu, które nie są realizowane przez idealne schematy podziału sekretu, co zostało wykazane w pracy Benaloha i Leichtera ([2, Theorem 3]).

Z drugiej strony, schematów podziału sekretu realizujących zadaną strukturę dostępu może być wiele.

Definicja 1.18. *Złożonością struktury dostępu Γ* nazywamy liczbę:

$$\rho(\Gamma) := \inf\{\rho(\mathbf{M})\colon \mathbf{M} \text{ jest doskonałym schematem podziału sekretu i realizuje } \Gamma\}.$$

Definicja 1.19. Strukturę dostępu Γ nazywamy *idealną*, jeśli istnieje idealny schemat podziału sekretu $\mathbf{M}$ realizujący Γ.

Idealne schematy podziału sekretu są z definicji doskonałe, co oznacza, że posiadanie częściowej informacji o sekrecie implikuje jego znajomość. Okazuje się, że taka sama implikacja dotyczy znajomości udziału dowolnego uczestnika w schematach spójnych, o czym mówi następujące twierdzenie.

Twierdzenie 1.20 (Brickell, Davenport [5, Theorem 3])**.** *Niech $\boldsymbol{M}$ będzie spójnym i idealnym schematem podziału sekretu. Jeśli uczestnicy ze zbioru $A \subseteq P$ mają częściową informację o udziale uczestnika $p \in P'$, to uczestnicy ze zbioru A znają udział uczestnika p.*

W zbiorze uczestników P' można wprowadzić pojęcie zależności.

Definicja 1.21. Zbiór uczestników $A \subseteq P'$ schematu podziału sekretu $\mathbf{M}$ nazywamy *zbiorem zależnym*, jeśli istnieje taki uczestnik $p \in A$, że uczestnicy ze zbioru $A \setminus \{p\}$ znają udział uczestnika p. W przeciwnym przypadku zbiór A nazywamy *zbiorem niezależnym*.

Przyjmujemy oznaczenie $\mathbf{D}(\mathbf{M})$ na rodzinę wszystkich zbiorów zależnych schematu $\mathbf{M}$. Wprost z powyższej definicji wynika, że jeśli $A \subseteq P$ jest zbiorem autoryzowanym, to $A \cup \{p_0\}$ jest zbiorem zależnym. Ponadto łatwo zauważyć, że każdy minimalny zbiór autoryzowany jest zbiorem niezależnym.

1.3 Własności idealnych schematów podziału sekretu

W tym podrozdziale omówimy kilka własności spójnych i idealnych schematów podziału sekretu. W szczególności zbadamy związek pomiędzy mocami zbiorów niezależnych i maksymalnych zbiorów nieautoryzowanych, czyli takich, które po dodaniu do nich dowolnego uczestnika stają się zbiorami autoryzowanymi. Zastosowanie uzyskanych wyników, opublikowanych w [13], opiszemy w podrozdziale 3.3.

Na początku zacytujmy interesujący wynik jaki został wykazany w pracy Brickella oraz Davenporta [5], który dotyczy budowy spójnego i idealnego schematu podziału sekretu $\mathbf{M}$. Na potrzeby tego podrozdziału przyjmijmy $q := |S| > 0$.

Lemat 1.22 (Brickell, Davenport [5, Proposition 1])**.** *Niech $\boldsymbol{M}$ będzie spójnym i idealnym schematem podziału sekretu. Jeśli $B \subseteq P$, to $|S(B)| = q^k$ dla pewnego $k \in \mathbb{N}$.*

Jeśli przyjmiemy dodatkowe założenia dotyczące zbioru $B \subseteq P$, to otrzymamy dokładniejszy wynik, o czym mówi następujący lemat.

Lemat 1.23 ([13, Lemma 2])**.** *Niech $\boldsymbol{M}$ będzie spójnym i idealnym schematem podziału sekretu. Jeśli $B \subseteq P'$ jest zbiorem niezależnym, to $|S(B)| = q^{|B|}$.*

Dowód. Niech $\mathbf{M}$ będzie spójnym i idealnym schematem podziału sekretu. Aby wykazać tezę, udowodnimy, że dla każdego $\bar{w} \in S^{|B|}$ istnieje taki wiersz r, że $\mathbf{M}(r, B) = \bar{w}$. Dowód będzie polegał na indukcji względem $k = |B|$. Dla $k = 1$ prawdziwość tezy wynika z lematu 1.16.

Niech $B := \{p_1, \ldots, p_k\}$ będzie takim zbiorem niezależnym, że $k \geqslant 2$. Zauważmy, że $\hat{B} := B \setminus \{p_k\}$ jest również zbiorem niezależnym. Rozważmy dowolny ciąg udziałów $(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k) \in S^k$. Z założenia indukcyjnego istnieje taki wiersz $\hat{r}$, że $\mathbf{M}(\hat{r}, \hat{B}) = (\alpha_1, \ldots, \alpha_{k-1})$. Z niezależności zbioru B wynika, że uczestnicy ze zbioru $\hat{B}$ nie mają żadnej informacji o udziale uczestnika p_k, dlatego też istnieje taki wiersz r, że $\mathbf{M}(r, \hat{B}) = \mathbf{M}(\hat{r}, \hat{B})$ i $\mathbf{M}(r, p_k) = \alpha_k$, co kończy dowód. □

Poniższe twierdzenie pozwala oszacować z góry liczbę wierszy w spójnym i idealnym schemacie podziału sekretu.

Twierdzenie 1.24 ([13, Theorem 3])**.** *Jeśli $\boldsymbol{M}$ jest spójnym i idealnym schematem podziału sekretu, to liczba wierszy w macierzy $\boldsymbol{M}$ jest nie większa niż $q^{|A|+1}$ dla każdego maksymalnego zbioru nieautoryzowanego $A \subseteq P$.*

Dowód. Niech $\mathbf{M}$ będzie spójnym i idealnym schematem podziału sekretu oraz niech $A \subseteq P$ będzie maksymalnym zbiorem nieautoryzowanym. Załóżmy nie wprost, że macierz $\mathbf{M}$ ma więcej niż $q^{|A|+1}$ wierszy. Wówczas istnieją takie dwa różne wiersze $\tilde{r}$, $\hat{r}$ w macierzy $\mathbf{M}$, że

$$\mathbf{M}(\tilde{r}, A \cup \{p_0\}) = \mathbf{M}(\hat{r}, A \cup \{p_0\}).$$

Ponadto z faktu, iż żadne dwa wiersze macierzy $\mathbf{M}$ nie są równe, wnioskujemy, że istnieje uczestnik $p \in P \setminus A$, dla którego $\mathbf{M}(\tilde{r}, p) \neq \mathbf{M}(\hat{r}, p)$. Ponieważ $A \cup \{p\}$ jest zbiorem autoryzowanym, więc dla każdego ciągu udziałów $\bar{w} \in S(A)$, $\alpha \in S(p)$, sekret jest wyznaczony jednoznacznie, to znaczy, jeśli $\mathbf{M}(r, A) = \bar{w} = \mathbf{M}(r', A)$ oraz $\mathbf{M}(r, p) = \alpha = \mathbf{M}(r', p)$, to $\mathbf{M}(r, p_0) = \mathbf{M}(r', p_0)$.

Przypuśćmy, że uczestnicy ze zbioru A próbują odgadnąć sekret, dla ustalonego udziału $\bar{w} \in S(A)$ sprawdzając wszystkie wartości $\alpha \in S(p)$. Liczba uzyskanych w ten sposób możliwych wartości sekretu jest nie większa niż liczba elementów zbioru $S(p)$, ale macierz $\mathbf{M}$ jest schematem idealnym, więc $S(p) = S$ na mocy lematu 1.16. Jednakże, rozpatrując wiersze $\tilde{r}$ i $\hat{r}$, dla dwóch różnych udziałów $\tilde{\alpha} = \mathbf{M}(\tilde{r}, p)$ i $\hat{\alpha} = \mathbf{M}(\hat{r}, p)$, uczestnicy ze zbioru A otrzymują ten sam sekret $\mathbf{M}(\tilde{r}, p_0) = \mathbf{M}(\hat{r}, p_0)$. Istnieje zatem co najmniej jedna wartość zbioru S, która nie może być w ten sposób uzyskana, co oznacza, że uczestnicy ze zbioru A mają częściową informację o sekrecie. Z doskonałości schematu $\mathbf{M}$ wynika więc, że zbiór A jest zbiorem autoryzowanym, w sprzeczności z początkowym założeniem. □

Wniosek płynący z powyższego twierdzenia jest następujący.

Wniosek 1.25 ([13, Theorem 4])**.** *Jeśli* $\boldsymbol{M}$ *jest spójnym i idealnym schematem podziału sekretu, to dla każdego maksymalnego zbioru nieautoryzowanego* $A \subseteq P$ *i każdego zbioru niezależnego* $B \subseteq P$ *zachodzi nierówność* $|B| \leqslant |A| + 1$*. Jeśli dodatkowo założymy, że zbiór* B *jest zbiorem nieautoryzowanym, to* $|B| \leqslant |A|$*.*

Dowód. Niech $\mathbf{M}$ będzie spójnym i idealnym schematem podziału sekretu oraz niech A i B będą zbiorami opisanymi w założeniach. Z lematu 1.23 otrzymujemy, że $\mathbf{M}$ ma co najmniej $q^{|B|}$ wierszy. Z drugiej strony, stosując twierdzenie 1.24, liczba wierszy macierzy $\mathbf{M}$ nie przekracza $q^{|A|+1}$. Stąd $q^{|B|} \leqslant q^{|A|+1}$, co implikuje pierwszą tezę.

Jeśli dodatkowo B jest zbiorem nieautoryzowanym, to dla każdego ciągu udziałów $\bar{w} \in S(B)$ oraz dla każdego elementu $\alpha \in S(p_0)$ istnieje taki wiersz r, że $\mathbf{M}(r, B) = \bar{w}$ oraz $\mathbf{M}(r, p_0) = \alpha$. Stąd macierz $\mathbf{M}$ ma w takim przypadku co najmniej $q^{|B|+1}$ wierszy. Zatem $q^{|B|+1} \leqslant q^{|A|+1}$, co kończy dowód tezy drugiej. □

Rozdział 2

Matroidy i polimatroidy

W tym rozdziale podamy podstawowe definicje i fakty dotyczące matroidów i polimatroidów. Odgrywają one istotną rolę w badaniu schematów podziału sekretu oraz struktur dostępu.

2.1 Matroidy

Matroidy zostały wprowadzone przez Whitneya [27] jako najbardziej ogólna struktura, w której można rozważać pojęcie niezależności rozważane dotąd w przestrzeniach liniowych. Istnieje wiele równoważnych definicji matroidu, a dla naszych potrzeb przedstawimy dwie z nich. Ich równoważność jest szczegółowo wykazana w monografii Oxleya [16].

Definicja 2.1. *Matroidem* $\mathcal{M}$ nazywamy parę (E, r), gdzie E jest niepustym zbiorem skończonym i odwzorowanie $r\colon \mathcal{P}(E) \to \mathbb{Z}$ spełnia warunki:

1. Jeśli $X \subseteq E$, to $0 \leqslant r(X) \leqslant |X|$.
2. Jeśli $X \subseteq Y \subseteq E$, to $r(X) \leqslant r(Y)$.
3. Jeśli $X, Y \subseteq E$, to $r(X \cup Y) + r(X \cap Y) \leqslant r(X) + r(Y)$.

Ponadto:

- Odwzorowanie r nazywamy *funkcją rangi* matroidu $\mathcal{M}$;
- Liczbę $r(X)$, $X \subseteq E$, nazywamy *rangą zbioru* X;
- Liczbę $r(E)$ nazywamy *rangą matroidu* $\mathcal{M}$;
- Warunek drugi nazywamy *monotonicznością* funkcji r;
- Warunek trzeci nazywamy *submodularnością* funkcji r.

Definicja 2.2. *Matroidem* $\mathcal{M}$ nazywamy parę $(E, \mathcal{I})$, gdzie E jest niepustym zbiorem skończonym i rodzina $\mathcal{I}$ podzbiorów zbioru E spełnia warunki:

1. $\emptyset \in \mathcal{I}$.
2. Jeśli $I_1 \in \mathcal{I}$ oraz $I_2 \subseteq I_1$, to $I_2 \in \mathcal{I}$.
3. Jeśli $I_1, I_2 \in \mathcal{I}$ oraz $|I_1| < |I_2|$, to istnieje taki element $e \in I_2 \setminus I_1$, że $I_1 \cup \{e\} \in \mathcal{I}$.

Ponadto:

- Elementy rodziny $\mathcal{I}$ nazywamy *zbiorami niezależnymi* matroidu $\mathcal{M}$;
- Podzbiór zbioru E nie należący do rodziny $\mathcal{I}$ nazywamy *zbiorem zależnym*;
- Każdy maksymalny zbiór niezależny nazywamy *bazą* matroidu $\mathcal{M}$;
- Każdy minimalny zbiór zależny nazywamy *obwodem* matroidu $\mathcal{M}$.

W dalszej części pracy będziemy korzystać z pewnych własności baz matroidu, które prezentujemy w poniższych lematach. Pierwszy stwierdza, iż wszystkie bazy matroidu są równoliczne, a własność baz opisana w drugim lemacie określana jest czasem aksjomatem wymiany.

Lemat 2.3 (Oxley [16, Lemma 1.2.1])**.** *Jeśli B_1 oraz B_2 są bazami pewnego matroidu, to $|B_1| = |B_2|$.*

Lemat 2.4 (Oxley [16, Lemma 1.2.2])**.** *Jeśli B_1 i B_2 są bazami matroidu $\mathcal{M}$, $e \in B_2 \setminus B_1$, to istnieje taki element $f \in B_1 \setminus B_2$, że zbiór $(B_2 \setminus \{e\}) \cup \{f\}$ jest również bazą $\mathcal{M}$.*

Jeśli matroid $\mathcal{M}$ jest zdefiniowany za pomocą rangi r, to rodzina $\mathcal{I}$ składa się z takich podzbiorów zbioru E, których ranga jest równa ich mocy:

$$\mathcal{I} := \{I \subseteq E : r(I) = |I|\}.$$

Jeśli matroid $\mathcal{M}$ jest zdefiniowany za pomocą rodziny zbiorów niezależnych $\mathcal{I}$, to wartość odwzorowania r dla dowolnego zbioru $X \subseteq E$ jest równa maksimum mocy zbiorów niezależnych zawartych w X:

$$r(X) := \max\{|I| : I \subseteq X, I \in \mathcal{I}\}.$$

Stąd i z równoliczności baz wynika, że ranga matroidu $\mathcal{M}$ jest równa mocy dowolnej jego bazy.

Przy pomocy obwodów matroidu możemy zdefiniować pojęcie matroidu spójnego.

Definicja 2.5. Matroid $(E, \mathcal{I})$ nazywamy *spójnym*, jeśli dla każdych dwóch różnych elementów $e, f \in E$ istnieje taki jego obwód C, że $e, f \in C$.

Dużą rolę w badaniach związanych ze schematami podziału sekretu i strukturami dostępu odgrywa pojęcie portu matroidu, o czym przekonamy się w podrozdziale 2.3. Jego definicja jest następująca.

Definicja 2.6. *Portem matroidu* $\mathcal{M} = (E, r)$ *w punkcie* $p_0 \in E$ nazywamy rodzinę:

$$\Gamma_{p_0}(\mathcal{M}) := \{X \subseteq E \setminus \{p_0\} : r(X \cup \{p_0\}) = r(X)\}.$$

W dalszej części pracy, zamiast precyzyjnego sformułowania „port matroidu, zdefiniowanego na zbiorze E, w punkcie p_0" będziemy często pisać po prostu „port matroidu", o ile nie będzie to prowadzić do żadnych nieporozumień.

Zauważmy, że port matroidu może być rodziną pustą, więc oczywiście jest wówczas rodziną monotoniczną. Jeśli port $\Gamma_{p_0}(\mathcal{M})$ matroidu $\mathcal{M}$ w punkcie p_0 nie jest rodziną pustą, to również jest rodziną monotoniczną. Istotnie, weźmy takie zbiory $X, Y \subseteq E \setminus \{p_0\}$, że $X \in \Gamma_{p_0}(\mathcal{M})$ oraz $X \subseteq Y$. Wówczas z submodularności funkcji r wynika, że

$$r(\{p_0\} \cup Y) + r(X) = r\Big((X \cup \{p_0\}) \cup Y\Big) + r\Big((X \cup \{p_0\}) \cap Y\Big) \leqslant \\ \leqslant r(X \cup \{p_0\}) + r(Y),$$

a z monotoniczności rangi oraz założenia $X \in \Gamma_{p_0}(\mathcal{M})$ otrzymujemy

$$r(Y) \leqslant r(\{p_0\} \cup Y) \leqslant r(Y).$$

Stąd $r(\{p_0\} \cup Y) = r(Y)$, czyli $Y \in \Gamma_{p_0}(\mathcal{M})$. Zatem, zgodnie z twierdzeniem 1.17, każdy port matroidu jest strukturą dostępu pewnego doskonałego schematu podziału sekretu.

Szczególną rodziną matroidów są matroidy reprezentowalne nad ciałem, które definiujemy następująco.

Definicja 2.7. Matroid (E, r) nazywamy *matroidem reprezentowalnym nad ciałem* $\mathbb{F}$, jeśli istnieją taka przestrzeń liniowa V o skończonym wymiarze nad ciałem $\mathbb{F}$ oraz takie odwzorowanie $\varphi\colon E \to V$, że

$$r(X) = \dim\Big(\operatorname{lin}\{\varphi(X)\}\Big)$$

dla każdego niepustego zbioru $X \subseteq E$.

W sytuacji, gdy wskazanie ciała $\mathbb{F}$ nie jest istotne, będziemy mówili po prostu o matroidzie reprezentowalnym.

2.2 Polimatroidy

Ten podrozdział poświęcimy polimatroidom, które stanowią uogólnienie klasy matroidów. Czytelnikom zainteresowanym szerszym omówieniem ich teorii polecamy monografię Schrijvera [19].

Definicja 2.8. *Polimatroidem* $\mathcal{S}$ nazywamy parę (Q, h), gdzie Q jest niepustym zbiorem skończonym i odwzorowanie $h\colon \mathcal{P}(Q) \to \mathbb{R}$ spełnia warunki:

1. $h(\emptyset) = 0$.
2. Jeśli $X \subseteq Y \subseteq Q$, to $h(X) \leqslant h(Y)$.
3. Jeśli $X, Y \subseteq Q$, to $h(X \cup Y) + h(X \cap Y) \leqslant h(X) + h(Y)$.

Ponadto:

– Odwzorowanie h nazywamy *funkcją rangi* polimatroidu $\mathcal{S}$;
– Liczbę $h(X)$, $X \subseteq Q$, nazywamy *rangą zbioru* X;
– Liczbę $h(Q)$ nazywamy *rangą polimatroidu* $\mathcal{S}$;
– Warunek drugi nazywamy *monotonicznością* funkcji h;
– Warunek trzeci nazywamy *submodularnością* funkcji h.

Definicja 2.9. *Punktem atomowym* polimatroidu $\mathcal{S} = (Q, h)$ nazywamy taki element $p_0 \in Q$, że dla każdego $X \subseteq Q$ zachodzi

$$h(X \cup \{p_0\}) = h(X) \quad \text{lub} \quad h(X \cup \{p_0\}) = h(X) + 1.$$

Zauważmy, że jeśli $\mathcal{S}$ jest matroidem, to każdy element należący do Q jest jego punktem atomowym.

Definicja 2.10. *Portem polimatroidu* $\mathcal{S} = (Q, h)$ *w punkcie atomowym* $p_0 \in Q$ nazywamy następującą rodzinę podzbiorów zbioru Q:

$$\Delta_{p_0}(\mathcal{S}) := \{X \subseteq Q \setminus \{p_0\} : h(X \cup \{p_0\}) = h(X)\}.$$

Port polimatroidu $\Delta_{p_0}(\mathcal{S})$ jest zawsze rodziną monotoniczną, co pokazujemy analogicznie jak w przypadku portu matroidu.

Definicja 2.11. *Polimatroidem całkowitym* nazywamy polimatroid, którego funkcja rangi przyjmuje wyłącznie wartości całkowite.

Jeśli $\mathcal{S} = (Q, h)$ jest polimatroidem całkowitym oraz dla każdego $X \subseteq Q$ spełniony jest warunek $h(X) \leqslant |X|$, to $\mathcal{S}$ jest matroidem.

Podobnie jak w przypadku matroidów, możemy wyróżnić rodzinę polimatroidów reprezentowalnych. Przyjmujemy oznaczenie $\mathcal{L}(V)$ na rodzinę wszystkich podprzestrzeni przestrzeni liniowej V.

Definicja 2.12. Polimatroid (Q, h) nazywamy *reprezentowalnym nad ciałem* $\mathbb{F}$, jeśli istnieją taka przestrzeń liniowa V nad ciałem $\mathbb{F}$, o skończonym wymiarze, oraz takie odwzorowanie $\varphi\colon Q \to \mathcal{L}(V)$, że

$$h(X) = \dim\Big(\sum_{i \in X} \varphi(i)\Big)$$

dla każdego niepustego zbioru $X \subseteq Q$.

Każdy polimatroid reprezentowalny jest również polimatroidem całkowitym. Nietrudno także zauważyć, że jeśli w powyższej definicji założymy dodatkowo, że $\dim(\varphi(i)) \leqslant 1$ dla każdego $i \in Q$, to otrzymamy równoważną definicję matroidu reprezentowalnego nad ciałem $\mathbb{F}$. Podobnie jak w przypadku matroidów, gdy wskazanie ciała $\mathbb{F}$ nie będzie istotne, będziemy używali pojęcia polimatroidu reprezentowalnego.

W dalszej części pracy będziemy rozpatrywali związek pomiędzy strukturami dostępu, a polimatroidami całkowitymi. W związku z tym przyjmujemy założenie, że wszystkie rozważane polimatroidy są całkowite.

W dalszym ciągu pracy przez $\mathcal{Z}$ oraz $\mathcal{Z}'$ będziemy oznaczać polimatroidy całkowite zdefiniowane odpowiednio na zbiorach $J_m := \{1, \ldots, m\}$ i $J'_m := \{0, \ldots, m\}$ oraz mające funkcje rangi h i h'. Symbol $\bar{e}_i$ oznaczać będzie wektor, którego i-ta współrzędna jest równa 1, natomiast pozostałe współrzędne są równe 0. Dla wektora $\bar{w} = (w_1, \ldots, w_m) \in \mathbb{N}_0^m$ i $X = \{i_1, \ldots, i_j\} \subseteq J_m$, $i_1 < \cdots < i_j$, przyjmujemy $\bar{w}(X) := (w_{i_1}, \ldots, w_{i_j})$, zaś $\bar{w}_X$ oznacza taki wektor $(\omega_1, \ldots, \omega_m)$, że:

$$\omega_i := \begin{cases} w_i, & \text{jeśli } i \in X; \\ 0, & \text{jeśli } i \notin X. \end{cases}$$

Definicja 2.13. Sumę współrzędnych wektora $\bar{w} \in \mathbb{N}_0^m$ nazywamy jego *wagą* i oznaczamy jako $|\bar{w}|$.

Zauważmy, że $|\bar{w}(X)| = |\bar{w}_X|$ dla dowolnych $\bar{w} \in \mathbb{N}_0^m$ oraz $X \subseteq J_m$.

Definicja 2.14. *Nośnikiem wektora* $\bar{w} \in \mathbb{N}_0^m$ nazywamy zbiór

$$\operatorname{supp} \bar{w} := \{i \in J_m : w_i \neq 0\}.$$

Jeśli Θ jest rodziną wektorów należących do $\mathbb{N}_0^m$, to zbiór

$$\operatorname{supp} \Theta := \{\operatorname{supp} \bar{w} : \bar{w} \in \Theta\}$$

nazywamy *nośnikiem rodziny* Θ.

Wprowadzimy teraz pojęcia zbioru wektorów niezależnych polimatroidu oraz baz polimatroidu. Zagadnienia te są szerzej omówione w pracy Herzoga i Hibi [11]. Pamiętajmy, że rozważamy jedynie polimatroidy całkowite.

Definicja 2.15. *Zbiorem wektorów niezależnych* polimatroidu $\mathcal{Z}$ nazywamy rodzinę

$$\mathcal{D}(\mathcal{Z}) := \{\bar{w} \in \mathbb{N}_0^m : |\bar{w}_X| \leqslant h(X) \text{ dla każdego } X \subseteq J_m\}.$$

Nie jest trudno zauważyć, że jeśli $\mathcal{Z}$ jest polimatroidem i $\mathcal{D}(\mathcal{Z})$ jego zbiorem wektorów niezależnych, to $h(X) = \max\{|\bar{w}_X| : \bar{w} \in \mathcal{D}(\mathcal{Z})\}$ dla każdego $X \subseteq J_m$.

Przypomnijmy, że przez porządek standardowy w zbiorze wektorów rozumiemy relację $\leqslant_s$ w zbiorze $\mathbb{Z}^m$ określoną jako:

$$\bar{w} \leqslant_s \bar{v} \iff \bigwedge_{i \in J_m} w_i \leqslant v_i, \qquad \bar{w}, \bar{v} \in \mathbb{Z}^m.$$

W [11] wykazano, że zbiór wektorów niezależnych $\mathcal{D}(\mathcal{Z})$ polimatroidu $\mathcal{Z}$ spełnia następujące warunki:

1. $\mathcal{D}(\mathcal{Z})$ jest niepusty i skończony.
2. Jeśli $\bar{w} \in \mathcal{D}(\mathcal{Z})$, $\bar{v} \in \mathbb{N}_0^m$ oraz $\bar{v} \leqslant_s \bar{w}$, to $\bar{v} \in \mathcal{D}(\mathcal{Z})$.
3. Jeśli $\bar{w}, \bar{v} \in \mathcal{D}(\mathcal{Z})$, $|\bar{w}| < |\bar{v}|$, to istnieje taki $i \in J_m$, że $w_i < v_i$ oraz $\bar{w} + \bar{e}_i \in \mathcal{D}(\mathcal{Z})$.

Geometrycznie $\mathcal{D}(\mathcal{Z})$ jest więc zbiorem punktów o nieujemnych i całkowitych współrzędnych zawartych w pewnym m-wymiarowym wielościanie wypukłym, który dodatkowo spełnia powyższe warunki. W tej samej pracy pokazano, że dla każdego zbioru $\mathcal{D} \subseteq \mathbb{N}_0^m$ spełniającego powyższe trzy warunki istnieje dokładnie jeden polimatroid całkowity $\mathcal{Z}$, którego zbiorem wektorów niezależnych jest $\mathcal{D}$.

Teraz przechodzimy do pojęcia bazy polimatroidu.

Definicja 2.16. Jeśli $\mathcal{Z}$ jest polimatroidem i $\mathcal{D}(\mathcal{Z})$ jego zbiorem wektorów niezależnych, to wektory maksymalne w sensie porządku standardowego $\leqslant_s$ w zbiorze $\mathcal{D}(\mathcal{Z})$ nazywamy *bazami* polimatroidu $\mathcal{Z}$. Zbiór baz polimatroidu $\mathcal{Z}$ oznaczamy $\mathcal{B}(\mathcal{Z})$.

Wagi wszystkich baz polimatroidu $\mathcal{Z}$ są równe $h(J_m)$, czyli są równe randze polimatroidu $\mathcal{Z}$. Ponadto nie jest trudno sprawdzić, że $(X, h|_{\mathcal{P}(X)})$ dla dowolnego $X \subseteq J_m$ jest również polimatroidem. Oznaczamy go symbolem $\mathcal{Z}|X$ i nazywamy polimatroidem $\mathcal{Z}$ ograniczonym do zbioru X.

Jeśli $\mathcal{Z}$ jest polimatroidem oraz $X \subseteq J_m$, to przez $\mathcal{B}(\mathcal{Z}, X)$ oznaczać będziemy zbiór takich wektorów niezależnych $\bar{w} \in \mathcal{D}(\mathcal{Z})$, że $\operatorname{supp} \bar{w} \subseteq X$ oraz $|\bar{w}| = h(X)$, czyli:

$$\mathcal{B}(\mathcal{Z}, X) = \{\bar{w} \in \mathbb{N}_0^m : \operatorname{supp} \bar{w} \subseteq X,\ \forall_{Y \subseteq X} |\bar{w}_Y| \leqslant h(Y),\ |\bar{w}_X| = h(X)\}. \quad (2.1)$$

Należy zwrócić uwagę na bliski związek zbioru $\mathcal{B}(\mathcal{Z}, X)$ oraz zbioru baz polimatroidu $\mathcal{Z}|X$. Istotnie, zauważmy, że

$$\bar{w} \in \mathcal{B}(\mathcal{Z}, X) \iff \operatorname{supp} \bar{w} \subseteq X \ \text{ oraz } \ \bar{w}(X) \in \mathcal{B}(\mathcal{Z}|X).$$

Uwaga 2.17. Rodzina $\mathcal{B}(\mathcal{Z}, X)$ zawsze jest niepusta. W skrajnych przypadkach, gdy $X = \emptyset$ lub funkcja rangi polimatroidu $\mathcal{Z}$ przyjmuje wyłącznie wartość równą 0, rodzina $\mathcal{B}(\mathcal{Z}, X)$ zawiera jedynie wektor zerowy.

Zwróćmy jeszcze uwagę na fakt, że jeśli $\mathcal{Z}$ jest matroidem, to wektory należące do rodziny $\mathcal{B}(\mathcal{Z}, X)$ mają tylko współrzędne równe 0 lub 1.

Często będziemy korzystać z następującego lematu.

Lemat 2.18. *Jeśli $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$, $X \subseteq J_m$, to $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$.*

Dowód. Wystarczy pokazać równość $|\bar{w}_{\operatorname{supp} \bar{w}}| = h(\operatorname{supp} \bar{w})$. Korzystając z założenia oraz monotoniczności funkcji h otrzymujemy:

$$|\bar{w}| = |\bar{w}_X| = h(X) \geqslant h(\operatorname{supp} \bar{w}) \geqslant |\bar{w}_{\operatorname{supp} \bar{w}}| = |\bar{w}|. \qquad \square$$

Przechodzimy teraz do rozważań, które dotyczą pojęcia rodziny kompatybilnej z polimatroidem. Rozpoczniemy od następującej definicji.

Definicja 2.19. Polimatroid $\mathcal{Z}' = (J'_m, h')$ nazywamy *uzupełnieniem polimatroidu* $\mathcal{Z}$, jeśli $h'(\{0\}) = 1$ oraz $\mathcal{Z} = \mathcal{Z}'|J_m$.

Zauważmy, że z warunku $h'(\{0\}) = 1$ wynika, iż 0 jest punktem atomowym polimatroidu $\mathcal{Z}'$. Istotnie, niech $X \subseteq J'_m$. Jeśli $0 \in X$, to $h'(X \cup \{0\}) = h'(X)$. Jeśli natomiast $0 \notin X$, to korzystając z submodularności funkcji h' otrzymujemy

$$\begin{aligned} h'(X \cup \{0\}) &= h'(X \cup \{0\}) + h'(\emptyset) = \\ &= h'(X \cup \{0\}) + h'(X \cap \{0\}) \leqslant h'(X) + h'(\{0\}) = h'(X) + 1. \end{aligned}$$

Jednakże z monotoniczności funkcji h' mamy $h'(X) \leqslant h'(X \cup \{0\})$, więc biorąc pod uwagę fakt, iż mamy do czynienia z polimatroidami całkowitymi, wnioskujemy, że $h'(X \cup \{0\}) = h'(X)$ lub $h'(X \cup \{p_0\}) = h'(X) + 1$.

Jeśli $\mathcal{Z}'$ jest uzupełnieniem polimatroidu $\mathcal{Z}$, to port $\mathcal{Z}'$ w punkcie atomowym 0 oznaczamy jako $\Delta(\mathcal{Z}')$, to znaczy $\Delta(\mathcal{Z}') := \Delta_0(\mathcal{Z}')$. Nietrudno zauważyć, że jeśli $\Delta(\mathcal{Z}') \neq \emptyset$, to z monotoniczności rodziny $\Delta(\mathcal{Z}')$ mamy $J_m \in \Delta(\mathcal{Z}')$. Należy pamiętać, że dla polimatroidu $\mathcal{Z}$ jego uzupełnienie nie jest wyznaczone jednoznacznie.

Definicja 2.20. Rodzinę monotoniczną $\Delta \subseteq \mathcal{P}(J_m)$ nazywamy *kompatybilną* z polimatroidem $\mathcal{Z}$, jeżeli istnieje uzupełnienie $\mathcal{Z}'$ polimatroidu $\mathcal{Z}$, dla którego $\Delta = \Delta(\mathcal{Z}')$.

Pokażemy, że jeśli rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$, to polimatroid $\mathcal{Z}'$ w powyższej definicji jest wyznaczony jednoznacznie. Załóżmy zatem, że rodzina monotoniczna $\Delta \subseteq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ oraz, że $\Delta(\mathcal{W}') = \Delta = \Delta(\mathcal{Z}')$, gdzie $\mathcal{W}'$ oraz $\mathcal{Z}'$ są uzupełnieniami polimatroidu $\mathcal{Z}$, których funkcje rangi są odpowiednio równe f' oraz h'. Weźmy dowolny zbiór $X \subseteq J'_m$ i rozpatrzmy dwa przypadki. Jeśli $0 \notin X$, to oczywiście $f'(X) = h(X) = h'(X)$. W przypadku, gdy $0 \in X$, przyjmijmy $Y := X \setminus \{0\}$ i ponownie rozważmy dwie możliwości. Jeśli $Y \in \Delta$, to

$$f'(X) = f'(Y \cup \{0\}) = f'(Y) = h(Y) = h'(Y) = h'(Y \cup \{0\}) = h'(X),$$

a jeśli $Y \notin \Delta$, to skoro 0 jest punktem atomowym, więc:

$$f'(X) = f'(Y \cup \{0\}) = f'(Y) + 1 = h(Y) + 1 = h'(Y) + 1 = h'(Y \cup \{0\}) = h'(X).$$

Pokazaliśmy, że dla każdego $X \subseteq J'_m$ mamy $f'(X) = h'(X)$, co oznacza, że polimatroidy $\mathcal{W}'$ oraz $\mathcal{Z}'$ są równe.

Zauważmy, że polimatroid $\mathcal{Z}$, którego funkcja rangi ma wszystkie wartości równe 0, jest kompatybilny jedynie z rodziną monotoniczną $\Delta = \emptyset$. Z drugiej strony, pusta rodzina monotoniczna jest kompatybilna z każdym polimatroidem $\mathcal{Z}$. Ponadto, jeśli $\Delta = \mathcal{P}(J_m)$, to rodzina Δ nie jest kompatybilna z żadnym polimatroidem. Stąd w dalszej części pracy wszystkie rozważane rodziny monotoniczne Δ są różne od $\emptyset$ i $\mathcal{P}(J_m)$. Zakładamy również, że funkcja rangi polimatroidu $\mathcal{Z}$ nie jest funkcją zerową. Rodzinę minimalnych, w sensie inkluzji, zbiorów należących do rodziny monotonicznej Δ oznaczamy jako $\min \Delta$.

Sprawdzenie kompatybilności dowolnej rodziny Δ z polimatroidem $\mathcal{Z}$ nie nastręcza trudności związanych z konstrukcją $\mathcal{Z}'$, jeśli zastosujemy poniższy lemat, który jest wnioskiem z wyniku uzyskanego przez Csirmaza [6, Proposition 2.3].

Lemat 2.21 (Farràs, Martí-Farré, Padró [8, Proposition 7])**.** *Rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy spełnione są następujące warunki:*

1. *Jeśli $Y \subseteq X \subseteq J_m$, $Y \notin \Delta$ i $X \in \Delta$, to $h(Y) < h(X)$.*
2. *Jeśli $X, Y \in \Delta$ i $X \cap Y \notin \Delta$, to $h(X \cap Y) + h(X \cup Y) < h(X) + h(Y)$.*

Będziemy bardzo często powoływać się na powyższy lemat w dalszej części pracy, dlatego będziemy używali nazwy lemat Csirmaza odwołując się do 2.21.

Warto jeszcze wspomnieć o pewnych możliwych uproszczeniach. Pierwsze z nich jest wynikiem pochodzącym od Schrijvera [19] i dotyczy submodularności funkcji rangi.

Twierdzenie 2.22 (Schrijver [19, Theorem 44.1])**.** *Przekształcenie $h : \mathcal{P}(Q) \to \mathbb{R}$ jest funkcją submodularną wtedy i tylko wtedy, gdy*

$$h(X) + h(X \cup \{i, j\}) \leqslant h(X \cup \{i\}) + h(X \cup \{j\})$$

dla wszystkich $i, j \in Q$, $i \neq j$, oraz dla wszystkich $X \subseteq Q \setminus \{i, j\}$.

Okazuje się, że dla lematu Csirmaza (2.21) istnieje prostsza, równoważna, wersja.

Lemat 2.23 (Martín, Padró, Yang [15, Proposition 2])**.** *Rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy spełnione są następujące warunki:*

1. *Jeśli* $X \subseteq J_m$, $X \notin \Delta$, $i \in J_m$ *oraz* $X \cup \{i\} \in \Delta$, *to* $h(X) < h(X \cup \{i\})$.
2. *Jeśli* $X \notin \Delta$, $i, j \in J_m$, $i \neq j$ *oraz* $X \cup \{i\}$, $X \cup \{j\} \in \Delta$, *to*

$$h(X) + h(X \cup \{i, j\}) < h(X \cup \{i\}) + h(X \cup \{j\}).$$

2.2.1 Polimatroidy jednorodne

Polimatroidy jednorodne będą odgrywać istotną rolę w naszych badaniach. Ich definicja jest następująca.

Definicja 2.24. Polimatroid całkowity $\mathcal{Z} = (J_m, h)$ nazywamy *jednorodnym*, gdy

$$|X| = |Y| \implies h(X) = h(Y)$$

dla wszystkich $X, Y \subseteq J_m$.

Zauważmy, iż przyjmując $h_i = h(X)$ dla $X \subseteq J_m$, $|X| = i$, otrzymujemy ciąg liczb całkowitych, który wyznacza funkcję rangi polimatroidu jednorodnego. Okazuje się, że prostą charakteryzację takich ciągów, a zatem i polimatroidów, można uzyskać badając własności ciągu jego przyrostów.

Stwierdzenie 2.25. *Jeśli para* (J_m, h) *jest polimatroidem jednorodnym, to ciąg* $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m-1}$, *określony wzorem*

$$g_t = h_{t+1} - h_t, \quad t = 0, 1, \ldots, m-1,$$

gdzie $h_i = h(X)$ *dla* $X \subseteq J_m$, $|X| = i$, *jest nierosnący i jego wyrazy są nieujemnymi liczbami całkowitymi.*

Dowód. Z definicji polimatroidu jednorodnego wynika, że liczby h_i, $i = 0, 1, \ldots, m$, a zatem również ciąg $\boldsymbol{g}$, są poprawnie określone. Z monotoniczności funkcji rangi wynika, że ciąg $(h_i)_{i=0,1,\ldots,m}$ jest niemalejący, więc ciąg $\boldsymbol{g}$ ma wyrazy nieujemne. Podobnie, skoro ranga h polimatroidu całkowitego przyjmuje jedynie wartości całkowite, zatem zarówno ciąg $(h_i)_{i=0,1,\ldots,m}$, jak i ciąg $\boldsymbol{g}$ mają wyłącznie wyrazy całkowite.

Weźmy teraz dowolne $t \in \{0, 1, \ldots, m-2\}$ oraz takie zbiory $X, Y \subseteq J_m$, że $|X| = |Y| = t + 1$, $|X \cap Y| = t$. Stąd $|X \cup Y| = t + 2$, więc z submodularności funkcji h otrzymujemy

$$h_{t+2} + h_t = h(X \cup Y) + h(X \cap Y) \leqslant h(X) + h(Y) = h_{t+1} + h_{t+1},$$

a stąd

$$g_{t+1} = h_{t+2} - h_{t+1} \leqslant h_{t+1} - h_t = g_t,$$

co oznacza, że ciąg $\boldsymbol{g}$ jest nierosnący. □

Niech teraz $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m-1}$ będzie dowolnym ciągiem liczb całkowitych. Definiujemy ciąg $(h_i)_{i=0,1,\ldots,m}$ przyjmując $h_0 = 0$ oraz

$$h_i = \sum_{t=0}^{i-1} g_t \quad \text{dla } i = 1, \ldots, m.$$

Przy pomocy liczb h_i określamy funkcję $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ wzorem $h(X) = h_{|X|}$ dla $X \subseteq J_m$.

Stwierdzenie 2.26. *Jeśli ciąg $\boldsymbol{g}$ jest nierosnący i jego wyrazy są nieujemnymi liczbami całkowitymi, to para (J_m, h) jest polimatroidem jednorodnym.*

Dowód. Należy sprawdzić, że określona powyżej funkcja h spełnia warunki rangi polimatroidu jednorodnego. Warunek $h(\emptyset) = h_0 = 0$ wynika bezpośrednio z przyjętego wzoru. Skoro wyrazy $\boldsymbol{g}$ są nieujemne, więc ciąg $(h_i)_{i=0,1,\ldots,m}$ jest niemalejący, skąd wynika monotoniczność funkcji h.

Aby udowodnić submodularność funkcji h, posłużymy się twierdzeniem 2.22. Istotnie, dla $i, j \in J_m$, $i \neq j$, $X \subseteq J_m \setminus \{i, j\}$, przyjmijmy $t = |X|$ i zauważmy, że skoro ciąg $\boldsymbol{g}$ jest nierosnący, to

$$\Big(h(X \cup \{i\}) + h(X \cup \{j\})\Big) - \Big(h(X) + h(X \cup \{i, j\})\Big) =$$
$$= 2h_{t+1} - h_t - h_{t+2} = (h_{t+1} - h_t) - (h_{t+2} - h_{t+1}) = g_t - g_{t+1} \geqslant 0.$$

Pokazaliśmy zatem, że (J_m, h) jest polimatroidem. Ponieważ liczby $(g_t)_{t=0,1,\ldots,m-1}$ są całkowite, więc to samo możemy powiedzieć o liczbach $(h_i)_{i=0,1,\ldots,m}$, a stąd funkcja h ma wyłącznie wartości całkowite. Na koniec, z określenia funkcji h, jeśli $|X| = |Y|$, to $h(X) = h_{|X|} = h_{|Y|} = h(Y)$, więc (J_m, h) jest polimatroidem jednorodnym. □

Z powyższych dwóch stwierdzeń wynika, że istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy rodziną polimatroidów jednorodnych zdefiniowanych na zbiorze J_m i rodziną m-elementowych nierosnących ciągów nieujemnych liczb całkowitych. Zauważmy, że wypowiedzi powyższych stwierdzeń nie zmienią się istotnie, jeśli dodatkowo będziemy przyjmować $g_m := 0$, co znacznie ułatwi nam kolejne wypowiedzi.

Definicja 2.27. Jeśli $\mathcal{Z} = (J_m, h)$ jest polimatroidem jednorodnym, to ciąg $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$, określony jako $g_m = 0$,

$$g_t = h_{t+1} - h_t, \quad t = 0, 1, \ldots, m-1,$$

gdzie $h_i = h(X)$ dla $X \subseteq J_m$, $|X| = i$, nazywamy *ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z}$*.

Jeśli ciąg $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ jest ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$, to uznajemy za zdefiniowane liczby $h_0 = 0$ oraz

$$h_i = \sum_{t=0}^{i-1} g_t \quad \text{dla } i = 1, \ldots, m.$$

Zauważmy, że

- $g_0 = 0 \iff h_1 = \cdots = h_m = 0$;
- $g_1 = 0 \iff h_1 = \cdots = h_m = g_0$.

Stąd, zgodnie z wcześniejszym założeniem, iż rozważamy jedynie polimatroidy $\mathcal{Z}$, których funkcja rangi jest niezerowa, w dalszej części pracy zakładamy, że dla wszystkich ciągów $\boldsymbol{g}$ oraz wszystkich polimatroidów jednorodnych $\mathcal{Z}$ zachodzi $g_0 \neq 0$ lub równoważnie $h_1 \neq 0$.

Wielokrotnie w dalszej części pracy będą wykorzystywane następujące lematy.

Lemat 2.28. *Jeśli $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ jest ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$, to dla dowolnych $i, j \in \{0, 1, \ldots, m\}$, $j < i$, zachodzi równość*

$$h_i - h_j = \sum_{t=j}^{i-1} g_t.$$

Dowód. Wystarczy zauważyć, że

$$h_i - h_j = \sum_{t=0}^{i-1} g_t - \sum_{t=0}^{j-1} g_t = \sum_{t=j}^{i-1} g_t. \qquad \square$$

Przypomnijmy, że zbiór $\mathcal{B}(\mathcal{Z}, X)$ jest określony za pomocą (2.1).

