Tarkistusmerkkijärjestelmistä algebrallisissa ryhmissä

Jukka Jylänki
jukkajyl@mail.student.oulu.fi

Matemaattisten tieteiden laitos
Oulun yliopisto
2011

Sisältö

1 Johdanto **3**

2 Perusteita **4**

3 Tarkisteyhtälö **10**
3.1 Tarkistusmerkin laskentakaava 11
3.2 Havainnoitavat virhetyypit 13
3.3 Virheiden tunnistamiseen vaaditut ehdot 15
3.3.1 Kaksoisvirhe ja hyppykaksoisvirhe 15
3.3.2 Vaihtovirhe ja hyppyvaihtovirhe 16

4 Täydelliset kuvaukset **19**
4.1 Olemassaolokriteeri Abelin ryhmissä 20
4.2 Ei-kommutatiiviset ryhmät 25
4.3 Laajennuslause ja sen seuraukset 27
4.4 Yhtäpitäviä muotoiluja 34

5 Antisymmetriset kuvaukset **40**

6 Sopivien kuvausten löytäminen **47**
6.1 Täydellinen enumeraatio 47
6.2 Eckerin ja Pochin algoritmi 50

7 Sovellukset **53**
7.1 Käytössä olevia järjestelmiä 53
7.1.1 1,3,7 -tarkiste 53
7.1.2 Luhnin modulo 10 54
7.1.3 Geometrinen modulo 11 54
7.1.4 Suomalainen henkilötunnusjärjestelmä 55
7.1.5 Verhoeffin D_5-järjestelmä 56
7.1.6 Mod97-10 -tarkiste 58
7.2 Uusia konstruktioita 59
7.2.1 Elementaarinen Abelin 2^k-ryhmä 59
7.2.2 10/16 -järjestelmä 60

7.2.3 10/32 -järjestelmä 61
7.3 Virheentunnistustehokkuus 61

8 Useampi tarkistusmerkki **64**
8.1 Graafien värityksistä 64
8.2 Useamman tarkistusmerkin järjestelmät 67
8.2.1 Kaksinkertainen 10/16 -järjestelmä 68
8.2.2 Kolminkertainen 10/16 -järjestelmä 70

A Permutaatioiden listaus **77**

B Täydellisten kuvausten konstruointi **80**

Luku 1

Johdanto

Sarjanumerojärjestelmiä sekä muita tunnistemerkkijonoja käyttäviä menetelmiä on laajasti käytössä monilla aloilla. Esimerkiksi tuotteiden ja henkilöiden erottelemiseen tarvitaan järjestelmiä, joissa jokaiselle käsiteltävälle kohteelle annetaan oma tunnistekoodi, jolla kohde tallennetaan tietokantaan. Riippuen tietojärjestelmän käyttöalasta, näitä koodeja saatetaan siirtää suullisesti saneltuna, paperilla tai tekstiviestillä, jolloin tunnistekoodi on käsin näppäiltävä päätelaitteelle haluttuun tietueeseen viittaamiseksi. Tällaisissa tilanteissa luku- ja näppäilyvirheet aiheuttavat osan tietojärjestelmässä tapahtuvista käyttövirheistä. Käyttäjä voi vahingossa esimerkiksi tehdä tilisiirron väärälle tilille tai tilata väärän tuotteen. Pahimmassa tapauksessa virhettä ei koskaan huomata tai se huomataan niin myöhään, että sitä ei enää voida korjata. Siksi tunnistejärjestelmiä suunniteltaessa yleisesti varaudutaan tällaisiin tilanteisiin lisäämällä tunnisteisiin tietyllä funktiolla laskettava tarkiste, jonka avulla tunnistetaan virheellisesti syötetyt merkkijonot. Erilaiset funktion valinnat johtavat erilaisiin virheentunnistusominaisuuksiin ja näistä menetelmistä jotkin toimivat toisia huomattavasti paremmin.

Tässä työssä käsittelen tarkistusmerkkijärjestelmiä, joiden konstruktiossa ja analyysissa käytetään algebrallisten ryhmien teoriaa. Keskeisenä osana ovat käsitteet täydellisistä ja antisymmetrisistä kuvauksista sekä kiintopistevapaat ryhmäautomorfismit. Tarkastelut johtavat kuuluisan Hall-Paige -konjektuurin käsittelyyn, joka liittyy täydellisten kuvausten olemassaoloon äärellisissä ryhmissä.

Oman osan tästä työstä muodostavat tietokoneajot, joiden avulla kokeellisesti haettiin uusia konstruktioita tarkistusmerkkijärjestelmille, enumeroitiin erilaisten sopivien kuvausten lukumääriä sekä laskettiin tunnettujen järjestelmien eri virheluokkien tunnistusfrekvenssejä. Työn viimeisessä osassa esittelen graafiteoriaan pohjautuen uusia tuloksia tarkistusmerkkijärjestelmien virheentunnistusrajoista ja konstruoin uuden menetelmän, joka tietyin rajoittein tunnistaa syötteessä tapahtuvat k virhettä käyttäen k:ta tarkistusmerkkiä.

Luku 2

Perusteita

Tässä työssä käytetään seuraavia vakiintuneita merkintöjä.

$\mathbb{Z}$: Kokonaislukujen joukko.

$\mathbb{Z}_+$: Aidosti positiivisten kokonaislukujen joukko.

$\mathbb{P}$: Alkulukujen joukko.

$\mathbb{Z}_n$: Jakojäännösluokkien joukko modulo n.

C_n: Kertalukua n oleva syklinen ryhmä.

S_G: Kaikkien ryhmän G alkioita operoivien permutaatioiden ryhmä.

e_G: Ryhmän G identiteettialkio. Jos ryhmästä ei ole epäselvyyttä, niin merkitään yksinkertaisesti e.

$g^a, a \in G$: Alkion g konjugointi ryhmän G alkiolla a eli tulo $a^{-1}ga$.

$|G|$, $|g|$: Ryhmän G tai alkion g kertaluku.

$H \leq G$: Ryhmä H on ryhmän G aliryhmä.

$N \lhd G$: Ryhmä N on ryhmän G aito normaali aliryhmä.

$[G : H]$: Aliryhmän H *indeksi* ryhmässä G eli osamäärä $\frac{|G|}{|H|}$.

$G \cong H$: Ryhmät G ja H ovat isomorfisia keskenään.

Yleissääntönä isot kirjaimet $G, H, \ldots$ varataan symboloimaan ryhmiä ja joukkoja ja pienet kirjaimet $g, h, \ldots$ niihin kuuluvia alkioita. Kaikki käsiteltävät ryhmät ja joukot tulee olettaa äärellisiksi, ellei toisin erikseen mainita.

Lukijan oletetaan entuudestaan tuntevan ryhmäteorian peruskäsitteitä kuten syklinen ryhmä, aliryhmä ja permutaatioryhmä. Tässä luvussa esitetään ilman todistusta myöhemmin tarvittavia perustuloksia, joiden taustatietoa varten suositellaan esimerkiksi M. Niemenmaan luentoja tai S. Langin kirjaa ([1], [2] ja [3]).

Lause 2.1 (Lagrange)**.** *Ryhmän G jokaiselle aliryhmälle H on voimassa ehto $|H| \mid |G|$. Jos $g \in G$, niin $|g| \mid |G|$.*

□

Propositio 2.2. *Jos H on ryhmän G aliryhmä ja $n := [G : H]$, niin on olemassa alkiot $g_1, \ldots, g_n \in G$ ja $g'_1, \ldots, g'_n \in G$, joille pätee*

$$G = g_1H \cup g_2H \cup \ldots \cup g_nH = Hg'_1 \cup Hg'_2 \cup \ldots \cup Hg'_n,$$

missä joukkoja g_iH sanotaan aliryhmän H vasemmanpuoleiseksi sivuluokiksi ja joukkoja Hg'_i vastaavasti aliryhmän H oikeanpuoleisiksi sivuluokiksi. Alkioita g_i sanotaan aliryhmän H vasemmanpuoleisten sivuluokkien edustajiksi sekä alkioita g'_i aliryhmän H oikeanpuoleisten sivuluokkien edustajiksi. Näille sivuluokille on voimassa ehdot $g_iH \cap g_jH \neq \emptyset \Rightarrow g_i = g_j$ sekä $Hg'_i \cap Hg'_j \neq \emptyset \Rightarrow g'_i = g'_j$.

Jokainen ryhmän G alkio g voidaan esittää yksikäsitteisesti muodossa $g = g_ih = h'g'_j$, missä $i, j \in \mathbb{Z}_+ \cap [1, n]$ ja $h, h' \in H$.

Määritelmä 2.3. *Ryhmän G aliryhmää N sanotaan normaaliksi aliryhmäksi ryhmässä G, jos kaikilla $g \in G$ ja $n \in N$ on voimassa ehto $gng^{-1} \in N$. Tällöin merkitään $N \trianglelefteq G$.*

Aliryhmien normaalius ei ole transitiivinen ominaisuus, eli ehdosta $A \trianglelefteq B \trianglelefteq C$ ei seuraa, että $A \trianglelefteq C$. Kuitenkin tekijäryhmien suhteen pitää paikkansa seuraava ominaisuus [4, lause 2.28(ii)].

Propositio 2.4. *Olkoon $H \trianglelefteq G$ ja K sellainen ryhmän G aliryhmä, jolle on voimassa $H \leq K$ ja $K/H \trianglelefteq G/H$. Tällöin $K \trianglelefteq G$.*

□

Ryhmän G ei-triviaalia normaalia aliryhmää N sanotaan ryhmän G minimaaliseksi normaaliksi aliryhmäksi, jos ehdosta $N' \leq N, N' \trianglelefteq G$ seuraa, että $N' = \{e\}$ tai $N' = N$. Ryhmän minimaalinen normaali aliryhmä ei ole välttämättä yksikäsitteinen, edes kertaluvultaan.

Lause 2.5. *Jos $H < G$ ja $[G : H] = 2$, niin $H \lhd G$.*

□

Ryhmän G kahdesta aliryhmästä A ja B voidaan muodostaa kompleksi $AB = \{ab : a \in A \text{ ja } b \in B\}$, jonka koko voidaan laskea kaavalla

$$|AB| = \frac{|A||B|}{|A \cap B|}. \tag{2.1}$$

Tämä joukko ei välttämättä ole ryhmän G aliryhmä.

Lemma 2.6. *Jos $A \trianglelefteq G$ tai $B \trianglelefteq G$, niin kompleksi AB on ryhmän G aliryhmä.*

□

Määritelmä 2.7. *Jos ei-triviaalilla ryhmällä G ei ole olemassa muita normaaleja aliryhmiä kuin triviaalit normaalit aliryhmät $\{e\}$ ja G, niin ryhmää G sanotaan yksinkertaiseksi ryhmäksi.*

Määritelmä 2.8. *Jos ryhmällä G on olemassa normaalien aliryhmien ketju*

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_k = G,$$

missä tekijäryhmät G_j/G_{j-1} ovat abeliaanisia kaikilla $j = 1, 2, \ldots, k$, niin ryhmää G sanotaan ratkeavaksi ryhmäksi.

Ratkeavan ryhmän kaikki aliryhmät ja tekijäryhmät ovat myös ratkeavia [4, lauseet 5.15, 5.16].

Määritelmä 2.9. *Ryhmää H, jonka kertaluku on muotoa $|H| = p^n$, missä $n \in \mathbb{Z}_+$ ja $p \in \mathbb{P}$, sanotaan p-ryhmäksi. Jos H on jonkin ryhmän G aliryhmä ja $p^{n+1} \nmid |G|$, niin ryhmää H sanotaan ryhmän G Sylowin p-aliryhmäksi.*

Kaikki ryhmän G Sylowin p-aliryhmät konjugoivat keskenään ryhmässä G [4, lause 4.12(i)].

Ratkeavan ryhmän minimaalisella normaalilla aliryhmällä on seuraava ominaisuus [5, harjoitus 9.1, 9.2].

Lause 2.10. *Jos N on ratkeavan ryhmän G minimaalinen normaali aliryhmä, niin tällöin N on kommutatiivinen p-ryhmä.*

□

Seuraavat rakenteet esiintyvät usein myöhemmissä tarkasteluissa.

Määritelmä 2.11. *Olkoon G ryhmä ja g jokin sen alkio. Alkion g sentralisoijaksi $C_G(g)$ kutsutaan ryhmän G kaikkia alkioita, jotka kommutoivat alkion g kanssa eli*

$$C_G(g) = \{x \in G : gx = xg\}.$$

Jos $A \subseteq G$, niin joukon A sentralisoija määritellään samaan tapaan kaavalla

$$C_G(A) = \{x \in G : \forall\ a \in A : ax = xa\}.$$

Ryhmän G sentralisoijaa itsessään $C_G(G)$ sanotaan ryhmän G keskukseksi ja sille käytetään merkintää $Z(G)$. Sentralisoijaan liittyy läheisesti seuraava käsite.

Määritelmä 2.12. *Olkoon G jokin ryhmä ja $M \subseteq G$. Tällöin joukkoa*

$$N_G(M) = \{g \in G : M^g = M\}$$

sanotaan joukon M normalisoijaksi ryhmässä G.

Joukot $C_G(a), C_G(A)$ ja $N_G(M)$ muodostavat ryhmän G aliryhmiä.

Määritelmä 2.13. *Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä ja θ kuvaus ryhmältä G ryhmälle H. Tällöin sanotaan, että kuvaus θ on **homomorfismi**, jos se toteuttaa ehdon*

$$\theta(a \cdot b) = \theta(a) * \theta(b).$$

kaikilla $a, b \in G$.

Huomaa, että homomorfismin ei tarvitse olla injektiivinen tai surjektiivinen. Bijektiivistä homomorfismia kutsutaan *isomorfismiksi*. Jos edellisessä määritelmässä $G = H$ ja kuvaus θ on bijektiivinen, niin tällöin kuvausta θ sanotaan ryhmän G *automorfismiksi*. Ryhmän G kaikkien automorfismien joukolle käytetään merkintää $Aut(G)$.

Määritelmä 2.14. *Olkoon N ja H ryhmiä ja kuvaus ϕ homomorfismi $H \mapsto Aut(N) : \phi(h) := \theta_h$. Tällöin määritellään kuvauksen ϕ indusoima puolisuora tulo pariksi $(N \rtimes_\phi H, *)$, missä $N \rtimes_\phi H = \{(n, h) : n \in N \text{ ja } h \in H\}$ ja operaatio $*$ on määritelty asettamalla*

$$(n_1, h_1) * (n_2, h_2) := (n_1\phi(h_1)(n_2), h_1h_2) = (n_1\theta_{h_1}(n_2), h_1h_2)$$

Lemma 2.15. *Pari $(N \rtimes_\phi H, *)$ on ryhmä.*

Todistus. Joukon $N \rtimes_\phi H$ neutraalialkiona toimii alkio (e_N, e_H), missä $e_N \in N$ ja $e_H \in H$ ovat ryhmien N ja H neutraalialkiot. Jos $(n_1, h_1) \in N \rtimes_\phi H$, niin

$$\begin{aligned} (n_1, h_1) * (e_N, e_H) &= (n_1\theta_{h_1}(e_N), h_1e_H) = (n_1, h_1) \text{ ja} \\ (e_N, e_H) * (n_1, h_1) &= (e_N\theta_{e_H}(n_1), e_Hh_1) = (n_1, h_1). \end{aligned}$$

Yllä $\theta_{e_H}(n_1) = \phi(e_H)(n_1) = n_1$, sillä ϕ kuvaa homomorfismina ryhmän H identiteettialkion ryhmän $Aut(N)$ identieettialkiolle. Alkion (n, h) käänteisalkio on alkio $(\theta_{h^{-1}}(n^{-1}), h^{-1})$, sillä

$$\begin{aligned} (n, h) * (\theta_{h^{-1}}(n^{-1}), h^{-1}) &= (n\theta_h(\theta_{h^{-1}}(n^{-1})), hh^{-1}) = (e_N, e_H) \text{ ja} \\ (\theta_{h^{-1}}(n^{-1}), h^{-1}) * (n, h) &= (\theta_{h^{-1}}(n^{-1})\theta_{h^{-1}}(n), h^{-1}h) = (e_N, e_H). \end{aligned}$$

Lisäksi $*$ on assosiatiivinen operaatio, koska

$$\begin{aligned} \big[(n_1, h_1) * (n_2, h_2)\big] * (n_3, h_3) &= (n_1\theta_{h_1}(n_2), h_1h_2) * (n_3, h_3) = \\ \big((n_1\theta_{h_1}(n_2))\theta_{h_1h_2}(n_3), (h_1h_2)h_3\big) &= \big(n_1(\theta_{h_1}(n_2\theta_{h_2}(n_3)), h_1(h_2h_3)\big) = \\ (n_1, h_1) * (n_2\theta_{h_2}(n_3), h_2h_3) &= (n_1, h_1) * \big[(n_2, h_2) * (n_3, h_3)\big]. \end{aligned}$$

Huomaa, että edellä $\theta_{h_1h_2}(n_3) = \theta_{h_1}(\theta_{h_2}(n_3))$.

□

Myöhemmin käytetään toistuvasti seuraavaa havaintoa.

Propositio 2.16. *Jos $G = N \rtimes_\phi H$, niin on olemassa ryhmät $N' \cong N$ ja $H' \cong H$, joille $N' \lhd G$ ja $H' \lhd G$.*

□

Kahden ryhmän G ja H *suora tulo* määritellään erikoistapauksena puolisuorasta tulosta valitsemalla $\forall\, h \in H : \phi(h) = id$, missä $id(n) = n$. Tällöin ryhmäoperaatio saa tutun muodon

$$(n_1, h_1) * (n_2, h_2) = (n_1 n_2, h_1 h_2).$$

Ryhmien G ja H suoralle tulolle käytetään merkintää $G \times H$.

Esimerkki. Valitaan

$$G := C_n =< a >, \quad H := C_2 = \{e_H, b\}, \quad \theta_{e_H} := id \text{ ja } \theta_b := inv,$$

missä $inv(n) = n^{-1}$. Tällöin määritelmän 2.14 puolisuora tulo antaa ryhmän, jonka alkiot ovat muotoa (x, y), missä $x \in C_n, y \in C_2$. Ryhmäoperaatio $*$ lasketaan kaavoilla

$$\begin{aligned}
(a^i, e_H) * (a^j, e_H) &= (a^{i+j}, e_H), \\
(a^i, e_H) * (a^j, b) &= (a^{i+j}, b), \\
(a^i, b) * (a^j, e_H) &= (a^{i-j}, b), \text{ sekä} \\
(a^i, b) * (a^j, b) &= (a^{i-j}, e_H).
\end{aligned}$$

Samaistetaan $(a^i, e_H) \sim a^i$, $(e_G, b) \sim b$ ja $(e_G, e_H) \sim e$, jolloin saadaan ryhmä

$$D_n := < a, b : a^n = e, b^2 = e, ab = ba^{-1} >,$$

jota kutsutaan astetta n olevaksi *dihedraaliseksi ryhmäksi*. Huomaa, että tässä notaatiossa $|D_n| = 2n$. Joissain lähteissä käytetään erilaista merkintätapaa, jossa $|D_{2n}| = 2n$.

Määritelmä 2.17. *Ryhmän G aliryhmää N sanotaan karakteristiseksi aliryhmäksi ryhmässä G ja merkitään N char G, jos kaikilla ryhmän G automorfismeilla θ on voimassa $\theta(N) = N$.*

Karakteristiset aliryhmät ovat aina samalla myös normaaleja aliryhmiä. Ryhmän karakteristisuus on transitiivinen ominaisuus ja toimii seuraavasti [5, lemma 6.1].

Lemma 2.18.

1. *Olkoon $N \trianglelefteq G$ ja M char N. Tällöin $M \trianglelefteq G$.*
2. *Olkoon U char B ja B char G. Tällöin U char G.*

□

Edellä määritelty ryhmän G keskus $Z(G)$ on aina karakteristinen ryhmässä G [4, harjoitus 5.25].

Seuraavaa tulos oletetaan myös tunnetuksi [5, lause 4.8].

Lause 2.19 (Frattini argument)**.** *Olkoon $K \trianglelefteq G$ ja P ryhmän K Sylowin p-aliryhmä. Tällöin $G = KN_G(P)$.*

Lisäksi tarvitaan vielä seuraavaa normaalien aliryhmien isomorfiaan liittyvää ominaisuutta [5, lause 2.3].

Lause 2.20. *Olkoon $U \leq G$ ja $N \trianglelefteq G$. Tällöin $(UN)/N \cong U/(U \cap N)$.*

Luku 3

Tarkisteyhtälö

Aiheeseen perehtymiseksi tarkastellaan aluksi muutamia esimerkkejä käytännössä olevista järjestelmistä.

Kansainvälisesti käytetyn **ISBN-10** -järjestelmän [6] numerosarjat koostuvat yhdeksästä numerosta a_1, ..., a_9, sekä tarkistenumerosta a_{10}, joka lasketaan kaavalla

$$a_{10} \equiv -\sum_{i=1}^{9}(11-i)\cdot a_i \pmod{11}.$$

Jos tällä menetelmällä laskettuna $a_{10} = 10$, niin se koodataan käyttämällä ylimääräistä merkkiä **X**.

Esimerkiksi kuvassa 3.1 esitetty ISBN-10 -koodi on kelvollinen, koska sen tarkistenumero täsmää:

$$a_{10} \equiv -(10\cdot\mathbf{0}+9\cdot\mathbf{4}+8\cdot\mathbf{7}+7\cdot\mathbf{0}+6\cdot\mathbf{8}+5\cdot\mathbf{4}+4\cdot\mathbf{6}+3\cdot\mathbf{7}+2\cdot\mathbf{4}) \equiv \mathbf{7} \pmod{11}$$

EAN-13 -järjestelmää [7] käytetään tunnistamaan Euroopassa markkinoilla olevia kulutustuotteita. EAN-koodi on kolmetoista merkkiä pitkä numerosarja $a_1a_2a_3\ldots a_{13}$, joista viimeinen a_{13} on tarkistusmerkki, joka lasketaan kaavalla

$$a_{13} = -(a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + \ldots a_{11} + 3a_{12}) \pmod{10}.$$



Kuva 3.1: ISBN-10 ja EAN-13 -koodit.

Sekä ISBN- että EAN -koodijärjestelmät havaitsevat kaikki syötteessä tapahtuvat *yksittäisvirheet*, eli sellaiset virheet, joissa oikeasta merkkijonosta täsmälleen yhdessä paikassa merkki muuttuu toiseksi. Modulo 10 -laskentaan perustuvat tarkistusmerkkijärjestelmät ovat käytännöllisiä, koska niissä tarvitaan vain numeroita 0-9. ISBN-järjestelmässä on otettava yksi lisäkirjain merkitsemään lukua 10.

Esimerkki. *Vaihtovirheeksi* tai *transpositiovirheeksi* sanotaan sellaista syötteessä tapahtuvaa virhettä, jossa kaksi vierekkäistä merkkiä vaihtavat järjestystä. Jos kuvassa 3.1 esitetyn EAN-13 -koodin näppäilyssä tapahtuu lopussa lukujen 0 ja 5 välillä transpositiovirhe, niin tätä virhettä ei havaita, sillä virheellisen syötejonon $6-410402-023509$ tarkistusmerkki on sattumalta sama kuin alkuperäisellä oikealla merkkijonolla:

$$a_{13} \equiv -(\mathbf{6}+3\cdot\mathbf{4}+\mathbf{1}+3\cdot\mathbf{0}+\mathbf{4}+3\cdot\mathbf{0}+\mathbf{2}+3\cdot\mathbf{0}+\mathbf{2}+3\cdot\mathbf{3}+\mathbf{5}+3\cdot\mathbf{0}) \equiv \mathbf{9} \pmod{10}.$$

Tämä johtuu tietenkin siitä, että $1 \cdot \mathbf{5} + 3 \cdot \mathbf{0} \equiv 1 \cdot \mathbf{0} + 3 \cdot \mathbf{5} \equiv 5 \pmod{10}$. ISBN-10 -järjestelmä sen sijaan havaitsee kaikki vaihtovirheet. Myöhemmin tullaan todistamaan, että mikään ryhmään $\mathbb{Z}_{10}$ perustuva tarkistusmerkkijärjestelmä ei voi samanaikaisesti havaita kaikkia yksittäisvirheitä sekä transpositiovirheitä. Tässä mielessä ISBN-10 -järjestelmän modulo 11 -tarkiste on tehokkaampi ratkaisu kuin EAN-13 -järjestelmän modulo 10 -rakenne. Hieman merkillistä onkin, että vuonna 2007 ISBN-10 -järjestelmän korvaavassa laajennetussa **ISBN-13** -järjestelmässä siirryttiin käyttämään samaa modulo 10 -tarkistetta kuin EAN-13 -järjestelmässä [8, 4.5].

