TURUN YLIOPISTO

Matroidien teorian perusteita

Sakari Saikkonen

LuK.-tutkielma
tammikuu 2024

Tarkastaja:
Dos. Ville Salo

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Sakari Saikkonen: Matroidien teorian perusteita
LuK.-tutkielma, 16 s.
Matematiikka
tammikuu 2024

Hassler Whitney esitteli artikkelissaan vuonna 1935 matroidit, joilla hän yleisti vektoreiden lineaarisen riippumattomuuden käsitteen mille tahansa perusjoukolle.

Tässä tutkielmassa esitellään viisi ekvivalenttia määritelmää matroideille. Määritelmien lähtökohtina ovat riippumattomat joukot, matroidin kannat, piirit ja astefunktio.

Asiasanat: matroidit, lineaarisen riippumattomuuden absktaktit ominaisuudet, riippumattomat joukot.

Sisällys

1 Johdanto

Hassler Whitney pyrki artikkelissaan [5] vuonna 1935 vakiinnuttamaan vektoriavaruudessa lineaarisen riippuvuuden ja riippumattomuuden käsitteiden abstraktit ominaisuudet ja luomaan niiden avulla aksiomaattisen määritelmän uudelle algebralliselle objektille *matroidille* (engl. *matroid*). Pari vuotta myöhemmin myös van der Waerden käsitteli lineaarista ja abstraktia riippuvuutta aksiomaattisesti algebran oppikirjassaan Moderne Algebra [4]. Osassa matroidin rakenteista on selkeästi nähtävissä niiden tausta lineaarialgebrassa, kun taas osa heijastelee graafiteoreettista taustaansa. Näin ollen nämä aksioomat abstrahoivat myös tiettyjä graafiteorian käsitteitä [2]. Whitneyn oma tausta graafiteorissa näkyykin joissakin graafeista lainatussa matroidien termistössä [4].

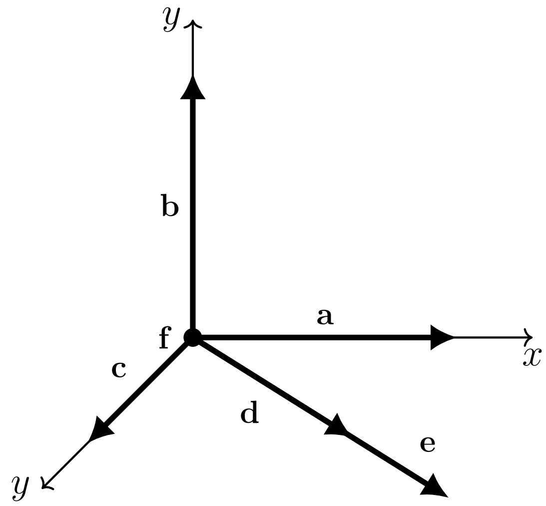
Myöhemmin matroideja on tutkittu ainakin niin hilateorian, geometrian kuin kombinatoriikankin piirissä. Tästä johtuen matroiditeorian termistö vaihtelee ja itse matroidiakin kutsutaan kirjoittajasta riippuen esimerkiksi *geometriaksi (geometry)*.[4]

Matroideille on useita määritelmiä, jotka korostavat kyseisessä käsittelyssä oleellisia matroidin ominaisuuksia. Tässä tutkielmassa esitetään äärelliselle matroideille viisi määritelmää, jotka osoitetaan yhtäpitäviksi, sekä esitellään joitakin niihin liittyviä tuloksia. Lopuksi tutustutaan lyhyesti vielä muutamiin matroidien lajitteluun liittyviin ominaisuuksiin.

Lauseiden todistukset seuraavat pääosin Welshin [4] esittämiä, paitsi missä todistus on hänen mukaansa ilmeinen, jolloin todistus on kirjoittajan.

2 Määritelmiä

2.1 Matroidin riippumattomat osajoukot



Kuva 1: Avaruuden $\mathbb{R}^3$ vektoreita.

Kuvassa 1 on esitelty joukko E_v avaruuden $\mathbb{R}^3$ vektoreita, joista vektorit **a**,**b**,**c** ovat koordinaattiakseleilla; **d**,**e** ovat keskenään samansuuntaisia xz-tasossa ja $\mathbf{f} = \mathbf{0}$ nollavektori. Lineaarialgebrassa vektorit ovat lineaarisesti riippumattomia, jos mitään niistä ei voi esittää muiden vektoreiden lineaarisena kombinaationa. Vektoreista voidaan muodostaa *joukkoperhe* (joukkojen joukko) $\mathcal{I}_v$, johon kuuluvat joukon E_v kaikki lineaarisesti riippumattomat osajoukot, eli ne osajoukot (myös tyhjä joukko $\varnothing$), joihin eivät sisälly nollavektori **f**, pari **d**,**e** taikka kolmikko **a**,**c**,**d** tai **a**,**c**,**e**, jotka ovat lineaarisesti riippuvia.

Nyt matroidi voidaan määritellä parin $(E_v, \mathcal{I}_v)$ avulla seuraavasti.

Määritelmä 1 (Riippumattomat joukot)**.** Olkoon E äärellinen joukko ja $\mathcal{I}$ sen riippumattomien osajoukkojen perhe. Pari $(E, \mathcal{I})$ on äärellinen matroidi M, E sen *perusjoukko (ground set)* ja $\mathcal{I}$ sen *riippumattomat joukot (independet sets)*, jos seuraavat aksioomat pätevät

(I1) $\varnothing \in \mathcal{I}$,

(I2) jos $X \in \mathcal{I}$, niin kaikille sen osajoukoille $Y \subset X$ pätee $Y \in \mathcal{I}$,

(I3) jos $X, Y \in \mathcal{I}$, ja $|X| = |Y| + 1$, niin on olemassa sellainen alkio $x \in X \setminus Y$, että $(Y \cup \{x\}) \in \mathcal{I}$.

Esimerkki 1. Kuvan 1 vektorijoukko E_v on äärellinen ja $\mathcal{I}_v$ on sen lineaarisesti riippumattomien osajoukkojen perhe.

Aksiooma (I2) edellyttää, että riippumattoman joukon osajoukot ovat myös riippumattomia. Esimerkiksi vektorijoukon osajoukko $X = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ on lineaarisesti riippumaton, kuten ovat myös sen kaikki osajoukot $\{$**a**,**b**$\}$, $\{$**a**,**c**$\}$,$\{$**b**,**c**$\}$ sekä yksittäisten vektoreiden muodostamat joukot ja tyhjä joukko. Sama voidaan osoittaa muillekin joukkoperheen $\mathcal{I}_v$ joukoille. Ensimmäinen aksiooma itse asiassa seuraa toisesta, sillä tyhjä joukko on jokaisen joukon osajoukko.

Olkoon X kuten edellä ja $Y = \{\mathbf{a}, \mathbf{d}\} \in \mathcal{I}_v$. Joukkojen kardinaliteeteille pätee $|X| = 3 = 2 + 1 = |Y| + 1$ ja $X \setminus Y = \{\mathbf{b}, \mathbf{c}\}$. Nyt $Y \cup \{\mathbf{b}\} = \{\mathbf{a}, \mathbf{b}, \mathbf{d}\} \in \mathcal{I}_v$, ja sama voidaan osoittaa muillakin lineaarisesti riippumattomilla joukoilla, joten joukkoperhe $\mathcal{I}_v$ toteuttaa myös aksiooman (I3). Tässä ei olisi voitu valita $x = \mathbf{c}$, sillä vektorit $\mathbf{a}$,$\mathbf{c}$ ja $\mathbf{d}$ ovat samassa tasossa ja siten linaarisesti riippuvia.