Lemat 2.29. *Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$, niech $X \subseteq J_m$, $k = |X|$ oraz $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$. Wówczas:*

1. *Dla każdego $i \in X$ zachodzi $w_i \geqslant g_{k-1}$.*
2. *Jeśli $w_i = g_{k-1}$ dla pewnego $i \in X$, to $\bar{w} - w_i \bar{e}_i \in \mathcal{B}(\mathcal{Z}, X \setminus \{i\})$.*

Dowód. 1. Zauważmy, że $|\bar{w}_X| = h(X) = h_k$, $|\bar{w}_{X\setminus\{i\}}| \leqslant h(X \setminus \{i\}) = h_{k-1}$, więc

$$w_i = |\bar{w}_X| - |\bar{w}_{X\setminus\{i\}}| \geqslant h_k - h_{k-1} = g_{k-1}.$$

2. Oznaczając $\bar{v} := \bar{w} - w_i \bar{e}_i$ mamy $\operatorname{supp} \bar{v} \subseteq X \setminus \{i\}$ oraz

$$|\bar{v}| = h_k - g_{k-1} = h_{k-1} = h(X \setminus \{i\}). \qquad \square$$

Lemat 2.30. *Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$. Jeśli $g_k = 0$ dla pewnego $1 \leqslant k \leqslant m$ oraz $Y, X \subseteq J_m$ są takimi zbiorami, że $|Y| \geqslant k$ i $Y \subseteq X$, to $\mathcal{B}(\mathcal{Z}, Y) \subseteq \mathcal{B}(\mathcal{Z}, X)$.*

Dowód. Weźmy dowolny wektor $\bar{w} \in \mathcal{B}(\mathcal{Z}, Y)$. Wystarczy pokazać, że $|\bar{w}_X| = h(X)$. Z faktu, że ciąg $\boldsymbol{g}$ jest ciągiem nierosnącym, a jego wyrazy są nieujemne wynika, że $g_k = \ldots = g_m = 0$. Zauważmy, że $\operatorname{supp} \bar{w} \subseteq Y \subseteq X$. Korzystając z założeń oraz lematu 2.28 otrzymujemy:

$$|\bar{w}_X| = |\bar{w}_Y| = h(Y) = h_{|Y|} = h_{|X|} - \sum_{t=|Y|}^{|X|-1} g_t = h_{|X|} = h(X),$$

co kończy dowód. □

Rozważmy teraz zagadnienie kompatybilności rodziny monotonicznej z polimatroidem jednorodnym. Wprowadzamy pewne pojęcia, które będą dogodne w dalszych zastosowaniach.

Definicja 2.31. Dla danej rodziny monotonicznej $\Delta \subsetneq \mathcal{P}(J_m)$ definiujemy zbiory $I_1(\Delta)$, $I_2(\Delta) \subseteq \{0, 1, \ldots, m-1\}$ następująco:

1. $k \in I_1(\Delta)$ wtedy i tylko wtedy, gdy istnieje taki zbiór $X \in \mathcal{P}(J_m) \setminus \Delta$ oraz taki element $i \in J_m$, że $|X| = k$ i $X \cup \{i\} \in \Delta$.
2. $k \in I_2(\Delta)$ wtedy i tylko wtedy, gdy istnieją taki zbiór $X \in \mathcal{P}(J_m) \setminus \Delta$ oraz takie elementy $i, j \in J_m,\ i \neq j$, że $|X| = k$ i $X \cup \{i\} \in \Delta, X \cup \{j\} \in \Delta$.

Definicja 2.32. Niech $\boldsymbol{g} = (g_0, g_1, \ldots, g_{m-1}, g_m)$, $g_m = 0$, będzie nierosnącym ciągiem nieujemnych liczb całkowitych. *Sygnaturą* ciągu $\boldsymbol{g}$ nazywamy taki ciąg zero-jedynkowy $\sigma(\boldsymbol{g}) = (\sigma_0, \sigma_1, \ldots, \sigma_{m-1})$, że

$$\sigma_i := \begin{cases} 1, & \text{gdy } g_i > g_{i+1}, \\ 0, & \text{gdy } g_i = g_{i+1}, \end{cases}$$

dla $i = 0, 1, \ldots, m-1$.

Zauważmy, że jeśli $k \in J_m$ jest największym takim wskaźnikiem, dla którego $\sigma_k = 1$, to $g_0 \geqslant \ldots \geqslant g_k > g_{k+1} = \ldots = g_{m-1} = g_m = 0$. W szczególności

$$\sigma(\boldsymbol{g}) = (0, \ldots, 0, 1) \iff g_0 = g_1 = \cdots = g_{m-1} > 0$$

oraz

$$\sigma(\boldsymbol{g}) = (1, \ldots, 1, 1) \iff g_0 > g_1 > \cdots > g_{m-1} > 0.$$

Twierdzenie 2.33. *Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$ oraz niech $\sigma(\boldsymbol{g}) = (\sigma_0, \sigma_1, \ldots, \sigma_{m-1})$ będzie sygnaturą ciągu $\boldsymbol{g}$. Rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy spełnione są warunki:*

1. *istnieje taka liczba* $l \in J_m$, $l \geqslant \max I_1(\Delta)$, *że* $\sigma_l = 1$.

2. $\sigma_k = 1$ *dla każdego* $k \in I_2(\Delta)$.

Dowód. Rozpocznijmy od implikacji „⇒" i przyjmijmy $n := \max I_1(\Delta)$. Stąd istnieją takie podzbiory $X \subseteq Y \subseteq J_m$, że $X \notin \Delta, Y \in \Delta$ oraz $|X| = n$, $|Y| = n+1$. Zgodnie z warunkiem 1 lematu 2.23 mamy $h_n = h(X) < h(Y) = h_{n+1}$, więc $g_n = h_{n+1} - h_n > 0$. Ponieważ $g_m = 0$, więc istnieje taka liczba naturalna l, że $n \leqslant l < m$ i $g_l > g_{l+1} = 0$, a to oznacza, że $\sigma_l = 1$.

Rozważmy teraz dowolną liczbę $k \in I_2(\Delta)$. Wtedy istnieją taki podzbiór $X \subseteq J_m$ i takie elementy $i, j \in J_m \setminus X$, $i \neq j$, że $|X| = k$, $X \notin \Delta$, $X \cup \{i\}$, $X \cup \{j\} \in \Delta$. Zgodnie z warunkiem 2 lematu 2.23 otrzymujemy

$$h(X) + h(X \cup \{i, j\}) < h(X \cup \{i\}) + h(X \cup \{j\}).$$

Stąd $h_k + h_{k+2} < 2h_{k+1}$. Następnie, po oczywistych przekształceniach otrzymujemy $g_{k+1} = h_{k+2} - h_{k+1} < h_{k+1} - h_k = g_k$, a stąd $\sigma_k = 1$.

Dla dowodu implikacji „⇐", załóżmy, że spełnione są warunki 1 i 2 tego twierdzenia. Z faktu, że $\sigma_l = 1$ dla pewnego $l \geqslant \max I_1(\Delta)$ wynika, iż $g_n > 0$ dla każdego $n \leqslant l$, więc $h(X) < h(Y)$ dla wszystkich $X \subseteq Y \subseteq J_m$, $|Y| - 1 = |X| = n$. Zauważmy, że jeśli $X \notin \Delta$, to $|X| \leqslant l$, więc w szczególności spełniony jest warunek 1 lematu 2.23.

Aby udowodnić warunek 2 lematu 2.23, rozważmy taki podzbiór $X \subseteq J_m$ oraz elementy $i, j \in J_m \setminus X$, że $i \neq j$, $X \notin \Delta$, $X \cup \{i\}, X \cup \{j\} \in \Delta$. To oznacza, że $|X| =: n \in I_2(\Delta)$, więc zgodnie z warunkiem 2 naszego twierdzenia $\sigma_n = 1$. Stąd

$$\Big(h(X) + h(X \cup \{i, j\})\Big) - \Big(h(X \cup \{i\}) + h(X \cup \{j\})\Big) =$$
$$= (h_n + h_{n+2}) - 2h_{n+1} = (h_{n+2} - h_{n+1}) - (h_{n+1} - h_n) = g_{n+1} - g_n < 0,$$

co kończy dowód. □

Wniosek 2.34. *Niech* $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ *oraz* $\tilde{\boldsymbol{g}} = (\tilde{g}_t)_{t=0,1,\ldots,m}$ *będą ciągami wyznaczonymi odpowiednio przez polimatroidy jednorodne* $\mathcal{Z} = (J_m, h)$ *oraz* $\tilde{\mathcal{Z}} = (J_m, \tilde{h})$. *Jeśli sygnatury ciągów* $\boldsymbol{g}$ *oraz* $\tilde{\boldsymbol{g}}$ *są równe, to rodzina monotoniczna* $\Delta \subsetneq \mathcal{P}(J_m)$ *jest kompatybilna z polimatroidem* $\mathcal{Z}$ *wtedy i tylko wtedy, gdy* Δ *jest kompatybilna z polimatroidem* $\tilde{\mathcal{Z}}$.

Dowód. Wniosek wynika bezpośrednio z twierdzenia 2.33. □

Powyższy wniosek pokazuje, że kompatybilność rodziny monotonicznej z polimatroidem jednorodnym nie zależy bezpośrednio od wartości jego funkcji rangi, ani od wartości wyrazów ciągu $\boldsymbol{g}$ wyznaczonego przez ten polimatroid, ale od rozmieszczenia tych indeksów, dla których wyrazy ciągu $\boldsymbol{g}$ zmieniają swoją wartość. Dlatego, do zbadania kompatybilności rodziny monotonicznej z polimatroidem wyznaczającym ciąg $\boldsymbol{g}$, można użyć polimatroidu wyznaczającego ciąg

$\tilde{\boldsymbol{g}} = (\tilde{g}_t)_{t=0,1,\ldots,m}$, którego wyrazy otrzymujemy z sygnatury $\sigma(\boldsymbol{g}) = (\sigma_0, \ldots, \sigma_{m-1})$ za pomocą wzoru:

$$\tilde{g}_t = \sum_{i=t}^{m-1} \sigma_t, \quad t \in \{0, \ldots, m-1\}.$$

Teraz zaprezentujemy kilka lematów, które będą wykorzystywane w dalszych rozdziałach pracy.

Lemat 2.35. *Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$. Jeśli $g_k = 0$ dla pewnego $1 \leqslant k \leqslant m$ oraz rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$, to wszystkie podzbiory zbioru J_m, które mają co najmniej k elementów, należą do Δ.*

Dowód. Przypuśćmy nie wprost, że pewien zbiór $Y \subseteq J_m$, $|Y| \geqslant k$, nie należy do rodziny Δ. Weźmy zatem taki zbiór X, że $Y \subseteq X$ i $X \in \Delta$. Taki zbiór X na pewno istnieje, jest nim na przykład J_m. Wówczas, na podstawie lematu Csirmaza (2.21) oraz lematu 2.28, otrzymujemy kolejno

$$h(Y) < h(X) \implies 0 < h(X) - h(Y) = h_{|X|} - h_{|Y|} = \sum_{t=|Y|}^{|X|-1} g_t \leqslant \sum_{t=k}^{|X|-1} g_t.$$

Z założenia $g_k = 0$, więc z monotoniczności ciągu $\boldsymbol{g}$ wynika, iż w ostatniej sumie wszystkie składniki są równe 0. Mamy zatem $0 < 0$, co jest sprzecznością. □

Przypomnijmy, że $\min \Delta$ oznacza rodzinę minimalnych zbiorów należących do rodziny monotonicznej Δ, a $\mathcal{P}_k(A)$ jest rodziną wszystkich podzbiorów k-elementowych zbioru A.

Lemat 2.36. *Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie takim ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$, że $g_{k-1} > g_k = 0$ dla pewnego $1 \leqslant k \leqslant m$, oraz niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie rodziną monotoniczną. Wówczas:*

1. *Jeśli $\mathcal{P}_k(J_m) \subseteq \Delta$, to dla takich zbiorów $Y \subseteq W \subseteq J_m$, że $Y \notin \Delta$ i $W \in \Delta$ mamy $h(Y) < h(W)$.*
2. *Jeśli $\mathcal{P}_k(J_m) \subseteq \Delta$ oraz $g_0 > g_1 > \cdots > g_{k-1} > g_k = \cdots = g_{m-1} = g_m = 0$, to rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.*
3. *Jeśli $\min \Delta = \{X\}$ dla pewnego $X \subseteq J_m$ oraz $k = m$, to rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.*

Dowód. 1. Weźmy takie zbiory $Y \subseteq W \subseteq J_m$, że $Y \notin \Delta$ i $W \in \Delta$. Oczywiście $|Y| < |W|$, więc z lematu 2.28 otrzymujemy

$$h(W) - h(Y) = h_{|W|} - h_{|Y|} = \sum_{t=|Y|}^{|W|-1} g_t.$$

Przypuśćmy, że powyższa suma jest równa 0. Wówczas suma ta ma wszystkie składniki równe $0 = g_{|Y|} = \cdots = g_{|W|-1}$, a zatem z założeń mamy $k \leqslant |Y|$. Ponieważ wszystkie podzbiory k-elementowe zbioru J_m należą do Δ, więc $Y \in \Delta$. W ten sposób otrzymaliśmy sprzeczność.

2. Zauważmy, że $\sigma(\boldsymbol{g}) = (\underbrace{1,\ldots,1}_{k},\underbrace{0,\ldots,0}_{m-k})$. Z założenia, iż wszystkie zbiory k-elementowe należą do Δ wynika, że $I_1(\Delta), I_2(\Delta) \subseteq \{0,1,\ldots,k-1\}$. Zatem warunek 1 twierdzenia 2.33 jest spełniony, skoro $\max I_1(\Delta) \leqslant k-1$ i $\sigma_{k-1} = 1$. Również warunek 2 tego twierdzenia jest spełniony, ponieważ $\sigma_i = 1$ dla każdego $i \in \{0,1,\ldots,k-1\}$.

3. Pokażemy, że spełnione są warunki lematu Csirmaza (2.21). Pierwszy warunek wynika z punktu 1 tego lematu, gdyż dla $k = m$ mamy $\mathcal{P}_k(J_m) = \{J_m\} \subseteq \Delta$, ponieważ J_m jest jedynym swoim m-elementowym podzbiorem oraz należy do dowolnej niepustej rodziny monotonicznej. Zauważmy, że jeśli $\min \Delta = \{X\}$ oraz $W, Y \in \Delta$, to $X \subseteq W$ oraz $X \subseteq Y$, skąd $X \subseteq W \cap Y$. Zatem warunek drugi lematu Csirmaza (2.21) jest spełniony pusto. □

Wniosek 2.37. *Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$. Jeśli $g_0 > g_1 > \cdots > g_{m-1} > g_m = 0$, to każda rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$.*

Dowód. Wystarczy zauważyć, że jedynym podzbiorem m-elementowym zbioru J_m jest on sam. Ponadto J_m należy do każdej niepustej rodziny monotonicznej Δ, stąd oraz lematu 2.36 (2) otrzymujemy wniosek. □

Na zakończenie tego podrozdziału wprowadzimy pojęcie wektora wierzchołkowego.

Definicja 2.38. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$. Jeśli $g_{k-1} > 0$, to każdy wektor, który powstaje z wektora

$$\sum_{i=0}^{k-1} g_i \bar{e}_i = (g_0, g_1, \ldots, g_{k-1}, \underbrace{0,\ldots,0}_{m-k})$$

przez dowolną permutację jego współrzędnych nazywamy *wektorem wierzchołkowym rzędu k*.

Zauważmy, że jeśli $g_{k-1} > 0$, to dowolny wektor wierzchołkowy rzędu k ma dokładnie k niezerowych współrzędnych o wartościach: $g_0, g_1, \ldots, g_{k-1}$. Nazwa wektorów wierzchołkowych nie jest przypadkowa, są to bowiem wierzchołki wielościanu $\mathcal{D}(\mathcal{Z})$.

Lemat 2.39. *Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid jednorodny $\mathcal{Z} = (J_m, h)$. Wówczas dla każdego wektora wierzchołkowego $\bar{w}$ mamy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$.*

Dowód. Niech $\bar{w}$ będzie dowolnym wektorem wierzchołkowym rzędu k. Oczywiście $|\operatorname{supp}\bar{w}| = k$. Weźmy dowolny podzbiór $Y \subseteq \operatorname{supp}\bar{w}$ i niech $|Y| =: l \leqslant k$. Wówczas, korzystając z tego, że ciąg $\boldsymbol{g}$ jest nierosnący oraz z lematu 2.28 otrzymujemy:

$$|\bar{w}_Y| \leqslant \sum_{i=0}^{l-1} g_i = h_l = h(Y).$$

Ponadto zauważmy, że jeśli $Y = \operatorname{supp}\bar{w}$, to $|Y| = k$ oraz w powyższej nierówności otrzymamy $|\bar{w}_{\operatorname{supp}\bar{w}}| = \sum_{i=0}^{k-1} g_i = h_k$. Stąd $|\bar{w}_{\operatorname{supp}\bar{w}}| = h(\operatorname{supp}\bar{w})$, co ostatecznie dowodzi, że $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{w})$. □

2.2.2 Jednorodne polimatroidy boolowskie

Jednorodne polimatroidy boolowskie będą odgrywać pewną rolę w naszych badaniach, o czym przekonamy się w podrozdziale 4.5. Ten podrozdział rozpoczniemy od definicji polimatroidu boolowskiego, a zakończymy warunkiem koniecznym i wystarczającym na to, aby polimatroid jednorodny był boolowski.

Definicja 2.40. Polimatroid całkowity $\mathcal{Z} = (J_m, h)$ nazywamy polimatroidem *boolowskim*, jeśli istnieje taka rodzina $\{B_i\}_{i\in J_m}$ zbiorów skończonych, że

$$h(X) = \left|\bigcup_{i\in X} B_i\right|$$

dla każdego $X \subseteq J_m$. Rodzinę $\{B_i\}_{i\in J_m}$ nazywamy *reprezentacją boolowską* polimatroidu $\mathcal{Z}$. Przyjmujemy oznaczenie $B := \bigcup_{i=1}^{m} B_i$.

Stwierdzenie 2.41. *Jeśli polimatroid całkowity $\mathcal{Z} = (J_m, h)$ jest polimatroidem boolowskim, to jest reprezentowalny nad każdym ciałem skończonym.*

Dowód. Niech $\{B_i\}_{i\in J_m}$ będzie reprezentacją boolowską polimatroidu $\mathcal{Z} = (J_m, h)$. Dalej, niech $\mathbb{F}$ będzie dowolnym ciałem skończonym. Przyjmijmy $r := |B|$. Bez straty ogólności możemy założyć, że B jest bazą przestrzeni liniowej $V := \mathbb{F}^r$. Wówczas, dla każdego $i \in J_m$, możemy zdefiniować podprzestrzeń liniową V_i przestrzeni V jako $V_i := \operatorname{lin}\{B_i\}$, czyli podprzestrzeń rozpiętą na takich wektorach bazy B, które należą do zbioru B_i. Oczywiście

$$h(X) = \dim(\operatorname{lin}\{\bigcup_{i\in X} B_i\}) = \dim\Big(\sum_{i\in X} V_i\Big),$$

dla każdego niepustego $X \subseteq J_m$. □

Niech rodzina $\{B_i\}_{i\in J_m}$ będzie rodziną zbiorów skończonych. Rozważmy funkcję $\Psi\colon B \to \mathcal{P}(J_m)$ zdefiniowaną wzorem $\Psi(x) := \{i \in J_m : x \in B_i\}$. Za pomocą tej funkcji definiujemy (parami rozłączne) zbiory

$$W_A := \{x \in B : \Psi(x) = A\} \quad \text{dla } A \in \mathcal{P}(J_m). \tag{2.2}$$

Zauważmy, że dla $A \in \mathcal{P}(J_m)$ oraz $x \in B$:

$$A = \Psi(x) \iff x \in W_A.$$

Oznaczmy $w_A := |W_A|$ dla $A \in \mathcal{P}(J_m)$ oraz $w_k^{\#} := \sum_{A \in \mathcal{P}_k(J_m)} w_A$.

Lemat 2.42. *Niech $\{B_i\}_{i \in J_m}$ będzie rodziną zbiorów skończonych. Wówczas dla dowolnego $I \subseteq J_m$ mamy*

$$\bigcup_{i \in I} B_i = \bigcup_{\substack{A \in \mathcal{P}(J_m) \\ A \cap I \neq \emptyset}} W_A.$$

Dowód. Niech $b \in \bigcup_{i \in I} B_i$, czyli $b \in B_k$ dla pewnego $k \in I$. Stąd $k \in \Psi(b) =: C$, więc $b \in W_C$. Ponieważ $k \in I \cap C$, więc $I \cap C \neq \emptyset$, skąd ostatecznie

$$b \in W_C \subseteq \bigcup_{\substack{A \in \mathcal{P}(J_m) \\ A \cap I \neq \emptyset}} W_A.$$

Niech teraz $b \in \bigcup_{A \in \mathcal{P}(J_m),\ A \cap I \neq \emptyset} W_A$. Zatem $b \in W_A$ dla pewnego $A \in \mathcal{P}(J_m)$, $A \cap I \neq \emptyset$. Stąd $\Psi(b) = A$, więc $b \in B_i$ dla każdego $i \in A$. Biorąc $k \in A \cap I$, otrzymujemy

$$b \in B_k \subseteq \bigcup_{i \in I} B_i. \qquad \square$$

Lemat 2.43. *Niech rodzina $\{B_i\}_{i \in J_m}$ będzie reprezentacją boolowską polimatroidu $\mathcal{Z} = (J_m, h)$. Jeśli polimatroid $\mathcal{Z}$ jest jednorodny, to istnieją takie liczby w_t, $t \in J_m$, że $w_C = w_t$ dla każdego t-elementowego zbioru $C \in \mathcal{P}(J_m)$. W szczególności $|C| = |C'| \Longrightarrow w_C = w_{C'}$ dla wszystkich $C, C' \in \mathcal{P}(J_m)$.*

Dowód. Zastosujemy indukcję względem t. Niech $t = 1$. Ustalmy $k \in J_m$ oraz niech $I := J_m \setminus \{k\}$. W tym przypadku każdy zbiór jednoelementowy, który nie jest rozłączny z I, jest zawarty w I, natomiast każdy zbiór, który ma co najmniej dwa elementy, ma niepusty przekrój z I. Stąd i z lematu 2.42 mamy

$$h_{m-1} = h(I) = \Big|\bigcup_{i \in I} B_i\Big| = \Big|\bigcup_{\substack{A \in \mathcal{P}(J_m) \\ A \cap I \neq \emptyset}} W_A\Big| = \sum_{\substack{A \in \mathcal{P}_1(J_m) \\ I \cap A \neq \emptyset}} w_A + \sum_{l=2}^{m} \sum_{\substack{A \in \mathcal{P}_l(J_m) \\ I \cap A \neq \emptyset}} w_A =$$

$$= w_1^{\#} - w_{\{k\}} + \sum_{l=2}^{m} w_l^{\#} = \sum_{l=1}^{m} w_l^{\#} - w_{\{k\}}.$$

Zatem przyjmując

$$w_1 := \sum_{l=1}^{m} w_l^{\#} - h_{m-1},$$

otrzymujemy $w_{\{k\}} = w_1$ dla każdego $k \in J_m$.

Załóżmy, że $1 < t \leqslant m$ i dla $1 \leqslant r < t$ zdefiniowaliśmy już takie liczby w_r, że $w_C = w_r$, gdy $C \in \mathcal{P}(J_m)$, $|C| = r$. Ustalmy zbiór $C \in \mathcal{P}(J_m)$, $|C| = t$ oraz

niech $I := J_m \setminus C$. Zauważmy, że każdy zbiór rozłączny z I jest zawarty w C, zaś każdy zbiór, który ma więcej niż t elementów, kroi się niepusto z I. Ponownie korzystając z lematu 2.42 oraz z założenia indukcyjnego otrzymujemy

$$\begin{aligned} h_{m-t} = h(I) &= \Big|\bigcup_{i\in I} B_i\Big| = \Big|\bigcup_{\substack{A\in\mathcal{P}(J_m)\\ A\cap I\neq\emptyset}} W_A\Big| = \\ &= \sum_{l=1}^{t-1} \sum_{\substack{A\in\mathcal{P}_l(J_m)\\ I\cap A\neq\emptyset}} w_A + \sum_{\substack{A\in\mathcal{P}_t(J_m)\\ I\cap A\neq\emptyset}} w_A + \sum_{l=t+1}^{m} \sum_{\substack{A\in\mathcal{P}_l(J_m)\\ I\cap A\neq\emptyset}} w_A = \\ &= \sum_{l=1}^{t-1} \left(w_l^{\#} - \binom{t}{l} w_l \right) + w_t^{\#} - w_C + \sum_{l=t+1}^{m} w_l^{\#} = \\ &= \sum_{l=1}^{m} w_l^{\#} - \sum_{l=1}^{t-1} \binom{t}{l} w_l - w_C. \end{aligned}$$

Zatem przyjmując

$$w_t := \sum_{l=1}^{m} w_l^{\#} - \sum_{l=1}^{t-1} \binom{t}{l} w_l - h_{m-t},$$

otrzymujemy $w_C = w_t$ dla dowolnych $C \in \mathcal{P}(J_m)$, $|C| = t$, co kończy krok indukcyjny. □

W dalszej części pracy liczby w_t, $t \in J_m$, oznaczają liczby opisane w powyższym lemacie.

Wniosek 2.44. *Niech rodzina $\{B_i\}_{i\in J_m}$ będzie reprezentacją boolowską polimatroidu $\mathcal{Z} = (J_m, h)$. Jeśli polimatroid $\mathcal{Z}$ jest jednorodny, to $w_k^{\#} = \binom{m}{k} w_k$ dla każdego $k \in J_m$.*

Dowód. Wniosek wynika bezpośrednio z lematu 2.43. □

Wniosek 2.45. *Niech rodzina $\{B_i\}_{i\in J_m}$ będzie reprezentacją boolowską polimatroidu $\mathcal{Z} = (J_m, h)$. Jeśli polimatroid $\mathcal{Z}$ jest jednorodny, to*

$$h_m = \sum_{l=1}^{m} \binom{m}{l} w_l \qquad \textit{oraz} \qquad h_t = h_m - \sum_{l=1}^{m-t} \binom{m-t}{l} w_l$$

dla $t = 1, 2, \ldots, m-1$.

Dowód. Stosując lematy 2.42, 2.43 oraz wniosek 2.44 otrzymujemy

$$h_m = h(J_m) = \Big|\bigcup_{i\in J_m} B_i\Big| = \Big|\bigcup_{A\in\mathcal{P}(J_m)} W_A\Big| = \sum_{A\in\mathcal{P}(J_m)} w_A = \sum_{l=1}^{m} w_l^{\#} = \sum_{l=1}^{m} \binom{m}{l} w_l.$$

Niech teraz $t < m$ oraz $I \subseteq J_m$, $|I| = t$. Wówczas

$$h_t = h(I) = \Big|\bigcup_{i\in I} B_i\Big| = \Big|\bigcup_{\substack{A\in\mathcal{P}(J_m)\\ A\cap I\neq\emptyset}} W_A\Big| = \sum_{l=1}^{m-t}\sum_{\substack{A\in\mathcal{P}_l(J_m)\\ I\cap A\neq\emptyset}} w_A + \sum_{l=m-t+1}^{m}\sum_{\substack{A\in\mathcal{P}_l(J_m)\\ I\cap A\neq\emptyset}} w_A =$$
$$= \sum_{l=1}^{m-t}\left(w_l^{\#} - \binom{m-t}{l} w_l\right) + \sum_{l=m-t+1}^{m} w_l^{\#} = \sum_{l=1}^{m} w_l^{\#} - \sum_{l=1}^{m-t}\binom{m-t}{l} w_l =$$
$$= h_m - \sum_{l=1}^{m-t}\binom{m-t}{l} w_l. \qquad \square$$

Lemat 2.46. *Niech rodzina $\{B_i\}_{i\in J_m}$ będzie reprezentacją boolowską polimatroidu $\mathcal{Z} = (J_m, h)$. Jeśli $\mathcal{Z}$ jest polimatroidem jednorodnym i wyznacza ciąg $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$, to*

$$g_t = \sum_{l=1}^{m-t}\binom{m-t-1}{l-1} w_l$$

dla $t = 0, 1, \ldots, m-1$.

Dowód. W dowodzie korzystamy ze znanej tożsamości

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Dla $t = 0$ otrzymujemy

$$g_0 = h_1 = h_m - \sum_{l=1}^{m-1}\binom{m-1}{l} w_l = \sum_{l=1}^{m}\binom{m}{l} w_l - \sum_{l=1}^{m-1}\binom{m-1}{l} w_l =$$
$$= w_m + \sum_{l=1}^{m-1}\left(\binom{m}{l} - \binom{m-1}{l}\right) w_l = \sum_{l=1}^{m-1}\binom{m-1}{l-1} w_l + w_m =$$
$$= \sum_{l=1}^{m}\binom{m-1}{l-1} w_l.$$

Gdy $t > 0$, to z wniosku 2.45 otrzymujemy

$$g_t = h_{t+1} - h_t =$$
$$= \left(h_m - \sum_{l=1}^{m-(t+1)}\binom{m-(t+1)}{l} w_l\right) - \left(h_m - \sum_{l=1}^{m-t}\binom{m-t}{l} w_l\right) =$$
$$= \sum_{l=1}^{m-t}\binom{m-t}{l} w_l - \sum_{l=1}^{m-t-1}\binom{m-t-1}{l} w_l =$$
$$= w_{m-t} + \sum_{l=1}^{m-t-1}\binom{m-t}{l} w_l - \sum_{l=1}^{m-t-1}\binom{m-t-1}{l} w_l =$$
$$= \sum_{l=1}^{m-t-1}\binom{m-t-1}{l-1} w_l + w_{m-t} = \sum_{l=1}^{m-t}\binom{m-t-1}{l-1} w_l. \qquad \square$$

Wniosek 2.47. *Niech rodzina* $\{B_i\}_{i\in J_m}$ *będzie reprezentacją boolowską polimatroidu* $\mathcal{Z} = (J_m, h)$. *Jeśli* $\mathcal{Z}$ *jest polimatroidem jednorodnym i wyznacza ciąg* $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$, *to*

$$\bar{\boldsymbol{g}} = \boldsymbol{F}\mathbf{w}, \tag{2.3}$$

gdzie wektory $\bar{\boldsymbol{g}} = [g_{m-1}, g_{m-2}, \ldots, g_1, g_0]^T$, $\mathbf{w} = [w_1, w_2, \ldots, w_{m-1}, w_m]^T$ *oraz macierz* $\boldsymbol{F} = \left[\binom{i-1}{j-1}\right]_{j=1,\ldots,m}^{i=1,\ldots,m}$.

Dowód. Wniosek wynika bezpośrednio z lematu 2.46. □

Wniosek 2.48. *Niech rodzina* $\{B_i\}_{i\in J_m}$ *będzie reprezentacją boolowską polimatroidu* $\mathcal{Z} = (J_m, h)$. *Jeśli* $\mathcal{Z}$ *jest polimatroidem jednorodnym i wyznacza ciąg* $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$, *to*

$$\mathbf{w} = \boldsymbol{F}^{-1}\bar{\boldsymbol{g}}, \tag{2.4}$$

gdzie wektory $\bar{\boldsymbol{g}} = [g_{m-1}, g_{m-2}, \ldots, g_1, g_0]^T$, $\mathbf{w} = [w_1, w_2, \ldots, w_{m-1}, w_m]^T$ *oraz macierz* $\boldsymbol{F}^{-1} = \left[(-1)^{i+j}\binom{i-1}{j-1}\right]_{j=1,\ldots,m}^{i=1,\ldots,m}$.

Dowód. Bezpośrednim, choć żmudnym rachunkiem można sprawdzić, że jeśli $\mathbf{F} = \left[\binom{i-1}{j-1}\right]_{j=1,\ldots,m}^{i=1,\ldots,m}$, to $\mathbf{F}^{-1} = \left[(-1)^{i+j}\binom{i-1}{j-1}\right]_{j=1,\ldots,m}^{i=1,\ldots,m}$. □

Zauważmy, że równości (2.3) oraz (2.4) z powyższych wniosków można zapisać następująco:

$$\begin{bmatrix} g_{m-1} \\ g_{m-2} \\ \vdots \\ g_1 \\ g_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 \\ 1 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & m-2 & \ldots & 1 & 0 \\ 1 & m-1 & \ldots & m-1 & 1 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_{m-1} \\ w_m \end{bmatrix}$$

oraz

$$\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_{m-1} \\ w_m \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 \\ -1 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (-1)^m & (-1)^{m+1}(m-2) & \ldots & 1 & 0 \\ (-1)^{m+1} & (-1)^{m+2}(m-1) & \ldots & -(m-1) & 1 \end{bmatrix} \begin{bmatrix} g_{m-1} \\ g_{m-2} \\ \vdots \\ g_1 \\ g_0 \end{bmatrix}.$$

Teraz przystępujemy do podania warunku koniecznego i wystarczającego na to, aby polimatroid jednorodny był polimatroidem boolowskim.

Twierdzenie 2.49. *Niech polimatroid* $\mathcal{Z} = (J_m, h)$ *będzie polimatroidem jednorodnym wyznaczającym ciąg* $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$. *Polimatroid* $\mathcal{Z}$ *jest polimatroidem boolowskim wtedy i tylko wtedy, gdy dla każdego* $t = 1, \ldots, m$ *zachodzi*

$$\sum_{l=1}^{t}(-1)^{l+t}\binom{t-1}{l-1}g_{m-l} \geqslant 0 \tag{2.5}$$

Dowód. Jeśli $\mathcal{Z}$ jest polimatroidem boolowskim, to istnieje rodzina zbiorów, która jest reprezentacją boolowską tego polimatroidu. Reprezentacja ta zgodnie ze wzorem (2.2) wyznacza rodzinę zbiorów $\{W_A : A \in \mathcal{P}(J_m)\}$. Stąd i z wniosku 2.48 mamy

$$\sum_{l=1}^{t}(-1)^{l+t}\binom{t-1}{l-1}g_{m-l} = w_t = |W_A| \geqslant 0$$

dla wszystkich $t = 1, \ldots, m$ i $A \in \mathcal{P}_t(J_m)$.

Dla dowodu odwrotnej implikacji załóżmy, że nierówności (2.5) są spełnione, to znaczy liczby $\tilde{w}_t := \sum_{l=1}^{t}(-1)^{l+t}\binom{t-1}{l-1}g_{m-l}$, $t = 1, \ldots, m$, są nieujemne. Niech X będzie wystarczająco dużym zbiorem skończonym. Dalej, niech $\mathcal{W} := \{W_A : A \in \mathcal{P}(J_m)\}$ będzie taką rodziną parami rozłącznych podzbiorów zbioru X, że $|W_A| = \tilde{w}_t$, gdy $|A| = t$. Dla każdego $i \in J_m$ tworzymy zbiór $B_i = \bigcup_{A\in\mathcal{P}(J_m), i\in A} W_A$.

Aby pokazać, że zbiory $B_1, \ldots, B_m$ są reprezentacją boolowską polimatroidu $\mathcal{Z}$, ponownie rozważmy funkcję $\Psi : \bigcup_{i\in J_m} B_i \longrightarrow \mathcal{P}(J_m)$ zdefiniowaną wzorem $\Psi(x) = \{i \in J_m \ : \ x \in B_i\}$. Załóżmy, że $x \in W_A$. Zauważmy, że ze względu na rozłączność zbiorów w rodzinie $\mathcal{W}$ element x należy do B_i wtedy i tylko wtedy, gdy $W_A \subseteq B_i$, a to ma miejsce wtedy i tylko wtedy, gdy $i \in A$. Stąd wynika, że $\Psi(x) = A$. W ten sposób pokazaliśmy, że $W_A = \{x \in B : \Psi(x) = A\}$.

Weźmy zbiór $I \subseteq J_m$, $|I| =: t > 0$. Pokażemy, że $|\bigcup_{i\in I} B_i| = h(I) = h_t$. Korzystając z lematu 2.42 otrzymujemy:

$$\begin{aligned}\Big|\bigcup_{i\in I} B_i\Big| = \Big|\bigcup_{\substack{A\in\mathcal{P}(J_m)\\ A\cap I\neq\emptyset}} W_A\Big| &= \sum_{l=1}^{m-t}\sum_{\substack{A\in\mathcal{P}_l(J_m)\\ I\cap A\neq\emptyset}}\tilde{w}_A + \sum_{l=m-t+1}^{m}\sum_{\substack{A\in\mathcal{P}_l(J_m)\\ I\cap A\neq\emptyset}}\tilde{w}_A = \\ &= \sum_{l=1}^{m-t}\left(\binom{m}{l} - \binom{m-t}{l}\right)\tilde{w}_l + \sum_{l=m-t+1}^{m}\binom{m}{l}\tilde{w}_l = \\ &= \sum_{l=1}^{m}\binom{m}{l}\tilde{w}_l - \sum_{l=1}^{m-t}\binom{m-t}{l}\tilde{w}_l.\end{aligned}$$

Korzystając z tożsamości

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

prawdziwej dla $i \geqslant 1$ oraz $k \geqslant i$, zauważmy, że dla $k = 1, \ldots, m$ mamy

$$\begin{aligned}\sum_{l=1}^{k}\binom{k}{l}\tilde{w}_l &= \sum_{l=1}^{k}\binom{k}{l}\sum_{i=1}^{l}(-1)^{i+l}\binom{l-1}{i-1}g_{m-i} = \\ &= \sum_{i=1}^{k} g_{m-i}\sum_{l=i}^{k}(-1)^{i+l}\binom{k}{l}\binom{l-1}{i-1} = \sum_{i=1}^{k} g_{m-i}.\end{aligned}$$

Zatem kontynuując wcześniejszy rachunek otrzymujemy

$$\Big|\bigcup_{i\in I} B_i\Big| = \sum_{l=1}^{m}\binom{m}{l}\tilde{w}_l - \sum_{l=1}^{m-t}\binom{m-t}{l}\tilde{w}_l = \sum_{i=1}^{m} g_{m-i} - \sum_{i=1}^{m-t} g_{m-i} =$$
$$= \sum_{i=m-t+1}^{m} g_{m-i} = \sum_{i=0}^{t-1} g_i = h_t,$$

gdzie ostatnia równość wynika z lematu 2.28.

Jeśli $t = 0$, to oczywiście $\left|\bigcup_{i\in I} B_i\right| = 0 = h_t = h(I)$. □

Przykład 2.50. Rozważmy polimatroid jednorodny $\mathcal{Z} = (J_3, h)$, który wyznacza ciąg $\boldsymbol{g} = (g_0, g_1, g_2, g_3)$, $g_3 = 0$. Z wniosku 2.48 wiemy, że następująca zależność definiuje liczby w_1, w_2, w_3:

$$\begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -2 & 1 \end{bmatrix} \begin{bmatrix} g_2 \\ g_1 \\ g_0 \end{bmatrix}$$

Zgodnie z twierdzeniem 2.49 polimatroid (J_3, h) ma reprezentację boolowską wtedy i tylko wtedy, gdy $g_2 \geqslant 0$, $-g_2 + g_1 \geqslant 0$ oraz $g_2 - 2g_1 + g_0 \geqslant 0$. Pierwsze dwie nierówności są spełnione dla każdego polimatroidu jednorodnego. Dlatego w tym przypadku polimatroid jednorodny jest boolowski wtedy i tylko wtedy, gdy $\frac{g_0+g_2}{2} \geqslant g_1$.

Przykład 2.51. Rozważmy polimatroid jednorodny $\mathcal{Z} = (J_4, h)$, który wyznacza ciąg $\boldsymbol{g} = (g_0, g_1, g_2, g_3, g_4)$, $g_4 = 0$. Z wniosku 2.48 wiemy, że następująca zależność definiuje liczby w_1, w_2, w_3, w_4:

$$\begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 1 & -2 & 1 & 0 \\ -1 & 3 & -3 & 1 \end{bmatrix} \begin{bmatrix} g_3 \\ g_2 \\ g_1 \\ g_0 \end{bmatrix}$$

Zgodnie z twierdzeniem 2.49 polimatroid (J_4, h) ma reprezentację boolowską wtedy i tylko wtedy, gdy $g_3 \geqslant 0$, $-g_3 + g_2 \geqslant 0$, $g_3 - 2g_2 + g_1 \geqslant 0$ oraz $-g_3 + 3g_2 - 3g_1 + g_0 \geqslant 0$. Pierwsze dwie nierówności są spełnione dla każdego polimatroidu jednorodnego. Dlatego w tym przypadku polimatroid jednorodny jest boolowski wtedy i tylko wtedy, gdy $\frac{g_1+g_3}{2} \geqslant g_2$ oraz $\frac{g_0-g_3}{3} \geqslant g_1 - g_2$.

2.3 Schematy podziału sekretu i matroidy

Rozdział ten zakończymy krótkim omówieniem związków, jakie łączą matroidy i polimatroidy ze schematami podziału sekretu. Przypomnijmy, że $\mathbf{D}(\mathbf{M})$ oznacza rodzinę wszystkich zbiorów zależnych schematu podziału sekretu $\mathbf{M}$. Rozpocznijmy od następującej definicji.

Definicja 2.52. Jeśli $\mathbf{M}$ jest schematem podziału sekretu w zbiorze uczestników P i istnieje taki matroid zdefiniowany na zbiorze $P' = P \cup \{p_0\}$, że $\mathbf{D}(\mathbf{M}) \subseteq \mathcal{P}(P')$ jest rodziną jego wszystkich zbiorów zależnych, to matroid ten nazywamy *matroidem stowarzyszonym ze schematem* $\mathbf{M}$ i oznaczamy $\mathfrak{M}(\mathbf{M})$.

Związek pomiędzy schematami podziału sekretu i matroidami został dostrzeżony przez Brickella i Davenporta i jest zaprezentowany w poniższych twierdzeniach.

Twierdzenie 2.53 (Brickell, Davenport [5, Theorem 1])**.** *Dla każdego spójnego i idealnego schematu podziału sekretu istnieje spójny matroid z nim stowarzyszony.*

Zauważmy, że jeśli $\mathbf{M}$ jest spójnym i idealnym schematem podziału sekretu, to stowarzyszony z nim matroid jest wyznaczony jednoznacznie. Jest to uzasadnione tym, że wskazując rodzinę $\mathbf{D}(\mathbf{M}) \subseteq \mathcal{P}(P')$ jako rodzinę wszystkich zbiorów zależnych matroidu zdefiniowanego na zbiorze $P' = P \cup \{p_0\}$, jednoznacznie go określamy.

Twierdzenie 2.54 (Brickell, Davenport [5, Theorem 2])**.** *Niech $\mathcal{M} = (E, r)$ będzie spójnym matroidem reprezentowalnym nad ciałem $\mathbb{F}$ oraz niech $e_0 \in E$. Wówczas istnieje taki spójny i idealny schemat podziału sekretu $\boldsymbol{M}$, że $P' = E$, $p_0 = e_0$, $S = \mathbb{F}$ oraz $\mathcal{M} = \mathfrak{M}(\boldsymbol{M})$ jest matroidem z nim stowarzyszonym.*

Zauważmy, że jeśli ustalimy spójny matroid $\mathcal{M} = (E, r)$ reprezentowalny nad ciałem $\mathbb{F}$ i zastosujemy powyższe twierdzenie, możemy uzyskać różne schematy podziału sekretu $\mathbf{M}$, w zależności od wyboru $e_0 \in E$.

Powyższe dwa twierdzenia mają swoje odpowiednie wersje wykorzystujące pojęcie portu matroidu i brzmią następująco.

Twierdzenie 2.55 (Farràs, Martí-Farré, Padró [9, Theorem 2.1])**.** *Jeśli $\Gamma \subsetneq \mathcal{P}(P)$ jest spójną i idealną strukturą dostępu, to istnieje taki spójny matroid zdefiniowany na zbiorze P', że Γ jest jego portem w punkcie p_0.*

Twierdzenie 2.56 (Farràs, Martí-Farré, Padró [9, Theorem 2.1])**.** *Niech matroid $\mathcal{M} = (E, r)$ będzie spójnym matroidem reprezentowalnym nad ciałem $\mathbb{F}$ oraz niech $e_0 \in E$. Wówczas port matroidu $\mathcal{M}$ w punkcie e_0 jest spójną i idealną strukturą dostępu $\Gamma \subsetneq \mathcal{P}(E \setminus \{e_0\})$.*

Podobnie jak w przypadku twierdzenia 2.54, jeśli ustalimy spójny matroid $\mathcal{M} = (E, r)$ reprezentowalny nad ciałem $\mathbb{F}$ i zastosujemy twierdzenie 2.56, możemy, w zależności od wyboru $e_0 \in E$, uzyskać różne struktury dostępu $\Gamma \subsetneq \mathcal{P}(E \setminus \{e_0\})$.