Vastaavanlaisia esimerkkejä löytyy paljon, sillä tarkistemerkkejä käytetään sarjanumerojärjestelmissä lähes kaikkialla. Suomessa käytettäviä järjestelmiä ovat esimerkiksi Y-tunnus [9], ALV-numero [10] sekä suomalainen henkilötunnus [11]. Yleisemmin tarkistemerkkejä käytetään kansainvälisesti IBAN-pankkitilinumerossa [12], passeissa [13, §iv-24] ja viisumeissa [14, §iv-17], sekä luottokorttien numeroissa [15].

Luvussa 7 esitellään lisää yleisesti vakiintuneita järjestelmiä ja vertaillaan niiden virheentunnistusominaisuuksia eri virheluokissa.

3.1 Tarkistusmerkin laskentakaava

Tarkistusmerkin laskemista voidaan käsitellä mielivaltaisen ryhmän $(G, \cdot)$ sisällä samaistamalla käsiteltävän merkkijonon aakkosto ryhmän G alkioiden kanssa. Olkoon tällöin $a_1a_2a_3\ldots a_{n-1}, a_i \in G$ merkkijono, jolle tarkistusmerkki halutaan laskea. Käyttämällä ryhmäoperaatiota $\cdot$ ja ennalta valittuja kuvauksia $\delta_1, \ldots, \delta_{n-1}$, missä $\delta_i : G \to G$ voidaan tarkistusmerkki määritellä sellaiseksi alkioksi a_n, joka toteuttaa kaavan

$$\delta_1(a_1) \cdot \delta_2(a_2) \cdot \ldots \cdot \delta_{n-1}(a_{n-1}) = a_n. \tag{3.1}$$

Tarkiste a_n sijoitetaan yleensä viimeiseksi alkioksi syötteen loppuun. Tällä tavoin konstruoituna tarkistusmerkkijärjestelmän virheentunnistuskyky riippuu valitusta ryhmästä G sekä siitä, millaisia kuvauksia δ_i käytetään.

Heti on ilmeistä, että kuvauksilla δ_i täytyy olla ominaisuus $\delta_i(x) \neq \delta_i(y)$ kaikilla $x, y \in G$ ja $\delta_i \in S_G$, koska muulloin yksittäisen merkin x muuttumista merkiksi y ei havaittaisi. Tämä ominaisuus otetaan tarkistusmerkkijärjestelmän perusvaatimukseksi ja tässä työssä käsitellään vain järjestelmiä, joissa kuvaukset δ_i ovat ryhmän G permutaatioita.

Joskus käytetään myös kaavaa

$$\delta_1(a_1) \cdot \delta_2(a_2) \cdot \ldots \cdot \delta_{n-1}(a_{n-1}) \cdot \delta_n(a_n) = e, \tag{3.2}$$

joka on ominaisuuksiensa puolesta yhtäpitävä yhtälön 3.1 kanssa.

Lähes kaikki käytössä olevat tarkistusmerkkijärjestelmät voidaan esittää kaavan 3.1 tai 3.2 muodossa. Esimerkiksi EAN-13 -järjestelmä saadaan valitsemalla $G = \mathbb{Z}_{10}$ ja käyttämällä yhtälöä 3.2, missä

$$\delta_{2k+1}(x) = x \text{ ja } \delta_{2k}(x) = 3x.$$

Mielivaltaista permutaatioiden δ_i valintaa voi olla hankala analysoida. Valitsemalla vain yhden permutaation δ ja merkitsemällä $\delta_i := \delta^i$ saadaan helpommin käsiteltävä rakenne, jolla on myös hyödyllisiä ominaisuuksia. Siten yhtälö 3.1 saa muodon

$$\delta(a_1) \cdot \delta^2(a_2) \cdot \delta^3(a_3) \cdot \ldots \cdot \delta^{n-1}(a_{n-1}) = a_n \tag{3.3}$$

tai vaihtoehtoisesti yhtälöstä 3.2,

$$\delta(a_1) \cdot \delta^2(a_2) \cdot \delta^3(a_3) \cdot \ldots \cdot \delta^n(a_n) = e. \tag{3.4}$$

Tällä tavoin käsiteltynä jokainen ryhmän G permutaatio δ yksistään määrittelee jonkin tarkistusmerkkijärjestelmän. Siten seuraava määritelmä on luonnollinen.

Määritelmä 3.1. *Ryhmässä G toimivaa tarkistusmerkkijärjestelmää, jossa käytetään yhtä ryhmän G permutaatiota δ ja tarkisteyhtälöä 3.3 tai 3.4, sanotaan parin (G, δ) muodostamaksi tarkistusmerkkijärjestelmäksi. Jos ryhmästä G ei ole epäselvyyttä, niin puhutaan myös pelkästään permutaation δ muodostamasta tarkistusmerkkijärjestelmästä.*

Jatkossa tarkistusmerkkijärjestelmää käsitellään myös diskreettinä funktiona $f : G^{n-1} \to G$, missä $f(a_1 a_2 \ldots a_{n-1}) = a_n$. Tämä funktio kuvaa syöteavaruuden $|G|^{n-1}$ alkiota vain $|G|$ kappaleeksi eri tarkistemerkkejä, joten törmääviä syötejonoja on paljon. Siten mielivaltaisia satunnaisvirheitä ei voida tunnistaa täydellisesti. Tämä motivoi erilaisten yleisimpien virhetyyppien luokitteluun ja sellaisten järjestelmien kehittämiseen, joissa ainakin nämä yleisimmät virhetyypit tulisi tunnistettua.

Virheluokka	Kuvaus ($a \neq b$)	Verhoeff	Beckley
yksittäisvirhe	$a \to b$	79.0%	86%
vaihtovirhe	$ab \to ba$	10.2%	8%
hyppyvaihtovirhe	$acb \to bca$	0.8%	
kaksoisvirhe	$aa \to bb$	0.6%	6%
foneettinen virhe	$a0 \leftrightarrow 1a, 2 \leq a \leq 9$	0.5%	
hyppykaksoisvirhe	$aca \to bcb$	0.3%	
muut virheet		8.6%	-

Taulukko 3.1: Virheluokkien esiintymistiheydet R.H. Schulzin esittämänä [7].

3.2 Havainnoitavat virhetyypit

Tarkistusmerkkijärjestelmien tarkoituksena on suojata pääasiassa ihmisten aiheuttamilta merkkijonojen kirjoitus- ja saneluvirheiltä ja siispä syntyvät virheet ovat kaikkea muuta kuin satunnaisia. Tämän luvun alussa esiteltiin kaksi yleisintä virhetyyppiä, jotka ovat yksittäisvirhe ja transpositiovirhe.

J. Verhoeff ja D.F. Beckley tutkivat [16] [17] tilastollisesti erilaisia kirjoitettaessa tapahtuvia virheitä ja jakoivat ne virheluokkiin, jotka on esitetty taulukossa 3.1. Yksittäisvirheiden ja vaihtovirheiden osuus kaikista virheistä on Verhoeffin mukaan yhteensä 89.2%, joten olisi toivottavaa, että tarkistusmerkkijärjestelmä tunnistaisi ainakin nämä molemmat virheluokat.

Taulukon 3.1 toisessa sarakkeessa kirjaimet tarkoittavat yksittäisiä ryhmän G alkioita ja tässä sarakkeessa näytetään vain ne merkit, jotka ovat oleellisia virheen kannalta. Esimerkiksi merkintä $acb \to bca$ hyppyvaihtovirheen kohdalla tarkoittaa, että merkkijonoon $a_1a_2 \ldots acb \ldots a_{n-1}a_n$ syntyy virhe, joka muuttaa merkkijonon muotoon $a_1a_2 \ldots bca \ldots a_{n-1}a_n$.

Tarkistusmerkkijärjestelmiä analysoitaessa on muistettava, että virhe voi syntyä myös itse tarkistusmerkkiin. Siksi yhtälöä 3.2 on toisinaan helpompi tarkastella kuin kaavaa 3.1, sillä yhtälössä 3.2 kaikkia syötejonon merkkejä käsitellään yhtenäisesti.

Foneettisella virheellä tarkoitetaan englannin kielellä saneltaessa tapahtuvaa virhettä, jossa esimerkiksi "fifty" (50) kuullaan väärin muotoon "fifteen" (15), tai toisinpäin. Tällaisia muunnoksia voi tapahtua kahdeksalla eri luvun a arvolla ($2 \leq a \leq 9$). Suomen kielellä saneltaessa näitä virheitä ei juurikaan tapahdu, koska näiden sanojen äänneasu on täysin erilainen.

A. Ecker ja G. Poch laajentavat Verhoeffin ja Beckleyn virhetyyppien listaa tunnistamalla yleisempiä kaksoisvirheiden tyyppejä. Nämä virhetyypit on esitelty taulukossa 3.2. Merkintä "..." symboloi välissäolevia nollaa tai useampaa määrää merkkejä, jotka eivät muutu. Vaikkapa muunnos $abcdefghj \to a\underline{ghdef}\underline{bcj}$ on esimerkki yleisestä kaksoistranspositiovirheestä.

Muunnosvirheessä m kappaletta merkkijonon perättäisiä merkkejä muuttuvat siten, että niiden kaikkien arvo kasvaa tai vähenee arvolla e. Tätä vir-

Virheluokka	Kuvaus
kaksi yksittäisvirhettä	$a \dots b \to c \dots d, a \neq c$ ja $b \neq d$
yleinen transpositio	$a \dots b \to b \dots a, a \neq b$
yleinen kaksoistranspositio	$ab \dots cd \to cd \dots ab, a \neq c$ ja $b \neq d$
muunnosvirhe	$abc \dots \to (a+x)(b+x)(c+x) \dots, x \neq e$

Taulukko 3.2: Kaksoisvirheiden tyyppejä A. Eckerin ja G. Pochin mukaan [18].

hetyyppiä ei käsitellä tässä työssä.

Tarkistusmerkkijärjestelmien käytön yhteydessä tapahtuvista kirjoitusvirheistä ei ole tiettävästi tehty muita kattavia tilastollisia tutkimuksia. F.J. Damerau [19] mainitsee oikolukujärjestelmiä koskevassa artikkelissaan yli 80% heidän havaitsemistaan kirjoitusvirheistä kuuluvan yhteen seuraavista tyypeistä:

1. Yksittäisen merkin lisäys. Esimerkiksi $abcde \to ab\underline{f}cde$.
2. Yksittäisen merkin katoaminen. Esimerkiksi $abc\underline{d}e \to abce$.
3. Yksittäisen merkin muuttuminen tai vaihtovirhe. Nämä ovat samat kuin Verhoeffilla ja Beckleyllä.

Esiintymistiheyksiä näiden luokkien välillä ei kuitenkaan eritelty.

Yleensä tarkistejärjestelmät perustuvat aina kiinteänpituisten merkkijonojen käyttöön vaikka teoria ei sitä estä, minkä perusteella havaitaan kaikki yksittäisten merkkien puuttumiset tai lisäykset, ellei näitä ole tapahtunut täsmälleen yhtä paljon. Kappaleessa 7.1.6 esiteltävä IBAN-järjestelmä on esimerkki tarkistusmerkkijärjestelmästä, jossa syötemerkkijonon pituus voi vaihdella.

Kahden yksittäisvirheen tapahtuminen yhtäaikaisesti on myös mahdollista. Kaikki taulukossa 3.1 esitetyt virhetyypit sekä taulukon 3.2 yleinen transpositiovirhe ovat erikoistapauksia tästä virheluokasta ja siten siis sisältyvät tähän virheluokkaan. Valitettavasti kaavaan 3.3 perustuva järjestelmä ei voi havaita mielivaltaisia kahta yksittäisvirhettä. Tätä rajoitetta käsitellään luvussa 8.

Edellä esitettyjä virheluokkia voidaan vielä yleistää ainakin muutamilla tavoilla. Näitä on esitetty taulukossa 3.3. Yleinen kaksoisvirhe yleistää kaksoisvirheen ja hyppykaksoisvirheen käsitteet sallimalla muuttuvien merkkien etäisyyden olla mielivaltainen. Transpositio- ja yksittäisvirhe on erikoistapaus kahdesta yksittäisvirheestä, kun muuttuvat merkit ovat vierekkäisiä. Kaksi transpositiota tarkoittaa kahta toisistaan erillään tapahtuvaa kahden vierekkäisen merkin vaihtumista. Se ei sisällä kolmen merkin rotaatiovirheitä eli virheitä $abc \leftrightarrow bca$.

Virheluokka	Kuvaus
yleinen kaksoisvirhe	$a \dots a \to b \dots b, a \neq b$
transpositio- ja yksittäisvirhe	$ax \to ya, a \neq x, x \neq y, a \neq y$
kaksi transpositiota	$ab \dots cd \to ba \dots dc, a \neq b$ ja $c \neq d$

Taulukko 3.3: Yleistettyjä kaksoisvirheitä.

3.3 Virheiden tunnistamiseen vaaditut ehdot

Tarkastellaan seuraavaksi millaisia ominaisuuksia tarkistusmerkkijärjestelmällä on yleisesti oltava, jotta se tunnistaisi edellä esitetyn tyyppisiä virheitä. Tässä kappaleessa käytetään kappaleen 3.1 merkintöjä.

Edellisessä kappaleessa mainittiin, että kuvausten δ_i on oltava permutaatioita, jotta yksittäisvirheet voitaisiin tunnistaa. Tämä voidaan tarkistaa seuraavasti. Oletetaan, että merkkijono $a_1a_2 \dots a \dots a_n$ muuttuu muotoon $a_1a_2 \dots b \dots a_n$. Jos tätä muutosta ei havaita, niin on oltava

$$\begin{aligned} \delta_1(a_1)\delta_2(a_2) \dots \delta_k(a) \dots \delta_n(a_n) &= \delta_1(a_1)\delta_2(a_2) \dots \delta_k(b) \dots \delta_n(a_n) \\ \delta_k(a) &= \delta_k(b), \end{aligned}$$

mistä voidaan päätellä, että kuvaus δ_k ei ole bijektio, sillä se kuvaa alkiot a ja b samalle arvolle.

3.3.1 Kaksoisvirhe ja hyppykaksoisvirhe

Viestissä tapahtuu kaksoisvirhe silloin kun muotoa aa oleva kahdennettu merkki muuttuu merkkipariksi bb, missä $a \neq b$. Oletetaan, että merkkijono $a_1a_2 \dots aa \dots a_n$ muuttuu muotoon $a_1a_2 \dots bb \dots a_n$. Tämä muutos havaitaan jos ja vain jos

$$\begin{aligned} \delta_1(a_1) \dots \delta_k(a)\delta_{k+1}(a) \dots \delta_n(a_n) &\neq \delta_1(a_1) \dots \delta_k(b)\delta_{k+1}(b) \dots \delta_n(a_n) \\ \delta_k(a)\delta_{k+1}(a) &\neq \delta_k(b)\delta_{k+1}(b). \end{aligned}$$

Tehdään merkintä $x := \delta_k(a)$ ja $y := \delta_k(b)$, jolloin $a = \delta_k^{-1}(x)$ ja $b = \delta_k^{-1}(y)$, sillä kuvaukset δ_i valittiin olevan ryhmän G permutaatioita. Tällöin edelläoleva ehto saa muodon

$$x\delta_{k+1}\big(\delta_k^{-1}(x)\big) \neq y\delta_{k+1}\big(\delta_k^{-1}(y)\big).$$

Merkitään vielä $\theta(\cdot) := \delta_{k+1}\big(\delta_k^{-1}(\cdot)\big)$, jolloin vaadittu ehto kaikkien kaksoisvirheiden tunnistamiseen on seuraava:

$$x\theta(x) \neq y\theta(y) \text{ kaikilla } x, y \in G, \text{ joilla } x \neq y.$$

Muotoillaan tämä kriteeri permutaation θ ominaisuutena seuraavasti.

Määritelmä 3.2. *Ryhmän G permutaatiota θ sanotaan täydelliseksi kuvaukseksi, jos kaikilla $x, y \in G$ yhtälöstä $x\theta(x) = y\theta(y)$ seuraa, että $x = y$. Yhtäpitävästi, kuvaus θ on täydellinen, jos kuvaus $\eta(x) := x\theta(x)$ on bijektio ryhmässä G.*

Luvussa 4 keskitytään käsittelemään tarkemmin täydellisiä kuvauksia.

Hyppykaksoisvirhe. Tämän virheen havainnointi johtaa hyvin samanlaiseen tilanteen kuin edellä. Hyppykaksoisvirheessä merkkijono *aca* muuttuu muotoon *bcb*. Etenemällä samanlaisella menettelyllä kuin edellä, nähdään että tällainen virhe tunnistetaan täsmälleen silloin, kun

$$\forall\, x, y, z \in G : xz\delta^2(x) \neq yz\delta^2(y).$$

3.3.2 Vaihtovirhe ja hyppyvaihtovirhe

Transpositio- tai vaihtovirheellä tarkoitetaan muunnosta $a_1a_2 \ldots ab \ldots a_n \to a_1a_2 \ldots ba \ldots a_n$. Jotta tämä virhe havaittaisiin, niin yhtälön 3.2 mukaan

$$\begin{aligned} \delta_1(a_1) \ldots \delta_k(a)\delta_{k+1}(b) \ldots \delta_n(a_n) &\neq \delta_1(a_1) \ldots \delta_k(b)\delta_{k+1}(a) \ldots \delta_n(a_n) \\ \delta_k(a)\delta_{k+1}(b) &\neq \delta_k(b)\delta_{k+1}(a). \end{aligned}$$

Korvataan yllä $x := \delta_k(a)$ ja $y := \delta_k(b)$. Kuvaukset δ_i valittiin aina permutaatioiksi, joten $a = \delta_k^{-1}(x)$ ja $b = \delta_k^{-1}(y)$. Saadaan yhtälö

$$x\delta_{k+1}\big(\delta_k^{-1}(y)\big) \neq y\delta_{k+1}\big(\delta_k^{-1}(x)\big).$$

Merkitään vielä $\phi(\cdot) := \delta_{k+1}\delta_k^{-1}(\cdot)$, jolloin transpositiovirheiden tunnistamiseen vaadittu ehto saa muodon

$$x\phi(y) \neq y\phi(x) \text{ kaikilla } x \neq y, \tag{3.5}$$

mikä tunnetaan yleisesti seuraavalla nimellä.

Määritelmä 3.3. *Ryhmän G permutaatiota ϕ sanotaan antisymmetriseksi kuvaukseksi, jos kaikilla $x, y \in G$ yhtälöstä $x\phi(y) = y\phi(x)$ seuraa, että $x = y$. Toisin sanottuna, jos $x \neq y$, niin $x\phi(y) \neq y\phi(x)$.*

Tämä ominaisuus perustelee aiempaa valintaa asettaa $\delta_i = \delta^i$, sillä tällöin $\phi(\cdot) = \delta_{k+1}\delta_k^{-1}(\cdot) = \delta^{k+1}\delta^{-k}(\cdot) = \delta(\cdot)$. Siten parin (G, δ) muodostama tarkistusmerkkijärjestelmä tunnistaa kaikki vaihtovirheet täsmälleen silloin kun permutaatio δ on antisymmetrinen kuvaus. Koska vaihtovirheet muodostavat toiseksi yleisimmän virheluokan, on antisymmetrisillä kuvauksilla erittäin tärkeä rooli tarkistusmerkkijärjestelmiä kehitettäessä. Antisymmetristen kuvausten olemassaoloa käsitellään luvussa 5.

Jos ryhmä G on kommutatiivinen, niin yhtälö 3.5 on yhtäpitävä muodon $x\big(\phi(x)\big)^{-1} \neq y\big(\phi(y)\big)^{-1}$ kanssa, mistä voidaan päätellä, että Abelin ryhmässä kuvaus ϕ havaitsee kaikki vaihtovirheet jos ja vain jos kuvaus $inv \circ \phi$, missä $inv(x) := x^{-1}$, on täydellinen kuvaus.

Hyppyvaihtovirhe eroaa vaihtovirheestä siten, että kahden paikkaa vaihtaneen merkin välissä on yksi paikallaan oleva merkki. Menettelemällä samoin kuin edellä, nähdään että hyppyvaihtovirhe havaitaan täsmälleen silloin kun

$$\delta_k(a)\delta_{k+1}(c)\delta_{k+2}(b) \neq \delta_k(b)\delta_{k+1}(c)\delta_{k+2}(a),$$

jolloin merkitsemällä $x := \delta_k(a), y := \delta_k(b)$ ja $z := \delta_{k+1}(c)$, saadaan tätä ehtoa hieman sievennettyä muotoon

$$xz\delta_{k+2}\big(\delta_k^{-1}(y)\big) \neq yz\delta_{k+2}\big(\delta_k^{-1}(x)\big).$$

Tästä on vaikea sanoa enempää tietämättä mitään permutaatioista δ_i. Jos tarkistusmerkkijärjestelmä on muodostettu käyttäen vain yhtä permutaatiota δ, niin päädytään ehtoon

$$xz\delta^2(y) \neq yz\delta^2(x) \text{ kaikilla } x, y, z \in G, \text{ joilla } x \neq y. \tag{3.6}$$

Yhteenvetona voidaan todeta seuraavaa. Ryhmän G tarkistusmerkkijärjestelmä $(G(X, \cdot), \delta)$ tunnistaa kaikki yksittäisvirheet sekä kohdissa 3.3.1 ja 3.3.2 esitetut virheet jos ja vain jos:

1. Permutaatio δ on sekä antisymmetrinen että täydellinen kuvaus.
2. $\forall\, x, y \in G : xz\delta^2(y) \neq yz\delta^2(x)$.
3. $\forall\, x, y \in G : xz\delta^2(x) \neq yz\delta^2(y)$.

Jos ryhmä G on Abelin ryhmä, niin lausekkeissa esiintyvä kerroin z voidaan pudottaa pois, jolloin edellä olevat ehdot saavat yksinkertaisemman muodon:

1. Permutaatio δ on sekä antisymmetrinen että täydellinen kuvaus.
2. Permutaatio δ^2 on sekä antisymmetrinen että täydellinen kuvaus.

Foneettiset virheet. Jos ryhmän alkiot samaistetaan lukujen $0-9$ kanssa, niin useissa kielissä, kuten englannissa ja saksassa, lukujen $12-19$ ääneen lausuminen muistuttaa läheisesti lukujen $20, 30, \ldots, 90$ äänneasua. Joillekin ihmisille luonteva tapa on luetella lukuja pareissa, jolloin sanelun perusteella näppäiltäessä saattaa syntyä *foneettinen virhe* $1a \leftrightarrow a0$. Olkoon $g_0 \sim 0, g_1 \sim 1, \ldots, g_9 \sim 9$. Tarkistusmerkkijärjestelmä havaitsee foneettisen virheen jos ja vain jos kaikilla $k \in \{1, \ldots, n-1\}$ ja kaikilla $i \in \{g_2, g_3, \ldots, g_9\}$ on voimassa ehto

$$\delta^k(g_i) \cdot \delta^{k+1}(g_0) \quad \neq \quad \delta^k(g_1) \cdot \delta^{k+1}(g_i).$$

Tämä ehto on edellisiin verrattuna hankalampi, sillä nyt virheentunnistus riippuu myös kokonaisluvusta k eli positiosta syötemerkkijonossa, jossa virhe tapahtuu. Kuitenkin, jos permutaatio δ on automorfismi (ja siten siis isomorfismi), niin tätä ehtoa voidaan käsitellä seuraavasti

$$\begin{aligned} \delta^k(g_i) \cdot \delta^k\big(\delta(g_0)\big) &\neq \delta^k(g_1) \cdot \delta^k\big(\delta(g_i)\big) \Leftrightarrow \\ \delta^k\big(g_i\delta(g_0)\big) &\neq \delta^k\big(g_1\delta(g_i)\big) \Leftrightarrow \\ g_i\delta(g_0) &\neq g_1\delta(g_i) \ \forall\ i \in \{2, 3, \ldots, 9\}. \end{aligned}$$

Jos G on abeliaaninen, niin tämä ehto saa seuraavan muodon:

$$\begin{aligned} g_i\delta(g_0) &\neq g_1\delta(g_i) \Leftrightarrow \\ g_i\big(\delta(g_i)\big)^{-1} &\neq g_1\big(\delta(g_0)\big)^{-1}. \end{aligned}$$

Tämä ehto pätee kahdeksalla eri indeksin i arvolla, joten yhtälön vasen puoli käy läpi korkeintaan kahdeksan eri ryhmän G alkiota. Valittaessa numeroiden $0, \ldots, 9$ edustajia ryhmässä G, yhtälön oikean puolen alkiot g_0 ja g_1 voidaan valita $10 \cdot 9 > 8$ eri tavalla. Siispä foneettisilta virheiltä voidaan aina suojautua, kunhan vain saneltavan merkkijonon luvut $0, \ldots, 9$ koodataan alkioiksi $g_0, \ldots, g_9$ siten, että ylläoleva ehto täyttyy. Näin ollen foneettisia virheitä voidaan käsitellä lähinnä esitystapaongelmana. Toisaalta, ei ole selvää, onko tällainen menettely aina järkevää. Esimerkiksi ryhmässä $\mathbb{Z}_{10}$ laskettaessa on luonnollisinta valita saneltavan numeron i edustajaksi alkio $\bar{i} \in \mathbb{Z}_{10}$ ja mikä tahansa muu vaihtoehtoinen koodaus lisää käytettävän järjestelmän monimutkaisuutta.