Joukkoperhe $\mathcal{I}_v$ toteuttaa kaikki määritelmän 1 aksioomat, joten $(E_v, \mathcal{I}_v)$ on matroidi ja $\mathcal{I}_v$ on sen riippumattomat joukot.

Esimerkissä joukkoperhe $\mathcal{I}_v$ määriteltiin niin, että se sisälsi perusjoukon kaikki riippumattomat osajoukot, mutta tämä ei ole välttämätöntä. Voidaankin määritellä perhe $\mathcal{I}_X = 2^X$ edellisen esimerkin joukon X potenssijoukkona eli sen kaikkina osajoukkoina. Tällöin $\mathcal{I}_X$ toteuttaa määritelmän 1 aksioomat ja siten myös pari $(E_v, \mathcal{I}_X)$ on matroidi ja $\mathcal{I}_X$ on sen riippumattomat joukot.

Vaikka tässä on rinnastettu riippumattomuus ja lineaarinen riippumattomuus, eivät ne ole täysin indenttiset käsitteet. Joukko vektoreita saattaa olla lineaarisesti riippumaton, mutta ei riippumaton tietyssä matroidissa. Esimerkiksi $\{\mathbf{d}\}$ on lineaarisesti riippumaton joukko, mutta $\{\mathbf{d}\} \notin \mathcal{I}_X$, joten se ei ole riippumaton matroidissa $M(E_v, \mathcal{I}_X)$.

Sanotaankin, että joukko Z on riippuva matroidissa $M(E, \mathcal{I})$, jos $Z \notin \mathcal{I}$, eli jos se ei ole riippumaton.

Tarkastellaan seuraavaksi erästä erityistä vektorijoukon E_v linaarisesti riippumattomien osajoukkojen perhettä.

2.2 Matroidin kannat

Lineaarialgebrassa vektoriavaruuden kanta on joukko lineaarisesti riippumattomia vektoreita, jotka virittävät koko vektoriavaruuden, eli muut vektorit voidaan esittää kantavektoreiden lineaarikombinaatioina.

Joukon $X \in \mathcal{I}$ sanotaan olevan *maksimaalinen riippumaton osajoukko*, jos mikä tahansa sen laajennus olisi riippuva, eli $(X \cup \{e\}) \notin \mathcal{I}$ kaikilla $e \in (E \setminus X)$. Vektoriavaruuden kannat ovat sen maksimaalisia lineaarisesti riippumattomia osajoukkoja. Tämä ajatus voidaan yleistää ja sanoa *kannoiksi (basis)* $\mathcal{B}$ kaikkia perusjoukon E maksimaalisia riippumattomia osajoukkoja, jolloin matroidi voidaan määritellä myös parin $(E, \mathcal{B})$ avulla

Määritelmä 2 (Kannat)**.** Olkoon E äärellinen joukko ja $\mathcal{B}$ sen maksimaalisten riippumattomien osajoukkojen perhe. Pari $(E, \mathcal{B})$ on äärellinen matroidi M ja $\mathcal{B}$ sen kannat, jos

(B1) $\mathcal{B} \neq \varnothing$,

(B2) kaikille $B_1, B_2 \in \mathcal{B}$ ja $x \in (B_1 \setminus B_2)$ on olemassa sellainen $y \in (B_2 \setminus B_1)$, jolla $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Esimerkki 2. Tiedetään, että vektoriavaruuden kannan kaardinaliteetti on sama kuin vektoriavaruuden dimensio. Kuvan 1 tapauksessa $\dim \mathbb{R}^3 = 3$, joten vektorijoukon E_v virittämän avaruuden kannassa on siis kolme vektoria. Vektorijoukon E_v kannat ovat kaikki perheen $\mathcal{I}_v$ joukot, joissa on kolme alkiota, eli $\mathcal{B}(E_v) = \{X \in$

$\mathcal{I}_v : |X| = 3\}$. Näiden kantojen virittämällä vektoriavaruudella on toki äärettömästi muita kantoja, mutta ne eivät sisälly joukkoon E_v.

Esimerkiksi $|\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}| = 3$, joten ensimmäinen aksiooma toteutuu.

Olkoot $B_1 = \{\mathbf{a}, \mathbf{b}, \mathbf{d}\}$ ja $B_2 = \{\mathbf{b}, \mathbf{c}, \mathbf{e}\}$. Nyt $B_1 \setminus B_2 = \{\mathbf{a}, \mathbf{d}\}$ ja $B_2 \setminus B_1 = \{\mathbf{c}, \mathbf{e}\}$. Valitaan esimerkiksi $y = \mathbf{c}$, jolloin

$$\begin{aligned} &\text{i)} \quad (B_1 \setminus \{\mathbf{a}\}) \cup \{\mathbf{c}\} = \{\mathbf{b}, \mathbf{c}, \mathbf{d}\} \in \mathcal{B}(E_v), \text{ ja} \\ &\text{ii)} \quad (B_1 \setminus \{\mathbf{d}\}) \cup \{\mathbf{c}\} = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\} \in \mathcal{B}(E_v). \end{aligned}$$

Sama voidaan osoittaa kaikille kannoille, jolloin $\mathcal{B}(E_v)$ toteuttaa myös aksiooman (B2) eli $M(E, \mathcal{B}(E_v))$ on matroidi määritelmän 2 mielessä.

Lineaarialgebrasta tiedetään vektoriavaruuden kannassa olevan aina avaruuden dimension verran vektoreita. Osoittautuu, että matroideilla pätee sama, eli matroidin kaikilla kannoilla on sama kardinaliteetti. Tämän toteamista varten todistetaan ensin seuraava lause [4].

Lause 1 (Täydennyslause)**.** *Oletetaan, että $X, Y \in \mathcal{I}$ ovat riippumattomia matroidissa M ja $|X| < |Y|$. Tällöin on olemassa sellainen osajoukko $Z \subseteq Y \setminus X$, että $|X \cup Z| = |Y|$ ja $X \cup Z \in \mathcal{I}$.*

Todistus. Olkoon Z_0 sellainen joukko, että yli kaikkien osajoukkojen $Z \subseteq Y \setminus X$, joilla $X \cup Z \in \mathcal{I}$, kardinaliteetti $|X \cup Z_0|$ on suurin.

Tehdään vastaoletus, että $|X \cup Z_0| < |Y|$. Tällöin on olemassa osajoukko $Y_0 \subseteq Y$, jonka kardinalitetti $|Y_0| = |X \cup Z_0| + 1$. Koska $Y_0 \in \mathcal{I}$ (I2), niin aksioomasta (I3) seuraa, että on olemassa sellainen $y \in Y_0 \setminus (X \cup Z_0)$, jolla $(X \cup Z_0) \cup \{y\} = X \cup (Z_0 \cup \{y\}) \in \mathcal{I}$ on riippumaton, mikä on ristiriidassa joukon Z_0 valinnan kanssa, sillä koska $y \notin X$ ja $y \notin Z_0$, niin $|X \cup (Z_0 \cup \{y\})| > |X \cup Z_0|$. □

Seuraus 1. *Kaikilla matroidin kannoilla $B_1, B_2 \in \mathcal{B}$ on sama kardinaliteetti $|B_1| = |B_2|$, kun*

i) $\mathcal{B}$ toteuttavat määritelmän 2 aksioomat, tai

ii) $\mathcal{B}$ ovat määritelmän 1 mukaisen matroidin maksimaaliset riippumattomat joukot.