Pierwsze pytanie, które można w tym momencie postawić, brzmi następująco: czy istnieje spójny matroid, którego co najmniej jeden port jest spójną, ale nie

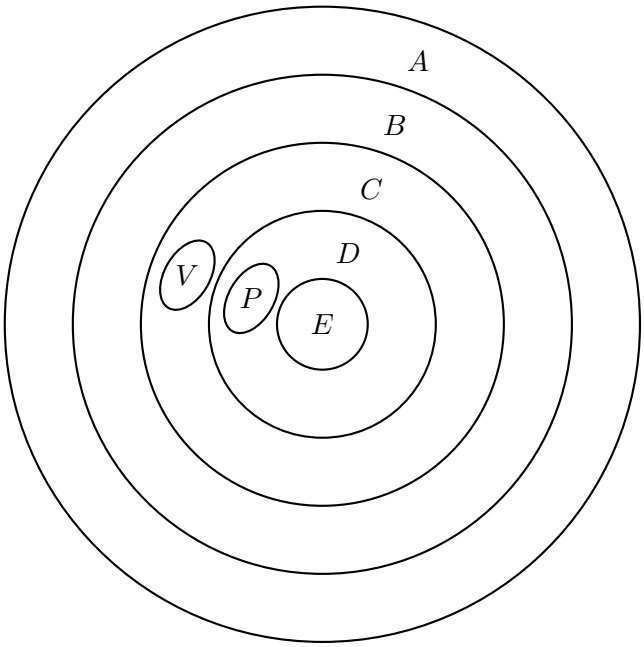
idealną strukturą dostępu? Odpowiedź jest pozytywna, a takim matroidem jest matroid Vamosa. Każdy z jego portów jest spójną, lecz nie idealną strukturą dostępu, co zostało wykazane przez Seymoura [20].

Kolejne pytanie, nad którym warto się zastanowić, jest następujące: czy istnieje spójny i niereprezentowalny nad żadnym ciałem matroid, którego co najmniej jeden port jest spójną i idealną strukturą dostępu? W tym przypadku również odpowiedź jest pozytywna, a matroidem takim jest matroid non-Pappus. Pomimo tego, iż ten matroid nie jest reprezentowalny nad żadnym ciałem, każdy z jego portów jest spójną i idealną strukturą dostępu, co zostało wykazane przez Simonisa i Ashikhmina [23].

Martí-Farré i Padró zaprezentowali interesujący wynik dotyczący złożoności struktury dostępu. Warto przy tym odnotować, iż w przypadku portów matroidu Vamosa zostało wykazane przez Beimela, Livne, Padró [1], że ich złożoności nie przekraczają $\frac{4}{3}$.

Twierdzenie 2.57 (Martí-Farré, Padró [14, Corollary 18])**.** *Jeśli $\Gamma \subsetneq \mathcal{P}(P)$ jest spójną strukturą dostępu oraz $\rho(\Gamma) < \frac{3}{2}$, to istnieje taki spójny matroid zdefiniowany na zbiorze P', że Γ jest jego portem w punkcie p_0.*

Podsumowaniem tego rozdziału jest rysunek 2.1 opisujący relacje pomiędzy omówionymi klasami struktur dostępu.



Rysunek 2.1: Relacje między klasami spójnych struktur dostępu:
A – zbiór spójnych struktur dostępu,
B – zbiór spójnych portów matroidów,
C – zbiór spójnych struktur dostępu, których złożoność jest mniejsza niż $\frac{3}{2}$,
D – zbiór spójnych i idealnych struktur dostępu,
E – zbiór spójnych portów matroidów reprezentowalnych,
P – zbiór portów matroidu non-Pappus,
V – zbiór portów matroidu Vamosa.

Rozdział 3

Wielodzielne struktury dostępu

3.1 Wiadomości wstępne

Badając własności struktur dostępu można zauważyć, że ze struktury tej wynika naturalna hierarchia wśród uczestników. Z drugiej strony, w zdecydowanej większości istniejących organizacji istnieje hierarchia należących do tych organizacji osób. Zatem, jeśli chcemy wprowadzić schemat podziału sekretu w pewnej organizacji, to rozsądne byłoby uwzględnić w strukturze dostępu tego schematu istniejącą w niej hierarchię. Rozpocznijmy od następujących definicji.

Definicja 3.1. Mówimy, że uczestnik $q \in P$ jest *hierarchicznie podrzędny lub równoważny* względem uczestnika $p \in P$ (lub, że uczestnik $p \in P$ jest *hierarchicznie nadrzędny lub równoważny* względem uczestnika $q \in P$) w strukturze dostępu $\Gamma \subsetneq \mathcal{P}(P)$, co oznaczamy $q \preccurlyeq_\Gamma p$, jeśli

$$\bigwedge_{A \subseteq P \setminus \{p,q\}} \Big(A \cup \{q\} \in \Gamma \Longrightarrow A \cup \{p\} \in \Gamma \Big).$$

Definicja 3.2. Mówimy, że uczestnicy $p, q \in P$ są *hierarchicznie równoważni* w strukturze dostępu $\Gamma \subsetneq \mathcal{P}(P)$, co oznaczamy $q \sim_\Gamma p$, jeśli $q \preccurlyeq_\Gamma p$ oraz $p \preccurlyeq_\Gamma q$.

Definicja 3.3. Mówimy, że uczestnik $q \in P$ jest *hierarchicznie podrzędny* względem uczestnika $p \in P$ (lub, że uczestnik $p \in P$ jest *hierarchicznie nadrzędny* względem uczestnika $q \in P$) w strukturze dostępu $\Gamma \subsetneq \mathcal{P}(P)$, co oznaczamy $q \prec_\Gamma p$, jeśli $q \preccurlyeq_\Gamma p$ oraz p i q nie są hierarchicznie równoważni w strukturze dostępu Γ.

O ile nie będzie to prowadzić do nieporozumień, posługując się powyższymi definicjami będziemy pomijać wyrażenie „w strukturze dostępu Γ".

Zauważmy, że definicja 3.2 wprowadza relację równoważności w zbiorze uczestników P przy ustalonej strukturze dostępu Γ. Jej zwrotność i symetryczność jest

oczywista. Pozostaje wykazać, że ta relacja jest przechodnia. Niech $q, p, r \in P$ będą takie, że $q \sim_\Gamma p$ oraz $p \sim_\Gamma r$. Pokażemy, że $q \preccurlyeq_\Gamma r$. Weźmy taki zbiór $A \subseteq P \setminus \{q, r\}$, że $A \cup \{q\} \in \Gamma$ i rozważmy następujące przypadki:

i) $p \notin A$. Wówczas z tego, że $q \preccurlyeq_\Gamma p$ i $p \preccurlyeq_\Gamma r$ otrzymujemy

$$A \cup \{q\} \in \Gamma \Longrightarrow A \cup \{p\} \in \Gamma \Longrightarrow A \cup \{r\} \in \Gamma,$$

co oznacza, że $q \preccurlyeq_\Gamma r$.

ii) $p \in A$. Rozważmy zbiór $B := A \setminus \{p\}$. Ponieważ $p \preccurlyeq_\Gamma r$ oraz $q \preccurlyeq_\Gamma p$, więc

$$A \cup \{q\} \in \Gamma \Longrightarrow B \cup \{p\} \cup \{q\} \in \Gamma \Longrightarrow B \cup \{q\} \cup \{r\} \in \Gamma \Longrightarrow$$

$$\Longrightarrow B \cup \{p\} \cup \{r\} \in \Gamma \Longrightarrow A \cup \{r\} \in \Gamma,$$

co oznacza, że $q \preccurlyeq_\Gamma r$.

Podsumowując, wykazaliśmy, że:

$$(q \preccurlyeq_\Gamma p \ \text{ i } \ p \preccurlyeq_\Gamma r) \implies q \preccurlyeq_\Gamma r. \tag{3.1}$$

Dowód faktu $r \preccurlyeq_\Gamma q$ przebiega analogicznie. W ten sposób wykazaliśmy, że relacja $\sim_\Gamma$ jest relacją równoważności w zbiorze uczestników P przy ustalonej strukturze dostępu Γ.

Definicja 3.4. Niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie strukturą dostępu. Zbiór klas abstrakcji względem relacji równoważności $\sim_\Gamma$ oznaczamy $\Pi_{ka}^{\Gamma} = \{P_1, \ldots, P_l\}$.

Klasy abstrakcji wyznaczają pewien podział zbioru P na rozłączne i niepuste podzbiory, a podział ten zależy ściśle od struktury dostępu, jaką rozważamy. Jednakże podział zbioru uczestników może być narzucony z góry, na przykład wynikając z hierarchii w danej organizacji, zanim jeszcze zaczniemy rozważać jakąkolwiek strukturę dostępu. Ta obserwacja uzasadnia wprowadzenie poniższej definicji 3.5. W dalszym ciągu pisząc o podziale zbioru P mamy na myśli podział zbioru uczestników P na rozłączne i niepuste podzbiory. Ponadto, rozłączne i niepuste podzbiory będące elementami podziału zbioru uczestników P będziemy nazywać blokami.

Definicja 3.5. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Mówimy, że struktura dostępu $\Gamma \subsetneq \mathcal{P}(P)$ jest Π-*dzielna*, jeśli:

$$\bigwedge_{i \in \{1,\ldots,m\}} \bigwedge_{p,q \in \Pi_i} p \sim_\Gamma q.$$

Dowolna struktura dostępu Γ jest Π_{ka}^{Γ}-dzielna. Jeśli rozważymy podział zbioru $P = \{p_1, p_2, \ldots, p_n\}$ na podzbiory jednoelementowe:

$$\Pi_u = \{\{p_1\}, \{p_2\}, \ldots, \{p_n\}\},$$

to każda struktura dostępu $\Gamma \subsetneq \mathcal{P}(P)$ jest Π_u-dzielna.

Uwaga 3.6. Niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie strukturą dostępu. Wówczas:

1. Jeśli Γ jest strukturą progową, to wszyscy uczestnicy są parami hierarchicznie równoważni, zatem $\Pi_{ka}^{\Gamma} = \{P\}$.
2. Jeśli Γ jest Π-dzielna dla $\Pi = \{P\}$, to Γ jest strukturą progową.

Ten wstęp podsumowuje następujące stwierdzenie.

Stwierdzenie 3.7. *Niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *będzie podziałem zbioru uczestników* P*. Jeśli* $\Gamma \subsetneq \mathcal{P}(P)$ *jest* Π*-dzielną strukturą dostępu, to* $\Pi_{ka}^{\Gamma} = \{P_1, \ldots, P_l\}$ *jest podziałem grubszym od* Π*, to znaczy*

$$\bigwedge_{i \in \{1,\ldots,m\}} \bigvee_{j \in \{1,\ldots,l\}} \Pi_i \subseteq P_j.$$

Dowód. Ustalmy dowolny blok Π_i podziału Π oraz dowolnego uczestnika $p \in \Pi_i$. Zauważmy, że istnieje takie $j \in \{1, \ldots, l\}$, że $p \in P_j$. Stąd wszyscy uczestnicy, z którymi p jest hierarchicznie równoważny, należą do P_j, więc $\Pi_i \subseteq P_j$. □

Dla dowolnej struktury dostępu Γ, najgrubszym podziałem, dla którego Γ jest Π-dzielna, jest Π_{ka}^{Γ}, natomiast najdrobniejszym podziałem, dla którego Γ jest Π-dzielna, jest Π_u.

Uwaga 3.8. W przypadku, gdy uczestnicy z różnych bloków Π_i oraz Π_j podziału Π są parami hierarchicznie równoważni w Π-dzielnej strukturze dostępu Γ, można rozważać podział grubszy, w którym wspomniani uczestnicy znajdą się w jednym bloku. Dokładniej, należy utworzyć podział Π', w którym bloki Π_j oraz Π_i są zastąpione blokiem $\Pi_j \cup \Pi_i$. Oczywiście Γ jest również strukturą Π'-dzielną. Sytuacja, gdy nie istnieją różne bloki Π_i oraz Π_j, których uczestnicy są parami hierarchicznie równoważni w Π-dzielnej strukturze dostępu Γ, ma miejsce wtedy i tylko wtedy, gdy podział Π jest równy podziałowi Π_{ka}^{Γ}. Zatem operację „redukcji" podziału można powtarzać wielokrotnie, aż do uzyskania podziału Π_{ka}^{Γ}.

Aby kontynuować dalsze rozważania, ustalmy podział $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ zbioru P oraz Π-dzielną strukturę dostępu $\Gamma \subsetneq \mathcal{P}(P)$. W zbiorze Π możemy zdefiniować następującą relację:

$$\Pi_i \preccurlyeq_{\Gamma} \Pi_j \iff \bigwedge_{q \in \Pi_i} \bigwedge_{p \in \Pi_j} q \preccurlyeq_{\Gamma} p.$$

Ze względu na implikację (3.1) możemy powyższą relację zapisać w następujący sposób:

$$\Pi_i \preccurlyeq_{\Gamma} \Pi_j \iff \bigvee_{q \in \Pi_i} \bigvee_{p \in \Pi_j} q \preccurlyeq_{\Gamma} p. \tag{3.2}$$

Powyższa relacja jest oczywiście zwrotna. Jest również relacją przechodnią, co nie jest trudne do wykazania, jeśli skorzystamy z implikacji (3.1). Jednakże relacja $\preccurlyeq_\Gamma$ w zbiorze Π nie musi być antysymetryczna. Relację, która jest zwrotna i przechodnia (niekoniecznie antysymetryczna) będziemy nazywać *praporządkiem.*

Uwaga 3.9. Relacja (3.2) jest antysymetryczna, a więc jest relacją częściowego porządku, wtedy i tylko wtedy, gdy podział Π jest równy podziałowi Π^Γ_{ka}

W poniższych definicjach (3.10 – 3.16) zakładamy, że $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ jest podziałem zbioru uczestników P oraz $\Gamma \subsetneq \mathcal{P}(P)$ jest Π-dzielną strukturą dostępu.

Definicja 3.10. Mówimy, że blok Π_i jest *hierarchicznie podrzędny lub równoważny* względem bloku Π_j (lub, że blok Π_j jest *hierarchicznie nadrzędny lub równoważny* względem bloku Π_i) w strukturze dostępu Γ, jeśli $\Pi_i \preccurlyeq_\Gamma \Pi_j$.

Definicja 3.11. Mówimy, że bloki Π_i oraz Π_j są *hierarchicznie równoważne* w strukturze dostępu Γ, co oznaczamy $\Pi_i \sim_\Gamma \Pi_j$, jeśli $\Pi_i \preccurlyeq_\Gamma \Pi_j$ i $\Pi_j \preccurlyeq_\Gamma \Pi_i$.

Zauważmy, że $\Pi = \Pi^\Gamma_{ka}$ wtedy i tylko wtedy, gdy w zbiorze Π nie ma dwóch różnych bloków, które byłyby hierarchicznie równoważne w strukturze dostępu Γ.

Definicja 3.12. Mówimy, że blok Π_i jest *hierarchicznie podrzędny* względem bloku Π_j (lub, że blok Π_j jest *hierarchicznie nadrzędny* względem bloku Π_i) w strukturze dostępu Γ, co oznaczamy $\Pi_i \prec_\Gamma \Pi_j$, jeśli $\Pi_i \preccurlyeq_\Gamma \Pi_j$ oraz Π_i i Π_j nie są hierarchicznie równoważne w strukturze dostępu Γ.

Definicja 3.13. Mówimy, że bloki Π_i oraz Π_j są *porównywalne* w strukturze dostępu Γ, jeśli $\Pi_i \preccurlyeq_\Gamma \Pi_j$ lub $\Pi_j \preccurlyeq_\Gamma \Pi_i$. W przeciwnym przypadku bloki Π_i oraz Π_j nazywamy *nieporównywalnymi* w strukturze dostępu Γ.

Definicja 3.14. Mówimy, że blok Π_i jest *maksymalny* w zbiorze $\Phi \subseteq \Pi$ w strukturze dostępu Γ, jeśli dla wszystkich takich bloków $\Pi_j \in \Phi$, że $\Pi_i \preccurlyeq_\Gamma \Pi_j$, otrzymujemy $\Pi_i = \Pi_j$.

Definicja 3.15. Mówimy, że blok Π_i jest *minimalny* w zbiorze $\Phi \subseteq \Pi$ w strukturze dostępu Γ, jeśli dla wszystkich takich bloków $\Pi_j \in \Phi$, że $\Pi_j \preccurlyeq_\Gamma \Pi_i$, otrzymujemy $\Pi_i = \Pi_j$.

Oczywiście, jeśli różne bloki Π_i oraz Π_j są hierarchicznie równoważne w strukturze dostępu Γ, to żaden z nich nie może być minimalny ani maksymalny w zbiorze, do którego oba te bloki należą.

Definicja 3.16. Mówimy, że zbiór bloków $\Phi \subseteq \Pi$ tworzy *prałańcuch* w strukturze dostępu Γ, jeśli każde dwa bloki należące do Φ są porównywalne w strukturze dostępu Γ.

Posługując się powyższymi definicjami będziemy pomijać wyrażenie „w strukturze dostępu Γ", o ile nie będzie to prowadzić do nieporozumień. Teraz podamy definicję, która wyjaśnia tytuł rozdziału.

Definicja 3.17. Strukturę dostępu $\Gamma \subsetneq \mathcal{P}(P)$ nazywamy *wielodzielną*, jeśli jest Π-dzielna dla pewnego podziału Π zbioru uczestników P.

Definicja 3.18. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Strukturę Π-dzielną $\Gamma \subsetneq \mathcal{P}(P)$ wraz z relacją częściowego porządku $(\Pi, \preccurlyeq_\Gamma)$ nazywamy *hierarchiczną*.

Zauważmy, że każda struktura dostępu Γ jest wielodzielna, ponieważ jest Π-dzielna na przykład dla $\Pi = \Pi_{ka}^\Gamma$ lub $\Pi = \Pi_u$. Ponadto powyższa definicja struktury hierarchicznej nie jest bezcelowa, ponieważ pojawia się wtedy, gdy chcemy badać strukturę Γ za pomocą relacji $\preccurlyeq_\Gamma$ zdefiniowanej w zbiorze Π. Jak już wspomnieliśmy wcześniej, relacja $\preccurlyeq_\Gamma$ wprowadza w zbiorze Π praporządek, który możemy interpretować jako hierarchię wśród bloków należących do podziału Π.

Wśród hierarchicznych struktur dostępu rozróżnia się dwa skrajne przypadki, których definicje są następujące.

Definicja 3.19. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Strukturę Γ nazywamy *ściśle hierarchiczną*, jeśli każde dwa bloki podziału Π są porównywalne w strukturze dostępu Γ.

Definicja 3.20. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Strukturę Γ nazywamy *oddziałową*, jeśli każde dwa bloki podziału Π, które są porównywalne w strukturze dostępu Γ, są hierarchicznie równoważne w strukturze dostępu Γ.

Warto zwrócić uwagę, że w literaturze często spotykana jest inna, równoważna 3.19, definicja ściśle hierarchicznej struktury dostępu.

Definicja 3.21. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Strukturę Γ nazywamy *ściśle hierarchiczną*, jeśli dla każdej pary uczestników $p, q \in P$ zachodzi $q \preccurlyeq_\Gamma p$ lub $p \preccurlyeq_\Gamma q$.

Struktury ściśle hierarchiczne oraz oddziałowe zostały bliżej zbadane, o czym piszemy w podrozdziałach 3.3 oraz 3.4. W obu przypadkach, to znaczy struktur ściśle hierarchicznych i oddziałowych, istnieją takie, które są portami matroidów, a nawet są idealne. Można zapytać, czy istnieją struktury dostępu, które są portami matroidów lub są idealne, ale nie są ani ściśle hierarchiczne ani oddziałowe? Pozytywną odpowiedź na to pytanie dajemy w rozdziale 4 niniejszej pracy.

Struktury dostępu, które są Π-dzielne dla pewnego podziału Π zbioru P składającego się z dwóch lub trzech bloków nazywa się odpowiednio strukturami *dwudzielnymi* i *trójdzielnymi*. Dwudzielne struktury dostępu, które są spójne i idealne, zostały pierwszy raz w pełni scharakteryzowane przez Padró i Sáeza, czego efektem jest następujące twierdzenie.

Twierdzenie 3.22 (Padró, Sáez [17, Theorem 3.7])**.** *Niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie spójną dwudzielną strukturą dostępu. Wówczas następujące warunki są równoważne:*

1. *Γ jest portem pewnego matroidu reprezentowalnego;*
2. *Γ jest strukturą idealną;*
3. *$\rho(\Gamma) < \frac{3}{2}$.*

Z powyższego twierdzenia wynika, że jeśli rozważamy tylko spójne dwudzielne struktury dostępu, to zbiory C, D i E na rysunku 2.1 są sobie równe. Posługując się teorią polimatroidów, jeszcze dokładniejszy wynik otrzymali Farràs, Martí-Farré i Padró, o czym mówi następujące twierdzenie.

Twierdzenie 3.23 (Farràs, Martí-Farré, Padró [9, Corollary 7.4])**.** *Niech rodzina $\Gamma \subsetneq \mathcal{P}(P)$ będzie spójną dwudzielną strukturą dostępu. Jeśli Γ jest portem pewnego matroidu, to Γ jest strukturą idealną. Dokładniej, jeśli Γ jest portem pewnego matroidu, to ten matroid jest reprezentowalny.*

Dokładnie taką samą charakteryzację udało się uzyskać temu samemu zespołowi dla trójdzielnych struktur dostępu.

Twierdzenie 3.24 (Farràs, Martí-Farré, Padró [9, Theorem 7.6])**.** *Niech rodzina $\Gamma \subsetneq \mathcal{P}(P)$ będzie spójną trójdzielną strukturą dostępu. Jeśli Γ jest portem pewnego matroidu, to Γ jest strukturą idealną. Dokładniej, jeśli Γ jest portem pewnego matroidu, to ten matroid jest reprezentowalny.*

Z powyższych twierdzeń wynika, że jeśli rozważamy tylko spójne dwudzielne lub trójdzielne struktury dostępu, to zbiory B, C, D i E na rysunku 2.1 są sobie równe. Wiadomo ponadto, że tego wyniku nie da się uogólnić na czterodzielne struktury dostępu. Przyczyną tego stanu rzeczy są porty matroidu Vamosa, które, jak już wiemy, nie są idealnymi strukturami dostępu, ale są strukturami czterodzielnymi.

3.2 Reprezentacja wektorowa zbiorów

Zanim przejdziemy do dalszych rozważań, warto wprowadzić bardzo wygodną reprezentację zbiorów za pomocą wektorów wprowadzoną przez Farràsa, Martí-Farré i Padró, zob. [8], [9]. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru

uczestników P. Rozważmy odwzorowanie $\pi : \mathcal{P}(P) \to \mathbb{N}_0^m$ określone wzorem

$$\pi(A) = (|A \cap \Pi_1|, \ldots, |A \cap \Pi_m|).$$

Dla dowolnej rodziny $\Lambda \subseteq \mathcal{P}(P)$ zdefiniujmy zbiór wektorów

$$\pi(\Lambda) = \{\pi(A) : A \in \Lambda\}. \tag{3.3}$$

W związku z powyższym zachodzi następujące stwierdzenie.

Stwierdzenie 3.25. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Jeśli $\Gamma \subsetneq \mathcal{P}(P)$ jest Π-dzielną strukturą dostępu, to*

$$A \in \Gamma \iff \pi(A) \in \pi(\Gamma).$$

Dowód. Niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Implikacja „$\Rightarrow$" jest oczywista. Wykażemy zatem implikację w drugą stronę. Weźmy taki zbiór $A \subseteq P$, że $\pi(A) \in \pi(\Gamma)$. Z definicji $\pi(\Gamma)$ wynika, iż istnieje taki zbiór $B \in \Gamma$, że $\pi(B) = \pi(A)$. Jeśli $A = B$, to dowód jest zakończony.

Jeśli $A \neq B$, to rozważmy zbiór uczestników $B \backslash A = \{p_1, p_2, \ldots, p_k\}$, który jest niepusty, ponieważ $|A| = \sum_{i=1}^m |A \cap \Pi_i| = \sum_{i=1}^m |B \cap \Pi_i| = |B|$. Oczywiście istnieje taki blok Π_i, że $p_1 \in \Pi_i$. Skoro $\pi(B) = \pi(A)$, to do bloku Π_i należy również element $q_1 \in A$. Uczestnicy p_1 i q_1 są hierarchicznie równoważni w strukturze Γ, więc $C_1 := B \setminus \{p_1\} \cup \{q_1\}$ jest zbiorem autoryzowanym. Ponadto $\pi(C_1) = \pi(A)$ oraz $C_1 \setminus A = \{p_2, \ldots, p_k\}$.

Powtarzamy powyższe rozumowanie jeszcze $k-1$ razy budując w i-tym kroku zbiór $C_i := C_{i-1} \setminus \{p_i\} \cup \{q_i\}$. Dla każdego $i \in \{2, \ldots, k-1\}$ zbiór C_i jest zbiorem autoryzowanym, $\pi(C_i) = \pi(A)$ oraz $C_i \setminus A = \{p_{i+1}, \ldots, p_k\}$. Natomiast zbiór C_k otrzymany w ostatnim kroku również jest zbiorem autoryzowanym oraz jest równy A. W ten sposób wykazaliśmy, że $A \in \Gamma$. □

Od tej pory Π-dzielna struktura dostępu Γ będzie utożsamiana ze zbiorem wektorów $\pi(\Gamma)$ definiowanym za pomocą (3.3). Oczywiście mając dany wektor należący do $\pi(\Gamma)$, wiemy, że odpowiada mu wiele zbiorów uczestników. Jednakże biorąc pod uwagę stwierdzenie 3.25, nie prowadzi to do żadnych nieporozumień. Bardzo często nie interesują nas konkretni uczestnicy należący do pewnego zbioru A, ale wiedza z jakiego bloku pochodzą, a taką właśnie informację przekazuje wektor $\pi(A)$. Wektor $\pi(A)$ nazywamy reprezentacją wektorową zbioru A.

Przyjmijmy $|\Pi_i| =: n_i$ i zauważmy, że

$$\pi(P) = (|P \cap \Pi_1|, \ldots, |P \cap \Pi_m|) = (|\Pi_1|, \ldots, |\Pi_m|) = (n_1, \ldots, n_m).$$

Wobec powyższego możemy napisać, że $\Gamma \subseteq J'_{n_1} \times \cdots \times J'_{n_m} \subseteq \mathbb{N}_0^m$. Nietrudno zauważyć, że własność monotoniczności struktury Γ ma następującą interpretację:

$$\Big((w_1, \ldots, w_m) \in \Gamma \wedge (w_1, \ldots, w_m) \leqslant_s (v_1, \ldots, v_m)\Big) \Longrightarrow (v_1, \ldots, v_m) \in \Gamma.$$

Stąd elementy $\min \Gamma$ są utożsamiane z wektorami minimalnymi względem porządku $(\mathbb{N}_0^m, \leqslant_s)$ ograniczonego do rodziny Γ, które nazywamy minimalnymi wektorami autoryzowanymi. Nie prowadzi to do żadnych nieporozumień ponieważ nietrudno sprawdzić, że

$$A \in \min \Gamma \iff \pi(A) \in \pi(\min \Gamma).$$

Warto także zwrócić uwagę na fakt, że z własności monotoniczności rodziny Γ wynika, iż rodzina $\operatorname{supp} \pi(\Gamma)$ (zob. definicja 2.14) również ma tę własność.

Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Zauważmy, że równoważny zapis relacji (3.2) jest następujący:

$$\Pi_i \preccurlyeq_\Gamma \Pi_j \iff \bigwedge_{\bar{w} \in \Gamma} \Big((w_i > 0 \wedge w_j < |\Pi_j|) \Longrightarrow \bar{w} - \bar{e}_i + \bar{e}_j \in \Gamma \Big). \tag{3.4}$$

Okazuje się, że aby wykazać, iż $\Pi_i \preccurlyeq_\Gamma \Pi_j$, wystarczy badać jedynie minimalne zbiory autoryzowane.

Lemat 3.26. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Wówczas:*

$$\Pi_i \preccurlyeq_\Gamma \Pi_j \iff \bigwedge_{\bar{w} \in \min \Gamma} \Big((w_i > 0 \wedge w_j < |\Pi_j|) \Longrightarrow \bar{w} - \bar{e}_i + \bar{e}_j \in \Gamma \Big).$$

Dowód. Dowodu wymaga jedynie implikacja „$\Leftarrow$”. Weźmy zatem dowolny wektor $\bar{w} \in \Gamma$, $w_i > 0$, $w_j < |\Pi_j|$. Jeśli pokażemy, że $\bar{w} - \bar{e}_i + \bar{e}_j \in \Gamma$, to zakończymy dowód. Oczywiście istnieje taki $\bar{v} \in \min \Gamma$, że $\bar{v} \leqslant_s \bar{w}$. Jeśli $v_i = 0$, to

$$\bar{v} + \bar{e}_j \leqslant_s \bar{w} - \bar{e}_i + \bar{e}_j$$

oraz $\bar{v} + \bar{e}_j \in \Gamma$. Jeśli $v_i > 0$, to z założenia $\bar{v} - \bar{e}_i + \bar{e}_j \in \Gamma$ oraz

$$\bar{v} - \bar{e}_i + \bar{e}_j \leqslant_s \bar{w} - \bar{e}_i + \bar{e}_j.$$

Z monotoniczności rodziny Γ otrzymujemy $\bar{w} - \bar{e}_i + \bar{e}_j \in \Gamma$. □

Na zakończenie tego podrozdziału dokonajmy pewnych obserwacji.

Uwaga 3.27. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Wówczas:

$$\Pi_i \preccurlyeq_\Gamma \Pi_j \Longrightarrow \bigwedge_{\substack{\bar{w} \in \min \Gamma \\ w_i > 0, w_j < |\Pi_j|}} \bar{w} - \min\{|\Pi_j| - w_j, w_i\}\bar{e}_i + \min\{|\Pi_j| - w_j, w_i\}\bar{e}_j \in \Gamma.$$

Powyższa uwaga wskazuje ilu maksymalnie uczestników w wektorze $\bar{w}$ z bloku Π_i można zamienić na uczestników z bloku Π_j tak, aby na i-tej współrzędnej nie pojawiła się liczba ujemna i na j-tej współrzędnej nie pojawiła się liczba większa od $|\Pi_j|$.

Uwaga 3.28. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Wówczas struktura Γ nie jest spójna, to znaczy istnieje taki uczestnik $p \in \Pi_k$ dla pewnego $k \in J_m$, że p nie należy do żadnego minimalnego zbioru autoryzowanego, wtedy i tylko wtedy, gdy $w_k = 0$ dla każdego $\bar{w} \in \min \Gamma$. Ponadto $\Pi_k \preccurlyeq_\Gamma \Pi_j$ dla każdego $j \in J_m$.

Uwaga 3.29. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie Π-dzielną strukturą dostępu. Jeśli istnieje taki blok Π_k, że $w_k = |\Pi_k|$ dla każdego $\bar{w} \in \min \Gamma$, to $\Pi_i \preccurlyeq_\Gamma \Pi_k$ dla każdego $i \in J_m$.

Powyższe uwagi 3.28 oraz 3.29 wynikają bezpośrednio ze wzoru (3.4). W przypadku uwagi 3.29 poprzednik implikacji jest pusto spełniony.

3.3 Ściśle hierarchiczne struktury dostępu

Pomysł ściśle hierarchicznych struktur dostępu pochodzi od Shamira [21]. Rozważa on schemat, w którym dana jest z góry pewna hierarchia w zbiorze uczestników. Na początku określamy, ile udziałów otrzyma uczestnik należący do danego stopnia w hierarchii: uczestnicy, stojący wyżej w tej hierarchii, otrzymują więcej udziałów od tych, którzy są umieszczeni niżej. Następnie konstruujemy schemat progowy Shamira, w którym liczba uczestników n jest sumą wszystkich potrzebnych udziałów, a próg t jest ustaloną liczbą naturalną, mniejszą bądź równą n. Każdy uczestnik otrzymuje tyle udziałów, ile zostało to ustalone wcześniej. Zbiór uczestników jest zbiorem autoryzowanym, jeśli liczba udziałów, którymi razem dysponują wynosi co najmniej t. Oczywiście taki schemat nie jest idealny.

Pomysł Shamira został uogólniony: zaczęto rozważać sytuację, w której każdy uczestnik ma przypisaną wagę, będącą dodatnią liczbę rzeczywistą. Łącząc w bloki uczestników z tą samą wagą otrzymujemy podział Π zbioru P. Zbiór uczestników jest autoryzowany wtedy i tylko wtedy, gdy suma wag uczestników należących do tego zbioru jest większa bądź równa od ustalonego wcześniej progu. Otrzymujemy w ten sposób tak zwaną wagową strukturę dostępu. Zauważmy, że jeśli w zbiorze autoryzowanym zamienimy uczestnika na innego z wagą równą lub większą, to otrzymamy również zbiór autoryzowany. Możemy zatem uznać, że każdy uczestnik jest hierarchicznie podrzędny lub równoważny względem uczestnika z wagą równą lub większą. Nie jest trudno zauważyć, że wagowa struktura dostępu $\Gamma \subsetneq \mathcal{P}(P)$ jest spójna i Π-dzielna oraz podział Π jest równy podziałowi Π_{ka}^Γ na klasy abstrakcji wyznaczone przez Γ.

Simmons [22] przy ustalonym podziale $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ zbioru P rozważał struktury dostępu postaci

$$\Gamma_\vee := \{A \subseteq P : \exists_{i \in \{1,\ldots,m\}} \ \ |A \cap (\cup_{j=1}^{i} \Pi_j)| \geqslant k_i\},$$

gdzie $(k_i)_{i=1,\ldots,m}$ jest silnie rosnącym ciągiem liczb naturalnych. Struktura dostępu $\Gamma_\vee$ była także rozważana przez Tassę w [24], który nazwał ją strukturą

dysjunkcyjną. W tym samym artykule badał także strukturę nazwaną koniunkcyjną, która ma postać

$$\Gamma_\wedge := \{A \subseteq P : \forall_{i\in\{1,\ldots,m\}} \ \ |A \cap (\cup_{j=1}^{i}\Pi_j)| \geqslant k_i\},$$

gdzie $(k_i)_{i=1,\ldots,m}$ jest również silnie rosnącym ciągiem liczb naturalnych. Tassa zauważył, że powyższe struktury $\Gamma_\vee$ oraz $\Gamma_\wedge$ stanowią dwa skrajne elementy rodziny $\{\Gamma_v : v = 1,\ldots,m\}$, gdzie

$$\Gamma_v := \{A \subseteq P : |A \cap (\cup_{j=1}^{i}\Pi_j)| \geqslant k_i \text{ dla co najmniej } v \text{ wartości } i \in \{1,\ldots,m\}\},$$

przy czym $(k_i)_{i=1,\ldots,m}$ jest oczywiście silnie rosnącym ciągiem liczb naturalnych. Jeśli $v = 1$, to $\Gamma_v = \Gamma_\vee$, natomiast dla $v = m$, mamy $\Gamma_v = \Gamma_\wedge$. Zauważmy, że dla każdego $v \in \{1,\ldots,m\}$ struktura dostępu Γ_v jest spójna i Π-dzielna. Bez trudu można dostrzec, że w powyższych przypadkach wszystkie struktury dostępu wyznaczają podział $\Pi_{ka}^{\Gamma_v}$ na klasy abstrakcji, który jest równy wyjściowemu podziałowi Π. Tassa wykazał, że istnieją idealne schematy podziału sekretu realizujące struktury $\Gamma_\vee$ oraz $\Gamma_\wedge$ konstruując te schematy. Sformułował także problem polegający na rozstrzygnięciu, czy pozostałe elementy rodziny Γ_v są również idealne.

Wszystkie opisane powyżej struktury dostępu są przykładami struktur ściśle hierarchicznych. Farràs i Padró udzielili negatywnej odpowiedzi na pytanie sformułowane przez Tassę. Odpowiedź ta była wnioskiem z charakteryzacji spójnych i idealnych ściśle hierarchicznych struktur dostępu ([10, Theorem 16]). W wyniku tej charakteryzacji otrzymali również poniższe twierdzenie.

Twierdzenie 3.30 (Farràs, Padró [10, Theorem 1])**.** *Niech Π będzie podziałem zbioru uczestników P oraz niech $\Gamma \subsetneq \mathcal{P}(P)$ będzie spójną Π-dzielną ściśle hierarchiczną strukturą dostępu. Wówczas następujące warunki są równoważne:*

1. *Γ jest portem pewnego matroidu reprezentowalnego;*
2. *Γ jest strukturą idealną;*
3. *$\rho(\Gamma) < \frac{3}{2}$;*
4. *Γ jest portem pewnego matroidu.*

Na zakończenie tego podrozdziału zaprezentujemy alternatywne uzasadnienie dlaczego odpowiedź na pytanie postawione przez Tassę jest negatywna. Zanim przejdziemy do twierdzenia rozwiązującego ten problem i korzystającego z wyników zaprezentowanych w podrozdziale 1.3, wprowadzimy na potrzeby dowodu następujące określenie.

Definicja 3.31. Niech $\Pi = \{\Pi_1,\ldots,\Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech $0 < k_1 < \ldots < k_m$ będzie ściśle rosnącym ciągiem liczb naturalnych.

Mówimy, że zbiór $A \subseteq P$ spełnia *progową własność na poziomie* i (w skrócie TP_i), jeśli $|A \cap (\bigcup_{j=1}^{i} \Pi_j)| \geqslant k_i$.

Twierdzenie 3.32 ([13, Theorem 6])**.** *Niech* $0 = k_0 < k_1 < \ldots < k_m$, $m > 2$, *będzie ściśle rosnącym ciągiem liczb naturalnych oraz niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *będzie takim podziałem zbioru uczestników* P, *że* $|\Pi_j| \geqslant k_j - k_{j-1}$ *dla każdego* $j = 1, \ldots, m$.

Jeśli $v \in \{2, \ldots, m-1\}$, $|\Pi_{m-v+1}| \geqslant k_m$ *oraz* $|\Pi_{m-v+2}| \geqslant k_m - k_1$, *to struktura dostępu* Γ_v *nie jest realizowana przez spójny i idealny schemat podziału sekretu.*

Dowód. Ustalmy $v \in \{2, \ldots, m-1\}$ i załóżmy nie wprost, że istnieje spójny i idealny schemat podziału sekretu $\mathbf{M}$, który realizuje Γ_v. Na podstawie twierdzenia 2.53 możemy rozważać matroid $\mathfrak{M}(\mathbf{M})$ stowarzyszony ze schematem $\mathbf{M}$. Przypomnijmy, że rodzina wszystkich zbiorów zależnych schematu $\mathbf{M}$ jest równa rodzinie wszystkich zbiorów zależnych matroidu z nim stowarzyszonego $\mathfrak{M}(\mathbf{M})$. Stąd wynika, że rodzina wszystkich zbiorów niezależnych schematu $\mathbf{M}$ jest równa rodzinie wszystkich zbiorów niezależnych matroidu $\mathfrak{M}(\mathbf{M})$.

Pierwsza część dowodu polega na wykazaniu, że ranga matroidu stowarzyszonego $\mathfrak{M}(\mathbf{M})$ wynosi co najwyżej k_m. Rozważmy taki zbiór uczestników $A \subseteq P$, że $\pi(A) := (t_1, t_2, \ldots, t_m)$, gdzie

$$t_j := \begin{cases} k_1 & \text{dla } j = 1; \\ k_j - k_{j-1} - 1 & \text{dla } j = v; \\ k_j - k_{j-1} & \text{w pozostałych przypadkach.} \end{cases}$$

Zauważmy, że A jest maksymalnym zbiorem nieautoryzowanym. Istotnie, jeśli $1 \leqslant i \leqslant v-1$, to

$$|A \cap (\bigcup_{j=1}^{i} \Pi_j)| = \sum_{j=1}^{i} t_j = k_i,$$

a jeśli $v \leqslant i \leqslant m$, to

$$|A \cap (\bigcup_{j=1}^{i} \Pi_j)| = \sum_{j=1}^{i} t_j = k_i - 1.$$

To pokazuje, że A nie spełnia TP_i dla $i \geqslant v$, więc A jest zbiorem nieautoryzowanym. Jednakże, dodając dowolnego uczestnika $p \in P \setminus A$ do zbioru A otrzymujemy zbiór autoryzowany, ponieważ $A \cup \{p\}$ spełnia TP_i dla $i \leqslant v-1$ oraz dla $i \geqslant j$, jeśli $p \in \Pi_j$. Zauważmy, że $|A| = k_m - 1$. Aby zastosować wniosek 1.25, rozważmy dowolny zbiór niezależny B schematu $\mathbf{M}$ i rozważmy dwa przypadki:

i) $p_0 \notin B$. Wówczas $B \subseteq P$, więc z pierwszej tezy wniosku 1.25 otrzymujemy $|B| \leqslant k_m$.

ii) $p_0 \in B$. Zauważmy, że zbiór $B \setminus \{p_0\}$ jest nieautoryzowany. Istotnie, gdyby $B \setminus \{p_0\}$ był autoryzowany, to zbiór B byłby zależny. Z drugiej tezy wniosku 1.25 otrzymujemy $|B \setminus \{p_0\}| \leqslant k_m - 1$, stąd $|B| \leqslant k_m$.

Zbiór B jest także zbiorem niezależnym matroidu $\mathfrak{M}(\mathbf{M})$. Z powyższych rozważań wynika, że moc każdego zbioru niezależnego matroidu stowarzyszonego $\mathfrak{M}(\mathbf{M})$, w szczególności każdej jego bazy, wynosi co najwyżej k_m. W ten sposób wykazaliśmy, że ranga matroidu stowarzyszonego $\mathfrak{M}(\mathbf{M})$ wynosi co najwyżej k_m.

W następnym kroku pokażemy, że ranga matroidu stowarzyszonego $\mathfrak{M}(\mathbf{M})$ wynosi dokładnie k_m. Wykażemy ten fakt wskazując minimalny zbiór autoryzowany, który zawiera dokładnie k_m uczestników. Rozważmy taki zbiór $B_1 \subseteq P$, że

$$B_1 := (\underbrace{0, \ldots, 0}_{m-v}, k_m, 0, \ldots, 0).$$

Łatwo widać, że B_1 spełnia TP_i dla $i = m-v+1, m-v+2, \ldots, m$. Ponadto żaden właściwy podzbiór zbioru B_1 nie spełnia TP_m. To pokazuje, że B_1 jest minimalnym zbiorem autoryzowanym schematu $\mathbf{M}$, stąd jest jego zbiorem niezależnym, więc jest także zbiorem niezależnym w matroidzie stowarzyszonym $\mathfrak{M}(\mathbf{M})$. W ten sposób wykazaliśmy, że ranga matroidu $\mathfrak{M}(\mathbf{M})$ wynosi dokładnie k_m oraz B_1 jest jego bazą.

Następnie rozważmy taki zbiór B_2, że

$$B_2 := (k_1, \underbrace{0, \ldots, 0}_{m-v}, k_m - k_1, 0, \ldots, 0).$$

Pokażemy, że B_2 jest także bazą matroidu stowarzyszonego $\mathfrak{M}(\mathbf{M})$ wykazując, że B_2 jest minimalnym zbiorem autoryzowanym schematu $\mathbf{M}$ mocy k_m. Łatwo sprawdzić, że spełnia TP_i dla $i = 1, m-v+2, \ldots, m$, to znaczy dokładnie v wartości spośród m możliwych. Dodatkowo zbiór $B_2 \setminus \{p\}$ nie spełnia TP_1 lub TP_m, jeśli odpowiednio $p \in \Pi_1 \cap B_2$ lub $p \in \Pi_{m-v+2} \cap B_2$.

W ostatnim kroku dowodu zastosujemy lemat 2.4. Dla $p \in B_2 \cap \Pi_1$ istnieje taki $p' \in B_1$, że $B_3 := (B_2 \setminus \{p\}) \cup \{p'\}$ jest bazą, stąd B_3 jest niezależny. Łatwo sprawdzić, że

$$B_3 = (k_1 - 1, \underbrace{0, \ldots, 0}_{m-v-1}, 1, k_m - k_1, 0, \cdots, 0),$$

ponieważ $B_1 \subseteq \Pi_{m-v+1}$. Oczywiście B_3 spełnia TP_i tylko dla $i = m-v+2, \ldots, m$, co pokazuje, że B_3 jest nieautoryzowany. Według drugiej tezy wniosku 1.25 mamy $k_m = |B_3| \leqslant |A| = k_m - 1$. Ta sprzeczność kończy dowód. □

3.4 Oddziałowe struktury dostępu

Oddziałowe struktury dostępu znajdują swoje zastosowanie w organizacjach składających się z kilku równorzędnych oddziałów, wśród których nie można wskazać żadnej hierarchii.

Pierwszy przykład oddziałowej struktury dostępu pojawił się w pracy Simmonsa [22], który przy ustalonym podziale $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ zbioru P rozważał

rodzinę:

$$\Gamma := \{A \subseteq P : \forall_{i\in\{1,\ldots,m\}} \ \ |A \cap \Pi_i| \geqslant k_i\},$$

gdzie$(k_i)_{i=1,\ldots,m}$ jest ciągiem liczb naturalnych. Zauważmy, że dla powyższej rodziny istnieje dokładnie jeden wektor minimalny: $(k_1, \ldots, k_m)$.