Luku 4

Täydelliset kuvaukset

Edellisen luvun tarkastelut motivoivat antisymmetristen ja täydellisten kuvausten etsimiseen. Vain pieni osa ryhmien kaikista permutaatioista täyttävät nämä vaatimukset ja joillakin ryhmillä ei ole olemassa yhtäkään täydellistä kuvausta. Tässä kappaleessa esitellään täydellisiä kuvauksia koskevia olemassaolotuloksia, joita voidaan soveltaa myöhemmin konstruoitaessa erilaisia tarkistusmerkkijärjestelmiä.

Tietyistä ryhmistä löydetään täydellisiä kuvauksia helposti.

Lemma 4.1. *Jos G on Abelin ryhmä ja $n \in \mathbb{Z}_+$ sellainen luku, että $n \perp |G|$ ja $n+1 \perp |G|$, niin permutaatio $\phi(x) = x^n$ on täydellinen kuvaus.*

Todistus. Näytetään, että lauseke $x\phi(x)$ on bijektiivinen. Jos x ja y ovat sellaisia ryhmän G alkioita, joille $x\phi(x) = y\phi(y)$, niin

$$\begin{aligned} x\phi(x) &= y\phi(y) \Leftrightarrow \\ x^{n+1} &= y^{n+1} \Leftrightarrow \\ (xy^{-1})^{n+1} &= e, \end{aligned}$$

mistä seuraa, että luku $n+1$ on jaollinen luvulla $|xy^{-1}|$. Lagrangen lauseen nojalla ryhmän G kertaluku $|G|$ on myös jaollinen luvulla $|xy^{-1}|$, mutta koska $n+1 \perp |G|$, niin $|xy^{-1}| = 1$, eli $x = y$. Siten permutaatio ϕ on täydellinen kuvaus.

□

Edellä nähtiin, että transpositiovirheiden havaitseminen vaatii antisymmetrisen kuvauksen. Abelin ryhmissä täydellisten kuvausten ja antisymmetristen kuvausten olemassaolon yhdistää seuraava lemma, jonka esittivät J. A. Gallian ja M. D. Mullin [20].

Lemma 4.2. *Abelin ryhmällä on olemassa antisymmetrinen kuvaus jos ja vain jos sillä on olemassa täydellinen kuvaus.*

Todistus. Abelin ryhmässä identiteetti $\phi(x)y = \phi(y)x$ on yhtäpitävä muodon $\big(\phi(x)\big)^{-1}x = \big(\phi(y)\big)^{-1}y$ kanssa. Merkitään $\psi := (\cdot)^{-1} \circ \phi$, jolloin edelläoleva ehto voidaan kirjoittaa muodossa $\psi(x)x = \psi(y)y$. Tällöin nähdään, että kuvaus ϕ on antisymmetrinen täsmälleen silloin, kun kuvaus ψ on täydellinen kuvaus.

Jos ryhmällä ei ole olemassa yhtään täydellistä kuvausta ψ, niin sillä ei voi siis myöskään olla olemassa yhtään antisymmetristä kuvausta ϕ ja päinvastoin. □

Huomaa, että lauseessa käsitellyt antisymmetrinen ja täydellinen kuvaus voivat olla eri kuvauksia. Vaikka kuvaus voi olla samalla sekä antisymmetrinen että myös täydellinen, niin näin ei välttämättä tarvitse olla.

4.1 Olemassaolokriteeri Abelin ryhmissä

Tässä kappaleessa esitellään karakterisaatio täydellisten kuvausten olemassaololle Abelin ryhmissä. Seuraavaksi esiteltävät tulokset ovat peräisin L.J. Paigen artikkelista A Note on Finite Abelian Groups [21].

Olkoon G kertalukua n oleva Abelin ryhmä. Jos θ on jokin ryhmän G permutaatio, niin tarkastellaan tästä johdettua kuvausta $\eta(x) := x\theta(x)$. Mitataan kuvauksen η bijektiivisyyttä funktiolla $O(\eta) := |\{\eta(x) : x \in G\}|$. Tällöin jos $O(\eta) = |G|$, niin kuvaus η on bijektio ja sitä vastaava permutaatio θ on täydellinen kuvaus. Jatkossa seuraava käsite osoittautuu hyödylliseksi.

Määritelmä 4.3. *Olkoon G ryhmä, jossa on n alkiota ja olkoon θ tämän ryhmän permutaatio, jolle $O(\eta) \geq n-1$. Tällöin sanotaan, että kuvaus θ on* ***melkein täydellinen kuvaus****.*

Merkitään symbolilla $p(G)$ ryhmän G kaikkien alkioiden tuloa. Tästä tulosta voidaan sanoa seuraavaa.

Lemma 4.4. *Tulo $p(G) = e$ silloin, kun ryhmässä G ei ole olemassa yhtään kertalukua kaksi olevaa alkiota, tai jos niitä on olemassa enemmän kuin yksi. Muulloin tulo $p(G)$ saa arvokseen tämän yksikäsitteisen kertalukua kaksi olevan alkion.*

Todistus. Olkoon $H \subseteq G$ joukko, joka koostuu identiteetistä ja kaikista ryhmän G kertalukua kaksi olevista alkioista. Tällöin joukko H on ryhmä, sillä $(ab)^2 = a^2b^2 = e \in H$ aina, kun $a, b \in H$.

Lasketaan seuraavaksi tulon $p(G)$ arvo. Olkoon a mielivaltainen joukon $G \setminus H$ alkio. Tällöin $a \neq a^{-1}$, joten sekä a että a^{-1} esiintyvät erikseen tulossa $p(G)$. Siten koska $aa^{-1} = e$, niin $p(G) = p(H)$.

Jos jokin alkuluku $p > 2$ jakaisi ryhmän H kertaluvun, niin H sisältäisi ei-triviaalin Sylowin p-aliryhmän eli ainakin yhden alkion, jonka kertaluku on alkuluvun p monikerta. Tämä ei ole mahdollista, joten $|H| = 2^n, n \geq 0$.

Jos $n = 0$, niin ryhmä H on triviaali ja $p(G) = e$. Jos taas $H = \{e, h\}$, niin $p(G) = h$. Oletetaan siis, että $|H| = 2^k$ jollakin $k \geq 2$. Tällöin ryhmän H generoivat täsmälleen k alkiota $h_1, \ldots, h_k$ ja $h_i h_j \neq e$ kaikilla $i \neq j$. Jokainen alkio $h \in H$ voidaan esittää muodossa $h = h_1^{n_1} h_2^{n_2} \ldots h_k^{n_k}$, missä $n_i \in \{0, 1\}$. Siten $p(H) = \prod h_1^{n_1} h_2^{n_2} \ldots h_k^{n_k}$, missä monikko $(n_1, \ldots, n_k)$ käy läpi kaikki kombinaatiot joukosta $\{0, 1\}^k$. Näistä täsmälleen puolessa jokainen n_i saa arvon 1, jolloin

$$p(H) = \prod h_1^{n_1} h_2^{n_2} \ldots h_k^{n_k} = (h_1 h_2 \ldots h_k)^{2^{k-1}} = e,$$

sillä $k \geq 2$. □

Seuraava tulos näyttää, että ehto $p(G) = e$ on välttämätön sille, että ryhmällä on olemassa täydellinen kuvaus.

Lemma 4.5. *Oletetaan, että Abelin ryhmällä G on olemassa täydellinen kuvaus θ. Tällöin $p(G) = e$.*

Todistus. Koska kuvaus θ on täydellinen kuvaus, niin lauseke $x\theta(x)$ on bijektio. Tällöin se käy läpi kaikki ryhmän G alkiot, kun x käy läpi kaikki ryhmän G alkiot. Kertomalla nämä kaikki keskenään saadaan

$$p(G) = \prod_{x \in G} x\theta(x) = \prod_{x \in G} x \prod_{x \in G} \theta(x) = p(G)^2,$$

mistä seuraa, että $p(G) = e$.

□

Siten jos $p(G) \neq e$, niin ryhmällä G ei ole olemassa täydellistä kuvausta, eli $O(\eta) < |G|$ kaikilla ryhmän G kuvauksilla θ.

Tämän kappaleen lopussa todistetaan, että ehto $p(G) = e$ on myöskin riittävä ehto täydellisen kuvauksen olemassaololle.

Seuraava aputulos osoittautuu hyödylliseksi myös kehitettäessä käytännöllistä algoritmia täydellisten kuvausten konstruointiin. Tämä ehkä hieman tekninen lemma kertoo, että kaikissa Abelin ryhmissä on olemassa melkein täydellisiä kuvauksia.

Lemma 4.6. *Olkoon G Abelin ryhmä. Jos θ on tämän ryhmän permutaatio, jolle $O(\eta) \leq n-2$, niin on olemassa ryhmän G permutaatio θ', jolle $O(\eta') > O(\eta)$.*

Todistus. Olkoon θ sellainen kuvaus, jolle $O(\eta) \leq n-2$. Olkoot $x_1, \ldots, x_r$ ne ryhmän G alkiot, joilla η saavuttaa erilliset arvonsa. Merkitään jäljellejääviä ryhmän G alkioita symboleilla $x_{r+1}, \ldots, x_n$.

Jos joillakin indekseillä $h, k > r$ on voimassa $x_h\theta(x_k) \neq x_i\theta(x_i) \forall\ i \leq r$, niin muodostetaan uusi kuvaus θ', jolle $\theta'(x_h) = \theta(x_k)$, $\theta'(x_k) = \theta(x_h)$

ja $\theta'(x_i) = \theta(x_i)$ kaikilla muilla indeksin i arvoilla. Tämä uusi kuvaus on permutaatio, jolle pätee $O(\eta') > O(\eta)$.

Muulloin jokaista $h, k > r$ kohti on olemassa jokin $i \leq r$, jolle $x_h\theta(x_k) = x_i\theta(x_i)$. Voidaan olettaa, että $x_{r+1}\theta(x_{r+1}) = x_1\theta(x_1)$. Jos

$$x_1\theta(x_{r+2}) \neq x_i\theta(x_i) \ \forall \ i \leq r,$$

niin muodostetaan uusi permutaatio θ' valitsemalla

$$\theta'(x_1) = \theta(x_{r+2}), \theta'(x_{r+2}) = \theta(x_1) \text{ ja } \theta'(x_i) = \theta(x_i) \text{ muulloin.}$$

Tälle permutaatiolle pätee myös $O(\eta') > O(\eta)$.

On siis oletettava, että $x_1\theta(x_{r+2}) = x_i\theta(x_i)$ jollakin indeksin $i \leq r$ arvolla, mutta indeksi 1 ei ole mahdollinen, koska muulloin olisi $\theta(x_{r+2}) = \theta(x_1)$ eli θ ei olisi edes permutaatio. Voidaan olettaa, että ristiriita tapahtuu arvolla $i = 2$. Tällöin siis $x_1\theta(x_{r+2}) = x_2\theta(x_2)$. Jos nyt $x_2\theta(x_1) \neq x_i\theta(x_i) \forall \ i \leq r$, niin tehdään valinta $\theta'(x_1) = \theta(x_{r+2}), \theta'(x_2) = \theta(x_1), \theta'(x_{r+2}) = \theta(x_2)$ ja $\theta'(x_i) = \theta(x_i)$ kaikilla muilla indeksin i arvoilla, jolloin kuvaukselle θ' pätee jälleen $O(\eta') > O(\eta)$. Siis pitää olettaa, että $x_2\theta(x_1) = x_i\theta(x_i)$ jollakin $i \leq r$.

Ei ole mahdollista, että $x_2\theta(x_1) = x_1\theta(x_1)$, tai että $x_2\theta(x_1) = x_2\theta(x_2)$, joten konfliktin on tapahduttava arvolla $3 \leq i \leq r$. Voidaan olettaa, että se tapahtuu arvolla $i = 3$. Tällöin $x_2\theta(x_1) = x_3\theta(x_3)$. Samoin kuten edellä, jos $x_3\theta(x_2) \neq x_i\theta(x_i) \forall \ i \leq r$, niin muodostetaan uusi permutaatio θ' valitsemalla $\theta'(x_1) = \theta(x_{r+2}), \theta'(x_2) = \theta(x_1), \theta'(x_3) = \theta(x_2), \theta'(x_{r+2}) = \theta(x_3)$ ja $\theta'(x_i) = \theta(x_i)$ kaikilla muilla indeksin i arvoilla. Siis on oletettava jälleen, että $x_3\theta(x_2) = x_i\theta(x_i)$ jollakin $i \leq r$. Tapaukset $x_3\theta(x_2) = x_3\theta(x_3)$ tai $x_3\theta(x_2) = x_2\theta(x_2)$ eivät ole mahdollisia. Lisäksi, $x_3\theta(x_2) = x_1\theta(x_1)$ ei ole myöskään mahdollinen, sillä tällöin $\eta(x_1)\theta(x_3) = x_3\theta(x_2)\theta(x_3) = \eta(x_3)\theta(x_2) = x_2\theta(x_1)\theta(x_2) = \theta(x_1)\eta(x_2) = x_1\theta(x_{r+2})\theta(x_1) = \theta(x_{r+2})\eta(x_1)$, josta saataisiin $\theta(x_3) = \theta(x_{r+2})$, mikä on mahdotonta. Siten $x_3\theta(x_2) = x_i\theta(x_i)$ jollakin $4 \leq i \leq r$ ja voidaan olettaa, että se tapahtuu arvolla $i = 4$.

Näin jatketaan askel kerrallaan ja saavutaan tilanteeseen, jossa seuraavat yhtälöt ovat voimassa johonkin indeksiin $k \leq r - 2$ saakka:

$$x_1\theta(x_{r+2}) = \eta(x_2), x_{i+1}\theta(x_i) = \eta(x_{i+2}), i = 1, \ldots, k.$$

Sillä jos jossain vaiheessa $x_{i+1}\theta(x_i) \neq \eta(x_j) \ \forall \ j \leq r$, niin valitaan uusi permutaatio menetellen kuten yllä, kunnes tämä ei enää toistu.

Näytetään, että tämä prosessi loppuu väistämättä jollakin askeleella. Yllaolevista yhtälöistä voidaan laskea seuraavat identiteetit:

$$\begin{aligned} \eta(x_1)\theta(x_{r+2}) &= x_1\theta(x_1)\theta(x_{r+2}) \\ = \eta(x_2)\theta(x_1) &= x_2\theta(x_2)\theta(x_1) \\ = \eta(x_3)\theta(x_2) &= \ldots, \end{aligned}$$

josta voidaan tehdä seuraava johtopäätös:

$$\eta(x_1)\theta(x_{r+2}) = \eta(x_{i+1})\theta(x_i),\ i = 1, 2, \ldots, k+1.$$

Nyt askeleella k todetaan jälleen, että $x_{k+1}\theta(x_k) \neq \eta(x_i)$ millään $i \leq k+1$, sillä jos $x_{k+1}\theta(x_k) = \eta(x_i)$ jollakin $i \leq k+1$, niin tällöin saadaan

$$\eta(x_i)\theta(x_{k+2}) = x_{k+2}\theta(x_{k+1})\theta(x_{k+2}) = \eta(x_{k+2})\theta(x_{k+1}) = \eta(x_i)\theta(x_{i-1}).$$

Tämä tarkoittaisi, että $\theta(x_{k+2}) = \theta(x_{i-1})$, mikä on ristiriita, sillä θ on permutaationa bijektiivinen. Siten jokaisella askeleella laskettavalle uudelle tulolle pätee $x_{k+1}\theta(x_k) = \eta(x_i)$ jollakin $k+2 \leq i \leq r$, joten jokaisella askeleella uusi tuotettu arvo $x_{i+1}\theta(x_i)$ eroaa kaikista edellä tuotetuista.

Viimeisellä mahdollisella askeleella lasketaan tulo $x_r\theta(x_{r-1})$, joka on erisuuri alkioiden $x_{r+1}\theta(x_{r+1}) = x_1\theta(x_1)$, $x_1\theta(x_{r+2})$, $x_2\theta(x_1)$, $x_3\theta(x_2)$, …, $x_{r-1}\theta(x_{r-2})$ kanssa. Näitä on täsmälleen r kappaletta, joten valitsemalla $\theta'(x_1) = \theta(x_{r+2})$, $\theta'(x_2) = \theta(x_1)$, $\theta'(x_3) = \theta(x_2)$, …, $\theta'(x_{r-1}) = \theta(x_{r-2})$, $\theta'(x_r) = \theta(x_{r-1})$, $\theta'(x_{r+2} = \theta(x_r)$ saadaan kuvaus θ', jolle $O(\eta') > O(\eta)$. □

Aloittamalla mielivaltaisesta permutaatiosta voidaan lemmaa 4.6 soveltaa toistuvasti, jolloin viimein päädytään melkein täydelliseen kuvaukseen. Lopullinen tulos saavutetaan todistamalla, että Abelin ryhmissä, joissa ehto $p(G) = e$ on voimassa, melkein täydelliset kuvaukset ovatkin aina itse asiassa täydellisiä kuvauksia.

Lemma 4.7. *Olkoon G Abelin ryhmä, jossa $p(G) = e$. Jos θ on tämän ryhmän permutaatio, jolle $O(\eta) \geq n-1$, niin itse asiassa $O(\eta) = n$ eli kuvaus θ on täydellinen kuvaus.*

Seuraus 4.8. *Jos Abelin ryhmässä G on voimassa ehto $p(G) = e$, niin tässä ryhmässä on olemassa täydellinen kuvaus..*

Todistus. Lemman oletusten nojalla kuvaus η saa $n-1$ erillistä arvoa, joten olkoot $x_1, \ldots, x_{n-1}$ ne ryhmän G alkiot, joilla kuvaus η saa nämä erilliset arvonsa. Olkoon alkio z se ryhmän G alkio, joka jää saavuttamatta, eli $z = G \setminus \{\eta(x_1), \ldots, \eta(x_{n-1})\}$. Muokataan identiteettiä

$$\prod_{i=1}^{n-1}[x_i\theta(x_i)] = \prod_{i=1}^{n-1}\eta(x_i)$$

lisäämällä puolittain vasemman puolen tulosta puuttuva viimeinen alkio $x_n\theta(x_n) = \eta(x_n)$ sekä oikean puolen tulosta puuttuva alkio z, jolloin saadaan

$$\begin{aligned} z\prod_{i=1}^{n}[x_i\theta(x_i)] &= x_n\theta(x_n)z\prod_{i=1}^{n-1}\eta(x_i) \\ zp(G)^2 &= \eta(x_n)p(G), \end{aligned}$$

mutta koska $p(G) = e$, niin nähdään, että $\eta(x_n) = z$, eli $O(\eta) = n$ ja kuvaus θ on täydellinen kuvaus.

Seuraus 4.8 saadaan yhdistämällä lemmat 4.6 ja 4.7. □

Lemma 4.5 ja edellinen seurauslause 4.8 määrittelevät täsmällisesti Abelin ryhmien tapauksen. Muistaen myös lemman 4.2, ehto $p(G) = e$ voidaan muotoilla Sylowin käsitteiden muodossa seuraavasti.

Lause 4.9. *Abelin ryhmällä on olemassa täydellinen kuvaus ja siten myös antisymmetrinen kuvaus jos ja vain jos sen Sylowin 2-aliryhmä on triviaali tai ei-syklinen.*

Todistus. Lemman 4.4 mukaan ryhmälle G on voimassa $p(G) = e$ täsmälleen silloin, kun sen Sylowin 2-aliryhmä on triviaali tai ei-syklinen. Väite seuraa tuloksista 4.5 ja 4.8. □

Sovellusten kannalta tämän tuloksen perusteella voidaan heti sulkea pois tarkasteluista tietyt Abelin ryhmät, sillä niissä ei voida konstruoida tehokasta tarkistusmerkkijärjestelmää. Esimerkiksi seuraavanlaiset ryhmät eivät ole kelvollisia.

Seuraus 4.10. *Sykliseen ryhmään C_{2n} pohjautuva tarkistusmerkkijärjestelmä, jossa tarkistusmerkki lasketaan käyttäen yhtälöä* 3.3*, ei voi havaita kaikkia transpositiovirheitä.*

Todistus. Ryhmän C_{2n} Sylowin 2-aliryhmä on syklinen ja ei-triviaali, joten lauseen 4.9 mukaan se ei sisällä yhtään täydellistä ja siten myös antisymmetristä kuvausta. Antisymmetrisen kuvauksen olemassaolo on välttämätöntä transpositiovirheiden havaitsemiseksi, joten ryhmään C_{2n} pohjautuva tarkistusmerkkijärjestelmä ei voi havaita kaikkia transpositiovirheitä. □

Edellinen havainto osoittaa myös tapauksen $\mathbb{Z}_{10}$. Aina voidaan kuitenkin konstruoida melkein täydellinen kuvaus, joka havainnoi kaikki vaihtovirheet yhtä merkkiparia lukuunottamatta. Mainittakoon, että vaihtoehtoisesti on mahdollista rakentaa tässä ryhmässä kuvaus, joka havaitsee kaikki vaihtovirheet, mutta tällöin se ei kykene tunnistamaan kaikkia yksittäisvirheitä, sillä tämä kuvaus ei ole bijektio. Esimerkki tällaisesta konstruktiosta löytyy A. Eckerin ja G. Pochin artikkelista [18, p.294].

Ryhmän $\mathbb{Z}_{10}$ soveltaminen olisi erittäin käytännöllistä, koska numeroiden $0 - 9$ upottaminen tähän ryhmään on luonnollista. Myöhemmin tullaan käsittelemään kahta eri lähestymistapaa ohittaa ryhmän $\mathbb{Z}_{10}$ ongelmat. Yksi tapa on siirtyä käyttämään isompaa kertalukua olevaa ryhmää, kuten ISBN-10 -järjestelmän tapauksessa tehdään. Toinen vaihtoehto on soveltaa kertalukua kymmenen olevaa dihedraalista ryhmää D_5, joka on ei-kommutatiivinen ryhmä. Tämän ryhmän tapausta käsitellään seuraavassa kappaleessa.

4.2 Ei-kommutatiiviset ryhmät

Edellisen kappaleen pohjalta tiedetään täsmälleen milloin abeliaaninen ryhmä sisältää täydellisen kuvauksen. Tilanne on selvästi vaikeampi ei-kommutatiivisten ryhmien osalta, mikä on tuottanut viimeisten kymmenien vuosien aikana useita julkaisuja, joissa täydellisten kuvausten olemassaoloa tarkastellaan tapauskohtaisesti ryhmä kerrallaan. Tätä aihetta käsitellään laajemmin kappaleessa 4.4.

Yleisestä tapauksesta tunnetaan seuraavat kaksi aritmeettista tulosta. Ensimmäiseen näistä antavat todistuksen A. Ecker ja G. Poch [18].

Lemma 4.11. *Jos G on paritonta kertalukua oleva ryhmä, niin kuvaus $\theta(x) = x$ on täydellinen kuvaus.*

Todistus. Ryhmän G kertaluku on muotoa $|G| = 2n+1$ jollain $n \geq 0$. Kuvaus θ on täydellinen silloin, kun kuvaus $\eta(x) = x\theta(x) = x^2$ on bijektio ryhmässä G. Jos x ja y ovat ryhmän G alkioita, joille $x\theta(x) = y\theta(y)$ eli $x^2 = y^2$, niin tällöin

$$x = x^{2n+2} = (x^2)^{n+1} = (y^2)^{n+1} = y^{2n+2} = y,$$

joten kuvaus η on bijektio ja θ täydellinen kuvaus ryhmässä G. □

Myöhempää lausetta varten osoitetaan ensin seuraava aputulos.