Todistus. Tehdään vastaoletus, että joillakin $B_1, B_2 \in \mathcal{B}$ on erisuuret kardinaliteetit $|B_1| < |B_2|$.

i) Kun suoritetaan aksiooman (B2) alkion vaihto $|B_1 \setminus B_2|$ kertaa eli jokainen joukkolle B_1 uniikki alkio on vaihdettu joukon B_2 alkioon, saadaan aikaan joukko $B' \in \mathcal{B}$, joka on joukon B_2 osajoukko, sillä $B' \setminus B_2 = \varnothing$. Tämän uuden joukon kardinaliteetti $|B'| = |B_1| < |B_2|$, eli on olemassa sellainen joukko $C = B_2 \setminus B'$, jolla $B' \cup C = B_2 \in \mathcal{B}$, mikä on ristiriidassa joukon B' maksimaalisuuden kanssa.

ii) Täydennyslauseen mukaan on olemassa sellainen $Z \subseteq B_2 \setminus B_1$, että $B_1 \cup Z \in \mathcal{I}$, mikä on ristiriidassa kannan määritelmän kanssa, että B_1 on maksimaalinen perheessä $\mathcal{I}$. □

Nyt voidaan osoittaa, että matroidi $M(E, \mathcal{I})$ toteuttaa matroidin määritelmän myös kantojen avulla.

Lause 2. *Olkoot E äärellinen joukko ja $\mathcal{I}$ sen riippumattomat joukot. Matroidin $M(E, \mathcal{I})$ maksimaalisten riippumattomien joukkojen perhe $\mathcal{B}(M)$ toteuttaa määritelmän 2 aksioomat.*

Todistus. Koska tyhjä joukko kuuluu riippumattomien joukkojen perheeseen, niin matroidin maksimaalisten riippumattomien joukkojen eli kantojen perhe $\mathcal{B}(M)$ ei ole tyhjä joukko. Sillä vaikka riippumattomat joukot olisivat pienin mahdollinen perhe $\mathcal{I} = \{\varnothing\}$, niin tyhjä joukko itsensä maksimaalisena osajoukkona olisi matroidin kanta ja $\mathcal{B}(M) = \{\varnothing\} \neq \varnothing$ (B1).

Olkoot $B_1, B_2 \in \mathcal{B}(M)$ matroidin kantoja. Seurauksen 1 nojalla $|B_1 \setminus \{x\}| = |B_1| - 1 < |B_2|$, kun $x \in B_1$. Jos käytetään täydennyslausetta riippumattomiin joukkoihin $B_1 \setminus \{x\}$ ja B_2, täytyy olla olemassa sellainen alkio $y \in B_2$, jolla $|(B_1 \setminus \{x\}) \cup \{y\}| = |B_2|$. Silloin $y \notin B_1$, eli $y \in B_2 \setminus B_1$, ja $\mathcal{B}(M)$ toteuttaa aksiooman (B2). □

Vastaavasti, kun tarkastellaan matroidia $M(E, \mathcal{B})$, voidaan todeta sen täyttävän matroidin määritelmän riippumattomien joukkojen avulla.

Lause 3. *Olkoot E äärellinen joukko ja $\mathcal{B}$ sen kannat. Kantojen osajoukkojen perhe toteuttaa määritelmän 1 aksioomat.*

Todistus. Olkoon $\mathcal{B}$ joukon E epätyhjä osajoukkojen perhe, joka toteuttaa määritelmän 2 aksioomat. Nyt voidaan määritellä perhe $\mathcal{I}_{\mathcal{B}}$ sisältämään kaikki joukon E osajoukot, jotka sisältyvät johonkin perheen $\mathcal{B}$ joukkoon, eli $\mathcal{I}_{\mathcal{B}} = \{X \subseteq E : X \subseteq B, \text{ jollakin } B \in \mathcal{B}\}$. Perhe $\mathcal{I}_{\mathcal{B}}$ on siis epätyhjä ja sisältää joukkojensa kaikki osajoukot, joten se toteuttaa aksioomat (I1) ja (I2).

Oletetaan sitten, että X ja Y ovat sellaiset perheen $\mathcal{I}_{\mathcal{B}}$ eri joukot, jotka ovat kantojen $B_1, B_2 \in \mathcal{B}$ osajoukot $X \subseteq B_1, Y \subseteq B_2$, ja joille pätee $|X| = |Y| + 1$. Olkoot joukot määritelty

$$\begin{aligned} X &= \{x_1, \ldots, x_p\} \\ B_1 &= \{x_1, \ldots, x_p, b_1, \ldots, b_q\} \\ Y &= \{y_1, \ldots, y_{p-1}\} \\ B_2 &= \{y_1, \ldots, y_{p-1}, c_1, \ldots, c_{q+1}\}. \end{aligned}$$

Aksiooman (B2) mukaan on olemassa sellainen alkio $z \in B_1$, jolla $(B_2 \setminus \{c_{q+1}\}) \cup \{z\} \in \mathcal{B}$. Nyt siis $(Y \cup \{z\}) \subseteq (B_2 \setminus \{c_{q+1}\}) \cup \{z\}$. Jos $z \in X$, niin $Y \cup \{z\} \in \mathcal{I}_{\mathcal{B}}$ ja $\mathcal{I}_{\mathcal{B}}$ toteuttaa aksiooman (I3).

Jos taas $z \notin X$, niin poistetaan kannasta $(B_2 \setminus \{c_{q+1}\}) \cup \{z\}$ vielä alkio c_q, jolloin löytyy jälleen sellainen alkio $z' \in B_1$, jolla pätee $((B_2 \setminus \{c_{q+1}\} \cup \{z\}) \setminus \{c_q\}) \cup \{z'\} \in \mathcal{B}$. Koska $|\{b_1, \ldots, b_q\}| < |\{c_1, \ldots, c_{q+1}\}|$, niin viimeistään, kun edellistä operaatiota on toteutettu q kertaa, jolloin $B_2' = \{y_1, \ldots, y_{p-1}, c_1, b_1, \ldots, b_q\}$, korvataan c_1 joukon X alkiolla. Tällöin siis $(B_2' \setminus \{c_1\}) \cup \{x_i\} = \{y_1, \ldots, y_{p-1}, x_i, b_1, \ldots, b_q\}$, josta nähdään, että $Y \cup \{x_i\} \subseteq (B_2' \setminus \{c_1\} \cup \{x_i\})$ eli $Y \cup \{x_i\} \in \mathcal{I}_{\mathcal{B}}$. Tällöin siis perhe $\mathcal{I}_{\mathcal{B}}$ toteuttaa aksiooman (I3) ja on matroidin $M(E, \mathcal{I}_{\mathcal{B}})$ riippumattomat joukot. □

Nähtiin siis että määritelmät 1 ja 2 ovat ekvivalentit, eli yhdellä tavalla määritelty matroidi on matroidi myös toisen määritelmän mukaan. Nämä ovat vieläpä sama matroidi, kun matroidin $M(E, \mathcal{I})$ kannat $\mathcal{B}(E, \mathcal{I})$ määritellään kuten edellä esimerkeissä perheen $\mathcal{I}$ maksimaalisina joukkoina, ja matroidin $M(E, \mathcal{B})$ riippumattomat joukot $\mathcal{I}(E, \mathcal{B})$ määritellään kantojen $\mathcal{B}$ kaikkien osajoukkojen perheenä. Tällöin siis määritelman 1 mukaisen matroidin $M(E, \mathcal{I}(E, \mathcal{B}))$ kannat ovat $\mathcal{B}(E, \mathcal{I}(E, \mathcal{B})) = \mathcal{B}$, ja ne toteuttavat aksioomat (B1) ja (B2). Vastaavasti määritelmän 2 mukaisen matroidin $M(E, \mathcal{B}(E, \mathcal{I}))$ aksioomat (I1)–(I3) toteuttavat riippumattomat joukot ovat $\mathcal{I}(E, \mathcal{B}(E, \mathcal{I})) = \mathcal{I}$. Saadaan siis

$$M(E, \mathcal{I}) = M(E, \mathcal{B}(E, \mathcal{I})) = M(E, \mathcal{B}(E, \mathcal{I}(E, \mathcal{B}))) = M(E, \mathcal{B}).$$