Brickell [4] natomiast, również przy ustalonym podziale $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ zbioru P, rozważał strukturę dostępu:

$$\Gamma := \{A \subseteq P : \forall_{i\in\{1,\ldots,m\}} \ \ |A \cap \Pi_i| \geqslant k_i \text{ oraz } |A| \geqslant k\}, \tag{3.5}$$

gdzie $(k_i)_{i=1,\ldots,m}$ jest także ciągiem liczb naturalnych oraz $k \geqslant \sum_{i=1}^{m} k_i$ jest liczbą naturalną. Zauważmy, że jeśli $k = \sum_{i=1}^{m} k_i$, to otrzymujemy strukturę, którą rozważał Simmons. Brickell w swojej pracy wykazał, że struktura dostępu postaci (3.5) jest strukturą idealną.

Oddziałowymi strukturami dostępu zainteresowali się także Tassa i Dyn, którzy w swojej pracy [25] rozważali przy ustalonym podziale $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ zbioru P strukturę

$$\Gamma_{do} := \{A \subseteq P : \text{istnieje taki } B \subseteq A, \text{ że } \forall_{i\in\{1,\ldots,m\}} \ |B \cap \Pi_i| \geqslant k_i \text{ oraz } |B| = k\}$$

oraz

$$\Gamma_{go} := \{A \subseteq P : \text{istnieje taki } B \subseteq A, \text{ że } \forall_{i\in\{1,\ldots,m\}} \ |B \cap \Pi_i| \leqslant l_i \text{ oraz } |B| = l\},$$

gdzie $(k_i)_{i=1,\ldots,m}$ oraz $k \geqslant \sum_{i=1}^{m} k_i$ są takie jak wyżej, natomiast $(l_i)_{i=1,\ldots,m}$ jest ciągiem liczb naturalnych oraz $l \leqslant \sum_{i=1}^{m} l_i$, $l \in \mathbb{N}$. Powyższe rodziny noszą nazwy odpowiednio struktury dostępu z dolnymi ograniczeniami oraz struktury dostępu z górnymi ograniczeniami. Zauważmy, że struktura dostępu Γ_{do} to struktura rozważana przez Brickella. Dyn i Tassa wykazali, korzystając z interpolacji dla wielomianów dwóch zmiennych, że rodziny Γ_{do} i Γ_{go} są idealnymi strukturami dostępu. Wszystkie powyższe struktury dostępu są spójne i Π-dzielne. Bez trudu można dostrzec, że w powyższych przypadkach struktura dostępu Γ wyznacza podział Π_{ka}^{Γ} na klasy abstrakcji, który jest równy wyjściowemu podziałowi Π.

Kolejny krok zrobił Farràs [7], który rozważał następującą strukturę dostępu, także przy wcześniej ustalonym podziale $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ zbioru P:

$$\min\Gamma := \{\bar{w} \in \mathbb{N}_0^m : |\bar{w}| = d \text{ oraz } \bar{a} \leqslant_s \bar{w} \leqslant_s \bar{b}\}, \tag{3.6}$$

gdzie d jest liczbą naturalną, natomiast $\bar{a} \in \mathbb{N}_0^m$ oraz $\bar{b} \in \mathbb{N}_0^m$ są wektorami. Zauważmy, że jeśli $\bar{a} = (0, \ldots, 0)$, to Γ jest strukturą z górnymi ograniczeniami. Ponadto, jeśli $\bar{b} = (|P_1|, \ldots, |P_m|)$, to Γ jest strukturą z dolnymi ograniczeniami. Stąd wniosek, że struktura dostępu rozważana przez Farràsa obejmuje wszystkie wcześniej wymienione struktury. Zauważmy jeszcze, że jeśli jednocześnie $\bar{a} = (0, \ldots, 0)$ oraz $\bar{b} = (|P_1|, \ldots, |P_m|)$, to Γ jest strukturą progową z progiem równym d. Farràs wykazał, że struktury postaci (3.6) są nie tylko idealne, ale także są portami pewnych matroidów reprezentowalnych.

Przyjrzyjmy się jeszcze bliżej strukturze dostępu (3.6). Nie ulega wątpliwości, że jest ona Π-dzielna. Okazuje się jednak, że nie musi być spójna. Weźmy takie $\bar{a}$ i $\bar{b}$, że $a_i = b_i = 0$ dla pewnego $i \in \{1, \ldots, m\}$. Wówczas, na podstawie uwagi 3.28, otrzymujemy, że struktura Γ nie jest spójna oraz $\Pi_i \preccurlyeq_\Gamma \Pi_j$ dla każdego $j \in \{1, \ldots, m\}$. Stąd widać, że struktury typu (3.6) obejmują także struktury dostępu, które nie są strukturami oddziałowymi w sensie definicji 3.20.

Niech zatem $\bar{a}$ i $\bar{b}$ będą wektorami, których każda współrzędna jest dodatnia. Wówczas struktury typu (3.6) są spójne i oddziałowe. Stąd otrzymujemy warunki wystarczające na to, aby struktura oddziałowa była strukturą idealną. Powstaje pytanie, czy są to także warunki konieczne aby struktura oddziałowa była strukturą idealną. Otóż negatywną odpowiedź dostarczy nam podrozdział 4.6, w którym wskażemy idealne oddziałowe struktury dostępu nie mające postaci 3.20.

Na zakończenie warto jeszcze przytoczyć pewien przykład oddziałowej struktury dostępu, która była rozważana przez Sáeza i Herranza [18]:

$$\Gamma = \{A \subseteq P\colon |A| \geqslant k,\ |A \cap \Pi_i| \geqslant 1 \text{ dla co najmniej } v \text{ wartości } i \in \{1, \ldots, m\}\},$$

gdzie $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ jest wcześniej ustalonym podziałem zbioru P oraz k jest taką liczbą naturalną, że $v \leqslant k$. Sáez i Herranz wykazali, że powyższa struktura jest idealna. Jest ona interesująca, ponieważ zbiór autoryzowany, oprócz ustalonej liczby k uczestników, musi „angażować" co najmniej v spośród m bloków. Zauważmy, że jeśli $v = m$, to mamy pewien szczególny przypadek struktury z dolnymi ograniczeniami, w którym $(k_i)_{i=1,\ldots,m}$ jest ciągiem złożonym z samych jedynek. Ponadto ta struktura jest spójna i Π-dzielna oraz wyznacza podział Π^Γ_{ka} na klasy abstrakcji, który jest równy podziałowi Π.

Podsumowując, w literaturze można spotkać wiele przykładów oddziałowych struktur dostępu, które są idealne, a także są portami pewnych matroidów reprezentowalnych. Jednakże do tej pory nie zostały podane warunki konieczne na to, aby oddziałowa struktura dostępu była idealna.

Rozdział 4

Hierarchiczne struktury dostępu

4.1 Wiadomości wstępne

Rozpoczniemy od przedstawienia twierdzenia, które jest naszym podstawowym narzędziem w budowaniu struktur dostępu, które są portami pewnych matroidów.

Twierdzenie 4.1 (Farràs, Martí-Farré, Padró [8, Theorem 8],[9, Theorem 5.3])**.** *Niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *będzie podziałem zbioru uczestników* P *oraz niech rodzina* $\Gamma \subsetneq \mathcal{P}(P)$ *będzie spójną* Π*-dzielną strukturą dostępu. Wówczas* Γ *jest portem pewnego matroidu wtedy i tylko wtedy, gdy istnieje taki polimatroid* $\mathcal{Z} = (J_m, h)$*, że* $h(\{k\}) \leqslant |\Pi_k|$ *dla każdego* $k \in J_m$ *oraz taka rodzina monotoniczna* $\Delta \subsetneq \mathcal{P}(J_m)$ *z nim kompatybilna, że*

$$\min \Gamma = \min\{\bar{w} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}. \tag{4.1}$$

Wykorzystanie powyższego twierdzenia odbywa się w następujący sposób:

1. Ustalamy $\Pi = \{\Pi_1, \ldots, \Pi_m\}$, $m \geqslant 2$, podział zbioru uczestników P.

2. Wybieramy polimatroid jednorodny $\mathcal{Z} = (J_m, h)$. Nasze badania zawężamy do polimatroidów jednorodnych, ponieważ ogólny przypadek jest bardzo skomplikowany. Dodatkowo zakładamy, że $h_m \leqslant |\Pi_k|$ dla każdego $k \in J_m$. Uzasadnienie takiego założenia znajduje się na końcu tego podrozdziału. Zauważmy, że z monotoniczności funkcji h oraz przyjętego założenia wynika, iż $h(\{k\}) = h_1 \leqslant |\Pi_k|$ dla każdego $k \in J_m$. Polimatroid jednorodny $\mathcal{Z} = (J_m, h)$, którego funkcja rangi h spełnia założenie $h_m \leqslant |\Pi_k|$ dla każdego $k \in J_m$, będziemy oznaczali $\mathcal{Z}(\Pi)$.

3. Wybieramy niepustą rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$.

4. Jeśli rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem jednorodnym $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$, to definiujemy rodzinę monotoniczną Γ

określając jej zbiory minimalne:

$$\min \Gamma := \min\{\bar{w} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}.$$

W ten sposób, na podstawie twierdzenia 4.1, uzyskaliśmy strukturę dostępu, o której można powiedzieć, że jest Π-dzielna. Ponadto, jeśli Γ jest spójna, to jest także portem pewnego matroidu. Jeśli dodatkowo założymy, że $m = 2$ lub $m = 3$, to z twierdzeń 3.23 i 3.24 otrzymamy, że Γ jest strukturą idealną, co więcej, jest portem pewnego matroidu reprezentowalnego. Struktur uzyskanych w ten sposób, które są spójne, jest stosunkowo dużo i są one opisane w stwierdzeniach od 4.30 do 4.33.

Celem naszej pracy jest badanie hierarchiczności w strukturach opisanych powyżej. Wprowadźmy ich formalną definicję.

Definicja 4.2. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym i niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie rodziną monotoniczną z nim kompatybilną. Strukturę Γ nazywamy *strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z}$ i rodzinę monotoniczną Δ*, jeśli

$$\min \Gamma = \min\{\bar{w} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}.$$

W podrozdziale 4.2 zaprezentujemy szereg twierdzeń pozwalających badać praporządek w zbiorze $(\Pi, \preccurlyeq_\Gamma)$ wyznaczony przez strukturę dostępu Γ zdefiniowaną za pomocą (4.1). Przypomnijmy, że chodzi o praporządek zadany równoważnymi wzorami (3.2) i (3.4). Zastosowanie otrzymanych wyników dla przypadków gdy $m = 2$, $m = 3$ lub $m = 4$ dobrze obrazują tabele 4.1, 4.2 oraz 4.3 znajdujące się w podrozdziale 4.4.

W całym rozdziale zakładamy, że $m \geqslant 2$. Jest to zrozumiałe założenie z tego względu, że praporządek w zbiorze $(\Pi, \preccurlyeq_\Gamma)$, $\Pi = \{\Pi_1, \ldots, \Pi_m\}$, dla $m = 1$ jest trywialny. Rozpocznijmy od kilku bardzo prostych obserwacji zawartych w poniższym lemacie, które ułatwią przeprowadzenie kolejnych dowodów.

Lemat 4.3. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech ponadto Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Wówczas:*

1. $\{\bar{w} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\} \subseteq \Gamma$.
2. $\operatorname{supp} \Gamma = \Delta$.
3. *Jeśli $\bar{w} \in \min \Gamma$, to $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ i $\operatorname{supp} \bar{w} \in \Delta$.*
4. *Jeśli $\bar{w} \in \Gamma$, to istnieje taki $\bar{v} \in \min \Gamma$, że $\bar{v} \leqslant_s \bar{w}$, $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{v})$ i $\operatorname{supp} \bar{v} \in \Delta$.*

Dowód. 1. Niech $\bar{v} \in \{\bar{w} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}$. Wówczas istnieje taki wektor $\bar{u}$, że $\bar{u} \leqslant_s \bar{v}$ oraz $\bar{u} \in \min\{\bar{w} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}$. Stąd otrzymujemy $\bar{u} \in \min \Gamma$, natomiast z własności monotoniczności Γ mamy $\bar{v} \in \Gamma$. Zauważmy, że inkluzja w drugą stronę nie musi zachodzić.

2. Weźmy $Y \in \operatorname{supp} \Gamma$. Wówczas istnieje takie $\bar{w} \in \Gamma$, że $\operatorname{supp} \bar{w} = Y$. Rozważmy dwa przypadki:

i) $\bar{w} \in \min \Gamma$. Wówczas istnieje takie $X \in \Delta$, że $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$, stąd $Y \subseteq X$. Jeśli $Y = X$, to $Y \in \Delta$. Jeśli $Y \subsetneq X$, to także $Y \in \Delta$. Istotnie, zauważmy, że $|\bar{w}_Y| \leqslant h(Y)$, $|\bar{w}_X| = h(X)$ i $|\bar{w}_Y| = |\bar{w}_X|$, gdzie ostatnia równość wynika z faktu, że $\operatorname{supp} \bar{w} = Y \subseteq X$. Ponadto, gdyby $Y \notin \Delta$, to z lematu Csirmaza (2.21, 1) otrzymujemy

$$h(X) = |\bar{w}_X| = |\bar{w}_Y| \leqslant h(Y) < h(X),$$

co jest sprzecznością.

ii) $\bar{w} \in \Gamma$ i $\bar{w} \notin \min \Gamma$. Wówczas istnieje takie $\bar{v} \in \min \Gamma$, że $\bar{v} \leqslant_s \bar{w}$. Z przypadku i) wynika, że $\operatorname{supp} \bar{v} \in \Delta$. Zauważmy, że $\operatorname{supp} \bar{v} \subseteq \operatorname{supp} \bar{w}$, ponadto Δ jest rodziną monotoniczną, stąd $Y = \operatorname{supp} \bar{w} \in \Delta$.

Teraz wykażemy inkluzję w drugą stronę. Weźmy $X \in \Delta$. Jak już zauważyliśmy w uwadze 2.17, rodzina $\mathcal{B}(\mathcal{Z}, X)$ nigdy nie jest pusta, stąd istnieje wektor $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$. Z punktu 1 otrzymujemy $\bar{w} \in \Gamma$, więc $\operatorname{supp} \bar{w} \in \operatorname{supp} \Gamma$. Rodzina $\operatorname{supp} \Gamma$ jest monotoniczna oraz $\operatorname{supp} \bar{w} \subseteq X$, stąd $X \in \operatorname{supp} \Gamma$.

3. Jeśli $\bar{w} \in \min \Gamma$, to $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$ dla pewnego $X \in \Delta$. Z lematu 2.18 wynika, że $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$. Ponadto $\operatorname{supp} \bar{w} \in \operatorname{supp} \Gamma$, stąd i na podstawie punktu 2 otrzymujemy $\operatorname{supp} \bar{w} \in \Delta$.

4. Wynika bezpośrednio z punktu 3. □

Lemat 4.4. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech ponadto Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$ oraz niech $\bar{w}$ będzie wektorem wierzchołkowym. Wówczas*

$$\operatorname{supp} \bar{w} \in \Delta \iff \bar{w} \in \Gamma.$$

Dowód. Jeśli $\bar{w}$ jest wektorem wierzchołkowym, to na podstawie lematu 2.39 otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$. Teraz stosując lemat 4.3 (1) uzyskujemy implikację „⇒”. Implikacja w drugą stronę wynika z lematu 4.3 (2). □

Pozostało do uzasadnienia pewne założenie przyjęte przy konstrukcji struktury dostępu opisanej na początku tego podrozdziału. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech ponadto Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i niepustą rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Przy wyborze polimatroidu jednorodnego zakładamy, że $h_m \leqslant |\Pi_k|$ dla każdego $k \in J_m$. Zauważmy, że dzięki

temu założeniu, rozważając wektor $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$ mamy zapewnione, iż wektor $\bar{w}' := \bar{w} - \alpha\bar{e}_i + \alpha\bar{e}_j$ dla każdego $\alpha \in \{1, \ldots, w_i\}$, $i \in \operatorname{supp}\bar{w}$ oraz $j \in J_m$ ma j-tą współrzędną nie przekraczającą $|\Pi_j|$. Istotnie, na podstawie definicji zbioru $\mathcal{B}(\mathcal{Z}, X)$ otrzymujemy $|\bar{w}'| = |\bar{w}| = h(X)$. Ponadto, z tego, że $i \in \operatorname{supp}\bar{w}$ wynika, iż $w_i \geqslant 1$ oraz $w_j \leqslant h(X) - w_i \leqslant h_m - w_i \leqslant |\Pi_j| - w_i$. Ostatecznie $w'_j = w_j + \alpha \leqslant w_j + w_i \leqslant |\Pi_j|$.

W dowodach twierdzeń zawartych w tym rozdziale bardzo często będziemy rozważać taki wektor wierzchołkowy $\bar{w}$, że $\operatorname{supp}\bar{w} \in \Delta$ oraz wektor $\bar{v} \in \min\Gamma$. Na podstawie lematu 2.39 otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{w})$, natomiast z lematu 4.3 (3) mamy $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{v})$, $\operatorname{supp}\bar{v} \in \Delta$. Stąd rozważając wektory

$$\bar{w}' := \bar{w} - \alpha\bar{e}_i + \alpha\bar{e}_j \quad \bar{v}' := \bar{v} - \beta\bar{e}_l + \beta\bar{e}_n,$$

gdzie $\alpha \in \{1, \ldots, w_i\}$, $\beta \in \{1, \ldots, v_l\}$, $i \in \operatorname{supp}\bar{w}$, $l \in \operatorname{supp}\bar{v}$ oraz $j, n \in J_m$, mamy pewność, że $\bar{w}'$,$\bar{v}' \in J'_{n_1} \times \cdots \times J'_{n_m} \subseteq \mathbb{N}_0^m$, gdzie $n_t = |\Pi_t|$, $t \in J_m$.

4.2 Praporządek w rodzinie bloków

Badania praporządku w zbiorze $(\Pi, \preccurlyeq_\Gamma)$ rozpoczniemy od poniższego twierdzenia i wynikającego z niego wniosku. Pamiętajmy, że wszystkie polimatroidy rozważane w tym podrozdziale są polimatroidami jednorodnymi, ale warto zwrócić uwagę na fakt, że 4.5 oraz 4.6 to jedyne twierdzenia, w których można pominąć założenie, iż $\mathcal{Z}$ jest polimatroidem jednorodnym.

Twierdzenie 4.5. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną.*

Jeśli $X \in \min\Delta$, to dla każdych $i, j \in X$, $i \neq j$, bloki Π_i oraz Π_j są nieporównywalne w strukturze dostępu Γ.

Dowód. Niech $X \in \min\Delta$ oraz niech i, j będą dowolnymi różnymi elementami ze zbioru X. Przypuśćmy, że $\Pi_i \preccurlyeq_\Gamma \Pi_j$ i weźmy wektor $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$. Na podstawie lematu 4.3 (1) mamy $\bar{w} \in \Gamma$. Jeśli $w_i = 0$, to powołując się na lemat 4.3 (2) otrzymujemy $X \setminus \{i\} \in \Delta$, co jest sprzeczne z minimalnością zbioru X.

Jeśli $w_i > 0$, to rozważmy wektor $\bar{w}' := \bar{w} - w_i\bar{e}_i + w_i\bar{e}_j$. Z założenia $\Pi_i \preccurlyeq_\Gamma \Pi_j$ otrzymujemy $\bar{w}' \in \Gamma$. Zauważmy, że $\operatorname{supp}\bar{w}' = X \setminus \{i\}$. Ponownie powołując się na lemat 4.3 (2) ponownie otrzymujemy $X \setminus \{i\} \in \Delta$, co jest sprzeczne z minimalnością zbioru X. Analogicznie doprowadzamy do sprzeczności przypuszczenie, że $\Pi_j \preccurlyeq_\Gamma \Pi_i$. □

Wniosek 4.6. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech ponadto Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną.*

Jeśli dla każdych $i, j \in J_m$, $i \neq j$, istnieje taki zbiór $X \in \min \Delta$, że $i, j \in X$, to każde dwa bloki należące do zbioru Π są nieporównywalne w strukturze dostępu Γ.

Dowód. Wniosek wynika bezpośrednio z twierdzenia 4.5. □

Kolejne twierdzenie i wynikające z niego dwa wnioski pozwalają na wyznaczanie pewnych elementów maksymalnych i minimalnych w zbiorze $(\Pi, \preccurlyeq_\Gamma)$.

Twierdzenie 4.7. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $X \in \min \Delta$, $1 \leqslant |X| =: k \leqslant m-1$ oraz $g_k > 0$, to dla każdych $i \in X$, $j \in J_m \setminus X$ blok Π_i nie jest hierarchicznie podrzędny lub równoważny względem bloku Π_j w strukturze dostępu Γ.

Dowód. Przypuśćmy, że dla pewnego $i \in X$ oraz dla pewnego $j \in J_m \setminus X$ mamy $\Pi_i \preccurlyeq_\Gamma \Pi_j$. Rozważmy taki wektor wierzchołkowy $\bar{w}$ rzędu k, że $\operatorname{supp} \bar{w} = X$ oraz $w_i = g_0 = h_1$. Oczywiście $\bar{w} \in \Gamma$ na podstawie lematu 4.4. Wtedy również wektor $\bar{w}' := \bar{w} - \bar{e}_i + \bar{e}_j$ należy do Γ. Rozważmy następujące przypadki:

i) $h_1 = 1$. Z lematu 4.3 (2) otrzymujemy $\operatorname{supp} \bar{w}' = X \setminus \{i\} \cup \{j\} \in \Delta$. Zauważmy ponadto, że $U := X \cap (X \setminus \{i\} \cup \{j\}) = X \setminus \{i\} \notin \Delta$. Istotnie, mamy $U \subsetneq X$, więc gdyby $U \in \Delta$, otrzymalibyśmy sprzeczność z minimalnością zbioru X. Oczywiście $|U| = k-1$. Stosując lemat Csirmaza (2.21, 2) otrzymujemy kolejno:

$$h(U) + h(X \cup \{j\}) < h(X) + h(X \setminus \{i\} \cup \{j\}),$$

$$h_{k-1} + h_{k+1} < h_k + h_k,$$

$$h_{k+1} - h_k < h_k - h_{k-1},$$

$$g_k < g_{k-1}.$$

Korzystając z założeń oraz faktu, iż ciąg $\boldsymbol{g}$ jest nierosnący, otrzymujemy

$$1 \leqslant g_k < g_{k-1} \leqslant g_0 = h_1 = 1,$$

co stanowi sprzeczność.

ii) $h_1 > 1$. Na podstawie lematu 4.3 (4) istnieje taki minimalny wektor autoryzowany $\bar{v}$, że $\bar{v} \leqslant_s \bar{w}'$, $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{v})$ oraz $\operatorname{supp} \bar{v} \in \Delta$. Zauważmy, że $h_{|\operatorname{supp} \bar{v}|} = |\bar{v}_{\operatorname{supp} \bar{v}}| = |\bar{v}| \leqslant |\bar{w}'| = |\bar{w}| = h_k$, gdzie ostatnia równość wynika z lematu 2.28. Z założenia $g_k > 0$ wynika, że ciąg $(h_i)_{i=0,\ldots,k+1}$ jest silnie rosnący, stąd $|\operatorname{supp} \bar{v}| \leqslant k$.

Ponadto $\operatorname{supp} \bar{v} \subseteq X \cup \{j\}$, ponieważ $\operatorname{supp} \bar{w}' = X \cup \{j\}$. Zauważmy, że $j \in \operatorname{supp} \bar{v}$. Gdyby $j \notin \operatorname{supp} \bar{v}$, to $\operatorname{supp} \bar{v} = X$, ponieważ $X \in \min \Delta$. W tym przypadku $|\bar{v}| \leqslant |\bar{w}'_X| = |\bar{w}_X| - 1 = |\bar{w}| - 1 = h_k - 1 < h_k$, co jest sprzeczne z założeniem, że $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{v}) = \mathcal{B}(\mathcal{Z}, X)$.

Przyjmijmy $\operatorname{supp}\bar{v} =: \{j\} \dot{\cup} Y$ oraz $l := |Y|$. Oczywiście nośniki wektorów $\bar{w}'$ oraz $\bar{v}$ są różne, ponieważ $|\operatorname{supp}\bar{v}| \leqslant k$, natomiast $|\operatorname{supp}\bar{w}'| = k+1$, więc $l < k$. Zauważmy, że $Y = X \cap \operatorname{supp}\bar{v} \subsetneq X$, stąd $Y \notin \Delta$. Istotnie, gdyby $Y \in \Delta$, otrzymalibyśmy sprzeczność z minimalnością zbioru X. Stosując lemat Csirmaza (2.21, 2) otrzymujemy

$$h_l + h_{k+1} = h(Y) + h(X \cup \{j\}) < h(X) + h(Y \cup \{j\}) = h_k + h_{l+1}.$$

Stąd $g_k = h_{k+1} - h_k < h_{l+1} - h_l = g_l$, a dalej $g_l \geqslant 2$, bo $0 < g_k < g_l$. Z drugiej strony, z lematu 2.29 (1) zastosowanego do wektora $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{v})$ wynika, że $1 = w'_j = v_j \geqslant g_l$. Stąd otrzymujemy sprzeczność. □

Wniosek 4.8. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech ponadto Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $\{i\} \in \min\Delta$ dla pewnego $i \in J_m$ oraz $g_1 > 0$, to blok Π_i jest maksymalny w zbiorze $(\Pi, \preccurlyeq_\Gamma)$.

Dowód. Można zastosować bezpośrednio twierdzenie 4.7. Wynika z niego, że dla dowolnego $j \in J_m, j \neq i$, blok Π_i nie jest hierarchicznie podrzędny lub równoważny względem Π_j, a to oznacza, że blok Π_i jest maksymalny w zbiorze $(\Pi, \preccurlyeq_\Gamma)$. □

Wniosek 4.9. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech ponadto Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $X \in \min\Delta$, $1 \leqslant |X| =: k \leqslant m-1$, $j \in J_m \setminus X$ oraz $g_k > 0$, to blok Π_j jest minimalny w zbiorze $(\{\Pi_j\} \cup \{\Pi_i : i \in X\}, \preccurlyeq_\Gamma)$.

Dowód. Z twierdzenia 4.7 wynika, że Π_i nie jest hierarchicznie podrzędny lub równoważny względem Π_j dla każdego $i \in X$, a to oznacza, że blok Π_j jest minimalny w zbiorze wszystkich bloków indeksowanych elementami ze zbioru $X \cup \{j\}$. □

Aby móc badać dalej praporządek w zbiorze $(\Pi, \preccurlyeq_\Gamma)$, potrzebne będą następujące lematy i stwierdzenia.

Lemat 4.10. *Niech $\mathcal{Z} = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie rodziną monotoniczną z nim kompatybilną. Dalej, niech ciąg $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $g_1 = \ldots = g_{n-1} > 0$ dla pewnego $2 \leqslant n \leqslant m$ oraz $X, Y \in \min\Delta$ i $|X \cup Y| \leqslant n$, to $X = Y$ lub oba zbiory są jednoelementowe.

Dowód. Dla $n = 2$ teza jest oczywista. Załóżmy zatem, że $n \geqslant 3$. Wystarczy rozważyć przypadek, gdy $X \neq Y$. Załóżmy, że co najmniej jeden z tych zbiorów, na przykład X, ma co najmniej 2 elementy. Ustalmy $x \in X$ i rozważmy zbiór

$$Y' := \begin{cases} Y & \text{gdy } X \cap Y \neq \emptyset; \\ Y \cup \{x\} & \text{gdy } X \cap Y = \emptyset. \end{cases}$$

Zauważmy, że $|X \cup Y'| = |X \cup Y| \leqslant n$ oraz $W := X \cap Y' \neq \emptyset$. Ponadto W jest właściwym podzbiorem zbioru minimalnego X, więc nie należy do Δ. Zatem zgodnie z lematem Csirmaza (2.21, 2) otrzymujemy

$$h(W) + h(X \cup Y') < h(X) + h(Y').$$

Z drugiej strony z założenia oraz lematu 2.28 wynika, że $h_l = g_0 + (l-1)g_1$ dla $1 \leqslant l \leqslant n$. Stąd otrzymujemy kolejno:

$$h_{|W|} + h_{(|X|+|Y'|-|W|)} < h_{|X|} + h_{|Y'|},$$

$$g_0 + (|W|-1)g_1 + g_0 + (|X|+|Y'|-|W|-1)g_1 < g_0 + (|X|-1)g_1 + g_0 + (|Y'|-1)g_1.$$

Łatwo widać, że powyższe wyrażenie po uproszczeniu wynosi $0 < 0$, co daje sprzeczność. To pokazuje, że zbiory X i Y nie mogą mieć więcej niż po jednym elemencie. □

Lemat 4.11. *Niech $\mathcal{Z} = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie rodziną monotoniczną z nim kompatybilną. Dalej, niech ciąg $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $g_0 = g_1 = \ldots = g_{n-1} > 0$ dla pewnego $1 \leqslant n \leqslant m$ oraz $X, Y \in \min \Delta$ i $|X \cup Y| \leqslant n$, to $X = Y$.

Dowód. Przypuśćmy, że $X \neq Y$. Zauważmy, że w tym przypadku $W := X \cap Y$ jest właściwym podzbiorem zbiorów minimalnych więc nie należy do Δ. Zatem zgodnie z lematem Csirmaza (2.21, 2) mamy $h(W) + h(X \cup Y) < h(X) + h(Y)$.

Z drugiej jednak strony z założenia oraz lematu 2.28 wynika, że $h_l = lg_0$ dla $0 \leqslant l \leqslant n$. Stąd otrzymujemy kolejno:

$$h_{|W|} + h_{(|X|+|Y|-|W|)} < h_{|X|} + h_{|Y|},$$

$$|W|g_0 + (|X| + |Y| - |W|)g_0 < |X|g_0 + |Y|g_0.$$

Łatwo widać, że powyższe wyrażenie po uproszczeniu wynosi $0 < 0$, co daje sprzeczność. To pokazuje, że zbiory X i Y nie mogą być różne. □

Lemat 4.12. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech ponadto Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Załóżmy, że $g_1 = \cdots = g_k \geqslant g_{k+1} \geqslant \cdots \geqslant g_{n-1} > 0$ *dla pewnych* $3 \leqslant n \leqslant m$, $1 \leqslant k \leqslant n-2$ *oraz istnieje taki zbiór* $X \in \min \Delta$, $k = |X| \leqslant n-1$, *oraz takie* $i, j \in J_m$, $i \neq j$, *że* $|X \setminus \{i, j\}| \geqslant 1$. *Jeśli*

1. *bloki* Π_j *i* Π_i *są porównywalne w strukturze dostępu* Γ *i* $X \cap \{i, j\} \neq \emptyset$
   lub
2. *bloki* Π_j *i* Π_i *są porównywalne w strukturze dostępu* Γ *i* $g_0 = g_1$,

to $g_1 = \cdots = g_{n-1}$.

Dowód. Przypuśćmy nie wprost, że $g_1 = \cdots = g_k = \cdots = g_{l-1} > g_l$ dla pewnej liczby $k+1 \leqslant l \leqslant n-1$. Bez straty ogólności możemy przyjąć, że $\Pi_j \preccurlyeq_\Gamma \Pi_i$. Zauważmy, że $j \notin X$. Istotnie, gdyby $i, j \in X$, wówczas na podstawie twierdzenia 4.5 bloki Π_j oraz Π_i byłyby nieporównywalne. Gdyby $j \in X$, $i \notin X$, wówczas na podstawie twierdzenia 4.7 blok Π_j nie byłby hierarchicznie podrzędny lub równoważny względem bloku Π_i.

Niech zatem $Y \subseteq J_m \setminus \{j\}$ będzie zbiorem l-elementowym zawierającym zbiór X oraz element i. Ustalmy również element $x \in X \setminus \{i, j\}$.

Rozważmy taki wektor wierzchołkowy $\bar{w}$ rzędu $l+1$, że nośnikiem jego jest zbiór $Y \cup \{j\}$, $w_i = g_0 = h_1$ oraz $w_x = g_l$. Z przyjętych założeń wynika, że wszystkie pozostałe niezerowe współrzędne wektora $\bar{w}$ są równe g_1, w szczególności mamy $w_j = g_1$. Dla każdego $0 < z \leqslant l$ z lematu 2.28 otrzymujemy

$$h_z = \sum_{t=0}^{z-1} g_t = g_0 + (z-1)g_1. \tag{4.2}$$

Zauważmy, że $Y \cup \{j\} \in \Delta$, bo $X \subseteq Y \cup \{j\}$. Stąd $\bar{w} \in \Gamma$ na podstawie lematu 4.4. Ponadto $h_{l+1} = |\bar{w}| = h_1 + (l-1)g_1 + g_l$. Z tego, że $\Pi_j \preccurlyeq_\Gamma \Pi_i$ wynika, iż $\bar{w}' := \bar{w} - g_1\bar{e}_j + g_1\bar{e}_i$ należy do Γ. Zauważmy, że $\operatorname{supp} \bar{w}' = Y$. Zatem na podstawie lematu 4.3 (4) istnieje taki minimalny wektor autoryzowany $\bar{v}$, że $\bar{v} \leqslant_s \bar{w}'$, $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{v})$ i $W := \operatorname{supp} \bar{v} \in \Delta$. Oczywiście $W \subseteq Y$, więc $|W| \leqslant l$. Jeśli $x \in W$, to korzystając z lematu 2.29 (1) mamy $g_1 = g_{|W|-1} \leqslant v_x \leqslant w'_x = w_x = g_l$, gdy $|W| \geqslant 2$. W przypadku $|W| = 1$ mamy $\bar{v} = g_l\bar{e}_x$, a stąd $g_0 = h_1 = |\bar{v}| = g_l$. W obu przypadkach otrzymujemy sprzeczność z założeniem. Zatem $x \notin W$.

Zauważmy, że $X \cup W \subseteq Y$ oraz $X \cap W \subsetneq X$, ponieważ nie zawiera x. Ponadto $X \in \min \Delta$, stąd $X \cap W \notin \Delta$. Korzystając z lematu Csirmaza (2.21, 2) otrzymujemy

$$h_{|X \cap W|} + h_{(|X|+|W|-|X \cap W|)} < h_{|X|} + h_{|W|}.$$

Jeśli $g_0 = g_1$, to z (4.2) wynika, iż dla każdego $0 \leqslant z \leqslant l$ otrzymujemy $h_z = zg_0$. Stąd oraz faktu, że wszystkie indeksy nie przekraczają l otrzymujemy

$$|X \cap W|g_0 + (|X| + |W| - |X \cap W|)g_0 < |X|g_0 + |W|g_0,$$

co jest sprzecznością.

Rozpatrzmy przypadek $g_0 > g_1$ oraz $X \cap \{i,j\} \neq \emptyset$. Ponieważ $j \notin X$, stąd $i \in X$. Przypuśćmy, że $i \notin W$. Wtedy wszystkie współrzędne wektora $\bar{v}$ są ograniczone przez g_1 więc

$$g_0 + (|W| - 1)g_1 = h_{|W|} = |\bar{v}| \leqslant |W|g_1,$$

stąd $g_0 = g_1$ wbrew przyjętemu założeniu. To pokazuje, że $X \cap W$ zawiera i więc jest niepusty. Zgodnie z równością (4.2) otrzymujemy

$$g_0+(|X\cap W|-1)g_1+g_0+(|X|+|W|-|X\cap W|-1)g_1 < g_0+(|X|-1)g_1+g_0+(|W|-1)g_1,$$

co po uproszczeniu daje sprzeczność.

W ten sposób pokazaliśmy, że przypuszczenie $g_{l-1} > g_l$ dla pewnej liczby $k+1 \leqslant l \leqslant n-1$ prowadzi do sprzeczności, co kończy dowód. □

Stwierdzenie 4.13. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Załóżmy, że $g_{n-1} > 0$ dla pewnego $3 \leqslant n \leqslant m$ oraz istnieje taki zbiór $X \in \min\Delta$, że $1 \leqslant |X| \leqslant n-2$. Jeśli istnieją takie $i,j \in J_m \setminus X$, że bloki Π_i oraz Π_j są porównywalne w strukturze dostępu Γ, to $g_0 = g_1 = \cdots = g_{n-1}$.

Dowód. Jeśli $h_1 = 1$, to zauważmy, że

$$1 = h_1 = g_0 \geqslant g_1 \geqslant \cdots \geqslant g_{n-1} \geqslant 1.$$

Stąd $g_0 = g_1 = \cdots = g_{n-1}$.

Dalej zakładamy, że $h_1 \geqslant 2$. Niech $X \in \min\Delta$, $1 \leqslant k := |X| \leqslant n-2$ oraz $i,j \in J_m \setminus X$. Jeśli bloki Π_i i Π_j są porównywalne, to bez straty ogólności możemy założyć, że blok Π_j jest hierarchicznie podrzędny lub równoważny względem Π_i.

Rozważmy taki wektor wierzchołkowy $\bar{w}$ rzędu $k+1$, którego nośnikiem jest zbiór $X \cup \{j\}$, że $w_j = g_0 = h_1$. Oczywiście $\bar{w} \in \Gamma$ na podstawie lematu 4.4. Wtedy również wektor $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_i$ należy do Γ oraz $\operatorname{supp}\bar{w}' = X \cup \{i,j\}$. Zatem na podstawie lematu 4.3 (4) istnieje taki minimalny wektor autoryzowany $\bar{v}$, że $\bar{v} \leqslant_s \bar{w}$, $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{v})$ i $\operatorname{supp}\bar{v} \in \Delta$. Zauważmy, że $\operatorname{supp}\bar{v} \subseteq X \cup \{i,j\}$, $v_i \leqslant w'_i = 1$ oraz $v_j \leqslant w'_j = h_1 - 1$. Oznaczmy $W := \operatorname{supp}\bar{v} \cap X$ i $|W| =: l$. Rozważmy cztery przypadki:

i) $i,j \notin \operatorname{supp}\bar{v}$. Wówczas $\operatorname{supp}\bar{v} \subseteq X$. Z założenia $X \in \min\Delta$, stąd $\operatorname{supp}\bar{v} = X$ oraz, na podstawie lematu 2.28, otrzymujemy

$$h_k = |\bar{v}| \leqslant |\bar{w}'_X| = |\bar{w}_X| = \sum_{t=1}^{k} g_t = h_{k+1} - g_0,$$

zatem $g_0 \leqslant h_{k+1} - h_k = g_k$. Ciąg $\boldsymbol{g}$ jest nierosnący, więc $g_0 = g_1 = \cdots = g_k$.

ii) $\operatorname{supp}\bar{v} = W \cup \{j\}$. Wówczas

$$h_{l+1} = |\bar{v}| \leqslant (h_1 - 1) + |\bar{w}'_W| = (h_1 - 1) + |\bar{w}_W|.$$

Zauważmy, że na współrzędnych wektora $\bar{w}_W$ znajduje się l elementów ze zbioru $\{g_0, g_1, \ldots, g_k\}$, wśród których nie ma $g_0 = h_1$, ponieważ ta wartość jest na współrzędnej j wektora $\bar{w}$, ale $j \notin W$. Zastosujmy do ciągu $(g_1, \ldots, g_k)$ fakt, że suma l dowolnych wyrazów ciągu nierosnącego jest mniejsza bądź równa sumie l początkowych wyrazów tego ciągu. Kontynuując rachunek i korzystając z lematu 2.28 otrzymujemy

$$h_{l+1} \leqslant (h_1 - 1) + |\bar{w}_W| \leqslant (h_1 - 1) + \sum_{t=1}^{l} g_t = (g_0 - 1) + \sum_{t=1}^{l} g_t = h_{l+1} - 1,$$

co jest sprzecznością.

iii) $\operatorname{supp}\bar{v} = W \cup \{i\}$. Wówczas

$$h_{l+1} = |\bar{v}| \leqslant 1 + |\bar{w}'_W| = 1 + |\bar{w}_W|.$$

Powołując się na ten sam argument co w poprzednim przypadku otrzymujemy

$$h_{l+1} \leqslant 1 + |\bar{w}_W| \leqslant 1 + \sum_{t=1}^{l} g_t = 1 + h_{l+1} - g_0 = h_{l+1} - (h_1 - 1),$$

co jest sprzecznością, bo $h_1 > 1$.

iv) $\operatorname{supp}\bar{v} = W \cup \{i, j\}$. Wówczas

$$h_{l+2} = |\bar{v}| \leqslant (h_1 - 1) + 1 + |\bar{w}'_W| = h_1 + |\bar{w}_W|.$$

Powołując się na ten sam argument co w drugim przypadku otrzymujemy

$$h_{l+2} \leqslant h_1 + |\bar{w}_W| \leqslant h_1 + \sum_{t=1}^{l} g_t = g_0 + \sum_{t=1}^{l} g_t = h_{l+1}.$$

Otrzymana nierówność $h_{l+2} \leqslant h_{l+1}$ pokazuje, że

$$g_{n-1} \leqslant g_{l+1} = h_{l+2} - h_{l+1} \leqslant 0,$$

co jest sprzeczne z założeniem.

W ten sposób wykazaliśmy, że przypadki ii), iii) oraz iv) prowadzą do sprzeczności. Natomiast z przypadku i) wynika, że $g_0 = g_1 = \cdots = g_k$ dla pewnego $k \in \{1, \ldots, n-2\}$. Aby zakończyć dowód wystarczy zastosować lemat 4.12. □

Stwierdzenie 4.14. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Załóżmy, że $g_{n-1} > 0$ dla pewnego $3 \leqslant n \leqslant m$ oraz istnieje taki zbiór $X \in \min\Delta$, że $2 \leqslant |X| \leqslant n-1$. Jeśli istnieją takie $i \in X$, $j \in J_m \setminus X$, że bloki Π_i i Π_j są porównywalne w strukturze dostępu Γ, to $g_1 = \cdots = g_{n-1}$.

Dowód. Niech $X \in \min \Delta$, $2 \leqslant k := |X| \leqslant n-1$, $i \in X$, $j \in J_m \setminus X$. Z tego, że $g_{n-1} > 0$, wynika $g_k > 0$ dla wszystkich $k \in \{2, \ldots, n-1\}$. Jeśli bloki Π_i i Π_j są porównywalne, to z twierdzenia 4.7 wynika, że blok Π_j jest hierarchicznie podrzędny względem bloku Π_i.

Rozważmy taki wektor wierzchołkowy $\bar{w}$ rzędu $k+1$, którego nośnikiem jest zbiór $X \cup \{j\}$, że $w_i = g_0 = h_1$ oraz $w_j = g_1$. Oczywiście $\bar{w} \in \Gamma$ na podstawie lematu 4.4. Wtedy również wektor $\bar{w}' := \bar{w} - g_1\bar{e}_j + g_1\bar{e}_i$ należy do Γ oraz $\operatorname{supp} \bar{w}' = X$. Zatem na lematu 4.3 (4) istnieje taki minimalny wektor autoryzowany $\bar{v}$, że $\bar{v} \leqslant_s \bar{w}$, $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{v})$ i $\operatorname{supp} \bar{v} \in \Delta$. Zauważmy, że $\operatorname{supp} \bar{v} = X$ bo $\operatorname{supp} \bar{v} \subseteq \operatorname{supp} \bar{w} = X \in \min \Delta$. Ponadto $v_i \leqslant h_1$ oraz $v_x \leqslant w'_x = w_x$ dla $x \in X$, $x \neq i$. Stąd oraz lematu 2.28 otrzymujemy

$$h_k = |\bar{v}| \leqslant |\bar{w}_X| = g_0 + \sum_{t=2}^{k} g_t = \sum_{t=0}^{k} g_t - g_1 = h_{k+1} - g_1.$$

Zatem $g_1 \leqslant h_{k+1} - h_k = g_k$. Ponieważ ciąg $\boldsymbol{g}$ jest nierosnący, więc $g_1 = g_k$, stąd oczywiście $g_1 = g_2 = \cdots = g_{k-1} = g_k$. Aby zakończyć dowód wystarczy zastosować lemat 4.12. □

Lemat 4.15. *Niech $\mathcal{Z} = (J_m, h)$ będzie polimatroidem jednorodnym, niech $X \subseteq J_m$, $i, j \in X$, $i \neq j$, oraz niech $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$.*

Jeśli $w_j > 0$, to wektor $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_i$ należy do $\mathcal{B}(\mathcal{Z}, X)$ lub istnieje taki zbiór $Y \subseteq X \setminus \{j\}$, $i \in Y$, że $\bar{v} := \bar{w}_Y \in \mathcal{B}(\mathcal{Z}, Y)$. Ponadto $\bar{v} \leqslant \bar{w}$ oraz $\bar{v} \leqslant \bar{w}'$.