Lemma 4.12. *Olkoon G kertalukua $2m$ oleva ryhmä, missä $m \in \mathbb{Z}_+$ on pariton kokonaisluku. Tällöin on olemassa kertalukua m oleva normaali aliryhmä $N \lhd G$.*

Todistus. Jos ryhmän G kertaluku on muotoa $2m$, missä m on pariton positiivinen kokonaisluku, niin ryhmän G Sylowin 2-aliryhmä S on muotoa $S = \{e, t\}$, missä alkio t on kertalukua kaksi. Tällöin saadaan ryhmän G permutaatioesitys kuvaamalla alkio $g \in G$ alkioksi $\sigma_g \in S_{2m}$, missä $\sigma_g(x) = gx$, kun $x \in G$.

Nyt funktio $f : g \mapsto \sigma_g$ on homomorfismi [5, lause 3.4]. Tämän homomorfismin ydin on triviaali, sillä vain $e \mapsto id$, joten $G \cong f(G)$. Permutaatio σ_t kuvaa alkion $x \in G$ alkiolle tx ja koska $tx \neq x \ \forall \ x \in G$, niin kuvaus σ_t siirtää jokaista ryhmän G alkiota, joita on $2m$ kappaletta. Lisäksi koska $\sigma_t^2(x) = \sigma_t(tx) = t^2x = x$, niin permutaatio σ_t koostuu m kappaleesta erillisiä transpooseja, joten se on pariton permutaatio.

Ryhmän G alkiot voidaan esittää osituksena

$$G = \{g_1, tg_1\} \cup \{g_2, tg_2\} \cup \ldots \cup \{g_m, tg_m\},$$

missä nämä joukot ovat pareittain erillisiä. Koska permutaatio σ_t on pariton permutaatio, niin täsmälleen toinen alkioista $f(g_i) = \sigma_{g_i}$ ja $f(tg_i) = \sigma_{tg_i}$ on pariton permutaatio. Tällöin nähdään, että ryhmä $f(G)$ sisältää täsmälleen m kappaletta parittomia sekä parillisia permutaatioita, joten $H := f(G) \cap$

A_{2m} muodostaa kertalukua m olevan aliryhmän ryhmässä S_{2m}. Kuvaus f on isomorfismi $G \to S_{2m}$, joten joukko $N := f^{-1}(H)$ muodostaa ryhmän G aliryhmän. Koska $|N| = m$, niin $[G : N] = 2$, joten $N \lhd G$. □

Seuraava tärkeä tulos on H.B. Mannin merkittävästä latinalaisia neliöitä käsittelevästä artikkelista [22]. Itse asiassa tämä oli ensimmäinen artikkeli, joka määritteli täydellisen kuvauksen.

Lause 4.13. *Ryhmällä, jonka kertaluku on $4k + 2, k \in \mathbb{Z}_+$, ei ole olemassa täydellistä kuvausta.*

Todistus. Olkoon G ryhmä, jolle $|G| = 4k+2 = 2(2k+1) = 2m$, missä m on jokin pariton kokonaisluku. Tällöin edellisen lemman 4.12 nojalla ryhmällä G on olemassa kertalukua m oleva normaali aliryhmä H. Merkitään tämän aliryhmän ainoaa sivuluokkaa symbolilla H'. Nyt $H \cap H' = \emptyset$ ja $G = H \cup H'$. Tämän sivuluokan generoi jokin kertalukua kaksi oleva alkio $g \in G \setminus H$, eli $H = \{h_1, \ldots, h_m\}$ ja $H' = \{gh_1, \ldots, gh_m\}$, missä $|g| = 2$. Todistetaan lause ristiriidan kautta eli oletetaan, että ryhmällä G on olemassa täydellinen kuvaus θ ja näytetään, että tämä on mahdotonta.

Jos $a, b \in H'$, niin $a = gh_i, b = gh_j$ joillakin $h_i, h_j \in H$. Tällöin $ab = gh_igh_j = g^2h_i'h_j = h_i'h_j \in H$, missä h_i' on jokin aliryhmän H alkio. Siten tarkastellessa tuloa $x\theta(x)$ ryhmän G alkiot jakautuvat neljään ryhmään:

1. a kappaletta alkioita $x \in H$, joille $\theta(x) \in H$. Tällöin $x\theta(x) \in H$.
2. b kappaletta alkioita $x \in H$, joille $\theta(x) \in H'$. Tällöin $x\theta(x) \in H'$.
3. c kappaletta alkioita $x \in H'$, joille $\theta(x) \in H$. Tällöin $x\theta(x) \in H'$.
4. Loput alkiot, joille $x \in H'$ ja $\theta(x) \in H'$. Tällöin $x\theta(x) \in H$, kuten edellä laskettiin.

Koska $|H| = m$, niin $a+b = m$ ja $a+c = m$. Samoin koska $|H'| = m$, niin $b+c = m$. Siispä $a = b$ ja $m = 2a$, mikä on ristiriita, sillä luku m oli pariton! Siten kertalukua $4k + 2$ olevista ryhmistä ei löydy täydellistä kuvausta. □

Seuraavan tuloksen osoitti P.T. Bateman vuonna 1950 [23] ja se mainittakoon täydellisyyden vuoksi, vaikka sillä tuskin on sovellusta tarkistusmerkkijärjestelmien yhteydessä.

Lause 4.14. *Kaikilla äärettömillä ryhmillä on olemassa täydellisiä kuvauksia.*

□

Näiden tulosten perusteella kaikilla paritonta kertalukua olevilla ryhmillä on olemassa täydellisiä kuvauksia, mutta kertalukua $4k + 2$ olevilla ryhmillä niitä ei ole olemassa, mikä siis jättää vain kertalukua $4k$ olevien ryhmien tapauksen enää käsittelemättä.

Kertaluvultaan muotoa 2^n olevista ryhmistä tunnetaan seuraava tulos. Tämän lauseen todistus pohjautuu hieman työlääseen ryhmän rakenteen tapauskohtaiseen tarkasteluun, joten se sivuutetaan tässä.

Lause 4.15. *Jokaisella ei-syklisellä 2-ryhmällä on olemassa täydellinen kuvaus.*

Todistus. Todistus löytyy kohdasta Theorem 4 artikkelista M. Hall, L. J. Paige. Complete Mappings of Finite Groups. Pacific Journal of Mathematics, vol. 5 no. 4, pp. 541-549, 1955. [24]. □

Pelkästään ryhmän kertaluvun perusteella on vaikea sanoa enempää. Seuraavassa kappaleessa käsitellään erilaista lähestymistapaa ja näytetään, miten sitä sovelletaan permutaatioryhmien tapauksessa.

4.3 Laajennuslause ja sen seuraukset

Seuraava tulos on keskeinen, sillä se antaa mahdollisuuden rakentaa täydellinen kuvaus ryhmälle, jonka aliryhmällä sellainen tiedetään jo olevan, olettaen että tämän aliryhmän sivuluokkien edustajat täyttävät tietyt ehdot. Tämän kappaleen tulokset ovat osoittaneet M. Hall ja L. J. Paige [24].

Lause 4.16. ***Täydellisten kuvausten laajennuslause.*** *Olkoon G ryhmä, H sen aliryhmä ja joukko $U = \{u_1, u_2, \ldots, u_n\}$ alkoita, joille on voimassa $G = u_1H + u_2H + \ldots + u_nH = Hu_1 + Hu_2 + \ldots + Hu_n$, missä $u_iH \cap u_jH = \emptyset$ ja $Hu_i \cap Hu_j = \emptyset$ kaikilla $i \neq j$. Tällöin jos aliryhmällä H on olemassa täydellinen kuvaus, ja jos on olemassa permutaatiot σ ja τ, jotka toteuttavat ehdon*

$$u\sigma(u)H = \tau(u)H \ \forall \ u \in U,$$

niin tällöin myös ryhmällä G on olemassa täydellinen kuvaus.

Todistus. Joukkoja u_iH sanotaan aliryhmän H vasemmanpuoleiseksi sivuluokiksi ja vastaavasti joukot Hu_i ovat aliryhmän H oikeanpuoleisia sivuluokkia. Alkioita u_i sanotaan näiden sivuluokkien edustajiksi ja lauseen ehto vaatii, että samat alkiot käyvät aliryhmän H sekä vasemmanpuoleisten että oikeanpuoleisten sivuluokkien edustajina. Huomaa, että nämäositukset voivat olla täysin erilaisia eikä yhtälö $u_iH = Hu_j$ ole välttämättä voimassa millään indekseillä i ja j.

Jokainen ryhmän G alkio voidaan yksikäsitteisesti esittää muodossa $g = uh = h'u'$, missä $u, u' \in U$ ja $h, h' \in H$. Toisin sanottuna, jos $u_1, u_2 \in U$ ja $h_1, h_2 \in H$, niin

$$u_1h_1 = u_2h_2 \text{ tai } h_1u_1 = h_2u_2 \Rightarrow \begin{cases} u_1 = u_2 \\ h_1 = h_2 \end{cases}. \qquad (YK)$$

Olkoon $g \in G$ alkio, jolla on esitys muodossa $g = uh = h'u'$, missä $u, u' \in U$ ja $h, h' \in H$. Määritellään tällöin seuraavat kuvaukset $\mathcal{U} : U \times H \to U$ sekä $\mathcal{H} : U \times H \to H$ seuraavasti:

$$\mathcal{U}(u,h) = u' \quad \text{ja} \quad \mathcal{H}(u,h) = h'.$$

Kuvauksilla $\mathcal{U}$ ja $\mathcal{H}$ voidaan siirtyä alkion esityksestä vasemman sivuluokan suhteen sen esitykseen oikeanpuoleisen sivuluokan edustajan avulla. Jokaiselle ryhmän G alkiolle g on siis olemassa yksikäsitteinen esitys muodossa $g = uh = \mathcal{H}(u,h)\mathcal{U}(u,h)$.

Jos kuvauksesta $\mathcal{H}$ kiinnitetään ensimmäinen argumentti, saadaan unaarinen funktio, jolle käytetään merkintätapaa $\mathcal{H}_u$. Soveltamalla tässä alkioon u permutaatiota σ, saadaan funktio $\mathcal{H}_{\sigma(u)} : H \to H$. Todistetaan, että tämä funktio on joukon H bijektio.

Jos joillakin $u \in U$ ja $h_1, h_2 \in H$ olisi voimassa $\mathcal{H}_{\sigma(u)}(h_1) = \mathcal{H}_{\sigma(u)}(h_2)$ eli

$$\mathcal{H}\big(\sigma(u), h_1\big) = \mathcal{H}\big(\sigma(u), h_2\big),$$

niin alkioille $\sigma(u)h_1 =: h_1'u_1'$ ja $\sigma(u)h_2 =: h_2'u_2'$, missä $h_1', h_2' \in H$ ja $u_1', u_2' \in U$, se tarkoittaisi, että $h_1' = h_2'$, jolloin

$$\begin{cases} \sigma(u)h_1 = h_1'u_1' \\ \sigma(u)h_2 = h_1'u_2' \end{cases} \Leftrightarrow \begin{cases} h_1'^{-1}\sigma(u) = u_1'h_1^{-1} \\ h_1'^{-1}\sigma(u) = u_2'h_2^{-1} \end{cases} \Rightarrow u_1'h_1^{-1} = u_2'h_2^{-1},$$

josta ehdon *(YK)* nojalla $h_1^{-1} = h_2^{-1}$ eli $h_1 = h_2$. Huomaa, että tässä kohden on tärkeää, että $u_1', u_2' \in U$, koska muuten ehtoa *(YK)* ei voitaisi soveltaa.

Siten ryhmän G alkiot voidaan esittää yksikäsitteisesti myös muodossa $g = u\mathcal{H}_{\sigma(u)}(h)$, missä $h \in H$ ja $u \in U$.

Olkoon nyt kuvaus θ oletuksen nojalla olemassaoleva aliryhmän H täydellinen kuvaus. Määritellään edellisiä merkintöjä käyttäen ryhmässä G kuvaus δ seuraavasti:

$$\delta\big(u\mathcal{H}_{\sigma(u)}(h)\big) := \mathcal{U}\big(\sigma(u), h\big)\theta(h).$$

Tämä kuvaus tulee olemaan haettu ryhmän G täydellinen kuvaus, mutta todistetaan ensin, että tämä kuvaus δ on bijektiivinen. Oletetaan, että alkioille $u_1, u_2 \in U$ ja $h_1, h_2 \in H$ on voimassa

$$\mathcal{U}\big(\sigma(u_1), h_1\big)\theta(h_1) = \mathcal{U}\big(\sigma(u_2), h_2\big)\theta(h_2).$$

Tällöin ehtoa *(YK)* voidaan soveltaa, joten $\mathcal{U}\big(\sigma(u_1), h_1\big) = \mathcal{U}\big(\sigma(u_2), h_2\big)$ ja $\theta(h_1) = \theta(h_2)$. Koska kuvaus θ on permutaatio, niin $h_1 = h_2$. Ensimmäinen yhtälö saa muodon $\mathcal{U}\big(\sigma(u_1), h_1\big) = \mathcal{U}\big(\sigma(u_2), h_1\big)$, mikä tarkoittaa, että $\sigma(u_1)h_1 = h_1'u$ ja $\sigma(u_2)h_1 = h_2'u$ joillakin $h_1', h_2' \in H$ ja $u \in U$. Täten

$$\begin{cases} h_1^{-1}u = \sigma(u_1)h_1'^{-1} \\ h_1^{-1}u = \sigma(u_2)h_2'^{-1} \end{cases} \Rightarrow \sigma(u_1)h_1'^{-1} = \sigma(u_2)h_2'^{-1} \overset{\star}{\Leftrightarrow} \begin{cases} \sigma(u_1) = \sigma(u_2) \\ h_1'^{-1} = h_2'^{-1} \end{cases},$$

josta seuraa, että $u_1 = u_2$ eli kuvaus δ on bijektiivinen. Edellä kohdassa $\star$ sovelletaan jälleen ehtoa *(YK)*, mihin tarvitaan oletusta, että kuvaus σ on suljettu joukkoon U.

Käsitellään seuraavaksi kuvausta $\eta(g) := g \cdot \delta(g)$ ja näytetään, että tämä on bijektio, jolloin kuvaus δ on vaadittu täydellinen kuvaus ryhmässä G. Nyt

$$\begin{aligned} \eta\big(u\mathcal{H}_{\sigma(u)}(h)\big) &= u\mathcal{H}_{\sigma(u)}(h) \cdot \delta\big(u\mathcal{H}_{\sigma(u)}(h)\big) \\ &= u\mathcal{H}\big(\sigma(u), h\big) \cdot \mathcal{U}\big(\sigma(u), h\big)\theta(h) \\ &= u\sigma(u)h\theta(h). \end{aligned}$$

Oletetaan, että alkioille $u_1, u_2 \in U$ ja $h_1, h_2 \in H$ on voimassa

$$u_1\sigma(u_1)h_1\theta(h_1) = u_2\sigma(u_2)h_2\theta(h_2). \tag{4.1}$$

Käsittelemällä tätä yhtälöä aliryhmän H sivuluokkien joukossa saadaan

$$\begin{aligned} u_1\sigma(u_1)h_1\theta(h_1)H &= u_2\sigma(u_2)h_2\theta(h_2)H \Leftrightarrow \\ u_1\sigma(u_1)H &= u_2\sigma(u_2)H, \end{aligned}$$

mikä on permutaation σ oletetun ominaisuuden nojalla yhtäpitävää muodon $\tau(u_1)H = \tau(u_2)H$ kanssa. Kuvaus τ on bijektio ja suljettu joukossa U, joten $u_1 = u_2$ sekä $u_1\sigma(u_1) \in U$. Siten yhtälöstä 4.1 voidaan päätellä ehtoa *(YK)* käyttämällä, että $h_1\theta(h_1) = h_2\theta(h_2)$, mikä on mahdollista vain silloin, kun $h_1 = h_2$, sillä kuvaus θ on täydellinen kuvaus ryhmässä H. Tämä todistaa, että kuvaus η on bijektio ryhmässä G, jolloin kuvaus δ on haluttu ryhmän G täydellinen kuvaus.

□

Edellä esitetty laajennuslause antaa välittömästi seuraavat hyödylliset muotoilut.

Seuraus 4.17. *Olkoon G ryhmä ja N sen normaali aliryhmä. Jos ryhmällä N ja tekijäryhmällä G/N on olemassa täydelliset kuvaukset, niin myös ryhmällä G on olemassa täydellinen kuvaus.*

Todistus. Koska ryhmä N on ryhmän G normaali aliryhmä, niin $gN = Ng$ kaikilla ryhmän G alkioilla g. Siten joukon U valinta ei tuota ongelmia. Tekijäryhmän G/N täydellinen kuvaus toimii permutaation σ roolissa, joten täydellisten kuvausten laajennuslausetta voidaan soveltaa. □

Seuraus 4.18. *Olkoon ryhmä G kahden ryhmän H_1 ja H_2 karteesinen tulo eli $G = H_1 \otimes H_2$. Jos ryhmillä H_1 ja H_2 on olemassa täydelliset kuvaukset, niin myös ryhmällä G on olemassa täydellinen kuvaus.*

Todistus. Ryhmällä G on normaali aliryhmä H, joka on isomorfinen ryhmän H_1 kanssa. Tällöin tekijäryhmä G/H on isomorfinen ryhmän H_2 kanssa, jolloin edellisen seurauslauseen 4.17 soveltaminen todistaa väitteen. □

Täydellisten kuvausten laajennuslausetta voidaan myös soveltaa tietyille tulomuotoa oleville ryhmille.

Seuraus 4.19. *Olkoon G ryhmä, joka voidaan esittää muodossa $G = A \cdot B$, missä A ja B ovat ryhmän G aliryhmiä ja $A \cap B = \{e\}$. Jos aliryhmillä A ja B on olemassa täydelliset kuvaukset θ_A ja θ_B, niin myös ryhmällä G on olemassa täydellinen kuvaus.*

Todistus. Tässä tapauksessa voidaan soveltaa täydellisten kuvausten laajennuslausetta valitsemalla ryhmän A alkiot joukon U rooliin. Tämä valinta on kelvollinen, sillä jos leikkaus $a_1B \cap a_2B$ sisältää jonkin alkion $x \neq e$, niin $x = a_1b_1 = a_2b_2$ joillakin $b_1, b_2 \in B$. Tällöin $a_2^{-1}a_1 = b_2b_1^{-1}$ ja koska yhtälön vasen puoli on ryhmän A alkio ja yhtälön oikea puoli on ryhmän B alkio, niin on oltava $a_2^{-1}a_1 = e$ eli $a_1 = a_2$. Samaa päättelyä voidaan käyttää todistamaan, että joukot $Ba, a \in A$ ovat erillisiä ja muodostavat ryhmän G osituksen sivuluokkiin. Ryhmän A alkiot käyvät siis sekä vasemmanpuoleisista että oikeanpuoleisista edustajista ja laajennuslauseen kuvauksen σ rooliin voidaan valita täydellinen kuvaus θ_A. Näillä valinnoilla laajennuslausetta on mahdollista soveltaa, mikä todistaa väitteen. □

Ratkaistaan seuraavaksi symmetristen ja alternoivien ryhmien tapaukset. Triviaalisti ryhmillä S_1, A_1 ja A_2 on olemassa täydellinen kuvaus, koska nämä ovat yhden alkion ryhmiä. Ryhmällä S_2 ei ole olemassa täydellistä kuvausta lauseen 4.9 takia, sillä $S_2 \cong C_2$. Lauseen 4.13 nojalla ryhmällä S_3 ei myöskään ole olemassa täydellistä kuvausta, sillä sen kertaluku on kuusi. Lause 4.11 kertoo, että ryhmällä A_3 on olemassa täydellinen kuvaus, sillä sen kertaluku on kolme. Ryhmät S_n ja A_n, missä $n \geq 4$, käsitellään seuraavaksi.

Lemma 4.20. *Ryhmillä S_4 ja A_4 on olemassa täydelliset kuvaukset.*

Todistus. Ryhmän S_4 täydellinen kuvaus on esitetty taulukossa 4.1 ja ryhmän A_4 täydellinen kuvaus löytyy taulukosta 4.2.

□

Edellisen syvällisen päättelyn jälkeen todistetaan yleinen tapaus.

Lause 4.21. *Ryhmillä S_n, missä $n \geq 4$, on olemassa täydellisiä kuvauksia.*

Todistus. Todistus etenee induktiolla luvun n suhteen. Alkuaskel $n = 4$ todistettiin edellisessä lemmassa.

Oletetaan, että ryhmässä S_n, missä $n \geq 4$, on olemassa täydellinen kuvaus ja näytetään, että myös ryhmässä S_{n+1} on olemassa täydellinen kuvaus. Valitaan

$$U = \{e, (1, n+1), (2, n+1), \ldots, (n, n+1)\}.$$

Jos $(i, n+1)S_n \cap (j, n+1)S_n$ sisältää jonkin ei-triviaalin alkion g, niin

$$g = (i, n+1)g_1 = (j, n+1)g_2 \quad \text{joillakin} \quad g_1, g_2 \in S_n.$$

g	$\theta(g)$	$g\theta(g)$	g	$\theta(g)$	$g\theta(g)$
e	e	e	(1 3 2)	(1 4)(2 3)	(1 4 3)
(1 4)	(1 2 4)	(1 2)	(2 3)	(3 4)	(2 3 4)
(1 2 3 4)	(1 2)(3 4)	(1 3)	(3 4)	(2 3)	(2 4 3)
(1 3)	(1 4 3)	(1 4)	(1 3 2 4)	(1 3 2 4)	(1 2)(3 4)
(2 4)	(2 3 4)	(2 3)	(1 2 4)	(1 3 4)	(1 3)(2 4)
(1 2)(3 4)	(1 2 3 4)	(2 4)	(1 2 4 3)	(1 2 4 3)	(1 4)(2 3)
(2 3 4)	(2 4)	(3 4)	(1 3 4)	(1 3 4 2)	(1 4 2 3)
(1 4 2 3)	(1 4)	(1 2 3)	(1 3)(2 4)	(1 4 3 2)	(1 2 3 4)
(1 4)(2 3)	(1 3 2)	(1 2 4)	(1 2)	(2 4 3)	(1 2 4 3)
(1 2 3)	(1 2 3)	(1 3 2)	(1 4 3 2)	(1 4 2)	(1 3 2 4)
(1 4 2)	(1 3)(2 4)	(1 3 4)	(1 4 3)	(1 4 2 3)	(1 3 4 2)
(1 3 4 2)	(1 3)	(1 4 2)	(2 4 3)	(1 2)	(1 4 3 2)

Taulukko 4.1: Esimerkki symmetrisen ryhmän S_4 täydellisestä kuvauksesta θ.

g	$\theta(g)$	$g\theta(g)$	g	$\theta(g)$	$g\theta(g)$
e	e	e	(1 2)(3 4)	(1 3 2)	(1 4 3)
(1 4 2)	(1 4)(2 3)	(1 2 3)	(2 4 3)	(2 4 3)	(2 3 4)
(1 3)(2 4)	(1 4 3)	(1 2 4)	(2 3 4)	(2 3 4)	(2 4 3)
(1 4)(2 3)	(1 2 4)	(1 3 2)	(1 3 2)	(1 3 4)	(1 2)(3 4)
(1 2 3)	(1 2)(3 4)	(1 3 4)	(1 4 3)	(1 4 2)	(1 3)(2 4)
(1 3 4)	(1 3)(2 4)	(1 4 2)	(1 2 4)	(1 2 3)	(1 4)(2 3)

Taulukko 4.2: Esimerkki alternoivan ryhmän A_4 täydellisestä kuvauksesta θ.

Tällöin $g_1 g_2^{-1} = (j, n+1)(i, n+1)$ ja koska $g_1 g_2^{-1} \in G$, niin myös $(i, j, n+1) \in G$. Jos $i \neq j$, niin $(j, n+1)(i, n+1) = (i, j, n+1)$, mikä ei ole mahdollista, sillä ryhmä S_n upotettuna ryhmään S_{n+1} koostuu kaikista niistä permutaatioista, jotka kiinnittävät alkion $n+1$. Siten $i = j$, mikä osoittaa, että $(1, n+1)S_n, \ldots, (n, n+1)S_n$ on ryhmän S_{n+1} ositus eli

$$S_{n+1} = S_n + (1, n+1)S_n + (2, n+1)S_n + \ldots + (n, n+1)S_n.$$

Toistamalla ylläoleva päättely ryhmän S_n oikeanpuoleisille sivuluokille, nähdään että myös

$$S_{n+1} = S_n + S_n(1, n+1) + S_n(2, n+1) + \ldots + S_n(n, n+1)$$

on ryhmän S_{n+1} ositus. Siten joukko U täyttää täydellisten kuvausten laajennuslauseen ehdot.