Tässä ensimmäinen yhtäsuuruus seuraa määritelmien ekvivalenttisuudesta ja siitä, että $\mathcal{B}(E, \mathcal{I})$ ovat matroidin $(E, \mathcal{I})$ kannat. Toinen yhtäsuuruus seuraa edellä esitetystä riippumattomien joukkojen määrittelemisestä kantojen avulla, ja samoin kolmas kantojen määrittelemisestä riippumattomien joukkojen avulla. [3]

2.3 Matroidin astefunktio

Matriisin aste määritellään lineaarialgebrassa matriisin pysty- tai vaakariviavaruuksien ulottuvuutena $r(A) = \dim P(A) = \dim V(A)$. Kuvan 1 vektoreista voidaan muodostaa matriisi esimerkiksi sijoittamalla ne matriisin pystyriveiksi

$$A_v = \begin{array}{c} \begin{matrix} \mathbf{a} & \mathbf{b} & \mathbf{c} & \mathbf{d} & \mathbf{e} & \mathbf{f} \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix} \end{array}.$$

Vektoreista todettiin jo aikaisemmin löytyvän avaruuden $\mathbb{R}^3$ kantoja, jolloin matriisin pystyriviavaruuden dimensiosta saadaan matriisin aste $\mathrm{r}(A_v) = \dim P(A_v) = 3$. Matriisin aste on siis sen pysty- tai vaakariviavaruuden maksimaalisten lineaarisesti riippumattomien osajoukkojen kaardinaliteetti. Samoin kuin aikaisemmin, tämä ajatus voidaan yleistää matriisin riveistä mille tahansa joukolle jonkin matroidirakanteen suhteen, määrittelemällä funktio

$$r: \ 2^E \to \mathbb{N}, \quad r(A) = \max(|X|: \ X \subseteq A, X \in \mathcal{I}), \text{ kaikilla } (A \subseteq E), \tag{1}$$

joka antaa joukon E osajoukon A asteen sen maksimaalisten riippumattomien joukkojen kardinaliteettina. Näin saadaan matroidille seuraava määritelmä.

Määritelmä 3 (Matroidin aste)**.** Olkoot E äärellinen joukko ja funktio r: $2^E \to \mathbb{N}$. Pari (E, r) on äärellinen matroidi M ja r on sen *astefunktio (rank-function)*, jos kaikille osajoukoille $X \subseteq E$ ja alkioille $y, z \in E$ pätee

(R1) $r(\varnothing) = 0$

(R2) $r(X) \leqslant r(X \cup \{y\}) \leqslant r(X) + 1$

(R3) jos $r(X \cup \{y\}) = r(X \cup \{z\}) = r(X)$, niin $r(X \cup \{y\} \cup \{z\}) = r(X)$.

Matroidin M aste on $r(E)$.

Esimerkki 3. Tarkastellaan taas kuvan 1 vektorijoukkoa E_v, kun aste r on vektorijoukon maksimaalisten lineaarisesti riippumattomien osajoukkojen kardinaliteettina kuten edellä. Nähdään, että (R1) pätee, sillä tyhjä joukko on itsensä ainoa osajoukko, ja sen kardinaliteetti on 0.

Olkoon Y osajoukon $X \subseteq E_v$ maksimaalinen lineaarisesti riippumaton osajoukko, jolloin $r(X) = |Y|$. Mikäli vektori $\mathbf{y}$ on lineaarisesti riippumaton joukossa Y (ja siis myös joukossa X), niin $r(X \cup \{\mathbf{y}\}) = |Y \cup \{\mathbf{y}\}| = |Y| + 1$, jos taas $\mathbf{y}$ on lineaarisesti riippuva joukossa Y, niin sen lisääminen joukkoon X ei muuta maksimaalisen riippumattoman osajoukon kokoa, ja $r(X \cup \{\mathbf{y}\}) = |Y| = r(X)$. Siis alkion lisääminen osajoukkoon kasvattaa sen astetta korkeintaan yhdellä, ja aste-funktio toteuttaa myös aksiooman (R2).

Jos vektorit $\mathbf{y}$ ja $\mathbf{z}$ ovat lineaarisesti riippuvia joukossa X, niin $\mathbf{z}$ on lineaariseti riippuva myös joukossa $X \cup \{\mathbf{y}\}$. Vektorijoukon aste toteuttaa siis aksiooman (R3) ja (E_v, r) on matroidi määritelmän 3 mielessä.

Lause 4. *Olkoot E äärellinen joukko ja $\mathcal{I}$ sen riippumattomat joukot. Matroidi $M(E, \mathcal{I})$ toteuttaa määritelmän 3 aksioomat, kun r on funktio* (1).

Todistus. Esimerkin perustelu ensimmäiselle aksioomalle pätee minkä tahansa perusjoukon yhteydessä, sillä tyhjä joukko on itsensä ainoa osajoukko riippumatta kontekstista. Samoin toisen aksiooman kohdalla voidaan perustelut laajentaa vektoreilta yleiselle joukolle ja sen riippumattomille osajoukoille, kun matroidin astefunktio on juuri funktio (1).

Kolmannen aksiooman kohdalla voidaan toisaalta tarkastella vastaoletusta, että joukon $A = X \cup \{y\} \cup \{z\} \subseteq E$ aste $r(A) > r(X)$ ja Y on joukon X maksimaalinen riippumaton osajoukko eli $r(X) = |Y|$. Täydennyslauseen mukaan Y voidaan täydentää joukon A maksimaaliseksi riippumattomaksi osajoukoksi $Y \cup Z$ jollakin joukolla $Z \subseteq A$, jolloin $r(A) = |Y \cup Z|$. Jotta $r(A) > r(X)$, niin täytyy vähintään toisen alkioista y, z kuulua joukkoon Z. Oletetaan, että $z \in Z$, jolloin $Y \cup \{z\}$ on riippumaton joukossa A, ja $r(X \cup \{z\}) = |Y \cup \{z\}| = |Y| + 1 > r(X)$, mikä on ristiriidassa aksiooman (R3) oletuksen $r(X \cup \{z\}) = r(X)$ kanssa. $\square$

Riippumattomien joukkojen avulla määritellyn matroidin astefunktio toteuttaa siis aksioomat (R1)–(R3), eli matroidi $(E, \mathcal{I})$ on myös matroidi määritelmän 3 mukaan. Vastaavasti voidaan osoittaa määritelmien ekvivalenttius myös toiseen suuntaan.