Dowód. Zauważmy, że $\operatorname{supp} \bar{w}' \subseteq X$ oraz $|\bar{w}'_X| = |\bar{w}_X| = h(X) = h_{|X|}$. Wystarczy rozważyć przypadek $\bar{w}' \notin \mathcal{B}(\mathcal{Z}, X)$, to znaczy istnieje taki zbiór $Y \subseteq X$, że $|\bar{w}'_Y| \geqslant h(Y)+1$. Wybierzmy minimalny zbiór Y o tej własności. Łatwo zauważyć, że $i \in Y$ oraz $j \notin Y$. Przyjmując oznaczenie $l := |Y|$, otrzymujemy kolejno:

$$(w_i + 1) + \sum_{t \in Y \setminus \{i\}} w_t \geqslant h_l + 1,$$

$$w_i + \sum_{t \in Y \setminus \{i\}} w_t \geqslant h_l,$$

$$|\bar{w}_Y| \geqslant h_l.$$

Stąd oraz założenia $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$ wynika, że $|\bar{w}_Y| = h_l$. Przyjmujemy $\bar{v} := \bar{w}_Y$. Wobec powyższego otrzymujemy $\bar{v} \in \mathcal{B}(\mathcal{Z}, Y)$. Łatwo sprawdzić, że $\bar{v} \leqslant_s \bar{w}$ oraz $\bar{v} \leqslant_s \bar{w}'$, co kończy dowód. □

Lemat 4.16. *Niech $\mathcal{Z} = (J_m, h)$ będzie polimatroidem jednorodnym, niech $X \subseteq J_m$, $j \in X$, $i \in J_m \setminus X$, oraz niech $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $g_{k-1} > g_k = \cdots = g_{m-1} = g_m = 0$ dla pewnego $1 \leqslant k \leqslant m-1$ oraz $|X| \geqslant k$ i $w_j > 0$, to $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_i \in \mathcal{B}(\mathcal{Z}, X \cup \{i\})$.

Dowód. Zauważmy, że $\operatorname{supp} \bar{w}' \subseteq X \cup \{i\}$ oraz $w'_i = 1$, $w'_j = w_j - 1$. Pokażemy, że dla każdego $Y \subseteq X \cup \{i\}$ otrzymujemy $|\bar{w}'_Y| \leqslant h_{|Y|}$. Rozważmy następujące przypadki, w każdym korzystając z tego, że $\bar{w} \in \mathcal{B}(\mathcal{Z}, X)$:

i) $j \in Y$, $i \in Y$. Wówczas

$$|\bar{w}'_Y| = |\bar{w}_{Y \setminus \{i\}}| \leqslant h_{|Y \setminus \{i\}|} \leqslant h_{|Y|}.$$

ii) $j \in Y$, $i \notin Y$. Wówczas

$$|\bar{w}'_Y| \leqslant |\bar{w}_Y| \leqslant h_{|Y|}.$$

iii) $j \notin Y$, $i \notin Y$. Wówczas

$$|\bar{w}'_Y| = |\bar{w}_Y| \leqslant h_{|Y|}.$$

iv) $j \notin Y$, $i \in Y$. Wówczas

$$|\bar{w}'_Y| \leqslant |\bar{w}_{Y \setminus \{i\} \cup \{j\}}| \leqslant h_{|Y|}.$$

Aby zakończyć dowód tego, że $\bar{w}' \in \mathcal{B}(\mathcal{Z}, X \cup \{i\})$, należy jeszcze wykazać, iż $|\bar{w}'_{X \cup \{i\}}| = h_{|X|+1} = h(X \cup \{i\})$. Zauważmy, że z założenia otrzymujemy $g_{|X|} = 0$, stąd $h_{|X|} = h_{|X|+1} - g_{|X|} = h_{|X|+1}$ oraz

$$|\bar{w}'_{X \cup \{i\}}| = |\bar{w}_X| = h_{|X|} = h_{|X|+1} = h(X \cup \{i\}). \qquad \square$$

Lemat 4.17. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Załóżmy, że zbiór jednoelementowy zawierający k należy do $\min \Delta$ dla pewnego $k \in J_m$ oraz $g_{m-2} > g_{m-1} = 0$. Jeśli $\bar{w} \in \min \Gamma$ oraz $k \in \operatorname{supp} \bar{w}$ lub $J_m \setminus \{k\} \subseteq \operatorname{supp} \bar{w}$, to $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_k \in \Gamma$ dla dowolnego $j \in \operatorname{supp} \bar{w}$.

Dowód. Rozważmy dowolny taki wektor $\bar{w} \in \min \Gamma$, że $w_j > 0$. Wówczas na podstawie lematu 4.3 (3) otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ i $\operatorname{supp} \bar{w} \in \Delta$. W związku z założeniami możemy rozważyć dwa przypadki:

i) $k \in \operatorname{supp} \bar{w}$. Z lematu 4.15 wynika, że $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_k \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ lub istnieją taki zbiór $Y \subseteq \operatorname{supp} \bar{w} \setminus \{j\}$, $k \in Y$, oraz taki wektor $\bar{v} \in \mathcal{B}(\mathcal{Z}, Y)$, że $\bar{v} \leqslant_s \bar{w}'$. Jeśli zachodzi pierwsza możliwość, to z lematu 4.3 (1) otrzymujemy $\bar{w}' \in \Gamma$. Jeśli zachodzi druga możliwość, to zauważmy, że $Y \in \Delta$, więc z lematu 4.3 (1) otrzymujemy $\bar{v} \in \Gamma$, stąd $\bar{w}' \in \Gamma$. Ten przypadek obejmuje także sytuację, gdy $\operatorname{supp} \bar{w} = J_m$.

ii) $\operatorname{supp} \bar{w} = J_m \setminus \{k\}$. Zauważmy, że na podstawie lematu 4.16 otrzymujemy $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_k \in \mathcal{B}(\mathcal{Z}, J_m)$. Ponieważ $J_m \in \Delta$, korzystamy z lematu 4.3 (1) i otrzymujemy $\bar{w}' \in \Gamma$. $\square$

Znaczna większość twierdzeń w tym podrozdziale w swojej wypowiedzi ma standardowy zestaw założeń. Poniższy lemat stanowi wyjątek od tej reguły.

Lemat 4.18. *Niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$, $m \geqslant 3$, *będzie podziałem zbioru uczestników* P. *Niech* $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ *będzie polimatroidem jednorodnym oraz niech* $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ *będzie ciągiem wyznaczonym przez polimatroid* $\mathcal{Z}$. *Niech* $\Delta \subsetneq \mathcal{P}(J_m)$ *będzie rodziną monotoniczną oraz niech* $k \in X \neq J_m$, $Y = J_m \setminus \{k\}$ *dla pewnego* $k \in J_m$.

Jeśli $g_{m-2} > g_{m-1} = 0$, X, $Y \in \Delta$ *oraz* $X \cap Y \notin \Delta$, *to*

$$h(X \cap Y) + h(X \cup Y) < h(X) + h(Y).$$

Dowód. Niech $\{k\} \subseteq X \neq J_m$ oraz $Y = J_m \setminus \{k\}$. Wówczas $|X \cup Y| = J_m$, $|X \cap Y| < |X| \leqslant m - 1$. Stąd, korzystając z założenia oraz lematu 2.28, kolejno otrzymujemy:

$$0 = g_{m-1} < g_{m-2} \leqslant g_{|X\cap Y|} \leqslant g_{|X\cap Y|} + \cdots + g_{|X|-1},$$

$$h_m - h_{m-1} < h_{|X|} - h_{|X\cap Y|},$$

$$h_{|X\cap Y|} + h_m < h_{|X|} + h_{m-1},$$

$$h_{|X\cap Y|} + h_{|X\cup Y|} < h_{|X|} + h_{|Y|},$$

$$h(X \cap Y) + h(X \cup Y) < h(X) + h(Y),$$

co kończy dowód. □

4.3 Hierarchiczne struktury dostępu wyznaczone przez polimatroidy jednorodne

Po wprowadzeniu niezbędnych lematów i stwierdzeń możemy przystąpić do badania hierarchiczności struktur dostępu wyznaczonych przez pewne polimatroidy jednorodne $\mathcal{Z} = (J_m, h)$ i kompatybilne z nimi rodziny monotoniczne $\Delta \subsetneq \mathcal{P}(J_m)$. Metody wyznaczania porządku hierarchicznego w strukturach dostępu w znacznym stopniu zależą od sygnatury ciągu $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ wyznaczonego przez polimatroid, a dokładniej od liczby $\max\{l \ : \ \sigma_l = 1\} = \max\{l \ : \ g_l > 0\}$. Jednak we wszystkich przypadkach można stosować podobną taktykę. Najpierw znajdujemy warunki konieczne istnienia bloków porównywalnych. Następnie pokazujemy, że te warunki są również wystarczające i wyznaczamy typy porządkowe poszczególnych struktur. Takie postępowanie daje dodatkowy efekt w postaci dowodu, że we wszystkich pozostałych przypadkach mamy do czynienia z oddziałowymi strukturami dostępu, w których uporządkowanie bloków jest antyliniowe.

Jak już wspomnieliśmy na początku tego rozdziału, tabele 4.1, 4.2 oraz 4.3 znajdujące się w podrozdziale 4.4, prezentują przykłady zastosowań otrzymanych

wyników dla odpowiednio $m = 2$, $m = 3$ i $m = 4$. Wiersze tabel odpowiadają wszystkim możliwym postaciom zbioru $\min \Delta$ z dokładnością do permutacji zbioru J_m, natomiast kolumny prezentują wszystkie możliwe ciągi $\boldsymbol{g}$ z dokładnością do sygnatury. Jak wiemy z rozdziału 2, w przypadku badania kompatybilności rodziny monotonicznej oraz polimatroidu jednorodnego Δ nie są istotne ani wartości funkcji rangi ani wartości ciągu $\boldsymbol{g}$ wyznaczonego przez $\mathcal{Z}$, lecz jedynie sygnatura ciągu $\boldsymbol{g}$. W podanych tabelach na przecięciu się wiersza i kolumny w odpowiedniej komórce są możliwe 2 przypadki:

i) jeśli widnieje symbol „–", oznacza to, że rodzina monotoniczna Δ nie jest kompatybilna z polimatroidem jednorodnym $\mathcal{Z}$, który wyznacza ciąg $\boldsymbol{g}$.

ii) jeśli widnieje pewna litera, oznacza to, że rodzina monotoniczna Δ jest kompatybilna z polimatroidem jednorodnym $\mathcal{Z}$, który wyznacza ciąg $\boldsymbol{g}$. Ponadto struktura hierarchiczna Γ wyznaczona przez polimatroid $\mathcal{Z}$ oraz rodzinę Δ charakteryzuje się hierarchicznością opisaną według legendy. Wykażemy, że dla $m = 2$, $m = 3$ i $m = 4$ na hierarchiczność struktury Γ nie mają wpływu wartości funkcji rangi ani wartości ciągu $\boldsymbol{g}$ wyznaczonego przez $\mathcal{Z}$, lecz jedynie sygnatura ciągu $\boldsymbol{g}$. Innymi słowy ustalona kolumna reprezentuje wszystkie polimatroidy, których sygnatura ciągu $\boldsymbol{g}$ jest równa sygnaturze ciągu widniejącego w nagłówku danej kolumny.

Po każdym twierdzeniu warto porównać tezy twierdzenia z wynikami zawartymi w tabelach.

Przypadek $g_{m-1} > 0$

W tym przypadku twierdzenie 4.19 zawiera warunki konieczne, na to aby pewne bloki uczestników w wielodzielnej strukturze dostępu były porównywalne. Następnie w twierdzeniach 4.22, 4.23 i 4.24 badamy szczegółowo strukturę hierarchiczną bloków we wszystkich przypadkach, gdy dla ciągu $\boldsymbol{g}$ wyznaczonego przez polimatroid $\mathcal{Z}$ i rodziny monotonicznej Δ kompatybilnej z $\mathcal{Z}$ spełnione są warunki konieczne.

Twierdzenie 4.19. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $g_{m-1} > 0$ oraz istnieją w zbiorze Π dwa różne bloki, które są porównywalne w strukturze dostępu Γ, to $g_1 = \ldots = g_{m-1}$ lub $\min \Delta = \{\{k\}\}$ dla pewnego $k \in J_m$.

Dowód. Załóżmy, że istnieją takie $i, j \in J_m$, że bloki Π_i i Π_j są porównywalne. Oczywiście nie może się zdarzyć, że $i, j \in X$ dla pewnego $X \in \min \Delta$, ponieważ Π_i i Π_j byłyby nieporównywalne na podstawie twierdzenia 4.5.

Jeśli $i, j \notin X$ dla pewnego $X \in \min \Delta$, to zgodnie ze stwierdzeniem 4.13 zastosowanym dla $n := m$ otrzymujemy $g_0 = g_1 = \ldots = g_{m-1}$.

Jeśli nie istnieje taki zbiór należący do $\min \Delta$, który nie zawiera i oraz j, to bez straty ogólności możemy założyć, że $i \in X$ oraz $j \notin X$ dla pewnego zbioru $X \in \min \Delta$. Jeśli $|X| \geqslant 2$, to zgodnie ze stwierdzeniem 4.14 zastosowanym dla $n := m$ otrzymujemy $g_1 = \ldots = g_{m-1}$. Jeśli $|X| = 1$, to $\min \Delta = \{\{i\}\}$, ponieważ w przeciwnym razie oba elementy i oraz j byłyby poza pewnym minimalnym zbiorem autoryzowanym, a ten przypadek teraz wykluczamy. □

Zauważmy, że jeśli $g_{m-1} > 0$, to z powyższego twierdzenia wynika, iż analizując tabele 4.2 oraz 4.3, struktur nie będących oddziałowymi należy spodziewać się w pierwszym wierszu lub dwóch ostatnich kolumnach. W przypadku tabeli 4.1 zastosowanie powyższego twierdzenia dotyczy tylko pierwszego wiersza i ostatniej kolumny.

Aby opisać praporządek w zbiorze Π, wprowadzamy oznaczenia $Ord_\Gamma(A, B)$ oraz $Ord^*_\Gamma(A, B)$ które definiujemy następująco.

Definicja 4.20. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech A i B będą rozłącznymi podzbiorami zbioru J_m. Stwierdzenie, że *uporządkowanie zbioru* $(\Pi, \preccurlyeq_\Gamma)$ *jest typu* $Ord_\Gamma(A, B)$ oznacza, że żadne dwa różne bloki nie są hierarchicznie równoważne w strukturze dostępu Γ oraz

$$\Pi_j \prec_\Gamma \Pi_i \iff j \in A, i \in B.$$

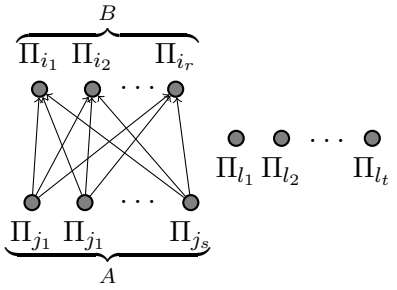
Można zauważyć, że jeśli zbiór A lub B jest pusty, to otrzymujemy praporządek $Ord_\Gamma(A, B)$, w którym każde dwa bloki są nieporównywalne.

Definicja 4.21. Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P oraz niech A i B będą rozłącznymi podzbiorami zbioru J_m. Stwierdzenie, że *uporządkowanie zbioru* $(\Pi, \preccurlyeq_\Gamma)$ *jest typu* $Ord^*_\Gamma(A, B)$ oznacza, że wszystkie bloki w zbiorze A są parami hierarchicznie równoważne w strukturze dostępu Γ, pozostałe bloki nie są parami hierarchicznie równoważne w strukturze dostępu Γ oraz

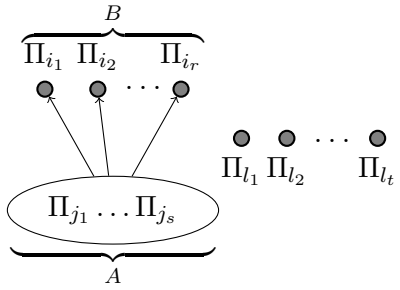
$$\Pi_j \prec_\Gamma \Pi_i \iff j \in A, i \in B.$$

Można zauważyć, że jeśli zbiór A jest pusty, to otrzymujemy praporządek $Ord^*_\Gamma(\emptyset, B)$, w którym każde dwa bloki są nieporównywalne. Jeśli natomiast zbiór B jest pusty, to otrzymujemy praporządek $Ord^*_\Gamma(A, \emptyset)$, w którym każde dwa bloki są porównywalne. Warte uwagi jest także spostrzeżenie, że jeśli $|A| \leqslant 1$, to $Ord_\Gamma(A, B) = Ord^*_\Gamma(A, B)$.

Tak zdefiniowane praporządki można przedstawić w postaci diagramów Hassego.



Uporządkowanie typu $Ord_\Gamma(A, B)$.



Uporządkowanie typu $Ord^*_\Gamma(A, B)$.

Poniższe twierdzenie opisuje hierarchiczność struktur dostępu wyznaczonych przez polimatroidy, dla których $g_0 = g_1 = \cdots = g_{m-1} > 0$, oraz rodziny z nimi kompatybilne. To twierdzenie szczegółowo wyjaśnia hierarchiczności struktur dostępu znajdujących się w ostatniej kolumnie każdej z tabel.

Twierdzenie 4.22. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Załóżmy, że $g_0 = g_1 = \cdots = g_{m-1} > 0$.*

1. *Wówczas rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy $\min \Delta = \{X\}$ dla pewnego $X \subseteq J_m$.*

2. *Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid $\mathcal{Z}$ i taką rodzinę monotoniczną $\Delta \subset \mathcal{P}(J_m)$, że $\min \Delta = \{X\}$ dla pewnego $X \subseteq J_m$. Wtedy:*

   a) *Wektor $\sum_{k \in X} h_1 \bar{e}_k$ jest jedynym minimalnym wektorem autoryzowanym w strukturze dostępu Γ.*

   b) *Uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(J_m \setminus X, X)$.*

Dowód. 1. Posłużmy się lematem 4.11 przyjmując $n := m$, z którego wynika, że gdy rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$, to $\min \Delta$ zawiera dokładnie jeden zbiór. Aby wykazać implikację odwrotną, wystarczy powołać się na lemat 2.36 (3).

2 a) Weźmy dowolny zbiór $Y \in \Delta$ oraz dowolny wektor $\bar{w} \in \mathcal{B}(\mathcal{Z}, Y)$ i zastosujmy lemat 2.29 (1). Jeśli $l := |Y|$, to dla każdego $z \in Y$ otrzymujemy

$$h_1 \geqslant w_z \geqslant g_{l-1} = g_0 = h_1 \Longrightarrow w_z = h_1.$$

Ponieważ $X \subseteq Y$, stąd $\bar{w} \geqslant \sum_{k \in X} h_1 \bar{e}_k$ dla każdego zbioru $Y \in \Delta$ oraz każdego wektora $\bar{w} \in \mathcal{B}(\mathcal{Z}, Y)$. To pokazuje, że wektor $\sum_{k \in X} h_1 \bar{e}_k$ jest jedynym minimalnym wektorem autoryzowanym.

2 b) Na wstępie zauważmy, że zgodnie ze stwierdzeniem 4.5 bloki indeksowane elementami należącymi do zbioru X są nieporównywalne. Gdy $X = J_m$, to w zbiorze Π każde dwa bloki są nieporównywalne, a więc uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(\emptyset, J_m)$.

Teraz zakładamy, że $|X| < m$. Rozważmy przypadki:

i) $i \in X$, $j \notin X$. Zgodnie z wnioskiem 4.9 bloki Π_j oraz Π_i są nieporównywalne albo $\Pi_j \prec_\Gamma \Pi_i$. Wykażemy, że $\Pi_j \preccurlyeq_\Gamma \Pi_i$. Korzystając z punktu a) oraz biorąc pod uwagę fakt, iż $j \notin X$ otrzymujemy, że taki wektor $\bar{w}$, dla którego $w_j > 0$ oraz $\bar{w} \in \min \Gamma$, nie istnieje. Stosując uwagę 3.28 otrzymujemy $\Pi_j \preccurlyeq_\Gamma \Pi_i$.

ii) $i, j \notin X$. Zgodnie z powyższym punktem a) otrzymujemy, że wektor $\sum_{k \in X} h_1 \bar{e}_k$ jest jedynym minimalnym wektorem autoryzowanym. Biorąc pod uwagę fakt, iż $i, j \notin X$ otrzymujemy, że taki wektor $\bar{w} \in \min \Gamma$, dla którego $w_i > 0$ lub $w_j > 0$, nie istnieje. Stosując uwagę 3.28 otrzymujemy, że bloki Π_j i Π_i są hierarchicznie równoważne.

W ten sposób pokazaliśmy, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(J_m \setminus X, X)$. □

Analogicznie do poprzedniego twierdzenia, poniższe twierdzenie opisuje hierarchiczność struktur dostępu wyznaczonych przez polimatroidy, dla których mamy $g_0 > g_1 = \cdots = g_{m-1} > 0$, oraz rodziny z nimi kompatybilne. To twierdzenie szczegółowo wyjaśnia hierarchiczności struktur dostępu znajdujących się w przedostatniej kolumnie każdej z tabel.

Twierdzenie 4.23. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Załóżmy, że $g_0 > g_1 = \cdots = g_{m-1} > 0$.*

1. *Wówczas rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy $\min \Delta = \{X\}$ dla pewnego $X \subseteq J_m$ lub $\min \Delta = \{\{k\} : k \in J_m\}$.*

2. *Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid $\mathcal{Z}$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Wtedy:*

   a) *Jeśli $\min \Delta = \{X\}$ dla pewnego $X \subseteq J_m$, to uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(J_m \setminus X, X)$.*

   b) *Jeśli $\min \Delta = \{\{k\} : k \in J_m\}$, to uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\emptyset, J_m)$.*

Dowód. 1. Niech X, Y będą dowolnymi zbiorami minimalnymi w Δ. Zgodnie z lematem 4.10, zastosowanym do $n := m$, jeśli te zbiory są różne, to muszą być jednoelementowe. Zatem jeśli Δ zawiera więcej niż jeden zbiór minimalny, to każdy zbiór minimalny jest jednoelementowy.

Załóżmy więc, że Δ zawiera więcej niż jeden zbiór minimalny. W związku z powyższym $\{a\}, \{b\} \in \min \Delta$ dla pewnych $a, b \in J_m$.

Przypuśćmy, że nie wszystkie zbiory jednoelementowe należą do $\min \Delta$, to znaczy istnieje takie $k \in J_m$, że $\{k\} \notin \min \Delta$. Oczywiście $\{a,k\}, \{b,k\} \in \Delta$, ale $(\{a\} \cup \{k\}) \cap (\{b\} \cup \{k\}) = \{k\} \notin \Delta$. Stosując lemat Csirmaza (2.21, 2) do zbiorów $\{a,k\}$ oraz $\{b,k\}$ otrzymujemy kolejno:

$$h(\{k\}) + h(\{a,b,k\}) < h(\{a,k\}) + h(\{b,k\}),$$

$$h_3 - h_2 < h_2 - h_1 \Longrightarrow g_2 < g_1,$$

stąd sprzeczność. Aby wykazać implikację odwrotną, rozważmy dwa przypadki:

i) $\min \Delta = \{X\}$ dla pewnego $X \subseteq J_m$. Tu wystarczy powołać się na lemat 2.36 (3).

ii) $\min \Delta = \{\{k\} : k \in J_m\}$, to znaczy każdy niepusty podzbiór zbioru J_m należy do Δ. W świetle lematu 2.36 (1) wystarczy sprawdzić, że warunek 2 lematu Csirmaza (2.21) jest spełniony. Weźmy zatem takie zbiory $W, Y \in \Delta$, że $W \cap Y \notin \Delta$. Oznacza to, że $W \cap Y = \emptyset$. Z przyjętych założeń oraz lematu 2.28 dla $l > 0$ mamy $h_l = g_0 + (l-1)g_1$. Przyjmijmy oznaczenia $s = |W|,\ r = |Y|$, stąd

$$\begin{aligned} h(W \cup Y) &= h_{s+r} = g_0 + (s+r-1)g_1 = \\ &= g_0 + (s-1)g_1 + g_0 + (r-1)g_1 - (g_0 - g_1) \\ &= h_s + h_r - (g_0 - g_1) < h(W) + h(Y). \end{aligned}$$

Ostatnia nierówność wynika z faktu, że $g_0 - g_1 > 0$.

2 a) Przyjmijmy $\min \Delta = \{X\}$ dla pewnego $X \subseteq J_m$. Fakt, że Π_i, Π_j dla $i, j \in X$ są nieporównywalne wynika wprost ze stwierdzenia 4.5. Jeśli $X = J_m$, to uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\emptyset, J_m)$.

Dalej możemy założyć, że $|X| < m$. Rozważmy $i \in X$ oraz $j \notin X$. Zgodnie z wnioskiem 4.9 bloki Π_j oraz Π_i są nieporównywalne albo $\Pi_j \prec_\Gamma \Pi_i$. Wykażemy, że $\Pi_j \preccurlyeq_\Gamma \Pi_i$. Niech $\bar{w}$ będzie takim wektorem minimalnym w Γ, że $w_j \neq 0$. Jeśli taki wektor nie istnieje, to na postawie uwagi 3.28 otrzymujemy $\Pi_j \preccurlyeq_\Gamma \Pi_i$. Jeśli taki wektor istnieje, to z lematu 4.3 (3) mamy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ i $\operatorname{supp} \bar{w} \in \Delta$, więc $X \subseteq \operatorname{supp} \bar{w}$, w szczególności $i \in \operatorname{supp} \bar{w}$. Zauważmy, że $|\operatorname{supp} \bar{w}| \geqslant 2$, ponieważ $j, i \in \operatorname{supp} \bar{w}$. Zgodnie z lematem 2.29 (1), przyjmując $k := |\operatorname{supp} \bar{w}|$, otrzymujemy $w_j \geqslant g_{k-1}$ Z założenia $g_{k-1} = g_1$, stąd możemy rozważyć dwa przypadki:

i) $w_j = g_1$, więc zgodnie z lematem 2.29 (2) $\bar{v} := \bar{w} - w_j \bar{e}_j \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w} \setminus \{j\})$, ale $X \subseteq \operatorname{supp} \bar{w} \setminus \{j\}$, więc z lematu 4.3 (1) otrzymujemy $\bar{v} \in \Gamma$. Wtedy oczywiście $\bar{v} \leqslant_s \bar{w} - \bar{e}_j + \bar{e}_i =: \bar{w}'$, stąd $\bar{w}' \in \Gamma$.

ii) $w_j > g_1$ i oznaczmy $W := \operatorname{supp} \bar{w}$. Zgodnie z lematem 4.15 otrzymujemy $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_i \in \mathcal{B}(\mathcal{Z}, W)$ lub istnieje taki zbiór $Y \subseteq W \setminus \{j\},\ i \in Y$, że

$\bar{v} := \bar{w}_Y \in \mathcal{B}(\mathcal{Z}, Y)$ i $\bar{v} \leqslant_s \bar{w}$, $\bar{v} \leqslant_s \bar{w}'$. W szczególności mamy $|\bar{w}_Y| = |\bar{v}| = h_{|Y|}$. Przedstawmy $W = Y \cup Z \cup \{j\}$ w postaci sumy trzech zbiorów rozłącznych, gdzie $Z = W \setminus (Y \cup \{j\})$. Wtedy na podstawie lematu 2.29 (1) oraz założeń otrzymujemy, że każda współrzędna wektora $\bar{w}$ wynosi co najmniej g_1, stąd:

$$h_{|W|} = |\bar{w}| = |\bar{w}_Y| + |\bar{w}_Z| + w_j > |\bar{v}| + |Z|g_1 + g_1 = h_{|Y|} + |Z|g_1 + g_1 = h_{|W|},$$

gdzie ostatnia równość wynika z lematu 2.28 w następujący sposób:

$$h_{|W|} - h_{|Y|} = \sum_{t=|Y|}^{|W|-1} g_t = |Z|g_1 + g_1.$$

Otrzymaliśmy sprzeczność, zatem $\bar{w}' \in \mathcal{B}(\mathcal{Z}, W)$, więc z lematu 4.3 (1) otrzymujemy $\bar{w}' \in \Gamma$.

W obu powyższych przypadkach otrzymaliśmy, że $\bar{w}' \in \Gamma$, stąd $\Pi_j \preccurlyeq_\Gamma \Pi_i$.

Pozostaje pokazać, że Π_j, Π_i są nieporównywalne, gdy $i, j \notin X$. Gdyby jednak było inaczej, to z lematu 4.13, przyjmując $n := m$, otrzymalibyśmy $g_0 = g_1$ wbrew przyjętemu tu założeniu. W ten sposób pokazaliśmy, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(J_m \setminus X, X)$.

2 b) Przyjmijmy $\min \Delta = \{\{k\} : k \in J_m\}$. Z wniosku 4.8 wynika, że Π_k jest maksymalny dla każdego $k \in J_m$. Gdyby $\Pi_j \preccurlyeq_\Gamma \Pi_i$ dla pewnych $i, j \in J_m$, to blok Π_j nie byłby maksymalny, stąd sprzeczność. W ten sposób pokazaliśmy, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\emptyset, J_m)$. □

Kolejne twierdzenie opisuje hierarchiczność struktur dostępu wyznaczonych przez polimatroidy, dla których $g_{m-1} > 0$ oraz rodziny, których zbiory minimalne składają się z jednego zbioru jednoelementowego. To twierdzenie szczegółowo wyjaśnia hierarchiczności struktur dostępu znajdujących się w pierwszym wierszu każdej z tabel.

Twierdzenie 4.24. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie taką rodziną monotoniczną, że $\min \Delta = \{\{k\}\}$ dla pewnego $k \in J_m$. Załóżmy, że $g_{m-1} > 0$.*

1. *Wówczas rodzina monotoniczna Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.*
2. *Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid $\mathcal{Z}$ i rodzinę monotoniczną Δ. Wtedy:*
   a) *Jeśli $g_0 = g_{m-1}$, to uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(J_m \setminus \{k\}, \{k\})$.*
   b) *Jeśli $g_0 > g_{m-1}$, to uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(J_m \setminus \{k\}, \{k\})$.*

Dowód. 1. Ten punkt otrzymujemy stosując lemat 2.36 (3).

2. Z wniosku 4.8 wynika, że Π_k jest maksymalny w zbiorze $(\Pi, \preccurlyeq_\Gamma)$, a więc Π_k nie jest równoważny z żadnym innym blokiem. Ustalmy $j \in J_m,\ j \neq k$. Rozważmy dowolny taki wektor $\bar{w} \in \min \Gamma$, że $w_j \neq 0$. Jeśli taki wektor nie istnieje, to na postawie uwagi 3.28 otrzymujemy $\Pi_j \prec_\Gamma \Pi_k$. Jeśli taki wektor istnieje, to na podstawie lematu 4.3 (3) otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ oraz $\operatorname{supp} \bar{w} \in \Delta$. Z założenia mamy $k \in \operatorname{supp} \bar{w}$. Z lematu 4.15 wynika, że $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_k \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ lub istnieją taki zbiór $Y \subseteq \operatorname{supp} \bar{w} \setminus \{j\}$, $k \in Y$ oraz taki wektor $\bar{v} \in \mathcal{B}(\mathcal{Z}, Y)$, że $\bar{v} \leqslant_s \bar{w}'$. W pierwszym przypadku z lematu 4.3 (1) otrzymujemy $\bar{w}' \in \Gamma$. Jeśli zachodzi drugi przypadek, to zauważmy, że $Y \in \Delta$, więc z lematu 4.3 (1) otrzymujemy $\bar{v} \in \Gamma$. To oznacza, że w obu przypadkach $\bar{w}' \in \Gamma$, stąd $\Pi_j \prec_\Gamma \Pi_k$. W sposób otrzymujemy wniosek, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(J_m \setminus \{k\}, \{k\})$ lub $Ord_\Gamma(J_m \setminus \{k\}, \{k\})$.

2 a) Zauważmy, że równość $g_0 = g_{m-1}$ wraz z monotonicznością ciągu $\boldsymbol{g}$ pociągają $g_0 = g_1 = \ldots = g_{m-1}$. Dalej wystarczy zastosować twierdzenie 4.22 (2b), aby otrzymać tezę.

2 b) Jeśli uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(J_m \setminus \{k\}, \{k\})$, wtedy bloki Π_i i Π_j są porównywalne dla pewnych $i, j \in J_m \setminus \{k\}$. Ze stwierdzenia 4.13, dla $n := m$, wynika, że $g_0 = g_1 = \cdots = g_{m-1}$. Stąd otrzymaliśmy sprzeczność z tym, że $g_0 > g_{m-1}$, więc że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(J_m \setminus \{k\}, \{k\})$. □

Podsumowując, opisaliśmy dokładnie hierarchiczność struktur dostępu wyznaczonych przez polimatroidy jednorodne, dla których $g_{m-1} > 0$, oraz rodziny monotoniczne z nimi kompatybilne.

Przypadek $g_{m-2} > g_{m-1} = 0$

Kontynuujemy nasze badania przechodząc do kolejnej grupy polimatroidów. Podamy teraz warunek konieczny istnienia bloków porównywalnych w przypadku, gdy dla ciągu $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ wyznaczonego przez polimatroid $\mathcal{Z}$ mamy $g_{m-2} > g_{m-1} = 0$. Następnie w twierdzeniach 4.26 oraz 4.27 wykażemy, że otrzymane warunki są także wystarczające. Poniższe trzy twierdzenia mają swoje zastosowanie do tabel 4.2 oraz 4.3.

Twierdzenie 4.25. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$, $m \geqslant 3$, będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $g_{m-2} > g_{m-1} = 0$ oraz istnieją w zbiorze Π dwa różne bloki, które są porównywalne w strukturze dostępu Γ, to $\min \Delta = \{X, Y\}$, gdzie $|X| = 1$, $Y \subseteq J_m \setminus X$, $|Y| \geqslant m - 2$.

Dowód. Z lematu 2.35 wynika, że każdy podzbiór $(m-1)$-elementowy należy do Δ. Korzystając z tego faktu łatwo zauważyć, że przekrój wszystkich zbiorów należących do Δ jest pusty, więc Δ nie zawiera elementu najmniejszego, zatem w rodzinie Δ istnieją co najmniej dwa zbiory minimalne. Załóżmy, że pewne dwa bloki Π_i oraz Π_j są porównywalne. Zgodnie z lematem 4.5 dowolny zbiór $(m-1)$-elementowy zawierający obydwa elementy i, j nie może być minimalny, więc zawiera właściwy podzbiór, który jest minimalny w Δ. Rozważmy dwa przypadki:

i) Istnieją takie dwa zbiory $X, Y \subseteq J_m$ minimalne w Δ, że $|X| \leqslant m-2$ oraz $|Y| = m-1$. Z faktu, że $Y \in \min \Delta$ i twierdzenia 4.5 wynika, że jeden z elementów i lub j nie należy do Y. Bez straty ogólności możemy przyjąć, że jest to element i. Z faktu, że X nie zawiera się w Y wynika, że $i \in X$, bo i jest jedynym elementem nie należącym do Y. Z twierdzenia 4.5 wynika, że $j \notin X$. Z twierdzenia 4.7 oraz z porównywalności bloków wynika, że $\Pi_j \preceq \Pi_i$.

Przypuśćmy, że $|X| \geqslant 2$, więc zbiory X i Y nie są rozłączne. Ustalmy element $l \in X \cap Y$. Zbiór $J_m \setminus \{l\}$ należy do Δ, bo ma $m-1$ elementów, nie zawiera zbiorów minimalnych X ani Y, nie jest także minimalny bo zawiera i, j, więc zawiera pewien inny zbiór minimalny W, $|W| \leqslant m-2$. Podobnie jak poprzednio z faktu, że W nie zawiera się w Y wynika, że $i \in W$, bo i jest jedynym elementem nie należącym do Y. Z twierdzenia 4.5 wynika, że $j \notin W$. Stąd otrzymujemy $|X \cup W| \leqslant m-1$. Zauważmy także, że $X \neq W$. Stosując stwierdzenie 4.14 dla $n := m-1$ otrzymujemy $g_1 = \ldots = g_{m-2}$. Następnie z lematu 4.10 wynika, że zbiory X i W są jednoelementowe, wbrew przyjętemu wcześniej założeniu, że $|X| \geqslant 2$. Pokazaliśmy, że $|X| = 1$ oraz $Y = J_m \setminus X$.

Należy jeszcze pokazać, że nie ma innych zbiorów minimalnych w Δ. Niech U będzie pewnym zbiorem minimalnym w Δ. Oczywiście U jako zbiór minimalny nie zawiera zbioru X. Jeśli U ma $m-1$ elementów, to jest równy Y, bo jest to jedyny zbiór $(m-1)$-elementowy, który nie zawiera X. Jeśli $|U| \leqslant m-2$, to stosując powyższe rozumowanie dla pary zbiorów U, Y stwierdzamy, że U jest zbiorem jednoelementowym rozłącznym z Y, a to pociąga $X = U$.

ii) Wszystkie zbiory minimalne w Δ mają co najwyżej $m-2$ elementów. Niech $X, Y \in \min \Delta$, $X \neq Y$. Zgodnie z twierdzeniem 4.7, najpierw zastosowanym do X, potem do Y, elementy należące do $X \cup Y$ są nieporównywalne, więc i, j nie mogą równocześnie należeć do sumy tych zbiorów. Stąd $|X \cup Y| \leqslant m-1$.

Rozważmy przypadek, gdy dokładnie jeden spośród elementów i, j należy do zbioru $X \cup Y$. Bez utraty ogólności możemy przyjąć, że $i \in X$. Wtedy $j \notin Y$. Jeśli $|X| \geqslant 2$, to ze stwierdzenia 4.14 zastosowanego dla $n := m-1$ otrzymujemy, $g_1 = \ldots = g_{m-2}$, co wraz z lematem 4.10 pociąga $|X| = 1$, stąd sprzeczność. Zatem $X = \{i\}$ nie zawiera się w zbiorze Y, który jest minimalny w Δ. Widzimy, że $i, j \notin Y$. Jeśli $|Y| \leqslant m-3$, to stosując stwierdzenie 4.13 dla $n := m-1$ otrzymujemy $g_0 = g_1 = \ldots = g_{m-2}$, a to zgodnie z lematem 4.11 daje równość

zbiorów X i Y, co jest sprzeczne z ich wyborem. Zatem zbiór Y ma $m-2$ elementów i jest rozłączny z jednoelementowym zbiorem X.

Przypuśćmy teraz, że i oraz j nie należą do $X \cup Y$, więc $|X \cup Y| \leqslant m-2$. Jeśli liczba elementów w jednym ze zbiorów X lub Y nie przekracza $m-3$ to stosując stwierdzenie 4.13 dla $n := m-1$ otrzymujemy $g_0 = g_1 = \ldots = g_{m-2}$. Następnie z lematu 4.11 wynika, że $X = Y$, co jest sprzeczne z wyborem tych zbiorów. Stąd wynika, że $|X| = |Y| = m-2$. Zatem $X = Y = J_m \setminus \{i, j\}$, co również jest sprzeczne z przyjętym założeniem o tych zbiorach. Pokazaliśmy, że przypadek gdy i oraz j nie należą do $X \cup Y$ jest niemożliwy.

Podsumowując przypadek ii), pokazaliśmy, że $|X| = 1$ oraz $Y \subseteq J_m \setminus X$, $|Y| = m-2$. Należy jeszcze pokazać, że nie ma innych zbiorów minimalnych w Δ. Niech U będzie pewnym zbiorem minimalnym w Δ. Jeśli zastosujemy powyższe rozumowanie do pary zbiorów X, U, to stwierdzimy, że $U \subseteq J_m \setminus X$ i $|U| = m-2$. Podobnie rozważając parę U, Y otrzymamy $U \subseteq J_m \setminus Y$ i $|U| = 1$. Stąd $m = 3$. W tym przypadku zbiory X, Y, U są minimalne w Δ, jednoelementowe oraz w sumie dają cały zbiór J_3. Oznacza to, że bloki Π_i oraz Π_j są maksymalne wbrew początkowym ustaleniom. Ta sprzeczność pokazuje, że $\min \Delta$ zawiera dokładnie dwa zbiory.

Ostatecznie wykazaliśmy, że $\min \Delta = \{X, Y\}$, gdzie $|X| = 1$, $Y \subseteq J_m \setminus X$, $|Y| \geqslant m-2$. □

Powyższe twierdzenie wskazuje, że w przypadku, gdy $g_{m-2} > g_{m-1} = 0$, struktury dostępu, które nie są oddziałowe, mogą być wyznaczone przez polimatroidy i tylko dwa typy rodzin monotonicznych. Poniższe dwa twierdzenia pokazują, że zaprezentowane warunki konieczne na to, aby pewne bloki uczestników w wielodzielnej strukturze dostępu były porównywalne, są także wystarczające. Odnosząc się do przykładów w postaci tabel, poniższe twierdzenie opisuje hierarchiczność struktury dostępu wyznaczonej przez polimatroid jednorodny $\mathcal{Z}$ oraz rodzinę monotoniczną Δ określone przez:

1. kolumnę 2 i 3 oraz wiersz 4 w tabeli 4.2;
2. kolumnę 4, 5, 6 i 7 oraz wiersz 9 w tabeli 4.3.

Twierdzenie 4.26. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$, $m \geqslant 3$, będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie taką rodziną monotoniczną, że $\min \Delta = \{\{k\}, J_m \setminus \{k\}\}$ dla pewnego $k \in J_m$. Załóżmy, że $g_{m-2} > g_{m-1} = 0$.*

1. *Wówczas rodzina monotoniczna Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.*
2. *Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid $\mathcal{Z}$ i rodzinę monotoniczną Δ. Wtedy uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(J_m \setminus \{k\}, \{k\})$.*

Dowód. 1. Posłużymy się lematem Csirmaza (2.21). Warunek 1 tego lematu jest spełniony po zastosowaniu lematu 2.36 (1), ponieważ każdy zbiór $(m-1)$-elementowy należy do Δ. Aby sprawdzić warunek 2, weźmy takie zbiory $X, Y \in \Delta$, że $X \cap Y \notin \Delta$. Zauważmy, że jest to możliwe wtedy i tylko wtedy, gdy $k \in X \neq J_m$ oraz $Y = J_m \setminus \{k\}$. Wówczas, korzystając z lematu 4.18, otrzymujemy, że warunek 2 lematu Csirmaza (2.21) jest również spełniony, więc rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.

2. Najpierw pokażemy, że $\Pi_j \preccurlyeq_\Gamma \Pi_k$, $j \in J_m \setminus k$. Z wniosku 4.8 wynika, że Π_k jest maksymalny w zbiorze $(\Pi, \preccurlyeq_\Gamma)$, a więc Π_k nie jest równoważny z żadnym innym blokiem. Rozważmy dowolny taki wektor $\bar{w} \in \min \Gamma$, że $w_j \neq 0$. Jeśli taki wektor nie istnieje, to na postawie uwagi 3.28 otrzymujemy $\Pi_j \prec_\Gamma \Pi_k$. Jeśli taki wektor istnieje, to na podstawie lematu 4.3 (3) otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ i $\operatorname{supp} \bar{w} \in \Delta$. Zauważmy, że z założenia $k \in \operatorname{supp} \bar{w}$ lub $J_m \setminus \{k\} \subseteq \operatorname{supp} \bar{w}$. W związku z tym możemy powołać się na lemat 4.17 i otrzymujemy z niego, że $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_k \in \Gamma$.

W ten sposób wykazaliśmy, że $\Pi_j \prec_\Gamma \Pi_k$. Wówczas uporządkowanie zbioru Π jest typu $Ord_\Gamma(J_m \setminus \{k\}, \{k\})$ lub $Ord^*_\Gamma(J_m \setminus \{k\}, \{k\})$. Biorąc pod uwagę twierdzenie 4.5 opcję drugą należy odrzucić. □

Poniższe twierdzenie opisuje hierarchiczność struktury dostępu wyznaczonej przez polimatroid jednorodny $\mathcal{Z}$ oraz rodzinę monotoniczną Δ określone przez kolumnę 4, 5, 6 i 7 oraz wiersz 6 w tabeli 4.3.

Twierdzenie 4.27. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$, $m \geqslant 4$, będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie taką rodziną monotoniczną, że $\min \Delta = \{\{k\}, J_m \setminus \{k, j\}\}$ dla pewnych $k, j \in J_m$. Załóżmy, że $g_{m-2} > g_{m-1} = 0$.*

1. *Wówczas rodzina monotoniczna Δ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy $g_{m-3} > g_{m-2}$.*

2. *Niech $g_{m-3} > g_{m-2}$ oraz niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid $\mathcal{Z}$ i rodzinę monotoniczną Δ. Wtedy uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\{j\}, \{k\})$.*

Dowód. 1. Najpierw wykażemy implikację „⇒”. Ustalmy takie $i \in J_m$, że $i \neq k$ oraz $i \neq j$. Weźmy $X = J_m \setminus \{i, j\}$ i $Y = J_m \setminus \{k, j\}$. Z faktów, że $X, Y \in \Delta$, $X \cap Y = J_m \setminus \{i, j, k\} \notin \Delta$, oraz lematu Csirmaza (2.21, 2) wynika kolejno, iż

$$h(X \cap Y) + h(X \cup Y) < h(X) + h(Y),$$

$$h_{m-3} + h_{m-1} < h_{m-2} + h_{m-2},$$

$$h_{m-1} - h_{m-2} < h_{m-2} - h_{m-3},$$

$$g_{m-2} < g_{m-3},$$

co należało udowodnić.