Määritellään kuvaus τ kaavalla $\tau[(i+1, n+1)] = (i, n+1)$, missä $1 \leq i \leq n-1$, sekä $\tau[(1, n+1)] = (n, n+1)$ ja $\tau(e) = e$, jolloin nähdään, että

$$\begin{aligned}
\textbf{a)}\ (i+1, n+1)\tau[(i+1, n+1)]S_n &= (i+1, n+1)(i, n+1)S_n \\
&= (i, i+1, n+1)S_n \\
&= (i, n+1)(i, i+1)S_n \\
&= (i, n+1)S_n, \forall\ 1 \leq i \leq n-1, \\
\textbf{b)}\ (1, n+1)\tau[(1, n+1)]S_n &= (1, n+1)(n, n+1)S_n \\
&= (n, 1, n+1)S_n \\
&= (n, n+1)(n, 1)S_n \\
&= (n, n+1)S_n, \\
\textbf{c)}\ e\tau(e)S_n &= S_n.
\end{aligned}$$

Edellä käytettiin identiteettiä $(abc) = (ab)(bc)$ sekä ryhmäoperaation ominaisuutta $abG = aG$, kun $b \in G$. Tämä laskenta osoittaa, että kuvaus $u\tau(u)$ on bijektiivinen joukossa U eli $u\tau(u) = \sigma(u)$ jollakin joukon U permutaatiolla σ. Siten ehdot täydellisten kuvausten laajennuslauseen soveltamiseen täyttyvät, joten ryhmällä S_{n+1} on olemassa täydellinen kuvaus. Väite seuraa induktiolla. □

Alternoiville ryhmille voidaan näyttää vastaava tulos.

Lause 4.22. *Alternoivilla ryhmillä A_n, missä $n \geq 3$, on olemassa täydellisiä kuvauksia.*

Todistus. Edellä näytettiin ryhmien A_3 ja A_4 sisältävän täydellisiä kuvauksia. Osoitetaan muut tapaukset induktiolla.

Oletetaan, että ryhmällä A_n, missä $n \geq 4$, on olemassa täydellinen kuvaus. Näytetään, että myös ryhmällä A_{n+1} on olemassa täydellinen kuvaus.

Tämän todistuksen strategia on samanlainen kuin symmetristen ryhmien tapauksissa. Valitaan joukko U seuraavasti:

$$U = \{e,\ (1,n+1)(1,n)\} \cup \{(1,n)(i,n+1) : 1 \leq i \leq n-1\}.$$

Todistetaan, että tämä joukko muodostaa aliryhmän A_n edustajien järjestelmän.

Sivuluokka $eA_n = A_n$ on selvästi erillinen kaikista muista sivuluokista, sillä edustajat $(1,n+1)(1,n)$ ja $(1,n)(i,n+1), 1 \leq i \leq n-1$ eivät kuulu ryhmään A_n.

Jos $(1,n+1)(1,n)g_1 = (1,n)(i,n+1)g_2$ joillakin $g_1, g_2 \in A_n$, niin $(i,n+1)(1,n)(1,n+1)(1,n) \in A_n$. Jos $i = 1$, niin $(1,n+1)(1,n)(1,n+1)(1,n) = (1,n+1,n) \in A_n$, mikä ei ole mahdollista, sillä $(1,n+1,n)$ ei kiinnitä alkiota $n+1$. Jos $i > 1$, niin $(i,n+1)(1,n)(1,n+1)(1,n) = (n,i,n+1) \in A_n$, mikä ei ole myöskään mahdollista. Siten sivuluokka $(1,n+1)(1,n)A_n$ on myös erillinen kaikista muista sivuluokista.

Oletetaan vielä, että $(1,n)(i,n+1)g_1 = (1,n)(j,n+1)g_2$ joillakin $g_1, g_2 \in A_n$ ja $i \neq j$. Tällöin $(j,n+1)(i,n+1) = (i,j,n+1) \in A_n$, mikä ei ole mahdollista. Siten joukko U on aliryhmän A_n vasemmanpuoleisten sivuluokkien edustajien joukko.

Samalla päättelyllä voidaan todeta, että U on myös aliryhmän A_n oikeanpuoleisten sivuluokkien edustajien joukko, joten se täyttää täydellisten kuvausten laajennnuslauseen ehdot.

Määritellään kuvaus τ seuraavasti:

$$\begin{aligned}
\tau(e) &= e, \\
\tau[(1,n+1)(1,n)] &= (1,n+1)(1,n), \\
\tau[(1,n)(1,n+1)] &= (1,n)(1,n+1), \\
\tau[(1,n)(n-1,n+1)] &= (1,n)(2,n+1), \text{ sekä} \\
\tau[(1,n)(i,n+1)] &= (1,n)(i+1,n+1)\ \forall\ i = 2,\ldots,n-2.
\end{aligned}$$

Näytetään, että tämä kuvaus toteuttaa laajennuslauseessa vaaditut ehdot, eli että $\tau(U)$ on edelleen aliryhmän A_n vasemmanpuoleisten sivuluokkien edustajien joukko.

a) $e\tau(e)A_n = eA_n,$

$$\begin{aligned}
\textbf{b)}\ (1,n+1)(1,n)\tau[(1,n+1)(1,n)]A_n &= (1,n+1,n)A_n \\
&= (1,n)(1,n+1)A_n,
\end{aligned}$$

$$\begin{aligned}
\textbf{c)}\ (1,n)(1,n+1)\tau[(1,n)(1,n+1)]A_n &= (1,n,n+1)A_n \\
&= (1,n+1)(1,n)A_n,
\end{aligned}$$

d) $(1,n)(n-1,n+1)\tau[(1,n)(n-1,n+1)]A_n = (2,n-1,n+1)A_n$
$= (2,n+1)(2,n-1)A_n$
$= (1,n)(2,n+1)A_n,$

e) $(1,n)(i,n+1)\tau[(1,n)(i,n+1)]A_n = (i,n+1,i+1)A_n$
$= (i+1,n+1)(i+1,i)A_n$
$= (1,n)(i+1,n+1)A_n,$
missä $2 \leq i \leq n-2$.

Kohtien $a-e$ perusteella joukko $\tau(U)$ antaa edelleen täyden ryhmän A_n vasemmanpuoleisten sivuluokkien edustajiston, joten täydellisten kuvausten laajennuslausetta voidaan soveltaa ja siten myös ryhmällä A_{n+1} on olemassa täydellinen kuvaus. □

4.4 Yhtäpitäviä muotoiluja

Tämän luvun lopuksi keskitytään vielä tarkastelemaan seuraavia kolmea ehtoa:

- A) Ryhmällä G on olemassa täydellinen kuvaus.
- B) Ryhmällä G ei ole olemassa Sylowin 2-aliryhmiä tai ryhmän G Sylowin 2-aliryhmät eivät ole syklisiä.
- C) Ryhmän G alkiot g_i voidaan asettaa sellaiseen järjestykseen, jossa $g_1g_2\ldots g_n = e$.

Kappaleessa 4.1 näytettiin, että Abelin ryhmissä nämä kaikki kolme ehtoa tiedetään olevan yhtäpitäviä. Lisäksi lemman 4.4 ja lauseen 4.9 perusteella Abelin ryhmissä ehdot *A*-*C* ovat ekvivalentteja myös seuraavan ehdon kanssa:

- D) Ryhmässä G ei ole olemassa kertalukua kaksi olevaa alkiota tai niitä on enemmän kuin yksi. Toisin sanottuna, ryhmässä G ei ole olemassa yksikäsitteistä kertalukua 2 olevaa alkiota.

Seuraavaksi esitettävät lauseet käsittelevät ei-kommutatiivista tapausta. Näistä varhaisimman tuloksen todisti L.J. Paige vuonna 1950 [25].

Lause 4.23. *($A \Rightarrow C$). Jos ryhmällä G on olemassa täydellinen kuvaus, niin ryhmän G alkiot voidaan laittaa järjestykseen $e = g_1, g_2, \ldots, g_n$, jolle on voimassa $g_1g_2\ldots g_n = e$.*

Todistus. Olkoon θ ryhmän G täydellinen kuvaus. Jos $e\theta(e) = g \in G$, niin voidaan käsitellä sen sijaan permutaatiota $\theta'(x) := \theta(x)g^{-1}$, jolle $e\theta'(e) = e\theta(e)g^{-1} = e$, mikä on myös täydellinen kuvaus. Siten voidaan olettaa, että $\theta(e) = e$.

Tarkastellaan tuloa $g_2\theta(g_2)$. Tässä tulossa ei voi olla $\theta(g_2) = g_2^{-1}$, koska silloin $e\theta(e) = g_2\theta(g_2)$ ja θ ei olisi täydellinen kuvaus. Siten merkitään $g_3 := \theta(g_2)^{-1}$. Muodostetaan seuraavaksi tulo $g_2\theta(g_2) \cdot g_3\theta(g_3)$ ja tarkastellaan, onko tämän tulon viimeisen alkion käänteisalkiota $\theta(g_3)^{-1}$ kiinnitetty jo johonkin indeksiin g_k, missä $k < 3$. Jos ei, niin jatketaan valitsemalla $g_4 := \theta(g_3)^{-1}$ ja muodostetaan seuraava tulo $g_2\theta(g_2) \cdot g_3\theta(g_3) \cdot g_4\theta(g_4)$. Näin voidaan jatkaa, kunnes saavutetaan tuloketju

$$p_1 := g_2\theta(g_2) \cdot g_3\theta(g_3) \dots g_i\theta(g_i),$$

missä alkio $\theta(g_i)^{-1} = g_k$ potentiaalisesti jollakin $2 \leq k \leq i$. Ei ole mahdollista, että $k = i$, sillä muuten $g_i\theta(g_i) = e = e\theta(e)$ ja kuvaus θ ei olisi täydellinen kuvaus. Ei ole myöskään mahdollista, että $k \geq 3$, sillä muuten $\theta(g_i)^{-1} = g_k = \theta(g_{k-1})^{-1}$ tai yhtäpitävästi $\theta(g_i) = \theta(g_{k-1})$, jolloin kuvaus θ ei olisi bijektio. Siten ainoa mahdollisuus on, että $\theta(g_i)^{-1} = g_2$, ja tällöin huomataan, että $p_1 = e$.

Jos $i \neq n$, niin aloitetaan sama prosessi alusta valitsemalla alkio g_{i+1}, jota ei vielä ole kiinnitetty ja rakennetaan tulo

$$p_2 := g_{i+1}\theta(g_{i+1}) \cdot \ldots \cdot g_j\theta(g_j),$$

mistä samoin päättelemällä nähdään, että viimein indeksille j on voimassa $\theta(g_j) = g_{i+1}^{-1}$, jolloin $p_2 = e$. Toistetaan tätä konstruktiota, kunnes kaikki ryhmän G alkiot on käyty läpi ja saadaan tulot $p_1 = e, p_2 = e, \dots, p_l = e$, jolloin laskemalla auki tulo $p_1p_2 \dots p_l$ saadaan yhtälö

$$g_1\theta(g_1) \cdot g_2\theta(g_2) \cdot \ldots \cdot g_n\theta(g_n) = e,$$

mutta koska kuvaus $x\theta(x)$ on bijektio, niin ylläolevassa lausekkeessa ovat peräkkäin kaikki ryhmän G alkiot jossain järjestyksessä ja niiden tulo on e. □

Lause 4.24 (Burnside)**.** *Olkoon G ryhmä, jonka Sylowin 2-aliryhmä S on syklinen. Tällöin ryhmällä G on olemassa kertalukua $[G : S]$ oleva normaali aliryhmä N.*

Todistus. Ryhmän G kertaluku voidaan kirjoittaa muodossa $|G| = 2^n m$, missä $n \in \mathbb{Z}_+$ ja $m \geq 0$ on pariton kokonaisluku. Todistetaan väite induktiolla luvun n suhteen.

Jos $n = 1$, niin $|G| = 2m$, missä m on pariton. Tällöin lemman 4.12 mukaan ryhmällä G on olemassa kertalukua m oleva normaali aliryhmä N, joten induktion alkuaskel pitää paikkansa.

Induktio-oletuksena kertalukua $2^{n-1}m$ olevilla ryhmillä G', joiden Sylowin 2-aliryhmä S' on syklinen, on olemassa kertalukua m oleva normaali aliryhmä N'. Todistetaan, että myös kertalukua $2^n m$ olevilla ryhmillä on olemassa kertalukua m oleva normaali aliryhmä.

Olkoon G ryhmä, jolle $|G| = 2^n m$ ja jonka Sylowin 2-aliryhmä S on syklinen. Tällöin $S =< s >= \{e, s, s^2, \ldots, s^{2^n-1}\}$ ja $|S| = 2^n$. Alkioiden s^k kertaluku on 2^n aina, kun eksponentti k on pariton. Siten täsmälleen puolet ryhmän S alkioista ovat kertalukua 2^n.

Kuvataan ryhmän G alkiot funktiolla $f : G \to S_{2^n}$ seuraavasti:

$$f(g) = \begin{pmatrix} x \\ gx \end{pmatrix}.$$

Tällöin kuvaus f on homomorfismi [5, Seuraus 3.5, p.11]. Ryhmän G kertalukua 2^n olevat alkiot kuvautuvat parittomille permutaatioille, joten aliryhmän $K := f(G) \cap A_n$ indeksi on 2 ryhmässä $f(G)$. Tällöin ryhmä $H := f^{-1}(K)$ on ryhmän G normaali aliryhmä. Ryhmän H Sylowin 2-aliryhmä on kertalukua 2^{n-1} ja se on myös syklinen, sillä se sisältyy johonkin ryhmän G sykliseen Sylowin 2-aliryhmään, joten induktio-oletuksen nojalla on olemassa $N \lhd H$, jolle $|N| = m$. Osoitetaan, että aliryhmä N on normaali myös ryhmässä G, mikä todistaa induktioväitteen.

Jos ryhmässä H olisi olemassa toinen kertalukua m oleva aliryhmä $N' < H$, missä $N' \neq N$, niin lemman 2.6 nojalla kompleksi NN' muodostaisi ryhmän H aliryhmän, sillä $N \lhd H$. Tällöin kaavan 2.1 mukaan

$$|NN'| = \frac{|N||N'|}{|N \cap N'|} \geq \frac{m^2}{m-1} > m,$$

mutta koska kertaluku $|NN'|$ on pariton sekä $|NN'| \big| 2^{n-1}m$, niin tämä on mahdotonta. Siten aliryhmä N on ainoa ryhmän H kertalukua m oleva aliryhmä.

Jos f on ryhmän H mielivaltainen automorfismi, niin $f(N) = N$, sillä automorfismit kuvaavat aliryhmät aliryhmille. Siten aliryhmä N on karakteristinen ryhmässä H ja koska $H \lhd G$, niin lemman 2.18 mukaan $N \lhd G$. Väite seuraa induktiolla. □

Lause 4.25. *[24] ($\neg B \Rightarrow \neg C$ eli $C \Rightarrow B$). Ryhmällä $G = \{g_1, g_2, \ldots, g_n\}$, jonka Sylowin 2-aliryhmä on syklinen ja ei-triviaali, ei ole olemassa sellaista alkioiden g_i permutaatiota τ, jolle $\tau(g_1)\tau(g_2)\ldots\tau(g_n) = e$.*

Todistus. Oletetaan, että parillista kertalukua olevan ryhmän G Sylowin 2-aliryhmä S on syklinen. Tällöin ryhmässä G on olemassa yksikäsitteinen kertalukua kaksi oleva alkio $t \in S$. Burnsiden lauseen nojalla on olemassa sellainen $N \lhd G$, jolle $G/N \cong S$ ja $|N| = m$, missä $m > 0$ on pariton kokonaisluku. Tällöin

$$(\prod_{g \in G} g)N = \prod_{g \in G} gN = \prod_{g=sn \in G} snN = \prod_{s \in S} (sN)^m = t^m N = tN,$$

josta vertailemalla sivuluokkien edustajia saadaan $\prod_{g\in G} g = t \neq e$ riippumatta siitä, missä järjestyksessä vasemman puolen tulo lasketaan. □

Vuonna 2003 M. Vaughan-Lee ja I.M. Wanless julkaisivat suoran todistuksen implikaatiolle $B \Rightarrow C$ [26], joten ei-kommutatiivisten ryhmien tapauksesta tiedetään nyt, että ehdot B ja C ovat ekvivalentteja. Edellisen lauseen 4.25 ja lauseen 4.23 päättelyt yhdistämällä saadaan implikaatio $A \Rightarrow B$.

Tapauksen $B \stackrel{?}{\Rightarrow} A$ ratkaiseminen on kestänyt kauan. Vuoden 1955 artikkelissa [24] M. Hall ja L. J. Paige esittivät kuuluisan konjektuurinsa.

Konjektuuri 4.26 (Hall-Paige)**.** *($B \Rightarrow A$). Äärellisellä ryhmällä, jonka Sylowin 2-aliryhmä ei ole syklinen on olemassa täydellinen kuvaus.*

Tähän ongelmaan ei saatu vastausta pitkään aikaan, kunnes vuonna 2009 Stewart Wilcox näytti [27], että vastaesimerkki tähän konjektuuriin täytyy olla jokin 26 sporadisesta ryhmästä tai Tits-ryhmä [28]. Vain vähän aikaa tämän jälkeen Anthony B. Evans osoitti [29], että näistä vain Jankon neljäs ryhmä voi tulla kyseeseen. Samassa artikkelissa hän viittaa John Brayn julkaisemattomaan tulokseen, jonka mukaan tämä viimeinenkin tapaus olisi poissuljettu. Siten Hall-Paige -konjektuuri olisi viimein ratkennut. Viittaamme tähän tulokseen silti konjektuurina, sillä John Brayn tutkimusta ei ole vielä julkaistu.

Tämän kappaleen päätteeksi todistetaan implikaatio $B \Rightarrow A$ ratkeaville ryhmille. Tätä varten tarvitaan seuraava aputulos, joka todistaa niin kutsuttujen Hall-aliryhmien olemassaolon ratkeavissa ryhmissä. Tämän lauseen todistus on peräisin J. Rotmanin kirjasta [4].

Lause 4.27 (Hall)**.** *Ratkeavalla ryhmällä G, jonka kertaluku on muotoa ab, missä $a \perp b$, on olemassa kertalukua a oleva aliryhmä.*

Todistus. Edetään täydellisellä induktiolla ryhmän G kertaluvun ab suhteen. Alkuaskeleena voidaan jo pelkästään Sylowin aliryhmien olemassaolotodistukseen perustuen tarkastaa kaikki tapaukset kertalukuun $ab = 29$ asti, sillä vasta $ab = 30 = 2\cdot 3\cdot 5$ on ensimmäinen kertaluku, joka on vähintään kolmen eri alkuluvun tulo.

Tehdään siis induktio-oletus, että Hallin lause pätee kaikille kertalukua ab pienemmille ryhmille ja näytetään, että myös kertalukua ab olevassa ryhmässä G on olemassa kertalukua a oleva aliryhmä, aina kun $a \perp b$.

Koska ryhmä G on ratkeava, niin sillä on olemassa ainakin yksi ei-triviaali normaali aliryhmä, jonka kertaluku voidaan merkitä muodossa $a'b'$, missä $a' \mid a$ ja $b' \mid b$.

Jos ryhmässä G olemassa sellainen aliryhmä $H \lhd G$, jolle $b \nmid |H|$, mikä on yhtäpitävää ehdon $b' < b$ kanssa, niin muodostetaan tekijäryhmä G/H. Tämän ryhmän kertaluku on muotoa $\frac{a}{a'} \cdot \frac{b}{b'} < ab$. Koska tekijäryhmä G/H on myös ratkeava, niin induktio-oletuksen nojalla sillä on olemassa aliryhmä

A/H, jonka kertaluku on $\frac{a}{a'}$. Tällöin ryhmässä G on olemassa tätä tekijäryhmää vastaava aliryhmä A, jolle $|A| = |A/H| \cdot |H| = \frac{a}{a'}a'b' = ab' < ab$. Siten induktio-oletuksen nojalla ryhmällä A on olemassa kertalukua a oleva aliryhmä.

Voidaan siis olettaa, että luku b jakaa jokaisen ryhmän G normaalin aliryhmän kertaluvun. Tämä on yhtäpitävää ehdon $b' = b$ kanssa. Olkoon H ryhmän G minimaalinen normaali aliryhmä. Tällöin lauseen 2.10 mukaan sen tiedetään olevan kommutatiivinen p-ryhmä, eli $|H| = p^n$ jollakin $n \in \mathbb{Z}_+$. Koska $|H| = a'b' = a'b$, niin $a'b = p^n$. Tämä on mahdollista vain, jos $a' = 1$, sillä $a' \perp b$. Siten $|G| = ap^n$, missä $p \nmid a$ ja lisäksi H on ryhmän G Sylowin p-aliryhmä. Koska $H \lhd G$ ja kaikki Sylowin p-aliryhmät konjugoivat ryhmässä, niin H on ryhmän G yksikäsitteinen minimaalinen normaali aliryhmä.

Muodostetaan tekijäryhmä G/H, jonka kertaluku on a. Olkoon K/H tämän tekijäryhmän minimaalinen normaali aliryhmä. Lauseen 2.10 mukaan $|K/H| = q^m$, missä q on jokin alkuluku ja $m \in \mathbb{Z}_+$. Koska $|K/H| \mid |G/H| = a$ ja $a \perp b = p^n$, niin $q \neq p$. Siten $|K| = p^n q^m$. Olkoon Q ryhmän K Sylowin q-aliryhmä, joka on siis muotoa $K = HQ$. Tehdään seuraavat merkinnät:

$$N^* := N_G(Q) \text{ ja } N := N_K(Q).$$

Koska $K < G$, niin $N = N^* \cap K$.

Kohdan 2.4 mukaan ehdoista $K/H \lhd G/H$ ja $H \lhd G$ seuraa, että $K \lhd G$. Siten Frattinin lausetta 2.19 voidaan soveltaa, jolloin $G = KN_G(Q)$, missä $N_G(Q)$ on ryhmän Q normalisoija ryhmässä G. Nyt lauseen 2.20 mukaan

$$G/K = KN^*/K \cong N^*/(N^* \cap K) = N^*/N,$$

mistä saadaan laskettua, että

$$|N^*| = \frac{|G||N|}{|K|}.$$

Normalisoijalle N on voimassa ehto $Q \leq N \leq K$, joten $K = HQ = HN$. Siten kompleksin tulokaavalla 2.1 saadaan

$$|K| = |HN| = \frac{|H||N|}{|H \cap N|},$$

minkä perusteella voidaan päätellä, että

$$|N^*| = \frac{|G|}{|H|}|H \cap N| = a|H \cap N|. \tag{4.2}$$

Näytetään seuraavaksi, että $H \cap N \leq Z(K) = \{e\}$.

Olkoon $x \in H \cap N$. Jokainen ryhmän $K = HQ$ alkio k voidaan esittää muodossa $k = hs$ joillakin $h \in H$ ja $s \in Q$. Tarkastellaan tuloa $xsx^{-1}s^{-1}$. Alkio $s^{x^{-1}} \in Q$, koska $x \in N_K(Q)$, joten $xsx^{-1}s^{-1} \in Q$. Lisäksi koska

$H \lhd G$, niin $xsx^{-1}s^{-1} = x(x^{-1})^{s^{-1}} \in H$. Siten $xsx^{-1}s^{-1} \in Q \cap H = \{e\}$, joten $xs = sx$. Alkio x kommutoi myös alkion h kanssa, sillä H oli ryhmän G minimaalisena normaalina aliryhmänä kommutatiivinen aliryhmä. Tällöin $xk = xhs = hsx = kx$ kaikilla $k \in K$, joten $H \cap N \leq Z(K)$.

Ryhmä K on normaali ryhmässä G ja $Z(K)$ on karakteristinen ryhmässä K, joten lemman 2.18 mukaan $Z(K) \lhd G$. Jos $Z(K)$ ei ole triviaali, niin se on itse joko ryhmän G minimaalinen normaali aliryhmä tai sisältää jonkin ryhmän G minimaalisen normaalin aliryhmän. Molemmissa tapauksissa tästä seuraa, että $H \leq Z(K)$, koska H on ryhmän G yksikäsitteinen minimaalinen normaali aliryhmä. Nyt koska $K = HQ$, niin ryhmän H alkiot kommutoivat ryhmän Q alkioiden kanssa, joten $Q \lhd K$. Koska Q on ryhmän K Sylowin q-aliryhmä ja kaikki Sylowin aliryhmät konjugoivat keskenään, niin Q char K ja siten lemman 2.18 mukaan $Q \lhd G$. Oletuksen nojalla p jakaa jokaisen ryhmän G normaalin aliryhmän kertaluvun, joten $p \mid |Q| = q^m$, mikä on ristiriita, sillä $p \neq q$. Siten $Z(K) = \{e\}$. Tällöin yhtälöstä 4.2 seuraa, että $|N^*| = a$, mikä todistaa induktioväitteen.