Lause 5. *Olkoot E äärellinen joukko ja $\mathcal{I}$ sen riippumattomat joukot. Määritelmän 3 aksioomat toteuttava funktio r on matroidin $M(E, \mathcal{I})$ astefunktio.*

Todistus. Olkoon $\mathcal{I}_r$ joukon E niiden osajoukkojen, joiden aste on yhtä suuri kuin kardinalitetti, perhe $\mathcal{I}_r = \{X \subseteq E : r(X) = |X|\}$. Aksioomasta (R1) saadaan, että $\varnothing \in \mathcal{I}_r$ (I1). Olkoon A perheen $\mathcal{I}_r$ joukko, eli $r(A) = |A|$, ja B sen osajoukko. Tehdään aksioomalle (I2) vastaoletus, että $B \notin \mathcal{I}_r$ eli sen aste $r(B) < |B|$. Nyt saadaan aksioomasta (R2), että $r(B \cup \{a_i\}) \leqslant r(B) + 1 < |B| + 1$, kun $A \setminus B = \{a_1, a_2, \dots, a_n\}$. Toistamalla tätä n kertaa, saadaan ristiriita

$$r(A) = r(B \cup \{a_1\} \cup \{a_2\} \cup \cdots \cup \{a_n\}) < |B| + n = |A|.$$

Oletetaan, että joukot X, Y kuuluvat perheeseen $\mathcal{I}_r$, ja

$$X = \{x_1, x_2, \dots, x_p, z_{p+1}, \dots, z_q, z_{q+1}\}$$
$$Y = \{x_1, x_2, \dots, x_p, y_{p+1}, \dots, y_q\},$$

missä $z_i \notin Y$ millään indeksillä i. Oletetaan sitten, että $Y \cup \{z_i\} \notin \mathcal{I}_r$ millään joukon X alkiolla z_i, jolloin $r(Y \cup \{z_i\}) = r(Y) = |Y|$. Aksiooman (R3) mukaan siis myös $r(Y \cup \{z_i\} \cup \{z_j\}) = r(Y) = |Y|$, ja toistamalla tämä kaikilla alkioilla z_i saadaan aikaan joukko $Y \cup \{z_{p+1}\} \cup \cdots \cup \{z_{q+1}\} = Y \cup (X \setminus Y) = X \cup (Y \setminus X)$, jonka asteelle pätee aksiooman (R2) mukaan

$$r(X) \leqslant r(X \cup (Y \setminus X)) = |Y| < |X|,$$

mikä on ristiriidassa sen kanssa, että $X \in \mathcal{I}_r$ eli $r(X) = |X|$. Joten täytyy olla jokin alkio z_i, jolla $Y \cup \{z_i\} \in \mathcal{I}_r$, ja perhe $\mathcal{I}_r$ toteuttaa myös aksiooman (I3). □

Näin siis määritelmät 1 ja 3 ovat ekvivalentit, kuin myös välillisesti määritelmä 2, ja määrittävät siten saman matroidin.

Whitney määritteli matroidin esitelleessä artikkelissaan [5] matroidin juuri näin astefunktion avulla, vaikka osoitti myös määrittelyt riippumattomien joukkojen, kantojen ja piirien avulla ekvivalenteiksi. Matroidi voidaan määritellä astefunktion avulla myös toisin, kuten von Randow kirjassaan [2] aivan ensimmäiseksi.

Määritelmä 4 (Matroidin aste 2)**.** Olkoot E äärellinen joukko ja funktio $r \colon 2^E \to \mathbb{N}$. Pari (E, r) on äärellinen matroidi ja r on sen astefunktio, jos kaikille osajoukoille $X, Y \subseteq E$ pätee

(R1') $r(X) \leqslant |X|$
(R2') jos $Y \subseteq X$, niin $r(Y) \leqslant r(X)$
(R3') $r(X \cup Y) + r(X \cap Y) \leqslant r(X) + r(Y)$.

Kolmannen aksiooman mukaan matroidin astefunktio on *submodulaarinen (submodular).* Tällä tarkotetaan joukoille määriteltyä funktiota, jossa funktion arvon kasvu on korkeintaan yhtä suuri, kun funktion argumenttina olevaan joukkoon lisätään jokin alkio, kuin jos sama alkio lisätään argumentin osajoukkoon. Eli jos $A \subseteq B$ niin $f(B \cup \{e\}) - f(B) \leqslant f(A \cup \{e\}) - f(A)$. Funktio siis toteuttaa taloustieteestä tuttua vähenevän tuoton lakia (diminishing returns).

Lause 6. *Olkoot E äärellinen joukko ja $\mathcal{I}$ sen riippumattomat joukot. Funktio* (1) *toteuttaa määritelmän 4 aksioomat ja määritelmän 4 aksioomat toteuttava funktio r toteuttaa määritelmän 3 aksioomat.*

Todistus. Joukon maksimaalinen riippumaton osajoukko on aina korkeintaan joukko itse, jolloin näiden kardinaliteetit toteuttavat aksiooman (R1'), kun r on funktio (1). Myös aksiooma (R2') toteutuu, sillä osajoukossa Y ei ole joukkoon X kuulumattomia alkioita, joten sen maksimaalinen riippumaton osajoukko ei voi olla joukon X vastaavaa suurempi. Aksiooman (R3') osoittamista varten olkoon A leikkauksen $X \cap Y$ riippumaton osajoukko, jonka kardinaliteetti $|A| = r(X \cap Y)$. Leikkaus on unionin osajoukko, joten unionilla on olemassa riippumaton osajoukko $B \subseteq X \cup Y$, jolla täydennyslauseen nojalla on osajoukko $A \subseteq B$, ja $|B| = r(X \cup Y)$. Olkoot joukot C, D sellaiset keskenään ja joukon A kanssa pareittain erilliset joukot, että $B = A \cup C \cup D$, kun $C \subseteq X \setminus Y$ ja $D \subseteq Y \setminus X$. Nyt riippumattoman joukon B osajoukkoina $A \cup C$ on riippumaton joukon X osajoukko, ja $A \cup D$ on riippumaton joukon Y osajoukko. Siten toisesta aksioomasta ja joukkojen erillisyydestä seuraa, että

$$\begin{aligned} r(X) + r(Y) &\geqslant r(A \cup C) + r(A \cup D) = |A \cup C| + |A \cup D| \\ &= |A| + |C| + |A| + |D| = (|A| + |C| + |D|) + |A| \\ &= |B| + |A| = r(X \cup Y) + r(X \cap Y), \end{aligned}$$

mikä on aksiooma (R3').

Vastaavasti, jos funktio r totetuttaa määritelmän 4 aksioomat, voidaan osoittaa, että se toteuttaa myös aksioomat (R1)–(R3). Tyhjän joukon kardinaliteetti on 0, joten (R1) seuraa ensimmäisestä aksioomasta. Koska $X \subseteq (X \cup \{y\})$, niin aksiooman (R2) ensimmäinen relaatio seuraa aksioomasta (R2'). Toinen relaatio taas saadaan aksioomasta (R1') sillä $r(X \cup \{y\}) \leqslant |X \cup \{y\}| \leqslant |X| + 1$.

Olkoot $y, z \in E$ perusjoukon alkioita, jolloin $(X \cup \{y\}) \cap (X \cup \{z\}) = X$. Nyt, jos $r(X \cup \{y\}) = r(X \cup \{z\}) = r(X)$, niin kolmannen aksiooman nojalla

$$\begin{aligned} &r([X \cup \{y\}] \cup [X \cup \{z\}]) + r([X \cup \{y\})] \cap [X \cup \{z\}]) \\ &\quad = r(X \cup \{y\} \cup \{z\}) + r(X) \leqslant (X \cup \{y\}) + (X \cup \{z\}) = r(X) + r(X), \end{aligned}$$

mistä saadaan, että

$$r(X \cup \{y\} \cup \{z\}) + r(X) \leqslant 2\, r(X), \text{ eli}$$

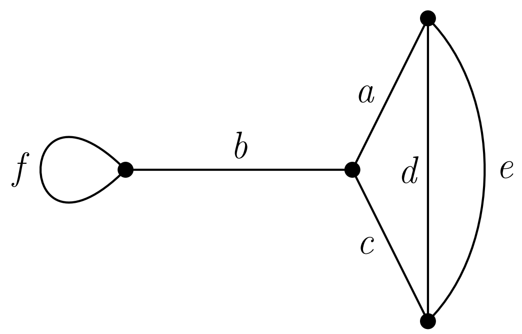
$$r(X \cup \{y\} \cup \{z\}) \leqslant r(X).$$

Koska alkioiden lisääminen joukkoon ei voi pienentää joukon astetta, seuraa tästä aksiooma (R3), eli $r(X \cup \{y\} \cup \{z\}) = r(X)$. $\square$

Nähtiin siis, että molemmat määritelmät matroidille astefuntion avulla määrittävät saman funktion (1).