Aby wykazać implikację „⇐", załóżmy, że $g_{m-2} < g_{m-3}$ i posłużmy się lematem Csirmaza (2.21). Warunek 1 lematu Csirmaza (2.21) jest spełniony po zastosowaniu lematu 2.36 (1), ponieważ każdy zbiór $(m-1)$-elementowy należy do Δ. Aby wykazać punkt drugi tego lematu, weźmy takie zbiory $X, Y \in \Delta$, że $X \cap Y \notin \Delta$. Zauważmy, że jest to możliwe wtedy i tylko wtedy, gdy $k \in X \neq J_m$ oraz $J_m \setminus \{k, j\} \subseteq Y \subseteq J_m \setminus \{k\}$. Rozważmy dwa przypadki:

i) $Y = J_m \setminus \{k\}$. Wówczas powołując się na lemat 4.18 otrzymujemy

$$h(X \cap Y) + h(X \cup Y) < h(X) + h(Y).$$

ii) $Y = J_m \setminus \{k, j\}$. Wówczas $|X \cup Y| \geqslant m-1$, $|X \cap Y| < |Y| = m-2$. Stąd, korzystając z założenia oraz lematu 2.28, kolejno otrzymujemy:

$$g_{m-2} < g_{m-3} \leqslant g_{|X\cap Y|} \leqslant g_{|X\cap Y|} + \cdots + g_{|X|-1},$$

$$h_{m-1} - h_{m-2} < h_{|X|} - h_{|X\cap Y|}.$$

Zauważmy, że z założenia $g_{m-1} = 0$ wynika, iż $h_m = h_{m-1} = h_{|X\cup Y|}$, więc kontynuując rachunek otrzymujemy kolejno:

$$h_{|X\cup Y|} - h_{|Y|} < h_{|X|} - h_{|X\cap Y|},$$

$$h_{|X\cap Y|} + h_{|X\cup Y|} < h_{|X|} + h_{|Y|},$$

$$h(X \cap Y) + h(X \cup Y) < h(X) + h(Y).$$

W ten sposób wykazaliśmy, że warunki lematu Csirmaza (2.21) są spełnione, więc rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.

2. W pierwszej kolejności wykażmy, że $\Pi_j \prec_\Gamma \Pi_k$. Zauważmy, że z wniosku 4.8 wynika, iż Π_k jest maksymalny w zbiorze $(\Pi, \preccurlyeq_\Gamma)$, a więc Π_k nie jest równoważny z żadnym innym blokiem. Rozważmy dowolny taki wektor $\bar{w} \in \min \Gamma$, że $w_j \neq 0$. Jeśli taki wektor nie istnieje, to na postawie uwagi 3.28 otrzymujemy $\Pi_j \prec_\Gamma \Pi_k$. Jeśli taki wektor istnieje, to na podstawie lematu 4.3 (3) otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ i $\operatorname{supp} \bar{w} \in \Delta$. Zauważmy, że z założenia $k \in \operatorname{supp} \bar{w}$ lub $J_m \setminus \{k, j\} \subseteq \operatorname{supp} \bar{w}$. Jeśli $J_m \setminus \{k, j\} \subseteq \operatorname{supp} \bar{w}$, to z tego, że $w_j > 0$ otrzymujemy $J_m \setminus \{k\} \subseteq \operatorname{supp} \bar{w}$. W związku z tym możemy powołać się na lemat 4.17 i otrzymujemy z niego, że $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_k \in \Gamma$. W ten sposób wykazaliśmy, że $\Pi_j \prec_\Gamma \Pi_k$.

Z twierdzenia 4.5 wynika, że bloki indeksowane elementami ze zbioru $J_m \setminus \{k, j\}$ są parami nieporównywalne. Ponadto stosując twierdzenie 4.7 dla $X = J_m \setminus \{k, j\}$ otrzymujemy, że każdy blok Π_i, $i \in J_m \setminus \{k, j\}$, nie jest hierarchicznie podrzędny lub równoważny względem bloku Π_k oraz nie jest hierarchicznie podrzędny lub równoważny względem bloku Π_j.

Blok Π_k jest maksymalny, w związku z powyższym jest nieporównywalny z każdym blokiem Π_i, $i \in J_m \setminus \{k, j\}$.

Przypuśćmy, że $\Pi_j \preceq \Pi_i$, dla pewnego $i \in J_m \setminus \{k, j\}$. Niech $\bar{w}$ będzie takim wektorem wierzchołkowym rzędu $m-1$, którego nośnikiem jest zbiór $J_m \setminus \{k\}$, że $w_i = g_0, w_j = g_{m-3}$. Tutaj korzystamy z założenia, że $m \geqslant 4$, dzięki któremu $g_0 \neq g_{m-3}$. Oczywiście z lematu 4.4 mamy $\bar{w} \in \Gamma$, gdyż $J_m \setminus \{k\} \in \Delta$. Przy takich założeniach również wektor $\bar{w}' := \bar{w} - g_{m-3}\bar{e}_j + g_{m-3}\bar{e}_i$ należy do Γ. Na podstawie lematu 4.3 (4) istnieje taki minimalny wektor autoryzowany $\bar{v}$, że $\bar{v} \leqslant_s \bar{w}'$, $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{v})$ oraz $\operatorname{supp} \bar{v} \in \Delta$. Stąd wynika, że $\operatorname{supp} \bar{v} = J_m \setminus \{k, j\}$, bo $J_m \setminus \{k, j\}$ jest zbiorem minimalnym w Δ. Ponadto $v_i \leqslant g_0$ oraz $v_t \leqslant w_t$ dla $t \neq i$. Stąd oraz lematu 2.28 otrzymujemy

$$h_{m-2} = |\bar{v}| \leqslant g_0 + \sum_{t \in J_m \setminus \{k,j,i\}} w_t = \sum_{t=0}^{m-2} g_t - g_{m-3} = h_{m-1} - g_{m-3}.$$

Zauważmy, że $h_{m-1} = h_{m-2} + g_{m-2}$, stąd kontynuując rachunek otrzymujemy

$$h_{m-1} - g_{m-3} = h_{m-2} + g_{m-2} - g_{m-3} < h_{m-2},$$

gdzie ostatnia nierówność wynika z założenia, że $g_{m-3} > g_{m-2}$. Ta sprzeczność pokazuje, że Π_j nie może być hierarchicznie podrzędny lub równoważny względem Π_i dla każdego $i \in J_m \setminus \{k, j\}$. Zatem $\Pi_j \prec_\Gamma \Pi_k$ jest jedyną nierównością pomiędzy różnymi blokami zbioru $(\Pi, \preccurlyeq_\Gamma)$, co dowodzi, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\{j\}, \{k\})$. □

Przypadek $g_0 \geqslant g_1 > g_2 = \cdots = g_{m-1} = g_m = 0$

Twierdzenie 4.28 omawia warunki konieczne i wystarczające na to, aby pewne bloki uczestników w wielodzielnej strukturze dostępu były porównywalne w przypadku, gdy dla rozważanych polimatroidów mamy $g_0 \geqslant g_1 > g_2 = 0$.

Poniższe twierdzenie ma swoje zastosowanie również tylko do tabel 4.2 oraz 4.3. W przypadku tabeli 4.2 opisuje hierarchiczność struktur dostępu wyznaczonych przez polimatroidy określone w kolumnach 2 i 3, oraz rodziny monotoniczne z nimi kompatybilne. W przypadku tabeli 4.3 podaje hierarchiczność struktur dostępu wyznaczonych przez polimatroidy określone w kolumnach 2 i 3, oraz rodziny monotoniczne z nimi kompatybilne.

Twierdzenie 4.28. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$, $m \geqslant 3$, będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Załóżmy, że $g_0 \geqslant g_1 > g_2 = \cdots = g_{m-1} = g_m = 0$.*

1. *Jeśli $g_0 > g_1$, to rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy istnieje taki podzbiór $X \subseteq J_m$, że $\min \Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J_m \setminus X)$.*

2. *Jeśli* $g_0 = g_1$, *to rodzina monotoniczna* $\Delta \subsetneq \mathcal{P}(J_m)$ *jest kompatybilna z polimatroidem* $\mathcal{Z}$ *wtedy i tylko wtedy, gdy istnieje taki podzbiór* $X \subseteq J_m$, $|X| \leqslant 1$, *że* $\min \Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J_m \setminus X)$.

3. *Niech* Γ *będzie strukturą dostępu wyznaczoną przez polimatroid* $\mathcal{Z}$ *i taką rodzinę monotoniczną* $\Delta \subsetneq \mathcal{P}(J_m)$, *że* $\min \Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J_m \setminus X)$ *dla pewnego* $X \subseteq J_m$. *Wtedy:*

   a) *Jeśli* X *jest niepustym podzbiorem zbioru* J_m, *to uporządkowanie zbioru* $(\Pi, \preccurlyeq_\Gamma)$ *jest typu* $Ord_\Gamma(J_m \setminus X, X)$.

   b) *Jeśli* $X = \emptyset$, *to* $\min \Delta = \mathcal{P}_2(J_m)$ *oraz uporządkowanie zbioru* $(\Pi, \preccurlyeq_\Gamma)$ *jest typu* $Ord_\Gamma(\emptyset, J_m)$.

Dowód. 1. W pierwszej kolejności wykażemy implikację „⇒”. Jeśli rodzina monotoniczna Δ jest kompatybilna z polimatroidem $\mathcal{Z}$, to z lematu 2.35 i założenia $g_2 = 0$ wynika, że wszystkie podzbiory dwuelementowe zbioru J_m należą do Δ. Zatem zbiory minimalne należące do Δ mają jeden lub dwa elementy. Niech $X \subseteq J_m$ oznacza rodzinę tych elementów, które tworzą jednoelementowe zbiory minimalne. Stąd pozostałe zbiory minimalne są dwuelementowe i nie zawierają żadnych elementów należących do X. Zatem $\min \Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J_m \setminus X)$.

Aby wykazać implikację odwrotną, rozważmy taką rodzinę monotoniczną Δ, że $\min \Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J_m \setminus X)$ dla pewnego $X \subseteq J_m$. Łatwo zauważyć, że wszystkie zbiory 2-elementowe należą do Δ. Aby wykazać, że ta rodzina jest kompatybilna z polimatroidem $\mathcal{Z}$, wystarczy skorzystać z lematu 2.36 (2).

2. Aby wykazać implikację „⇒”, przeprowadzamy analogiczne rozumowanie jak w punkcie 1 i otrzymujemy $\min \Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J_m \setminus X)$ dla takiego $X \subseteq J_m$, że X jest rodziną tych elementów, które tworzą jednoelementowe zbiory minimalne. Pozostaje wykazać, iż $|X| \leqslant 1$. Przypuśćmy zatem, że $|X| \geqslant 2$. Stąd istnieją takie $i, j \in X$, że $i \neq j$. Oczywiście $\{i\}, \{j\} \in \Delta$, lecz $\{i\} \cap \{j\} = \emptyset \notin \Delta$. Zatem z lematu Csirmaza (2.21, 2) otrzymujemy

$$h(\{i,j\}) < h(\{i\}) + h(\{j\}) \Longrightarrow h_2 < 2h_1 \Longrightarrow h_2 - h_1 < h_1 \Longrightarrow g_1 < g_0,$$

co jest sprzeczne z założeniem.

Aby wykazać implikację odwrotną, rozważmy taką rodzinę monotoniczną Δ, że $\min \Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J_m \setminus X)$ dla pewnego $X \subset J_m$, $|X| \leqslant 1$. Zauważmy, że sygnatura ciągu $\boldsymbol{g}$ ma postać $(0, 1, 0, \ldots, 0)$. Rozważmy dwa przypadki:

i) $|X| = 1$. Łatwo sprawdzić, że $I_1(\Delta) = \{0, 1\}$ oraz $I_2(\Delta) = \{1\}$. Zauważmy, że spełnione są warunki 1 i 2 twierdzenia 2.33, więc rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.

ii) $|X| = 0$, stąd $\min \Delta = \mathcal{P}_2(J_m)$. Łatwo sprawdzić, że w tym przypadku $I_1(\Delta) = \{1\}$ oraz $I_2(\Delta) = \{1\}$. Podobnie jak poprzednio spełnione są warunki 1 i 2 twierdzenia 2.33, więc rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$.

3 a) Zauważmy, że zgodnie z wnioskiem 4.8 bloki indeksowane elementami zbioru X są maksymalne w $(\Pi, \preccurlyeq_\Gamma)$, więc nie mogą być parami porównywalne. Rozważmy przypadki:

i) $X = J_m$. Na podstawie powyższej uwagi otrzymujemy, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\emptyset, X) = Ord_\Gamma(J_m \setminus X, X)$.

ii) $X \subsetneq J_m$. W tym przypadku bloki indeksowane elementami zbioru X nie mogą być hierarchicznie podrzędne względem bloków indeksowanych elementami ze zbioru $J_m \setminus X$. Ponadto każde dwa elementy należące do $J_m \setminus X$ tworzą zbiór należący do $\min \Delta$ więc zgodnie z twierdzeniem 4.5 indeksowane nimi bloki są nieporównywalne.

Pozostaje do wykazania, że $\Pi_j \prec_\Gamma \Pi_i$ dla $i \in X$ oraz $j \in J_m \setminus X$. Niech $\bar{w}$ będzie takim wektorem minimalnym w Γ, że $w_j \neq 0$. Jeśli taki wektor nie istnieje, to na postawie uwagi 3.28 otrzymujemy $\Pi_j \prec_\Gamma \Pi_i$. Jeśli taki wektor istnieje, to na podstawie lematu 4.3 (3) otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ oraz $\operatorname{supp} \bar{w} \in \Delta$. Zauważmy, że zbiór $\{j\}$ nie należy do $\min \Delta$, więc $|\operatorname{supp} \bar{w}| \geqslant 2$. Zgodnie z lematem 2.30 otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w}) \subseteq \mathcal{B}(\mathcal{Z}, J_m)$. Z lematu 4.15 wynika, że $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_i \in \mathcal{B}(\mathcal{Z}, J_m)$ lub istnieją taki zbiór $Y \subseteq J_m \setminus \{j\}$, $i \in Y$, oraz taki wektor $\bar{v} \in \mathcal{B}(\mathcal{Z}, Y)$, że $\bar{v} \leqslant_s \bar{w}'$. W pierwszym przypadku z lematu 4.3 (1) otrzymujemy $\bar{w}' \in \Gamma$. Jeśli zachodzi drugi przypadek, to zauważmy, że $Y \in \Delta$, więc z lematu 4.3 (1) otrzymujemy $\bar{v} \in \Gamma$, stąd $\bar{w}' \in \Gamma$. Ostatecznie $\Pi_j \prec_\Gamma \Pi_i$. W ten sposób wykazaliśmy, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(J_m \setminus X, X)$.

3 b) Tezę, że uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\emptyset, J_m)$ otrzymujemy natychmiast z wniosku 4.6. □

Przypadek $g_0 > g_1 = \cdots = g_{m-1} = g_m = 0$

Kończymy nasze badania przechodząc do ostatniej grupy polimatroidów. Podamy teraz warunek konieczny i wystarczający istnienia bloków porównywalnych w przypadku, gdy dla ciągu $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ wyznaczonego przez polimatroid $\mathcal{Z}$ mamy $g_0 > g_1 = \cdots = g_{m-1} = g_m = 0$.

Poniższe twierdzenie ma zastosowanie do tabel 4.1, 4.2 oraz 4.3. Uzasadnia, że struktura dostępu wyznaczona przez polimatroid jednorodny, dla którego $g_0 > g_1 = \cdots = g_{m-1} = g_m = 0$ (pierwsza kolumna), oraz rodzinę monotoniczną z nim kompatybilną, jest progowa.

Twierdzenie 4.29. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Załóżmy, że $g_0 > g_1 = \cdots = g_{m-1} = g_m = 0$.*

1. *Wówczas rodzina monotoniczna $\Delta \subsetneq \mathcal{P}(J_m)$ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy $\min \Delta = \{\{k\} : k \in J_m\}$.*

2. *Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid $\mathcal{Z}$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Wtedy uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(J_m, \emptyset)$*

Dowód. 1. Jeśli $g_1 = 0$ oraz rodzina monotoniczna Δ jest kompatybilna z polimatroidem $\mathcal{Z}$, to na podstawie lematu 2.35 każdy podzbiór mający co najmniej jeden element należy do Δ. Ponieważ $\Delta \neq \mathcal{P}(J_m)$, stąd $\min \Delta = \{\{k\} : k \in J_m\}$.

Implikację „$\Leftarrow$" otrzymujemy bezpośrednio z lematu 2.36 (2).

2. Załóżmy, że $\min \Delta = \{\{k\} : k \in J_m\}$. Wybierzmy dowolne $i, j \in J_m$. Pokażemy, że $\Pi_j \preccurlyeq_\Gamma \Pi_i$. Rozważmy taki wektor $\bar{w} \in \min \Gamma$, że $w_j > 0$. Jeśli taki wektor nie istnieje, to na postawie uwagi 3.28 otrzymujemy $\Pi_j \preccurlyeq_\Gamma \Pi_i$. W przeciwnym przypadku, na podstawie lematu 4.3 (3), otrzymujemy $\bar{w} \in B(\mathcal{Z}, \operatorname{supp} \bar{w})$ oraz $\operatorname{supp} \bar{w} \in \Delta$. Rozważmy wektor $\bar{w}' := \bar{w} - \bar{e}_j + \bar{e}_i$. Oczywiście $w'_i = w_i + 1$, $w'_j = w_j - 1$. Rozważmy przypadki:

i) $i \in \operatorname{supp} \bar{w}$. Korzystając z lematu 4.15, otrzymujemy $\bar{w}' \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$ lub istnieją taki zbiór $Y \subseteq \operatorname{supp} \bar{w} \setminus \{j\}$, $i \in Y$, oraz taki wektor $\bar{v} \in \mathcal{B}(\mathcal{Z}, Y)$, że $\bar{v} \leqslant_s \bar{w}'$. Jeśli $\bar{w}' \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w})$, to na podstawie lematu 4.3 (1) otrzymujemy $\bar{w}' \in \Gamma$. Jeśli zachodzi druga możliwość, to zauważmy, że $\{i\} \in \Delta$, stąd $Y \in \Delta$ i na podstawie lematu 4.3 (1) otrzymujemy $\bar{v} \in \Gamma$, więc $\bar{w}' \in \Gamma$.

ii) $i \notin \operatorname{supp} \bar{w}$. Wówczas z lematu 4.16 otrzymujemy $\bar{w}' \in \mathcal{B}(\mathcal{Z}, \operatorname{supp} \bar{w} \cup \{i\})$. Oczywiście $\operatorname{supp} \bar{w} \cup \{i\} \in \Delta$, więc na podstawie lematu 4.3 (1) mamy $\bar{w}' \in \Gamma$.

Pokazując, że $\bar{w}' \in \Gamma$ wykazaliśmy, iż $\Pi_j \preccurlyeq_\Gamma \Pi_i$ dla dowolnych $i, j \in J_m$. Stąd uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord^*_\Gamma(J_m, \emptyset)$. □

Widzimy, że w powyższym przypadku każde dwa bloki są hierarchicznie równoważne w strukturze dostępu Γ. Zgodnie z uwagą 3.8 możemy dokonać redukcji podziału Π zastępując jego bloki ich sumą. Ponadto na podstawie uwagi 3.6 (2) dochodzimy do wniosku, że Γ jest strukturą progową z progiem równym g_0.

Zauważmy, że wyniki prezentowane w dotychczasowych twierdzeniach nie zależą od wartości funkcji rangi polimatroidu $\mathcal{Z}$ ani od wartości wyznaczonego przez $\mathcal{Z}$ ciągu $\boldsymbol{g}$. Jedyny wpływ na hierarchiczność opisywanych struktur mają sygnatury ciągów $\boldsymbol{g}$. Wyniki zawarte w tych twierdzeniach są ogólne i całkowicie wyjaśniają hierarchiczność struktur dostępu dla $m = 2$, $m = 3$ i $m = 4$.

Spójność struktur dostępu

Teraz zaprezentujemy stwierdzenia, za pomocą których będziemy mogli w większości przypadków zweryfikować spójność struktur dostępu wyznaczonych przez polimatroidy jednorodne i kompatybilne z nimi rodziny monotoniczne.

Stwierdzenie 4.30. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Jeśli $\min\Delta \neq \{J_m\}$ *oraz* $g_0 = g_1 = \cdots = g_{m-1} > 0$, *to struktura dostępu* Γ *nie jest spójna.*

Dowód. Jeśli $\min\Delta \neq \{J_m\}$ oraz $g_0 = g_1 = \cdots = g_{m-1} > 0$, to z twierdzenia 4.22 (1) wynika, że rodzina Δ jest kompatybilna z polimatroidem $\mathcal{Z}$ wtedy i tylko wtedy, gdy $\min\Delta = \{X\}$ dla pewnego $X \subsetneq J_m$. Dalej, z twierdzenia 4.22 (2 a) otrzymujemy, że wektor $\bar{w} := \sum_{k\in X} h_1\bar{e}_k$ jest jedynym minimalnym wektorem autoryzowanym. Jeśli $\min\Delta \neq \{J_m\}$, to istnieje takie $i \notin X$, że $w_i = 0$. Zgodnie z uwagą 3.28 otrzymujemy, że struktura Γ nie jest spójna. □

Stwierdzenie 4.31. *Niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *będzie podziałem zbioru uczestników* P. *Niech* Γ *będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny* $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ *i rodzinę monotoniczną* $\Delta \subsetneq \mathcal{P}(J_m)$ *z nim kompatybilną.*

Jeśli nie istnieje taki blok Π_k *dla pewnego* $k \in J_m$, *że* $\Pi_k \preccurlyeq_\Gamma \Pi_j$ *dla każdego* $j \in J_m$, *to struktura dostępu* Γ *jest spójna.*

Dowód. Dowód tego stwierdzenia wynika bezpośrednio z uwagi 3.28. □

Zauważmy, że aby potwierdzić spójność struktur dostępu opisanych w tabelach 4.2 i 4.3, poza tymi odpowiadającymi ostatniej kolumnie, należy jeszcze wykazać spójność struktur dostępu, dla których w zbiorze bloków istnieje jeden blok hierarchicznie podrzędny względem pozostałych bloków, a dokładniej, dla których uporządkowanie zbioru bloków jest oznaczone literą D.

Stwierdzenie 4.32. *Niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *będzie podziałem zbioru uczestników* P. *Niech* $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ *będzie polimatroidem jednorodnym oraz niech* $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ *będzie ciągiem wyznaczonym przez polimatroid* $\mathcal{Z}$. *Załóżmy, że* $g_0 > g_1 = g_2 = \ldots. = g_{m-1} > 0$.

Jeśli Γ *jest strukturą dostępu wyznaczoną przez polimatroid* $\mathcal{Z}$ *i rodzinę monotoniczną* $\Delta \subsetneq \mathcal{P}(P)$ *z nim kompatybilną, to* Γ *jest spójna.*

Dowód. Rodziny kompatybilne z polimatroidem $\mathcal{Z}$ są wskazane w twierdzeniu 4.23 (1). Według twierdzenia 4.31 pozostaje do wykazania spójność struktury dostępu Γ wyznaczonej przez polimatroid $\mathcal{Z}$ oraz taką rodzinę monotoniczną Δ, że $\min\Delta = \{J_m \setminus \{j\}\}$ dla pewnego $j \in J_m$. Uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\{j\}, J_m \setminus \{j\})$ i wynika z twierdzenia 4.23 (2 a). Aby wykazać spójność struktury Γ, na podstawie uwagi 3.28 należy wskazać taki wektor $\bar{w} \in \min\Gamma$, że $w_j > 0$. Rozważmy wektor wierzchołkowy $\bar{w}$ rzędu m, w którym $w_j := g_0$, natomiast pozostałe współrzędne są równe g_1. Na podstawie lematu 2.39 otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{w}) = \mathcal{B}(\mathcal{Z}, J_m)$, natomiast z lematu 4.4 mamy $\bar{w} \in \Gamma$. Przypuśćmy, że taki istnieje wektor $\bar{v} \in \min\Gamma$, że $\bar{v} \leqslant_s \bar{w}$ i $\bar{v} \neq \bar{w}$. Wektory należące do $\mathcal{B}(\mathcal{Z}, J_m)$ mają równe wagi, stąd są nieporównywalne, więc $\operatorname{supp}\bar{v} = J_m \setminus \{j\}$. Oczywiście $\bar{v} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{v})$. Stąd

$$|\bar{v}| = |\bar{v}_{\operatorname{supp}\bar{v}}| = h(\operatorname{supp}\bar{v}) = h_{m-1} = h_m - g_{m-1} = h_m - g_1.$$

Z drugiej jednak strony

$$h_m - g_1 = |\bar{v}| = |\bar{v}_{\operatorname{supp}\bar{v}}| \leqslant |\bar{w}_{\operatorname{supp}\bar{v}}| = (m-1)g_1 = h_m - g_0.$$

Stąd otrzymujemy $g_0 \leqslant g_1$, co jest sprzeczne z założeniem. Podsumowując, wskazaliśmy taki wektor $\bar{w} \in \min \Gamma$, że $w_j > 0$. Stąd wnioskujemy, na podstawie uwagi 3.28, że struktura Γ jest spójna. □

Stwierdzenie 4.33. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie polimatroidem jednorodnym oraz niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$. Załóżmy, że $g_0 > g_1 > g_2 = \cdots = g_m = 0$.*

Jeśli Γ jest strukturą dostępu wyznaczoną przez polimatroid $\mathcal{Z}$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(P)$ z nim kompatybilną, to Γ jest spójna.

Dowód. Rodziny kompatybilne z polimatroidem $\mathcal{Z}$ są wskazane w twierdzeniu 4.28 (1). Według twierdzenia 4.31 pozostaje do wykazania spójność struktury dostępu Γ wyznaczonej przez polimatroid $\mathcal{Z}$ oraz taką rodzinę monotoniczną Δ, że $\min \Delta = \{\{k\} : k \in J_m\} \setminus \{j\}$ dla pewnego $j \in J_m$. Uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(\{j\}, J_m \setminus \{j\})$, co wynika z twierdzenia 4.28 (3 a). Aby wykazać spójność struktury Γ, na podstawie uwagi 3.28 należy wskazać taki wektor $\bar{w} \in \min \Gamma$, że $w_j > 0$.

Rozważmy wektor wierzchołkowy $\bar{w}$ rzędu 2, w którym $w_j := g_0$, natomiast $w_i := g_1$ dla pewnego $i \in J_m$, $i \neq j$. Na podstawie lematu 2.39 otrzymujemy $\bar{w} \in \mathcal{B}(\mathcal{Z}, \operatorname{supp}\bar{w}) = \mathcal{B}(\mathcal{Z}, \{i,j\})$, natomiast z lematu 4.4 mamy $\bar{w} \in \Gamma$. Przypuśćmy, że taki istnieje wektor $\bar{v} \in \min \Gamma$, że $\bar{v} \leqslant_s \bar{w}$ i $\bar{v} \neq \bar{w}$. Wówczas $\operatorname{supp}\bar{v} = \{i\}$, ponieważ wektory należące do $\mathcal{B}(\mathcal{Z}, \{i,j\})$ mają równe wagi. Oczywiście $\bar{v} \in \mathcal{B}(\mathcal{Z}, \{i\})$. Stąd $v_i = g_0$, czyli

$$g_0 = v_i \leqslant w_i = g_1,$$

co jest sprzeczne z założeniem. Podsumowując, wskazaliśmy taki wektor $\bar{w} \in \min \Gamma$, że $w_j > 0$. Stąd wnioskujemy, na podstawie uwagi 3.28, że struktura Γ jest spójna. □

Za pomocą powyższych twierdzeń wykazaliśmy, że znaczna większość struktur dostępu wyznaczonych przez polimatroidy jednorodne i kompatybilne z nimi rodziny, jest spójna, a na podstawie 4.1 wnioskujemy, że są także portami pewnych matroidów. Używamy sformułowania „znaczna większość", ponieważ wiemy na pewno, iż struktury wyznaczone przez polimatroidy, których ciąg $\boldsymbol{g}$ jest stały, oraz kompatybilne z nimi rodziny monotoniczne, nie są spójne. W prezentowanych tabelach odnosi się to do struktur odpowiadających ostatnim kolumnom. Ponadto pod znakiem zapytania stoi także spójność ewentualnych struktur dostępu, dla których w zbiorze $(\Pi, \preccurlyeq_\Gamma)$ istnieje jeden blok hierarchicznie podrzędny

względem pozostałych. Te wątpliwości zostały rozwiane dla dwóch takich przypadków za pomocą powyższych dwóch twierdzeń, stąd dla $m = 3$ oraz $m = 4$, poza strukturami reprezentowanymi przez ostatnią kolumnę, wszystkie struktury są spójne.

Jak już wiemy na podstawie z twierdzeń 3.23 i 3.24, struktury dostępu sklasyfikowane w tabelach 4.1 oraz 4.2, które są spójne, są także strukturami idealnymi, co więcej, są portami pewnych matroidów reprezentowalnych. W podrozdziale 4.5 wskażemy te struktury dostępu, które są portami pewnych matroidów reprezentowalnych w przypadku, gdy $m \geqslant 4$.

4.4 Wielodzielne struktury dostępu z małą liczbą bloków

W tym podrozdziale prezentujemy tabele, które doskonale ilustrują działanie twierdzeń będących treścią poprzedniego podrozdziału. Tabele zostały wygenerowane komputerowo i potwierdzają otrzymane teoretyczne wyniki. Pamiętajmy, że ustalona kolumna reprezentuje wszystkie polimatroidy, których sygnatura ciągu $\boldsymbol{g}$ jest równa sygnaturze ciągu widniejącego w nagłówku danej kolumny. Typów porządków występujących w prezentowanych trzech przypadkach jest niewiele, więc dla czytelności tabel każdemu z typów jest przypisana odpowiednia litera według załączonych legend.

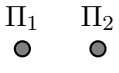
Symbol „–” oznacza, że rodzina monotoniczna Δ nie jest kompatybilna z danym polimatroidem.

Tabela 4.1: Tabela dla przypadku $m = 2$.

		1	2	3
	g_0	1	2	1
	$\min\Delta$ \ g_1	0	1	1
1	$\{\{1\}\}$	–	I	I
2	$\{\{1\},\{2\}\}$	p	A	–
3	$\{\{1,2\}\}$	–	A	A

Legenda:

$p := Ord^*_\Gamma(J_2, \emptyset)$



$A := Ord_\Gamma(\emptyset, J_2)$

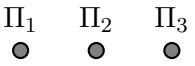
$I := Ord_\Gamma(\{2\},\{1\})$

Tabela 4.2: Tabela dla przypadku $m = 3$.

		1	2	3	4	5	6	7
	g_0	1	2	1	3	2	2	1
	g_1	0	1	1	2	2	1	1
	$\min\Delta$ g_2	0	0	0	1	1	1	1
1	$\{\{1\}\}$	–	–	–	G	G	G	I
2	$\{\{1\},\{2\}\}$	–	D	–	A	–	–	–
3	$\{\{1\},\{2\},\{3\}\}$	p	A	–	A	–	A	–
4	$\{\{1\},\{2,3\}\}$	–	G	G	A	A	–	–
5	$\{\{1,2\}\}$	–	–	–	A	A	D	D
6	$\{\{1,2\},\{1,3\}\}$	–	–	–	A	A	–	–
7	$\{\{1,2\},\{1,3\},\{2,3\}\}$	–	A	A	A	A	–	–
8	$\{\{1,2,3\}\}$	–	–	–	A	A	A	A

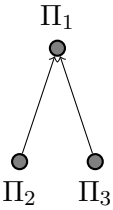
Legenda:

$p := Ord^*_\Gamma(J_3, \emptyset)$

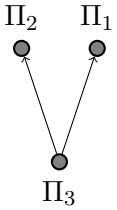


$A := Ord_\Gamma(\emptyset, J_3)$

$I := Ord^*_\Gamma(\{2,3\},\{1\})$



$G := Ord_\Gamma(\{2,3\},\{1\})$



$D := Ord_\Gamma(\{3\},\{1,2\})$

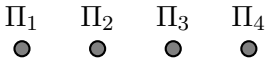
Tabela 4.3: Tabela dla przypadku $m = 4$.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	g_0	1	2	1	3	2	2	1	3	2	4	3	3	2	2	1
	g_1	0	1	1	2	2	1	1	2	2	3	3	2	2	1	1
	g_2	0	0	0	1	1	1	1	1	1	2	2	2	2	1	1
	$\min\Delta$ g_3	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	$\{\{1\}\}$	–	–	–	–	–	–	–	G	G	G	G	G	G	G	I
2	$\{\{1\},\{2\}\}$	–	–	–	A	–	–	–	–	–	A	–	–	–	–	–
3	$\{\{1\},\{2\},\{3\}\}$	–	D	–	A	–	–	–	A	–	A	–	–	–	–	–
4	$\{\{1\},\{2\},\{3\},\{4\}\}$	p	A	–	A	–	A	–	A	–	A	–	A	–	A	–
5	$\{\{1\},\{2\},\{3,4\}\}$	–	H	–	A	–	–	–	A	–	A	–	–	–	–	–
6	$\{\{1\},\{2,3\}\}$	–	–	–	C	C	–	–	–	–	A	A	–	–	–	–
7	$\{\{1\},\{2,3\},\{2,4\}\}$	–	–	–	A	A	–	–	–	–	A	A	–	–	–	–
8	$\{\{1\},\{2,3\},\{2,4\},\{3,4\}\}$	–	G	G	A	A	–	–	A	A	A	A	–	–	–	–
9	$\{\{1\},\{2,3,4\}\}$	–	–	–	G	G	G	G	–	–	A	A	A	A	–	–
10	$\{\{1,2\}\}$	–	–	–	–	–	–	–	A	A	A	A	A	A	H	F
11	$\{\{1,2\},\{1,3\}\}$	–	–	–	–	–	–	–	–	–	A	A	–	–	–	–
12	$\{\{1,2\},\{3,4\}\}$	–	–	–	A	A	A	A	–	–	A	A	A	A	–	–
13	$\{\{1,2\},\{1,3\},\{1,4\}\}$	–	–	–	–	–	–	–	A	A	A	A	–	–	–	–
14	$\{\{1,2\},\{1,3\},\{2,3\}\}$	–	–	–	A	A	–	–	–	–	A	A	–	–	–	–

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	g_0	1	2	1	3	2	2	1	3	2	4	3	3	2	2	1
	g_1	0	1	1	2	2	1	1	2	2	3	3	2	2	1	1
	g_2	0	0	0	1	1	1	1	1	1	2	2	2	2	1	1
	$\min\Delta$ g_3	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
15	$\{\{1,2\},\{2,3\},\{1,4\}\}$	–	–	–	*A*	*A*	–	–	–	–	*A*	*A*	–	–	–	–
16	$\{\{1,3\},\{2,3\},\{1,4\},\{2,4\}\}$	–	–	–	*A*	*A*	–	–	–	–	*A*	*A*	–	–	–	–
17	$\{\{1,2\},\{1,3\},\{2,3\}\{1,4\}\}$	–	–	–	*A*	*A*	–	–	–	–	*A*	*A*	–	–	–	–
18	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\}\}$	–	–	–	*A*	*A*	–	–	–	–	*A*	*A*	–	–	–	–
19	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\},\{3,4\}$	–	*A*	*A*	*A*	*A*	–	–	*A*	*A*	*A*	*A*	–	–	–	–
20	$\{\{1,2\},\{1,3,4\}\}$	–	–	–	–	–	–	–	–	–	*A*	*A*	*A*	*A*	–	–
21	$\{\{1,2\},\{1,3\},\{2,3,4\}\}$	–	–	–	*A*	*A*	–	–	–	–	*A*	*A*	–	–	–	–
22	$\{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$	–	–	–	*A*	*A*	–	–	–	–	*A*	*A*	–	–	–	–
23	$\{\{1,2\},\{1,3,4\},\{2,3,4\}\}$	–	–	–	*A*	*A*	*A*	*A*	–	–	*A*	*A*	*A*	*A*	–	–
24	$\{\{1,2,3\}\}$	–	–	–	–	–	–	–	*A*	*A*	*A*	*A*	*A*	*A*	*D*	*D*
25	$\{\{1,2,3\},\{1,2,4\}\}$	–	–	–	–	–	–	–	–	–	*A*	*A*	*A*	*A*	–	–
26	$\{\{1,2,3\},\{1,2,4\},\{1,3,4\}\}$	–	–	–	–	–	–	–	–	–	*A*	*A*	*A*	*A*	–	–
27	$\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$	–	–	–	*A*	*A*	*A*	*A*	–	–	*A*	*A*	*A*	*A*	–	–
28	$\{\{1,2,3,4\}\}$	–	–	–	–	–	–	–	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*

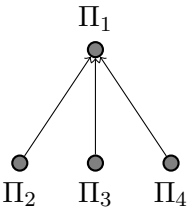
Legenda:

$p := Ord^*_\Gamma(J_4, \emptyset)$

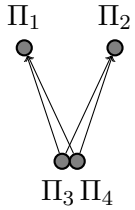


$A := Ord_\Gamma(\emptyset, J_4)$

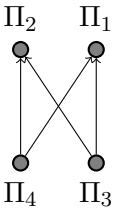
$I := Ord^*_\Gamma(\{2,3,4\}, \{1\})$



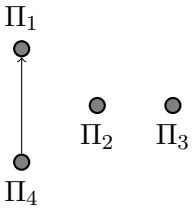
$G := Ord_\Gamma(\{2,3,4\}, \{1\})$



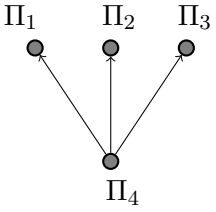
$F := Ord^*_\Gamma(\{3,4\}, \{1,2\})$



$H := Ord_\Gamma(\{3,4\}, \{1,2\})$



$C := Ord_\Gamma(\{4\}, \{1\})$



$D := Ord_\Gamma(\{4\}, \{1,2,3\})$

4.5 Struktury dostępu wyznaczone przez jednorodne polimatroidy boolowskie

Rozpocznijmy od następującego twierdzenia podającego warunek wystarczający na to, aby struktura dostępu wyznaczona przez polimatroid jednorodny i rodzinę monotoniczną była portem pewnego matroidu reprezentowalnego.

Twierdzenie 4.34 (Farràs, Martí-Farré, Padró [9, Corollary 6.7])**.** *Załóżmy, że* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *jest podziałem zbioru uczestników* P *oraz rodzina* $\Gamma \subsetneq \mathcal{P}(P)$ *jest spójną* Π*-dzielną strukturą dostępu. Niech* Γ *będzie portem pewnego matroidu, to znaczy istnieje taki polimatroid* $\mathcal{Z} = (J_m, h)$*, że* $h(\{k\}) \leqslant |\Pi_k|$ *dla każdego* $k \in J_m$ *oraz taka rodzina monotoniczna* $\Delta \subsetneq \mathcal{P}(J_m)$ *z nim kompatybilna, że*

$$\min \Gamma = \min\{\bar{w} \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}.$$

Struktura Γ *jest portem pewnego matroidu reprezentowalnego, jeśli takie uzupełnienie* $\mathcal{Z}' = (J'_m, h')$ *polimatroidu* $\mathcal{Z}$*, że* $\Delta = \Delta(\mathcal{Z}')$*, jest polimatroidem reprezentowalnym.*

Pamiętajmy, że w powyższym twierdzeniu takie uzupełnienie $\mathcal{Z}' = (J'_m, h')$ polimatroidu $\mathcal{Z}$, że $\Delta = \Delta(\mathcal{Z}')$, zawsze istnieje. Wynika to z definicji kompatybilności rodziny Δ z polimatroidem $\mathcal{Z}$. Jak już wspomnieliśmy w podrozdziale 2.2.2, każdy polimatroid boolowski jest polimatroidem reprezentowalnym. Niestety, według powyższego twierdzenia, to czy struktura dostępu wyznaczona przez polimatroid $\mathcal{Z}$ oraz pewną rodzinę monotoniczną z nim kompatybilną Δ jest portem pewnego matroidu reprezentowalnego, nie zależy od tego czy $\mathcal{Z}$ jest reprezentowalny, ale od tego czy jego takie uzupełnienie $\mathcal{Z}'$, że $\Delta = \Delta(\mathcal{Z}')$, jest polimatroidem reprezentowanym. Naszym celem w tym podrozdziale jest wskazanie, kiedy uzupełnienie jednorodnego polimatroidu boolowskiego $\mathcal{Z}$ jest także polimatroidem boolowskim. Wówczas, korzystając z twierdzenia 4.34 będziemy mogli wskazać struktury dostępu, które są portami pewnych matroidów reprezentowalnych. Oznaczenia przyjęte w podrozdziale 2.2.2 obowiązują również w tym podrozdziale. Rozpocznijmy od następującego lematu.

Lemat 4.35. *Niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *będzie podziałem zbioru uczestników* P*. Niech* $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ *będzie polimatroidem i niech* $\Delta \subsetneq \mathcal{P}(J_m)$ *będzie rodziną monotoniczną z nim kompatybilną.*

Jeśli takie uzupełnienie $\mathcal{Z}' = (J'_m, h')$ *polimatroidu* $\mathcal{Z}$*, że* $\Delta = \Delta(\mathcal{Z}')$*, jest polimatroidem boolowskim, to* $\min \Delta \subseteq \mathcal{P}_1(J_m)$*.*

Dowód. Niech rodzina $\{B_i\}_{i=0,1,\ldots,m}$ będzie reprezentacją boolowską uzupełnienia $\mathcal{Z}'$ polimatroidu $\mathcal{Z}$. Wtedy $B_0 = \{x\}$ jest zbiorem jednoelementowym, ponieważ $h(\{0\}) = 1$, gdzie $x \in \bigcup_{i \in J_m} B_i$. Gdyby $x \notin \bigcup_{i \in J_m} B_i$, to Δ byłaby zbiorem

pustym. Załóżmy, że $A \in \Delta$. Wtedy

$$h(A \cup \{0\}) = |\bigcup_{i \in A} B_i \cup B_0| = h(A),$$

zatem $x \in \bigcup_{i \in A} B_i$, a stąd $x \in B_i$ dla pewnego $i \in A$. Ponadto zauważmy, że $h(\{0, i\}) = h(\{i\})$, więc $\{i\} \in \Delta$. To pokazuje, że jedynie zbiory jednoelementowe są możliwymi zbiorami minimalnymi rodziny Δ. □

Na postawie powyższego twierdzenia widzimy, że poszukiwania struktur dostępu będących portami matroidów reprezentowalnych należy zawęzić do takich struktur, które są wyznaczone przez jednorodne polimatroidy boolowskie i rodziny monotoniczne z nimi kompatybilne, których zbiory minimalne są jednoelementowe.

Twierdzenie 4.36. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ będzie jednorodnym polimatroidem boolowskim i niech $\Delta \subseteq \mathcal{P}(P)$ będzie taką rodziną monotoniczną z nim kompatybilną, że $\min \Delta = \mathcal{P}_1(X)$ dla pewnego $X \subseteq J_m$.*

Jeśli liczba w_k, $k = |X|$, jest dodatnia, to struktura dostępu Γ wyznaczona przez polimatroid $\mathcal{Z}$ i rodzinę Δ jest portem pewnego matroidu reprezentowalnego.

Dowód. Niech $\{B_i\}_{i=1,\ldots,m}$ będzie reprezentacją boolowską polimatroidu $\mathcal{Z}$. Na podstawie twierdzenia 2.49 otrzymujemy, że $w_k \geqslant 0$ dla każdego $k \in J_m$.