□

Hallin lauseen avulla voidaan todistaa, että Hall-Paige -konjektuuri pitää paikkansa ratkeaville ryhmille.

Lause 4.28. *[24](Ratkeaville ryhmille $B \Rightarrow A$). Äärellisellä ratkeavalla ryhmällä, jonka Sylowin 2-aliryhmä ei ole syklinen, on olemassa täydellinen kuvaus.*

Todistus. Olkoon G sellainen ratkeava ryhmä, jonka Sylowin 2-aliryhmä S_2 ei ole syklinen. Hallin lauseen nojalla $G = S_2 \cdot H$. Tällöin $S_2 \cap H = \{e\}$, sillä $|S_2| \perp |H|$. Lauseen 4.15 nojalla ryhmällä S_2 on olemassa täydellinen kuvaus. Lauseen 4.11 mukaan ryhmällä H on myös olemassa täydellinen kuvaus, sillä sen kertaluku on pariton. Siten täydellisten kuvausten laajennuslauseen seurausta 4.19 voidaan soveltaa, joten ryhmällä G on myös olemassa täydellinen kuvaus. □

Luku 5

Antisymmetriset kuvaukset

Kappaleessa 3.1 nähtiin, että täydellisten kuvausten lisäksi antisymmetrisillä kuvauksilla on hyviä ominaisuuksia sovellettavaksi tarkistusmerkkijärjestelmiin. Tämä kappale kokoaa yhteen näiden kuvausten osalta tunnettuja olemassaolo- sekä konstruktiotodistuksia. Harmillisesti antisymmetristen kuvausten teoria on vielä hieman puutteellinen, joten tämä kappale päättyy erään teoriaan liittyvän konjektuurin käsittelyyn.

Edellisen kappaleen lause 4.2 todisti, että Abelin ryhmissä antisymmetristen kuvausten olemassaolo määräytyy samalla kriteerillä kuin täydellisten kuvausten olemassaolo. Seuraava lemma konstruoi antisymmetrisiä kuvauksia paritonta kertalukua olevista Abelin ryhmistä.

Lemma 5.1. *Jos G on Abelin ryhmä ja $n \in \mathbb{Z}_+$ sellainen luku, jolle $n-1 \perp |G|$ ja $n \perp |G|$, niin permutaatio $\phi(x) = x^n$ on antisymmetrinen kuvaus.*

Todistus. Tämän lauseen todistus etenee täsmälleen kuten lemmassa 4.1. □

Seuraavan lauseen avulla löydetään antisymmetrisiä kuvauksia myös tietyistä ei-kommutatiivisista ryhmistä.

Lause 5.2. *[20] Olkoon G ryhmä ja a jokin sen alkio. Kuvaus $\phi(x) = x^{-1}a$ on antisymmetrinen jos ja vain jos alkio a ei kommutoi ryhmässä G minkään kertalukua kaksi olevan alkion kanssa.*

Todistus. Olkoon $a \in G$ sellainen alkio, joka kommutoi jonkin kertalukua kaksi olevan alkion $x \in G$ kanssa. Tällöin kuvaus $\phi(x) = x^{-1}a$ ei ole antisymmetrinen, koska jos $x \, in G \setminus \{e\}$, niin

$$\phi(x)e = x^{-1}ae = xa = ax = e^{-1}ax = \phi(e)x.$$

Olkoon seuraavaksi $a \in G$ sellainen alkio, joka ei kommutoi minkään ryhmän G kertalukua kaksi olevan alkion kanssa. Alkion a kertaluku on oltava pariton, sillä jos $|a| = 2k, k \in \mathbb{Z}_+$, niin a kommutoisi alkion a^k kanssa, joka

on kertalukua kaksi ja erisuuri kuin a. Siten $|a| = 2k + 1$ jollain kokonaisluvulla $k \in \mathbb{Z}_+$.

Oletetaan, että kuvaus ϕ ei ole antisymmetrinen, jolloin on olemassa alkiot $x, y \in G, x \neq y$ siten, että $x^{-1}ay = y^{-1}ax$. Kertomalla tämä yhtälö vasemmalta puolelta alkiolla y ja oikealta puolelta alkiolla x^{-1} saadaan

$$(yx^{-1})a(yx^{-1}) = a, \tag{5.1}$$

sekä myös identiteetit

$$\begin{aligned} (yx^{-1})a &= a(yx^{-1})^{-1} \text{ ja} \\ (yx^{-1})^{-1}a &= a(yx^{-1}). \end{aligned}$$

Tällöin nähdään, että alkio a^2 kommutoi alkion yx^{-1} kanssa, sillä

$$\begin{aligned} (yx^{-1})a^2 &= (yx^{-1})a \cdot a \\ &= a(yx^{-1})^{-1}a \\ &= a \cdot a(yx^{-1})^{-1} \\ &= a^2(yx^{-1}). \end{aligned}$$

Koska lisäksi alkion a kertaluku oli pariton, niin myös alkio a kommutoi alkion yx^{-1} kanssa, sillä

$$\begin{aligned} (yx^{-1})a &= (yx^{-1})a^{2k+2} \\ &= (yx^{-1})(a^2)^{k+1} \\ &= (a^2)^{k+1}(yx^{-1}) \\ &= a(yx^{-1}). \end{aligned}$$

Tämän seurauksena yhtälö 5.1 näyttää, että alkion yx^{-1} kertaluku onkin kaksi:

$$\begin{aligned} (yx^{-1})a(yx^{-1}) &= a \\ (yx^{-1})(yx^{-1})a &= a \\ (yx^{-1})^2 &= e. \end{aligned}$$

Siten alkio a kommutoi kertalukua kaksi olevan alkion kanssa, mikä on ristiriidassa alkion a valinnan kanssa. Siispä kuvaus ϕ on antisymmetrinen kuvaus. □

Tästä tuloksesta saadaan välittömästi seuraava ominaisuus.

Seuraus 5.3. *Kaikilla paritonta kertalukua olevilla ryhmillä on olemassa antisymmetrisiä kuvauksia.*

Todistus. Edellisessä lauseessa esitetty permutaatio ϕ on antisymmetrinen kuvaus jos se ei kommutoi minkään ryhmän kertalukua kaksi olevan alkion kanssa. Lagrangen lausetta käänteisesti soveltamalla paritonta kertalukua olevassa ryhmässä ei ole olemassa alkiota, jonka kertaluku olisi kaksi. Siten kuvaus ϕ on tällaisessa ryhmässä antisymmetrinen kuvaus. □

Tästä tuloksesta seuraa, että kaikilla p-ryhmillä, missä $p \neq 2$, on olemassa antisymmetrisiä kuvauksia. Lause 4.9 kertoi, että kommutatiivisella 2-ryhmällä on olemassa antisymmetrinen kuvaus jos ja vain jos se ei ole syklinen ryhmä. Tällöin jäljelle jää enää ei-kommutatiivisisten 2-ryhmien tapaus.

Lause 5.4. *Ei-kommutatiivisilla 2-ryhmillä on olemassa antisymmetrisiä kuvauksia.*

Todistus. Tämä todistus pohjautuu kaikkien mahdollisten kertalukua 2^n olevien ryhmien rakenteiden tapauskohtaiseen tarkasteluun ([20], [30] ja [24]). □

Siten nämä päättelyt yhteen koottuna kertovat kaikkien p-ryhmien tapaukset.

Seuraus 5.5. *Äärellisellä p-ryhmällä on olemassa antisymmetrinen kuvaus jos ja vain jos se ei ole syklinen 2-ryhmä.*

□

Ryhmät S_1, A_1 ja A_2 ovat triviaaleja ryhmiä, joten niissä on olemassa antisymmetrinen kuvaus. Lauseen 4.10 nojalla ryhmässä S_2 ei ole olemassa antisymmetristä kuvausta, sillä $S_2 \cong C_2$. Lausetta 5.2 voidaan soveltaa isompaa kertalukua oleviin symmetrisiin ja alternoiviin ryhmiin, jolloin saadaan seuraava tulos.

Seuraus 5.6. *Ryhmillä S_n ja A_n, missä $n > 2$, on olemassa antisymmetrisiä kuvauksia.*

Todistus. Ryhmissä S_n ja A_n kertalukua kaksi olevat alkiot ovat sykliraken-teeltaan erillisten transpoosien tuloja. Kaksi permutaatiota, joilla on erillinen syklirakenne, kommutoivat näissä ryhmissä jos ja vain jos ne eivät siirrä yhtään samaa alkiota.

Ryhmä S_n, missä $n > 2$, sisältää n-syklin, joka ei kommutoi minkään transpoosin kanssa, joten se ei myöskään kommutoi minkään kertalukua kaksi olevan alkion kanssa. Valitaan alkioksi a jokin n-sykli.

Jos luku n on pariton, niin myös ryhmä A_n sisältää n-syklin. Valitaan alkioksi a jokin n-sykli.

Jos luku n on parillinen, niin ryhmä A_n sisältää $n-1$-syklin, missä $n-1 \geq 3$, joten se ei ole transpoosi, eikä sen rata voi olla erillinen minkään ryhmän A_n transpoosin kanssa, sillä $n-1$-sykli kiinnittää vain yhden alkion joukosta $1, \ldots, n$. Valitaan alkioksi a jokin $n-1$-sykli.

Kussakin tapauksessa kuvaus $\phi(x) = x^{-1}a$ on lauseen 5.2 nojalla antisymmetrinen kuvaus. □

Lauseesta 5.2 seuraa myös toinen hyödyllinen tulos.

Seuraus 5.7. *Jos ryhmässä G on olemassa alkio a, jonka sentralisoijan $C_G(a)$ kertaluku on pariton, niin tällöin ryhmässä G on olemassa antisymmetrinen kuvaus.*

Todistus. Sentralisoija $C_G(a)$ muodostaa ryhmän, jolloin siihen kuuluvien alkioiden kertaluvut jakavat sentralisoijan kertaluvun. Jos sentralisoijan kertaluku on pariton, niin ryhmässä G ei ole olemassa kertalukua kaksi olevaa alkiota, joka kommutoisi alkion a kanssa. Tällöin lauseen 5.2 mukaan kuvaus $\phi(x) = x^{-1}a$ on antisymmetrinen kuvaus. □

Tämä seurauslause osoittautuu yllättävän vahvaksi, sillä Gallian ja Mullin soveltavat sitä ja yksinkertaisten ryhmien luokittelua [28] todistamaan seuraavan lauseen.

Lause 5.8. *Lukuunottamatta ryhmää $\mathbb{Z}_2$, jokaisella äärellisellä yksinkertaisella ryhmällä on olemassa antisymmetrinen kuvaus.*

Todistus. Äärelliset yksinkertaiset ryhmät jakautuvat seuraaviin luokkiin [5, sivu 30]:

- Sykliset ryhmät, joiden kertaluku on alkuluku.
- Alternoivat ryhmät.
- Lien tyyppiset ryhmät.
- Sporadiset ryhmät, joita on 26 kappaletta.

Seurauslauseita 5.3 ja 5.6 voidaan soveltaa syklisten ja alternoivien ryhmien tapauksissa. Seurauslausetta 5.7 taas voidaan soveltaa Lien tyyppisten ryhmien ja sporadisten ryhmien tapauksissa, sillä näistä kaikista löytyy alkio, jonka sentralisoijan kertaluku on pariton ([20, lause 5.1], [28]). □

Seuraava tulos kertoo, miksi ei-kommutatiivisen ryhmän D_5 soveltaminen tarkistusmerkkijärjestelmissä on suotuisampaa kuin kommutatiivisen ryhmän $\mathbb{Z}_{10}$ käyttäminen.

Lause 5.9. *Dihedraalisilla ryhmillä $D_n = \{a, b | a^n = e, ab = ba^{-1}\}$, missä $n \geq 3$, on olemassa antisymmetrisiä kuvauksia.*

Todistus. Olkoon $n \geq 3$ pariton kokonaisluku. Näytetään, että kuvaus

$$\phi(a^i) = a^{2-i}, \quad \phi(ba^i) = ba^i$$

on antisymmetrinen. Käydään läpi kaikki neljä eri vaihtoehtoa, kun $x \in \{a^i, ba^i\}$ ja $y \in \{a^j, ba^j\}$, missä $i, j \in \mathbb{Z}_+ \cap [1, n]$.

1. $x = ba^i, y = a^j$: Tällöin $\phi(ba^i)a^j = \phi(a^j)ba^i \Leftrightarrow ba^{i+j} = ba^{i+j-2} \Leftrightarrow a^2 = e$, mikä ei ole mahdollista, sillä $|a| = n$.

2. Tilanne $x = a^i, y = ba^j$ on symmetrinen edellisen kanssa.

3. $x = a^i, y = a^j$: Tällöin $\phi(a^i)a^j = \phi(a^j)a^i \Leftrightarrow a^{j+2-i} = a^{i+2-j} \Leftrightarrow a^{2j-2i} = e$, joten $n \mid 2j - 2i = 2(j - i)$. Koska luku n on pariton, niin $n \mid j - i$, mutta koska $j - i \leq n - 1$, niin tämä on mahdollista vain, jos $i = j$ eli $x = y$.

4. $x = ba^i, y = ba^j$: Tällöin $\phi(ba^i)ba^j = \phi(ba^j)ba^i \Leftrightarrow a^{j-i} = a^{i-j} \Leftrightarrow a^{2i-2j} = e$, joten $n \mid 2i - 2j = 2(i - j)$. Koska luku n on pariton, niin $n \mid i - j$, mutta koska $i - j \leq n - 1$, niin tämä on mahdollista vain, jos $i = j$ eli $x = y$.

Kaikissa sopivissa tapauksissa toteutuu $x\phi(y) = y\phi(x) \Rightarrow x = y$, joten kuvaus ϕ on antisymmetrinen kuvaus, kun n on pariton kokonaisluku.

Ryhmille D_n, missä $n = 2k$ jollakin $k \in \mathbb{Z}_+ > 2$, määritellään kuvaus φ seuraavasti:

$$\begin{aligned}
\varphi(e) &= b, \\
\varphi(a) &= e, \\
\varphi(a^i) &= a^{1-i}, \text{ kun } 2 \leq i \leq k, \\
\varphi(a^i) &= ba^{1-i}, \text{ kun } k+1 \leq i \leq n-1, \\
\varphi(ba^i) &= a^{i+1}, \text{ kun } 0 \leq i \leq k-1, \\
\varphi(ba^i) &= ba^{i+1}, \text{ kun } k \leq i \leq n-2 \text{ ja} \\
\varphi(ba^{n-1}) &= ba.
\end{aligned}$$

Tämä kuvaus voidaan laskemalla samalla tavoin kuin edellä varmistaa antisymmetriseksi kuvaukseksi. □

Ryhmälaajennuksia konstruoitaessa antisymmetristen kuvausten olemassaolo välittyy seuraavasti.

Lause 5.10. ***Antisymmetristen kuvausten laajennuslause****. [20] Olkoon G ryhmä ja N ryhmän G normaali aliryhmä. Jos permutaatio ϕ on ryhmän N antisymmetrinen kuvaus, sekä permutaatio ψ ryhmän G/N antisymmetrinen kuvaus, niin ryhmällä G on olemassa antisymmetrinen kuvaus.*

Todistus. Normaali aliryhmä N jakaa ryhmän G erillisiin sivuluokkiin. Kiinnitetään jokaisesta sivuluokasta yksi edustaja (katso propositio 2.2) ja merkitään niitä alkioilla $x_1, \ldots, x_k$, missä $k = \frac{|G|}{|N|}$. Tällöin jokainen ryhmän G alkio x voidaan esittää muodossa $x = x_i n$, missä $n \in N$ ja x_i on sen sivuluokan edustaja, johon alkio x kuuluu. Jos $X \in G/N$, niin merkitään symbolilla

$[X]$ joukon $X \cap \{x_1, \ldots, x_k\}$ ainoata alkiota. Määritellään kuvaus $\theta : G \mapsto G$ kaavalla

$$\theta(x) = \theta(x_i n) := \phi(n)[\psi(Nx_i)].$$

Näytetään, että tämä kuvaus on antisymmetrinen ryhmässä G. Olkoon $x, y \in G$ sellaisia alkioita, joille $x\theta(y) = y\theta(x)$. Tällöin alkiot x ja y voidaan esittää muodossa $x = x_i n_1$ ja $y = x_j n_2$ joillakin $n_1, n_2 \in N$ ja

$$x\theta(y) = y\theta(x) \Leftrightarrow x_i n_1 \phi(n_2)[\psi(Nx_j)] = x_j n_2 \phi(n_1)[\psi(Nx_i)].$$

Tehdään merkinnät $m_1 := n_1\phi(n_2)$ ja $m_2 := n_2\phi(n_1)$ ja saadaan yhtälö

$$x_i m_1[\psi(Nx_j)] = x_j m_2[\psi(Nx_i)].$$

Koska $m_1, m_2 \in N \trianglelefteq G$, niin $m_1[\psi(Nx_j)] = [\psi(Nx_j)]m_1'$ ja $m_2[\psi(Nx_i)] = [\psi(Nx_i)]m_2'$ joillakin $m_1', m_2' \in N$, joille $m_1' = m_2'$ joss $m_1 = m_2$. Lisäksi koska $x_i[\psi(Nx_j)] = [Nx_i][\psi(Nx_j)] = [Nx_i\psi(Nx_j)]$, niin edellinen ehto saa muodon

$$[Nx_i\psi(Nx_j)]m_1' = [Nx_j\psi(Nx_i)]m_2',$$

mikä voi pitää paikkansa vain jos $Nx_i\psi(Nx_j) = Nx_j\psi(Nx_i)$ ja $m_1' = m_2'$. Koska permutaatio ψ on antisymmetrinen ryhmässä G/N, niin ensimmäinen ehto voi pitää paikkansa vain jos $Nx_i = Nx_j$ eli $x_i = x_j$. Samoin ehdosta $m_1' = m_2'$ seuraa, että $n_1 = n_2$, sillä kuvaus ϕ on antisymmetrinen ryhmässä N. Täten $x = y$, mikä todistaa, että permutaatio θ on antisymmetrinen kuvaus ryhmässä G. □

Seuraus 5.11. *Jos A ja B ovat ryhmiä, joilla molemmilla on olemassa antisymmetrinen kuvaus ja kuvaus π on homomorfismi ryhmältä B ryhmän A automorfismiryhmälle, niin puolisuora tulo $G = A \rtimes_\pi B$ sisältää antisymmetrisen kuvauksen.*

Todistus. Proposition 2.16 mukaan ryhmällä G on olemassa aliryhmä $A' = \{(a, e_B) : a \in A\}$, joka on isomorfinen ryhmän A kanssa ja normaali ryhmässä G. Lisäksi tekijäryhmä G/A' on isomorfinen ryhmän B kanssa. Oletusten mukaan molemmilla ryhmillä on olemassa antisymmetrinen kuvaus, joten laajennuslauseen mukaan ryhmällä $A \rtimes_\pi B$ on myös olemassa antisymmetrinen kuvaus. □

Seuraus 5.12. *Jos A ja B ovat ryhmiä, joilla molemmilla on olemassa antisymmetrinen kuvaus, niin myös ryhmällä $A \times B$ on antisymmetrinen kuvaus.*

Todistus. Valitsemalla edellisessä lauseessa ryhmähomomorfismiksi identiteettikuvauksen, puolisuora tulo $A \rtimes_\pi B$ vastaa ryhmien suoraa tuloa $A \times B$. □

Äärellisen ryhmän G sanotaan olevan *nilpotentti ryhmä*, jos se on rakenteeltaan suora tulo sen omista Sylowin p-aliryhmistään. Antisymmetristen kuvausten laajennuslauseen ansiosta myös näiden ryhmien tapaukset tunnetaan tarkasti.

Seuraus 5.13. *[20] Äärellisellä nilpotentilla ryhmällä G, jonka Sylowin 2-aliryhmä on triviaali tai ei-syklinen on olemassa antisymmetrinen kuvaus.*

Todistus. Lauseen 5.3 mukaan kaikilla ryhmän G Sylowin p-aliryhmillä, joissa p on pariton, on olemassa antisymmetrinen kuvaus. Lauseen 5.5 mukaan ryhmän G Sylowin 2-aliryhmällä, jos se ei ole triviaali, on olemassa antisymmetrinen kuvaus. Nilpotentti ryhmä on suora tulo sen Sylowin aliryhmistä, joten seurauksen 5.12 nojalla ryhmällä G on myös olemassa antisymmetrinen kuvaus. □

Edellisten tulosten pohjalta J.A. Gallian ja M.D. Mullin esittivät vuoden 1995 julkaisussaan **Groups with anti-symmetric mappings** [20] seuraavan johtopäätöksen.

Konjektuuri 5.14 (Gallian, Mullin)**.** *Jokaisella ei-kommutatiivisella ryhmällä on olemassa antisymmetrinen kuvaus.*

Tätä konjektuuria ei ole vieläkään tiettävästi ratkaistu. Vuonna 1997 S. Heiss pystyi todistamaan sen paikkansapitävyyden ratkeavien ryhmien tapauksessa [31].

Lause 5.15 (Heiss)**.** *Jokaisella ratkeavalla ei-kommutatiivisella ryhmällä on olemassa antisymmetrinen kuvaus.*

Tämän lauseen todistus perustuu tekniseen tapauskohtaiseen analyysiin ja se sivuutetaan tässä.

□

Mielenkiintoisesti tätä aihetta tutkiessa löytyi ainakin R.H. Schulzin [32], G.B. Belyavskayan ja A. Diordievin [33] sekä G.B. Belyavskayan, V.I. Izbashin ja V.A. Shcherbacovin [34] julkaisut, jotka mainitsevat Heissin todistaneen myös yleisen tapauksen vuonna 1999 preprint-tekstissä **Antisymmetric mappings for finite groups** [35]. Schulz kirjoittaa myöhemmässä julkaisussaan [7] tämän tiedon olevan peräisin vuonna 1997 Itävallassa Grazissa pidetystä DMV-ÖMG -kongressista, jossa Heiss ilmoitti todistaneensa Gallianin ja Mullinin konjektuurin oikeaksi. Kysyttäessä asiaa henkilökohtaisesti elokuussa 2010 [36], Schulz kuitenkin mainitsi, ettei hän ole vieläkään tietoinen Heissin todistuksen julkaisusta. Tosin tulosten 5.8, 5.10, 5.13 ja 5.15 valossa Gallianin ja Mullinin konjektuurin oikeellisuutta on hyvin vaikea epäillä.

Luku 6

Sopivien kuvausten löytäminen

Muodostettaessa uusia tarkistusmerkkijärjestelmiä on ryhmän G ja permutaation δ valinnalla kriittinen rooli. Edellisten kappaleiden teorian pohjalta ymmärretään paremmin, millaisia ryhmiä valita, mutta miten löydetään sopiva antisymmetrinen tai täydellinen kuvaus valitusta ryhmästä? Tämän ongelman ratkaisemiseksi on julkaistu vähän menetelmiä, tiettävästi ainoa tunnettu on L.J. Paigen täydellisiä kuvauksia koskevaan tulokseen [21] pohjautuva A. Eckerin ja G. Pochin algoritmi [18] melkein täydellisten kuvausten konstruoimiseksi. Tässä kappaleessa käsitellään erilaisia toimivaksi todettuja menetelmiä antisymmetristen ja täydellisten kuvauksien löytämiseksi, sekä esitetään näihin pohjautuvien tietokoneajojen tuloksia.

6.1 Täydellinen enumeraatio

Yksittäisen antisymmetrisen kuvauksen löytäminen ei vielä välttämättä riitä, koska sillä voi olla huono virheentunnistuskyky muissa virheluokissa. Haettaessa parasta kaavassa 3.3 käytettävää kuvausta δ voidaan luonnollisesti kokeilla läpi ryhmän kaikki mahdolliset permutaatiot ja valita niistä parhaan virheentunnistustehokkuuden antava. Dihedraalisten ryhmien tapauksessa tätä lähestymistapaa ovat soveltaneet S. Giese [37] ja S. Ugan [38], jotka luokittelevat dihedraalisesta ryhmästä D_5 löydetyt antisymmetriset kuvaukset vahvoihin ja heikkoihin ekvivalenssiluokkiin niiden virheentunnistustehokkuuden mukaan. Nämä tulokset on julkaistu myöhemmin englannin kielellä R-H. Schulzin artikkeleissa ([32], [39]).