2.4 Matroidin piirit

Tähän mennessä matroidien tarkastelun lähtökohtana on ollut lineaarialgebra ja vektoriavaruus. Tutkitaan seuraavaksi, kuinka matroidit voidaan määritellä, kun lähtökohtana on niiden sijaan graafiteoria. Esimerkiksi William Thomas Tutte, joka kehitti matroidien teoriaa Whitneyn jälkeen, oli taustaltaan graafiteorian tutkija. Hän käyttikin matroidien määrittelyn lähtökohtana graafiteoriasta juontuvia ominaisuuksia [5].



Kuva 2: Kuusi viivaa sisältävä graafi.

Tarkastellaan kuvan 2 graafia (graph), jossa on neljä pistettä (vertex) ja kuusi viivaa (edge). Graafi on rakennettu ja nimetty niin, että sen virittävät puut (spanning trees)

$$\mathcal{T}_G = \{\{a, b, c\}, \{a, b, d, \}, \{a, b, e\}, \{b, c, d\}, \{b, c, e\}\},$$

eli ne piirittömät aligraafit, jotka sisältävät kaikki graafin pisteet, ovat samoin nimetyt kuin vektorijoukon E_v kannat. Voidaan siis olettaa, että nämä graafi ja vektorijoukko voisivat olla pohjana samalle matroidille. Toinen graafin mielenkiintoinen viivajoukkojen perhe on sen piirit (circuits), joita ovat suljetun polun muodostavat graafin viivajoukot. Tämän graafin piirit ovat

$$\mathcal{C}_G = \{\{a, c, d\}, \{a, c, e\}, \{d, e\}, \{f\}\}.$$

Samoin kuin kannat, myös piirit ovat perusjoukolle sikäli kuvaavia, että matroidi voidaan määritellä myös niiden avulla.

Määritelmä 5 (Matroidin piirit)**.** Olkoot E äärellinen joukko ja $\mathcal{C}$ sen osajoukkojen perhe. Pari $(E, \mathcal{C})$ on äärellinen matroidi ja $\mathcal{C}$ sen *piirit (circuits)* eli minimaaliset riippuvat osajoukot, jos seuraavat aksioomat pätevät

(C1) jos $X \in \mathcal{C}$, niin sen aidoille osajoukoille $Y \subset X$ pätee $Y \notin \mathcal{C}$,

(C2) jos $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$ ja $z \in C_1 \cap C_2$, niin on olemassa sellainen $C_3 \in \mathcal{C}$, että $C_3 \subseteq (C_1 \cup C_2) \setminus \{z\}$.

Lause 7. *Olkoon $M(E, \mathcal{I})$ määritelmän 1 mukainen matroidi. Matroidin minimaaliset riippuvat osajoukot toteuttavat määritelmän 5 aksioomat ja ovat siis matroidin piirit.*

Todistus. Riippuva osajoukko on minimaalinen, jos minkä tahansa alkion poistaminen tekee siitä riippumattoman. Näin ollen mikään tällaisen joukon aito osajoukko ei ole riippuva eikä siis voi olla piiri (C1). Jos oletetaan toista aksioomaa varten, että C_1 ja C_2 ovat piirejä, mutta esitettyä piiriä C_3 ei ole olemassa, niin joukko $(C_1 \cup C_2) \setminus \{z\}$ on siinä tapauksessa riippumaton, sillä sen kaikki osajoukot ovat riippumattomia. Näin ollen $r((C_1 \cup C_2) \setminus \{z\}) = |(C_1 \cup C_2) \setminus \{z\}| = |C_1 \cup C_2| - 1$. Toisaalta kussakin piirissä on vain yksi alkio enemmän kuin sen suurimmassa riippumattomassa osajoukossa, jolloin $r(C_i) = |C_i| - 1$. Nyt saadaan astefunktion submodulaarisuudesta ja unionin kardinaliteetin kaavasta piirien unionin ja leikkauksen asteiden summalle yläraja

$$\begin{aligned} r(C_1 \cup C_2) + r(C_1 \cap C_2) &\leqslant r(C_1) + r(C_2) \\ &= |C_1| - 1 + |C_2| - 1 = |C_1| + |C_2| - 2 \\ &= |C_1 \cup C_2| + |C_1 \cap C_2| - 2. \end{aligned}$$

Toisaalta aksiooman (R2) mukaan $r(C_1 \cup C_2) \geqslant r((C_1 \cup C_2) \setminus \{z\}) = |C_1 \cup C_2| - 1$, ja $r(C_1 \cap C_2) = |C_1 \cap C_2|$, sillä piirien leikkaus on osajoukkona riippumaton. Näin saadaan unionin ja leikkauksen summalle alaraja

$$r(C_1 \cup C_2) + r(C_1 \cap C_2) \geqslant |C_1 \cup C_2| + |C_1 \cap C_2| - 1,$$

joka on ylärajaa suurempi, mikä on ristiriita. Näin ollen joukon $(C_1 \cup C_2) \setminus \{z\}$ on oltava riippuva ja sisällettävä vähintään yksi piiri. □

Todistetaan jatkoa varten aksioomaa (C2) muistuttava vahvempi tulos.

Lause 8. *Jos matroidin piirit $C_1 \neq C_2$ ja alkio $x \in C_1 \cap C_2$, niin jokaiselle alkiolle $y \in C_1 \setminus C_2$ on olemassa sellainen piiri C, että*

$$y \in C \subseteq (C_1 \cup C_2) \setminus \{x\}.$$

Todistus. Tehdään vastaoletus, että on olemassa sellaiset piirit C_1, C_2 ja alkiot x, y, että y ei kuulu mihinkään joukon $(C_1 \cup C_2) \setminus \{x\}$ sisältämään piiriin. Oletetaan lisäksi, että sellaisilla piireillä, joilla lause ei näin päde, kardinaliteetti $|C_1 \cup C_2|$ on pienin mahdollinen. Aksiooman (C2) mukaan on olemassa joukkoon $(C_1 \cup C_2) \setminus \{x\}$ sisältyvä piiri C_3, mutta vastaoletuksen mukaan $y \notin C_3$. Koska $y \notin C_2 \cup C_3$, niin $C_2 \cup C_3$ on unionin $C_1 \cup C_2$ aito osajoukko. Ja koska unioni $C_1 \cup C_2$ oli valittu pienimmäksi mahdolliseksi, jolle lause ei päde, sen täytyy päteä piireillä C_2 ja C_3.

Piirissä C_3 täytyy olla erotuksen $C_2 \setminus C_1$ alkioita, sillä aksiooman (C1) mukaan C_3 ei voi olla piirin C_1 osajoukko, eli $C_3 \cap (C_2 \setminus C_1) \neq \varnothing$. Olkoon z nyt tämän leikkauksen alkio $z \in C_3 \cap (C_2 \setminus C_1)$, jolloin $z \in C_2 \cap C_3$. Myös piirin C_3 valinnan mukaan $x \notin C_3$, joten $x \in C_2 \setminus C_3$. Lauseen mukaan on siis olemassa piiri C_4, jolla

$$x \in C_4 \subseteq (C_2 \cup C_3) \setminus \{z\}.$$

Nyt $x \in C_1 \cap C_4$ ja $y \in C_1 \setminus C_4$, sillä $y \notin C_4 \subseteq C_2 \cup C_3$. Jälleen $C_1 \cup C_4$ on unionin $C_1 \cup C_2$ aito osajoukko, sillä $z \notin C_1 \cup C_4$. Näin ollen lause pätee piireille C_1 ja C_4, jolloin on olemassa piiri C_5, jolla

$$y \in C_5 \subseteq (C_1 \cup C_4) \setminus \{x\} \subseteq (C_1 \cup C_2) \setminus \{x\}.$$

Tämä on ristiriita vastaoletuksen kanssa, ettei ole olemassa piiriä $C = C_5$, johon y kuuluisi. □

Määritellään funktio

$$\rho : S \subseteq E \to \mathbb{N}, \quad \rho(x_1, \ldots, x_n) = \sum_{i=1}^{n} \phi_i, \tag{2}$$

missä $(x_1, \ldots, x_n)$ on joukon S alkioiden järjestetty joukko, ja $\phi_i = 0$, jos $(x_1, \ldots, x_i)$ sisältää sellaisen piirin $C \in \mathcal{C}$, joka sisältää alkion x_i, ja muulloin $\phi_i = 1$. Osoitetaan välituloksena, että funktion arvo ei ole riippuvainen joukon järjestyksestä.