Wykażemy, iż takie uzupełnienie $\mathcal{Z}' = (J'_m, h')$ polimatroidu $\mathcal{Z}$, że $\Delta = \Delta(\mathcal{Z}')$, jest polimatroidem boolowskim. Jedyne, co należy zrobić, to wskazać punkt x ze zbioru $B = \bigcup_{i=1}^{m} B_i$, który reprezentowałby podzbiór $\{0\} \in \mathcal{P}(J'_m)$. Z założenia $w_k > 0$ otrzymujemy, że zbiór W_X jest niepusty. Niech zatem x będzie dowolnie wybranym elementem zbioru W_X. Wykażemy, że $B_0 := \{x\}$ jest dobrze zdefiniowany, to znaczy

$$h(Y) = \left|\bigcup_{i \in Y} B_i\right|$$

dla każdego $Y \subseteq J'_m$. Załóżmy, że $Y \subseteq J'_m$ i rozpatrzmy następujące przypadki:

i) $0 \notin Y$. Wówczas

$$h'(Y) = h(Y) = \left|\bigcup_{i \in Y} B_i\right|.$$

ii) $0 \in Y$. Wtedy rozważmy zbiór $U := Y \setminus \{0\}$ i ponownie rozpatrzmy dwie możliwości. Jeśli $U \in \Delta$, to istnieje takie $u \in U$, że $\{u\} \in \min \Delta$, to znaczy $u \in X$. Stąd $x \in B_u$ oraz

$$h'(Y) = h'(U \cup \{0\}) = h'(U) = h(U) = \left|\bigcup_{i \in U} B_i\right| = \left|\bigcup_{i \in U} B_i \cup B_0\right| = \left|\bigcup_{i \in Y} B_i\right|.$$

Jeśli $U \notin \Delta$, to dla każdego $u \in U$ mamy $\{u\} \notin \min\Delta$, to znaczy $u \notin X$. Stąd $x \notin B_u$ to dla każdego $u \in U$ oraz

$$h'(Y) = h'(U \cup \{0\}) = h'(U)+1 = h(U)+1 = \left|\bigcup_{i\in U} B_i\right|+1 = \left|\bigcup_{i\in U} B_i \cup B_0\right| = \left|\bigcup_{i\in Y} B_i\right|.$$

Na podstawie stwierdzenia 2.41 otrzymujemy, iż takie uzupełnienie $\mathcal{Z}' = (J'_m, h')$ polimatroidu $\mathcal{Z}$, że $\Delta = \Delta(\mathcal{Z}')$, jest polimatroidem reprezentowalnym. Stosując teraz twierdzenie 4.34 otrzymujemy tezę. □

Przykład 4.37. Rozważmy polimatroid jednorodny $\mathcal{Z} = (J_4, h)$, który wyznacza ciąg $\boldsymbol{g} = (g_0, g_1, g_2, g_3, g_4)$, $g_4 = 0$. Z przykładu 2.51 wiemy, że polimatroid (J_4, h) ma reprezentację boolowską wtedy i tylko wtedy, gdy $\frac{g_1+g_3}{2} \geqslant g_2$ oraz $\frac{g_0-g_3}{3} \geqslant g_1 - g_2$. Zauważmy, że jeśli przyjmiemy $g_0 = 4, g_1 = 3, g_2 = 2, g_3 = 1$, to polimatroid $\mathcal{Z}$ jest boolowski.

Dalej, niech $\min\Delta = \{\{1\}\}$. Zauważmy, że z wniosku 2.48, a dokładniej z (2.4), otrzymujemy, że $w_1 = g_3 > 0$. Stosując teraz twierdzenie 4.36, wnioskujemy, że struktura dostępu Γ wyznaczona przez polimatroid $\mathcal{Z}$ i rodzinę Δ jest portem pewnego matroidu reprezentowalnego. Warte zauważenia jest, że w tym przypadku uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest typu $Ord_\Gamma(J_m \setminus \{1\}, \{1\})$. W ten sposób wykazaliśmy, że istnieją hierarchiczne struktury dostępu, które są portami pewnych matroidów reprezentowalnych, ale nie są strukturami oddziałowymi ani ściśle hierarchicznymi.

Przykład 4.38. Rozważmy polimatroid jednorodny $\mathcal{Z} = (J_4, h)$, który wyznacza ciąg $\boldsymbol{g} = (g_0, g_1, g_2, g_3, g_4)$, $g_4 = 0$. Zauważmy, że jeśli przyjmiemy $g_0 = 8, g_1 = 6$, $g_2 = 4, g_3 = 1$, to polimatroid $\mathcal{Z}$ jest nie jest polimatroidem boolowskim ponieważ $\frac{g_1+g_3}{2} = \frac{7}{2} < 4 = g_2$. Jednakże sygnatura ciągu $\boldsymbol{g}$ jest taka sama, jak sygnatura ciągu z powyższego przykładu. Jeśli $\min\Delta = \{\{1\}\}$, to struktura dostępu Γ wyznaczona przez polimatroid $\mathcal{Z}$ i rodzinę Δ nie musi być portem żadnego polimatroidu reprezentowalnego. W tym przypadku uporządkowanie zbioru $(\Pi, \preccurlyeq_\Gamma)$ jest również typu $Ord_\Gamma(J_m \setminus \{1\}, \{1\})$.

4.6 Przykłady idealnej oddziałowej struktury dostępu

W podrozdziale 3.4 omówiliśmy znane oddziałowe struktury dostępu, które są idealne. Jak dotąd, najszerszą klasę taki struktur podał Farràs [7]. Są to struktury postaci 3.6. Farràs zdołał także wykazać, że te struktury dostępu są portami pewnych matroidów reprezentowalnych.

Wykażemy, że warunki podane przez Farràsa nie są warunkami koniecznymi, aby oddziałowa struktura dostępu była portem pewnego matroidu reprezentowalnego, to znaczy pokażemy, że istnieją inne trójdzielne, oddziałowe struktury dostępu, które są portami matroidów reprezentowalnych.

Niech $\Pi = \{\Pi_1, \Pi_2, \Pi_3\}$ będzie podziałem zbioru uczestników P. Niech Γ będzie taką strukturą dostępu, że $\min \Gamma = \{\bar{w} \in \mathbb{N}_0^3 : \bar{a} \leqslant_s \bar{w} \leqslant_s \bar{b}, |\bar{w}| = d\}$, dla pewnych $d \in \mathbb{N}$ oraz $\bar{a}, \bar{b} \in \mathbb{N}_0^3$. Załóżmy, że ta struktura dostępu jest wyznaczona przez pewien polimatroid jednorodny $\mathcal{Z} = (J_3, h)$ i kompatybilną z nim rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(P)$. Załóżmy ponadto, że $\boldsymbol{g} = (g_0, g_1, g_2)$ jest ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$ oraz $g_0 > g_2 > 0$. Z przyjętych założeń wynika, że

$$\{\bar{w} \ : \bar{a} \leqslant_s \bar{w} \leqslant_s \bar{b}, |\bar{w}| = d\} = \min \Gamma = \min(\mathcal{B}(\mathcal{Z}, X) \ : \ X \in \Delta).$$

Zauważmy, że dla każdego wektora minimalnego $\bar{w}$ mamy $d = |\bar{w}| = h_{|\operatorname{supp} \bar{w}|}$, więc nośniki wszystkich minimalnych wektorów autoryzowanych są równoliczne, bo ciąg h_1, h_2, h_3 jest rosnący.

Przypuśćmy, że wszystkie minimalne wektory autoryzowane mają nośniki jednoelementowe, więc $\{(d,0,0),(0,d,0),(0,0,d)\} = \min \Gamma$. Gdyby któryś z tych wektorów nie był minimalny, to struktura dostępu nie byłaby spójna, a zatem nie byłaby oddziałowa (zob. 3.28). Z definicji zbioru minimalnego mamy $\bar{a} = (0,0,0)$ oraz $(d,d,d) = \bar{b}$. Ale w takim przypadku

$$\bar{v} := (d-1,1,0) \in \{\bar{w} \ : \bar{a} \leqslant_s \bar{w} \leqslant_s \bar{b}, |\bar{w}| = d\} = \min \Gamma$$

i $|\operatorname{supp} \bar{v}| = 2$, bo $d = h_1 > 1$, co jest sprzeczne z założeniem, że minimalne wektory autoryzowane mają nośniki jednoelementowe.

Przypuśćmy, że minimalne wektory autoryzowane mają nośniki dwuelementowe. Podobnie jak poprzednio muszą być co najmniej dwa takie wektory, na przykład $\bar{w} = (w_1, w_2, 0), \bar{v} = (v_1, 0, v_3)$, bo w przeciwnym razie struktura byłaby niespójna. Z założeń wynika, że $w_1 + w_2 = d$ oraz $\bar{a} = (a,0,0)$. Oczywiście $\bar{w} \in \mathcal{B}(\mathcal{Z}, \{1,2\})$, $d = |\bar{w}| = h_2 = g_0 + g_1 \geqslant 3$. Jeśli $a < w_1$, to wektor $(w_1 - 1, w_2, 1)$ jest minimalnym wektorem autoryzowanym z nośnikiem 3-elementowym, co daje sprzeczność. Jeśli $w_2 > 1$, to znów otrzymujemy sprzeczność, bo wektor $(w_1, w_2 - 1, 1)$ jest minimalnym wektorem autoryzowanym z nośnikiem 3-elementowym. To pokazuje, że $\bar{w} = (a,1,0) \in \mathcal{B}(\mathcal{Z}, \{1,2\})$ lecz również $\bar{w}' = (1,a,0) \in \mathcal{B}(\mathcal{Z}, \{1,2\})$. Stąd wynika, że $a = 1$ i dalej $3 \leqslant h_2 = |\bar{w}| = 2$, co znowu daje sprzeczność.

Z tych obliczeń wynika, że nośniki wektorów minimalnych mają 3 elementy, zatem $\Delta = \{J_3\}$. W ten sposób pokazaliśmy, że trójdzielna, oddziałowa struktura dostępu Γ wyznaczona przez polimatroid z $g_0 > g_2 > 0$ i kompatybilną z nim rodzinę monotoniczną $\Delta \neq \{J_3\}$ nie jest postaci 3.6. Takie struktury dostępu znajdziemy w kolumnach 4-6 tabeli 4.2, z wyłączeniem wiersza pierwszego i ostatniego. Teraz stosując twierdzenie 3.24 otrzymujemy, że te struktury dostępu są także portami pewnych matroidów reprezentowalnych.

Rozdział 5

Algebraiczna charakteryzacja porządku hierarchicznego

Celem tego rozdziału jest uogólnienie pojęcia hierarchicznie minimalnych zbiorów autoryzowanych zdefiniowanych przez Farràsa i Padró w pracy [10] poświęconej ściśle hierarchicznym strukturom dostępu. Badanie struktur dostępu za ich pomocą ma istotną zaletę, gdyż tworzą one podzbiór rodziny minimalnych zbiorów autoryzowanych, a zatem jest ich mniej. Rozpoczniemy od wprowadzenia nowego porządku w zbiorze wektorowych reprezentacji podzbiorów uczestników. Porządek ten umożliwi nam zdefiniowanie rodziny hierarchicznie minimalnych zbiorów autoryzowanych, które, jak się przekonamy, wyznaczają strukturę dostępu. Przedstawimy także metodę, nawiązującą do znanego z teorii badań operacyjnych „zadania transportowego", pozwalającą efektywnie porównywać reprezentacje wektorowe podzbiorów uczestników w sensie tego właśnie porządku.

Ustalmy strukturę dostępu $\Gamma \subsetneq \mathcal{P}(P)$ oraz niech $\Pi_{ka}^{\Gamma} = \{P_1, \ldots, P_l\}$ będzie podziałem zbioru P na klasy abstrakcji wyznaczone przez Γ (zob. 3.4). Zgodnie z wcześniejszymi rozważaniami, relacja $\preccurlyeq_{\Gamma}$ zadana wzorem (3.2) (lub równoważnie (3.4)) jest w zbiorze Π_{ka}^{Γ} nie tylko praporządkiem, lecz porządkiem częściowym (zob. uwaga 3.9). Porządek ten pozwala nam zdefiniować częściowy porządek w zbiorze $J_l = \{1, \ldots, l\}$ wzorem:

$$i \preccurlyeq_{\Gamma} j \iff P_i \preccurlyeq_{\Gamma} P_j. \tag{5.1}$$

W poprzednich rozdziałach rozważaliśmy zbiór $\pi(\mathcal{P}(P)) \subseteq \mathbb{Z}^l$, wprowadzony w podrozdziale 3.2, czyli rodzinę wektorowych reprezentacji podzbiorów zbioru uczestników P, wraz z porządkiem standardowym $\leqslant_s$ dziedziczonym z $\mathbb{Z}^l$. Pokażemy teraz jak w zbiorze $\mathbb{Z}^l$, a zatem również w $\pi(\mathcal{P}(P))$, wprowadzić porządek za pomocą porządku określonego na zbiorze J_l.

Stwierdzenie 5.1. *Niech $(J_l, \preccurlyeq)$ będzie zbiorem częściowego uporządkowanym oraz niech*

$$T = \{(i,j) \in J_l \times J_l : i \text{ jest bezpośrednim poprzednikiem } j\}.$$

Relacja w zbiorze $\mathbb{Z}^l$, określona dla $\bar{w}, \bar{v} \in Z^l$ wzorem:

$$\bar{w} \preccurlyeq \bar{v} \iff \begin{cases} \bar{w} \leqslant_s \bar{v}, & \text{jeśli } T = \emptyset, \\ \bigvee\limits_{\substack{\alpha_{ij} \in \mathbb{N}_0 \\ (i,j) \in T}} \bar{w} + \sum\limits_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{v}, & \text{jeśli } T \neq \emptyset \end{cases} \tag{5.2}$$

jest relacją częściowego porządku. Ponadto

$$\bar{w} \leqslant_s \bar{v} \implies \bar{w} \preccurlyeq \bar{v}$$

dla dowolnych $\bar{w}, \bar{v} \in \mathbb{Z}^l$.

Dowód. Tezę dodatkową oraz zwrotność otrzymujemy natychmiast, przyjmując współczynniki $\alpha_{ij} = 0$, $(i,j) \in T$. W celu sprawdzenia przechodniości weźmy takie wektory $\bar{w}, \bar{v}, \bar{u} \in \mathbb{Z}^l$, że $\bar{w} \preccurlyeq \bar{v}$ i $\bar{v} \preccurlyeq \bar{u}$. Wówczas istnieją takie α_{ij}, $\beta_{ij} \in \mathbb{N}_0$, $(i,j) \in T$, że

$$\bar{w} + \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{v} \quad \text{oraz} \quad \bar{v} + \sum_{(i,j)\in T} \beta_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{u}.$$

Dodając nierówności stronami i odejmując $\bar{v}$, otrzymujemy

$$\bar{w} + \sum_{(i,j)\in T} (\alpha_{ij} + \beta_{ij})(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{u},$$

co pokazuje, że $\bar{w} \preccurlyeq \bar{u}$.

Wykazanie własności antysymetrii będzie wymagało nieco więcej wysiłku. Weźmy bowiem takie $\bar{w}, \bar{v} \in \mathbb{Z}^l$, że $\bar{w} \preccurlyeq \bar{v}$ oraz $\bar{v} \preccurlyeq \bar{w}$, a więc istnieją takie współczynniki $\alpha_{ij}, \beta_{ij} \in \mathbb{N}_0$, $(i,j) \in T$, że

$$\bar{w} + \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{v} \quad \text{oraz} \quad \bar{v} + \sum_{(i,j)\in T} \beta_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{w}.$$

Dodając stronami obie nierówności i odejmując $\bar{v} + \bar{w}$, dostajemy

$$\bar{u} := \sum_{(i,j)\in T} (\alpha_{ij} + \beta_{ij})(\bar{e}_j - \bar{e}_i) \leqslant_s \theta_l, \tag{5.3}$$

gdzie $\theta_l \in \mathbb{Z}^l$ jest wektorem zerowym.

Pokażemy, że z warunku (5.3) wynikają warunki

$$\gamma_{ij} := \alpha_{ij} + \beta_{ij} = 0, \quad \text{dla każdego } (i,j) \in T,$$

skąd wynikać będzie również, iż $\alpha_{ij} = \beta_{ij} = 0$ dla każdego $(i,j) \in T$, a w konsekwencji $\bar{v} = \bar{w}$. Uczynimy to za pomocą indukcji względem malejącej rangi elementu j w zbiorze $(J_l, \preccurlyeq)$. Przypomnijmy, że rangą $r(j)$ elementu j w zbiorze uporządkowanym nazywamy długość najdłuższego łańcucha spośród wszystkich łańcuchów o końcu w j. Przyjmijmy oznaczenie $J_l^{(r)} = \{j \in (J_l, \preccurlyeq) : r(j) = r\}$ na zbiór złożony z elementów zbioru J_l o randze równej r, oraz niech

$$z := \max\{r(j) : j \in (J_l, \preccurlyeq)\}$$

będzie maksymalną rangą w $(J_l, \preccurlyeq)$. Zauważmy również, że współrzędna o indeksie $m \in J_l$ wektora $\bar{u} = \sum_{(i,j)\in T} \gamma_{ij}(\bar{e}_j - \bar{e}_i)$ jest równa

$$u_m = \sum_{(i,m)\in T} \gamma_{im} - \sum_{(m,j)\in T} \gamma_{mj}.$$

Elementy o randze z są elementami maksymalnymi w $(J_l, \preccurlyeq)$, a zatem nie mogą być poprzednikami innych elementów z J_l. Stąd współrzędna o indeksie $m \in J_l^{(z)}$ wektora $\bar{u}$ jest równa

$$u_m = \sum_{(i,m)\in T} \gamma_{im} \geqslant 0. \tag{5.4}$$

Biorąc pod uwagę nierówność (5.3), otrzymujemy $u_m = 0$, więc $\gamma_{im} = 0$ dla $(i,m) \in T$, $m \in J_l^z$.

Niech teraz $0 \leqslant k < z$ oraz załóżmy (założenie indukcyjne), że $\gamma_{im} = 0$ dla $(i,m) \in T$, $m \in \bigcup_{r>k} J_l^{(r)}$. Pokażemy, że $\gamma_{im} = 0$ dla $(i,m) \in T$, $m \in J_l^{(k)}$. Istotnie, jeśli $(m,j) \in T$, $m \in J_l^{(k)}$, to $j \in \bigcup_{r>k} J_l^{(r)}$ jest elementem rangi większej niż k, więc z założenia indukcyjnego $\gamma_{mj} = 0$ dla $(m,j) \in T$. Stąd dla $m \in J_l^{(k)}$ ponownie zachodzi nierówność (5.4), co wraz z (5.3) daje nam $\gamma_{im} = 0$ dla $(i,m) \in T$, $m \in J_l^{(k)}$, i dowodzi kroku indukcyjnego.

W ten sposób pokazaliśmy, że $\gamma_{ij} = 0$ dla każdego $(i,j) \in T$, a zatem określona wzorem (5.2) relacja $\preccurlyeq$ jest antysymetryczna. □

Stosując powyższe stwierdzenie do zbioru $(J_l, \preccurlyeq_\Gamma)$, z porządkiem określonym wzorem (5.1), otrzymujemy porządek częściowy $\preccurlyeq_\Gamma$ na $\mathbb{Z}^l$, który ograniczony do $\pi(\mathcal{P}(P))$, ma następującą interpretację, wynikającą z definicji (5.2). Niech bowiem $\bar{w}, \bar{v} \in \pi(\mathcal{P}(P))$ oraz $\bar{w} \in \pi(\Gamma)$, a więc istnieją zbiory uczestników $A, B \subseteq P$ reprezentowane przez te wektory oraz $A \in \Gamma$ jest zbiorem autoryzowanym. Jeśli $\bar{w} \preccurlyeq_\Gamma \bar{v}$, to możemy wymienić pewną liczbę uczestników ze zbioru A na innych, hierarchicznie nadrzędnych i otrzymać zbiór zawarty w zbiorze B reprezentowanym przez $\bar{v}$. Zatem zbiór B reprezentowany przez $\bar{v}$ również jest zbiorem autoryzowanym.

Szczególnie interesujące dla nas będą wektory w zbiorze $\pi(\Gamma) \subseteq (\mathbb{Z}^l, \preccurlyeq_\Gamma)$, minimalne względem tego porządku. Wprowadźmy następującą definicję.

Definicja 5.2. *Hierarchicznie minimalnymi zbiorami autoryzowanymi* nazywamy zbiory reprezentowane przez wektory minimalne w zbiorze $\pi(\Gamma)$ względem porządku $(\mathbb{Z}^l, \preccurlyeq_\Gamma)$. Rodzinę hierarchicznie minimalnych zbiorów autoryzowanych struktury dostępu Γ oznaczamy $\operatorname{hmin}\Gamma$.

Zauważmy, że $\operatorname{hmin}\Gamma \subseteq \min\Gamma$. Istotnie, niech $A \in \operatorname{hmin}\Gamma$ oraz $B \in \Gamma$, $B \subseteq A$. Niech wektory $\bar{w}, \bar{v} \in \pi(\Gamma)$ reprezentują zbiory A i B, odpowiednio. Skoro $B \subseteq A$, to $\bar{v} \leqslant_s \bar{w}$, skąd $\bar{v} \preccurlyeq_\Gamma \bar{w}$, więc z minimalności $\bar{w}$ mamy $\bar{v} = \bar{w}$. Jednakże $B \subseteq A$, więc $B = A$, zatem A jest zbiorem minimalnym w Γ. Jasne jest ponadto, że jeśli weźmiemy zbiór należący do $\operatorname{hmin}\Gamma$, a następnie dowolnego uczestnika w tym zbiorze zamienimy na innego, hierarchicznie podrzędnego, to otrzymamy zbiór nieautoryzowany.

Celem dalszych rozważań jest przedstawienie prostszego sposobu, równoważnego wzorowi 5.2, na porównywanie wektorów należących do $(\pi(\mathcal{P}(P)), \preccurlyeq_\Gamma)$. Sposób ten będzie polegał na porównywaniu odpowiednich sum, których składnikami będą współrzędne porównywanych wektorów.

5.1 Zmodyfikowane zadanie transportowe

W tym podrozdziale sformułujemy problem, który nazwiemy zmodyfikowanym zadaniem transportowym. W istocie będzie to znane z teorii programowania liniowego zadanie transportowe, z dodatkowymi ograniczeniami nałożonymi na rozwiązania. Pokażemy także warunki, przy których zadanie to będzie miało rozwiązanie dopuszczalne. Zaprezentujemy również algorytm prowadzący do tego rozwiązania. W dalszej części pracy pokażemy jak te wyniki wykorzystać do porównywania wektorów reprezentujących podzbiory uczestników schematu dzielenia sekretu.

Na początku przedstawimy klasyczne zadanie transportowe zaprezentowane na przykład w [26]. Zadanie transportowe polega na opracowaniu planu przewozów pewnego towaru od dostawców do odbiorców, w oparciu o zgłaszane przez nich wielkości podaży i popytu, który to plan będzie minimalizował łączne koszty transportu. W celu jego omówienia przyjmijmy następujące oznaczenia:

- m – liczba dostawców,
- n – liczba odbiorców,
- $\mathbf{D} = \{D_1, \ldots, D_m\}$ – zbiór dostawców,
- $\mathbf{O} = \{O_1, \ldots, O_n\}$ – zbiór odbiorców,
- d_i – podaż i-tego dostawcy, $i = 1, \ldots, m$,
- o_j – popyt j-tego odbiorcy, $j = 1, \ldots, n$,
- c_{ij} – koszt przewozu jednostki towaru od i-tego dostawcy do j-tego odbiorcy,

- x_{ij} – ilość towaru przewożona od i-tego dostawcy do j-tego odbiorcy.

Możemy wówczas sformułować problem następująco:

$$\begin{cases} \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} x_{ij} \to \min, \\ \sum_{j=1}^{n} x_{ij} = d_i \text{ dla } i = 1, \ldots, m, \\ \sum_{i=1}^{m} x_{ij} = o_j \text{ dla } j = 1, \ldots, n, \\ x_{ij} \geqslant 0, \text{ dla } i = 1, \ldots, m, \ j = 1, \ldots, n. \end{cases}$$

Zadanie transportowe jest szczególnym przypadkiem zadania programowania liniowego, a więc można rozwiązywać je metodą simpleks, jednakże wykorzystując jego specyficzne cechy opracowano wygodniejsze i bardziej efektywne metody jego rozwiązywania. Podobnie jednak jak w metodzie simpleks, w pierwszej fazie poszukuje się pewnego rozwiązania dopuszczalnego, a w drugiej fazie iteracyjnie ulepsza się je, przechodząc od jednego rozwiązania dopuszczalnego do następnego. Jeśli zadanie jest zbilansowane, to znaczy łączna podaż dostawców jest równa łącznemu popytowi odbiorców:

$$\sum_{i=1}^{m} d_i = \sum_{j=1}^{n} o_j,$$

to rozwiązanie dopuszczalne zawsze istnieje. Jeśli łączna podaż przewyższa łączny popyt, rozwiązanie konstruuje się wprowadzając fikcyjnego odbiorcę, a wówczas popyt wszystkich odbiorców jest zaspokojony, natomiast u dostawców pozostaje nadwyżka towaru. W sytuacji przeciwnej, gdy łączny popyt przewyższa łączną podaż, dodatkową podaż zapewnia fikcyjny dostawca, podaż wszystkich dostawców zostaje przetransportowana do odbiorców, natomiast popyt odbiorców nie jest w pełni zaspokojony. Ze sformułowania problemu widać ponadto, że zbiór rozwiązań dopuszczalnych jest domknięty i ograniczony w przestrzeni $\mathbb{R}^{mn}$, więc skoro zbiór ten jest niepusty, istnienie rozwiązania optymalnego wynika z ciągłości funkcji celu.

Istnienie rozwiązania dopuszczalnego dla zadania zbilansowanego wynika z prostego algorytmu, którym można się posłużyć do konstrukcji takiego rozwiązania, zwanego metodą kąta północno-zachodniego. Polega ona na wypełnianiu macierzy przewozów $(x_{ij})_{i=1,\ldots,m}^{j=1,\ldots,n}$ maksymalnymi możliwymi wielkościami transportu pomiędzy kolejnymi dostawcami a odbiorcami, począwszy od górnego, lewego elementu tej macierzy:

1. $i := 1$, $j := 1$.
2. Jeśli $d_i > o_j$, to
   - $x_{ij} := o_j$, $x_{kj} = 0$ dla $k > i$,
   - $o_j := 0$, $d_i := d_i - o_j$,

- $j := j + 1$, idź do kroku 5.

3. Jeśli $d_i < o_j$, to
   - $x_{ij} := d_i$, $x_{ik} = 0$ dla $k > j$,
   - $d_i := 0$, $o_j := o_j - d_i$,
   - $i := i + 1$, idź do kroku 5.
4. Jeśli $d_i = o_j$, to
   - $x_{ij} := d_i$, $x_{ik} = 0$ dla $k > j$, $x_{kj} = 0$ dla $k > i$,
   - $o_j := 0$, $d_i := 0$,
   - $j := j + 1$, $i := i + 1$, idź do kroku 5.
5. Jeśli $i \leqslant m$ oraz $j \leqslant n$, idź do kroku 2.

Zauważmy, iż z algorytmu tego wynika ponadto, iż jeśli zgłaszany popyt i podaż wyrażony jest w liczbach całkowitych, to uzyskane rozwiązanie również będzie całkowitoliczbowe.

Przedstawimy teraz problem będący modyfikacją przedstawionego powyżej zadania transportowego. W klasycznym problemie wprowadzamy trzy zmiany. Po pierwsze, transport towaru na wybranych trasach, pomiędzy niektórymi dostawcami i odbiorcami, jest niedozwolony. Po drugie, zależy nam jedynie na zaspokojeniu popytu odbiorców. Nadwyżka podaży może pozostać u dostawców. Po trzecie, ponieważ interesować nas będzie jedynie istnienie rozwiązania dopuszczalnego, w sformułowaniu problemu pomijamy całkowicie funkcję celu.

Definicja 5.3. Zmodyfikowanym zadaniem transportowym z m dostawcami oraz n odbiorcami nazywamy problem:

$$\begin{cases} \sum_{j=1}^{n} x_{ij} \leqslant d_i \text{ dla } i = 1, \ldots, m, \\ \sum_{i=1}^{m} x_{ij} = o_j \text{ dla } j = 1, \ldots, n, \\ x_{ij} \geqslant 0, \text{ dla } (i,j) \in R, \\ x_{ij} = 0, \text{ dla } (i,j) \notin R. \end{cases} \tag{5.5}$$

gdzie $R \subseteq \{1, \ldots, m\} \times \{1, \ldots, n\}$ jest ustalonym zbiorem dozwolonych tras.

Pomimo, iż pomijamy funkcję celu, aby być w zgodzie z tradycyjną terminologią, dowolne rozwiązanie $(x_{ij})_{i=1,\ldots,m}^{j=1,\ldots,n}$ powyższego problemu nazywać będziemy rozwiązaniem dopuszczalnym zmodyfikowanego zadania transportowego.

Przedstawimy teraz algorytm prowadzący do pewnego rozwiązania dopuszczalnego tego problemu. Idea tego algorytmu polega na rekurencyjnym podziale danego zadania na zadania z mniejszą liczbą odbiorców, do momentu, w którym do otrzymanego w wyniku podziału zadania będzie można zastosować metodę

kąta północno-zachodniego. Przyjmijmy następujące oznaczenie na zbiór wskaźników tych dostawców, którzy mogą dostarczać towar odbiorcy O_j:

$$\overline{O}_j = \{i \in \{1, \ldots, m\} : (i, j) \in R\}, \quad j = 1, \ldots, n.$$

Zauważmy, że znajomość zbiorów $\overline{O}_j$, $j = 1, \ldots, n$, jest równoważna znajomości zbioru R, więc możemy formułować zmodyfikowane zadanie transportowe określając zamiast zbioru R powyższe zbiory. Rozpoczniemy od trywialnej obserwacji.

Lemat 5.4. *Zmodyfikowane zadanie transportowe z jednym odbiorcą ma rozwiązanie dopuszczalne, jeżeli*

$$o_1 \leqslant \sum_{i \in \overline{O}_1} d_i,$$

Dowód. Niech $\bar{k} = \min\left\{k \in \overline{O}_1 : o_1 \leqslant \sum_{i \in \overline{O}_1,\, i \leqslant k} d_i\right\}$. Wówczas

$$x_{i1} = \begin{cases} d_i & \text{dla } i \in \overline{O}_1,\ i < \bar{k}, \\ o_1 - \displaystyle\sum_{i \in \overline{O}_1,\, i < \bar{k}} d_i, & \text{dla } i = \bar{k}, \\ 0 & \text{dla pozostałych } i \in \{1, \ldots, m\} \end{cases}$$

jest poszukiwanym rozwiązaniem. □

Kolejny lemat pokazuje jak znaleźć rozwiązanie zadania z dwoma odbiorcami.

Lemat 5.5. *Zmodyfikowane zadanie transportowe z dwoma odbiorcami ma rozwiązanie dopuszczalne, jeżeli*

1. $o_j \leqslant \sum_{i \in \overline{O}_j} d_i$, $j \in \{1, 2\}$,
2. $o_1 + o_2 \leqslant \sum_{i \in \overline{O}_1 \cup \overline{O}_2} d_i$.

Dowód. Rozważmy następujące przypadki:

i) $o_1 \leqslant \sum_{i \in \overline{O}_1 \setminus \overline{O}_2} d_i$ oraz $o_2 \leqslant \sum_{i \in \overline{O}_2 \setminus \overline{O}_1} d_i$. W tym przypadku popyt odbiorców jest zaspokajany przez ich „wyłącznych dostawców". Wystarczy zatem rozważyć dwa zmodyfikowane zadania transportowe z jednym odbiorcą: pierwsze z odbiorcą O_1 i dostawcami o indeksach ze zbioru $\overline{O}_1 \setminus \overline{O}_2$, drugie z odbiorcą O_2 i dostawcami o indeksach ze zbioru $\overline{O}_2 \setminus \overline{O}_1$.

ii) $o_1 \leqslant \sum_{i \in \overline{O}_1 \setminus \overline{O}_2} d_i$ oraz $o_2 > \sum_{i \in \overline{O}_2 \setminus \overline{O}_1} d_i$. Ponieważ zbiory $\overline{O}_1 \setminus \overline{O}_2$ oraz $\overline{O}_2$ są rozłączne, popyt odbiorcy O_1 możemy dzięki założeniom tego przypadku zaspokoić podażą jego wyłącznych dostawców, a popyt odbiorcy O_2, na mocy założenia $o_2 \leqslant \sum_{i \in \overline{O}_2} d_i$, możemy zaspokoić korzystając z podaży dostawców o indeksach ze zbioru $\overline{O}_2$. Ponownie wystarczy zatem rozważyć odpowiednie zadania z jednym odbiorcą: pierwsze z odbiorcą O_1 i dostawcami o indeksach z $\overline{O}_1 \setminus \overline{O}_2$, drugie z odbiorcą O_2 i dostawcami o indeksach z $\overline{O}_2$.

iii) $o_1 > \sum_{i\in\overline{O}_1\setminus\overline{O}_2} d_i$ oraz $o_2 \leqslant \sum_{i\in\overline{O}_2\setminus\overline{O}_1} d_i$. Przypadek symetryczny do poprzedniego.

iv) $o_1 > \sum_{i\in\overline{O}_1\setminus\overline{O}_2} d_i$ oraz $o_2 > \sum_{i\in\overline{O}_2\setminus\overline{O}_1} d_i$. Jest to najtrudniejszy przypadek. W pierwszym kroku przydzielamy odbiorcom towar od ich wyłącznych dostawców: całość towaru od dostawców o indeksach ze zbioru $\overline{O}_1 \setminus \overline{O}_2$ do odbiorcy O_1 oraz całość towaru od dostawców o indeksach ze zbioru $\overline{O}_2 \setminus \overline{O}_1$ do odbiorcy O_2. Zgodnie z założeniami rozpatrywanego przypadku nie wystarcza to jednakże do zaspokojenia ich popytu. Zatem w drugim kroku tworzymy nowe, zredukowane zadanie transportowe, w którym zbiór dostawców to $\{D_i : i \in \overline{O}_1 \cap \overline{O}_2\}$, a odbiorcy zgłaszają popyt obniżony o wielkość zaspokojoną w pierwszym kroku: $\tilde{o}_1 := o_1 - \sum_{i\in\overline{O}_1\setminus\overline{O}_2} d_i$, $\tilde{o}_2 := o_2 - \sum_{i\in\overline{O}_2\setminus\overline{O}_1} d_i$. Kluczowy jednakże jest teraz fakt, iż w tym zadaniu wszystkie trasy są dozwolone: $R = (\overline{O}_1 \cap \overline{O}_2) \times \{1, 2\}$. Zgodnie z założeniami lematu mamy teraz

$$o_1 + o_2 \leqslant \sum_{i\in\overline{O}_1\cup\overline{O}_2} d_i = \sum_{i\in\overline{O}_1\setminus\overline{O}_2} d_i + \sum_{i\in\overline{O}_2\setminus\overline{O}_1} d_i + \sum_{i\in\overline{O}_1\cap\overline{O}_2} d_i,$$

więc

$$\tilde{o}_1 + \tilde{o}_2 = o_1 + o_2 - \sum_{i\in\overline{O}_1\setminus\overline{O}_2} d_i - \sum_{i\in\overline{O}_2\setminus\overline{O}_1} d_i \leqslant \sum_{i\in\overline{O}_1\cap\overline{O}_2} d_i.$$

Zatem popyt odbiorców w nowym zadaniu transportowym można zaspokoić podażą pozostałych w nim dostawców. Ponieważ wszystkie trasy są dozwolone, rozwiązanie tego zadania uzyskujemy stosując, na przykład, metodę kąta północnozachodniego (po ewentualnym zbilansowaniu dodatkowym odbiorcą). □

Przejdźmy do problemu z dowolną liczbę odbiorców.

Stwierdzenie 5.6. *Jeśli spełniony jest warunek:*

$$\bigwedge_{L\subseteq\{1,\ldots,n\}} \left(\sum_{j\in L} o_j \leqslant \sum_{i\in\bigcup_{j\in L}\overline{O}_j} d_i \right), \tag{5.6}$$

to istnieje rozwiązanie dopuszczalne zmodyfikowanego zadania transportowego z n odbiorcami.

Dowód. Pokażemy jak konstruować rozwiązanie poprzez podział na zadania z mniejszą liczbą odbiorców. Na początek zauważmy, że założenia lematów 5.4 i 5.5 są szczególnymi przypadkami warunku (5.6), odpowiednio dla $n = 1$ i $n = 2$, zatem pierwsze dwa kroki indukcji wynikają z tych lematów. Ustalmy $n > 2$ i załóżmy, że teza stwierdzenia jest spełniona dla dowolnego zmodyfikowanego zadania transportowego z k odbiorcami, gdzie $k < n$.

Rozważmy zadanie z n odbiorcami. Dla niepustych podzbiorów $\emptyset \neq A \subseteq \{1, \ldots, n\}$ przyjmujemy

$$\Phi(A) := \sum_{i\in\overline{O}_A} d_i - \sum_{j\in A} o_j,$$

gdzie

$$\overline{O}_A := \bigcup_{j\in A} \overline{O}_j,$$

oznacza zbiór indeksów dostawców, którzy mogą dostarczać towar do odbiorców o indeksach ze zbioru A, oraz niech

$$\Phi^* = \min\{\Phi(A) : \emptyset \neq A \subsetneq \{1,\dots,n\}\}.$$

Z założenia (5.6) wynika, że $\Phi^* \geqslant 0$. Niech M będzie dowolnym zbiorem realizującym to minimum:

$$\Phi(M) = \Phi^* \leqslant \Phi(A), \quad A \subsetneq \{1,\dots,n\}. \tag{5.7}$$

Rozważmy zadanie transportowe z dostawcami D_i o podaży d_i, $i \in \{1,\dots,m\}$, ograniczone do odbiorców O_j, $j \in M$, z popytem o_j i zbiorami dostawców $\{D_i : i \in \overline{O}_j\}$, $j \in M$. Ponieważ M jest właściwym podzbiorem $\{1,\dots,n\}$, więc $|M| < n$, a warunek (5.6) jest spełniony w szczególności dla podzbiorów M, zatem na mocy założenia indukcyjnego, zadanie to ma rozwiązanie dopuszczalne x_{ij}, $i \in \{1,\dots,m\}$, $j \in M$. Rozwiązanie to stanowi część rozwiązania wyjściowego problemu z n odbiorcami. Zauważmy, że w rozwiązaniu tym $x_{ij} = 0$ dla $i \in \{1,\dots,m\} \setminus \overline{O}_M$, $j \in M$.

Aby znaleźć rozwiązanie dla pozostałych odbiorców O_j, $j \in \{1,\dots,n\} \setminus M$, rozważmy kolejne zadanie transportowe, zredukowane do tych odbiorców. W tym zadaniu popyt o_j oraz zbiory dozwolonych dostawców $\{D_i : i \in \overline{O}_j\}$, gdzie $j \in \{1,\dots,n\} \setminus M$, są takie jak w wyjściowym problemie z n odbiorcami, natomiast dostawcy D_i, $i \in \{1,\dots,m\}$, dysponują podażą pomniejszoną o ilość towaru przydzieloną w poprzednim kroku odbiorcom o indeksach ze zbioru M:

$$\tilde{d}_i = d_i - \sum_{j\in M} x_{ij}, \quad i \in \{1,\dots,m\}.$$

Pokażemy, że dla tego zadania spełniony jest warunek (5.6). Ustalmy niepusty zbiór $A \subseteq \{1,\dots,n\} \setminus M$. Z własności (5.7) mamy $\Phi(M) \leqslant \Phi(A \cup M)$, czyli

$$\sum_{i\in\overline{O}_M} d_i - \sum_{j\in M} o_j \leqslant \sum_{i\in\overline{O}_{M\cup A}} d_i - \sum_{j\in M\cup A} o_j.$$

Ponieważ $\sum_{j\in A} o_j = \sum_{j\in M\cup A} o_j - \sum_{j\in M} o_j$ oraz

$$\overline{O}_{M\cup A} = \overline{O}_M \cup \overline{O}_A = \overline{O}_M \cup (\overline{O}_A \setminus \overline{O}_M),$$

więc z ostatniej nierówności wynika, że

$$\sum_{i\in A} o_j = \sum_{j\in M\cup A} o_j - \sum_{j\in M} o_j \leqslant \sum_{i\in\overline{O}_{M\cup A}} d_i - \sum_{i\in\overline{O}_M} d_i = \sum_{i\in\overline{O}_A\setminus\overline{O}_M} d_i.$$

Zatem

$$\sum_{i\in A} o_j \leqslant \sum_{i\in\overline{O}_A\setminus\overline{O}_M} d_i = \sum_{i\in\overline{O}_A\setminus\overline{O}_M} d_i - \sum_{i\in\overline{O}_A\setminus\overline{O}_M}\sum_{j\in M} x_{ij} =$$
$$= \sum_{i\in\overline{O}_A\setminus\overline{O}_M}\Big(d_i - \sum_{j\in M} x_{ij}\Big) = \sum_{i\in\overline{O}_A\setminus\overline{O}_M} \tilde{d}_i \leqslant \sum_{i\in\overline{O}_A} \tilde{d}_i,$$

co należało pokazać. Ponownie korzystając z założenia indukcyjnego, zadanie to ma rozwiązanie dopuszczalne x_{ij}, $i \in \{1,\ldots,m\}$, $j \in \{1,\ldots,n\}\setminus M$, które jednocześnie określa brakujące wielkości przewozów do odbiorców O_j, $j\in \{1,\ldots,n\}\setminus M$, w wyjściowym zadaniu z n odbiorcami. □

Przedstawimy teraz przykład ilustrujący opisaną powyżej metodę rozwiązywanie zmodyfikowanego zadania transportowego.

Przykład 5.7. Rozważmy zadanie z czterema odbiorcami O_1, O_2, O_3, O_4 oraz ośmioma dostawcami $D_1,\ldots,D_8$. Poniższa tabela zawiera warunki początkowe zadania. Pierwsza kolumna zawiera wartości podaży dostawców, a liczby w pierwszym wierszu to popyt odbiorców. Znak „X" w ciele tabeli oznacza, że droga pomiędzy dostawcą a odbiorcą jest niedozwolona. Pola tabeli odpowiadające zbiorowi dozwolonych tras R są na początku puste.

		9	10	8	10
		O_1	O_2	O_3	O_4
8	D_1		X		
4	D_2				X
6	D_3			X	
9	D_4	X			
7	D_5		X		X
3	D_6			X	X
5	D_7	X	X	X	
5	D_8			X	

Tabela 1. Warunki początkowe zadania z czterema odbiorcami.

W pierwszym kroku wyznaczamy podzbiór zbioru odbiorców, dla którego nadwyżka dostępnej dla tych odbiorców podaży nad zgłaszanym przez nich popytem jest najmniejsza. Przy czterech odbiorcach musimy wykonać obliczenia dla $2^4 - 2 = 14$ zbiorów (pomijamy zbiór pusty i zbiór wszystkich odbiorców). W naszym przykładzie minimum realizuje podzbiór $\{O_1, O_2, O_3\}$, dla którego nadwyżka ta jest równa:

$$(o_1 + o_2 + o_3) - (d_1 + d_2 + d_3 + d_4 + d_5 + d_6 + d_8) = 15.$$

Zatem w kroku drugim rozważamy zadanie zredukowane do zbioru odbiorców $\{O_1, O_2, O_3\}$, którego warunki początkowe przedstawia tabela 2.

		9	10	8
		O_1	O_2	O_3
8	D_1		X	
4	D_2			
6	D_3			X
9	D_4	X		
7	D_5		X	
3	D_6			X
5	D_7	X	X	X
5	D_8			X

Tabela 2. Warunki początkowe zadania zredukowanego do zbioru odbiorców $\{O_1, O_2, O_3\}$.

Aby rozwiązać to zadanie ponownie szukamy zbioru minimalizującego nadwyżkę podaży nad popytem. Tym razem minimum realizuje zbiór $\{O_2\}$, zatem w kolejnym kroku rozwiązujemy zadanie z jednym tylko odbiorcą, które rozwiązujemy zgodnie z lematem 5.4, przydzielając towar od kolejnych dostawców do wyczerpania popytu. Tabele 3a i 3b przedstawiają warunki początkowe oraz rozwiązanie tego zadania.

		10
		O_2
8	D_1	X
4	D_2	
6	D_3	
9	D_4	
7	D_5	X
3	D_6	
5	D_7	X
5	D_8	

		10
		O_2
8	D_1	0
0	D_2	4
0	D_3	6
9	D_4	0
7	D_5	0
3	D_6	0
5	D_7	0
5	D_8	0

Tabela 3. Zadanie z odbiorcą O_2. a) Warunki początkowe, b) Rozwiązanie.

Pierwsza kolumna tabeli 3a zawiera podaż dostawców pomniejszoną o ilość towaru przydzielonego odbiorcy O_2. Wartości te wykorzystujemy w kolejnym kroku,

jako wartości podaży dostawców w zadaniu z pozostałymi odbiorcami zadania z kroku 2, czyli z odbiorcami O_1 i O_3. Zadanie to możemy rozwiązać metodą opisaną w lemacie 5.5. Warunki początkowe i rozwiązanie tego zadania przedstawiają tabele 4a i 4b. Ponownie w pierwszej kolumnie tabeli z rozwiązaniem popyt został pomniejszony o wielkości towaru przydzielonego odbiorcom.

		9	8
		O_1	O_3
8	D_1		
0	D_2		
0	D_3		X
9	D_4	X	
7	D_5		
3	D_6		X
5	D_7	X	X
5	D_8		X

		9	8
		O_1	O_3
7	D_1	1	0
0	D_2	0	0
0	D_3	0	0
1	D_4	0	8
7	D_5	0	0
0	D_6	3	0
5	D_7	0	0
0	D_8	5	0

Tabela 4. Zadanie z odbiorcami O_1 i O_3. a) Warunki początkowe b) Rozwiązanie.