Kaikki permutaatiot läpikäymällä saadaan myös sivutuotteena laskettua absoluuttinen lukumäärä ryhmän antisymmetrisille kuvauksille. Yksinkertainen tapa iteroida ryhmän G kaikki permutaatiot läpi on muodostaa niinsanottu leksikografinen järjestys. Tähän tarvittava koodi löytyy esimerkiksi R. Sedgewickin teoksesta Algorithms [40]. Tällaisen ohjelman rakenne on esitelty algoritmissa 1. Symboli id tarkoittaa identiteettikuvausta ja funktio $Succ(p)$ palauttaa leksikografisessa järjestyksessä permutaatiota p seuraa-

Algoritmi 1: Ryhmän antisymmetristen kuvausten täydellinen enumeraatio.

```
n ← 0
p ← id
while p ≠ NULL do
    if IsAntiSymmetric(p) then
        n ← n + 1
    p ←Succ(p)
return n
```

van permutaation tai symbolin NULL, jos sellaista ei ole. Lopuksi ohjelma palauttaa löydettyjen antisymmetristen kuvausten lukumäärän. Vastaavanlaisella koodilla voidaan laskea myös kaikki ryhmän sisältämät täydellisten kuvausten ja ryhmäautomorfismien lukumäärät.

Tällä menettelyllä voidaan käydä läpi pientä kertalukua olevat ryhmät (10 tai vähemmän alkiota) kohtuullisessa ajassa. Isompien ryhmien käsittelyä ei ole mahdollista lähestyä näin naiivisti, sillä ryhmän permutaatioiden lukumäärä kasvaa kertomafunktion nopeudella.

Paremman, mutta monimutkaisemman menetelmän esittelee D.E. Knuth [41, pp. 49-52], jonka on kehittänyt B.R. Heap. Tässä ajatuksena on muodostaa permutaatioista puurakenne, jonka solmuja kuljettaessa voidaan huonot haarat poissulkea ilman, että kaikkia sen sisältämiä permutaatioita tarvitsee käsitellä yksitellen. Kyseessä on eräänlainen backtracking-lähestymistapa. Knuthin esittelemän algoritmin C++ -kielinen implementaatio löytyy liitteestä A.

Heapin menetelmään perustuen haettiin sopivia kuvauksia käytettäväksi uusissa järjestelmissä sekä laskettiin yleisimmistä pientä kertalukua olevista ryhmistä erilaisten kuvausten lukumääriä. Tulokset on esitelty taulukossa 6.1. Tämän taulukon vasemmanpuoleinen sarake ilmoittaa kyseessä olevan ryhmän ja toinen sarake näyttää tässä ryhmässä olevien antisymmetristen kuvausten lukumäärän. Kolmannessa sarakkeessa on ryhmän täydellisten kuvausten lukumäärä ja neljäs sarake ilmoittaa niiden kuvausten lukumäärän, jotka ovat samanaikaisesti sekä antisymmetrisiä että täydellisiä kuvauksia.

Taulukon viimeisessä sarakkeessa on ilmoitettu sellaisten ryhmän automorfismien lukumäärä, jotka ovat samalla myös antisymmetrisiä sekä täydellisiä kuvauksia. Tämäntyyppiset automorfismit ovat tärkeässä roolissa konstruoitaessa moninkertaisia tarkistusmerkkijärjestelmiä, mutta valitettavasti monissa ryhmissä niitä ei ole olemassa laisinkaan. Moninkertaisia tarkistusmerkkijärjestelmiä käsitellään luvussa 8.

Vastaavanlaista tutkimusta antisymmetristen kuvausten lukumääristä on tehnyt H.M. Damm diplomityössään [42], missä hän muotoilee erilaisen algoritmin ryhmän antisymmetristen kuvausten laskemiselle ja esittelee tähän pohjautuen antisymmetristen kuvausten lukumääriä pientä kertalukua ole-

Ryhmä	Antisymm.	Täydell.	As. & T.	Am, As & T.
$\lvert D_2\rvert = 4$	8	8	8	2
$\lvert D_3\rvert = 6$	120	-	-	-
$\lvert D_4\rvert = 8$	1,472	384	256	-
$\lvert D_5\rvert = 10$	34,040	-	-	-
$\lvert D_6\rvert = 12$	1,412,928	76,032	6,912	-
$\lvert D_7\rvert = 14$	100,229,976	-	-	-
$\lvert D_8\rvert = 16$	6,744,202,240	62,881,792	3,252,224	-
$\lvert \mathbb{Z}_2^2\rvert = 4$	8	$*^1$	$*^1$	4
$\lvert \mathbb{Z}_2^3\rvert = 8$	384	$*^1$	$*^1$	48
$\lvert \mathbb{Z}_2^4\rvert = 16$	244,744,192	$*^1$	$*^1$	5,824
$\lvert \mathbb{Z}_2^5\rvert = 32$	$\geq 2,887,680$	$*^1$	$*^1$	2,887,680
$\lvert \mathbb{Z}_2^6\rvert = 64$	$\geq 3,498,268,326$	$*^1$	$*^1$	$\geq 3,498,268,326$
$\lvert Dic_2\rvert = 8$	1,152	384	-	-
$\lvert Dic_3\rvert = 12$	1,403,136	-	-	-
$\lvert S_3\rvert = 6$	120	-	-	-
$\lvert A_4\rvert = 12$	1,532,928	46,080	-	-
$\lvert S_4\rvert = 24$	$\geq 4,059,515,089$	$\geq 3,545,192$	?	-
$\lvert A_5\rvert = 60$	$\geq 410,809,281$	?	?	-
$\lvert C_3\rvert = 3$	3	$*^2$	-	-
$\lvert C_5\rvert = 5$	15	$*^2$	10	2
$\lvert C_7\rvert = 7$	133	$*^2$	28	4
$\lvert C_9\rvert = 9$	2,025	$*^2$	-	-
$\lvert C_{11}\rvert = 11$	37,851	$*^2$	88	8
$\lvert C_{13}\rvert = 13$	1,030,367	$*^2$	4,524	10

Taulukko 6.1: Erityyppisten kuvausten lukumääriä. 1) Näissä ryhmissä antisymmetrisen ja täydellisen kuvauksen määritelmät yhtyvät, joten lukumäärät ovat samoja kuin vasemmanpuoleisessa solussa. 2) Jokaisella täydellisellä kuvauksella on parina oma antisymmetrinen kuvaus, joten lukumäärät ovat samoja kuin vasemmanpuoleisessa solussa.

vissa dihedraalisissa ja syklisissä ryhmissä. Tämän työtä kirjoitettaessa lasketut taulukon 6.1 tulokset yhtyvät Dammin esittämiin. Lisäksi hän näyttää, että kertalukua n olevan ryhmän G antisymmetristen kuvausten $Ant(G)$ lukumäärälle on voimassa yläraja $|Ant(G)| \leq \frac{n!}{e} + \frac{n}{2}$, mikä on kuitenkin valitettavan heikko, sillä se kasvaa asymptoottisesti yhtä nopeasti kuin kokoa n olevien permutaatioiden lukumäärä.

Laskentakapasiteetin rajat tulevat isommilla ryhmillä nopeasti vastaan. Taulukon 6.1 merkintä $\geq x$ tarkoittaa, että kyseisentyyppisiä kuvauksia listattiin ryhmästä ainakin näin monta, ennen kuin ohjelman ajo katkaistiin ajanpuutteen vuoksi. Symboli ? tarkoittaa, että ryhmän koko oli liian iso käsiteltäväksi esitetyillä menetelmillä. Viiva solun kohdalla merkitsee, että kyseisentyyppisiä kuvauksia ei ole olemassa kyseisessä ryhmässä yhtään kappaletta.

6.2 Eckerin ja Pochin algoritmi

Isoissa ryhmissä kaikkien permutaatioiden täydellinen enumerointi ei ole laskennallisesti mahdollista ilman parempaa teoriaa. L.J. Paigen lauseessa 4.6 esitetty tulos on luonteeltaan konstruktiivinen, minkä perusteella A. Ecker ja G. Poch julkaisivat algoritmin [18, pp. 290-293], joka konstruoi mistä tahansa Abelin ryhmästä ainakin melkein täydellisen kuvauksen. Tässä kappaleessa esitellään tämä algoritmi pienin muutoksin, jolloin sitä voidaan käyttää heuristisesti täydellisen kuvauksen etsimiseen myös ei-kommutatiivisissa ryhmissä. Vaikka tällöin algoritmi ei takaa, että sen lopputuloksena tuottama permutaatio olisi täydellinen kuvaus tai edes melkein täydellinen kuvaus, niin käytännössä tämän algoritmin toistettu ajaminen satunnaisella lähtöpermutaatiolla onnistui löytämään täydellisiä kuvauksia myös ei-kommutatiivisista ryhmistä.

M. Hall, Jr. julkaisi konstruktiivisen todistuksen [43] tähän läheisesti liittyvään kombinatoriseen ongelmaan, joka on tietyllä tavalla yleistys täydellisen kuvauksen konstruointiongelmasta Abelin ryhmissä. Eckerin ja Pochin algoritmia voitaisiin aivan yhtä hyvin kutsua myös Paigen algoritmiksi tai Hallin algoritmiksi, mutta tässä käytetään Eckerin ja Pochin nimeä, koska heidän artikkelinsa oli ensimmäinen jossa algoritminen esitystapa oli eksplisiittisesti omaksuttu.

Eckerin ja Pochin algoritmi on luonteeltaan ahne algoritmi [44, kappale 16] ja se toimii kolmessa vaiheessa. Ensimmäisessä vaiheessa kiinnitetään satunnaisesti rakennettavalle täydelliselle kuvaukselle niin monta arvoa kuin mahdollista ilman ristiriitaa. Toisessa vaiheessa pyritään etenemään korjaamalla syntyviä ristiriitoja yksinkertaisilla kahden alkion vaihdoilla ja kolmannessa vaiheessa kokeillaan siirtää jo päätettyjä permutaation arvoja syklinä, jotta uusi arvo voitaisiin kiinnittää. Nämä kolme vaihetta ovat täsmälleen samat kuin se rakenne, missä lemman 4.6 päättely etenee. Abeliaanisessa

tapauksessa näiden kolmen vaiheen perättäinen applikaatio tuottaa täydellisen kuvauksen, mikä oli lemman 4.6 todistuksen sisältö, ja tämän takia sen todistusta ei toisteta tässä. Samaa menettelyä voidaan soveltaa myös ei-abeliaanisissa ryhmissä, mutta tällöin prosessi on vain heuristinen.

Eckerin ja Pochin algoritmi on kuvattu listauksessa 2 ja siinä käytetään seuraavassa esitettävää notaatiota. Algoritmi muodostaa kaksi permutaatiota Abelin ryhmän G alkioista, joita merkitään symboleilla $a_1, \ldots, a_n$ ja $b_1, \ldots, b_n$. Suorituksen tulosteena on permutaatio δ, jonka arvot määräytyvät lausekkeesta $\delta(a_i) := b_i$. Suorituksen aikana käytetään apumuuttujaa r, joka määrää seuraavat alkiot a_r ja b_r, joiden arvot tullaan kiinnittämään. Vaihe kerrallaan muuttujan r arvoa kasvatetaan yhdellä ja algoritmin suoritus päättyy kun $r = n$. Merkinnän helpottamiseksi käytetään apusymboleita $c_1, \ldots, c_n$, jotka määräytyvät kaavalla $c_i := a_i b_i = a_i \delta(a_i)$. Jokaisen vaiheen lopussa pätee invariantti ehto $c_i \neq c_j \ \forall \ i, j < r$, joille $i \neq j$. Alkioita $a_1, \ldots, a_{r-1}$ ja $b_1, \ldots, b_{r-1}$ sanotaan kiinnitetyiksi alkioiksi. Merkitään jäljellejääviä ryhmän G alkioiden joukkoja symboleilla $A = G \setminus \{a_1, \ldots, a_{r-1}\}$ ja $B = G \setminus \{b_1, \ldots, b_{r-1}\}$. Näiden joukkojen alkioita sanotaan vapaiksi alkioiksi. Alkiot $c_1, \ldots, c_{r-1}$ ovat varattuja arvoja, ja vastaavasti alkioita $G \setminus \{c_1, \ldots, c_{r-1}\}$ sanotaan vapaiksi arvoiksi.

Tämän algoritmin C++ -kielinen toteutus löytyy liitteestä B. Kokonaisuudessaan tähän aiheeseen liittyvän ohjelmakoodin pituus oli hieman yli 3500 riviä, joten muun muassa Eckerin ja Pochin algoritmin toimintaan liittyvät testiajot sekä seuraavassa luvussa esitettävien virheentunnistusfrekvenssien laskentaan käytetty ohjelmakoodi on jätetty listauksesta pois. Koko ohjelman lähdekoodi on saatavilla kirjoittajalta tarvittaessa.

Algoritmi 2: Ryhmän antisymmetristen kuvausten täydellinen enumeraatio.

Alustusvaihe. Aseta $r \leftarrow 1$. Siirry vaiheeseen 1.

Vaihe 1. Jos on olemassa sellaiset alkiot $a \in A$ ja $b \in B$, joille $c := a \cdot b$ on vapaa arvo, niin valitse $a_r \leftarrow a$ ja $b_r \leftarrow b$.
Aseta $r \leftarrow r + 1$.
Toista tätä vaihetta, kunnes tällaisia alkioita ei enää löydy.
Jos $r = n$, lopeta suoritus. Muuten siirry vaiheeseen 2.

Vaihe 2. Jos on olemassa sellaiset alkiot $a \in A$ ja $b \in B$ ja indeksi $i < r$, jolle $ab = c_i$, ja jos lisäksi toinen seuraavista ehdoista on voimassa:

- Jos on olemassa alkio $a' \in A \setminus \{a\}$, jolle $a'b_i$ ei ole varattu arvo, niin korvaa $a_i \leftarrow a'$ ja tee valinta $a_r \leftarrow a$ ja $b_r \leftarrow b$. Aseta $r \leftarrow r + 1$. Jos $r = n$, lopeta suoritus.
- Jos on olemassa alkio $b' \in B \setminus \{b\}$, jolle a_ib' ei ole varattu arvo, niin korvaa $b_i \leftarrow b'$ ja tee valinta $a_r \leftarrow a$ ja $b_r \leftarrow b$. Aseta $r \leftarrow r + 1$. Jos $r = n$, lopeta suoritus.

Jos tällaisia alkioita ei löydy, niin siirry vaiheeseen 3. Muussa tapauksessa siirry takaisin vaiheeseen 1.

Vaihe 3. Valitaan mielivaltaiset $a \in A$ ja $b, b' \in B$.
Tavoitteena on pakottaa seuraavaksi valinnaksi $\delta(a) = b$, mutta tämän tekemiseksi täytyy korjata ristiriita, sillä tulo ab on varattu arvo. Numeroidaan jo varatut alkiot a_i ja b_i järjestyksessä uudelleen siten, että a_1 ja b_1 ovat ne alkiot, joille $a_1b_1 = ab$. Jos tulo a_1b' on varattu arvo, niin olkoon a_2 ja b_2 ne alkiot, joille $a_1b' = a_2b_2$. Jos a_2b_1 on varattu arvo, niin olkoon a_3 ja b_3 ne alkiot, joille $a_2b_1 = a_3b_3$. Jatketaan tätä ketjua tarkastelemalla onko $a_{i+1}b_i$ varattu arvo, ja indeksöimällä symboleilla a_{i+2} ja b_{i+2} niitä varattuja alkioita, joiden tulo antaa tämän arvon. Jos ryhmä G on abeliaaninen, niin päädytään lopulta tuloon $a_{j+1}b_j$, joka on lemman 4.6 nojalla vapaa arvo. Tällöin tee seuraava vaihtoketju:

$$b' \to b_1 \to b_2 \to \ldots \to b_j$$

Lopuksi aseta $r \leftarrow r + 1$ ja palaa takaisin vaiheeseen 1, jos $r < n$. Muuten lopeta suoritus.

Ei-abeliaanisen ryhmän tapauksessa tulona $a_{i+1}b_i$ voi esiintyä arvo, joka on tavattu jo aiemmin, tai varatut alkiot tulevat kaikki käydyksi läpi, eikä uutta vapaata arvoa löydy. Tällöin voidaan kokeilla jotain toista alkoiden a, b ja b' valintaa tai pysähtyä ja palauttaa virheen.

Luku 7

Sovellukset

Tässä luvussa esitellään erilaisia yleisesti käytössä olevia tarkistusmerkkijärjestelmiä ja vertaillaan niiden virheentunnistusominaisuuksia edellisissä luvuissa esitetyn teorian pohjalta. Lisäksi luodaan uusia konstruktioita tarkistusmerkkijärjestelmistä, joiden ominaisuudet eroavat joillain tavoin muista käsitellyistä.

7.1 Käytössä olevia järjestelmiä

Seuraavaksi esitetään maailmalla laajasti käytössä olevia järjestelmiä sekä Suomessa erityisesti vakiintuneita menetelmiä, joista ei tiettävästi ole aiemmin julkaistu vastaavaa analyysia.

7.1.1 1,3,7 -tarkiste

Suomessa Finanssialan Keskusliitto julkaisee ohjeistusta pankkisiirtojen viitenumerojärjestelmästä [45]. Tämä järjestelmä perustuu ryhmään $\mathbb{Z}_{10}$, jossa laskun viitenumeron tarkistusmerkki saadaan painottamalla syötemerkkijonon lukuja järjestyksessä oikealta vasemmalle kertoimilla $1, 7, 3, 1, 7, 3, 1, \ldots$ ja summaamalla nämä luvut yhteen modulo 10. Tarkistusmerkki a_n on luku, jolla tämä summa saa arvon nolla. Esimerkiksi, jos luku n on kolmella jaollinen, niin tarkisteyhtälö on muotoa

$$\mathbf{3}a_1 + \mathbf{7}a_2 + \ldots + \mathbf{1}a_{n-3} + \mathbf{3}a_{n-2} + \mathbf{7}a_{n-1} + \mathbf{1}a_n = 0.$$

Tämä järjestelmä havaitsee kaikki yksittäisvirheet, mutta valitettavasti vain 88.9% kaikista vaihtovirheistä ja 59.3% kaikista kaksoisvirheistä. EAN-13 -järjestelmän ohella se on yksi heikoimmista kertalukua 10 olevaan ryhmään perustuvista järjestelmistä.

7.1.2 Luhnin modulo 10

Maailmalla ehkä yleisimmin käytettyä menetelmää tarkistusmerkin laskemiseen kutsutaan *Luhnin modulo 10* -menetelmäksi sen keksijän Hans P. Luhnin mukaan, joka alunperin kehitti ja patentoi [46] menetelmän ja mekaanisen koneen tarkistusmerkin laskemiseen vuonna 1954.

Sittemmin tämä menetelmä on omaksuttu erittäin laajasti, muun muassa suomalaisten pankkien tilinumeroissa [47], matkapuhelinvalmistaja Nokian puhelinten IMEI-sarjanumeroissa [48], GSM-puhelinten SIM-korttien sarjanumeroissa [49] sekä kansainvälisesti luottokorttinumeroiden [15] tarkisteena. Luhnin modulo 10 -järjestelmä on myös määritelty kansainvälisessä ISO/IEC 7064:2003 -standardissa [50]. Tämän järjestelmän käyttökohteita on niin paljon, että yksittäisten järjestelmien sarjanumeromuotoja ei voida tässä käsitellä. Sen sijaan Luhnin modulo 10 -järjestelmää analysoidaan yleisessä muodossaan.

Tässä menetelmässä operoidaan ryhmässä $\mathbb{Z}_{10}$ käyttäen seuraavaa permutaatiota δ:

$$\delta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}.$$

Syötemerkkijonon $a_1 a_2 \dots a_{n-1}$ tarkistusmerkki määräytyy alkiona a_n, joka toteuttaa seuraavan yhtälön:

$$a_n + \delta a_{n-1} + a_{n-2} + \delta a_{n-3} + \ldots + \delta a_2 + a_1 = 0, \text{ jos n on pariton.}$$

$$a_n + \delta a_{n-1} + a_{n-2} + \delta a_{n-3} + \ldots + a_2 + \delta a_1 = 0, \text{ jos n on parillinen.}$$

Luhnin laskentakaava ei siis noudata valintaa $\delta_i := \delta^i$, kuten yhtälössä 3.3. Tässä järjestelmässä $\delta_i \delta_{i-1} = \delta$ tai $\delta_i \delta_{i-1}^{-1} = \delta^{-1}$ riippuen indeksin i pariteetista. Ryhmän $\mathbb{Z}_{10}$ valinnasta johtuen tiedetään, että kuvaus δ tai δ^{-1} ei ole täydellinen eikä antisymmetrinen kuvaus, joten tämä järjestelmä ei tunnista kaikkia transpositiovirheitä eikä kaksoisvirheitä.

Koska Luhnin menetelmässä toimitaan abeliaanisessa ryhmässä ja syötemerkkijonon joka toiseen merkkiin kohdistetaan täsmälleen sama permutaatio ennen summausta (id tai δ indeksistä riippuen), niin tämä järjestelmä ei pysty tunnistamaan yhtäkään hyppyvaihtovirhettä.

7.1.3 Geometrinen modulo 11

Luvussa 3 esiteltiin esimerkkinä maailmalla laajasti käytetty ISBN-10 -järjestelmä, jossa käytetään modulo 11 -laskentaa. Tätä modulusta voidaan käyttää rakentamaan hieman erilainen tarkistusmerkkijärjestelmä, joka kykenee tunnistamaan kaikki kaksoisvirheet ja foneettiset virheet, mitä ISBN-10 -järjestelmä ei tee. Tämän järjestelmän esitteli D. F. Beckley [17] ja siinä käytetään syötemerkkijonossa numeroita $0, \ldots, 9$ sekä tarkisteessa ylimääräistä symbolia X korvaamaan lukua 10. Toisin kuin ISBN-10 -järjestelmä,

tämä järjestelmä käyttää vain yhtä permutaatiota δ ja perustuu yhtälöön 3.1. Permutaatio δ määritellään kaavalla

$$\delta(x) = 2x.$$

Tätä järjestelmää kutsutaan geometriseksi järjestelmäksi, koska permutaation δ kertoimen kaksi takia syötejonon lukujen painokertoimet kasvavat geometrisesti $1, 2, 4, 8, \ldots$.

Tämän geometrisen modulo 11 -järjestelmän analyysi tapahtuu kuten seuraavassa kappaleessa esitettävän suomalaisen henkilötunnusjärjestelmän tapauksessa.

7.1.4 Suomalainen henkilötunnusjärjestelmä

Väestörekisterikeskus hallinnoi Suomessa henkilöiden tunnistamisjärjestelmää [11]. Jokaiselle kansalaiselle annetaan oma henkilötunnus, joka on muotoa

$$d_1d_2m_1m_2y_1y_2 - a_1a_2a_3c, \text{ missä}$$

- d_1d_2 on henkilön syntymäpäivä väliltä $01, \ldots, 31$.
- m_1m_2 on henkilön syntymäkuukausi väliltä $01, \ldots, 12$.
- y_1y_2 on henkilön syntymävuoden kaksi viimeistä numeroa väliltä $00, \ldots, 99$.
- $a_1a_2a_3$ on väestörekisterikeskuksen henkilöä yksilöivä numerosarja väliltä $000, \ldots, 999$.
- luku c on henkilötunnuksen tarkistemerkki, jossa merkitään kirjaimilla tiettyjä lukuja seuraavasti: $0 = 0$, $1 = 1$, ..., $9 = 9$, $10 = A$, $11 = B$, ..., $15 = F$, $16 = H$, $17 = J$, ..., $21 = N$, $22 = P$, $23 = R$, ..., $30 = Y$. Kirjaimet G, I, O ja Q jätetään käyttämättä sekaannusten välttämiseksi.

Yksinumeroisiin päiviin, kuukausiin ja vuosiin lisätään eteen numero nolla, jotta jokainen kenttä on aina kaksinumeroinen luku. Esimerkiksi helmikuun viidentenä päivänä vuonna 1909 syntynyt henkilö saisi henkilötunnuksen, jonka alkuosa on 050209−.

Tarkistemerkin c laskenta tapahtuu käsittelemällä syötemerkkijonoa lukuna kymmenkantajärjestelmässä ja hakemalla sen edustaja jakojäännösluokasta $\mathbb{Z}_{31}$. Tällöin luku c saa sen arvon $0 \leq c \leq 30$, joka on kongruentti luvun $d_1d_2m_1m_2y_1y_2a_1a_2a_3$ kanssa modulo 31. Tämä mahdollisesti kaksinumeroinen luku muutetaan yhdeksi symboliksi käyttäen apuna kirjaimia kuten yllä on esitetty.