Lemma 1. $\rho(x_1, \ldots, x_{n-2}, x_{n-1}, x_n) = \rho(x_1, \ldots, x_{n-2}, x_n, x_{n-1})$.

Todistus. Olkoon X järjestetty joukko $(x_1, \ldots, x_{n-2})$ ja merkitään funktion arvoja

$$\begin{aligned} &\rho(X) = r, \qquad \rho(X, x_{n-1}) = r_1, \qquad \rho(X, x_n) = r_2 \\ &\rho(X, x_{n-1}, x_n) = r_{12}, \qquad \rho(X, x_n, x_{n-1}) = r_{21}. \end{aligned}$$

Täytyy tarkastella neljää tapausta:

i) Oletetaan, että mikään piiri joukossa $X \cup \{x_{n-1}\}$ ei sisällä alkiota x_{n-1} eikä joukossa $X \cup \{x_n\}$ alkiota x_n. Tällöin termin ϕ_i mukaan $r_1 = r_2 = r+1$. Jos joukossa $X \cup \{x_{n-1}\} \cup \{x_n\}$ on piiri, joka sisältää alkiot x_{n-1} ja x_n, niin viimeinen termi $\phi_n = 0$ kummallakin järjestyksellä, eli

$$r_{12} = r_1 = r_2 = r_{21},$$

muuten $\phi_n = 1$ ja

$$r_{12} = r_1 + 1 = r_2 + 1 = r_{21}.$$

ii) Oletetaan, että joukossa $X \cup \{x_{n-1}\}$ on piiri C_2, jossa on alkio x_{n-1}, ja joukossa $X \cup \{x_{n-1}\} \cup \{x_n\}$ on piiri C_1, jossa on alkiot x_{n-1} ja x_n. Tällöin lauseen 8 mukaan on olemassa piiri C_3, jolla

$$x_n \in C_3 \subseteq (C_1 \cup C_2) \setminus \{x_{n-1}\} \subseteq X \cup \{x_n\},$$

eli kummassakin järjestyksessä $\phi_i = 0$ kahden viimeisen alkion kohdalla ja

$$r_{12} = r_1 = r = r_2 = r_{21}.$$

iii) Oletetaan, että on olemassa piiri C_2 kuten edellisessä tapauksessa, eli $r_1 = r$, muttei piiriä C_1. Jos on olemassa piiri $C_3 \subseteq X \cup \{x_n\}$, jossa on alkio x_n, niin $r_2 = r$ ja piirien C_2, C_3 avulla myös $\phi_n = 0$ molemmilla järjestyksillä, ja

$$r_{12} = r_1 = r = r_2 = r_{21}.$$

Jos taas ei ole olemassa tällaista piiriä C_3, niin $r_2 = r + 1$ ja $r_{12} = r_1 + 1$, mutta $\phi_n = 0$, kun viimeinen termi on x_{n-1}, eli

$$r_{12} = r_1 + 1 = r + 1 = r_2 = r_{21}.$$

iv) Vastaavasti, jos on olemassa piiri C_3 kuten tapauksessa (iii), mutta ei piiriä C_1 kuten tapauksessa (ii), niin edellisen kohdan päättely pätee edelleen.

Näin saatiin, että kaikissa mahdollisissa tapauksissa $r_{12} = r_{21}$, eli kahden viimeisen alkion järjestyksellä ei ole väliä funktion arvon kannalta. □

Seuraus 2. *Funktion $\rho(S)$ arvo ei riipu joukon S järjestyksestä.*

Todistus. Edellisen lemman mukaan kahden viimeisen alkion paikan vaihtaminen ei vaikuttanut funktion arvoon, ja sama pätee mihin tahansa prefiksiin eli järjestetyn joukon alkupään osajoukkoon. Suffiksien eli järjestetyn joukon lopun osajoukkojen järjestys ei muuttunut, joten sen alkioiden tarkastelu ja funktion arvo pysyivät samana. Tällöin minkä tahansa kahden vierekkäisen alkion paikkaa voidaan vaihtaa funktion arvon muuttumatta, ja edelleen mikä tahansa joukon permutaatio voidaan muodostaa peräkkäisillä kahden vierekkäisen alkion vaihdoilla, joten todistus seuraa lemmasta 1. □

Lause 9. *Määritelmän 5 mukaan määritelty matroidi $M(E, \mathcal{C})$ on matroidi myös määritelmän 3 mukaan.*

Todistus. Olkoot $X \subseteq E$ ja $y, z \in E$. Nyt voidaan todeta, että $\rho(\varnothing) = 0$, sillä funktiossa ei ole ainuttakaan sumattavaa. Toisaalta $\phi_i \in \{0, 1\}$, joten jos joukkoon lisätään yksi alkio, niin $\rho(X) + 1 \geqslant \rho(X, y) \geqslant \rho(X)$. Lisäksi jos oletetaan, että $\rho(X, y) = \rho(X, z) = \rho(X)$, niin tiedetään, että on olemassa sellaiset piirit $C_1, C_2 \in \mathcal{C}$, joilla

$$\begin{aligned} y \in C_1 \subseteq X \cup \{y\} \\ z \in C_2 \subseteq X \cup \{z\}, \end{aligned}$$

jolloin edellisen lemman mukaan riippumatta alkioiden lisäämisjärjestyksestä $\rho(X, y, z) = \rho(X)$. Eli funktio ρ toteuttaa siis matroidin astefunktion aksioomat (R1)–(R3). □

Matroidi $M(E, \mathcal{C})$ on siis matroidi määritelmän 3 ja välillisesti myös kaikkien muiden esitettyjen määritelmien mukaan. Tässä luvussa todistettujen lauseiden mukaan millä tahansa esitetyllä tavalla määritelty matroidi toteuttaa myös minkä tahansa muun matroidin määritelmän ja esitetyt määritelmät ovat siis keskenään ekvivalentit.

2.5 Muita matroidin määritelmiä

Edellä on esitelty matroidille viisi eri määritelmää neljästä eri lähtökohdasta. Esiteltyjen lisäksi matroidit voidaan määritellä esimerkiksi joukkojen sulkeumafunktion (closure), suljettujen joukkojen (flats) tai riippumattomuusfunktion avulla [4]. Matroidin määritelmän valinta kuvastaa käyttäjän taustaa ja sitä, mitkä matroidin ominaisuudet ovat työlle oleellisia.