W ten sposób rozwiązaliśmy zadanie z odbiorcami $\{O_1, O_2, O_3\}$. Wracając do wyjściowego zadania z 4 odbiorcami, pozostaje do rozwiązania zadanie z odbiorcą O_4, przy podaży dostawców wyznaczonej w ostatnim kroku. To zadanie wraz z rozwiązaniem przedstawia tabela 5.

		10
		O_4
7	D_1	
0	D_2	X
0	D_3	
1	D_4	
7	D_5	X
0	D_6	X
5	D_7	
0	D_8	

		10
		O_4
0	D_1	7
0	D_2	0
0	D_3	0
0	D_4	1
7	D_5	0
0	D_6	0
3	D_7	2
0	D_8	0

Tabela 5. Zadanie zredukowane z odbiorcą O_4. a) Warunki początkowe b) Rozwiązanie.

Łącząc rozwiązanie z kolejnych kroków otrzymujemy rozwiązanie zadania z 4 odbiorcami, przedstawione w tabeli 6. Dodatkowa, ostatnia kolumna zawiera wielkość niezrealizowanej podaży.

		9	10	8	10	
		O_1	O_2	O_3	O_4	
8	D_1	1	0	0	7	0
4	D_2	0	4	0	0	0
6	D_3	0	6	0	0	0
9	D_4	0	0	8	1	0
7	D_5	0	0	0	0	7
3	D_6	3	0	0	0	0
5	D_7	0	0	0	2	3
5	D_8	5	0	0	0	0

Tabela 6. Rozwiązanie zadania z 4 odbiorcami. Wartości w ostatniej kolumnie oznaczają niezrealizowaną podaż dostawców.

5.2 Charakteryzacja porządku hierarchicznego

W tym podrozdziale pokażemy zastosowanie stwierdzenia 5.6 do porównywania reprezentacji wektorowych zbiorów uczestników struktury dostępu. Ustalmy $l \in \mathbb{N}$ oraz częściowy porządek $\preccurlyeq$ w zbiorze J_l. Przypomnijmy, że

$$T = \{(i, j) \in J_l \times J_l : i \text{ jest bezpośrednim poprzednikiem } j\}.$$

Wprowadźmy następującą definicję.

Definicja 5.8. Podzbiór $I \subseteq J_l$ nazywamy *podzbiorem monotonicznym* zbioru J_l, jeśli

$$\bigwedge_{i \in I} \bigwedge_{j \in J_l} (i \preccurlyeq j \Longrightarrow j \in I).$$

Definiujemy zbiory:

- $H_0^l := \{\sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \in \mathbb{Z}^l : \alpha_{ij} \in \mathbb{N}_0\}$,
- $H^l := H_0^l + \mathbb{N}_0^l$.

Lemat 5.9. *Jeśli wektor $\bar{w} \in H^l$, to $\sum_{k\in I} w_k \geqslant 0$ dla każdego niepustego, monotonicznego podzbioru I zbioru J_l.*

Dowód. Niech $I \subseteq J_l$ będzie niepustym podzbiorem monotonicznym zbioru J_l. Rozważmy wektor charakterystyczny zbioru I, to znaczy taki wektor $\bar{c}$ o długości l, że $c_k = 1$, gdy $k \in I$ oraz $c_k = 0$ w przeciwnym przypadku. Jeśli $\bar{w} \in H^l$, to

$$\bar{w} = \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) + \sum_{k\in J_l} \beta_k \bar{e}_k$$

dla pewnych $\alpha_{ij}, \beta_k \in \mathbb{N}_0$. Obliczając iloczyn skalarny $\bar{w} \circ \bar{c}$ otrzymujemy

$$\begin{aligned}\sum_{k\in I} w_k = \bar{w} \circ \bar{c} &= \left(\sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) + \sum_{k\in J_l} \beta_k \bar{e}_k \right) \circ \bar{c} = \\ &= \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \circ \bar{c} + \sum_{k\in J_l} \beta_k \bar{e}_k \circ \bar{c}.\end{aligned}$$

Jeśli $(i,j) \in T$, to z monotoniczności I mamy następujące przypadki:

$$(\bar{e}_j - \bar{e}_i) \circ \bar{c} = \begin{cases} 0 & \text{gdy } j \notin I, \\ 1 & \text{gdy } j \in I, i \notin I, \\ 0 & \text{gdy } i,j \in I, \end{cases}$$

a zatem kontynuując powyższy rachunek

$$\sum_{k\in I} w_k = \sum_{\substack{(i,j)\in T \\ j\in I, i\notin I}} \alpha_{ij} + \sum_{k\in I} \beta_k \geqslant 0. \qquad \square$$

Stwierdzenie 5.10. *Niech $\bar{w} \in \mathbb{Z}^l$. Jeśli $\sum_{k\in I} w_k \geqslant 0$ dla każdego niepustego, monotonicznego podzbioru I zbioru J_l, to $\bar{w} \in H^l$.*

Dowód. Ustalmy wektor $\bar{w} \in \mathbb{Z}^l$ o własności opisanej w założeniach lematu. Aby wykazać, że $\bar{w} \in H^l$, należy wskazać takie $\alpha_{ij}, \beta_k \in \mathbb{N}_0$, że

$$\bar{w} = \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) + \sum_{k\in J_l} \beta_k \bar{e}_k. \tag{5.8}$$

Jeśli wszystkie współrzędne wektora $\bar{w}$ są nieujemne, to wystarczy przyjąć $\alpha_{i,j} = 0$ dla każdego $(i,j) \in T$ oraz $\beta_k = w_k$ dla każdego $k \in J_l$.

W przeciwnym przypadku współczynniki $\alpha_{ij}, \beta_k \in \mathbb{N}_0$ można odnaleźć wyznaczając rozwiązanie dopuszczalne zmodyfikowanego zadania transportowego. W zadaniu tym dostawcami będą indeksy współrzędnych wektora $\bar{w}$ o wartościach dodatnich:

$$\mathbf{D} := \{k \in J_l : w_k > 0\},$$

a odbiorcami indeksy współrzędnych wektora $\bar{w}$ o wartościach ujemnych:

$$\mathbf{O} := \{k \in J_l : w_k < 0\}.$$

W celu ułatwienia wypowiedzi zamiast $k \in \mathbf{D}$ lub $k \in \mathbf{O}$ czasami będziemy po prostu pisać D_k lub O_k. Pomijamy indeksy wektora $\bar{w}$ o współrzędnych równych 0. Za popyt i podaż przyjmujemy wartości bezwzględne odpowiednich współrzędnych wektora $\bar{w}$:

$$d_k := w_k, \quad \text{dla } k \in \mathbf{D}, \qquad o_k := |w_k| = -w_k, \quad \text{dla } k \in \mathbf{O}.$$

Transport od dostawcy D_i do odbiorcy O_j jest dozwolony, jeśli istnieje łańcuch (niekoniecznie wyznaczony jednoznacznie) w zbiorze $(J_l, \preccurlyeq)$ o początku w j oraz końcu w i. Zatem zbiór dozwolonych tras jest równy

$$R = \{(i,j) \in J_l \times J_l : i \in \mathbf{D},\ j \in \mathbf{O},\ j \preccurlyeq i\},$$

a stąd zbiór indeksów dostawców, którzy mogą dostarczać towar odbiorcy O_j, jest równy

$$\overline{O}_j := \{i \in \mathbf{D} : j \preccurlyeq i\}, \quad j \in \mathbf{O}.$$

Pokażemy teraz, że z założenia o wektorze $\bar{w}$, wynika założenie (5.6) lematu 5.6, które zapiszemy tu w postaci

$$\bigwedge_{L \subseteq \mathbf{O}} \left(\sum_{j \in L} o_j \leqslant \sum_{i \in \bigcup_{j \in L} \overline{O}_j} d_i \right).$$

Ustalmy zbiór $L \subseteq \mathbf{O}$. Niech

$$K = L \cup \bigcup_{j \in L} \overline{O}_j = L \cup \{i \in \mathbf{D} :\ \text{istnieje takie } j \in L,\ \text{że } j \preccurlyeq i\}$$

oraz niech $I = \{k \in J_l :\ \text{istnieje takie } i \in K,\ \text{że } i \preccurlyeq k, \}$ będzie najmniejszym podzbiorem monotonicznym J_l zawierającym K. Zauważmy, że jeśli $k \in I \setminus K$, to $w_k \leqslant 0$. W przeciwnym wypadku k byłby dostawcą, a będąc większym od elementów zbioru K, musiałby również być większy od pewnego odbiorcy ze zbioru L, a zatem musiałby należeć do K. Skoro I jest zbiorem monotonicznym, to z założenia $0 \leqslant \sum_{k \in I} w_k = \sum_{k \in K} w_k + \sum_{k \in I \setminus K} w_k$, więc dzięki naszej obserwacji mamy również

$$0 \leqslant \sum_{k \in K} w_k = \sum_{k \in L} w_k + \sum_{k \in \bigcup_{j \in L} \overline{O}_j} w_k = -\sum_{j \in L} o_j + \sum_{i \in \bigcup_{j \in L} \overline{O}_j} d_i,$$

co pokazuje żądany warunek. Możemy zatem zastosować lemat 5.6, otrzymując rozwiązanie dopuszczalne naszego zmodyfikowanego zadania transportowego, więc takie liczby $x_{ij}, i \in \mathbf{D}, j \in \mathbf{O}$, że

$$\begin{cases} \sum_{j \in \mathbf{O}} x_{ij} \leqslant d_i = w_i \text{ dla } i \in \mathbf{D}, \\ \sum_{i \in \mathbf{D}} x_{ij} = o_j = -w_j = |w_j| \text{ dla } j \in \mathbf{O}, \\ x_{ij} \geqslant 0, \text{ dla } j \preccurlyeq i,\ i \in \mathbf{D},\ j \in \mathbf{O}, \\ x_{ij} = 0, \text{ dla pozostałych } i \in \mathbf{D},\ j \in \mathbf{O}. \end{cases}$$

Rozważmy teraz graf skierowany G będący diagramem Hassego zbioru $(J_l, \preccurlyeq)$. Zauważmy, że zbiór T jest zbiorem krawędzi tego grafu. Wykonujemy następujące kroki:

1. Wszystkim krawędziom grafu G przypisujemy wagi równe 0.
2. Jeśli transport pomiędzy odbiorcą O_r a dostawcą D_s jest dozwolony, czyli $r \preccurlyeq s$, to wybieramy jedną ścieżkę $\mathfrak{L}_{r,s}$ grafu G o początku w r i końcu w s. Zbiór ustalonych w ten sposób ścieżek oznaczamy przez $\mathfrak{L}$.
3. Do wagi każdej krawędzi należącej do ścieżki $\mathfrak{L}_{r,s}$ dodajemy x_{sr}. Pewne krawędzie mogą być zawarte w wielu ścieżkach, więc wagi tych krawędzi będą powiększane tyle razy, ile jest zawierających je ścieżek, ustalonych w punkcie drugim.

Współczynnik α_{ij}, $(i,j) \in T$, definiujemy teraz jako wagę krawędzi (i,j) grafu G, czyli

$$\alpha_{ij} := \sum_{\substack{\mathfrak{L}_{r,s} \in \mathfrak{L} \\ (i,j) \in \mathfrak{L}_{r,s}}} x_{sr}. \tag{5.9}$$

Za β_k dla $k \in \mathbf{D}$ przyjmujemy niezrealizowaną podaż dostawcy D_k:

$$\beta_k := d_k - \sum_{j \in \mathbf{O}} x_{kj} = w_k - \sum_{j \preccurlyeq k, j \in \mathbf{O}} x_{kj}, \quad k \in \mathbf{D}.$$

Dla $k \in J_l \setminus \mathbf{D}$ przyjmujemy $\beta_k := 0$. Oczywiście $\alpha_{ij}, \beta_k \in N_0$.

Pozostało pokazać, że tak określone współczynniki spełniają równość (5.8), czyli równoważnie, że k-ta współrzędna wektora $\bar{w}$, czyli w_k, jest równa

$$\gamma_k := \sum_{(i,k) \in T} \alpha_{ik} - \sum_{(k,j) \in T} \alpha_{kj} + \beta_k, \quad k \in J_l.$$

Ustalmy $k \in J_l$ i przyjmijmy

$$L_1 := \{\mathfrak{L}_{r,s} \in \mathfrak{L} : \text{ istnieje takie } i \in J_l, \text{ że krawędź } (i,k) \in \mathfrak{L}_{r,s}\},$$
$$L_2 := \{\mathfrak{L}_{r,s} \in \mathfrak{L} : \text{ istnieje takie } j \in J_l, \text{ że krawędź } (k,j) \in \mathfrak{L}_{r,s}\},$$

i rozważmy następujące przypadki:

i) Jeśli $k \in \mathbf{D}$ jest dostawcą, to podstawiając zdefiniowane powyżej wartości współczynników α_{ij}, β_k otrzymujemy

$$\gamma_k = \sum_{(i,k) \in T} \sum_{\substack{\mathfrak{L}_{r,s} \in \mathfrak{L} \\ (i,k) \in \mathfrak{L}_{r,s}}} x_{sr} - \sum_{(k,j) \in T} \sum_{\substack{\mathfrak{L}_{r,s} \in \mathfrak{L} \\ (k,j) \in \mathfrak{L}_{r,s}}} x_{sr} + w_k - \sum_{j \preccurlyeq k, j \in \mathbf{O}} x_{kj}. \tag{5.10}$$

Skoro k jest dostawcą i należy do ścieżki $\mathfrak{L}_{r,s}$ wraz ze swoim bezpośrednim poprzednikiem, to należy do niej również z pewnym swoim bezpośrednim następnikiem, poza przypadkiem, gdy ścieżka ta kończy się w k. Stąd otrzymujemy $L_2 \subseteq L_1$, oraz

$$L_1 \setminus L_2 = \{\mathfrak{L}_{r,k} \in \mathfrak{L} : \text{ istnieje takie } i \in J_l, \text{ że krawędź } (i,k) \in \mathfrak{L}_{r,k}\}.$$

Ponadto oczywista jest równość

$$\{r \in J_l : \mathfrak{L}_{r,k} \in \mathfrak{L} \text{ oraz istnieje takie } i \in J_l, \text{ że krawędź } (i,k) \in \mathfrak{L}_{r,k}\} = \\ = \{r \in J_l : r \preccurlyeq k, r \in \mathbf{O}\}.$$

Zatem

$$\sum_{(i,k)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (i,k)\in\mathfrak{L}_{r,s}}} x_{sr} - \sum_{(k,j)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (k,j)\in\mathfrak{L}_{r,s}}} x_{sr} = \sum_{j\preccurlyeq k, j\in\mathbf{O}} x_{kj}.$$

Wstawiając otrzymane wyrażenie do (5.10) otrzymujemy $\gamma_k = w_k$ dla $k \in \mathbf{D}$.

ii) Dla $k \in J_l \setminus \mathbf{D}$, skoro $\beta_k = 0$, mamy nieco prostsze wyrażenie

$$\gamma_k = \sum_{(i,k)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (i,k)\in\mathfrak{L}_{r,s}}} x_{sr} - \sum_{(k,j)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (k,j)\in\mathfrak{L}_{r,s}}} x_{sr}.$$

Jeśli $k \in \mathbf{O}$ jest odbiorcą oraz należy do ścieżki $\mathfrak{L}_{r,s}$ wraz ze swoim bezpośrednim następnikiem, to należy do niej również z pewnym swoim bezpośrednim poprzednikiem, chyba że ścieżka ta rozpoczyna się w k, zatem tym razem mamy $L_1 \subseteq L_2$ oraz

$$L_2 \setminus L_1 = \{\mathfrak{L}_{k,s} \in \mathfrak{L} : \text{ istnieje takie } j \in J_l, \text{ że krawędź } (k,j) \in \mathfrak{L}_{k,s}\}.$$

oraz oczywiście

$$\{s \in J_l : \mathfrak{L}_{k,s} \in \mathfrak{L} \text{ oraz istnieje takie } j \in J_l, \text{ że krawędź } (k,j) \in \mathfrak{L}_{k,s}\} = \\ = \{s \in J_l : k \preccurlyeq s, s \in \mathbf{D}\}.$$

Stąd i z własności rozwiązania zadania transportowego dla $k \in \mathbf{O}$ mamy zatem

$$\gamma_k = \sum_{(i,k)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (i,k)\in\mathfrak{L}_{r,s}}} x_{sr} - \sum_{(k,j)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (k,j)\in\mathfrak{L}_{r,s}}} x_{sr} = - \sum_{k\preccurlyeq j, j\in\mathbf{D}} x_{jk} = -o_k = w_k.$$

Jeśli $k \in J_l \setminus (\mathbf{D} \cup \mathbf{O})$ nie jest odbiorcą ani dostawcą (co ma miejsce, gdy $w_k = 0$), to $L_1 = L_2$. Jest tak, gdyż żadna ścieżka nie kończy się, ani nie zaczyna w k, więc jeśli k należy do jakiejś ścieżki ze swoim bezpośrednim poprzednikiem, to należy do niej również ze pewnym swoim bezpośrednim następnikiem. Stąd

$$\gamma_k = \sum_{(i,k)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (i,k)\in\mathfrak{L}_{r,s}}} x_{sr} - \sum_{(k,j)\in T} \sum_{\substack{\mathfrak{L}_{r,s}\in\mathfrak{L} \\ (k,j)\in\mathfrak{L}_{r,s}}} x_{sr} = 0 = w_k, \qquad k \in J_l \setminus (\mathbf{D} \cup \mathbf{O}),$$

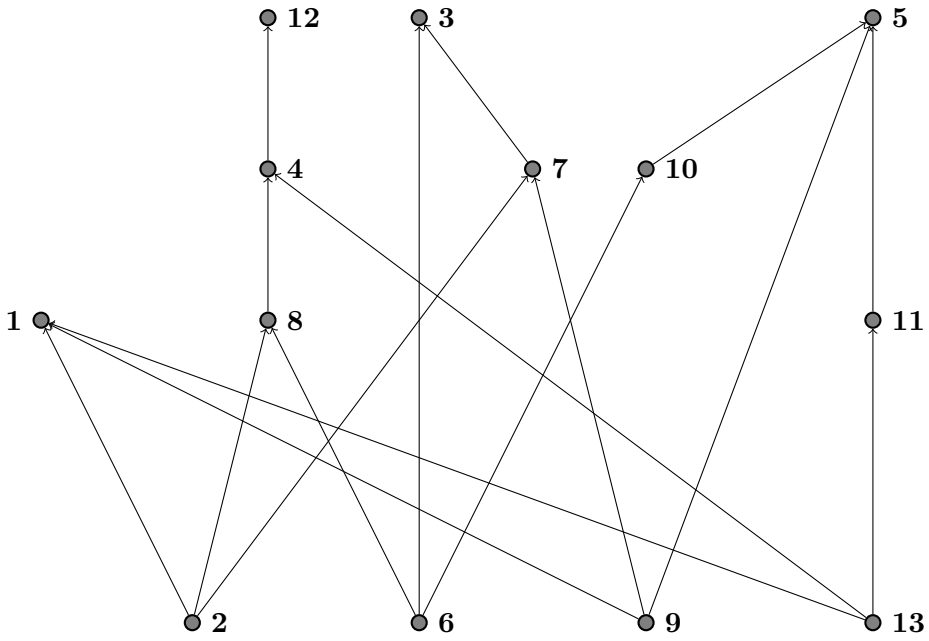
co ostatecznie dowodzi (5.8). □

Zilustrujemy teraz rozumowanie przedstawione w dowodzie powyższego stwierdzenia na przykładzie.

Przykład 5.11. Rozważmy zbiór częściowo uporządkowany $(J_{13}, \preccurlyeq)$, którego diagram Hassego jest przedstawiony na rysunku 5.1. Dalej, rozważmy wektor

$$\bar{w} = (8, -9, 4, 6, 9, -10, 7, 3, -8, 0, 5, 5, -10) \in J_{13}.$$

Po sprawdzeniu, że $\sum_{k \in I} w_k \geqslant 0$ dla każdego niepustego, monotonicznego podzbioru $I \subseteq J_{13}$, możemy przystąpić do przeprowadzenia procedury opisanej w dowodzie stwierdzenia 5.10.



Rysunek 5.1: Diagram Hassego zbioru częściowo uporządkowanego $(J_{13}, \preccurlyeq)$.

Rozpoczynamy od przeformułowania tego problemu na zmodyfikowane zadanie transportowe, które prezentujemy w tabeli 7a. Zauważmy, że z dokładnością do zmiany etykiet dostawców i odbiorców, jest to ten sam problem transportowy, który rozwiązaliśmy w przykładzie 5.7, w związku z czym po prawej stronie (tabela 7b) zamieszczamy jego rozwiązanie. Zawiera ono wartości x_{rs}, czyli liczbę jednostek towaru, jakie dostawca D_r powinien przetransportować do odbiorcy O_s. Ponadto pierwsza kolumna tabeli z rozwiązaniem zawiera wielkości niewykorzystanej podaży dostawców. Wykonujemy następujące kroki:

1. Wszystkim krawędziom diagramu Hassego przypisujemy wagi równe 0.
2. Ustalamy ścieżki pomiędzy odbiorcami i dostawcami, między którymi transport towaru jest dozwolony. Zbiór ścieżek $\mathfrak{L}$ w naszym przykładzie składa się z (ścieżki zostały pogrupowane według odbiorców, w których się zaczynają):

		9	10	8	10
		O_2	O_6	O_9	O_{13}
8	D_1		X		
4	D_3				X
6	D_4			X	
9	D_5	X			
7	D_7		X		X
3	D_8			X	X
5	D_{11}	X	X	X	
5	D_{12}			X	

		0	0	0	0
		O_2	O_6	O_9	O_{13}
0	D_1	1	0	0	7
0	D_3	0	4	0	0
0	D_4	0	6	0	0
0	D_5	0	0	8	1
7	D_7	0	0	0	0
0	D_8	3	0	0	0
3	D_{11}	0	0	0	2
0	D_{12}	5	0	0	0

Tabela 7. Zmodyfikowane zadanie transportowe dla wektora $\bar{w}$.
Warunki początkowe (a) i jego rozwiązanie (b).

$\mathfrak{L}_{2,1} = (2,1)$, $\mathfrak{L}_{2,3} = (2,7,3)$, $\mathfrak{L}_{2,4} = (2,8,4)$, $\mathfrak{L}_{2,7} = (2,7)$, $\mathfrak{L}_{2,8} = (2,8)$, $\mathfrak{L}_{2,12} = (2,8,4,12)$;

$\mathfrak{L}_{6,3} = (6,3)$, $\mathfrak{L}_{6,4} = (6,8,4)$, $\mathfrak{L}_{6,5} = (6,10,5)$, $\mathfrak{L}_{6,8} = (6,8)$, $\mathfrak{L}_{6,12} = (6,8,4,12)$;

$\mathfrak{L}_{9,1} = (9,1)$, $\mathfrak{L}_{9,3} = (9,7,3)$, $\mathfrak{L}_{9,5} = (9,5)$, $\mathfrak{L}_{9,7} = (9,7)$;

$\mathfrak{L}_{13,1} = (13,1)$, $\mathfrak{L}_{13,4} = (13,4)$, $\mathfrak{L}_{13,5} = (13,11,5)$, $\mathfrak{L}_{13,11} = (13,11)$, $\mathfrak{L}_{13,12} = (13,4,12)$.

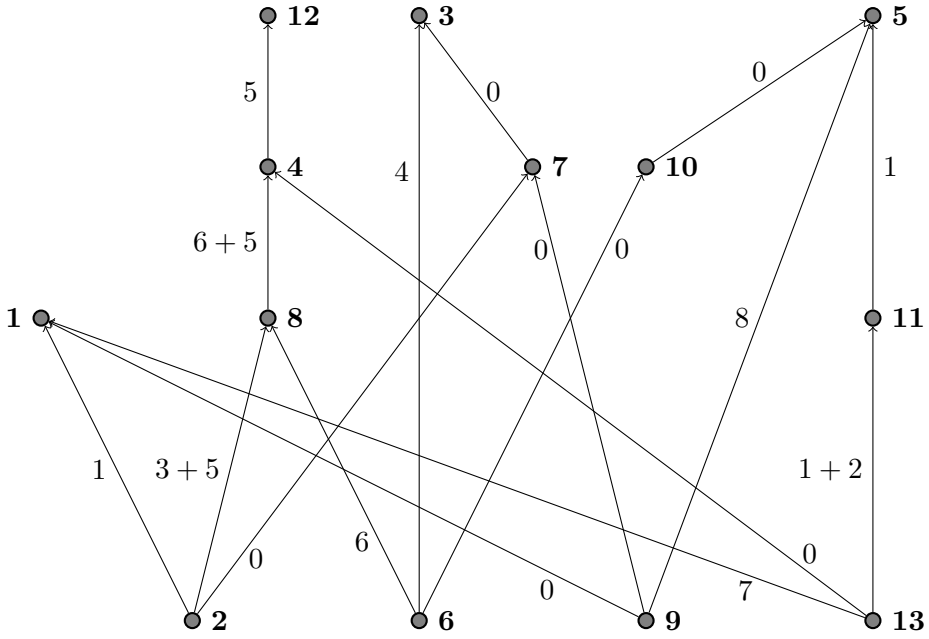
3. Przypisujemy krawędziom wagi, dodając x_{sr} do każdej krawędzi należącej do ścieżki $\mathfrak{L}_{r,s}$. Na przykład krawędź $(8,4)$ jest zawarta w ścieżkach $\mathfrak{L}_{2,4}$, $\mathfrak{L}_{2,12}$ i $\mathfrak{L}_{6,4}$, stąd jej waga wynosi $0+5+6 = 11$. Wagi przypisane krawędziom są zaprezentowane na rysunku 5.2.

Odczytujemy z grafu wartości α_{ij}, $(i,j) \in T$, natomiast z rozwiązania zadania transportowego dostajemy wartości β_k, $k \in J$, otrzymując:

$$\begin{aligned}\bar{w} &= \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) + \sum_{k\in J_l} \beta_k \bar{e}_k = \\ &= 1(\bar{e}_1 - \bar{e}_2) + 7(\bar{e}_1 - \bar{e}_{13}) + 8(\bar{e}_8 - \bar{e}_2) + 4(\bar{e}_3 - \bar{e}_6) + 11(\bar{e}_4 - \bar{e}_8) + \\ &+ 5(\bar{e}_{12} - \bar{e}_4) + 8(\bar{e}_5 - \bar{e}_9) + 1(\bar{e}_5 - \bar{e}_{11}) + 6(\bar{e}_8 - \bar{e}_6) + 3(\bar{e}_{11} - \bar{e}_{13}) + \\ &+ 7\bar{e}_7 + 3\bar{e}_{11} \in H^l.\end{aligned}$$

W ten sposób przedstawiliśmy wektor $\bar{w}$ w postaci 5.8.

Powrócimy teraz do rozważań, którymi rozpoczęliśmy ten rozdział. Niech rodzina $\Gamma \subsetneq \mathcal{P}(P)$ będzie strukturą dostępu oraz $\Pi^{\Gamma}_{ka} = \{P_1, \ldots, P_l\}$ będzie podziałem zbioru P na klasy abstrakcji wyznaczone przez Γ. Dalej, niech $(J_l, \preccurlyeq_\Gamma)$



Rysunek 5.2: Diagram Hassego z przypisanymi wagami.

będzie zbiorem częściowo uporządkowanym, gdzie relacja $\preccurlyeq_\Gamma$ jest zadana wzorem 5.1, natomiast w $\mathbb{Z}^l$ rozważamy częściowy porządek $\preccurlyeq_\Gamma$ zadany wzorem (5.2).

Jeśli dla dowolnych $\bar{u}, \bar{v} \in \mathbb{Z}^l$ chcielibyśmy rozstrzygnąć, czy $\bar{u} \preccurlyeq_\Gamma \bar{v}$, to wykorzystanie do tego zadania definicji (5.2) mogłoby nastręczyć pewnych trudności związanych z koniecznością wyznaczenia współczynników $\alpha_{ij} \in \mathbb{N}_0$, $(i,j) \in T$. Podamy teraz wygodniejszy, niż polegający na korzystaniu z definicji, sposób porównywania wektorów w $(\mathbb{Z}^l, \preccurlyeq_\Gamma)$.

Twierdzenie 5.12. *Niech $\bar{u}, \bar{v} \in \mathbb{Z}^l$. Wówczas $\bar{u} \preccurlyeq_\Gamma \bar{v}$ wtedy i tylko wtedy, gdy dla każdego niepustego, monotonicznego podzbioru I zbioru J_l zachodzi*

$$\sum_{k\in I} u_k \leqslant \sum_{k\in I} v_k. \tag{5.11}$$

Dowód. Załóżmy, że $\bar{u} \preccurlyeq_\Gamma \bar{v}$. Jeśli $T = \emptyset$, to z definicji mamy $\bar{u} \leqslant_s \bar{v}$, więc nierówność $\sum_{k\in I} u_k \leqslant \sum_{k\in I} v_k$ zachodzi dla dowolnego niepustego podzbioru $I \subseteq J_l$. Załóżmy zatem, że $T \neq \emptyset$. Istnieją wówczas takie współczynniki $\alpha_{ij} \in \mathbb{N}_0$, $(i,j) \in T$, że

$$\bar{u} + \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{v} \iff \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{v} - \bar{u}.$$

Stąd dla pewnych liczb $\beta_k \in \mathbb{N}_0$, mamy

$$\sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) + \sum_{k\in J_l} \beta_k \bar{e}_k = \bar{v} - \bar{u} =: \bar{w}.$$

Zauważmy, że wektor $\bar{w} \in H^l$, zatem na mocy lematu 5.9 otrzymujemy

$$0 \leqslant \sum_{k\in I} w_k = \sum_{k\in I}(v_k - u_k) \implies \sum_{k\in I} u_k \leqslant \sum_{k\in I} v_k,$$

dla dowolnego niepustego, monotonicznego podzbioru I zbioru J_l, co należało wykazać.

Załóżmy teraz, że $\sum_{k\in I} u_k \leqslant \sum_{k\in I} v_k$ dla każdego niepustego, monotonicznego podzbioru I zbioru J_l. Jeśli $T = \emptyset$, to każdy podzbiór zbioru J_l jest monotoniczny, w szczególności podzbiory jednoelementowe $\{1\}, \ldots, \{l\}$, a stąd

$$u_1 \leqslant v_1, \ldots, u_l \leqslant v_l \implies \bar{u} \leqslant_s \bar{v} \implies \bar{u} \preccurlyeq_\Gamma \bar{v}.$$

Rozważmy teraz przypadek, gdy $T \neq \emptyset$. Niech $\bar{w} := \bar{v} - \bar{u}$. Wówczas dla każdego niepustego, monotonicznego podzbioru $I \subseteq J_l$ mamy

$$\sum_{k\in I} u_k \leqslant \sum_{k\in I} v_k \implies \sum_{k\in I} w_k = \sum_{k\in I}(v_k - u_k) \geqslant 0.$$

Z lematu 5.10 wynika więc, że $\bar{w} \in H^l$, czyli

$$\bar{w} = \bar{v} - \bar{u} = \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) + \sum_{k\in J_l} \beta_k \bar{e}_k$$

dla pewnych $\alpha_{ij}, \beta_k \in \mathbb{N}_0$. Stąd

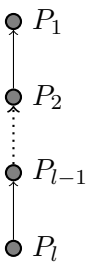
$$\bar{u} + \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) + \sum_{k\in J_l} \beta_k \bar{e}_k = \bar{v} \implies \bar{u} + \sum_{(i,j)\in T} \alpha_{ij}(\bar{e}_j - \bar{e}_i) \leqslant_s \bar{v},$$

co oznacza, że $\bar{u} \preccurlyeq_\Gamma \bar{v}$. □

Uwaga 5.13. Nie jest trudno zauważyć, że jeśli $\bar{u}, \bar{v} \in \mathbb{Z}^l$ to $\bar{u} \preccurlyeq_\Gamma \bar{v}$ wtedy i tylko wtedy, gdy dla każdego niepustego, monotonicznego podzbioru I, który nie jest sumą pewnych rozłącznych podzbiorów monotonicznych zbioru J_l zbioru J_l, zachodzi

$$\sum_{k\in I} u_k \leqslant \sum_{k\in I} v_k.$$

Przykład 5.14. Jeśli Γ jest strukturą ściśle hierarchiczną, to diagram Hassego zbioru $(\Pi^\Gamma_{ka}, \preccurlyeq_\Gamma)$ ma postać:



Warto w tym miejscu zwrócić uwagę, że dla struktur ściśle hierarchicznych Farràs i Padró [10] zdefiniowali zbiory hierarchicznie minimalne jako te, które są reprezentowane przez wektory minimalne względem częściowego porządku $(\pi(\mathcal{P}(P)), \preceq)$, gdzie $\preceq$ jest zdefiniowany następująco:

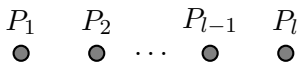
$$\bar{u} \preceq \bar{v} \iff \sum_{i=1}^{j} u_j \leqslant \sum_{i=1}^{j} v_j \tag{5.12}$$

dla każdego $j \in J_l$.

Zauważmy, że jeśli Γ jest strukturą ściśle hierarchiczną, to relacja (5.12) jest równa relacji $\preccurlyeq_\Gamma$. Istotnie, w takiej sytuacji podzbiory monotoniczne zbioru J_l to: $\{1\}, \{1,2\}, \ldots, \{1,2,\ldots,l-1\}, \{1,2,\ldots,l-1,l\}$, więc na podstawie twierdzenia 5.12 otrzymujemy

$$\bar{u} \preccurlyeq_\Gamma \bar{v} \iff \begin{cases} u_1 \leqslant v_1; \\ u_1 + u_2 \leqslant v_1 + v_2; \\ \ldots \\ u_1 + u_2 + \cdots + u_{l-1} \leqslant v_1 + v_2 + \cdots + v_{l-1}; \\ u_1 + u_2 + \cdots + u_{l-1} + u_l \leqslant v_1 + v_2 + \cdots + v_{l-1} + v_l. \end{cases}$$

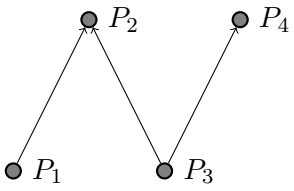
Przykład 5.15. Jeśli Γ jest strukturą oddziałową, to diagram Hassego zbioru $(\Pi_{ka}^{\Gamma}, \preccurlyeq_\Gamma)$ jest następujący:



Już we wcześniejszych rozważaniach zauważyliśmy, że w takim przypadku każdy niepusty podzbiór zbioru J_l jest jego podzbiorem monotonicznym. W świetle uwagi 5.13 otrzymujemy

$$\bar{u} \preccurlyeq_\Gamma \bar{v} \iff u_k \leqslant v_k \text{ dla każdego } k \in J_l.$$

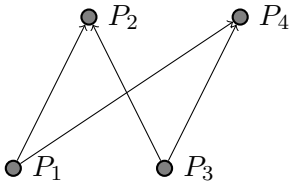
Przykład 5.16. Niech $l = 4$ oraz Γ będzie taką strukturą hierarchiczną, że diagram Hassego zbioru $(\Pi_{ka}^{\Gamma}, \preccurlyeq_\Gamma)$ jest następujący:



Podzbiory monotoniczne zbioru J_4 to: $\{2\}$, $\{4\}$, $\{1,2\}$, $\{2,3,4\}$, $\{1,2,3,4\}$, a stąd

$$\bar{u} \preccurlyeq_\Gamma \bar{v} \iff \begin{cases} u_2 \leqslant v_2; \\ u_4 \leqslant v_4; \\ u_1 + u_2 \leqslant v_1 + v_2; \\ u_2 + u_3 + u_4 \leqslant v_2 + v_3 + v_4; \\ u_1 + u_2 + u_3 + u_4 \leqslant v_1 + v_2 + v_3 + v_4. \end{cases}$$

Przykład 5.17. Niech $l = 4$ oraz Γ będzie taką strukturą hierarchiczną, że diagram Hassego zbioru $(\Pi_{ka}^{\Gamma}, \preccurlyeq_\Gamma)$ jest następujący:



Podzbiory monotoniczne zbioru J_4 to: $\{2\}$, $\{4\}$, $\{1,2,4\}$, $\{2,3,4\}$, $\{1,2,3,4\}$, a stąd

$$\bar{u} \preccurlyeq_\Gamma \bar{v} \iff \begin{cases} u_2 \leqslant v_2; \\ u_4 \leqslant v_4; \\ u_1 + u_2 + u_4 \leqslant v_1 + v_2 + v_4; \\ u_2 + u_3 + u_4 \leqslant v_2 + v_3 + v_4; \\ u_1 + u_2 + u_3 + u_4 \leqslant v_1 + v_2 + v_3 + v_4. \end{cases}$$

Zakończenie

Niniejsza rozprawa nie wyczerpuje w pełni zagadnienia dotyczącego badania hierarchiczności wielodzielnych struktur dostępu. Podczas pracy powstały pewne hipotezy, które mogą stanowić punkt wyjścia do kontynuacji badań.

Jak wiemy z rozdziału 2, w przypadku badania kompatybilności rodziny monotonicznej oraz polimatroidu jednorodnego nie są istotne ani wartości funkcji rangi, ani wartości ciągu $\boldsymbol{g}$ wyznaczonego przez ten polimatroid, lecz jedynie sygnatura ciągu $\boldsymbol{g}$. Ponadto, jeśli Γ jest strukturą wyznaczoną przez pewien polimatroid oraz rodzinę monotoniczną z nim kompatybilną, to typ uporządkowania zbioru $(\Pi, \preccurlyeq_\Gamma)$ w dowodach twierdzeń zawartych w rozdziale 4 również nie zależał od wartości wartości funkcji rangi ani wartości ciągu $\boldsymbol{g}$ wyznaczonego przez ten polimatroid. W związku z tym nasuwa się następująca hipoteza.

Hipoteza. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ oraz $\tilde{\boldsymbol{g}} = (\tilde{g}_t)_{t=0,1,\ldots,m}$ będą ciągami wyznaczonymi odpowiednio przez polimatroidy jednorodne $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i $\tilde{\mathcal{Z}} = \tilde{\mathcal{Z}}(\Pi) = (J_m, \tilde{h})$. Niech $\Delta \subsetneq \mathcal{P}(J_m)$ będzie rodziną monotoniczną kompatybilną z $\mathcal{Z}$ oraz $\tilde{\mathcal{Z}}$. Jeśli Γ oraz $\tilde{\Gamma}$ są strukturami dostępu wyznaczonymi odpowiednio przez $\mathcal{Z}$ i Δ oraz $\tilde{\mathcal{Z}}$ i Δ, to zbiory $(\Pi, \preccurlyeq_\Gamma)$ oraz $(\Pi, \preccurlyeq_{\tilde{\Gamma}})$ są równe.*

Przy badaniu spójności struktur dostępu pojawiła się hipoteza, że warunek wystarczający podany w twierdzeniu 4.30, na to, aby struktura nie była spójna, jest także warunkiem koniecznym.

Hipoteza. *Niech $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ będzie podziałem zbioru uczestników P. Niech rodzina $\Gamma \subseteq \mathcal{P}(P)$ będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ i rodzinę monotoniczną $\Delta \subsetneq \mathcal{P}(J_m)$ z nim kompatybilną. Niech $\boldsymbol{g} = (g_t)_{t=0,1,\ldots,m}$ będzie ciągiem wyznaczonym przez polimatroid $\mathcal{Z}$.*

Wtedy struktura dostępu Γ nie jest spójna wtedy i tylko wtedy, gdy $\min \Delta \neq \{J_m\}$ *oraz $g_0 = g_1 = \cdots = g_{m-1} > 0$.*

W naszych rozważaniach nie pojawiła się Π-dzielna struktura dostępu Γ, dla której w zbiorze $(\Pi, \preccurlyeq_\Gamma)$ istniałby prałańcuch długości co najmniej 2. Stąd przypuszczenie, że jest to cecha wszystkich struktur dostępu wyznaczonych przez polimatroidy jednorodne i kompatybilne z nimi rodziny monotoniczne.

Hipoteza. *Niech* $\Pi = \{\Pi_1, \ldots, \Pi_m\}$ *będzie podziałem zbioru uczestników* P. *Niech rodzina* Γ *będzie strukturą dostępu wyznaczoną przez polimatroid jednorodny* $\mathcal{Z} = \mathcal{Z}(\Pi) = (J_m, h)$ *i rodzinę monotoniczną* $\Delta \subsetneq \mathcal{P}(J_m)$ *z nim kompatybilną. Wówczas w zbiorze* $(\Pi, \preccurlyeq_\Gamma)$ *nie istnieje prałańcuch o długości przekraczającej 1.*

Bibliografia

[1] Beimel A., Livne N., Padró C., *Matroids Can Be Far from Ideal Secret Sharing*, Proceedings of the 5th Theory of Cryptography Conference 2008, Lecture Notes in Computer Science 4948, 194–212, (2008)

[2] Benaloh J., Leichter J., *Generalized Secret Sharing and Monotone Functions*, Proceedings of CRYPTO'88, Lecture Notes in Computer Science 403, 27–35, (1990)

[3] Blakley G. R., *Safeguarding Cryptographic Keys*, Proceedings of the National Computer Conference 48, 313–317, (1979)

[4] Brickell E., *Some Ideal Secret Sharing Schemes*, Proceedings of EUROCRYPT'89, Lecture Notes in Computer Science 434, 468–475, (1990)

[5] Brickell E., Davenport D., *On the Classification of Ideal Secret Sharing Schemes*, Journal of Cryptology 4 (2), 123–134, (1991)

[6] Csirmaz L., *The Size of a Share Must Be Large*, Journal of Cryptology 10 (4), 223–231, (1997)

[7] Farràs O., *Multipartite Secret Sharing Schemes*, rozprawa doktorska, (2010)

[8] Farràs O., Martí-Farré J., Padró C., *Ideal Multipartite Secret Sharing Schemes*, Proceedings of EUROCRYPT 2007, Lecture Notes in Computer Science 4515, 448–465, (2007)

[9] Farràs O., Martí-Farré J., Padró C., *Ideal Multipartite Secret Sharing Schemes*, Journal of Cryptology 25 (3), 434–463, (2012)

[10] Farràs O., Padró C., *Ideal Hierarchical Secret Sharing Schemes*, Proceedings of the 7th Theory of Cryptography Conference 2010, Lecture Notes in Computer Science 5978, 219–236, (2010)

[11] Herzog J., Hibi T., *Discrete Polimatroids*, Journal of Algebraic Combinatorics 16 (3), 239–268, (2002)

[12] Ito M., Saito A., Nishizeki T., *Secret Sharing Scheme Realizing General Access Structure*, Proceedings of the IEEE Global Telecommunications Conference 1987, 99–102, (1987)

[13] Kawa R., Kula M., *A Remark on Hierarchical Threshold Secret Sharing*, Annales UMCS sec. Informatica 12 (3), 55–64, (2012)

[14] Martí-Farré J., Padró C., *On Secret Sharing Schemes, Matroids and Polymatroids*, Proceedings of the 4th Theory of Cryptography Conference 2007, Lecture Notes in Computer Science 4392, 273–290, (2007)

[15] Martín S., Padró C., Yang A., *Secret Sharing, Rank Inequalities and Information Inequalities*, Proceedings of CRYPTO 2013, Lecture Notes in Computer Science 8043, 277–288, (2013)

[16] Oxley J. G., *Matroid Theory*, Oxford University Press, New York, (1992)

[17] Padró C., Sáez G., *Secret Sharing Schemes with Bipartite Access Structure*, IEEE Transactions on Information Theory 46 (7), 2596–2604, (2000)

[18] Sáez G., Herranz J., *New Results on Multipartite Access Structures*, IEE Proceedings – Information Security 153 (4), 153–162, (2006)

[19] Schrijver A., *Combinatorial Optimization: Polyhedra and Efficiency*, Springer, Berlin, (2003)

[20] Seymour P. D., *On Secret-Sharing Matroids*, Journal of Combinatorial Theory B 56 (1), 69–73, (1992)

[21] Shamir A., *How to Share a Secret*, Communications of the ACM 22 (11), 612–613, (1979)

[22] Simmons G.J., *How to (Really) Share a Secret*, Proceedings of CRYPTO'88, Lecture Notes in Computer Science 403, 390–448, (1990)

[23] Simonis J., Ashikhmin A. E., *Almost Affine Codes*, Designs, Codes and Cryptography 14 (2), 179–197, (1998)

[24] Tassa T., *Hierarchical Threshold Secret Sharing*, Journal of Cryptology 20 (2), 237–264, (2007)

[25] Tassa T., Dyn N., *Multipartite Secret Sharing by Bivariate Interpolation*, Journal of Cryptology 22 (2), 227–258, (2009)

[26] Trzaskalik T., *Wprowadzenie do badań operacyjnych z komputerem*, Polskie Wydawnictwo Ekonomiczne, Warszawa, (2008)

[27] Whitney H., *On the Abstract Properties of Linear Dependence*, American Journal of Mathematics 57 (3), 509–533, (1935)