Lisäksi myös esitettyjen määritelmien aksioomille on eri muotoiluja. Esimerkiksi Oxley määrittelee kantojen perheen epätyhjyyden aksioomassa (B1) [1], mutta Welsh sisällyttää sen perheen $\mathcal{B}$ määritelmään ja esittää vain yhden aksiooman (B2) [4]. Whitneyn ja Randow'n määritelmissä taas kantojen ensimmäinen aksiooma on muodossa

(B1') Jos $X \subset B \in \mathcal{B}$, ja $X \neq B$, niin $X \notin \mathcal{B}$,

eli kantojen aidot osajoukot eivät ole kantoja [5][2], mikä on muotoilultaan vastaava kuin piirien aksiooma (C1).

Randow vaatii piirien erillisessä aksioomassa eksplisiittisesti, ettei tyhjä joukko ole piiri, kun taas Whitneyn toinen piirien aksiooma on tässä tutkielmassa esitetty lause 8.

3 Matroidien ominaisuuksia

3.1 Isomorfiset matroidit

Matroidien sanotaan olevan isomorfisia, jos niiden perusjoukkojen välille voidaan määritellä sellainen bijektio, että joukko on riippumaton matroidissa, jos ja vain jos sen kuva toisessa matroidissa on riippumaton [1]. Esimerkiksi perusjoukolla $E = \{1, 2\}$ voisi olla riippumattomat joukot $\mathcal{I}_1 = \{\varnothing, \{1\}\}$ ja $\mathcal{I}_2 = \{\varnothing, \{2\}\}$. Kun nyt määrittellään bijektio $\alpha : E \to E$

$$\begin{cases} \alpha(\{1\}) & = \{2\} \\ \alpha(\{2\}) & = \{1\} \end{cases}$$

nähdään, että $\alpha(\mathcal{I}_1) = \mathcal{I}_2$, eli matroidit ovat isomorfisia ja merkitään $M(E, \mathcal{I}_1) \cong M(E, \mathcal{I}_2)$.

Isomorfisuus vaatii siis ensinnäkin sen, että matroidien perusjoukot ovat yhtämahtavat eli niiden kardinaliteetit ovat samat. Lisäksi riippumattomien joukkojen täytyy olla rakenteeltaan samat, eli että ne sisältävät yhtä monta joukkoa kutakin kardinaliteettia. Oletetaan esimerkiksi, että kuvaus $\alpha : E_A \to E_B$ on bijektio, eli jokaista alkiota $a \in E_A$ vastaa yksikäsitteinen alkio $\alpha(a) = b \in E_B$ ja kaikilla joukon E_B alkioilla on alkukuva joukossa E_A, siis $|E_A| = |E_B|$. Siten myös kaikille osajoukoille $A \subseteq E_A$ pätee $|A| = |\alpha(A)|$, ja jokaisen riippumattoman joukon kuvajoukko toisessa matroidissa on yhtämahtava sen alkukuvan kanssa.

Matroidin kannan määritelmästä seuraa, että kannan kuva on kanta myös toisessa matroidissa ja myöskin piirien kuvat ovat piirejä. Samoin isomorfisten matroidien asteet ovat samat.

Isomorfisten matroidien perusjoukkojen alkioiden ei toki tarvitse olla samaa lajia (edellä kokonaislukuja). Esimerkiksi myös vektorimatroidi $(\{\mathbf{a}, \mathbf{b}\}, \{\varnothing, \{\mathbf{a}\}\})$ on isomorfinen edellisten matroidien kanssa.

3.2 Lineaariset matroidit

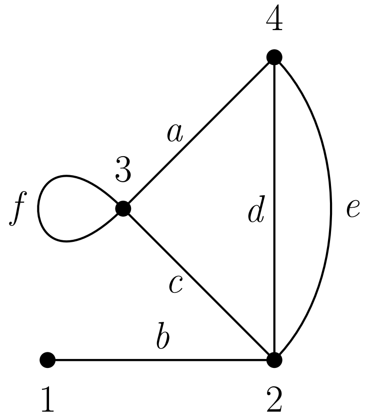
Matroidia, joka saadaan vektorijoukosta tai matriisin A pystyrivivektoreista, kun riippumattomat joukot ovat lineaarisesti riippumattomien vektorien joukot, kutsutaan *vektorimatroidiksi (vector matroid)* ja merkitään $M[A]$. Edelleen matroidia, joka on isomorfinen vektorimatroidin kanssa, kutsutaan *lineaariseksi matroidiksi (linear matroid)*, vaikka sen lähtökohtana ei olisikaan ollut matriisi.

Kun matriisin alkiot kuuluvat kuntaan K, niin lineaarista matroidia sanotaan *K-esittyväksi (representable)* matroidiksi. Esimerkiksi tämän tutkielman esimerkeissä olleet matroidit ovat reaaliesittyviä. Toisaalta voidaan sanoa, että matriisi A esittää matroidin M. [1]

3.3 Graafiset matroidit

Matroidin sanotaan olevan *graafinen (graphic/cycle/polygon matroid)*, jos se on isomorfinen jonkin graafin G viivojen (E) ja piirien ($\mathcal{C}$) avulla muodostetun matroidin kanssa. Tällöin merkitään $M(E, \mathcal{C}) = M(G)$. Vaikka matroidit ovat käteviä joidenkin graafeihin liittyvien aspektien käsittelyssä, on kuitenkin monia graafiteorian ongelmia, joihin matroidit eivät sovellu, sillä esimerkiksi graafin pisteille ei ole vastaavaa käsitettä matroidien teoriassa. [4]

Matroidi ei siis sisällä kaikkea graafin informaatiota. Näin esimerkiksi kaikki *metsät* eli piirittömät graafit, joissa on yhtä monta viivaa, tuottavat isomorfiset matroidit, vaikkeivat itse graafit ole isomorfisia, sillä graafien isomorfisuus määritellään niiden pisteiden bijektion kautta. Samoin kuvan 3 graafissa G_2 on sama määrä viivoja sekä samat piirit kuin kuvan 2 graafissa, jolloin ne tuottavat saman matroidin, vaikka niiden pisteet ovat hyvin erilaiset. Selkein ero on piste 1, joka on loppupiste graafissa G_2, mutta toisessa graafissa ei ole yhtään loppupistettä.



Kuva 3: Graafi, joka tuottaa isomorfisen matroidin kuvan 2 graafin kanssa.

Graafille G_2 voidaan luoda insidenssimatriisi eli matriisi, jossa pystyrivit on nimetty kuten graafin viivat ja vaakarivit kuten graafin pisteet. Jos viiva on silmukka eli sen molemmat päät ovat samassa pisteessä, sen pystyrivin kaikki alkiot ovat nollia. Muuten alkio a_{ij} on 1, jos piste i on viivan j päätepiste, ja 0, jos se ei ole. Graafin G_2 insidenssimatriisi on

$$A_{G_2} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \end{array}.$$

Insidenssimatriisista nähdään, että sen pystyrivivektorien joukko on lineaarisesti riippumaton, jos se ei sisällä graafin piiriä. Näin ollen graafin piirit ja insidenssimatriisin riippumattomat pystyrivit tuottavat saman lineaarisen matroidin $M(G) = M[A_{G_2}]$. [1]

Yleisemmin voidaan todeta, että kaikki graafiset matroidit ovat lineaarisia. Tämän todistus on esimerkiksi Oxleyllä [1].

Viitteet

[1] Oxley, J. *What is a Matroid?*. https://www.math.lsu.edu/~oxley/survey4.pdf, 2005. Luettu 20.10.2023.

[2] Randow, R. von. *Introduction to the Theory of Matroids.* Springer, 1975.

[3] Salo, V. Sähköpostikirjeenvaihto, tutkielmanohjaus. 2023.

[4] Welsh, D. J. A. *Matroid Theory.* Academic Press, 1976.

[5] Whitney, H. "On the Abstract Properties of Linear Dependence." *American Journal of Mathematics*, vol. 57, no. 3, 1935, pp. 509–33, https://doi.org/10.2307/2371182.