Käyttäen aiempien kappaleiden teoriaa, tämä järjestelmä voidaan esittää tarkistusmerkkiyhtälön 3.3 avulla seuraavasti.

$$\begin{aligned} c &\equiv d_1 d_2 m_1 m_2 y_1 y_2 a_1 a_2 a_3 \pmod{31} \Leftrightarrow \\ c &\equiv 10^8 d_1 + 10^7 d_2 + 10^6 m_1 + \ldots + 10^2 a_1 + 10 a_2 + a_3 \pmod{31} \Leftrightarrow \\ c &\equiv \delta^8 d_1 + \delta^7 d_2 + \delta^6 m_1 + \ldots + \delta^2 a_1 + \delta a_2 + a_3 \pmod{31}, \end{aligned}$$

missä $\delta(x) = 10x \pmod{31} = x + x + \ldots + x$ tai multiplikatiivisesti syklistä ryhmää $\mathbb{Z}_{31}$ tulkiten $\delta(x) = x^{10}$. Tässä lausekkeessa permutaation δ potenssit kasvavat oikealta vasemmalle päin, mutta tämä on vain merkinnällinen ero.

Tämän järjestelmän analysoiminen on helppoa edellä esitetyn teorian pohjalta. Ryhmä $\mathbb{Z}_{31}$ on syklisenä ryhmänä kommutatiivinen. Koska $10 \perp 31$, niin kuvaus δ on ryhmän $\mathbb{Z}_{31}$ automorfismi. Lisäksi $11 \perp 31$, joten lemman 4.1 nojalla kuvaus δ on myös täydellinen kuvaus. Samoin lemman 5.1 mukaan kuvaus δ on antisymmetrinen kuvaus, sillä $9 \perp 31$.

Lisäksi $\delta^2(x) = x^{20}$ ja koska $19 \perp 31$, $20 \perp 31$ ja $21 \perp 31$, niin myös kuvaus δ^2 on ryhmän $\mathbb{Z}_{31}$ täydellinen sekä antisymmetrinen automorfismi.

Itse asiassa kuvauksen δ kertaluku on 15 ja voidaan laskea, että kuvaus δ^i on sekä täydellinen että antisymmetrinen automorfismi kaikilla $1 \leq i \leq 15$. Siten tämä järjestelmä tunnistaa myös kaikki yleiset vaihtovirheet ja kaksoisvirheet (ks. lause 7.3).

7.1.5 Verhoeffin D_5-järjestelmä

Kuten lauseen 4.10 pohjalta tiedetään, niin ryhmässä $\mathbb{Z}_{10}$ ei ole olemassa antisymmetrisiä eikä täydellisiä kuvauksia, mikä estää vaihto- ja kaksoisvirheiden tunnistamisen täydellisesti. Tämän ongelman korjaamiseksi ei ole kuitenkään välttämätöntä siirtyä isompaa kertalukua olevaan ryhmään, sillä sen sijasta voidaan käyttää ei-kommutatiivista kertalukua 10 olevaa dihedraalista ryhmää D_5.

Vuonna 1969 J. Verhoeff julkaisi ryhmään D_5 perustuvan tarkistusmerkkijärjestelmän [16]. Tässä ryhmässä on olemassa useita antisymmetrisiä kuvauksia. Kappaleessa 6.1 esitetyllä tietokonehaulla niitä löydettiin kaikenkaikkiaan 34,040 kappaletta (taulukko 6.1). J. Verhoeffin järjestelmässä käytetään yhtä permutaatiota δ ja tarkisteyhtälöä 3.2, missä $\delta_i = \delta^i$, kun $1 \leq i \leq n-1$ ja $\delta^n = id$. Numerot $0, \ldots, 9$ koodataan ryhmän D_5 alkioiksi kuten on esitetty taulukossa 7.1. J.Verhoeff valitsi ryhmän D_5 permutaatioista käytettäväksi seuraavan kuvauksen δ:

$$\delta = (0, 1, 5, 8, 9, 4, 2, 7)(3, 6)$$

Permutaatio δ on antisymmetrinen kuvaus, joten se tunnistaa kaikki vaihtovirheet. Kaikkia kaksoisvirheitä se ei kuitenkaan pysty tunnistamaan, sillä se ei ole täydellinen kuvaus. Itse asiassa ryhmään D_5 perustuen ei voidakaan

$0 \mapsto e$	$5 \mapsto b$
$1 \mapsto a$	$6 \mapsto ba$
$2 \mapsto a^2$	$7 \mapsto ba^2$
$3 \mapsto a^3$	$8 \mapsto ba^3$
$4 \mapsto a^4$	$9 \mapsto ba^4$

Taulukko 7.1: Lukujen $0, \ldots, 9$ upottaminen ryhmän D_5 alkioiksi.



Kuva 7.1: Saksalaisissa pankkiseteleissä käytettiin vuodesta 1990 lähtien Verhoeffin D_5-järjestelmää. Kuvan lähde: [51].

rakentaa järjestelmää, joka tunnistaisi kaikki kaksoisvirheet, sillä lauseen 4.13 mukaan tässä ryhmässä ei ole olemassa yhtään täydellistä kuvausta.

Saksan kansallispankki (Deutsche Bundesbank) otti vuonna 1990 käyttöön pankkiseteleissään Verhoeffin järjestelmän [52]. Seteleiden tunnisteet ovat 11 merkkiä pitkiä numerosarjoja, joiden viimeinen luku on tarkiste. Lukujen lisäksi käytetään kirjaimia $A, D, G, K, L, N, S, U, Y, Z$, jotka vastaavat numeroita $0, \ldots, 9$. Tämä järjestelmä pysyi käytössä vuoteen 2002 asti, jolloin euro syrjäytti Saksan markan.

Esimerkki. Kuvassa 7.1 esitetyn setelin sarjanumeron $AG5565747G4$ voi tarkistaa oikeaksi laskemalla Verhoeffin kaavalla

$$\delta(0)\delta^2(2)\delta^3(5)\delta^4(5)\delta^5(6)\delta^6(5)\delta^7(7)\delta^8(4)\delta^9(7)\delta^{10}(2) \cdot 4 =$$
$$1 \cdot 0 \cdot 4 \cdot 2 \cdot 3 \cdot 0 \cdot 2 \cdot 4 \cdot 0 \cdot 0 = 0,$$

mistä tulos on nolla, kuten pitääkin. Tässä kohden on syytä huomauttaa, että tarkistusmerkkijärjestelmä ei ole turvaominaisuus, eli sillä ei voi estää setelien väärentämistä.

Lisäksi Verhoeffin tarkistusmerkkijärjestelmä on käytössä ainakin lääketieteellisessä SNOMED Clinical Term Identifier -referenssinimitermistössä [53].

7.1.6 Mod97-10 -tarkiste

Pankkien kansainvälisen rahaliikenteen helpottamiseksi on kehitetty yhtenäinen IBAN-pankkitilinumerointi [12], jossa käytetään ISO/IEC 7064-standardin [50] mukaista tarkistetta. Tämä tarkiste toimii kertalukua 97 olevassa syklisessä ryhmässä ja tarkisteen laskenta tapahtuu samalla tavalla kuin HETU-järjestelmässä tulkitsemalla numerosarjaa kymmenlukujärjestelmän lukuna, mutta modulon 31 sijasta lasketaan jakojäännös luvusta 97. Tämä luku on valittu siksi, että se on suurin lukua 100 pienempi alkuluku.

IBAN-tilinumerot sisältävät myös maa- ja pankkitunnisteena kirjaimia, jotka muutetaan kaksinumeroisiksi luvuiksi säännöllä

$$A \to 10, B \to 11, \ldots, Z \to 35.$$

Tämä aiheuttaa hieman kompleksisuutta järjestelmän analyysiin, sillä kirjaimen muuttaminen luvuksi tarkoittaa yhden symbolin korvaamista kahdella, mikä kasvattaa kaikkien kirjainta vasemmalla puolella esiintyvien lukujen kerrointa 10-kertaiseksi. Tämä aiheuttaa muun muassa sen, että IBAN-järjestelmä ei havaitse vaihtovirheitä $B1 \leftrightarrow 1B, M1 \leftrightarrow 1M, X1 \leftrightarrow 1X$ tai kaksoisvirheitä $11 \leftrightarrow RR, 44 \leftrightarrow BB, 88 \leftrightarrow MM$. Toisaalta tämä ei välttämättä ole iso ongelma, sillä ne indeksit, joissa kirjaimia esiintyy ovat ennalta määrättyjä ja kirjainyhdisteet tunnettuja, jolloin osa näissä tapahtuvista virheistä voidaan tunnistaa muilla keinoin. Esimerkiksi maakoodin FI muuntuminen vaikkapa koodiksi EI tiedetään hylätä ilman tarkistusmerkkiäkin, sillä maakoodia EI ei ole rekisteröity.

Tämän kirjaimiin liittyvän ominaisuuden takia modulo 97-järjestelmän virheentunnistuskykyä kokeiltiin kahdessa eri muodossa. Mod97-10 -järjestelmäksi kutsutaan menettelyä, jossa ei käytetä kirjaimia ollenkaan. IBAN-järjestelmäksi taas kutsutaan Mod97-10 -järjestelmän versiota, jossa kirjaimet ovat sallittuja.

Mod97-10 -järjestelmän virheentunnistuskyky on erittäin vahva ja se tunnistaa kaikki yksittäisvirheet, vaihtovirheet, kaksoisvirheet, foneettiset virheet sekä yleiset kaksois- ja vaihtovirheet. Nämä ominaisuudet seuraavat samalla päättelyllä kuin HETU-järjestelmän yhteydessä, sillä $10 \perp 97$. Mod97-10 -järjestelmä tunnistaa myös lähes kaikki (97.9%) kahden yksittäisen merkin muutokset, mikä johtuu luvun 97 suuruudesta verrattuna lukuun 10. Kaikkien kahden yksittäisvirheen tunnistaminen ei ole kuitenkaan mahdollista, koska $97 < 10^2$.

Luvun 97 sijasta voidaan tietenkin käyttää mitä tahansa muuta alkulukua, jolloin saadaan kaikki taulukon 3.1 virheet tunnistava järjestelmä. Alkuluku 37 voi olla erityisen mielenkiintoinen, jolloin voidaan käyttää symboleja $\{0, \ldots, 9, A, \ldots, Z, *\}$. Tällaista järjestelmää käsitellään esimerkiksi Eckerin ja Pochin artikkelissa [18].

7.2 Uusia konstruktioita

Tässä kappaleessa esitetään uusia järjestelmiä, jotka voisivat olla käyttökelpoisia vaihtoehtoja vakiintuneille menetelmille.

7.2.1 Elementaarinen Abelin 2^k-ryhmä

Tarkastellaan ryhmää $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, joka on kommutatiivinen ryhmä. Jokainen tämän ryhmän G_2 alkio voidaan esittää monikkona (a_1, a_2, a_3, a_4), missä $a_i \in \{0, 1\}$. Näitä alkioita on luonnollista tulkita heksadesimaalilukuina luvun $(a_1a_2a_3a_4)_2$ kardinaliteetin mukaan.

Tässä ryhmässä sopivien kuvausten etsiminen on hieman helpompaa, koska $x = x^{-1}$ aina, kun $x \in G_2$, jolloin lause 4.2 voidaan esittää yksinkertaisemmin seuraavasti.

Lemma 7.1. *Olkoon G Abelin ryhmä, jossa $x = x^{-1}$ aina, kun $x \in G$. Permutaatio θ on antisymmetrinen kuvaus täsmälleen silloin kun se on täydellinen kuvaus.*

□

M. Niemenmaa [54] näytti, että ryhmän G_2 automorfismi

$$P\big((a, b, c, d)\big) = (a + b, c, d, a),$$

sekä sen neliö P^2 ovat antisymmetrisiä ja täydellisiä kuvauksia, ja siten kappaleessa 3.3.2 esitettyjen ehtojen mukaan P havaitsee kaikki yksittäisvirheet, vaihtovirheet, kaksoisvirheet, hyppyvaihtovirheet ja hyppykaksoisvirheet.

Tämä järjestelmä havaitsee 7/8(87.5%) foneettisista virheistä. Muunnosta $18 \to 80$ ei havaita, sillä

$$1+P(8) = 1+P\big((1,0,0,0)\big) = (0,0,0,1)+(1,0,0,1) = (1,0,0,0) = 8+P(0).$$

Tietokonehaun tuloksena löydettiin automorfismi

$$Q(a, b, c, d) = (a + b + c, d, a, a + b),$$

joka havaitsee samat edellä esitetyt virheet kuin kuvaus P, mutta lisäksi tunnistaa myös kaikki foneettiset virheet.

Automorfismeilla P ja Q on muitakin virheentunnistusominaisuuksia.

Lemma 7.2. *Olkoon G Abelin ryhmä ja kuvaus θ jokin sen automorfismi ja täydellinen kuvaus. Tällöin θ ei kiinnitä yhtään ryhmän G kertalukua kaksi olevaa alkiota.*

Todistus. Jos θ kiinnittäisi jonkin kertalukua kaksi olevan alkion $x \in G$, eli $\theta(x) = x$, niin $x\theta(x) = x^2 = e = e\theta(e)$, mikä on ristiriita, sillä $x \neq e$. □

Olkoon $G \leq S_n$ jokin permutaatioryhmä, joka operoi joukon X alkoita. Joukon X alkioille voidaan määritellä relaatio $\equiv$ seuraavasti:

$$a \equiv b \Leftrightarrow \exists\ g \in G : g(a) = b.$$

Tämä relaatio on ekvivalenssirelaatio (symmetrinen, refleksiivinen ja transitiivinen). Tällöin relaation $\equiv$ muodostamia joukon X ekvivalenssiluokkia sanotaan permutaatioryhmän G *radoiksi.*

Lause 7.3. *Olkoon θ ryhmän G_2 automorfismi ja täydellinen kuvaus ja $k > 1$ permutaation θ lyhimmän ei-triviaalin radan pituus. Tällöin θ^i on täydellinen kuvaus aina, kun $i < k$.*

Todistus. Olkoon $i < k, i \in \mathbb{Z}_+$. Jos $x, y \in G_2$ ovat sellaisia alkioita, joille $x+\theta^i(x) = y+\theta^i(y)$, niin $x+y = \theta^i(x+y)$, eli θ^i kiinnittää alkion $x+y$. Koska $i < k$, niin alkio $x + y$ kuuluu johonkin kuvauksen θ triviaaleista radoista, mutta edellisen lauseen nojalla vain identiteettialkio tulee kyseeseen. Siten $x = y$, eli kuvaus θ^i on täydellinen kuvaus. □

Edellä esitetyt automorfismit P ja Q ovat molemmat 15-syklejä, joten niiden kertaluku ja lyhimmän ei-triviaalin radan pituus on 15. Siten kaikki automorfismit $P^i, Q^i, 1 \leq i \leq 14$ ovat ryhmän G_2 täydellisiä kuvauksia. Tästä seuraa, että automorfismit P ja Q havaitsevat kaikki yleistetyt transpositiovirheet sekä yleistetyt kaksoisvirheet siinä tapauksessa, että niiden merkkien etäisyys syötemerkkijonossa, joissa tämä virhe tapahtuu ei ole luvun 15 monikerta.

7.2.2 10/16 -järjestelmä

Aiemmin esitetyistä järjestelmistä ISBN-10 -menetelmässä syötemerkkijonoissa käytetään vain kymmentä ryhmän $\mathbb{Z}_{11}$ yhdestätoista alkiosta. IBAN-menetelmä on samanhenkinen ja siinä syötemerkkijonot koostuvat myös vain numeroista $0, \ldots, 9$, vaikka tässä järjestelmässä toimitaan ryhmässä $\mathbb{Z}_{97}$. Tällaisilla ryhmän osajoukkoon perustuvilla menetelmillä on selkeä etu sellaisiin menetelmiin verrattuna, joissa sekä syötemerkit että tarkistemerkki käyttävät samaa aakkostoa. Tämä johtuu yksinkertaisesti siitä, että koska tarkistemerkki voi saada useamman arvon verrattuna syötemerkkeihin, on virheen sattuessa tarkistefunktion törmäyksen vaara pienempi. HETU-järjestelmässä käytetään lukujen $0, \ldots, 9$ jatkeena kirjaimia symboloimaan merkkejä $10, \ldots, 30$, jolloin tarkiste voidaan kirjoittaa käyttäen vain yhtä merkkiä. Lisäksi tällaisella menettelyllä on ihmismuistin kannalta tietty etu, sillä numeroista koostuvat merkkijonot, jotka päättyvät (mahdollisesti) kirjaimeen voivat olla helpompia muistaa.

Näiden havaintojen sekä edellisen kappaleen heksadesimaalijärjestelmän innoittamana on kehitelty tämä 10/16 -järjestelmä. Tässä järjestelmässä toimitaan elementaarisessa Abelin ryhmässä $\mathbb{Z}_2^4$. Syötemerkkijonoissa käytetään

vain lukuja $0, \ldots, 9$, mutta tarkistemerkki voi olla mikä tahansa ryhmän $\mathbb{Z}_2^4$ kuudestatoista alkiosta. Tarkistemerkki voidaan koodata käyttäen symboleita $0, \ldots, 9, A, B, C, D, E, F$ tai vaihtoehtoisesti vaikkapa käyttäen kirjaimia $A, B, C, D, E, F, G, H, J, K, L, M, N, O, P, Q$.

Tähän menetelmään käytettävä permutaatio haettiin ohjelmallisesti kaikista ryhmän $\mathbb{Z}_2^4$ automorfismien joukosta, joita on ryhmässä $\mathbb{Z}_2^4$ $20,160$ kappaletta. Näistä taulukon 6.1 mukaan $5,824$ on sellaisia, jotka ovat myös samalla täydellisiä sekä antisymmetrisiä kuvauksia. Näiden joukosta virheentunnistusominaisuuksiltaan parhaimmaksi osoittautui permutaatio

$$\delta_1 = (0)(12AEFD796BC5384),$$

joka on kertalukua 15 oleva antisymmetrinen ja täydellinen automorfismi. Mielenkiintoisena yksityiskohtana haussa löytyi vain kaksi muuta automorfismia $\delta_2 = (0)(124936DA5B7FEC81)$ ja $\delta_3 = (0)(1C3BA65E4279DF8)$, jotka eivät olleet vertailtavissa permutaation δ_1 kanssa, kun kriteerinä oli seuraavassa kappaleessa esitettävien taulukoiden 7.2 ja 7.3 sisältämien virheluokkien tunnistusfrekvenssit.

Seuraavassa luvussa käsitellään kahden yksittäisvirheen tunnistustehokkuuden ylärajaa ja siinä esitettävän lauseen mukaan ryhmään $\mathbb{Z}_2^4$ perustuva järjestelmä tunnistaa noin 94.1% tämän virheluokan virheistä. Koska tämä 10/16 -järjestelmä käyttää syötteessä vain kymmentä ryhmän kuudestatoista alkiosta, niin kahden yksittäisvirheen tunnistustehokkuus havaittiin olevan hieman parempi, noin 94.7%.

7.2.3 10/32 -järjestelmä

Elementaarisen Abelin ryhmän $\mathbb{Z}_2^4$ sijasta voidaan myös käyttää ryhmää $\mathbb{Z}_2^5$. Tämän ryhmän soveltaminen on kätevää, sillä numerot $0, \ldots, 9$ ja kirjaimet $A. \ldots, Z$ riittävät vielä 32 eri merkin esittämiseen. Muuten menettely tapahtuu täsmälleen samoin kuten edellä.

Tähän järjestelmään valittiin sopiva automorfismi myös ohjelmallisesti ryhmän $\mathbb{Z}_2^5$ kaikkien automorfismien joukosta, joita on $9,999,360$ kappaletta. Näistä $2,887,680$ on samanaikaisesti sekä antisymmetrisiä että täydellisiä, joista tietokonehaku päätyi seuraavaan permutaatioon

$$\begin{aligned}\theta \;=\; & (1)(2, 24, 26, 21, 11, 7, 16, 27, 8, 25, 4, 20, 19, 6, 29, 9,\\ & 3, 5, 12, 18, 23, 15, 14, 31, 13, 10, 22, 30, 32, 3, 8, 17),\end{aligned}$$

joka on kertalukua 31 oleva täydellinen ja antisymmetrinen automorfismi.

7.3 Virheentunnistustehokkuus

Edellisessä kappaleessa 7.1 esitetyt järjestelmät eroavat paljon virheentunnistusominaisuuksiltaan. Teorian pohjalta voidaan selvittää, milloin järjestelmä

Järjestelmä	$\|G\|$	$ab \to ba$	$aa \to bb$	$acb \to bca$	$aca \to bcb$	$a0 \leftrightarrow 1a$
EAN-13	10	88.9%	88.9%	0%	88.9%	100%
$1, 3, 7$	10	88.9%	59.3%	88.9%	59.3%	100%
Luhn mod 10	10	97.8%	93.3%	0%	88.9%	87.5%
Verhoeff D_5	10	100%	95.6%	94.2%	94.2%	87.5%
ISBN-10	10/11	100%	88.9%	100%	100%	88.9%
Geom. mod 11	10/11	100%	100%	100%	100%	100%
Niemenmaa	16	100%	100%	100%	100%	87.5%
Niemenmaa-2	16	100%	100%	100%	100%	100%
10/16	10/16	100%	100%	100%	100%	100%
HETU	10/31	100%	100%	100%	100%	87.5%
10/32	10/32	100%	100%	100%	100%	100%
IBAN	36/97	99.6%	99.5%	99.6%	99.6%	100%
Mod97-10	10/97	100%	100%	100%	100%	100%

Taulukko 7.2: Yksinkertaisten virheiden virheentunnistusfrekvenssit.

Järjestelmä	$ax \to ya$	$a..b \to b..a$	$ab..cd \to cd..ab$	$a..a \to b..b$	$a..b \to c..d$
EAN-13	91.1%	44.4%	39.5%	88.9%	90.9%[1]
$1, 3, 7$	91.1%	59.3%	52.7%	69.1%	90.9%[1]
Luhn mod 10	90.2%	48.9%	44.6%	91.1%	90.9%[1]
Verhoeff D_5	90.0%	94.2%	89.7%	94.2%	90.9%[1]
ISBN-10	91.1%	100%	90.0%	88.9%	91.8%
Geom. mod 11	91.1%	100%	90.0%	100%	91.7%
Niemenmaa	93.8%	100%[2]	93.3%	100%[2]	94.1%[1]
Niemenmaa-2	93.8%	100%[2]	93.3%	100%[2]	94.1%[1]
10/16	94.4%	100%[2]	93.3%	100%[2]	94.7%
HETU	97.6%	100%	97.2%	100%	97.7%
10/32	97.8%	100%[3]	97.2%	100%[3]	97.7%
IBAN	99.1%	99.6%	98.9%	99.6%	99.0%
Mod97-10	100%	100%	99.9%	100%	97.9%

Taulukko 7.3: Yleistettyjen virheiden tunnistusfrekvenssit. 1) Käsitellään seuraavassa luvussa. 2) 100% kunhan indeksien etäisyys, joissa virhe tapahtuu, ei ole luvun 15 monikerta, ks. lause 7.3. 3) 100% kunhan indeksien etäisyys, joissa virhe tapahtuu, ei ole luvun 31 monikerta.

tunnistaa kaikki tietyntyyppiset virheet, mutta virheentunnistusominaisuuden puuttuessa teorian perusteella ei voida sanoa, kuinka lähelle täydellisyyttä menetelmä pääsee. Varsinkin kertalukuun kymmenen perustuvissa järjestelmissä on merkittäviä käytännön eroja.

Kaikki edellä esitetyt menetelmät toteutettiin tietokoneohjelmana, jossa käytiin läpi kattavasti jokaista virheluokkaa kohden kaikki mahdolliset virheet. Jokaista menetelmää ja virheluokkaa kohden laskettiin kuinka ison osan kaikista tämän tyypin virheistä menetelmä tunnistaa. Tulokset on esitelty taulukoissa 7.2 ja 7.3. Jokainen näissä taulukoissa esitettävä menetelmä tunnistavaa kaikki yksittäisvirheet, joten niiden tunnistusfrekvenssiä ei ole merkitty. Taulukon 7.2 toinen sarake kertoo, kuinka montaa alkiota kyseisessä tarkistusmerkkijärjestelmässä käytetään. Merkintä x/y tarkoittaa, että järjestelmän syötemerkkijonossa käytetään x kappaletta eri alkioita, mutta tarkisteluvulla voi olla y eri arvoa. Tällaisen menettelyn tehokkuus on ilmeinen esimerkiksi IBAN-järjestelmän yhteydessä, sillä se tunnistaa jopa 98.3% kaikista kahdesta yksittäisvirheestä.

Teorian näyttämä kertalukua 10 olevien abeliaanisten ryhmien puutteet voidaan lukea tästä selvästi. Näiden ongelmien kiertämiseksi esiteltiin kaksi järjestelmää, Verhoeffin ryhmään D_5 perustuva menetelmä sekä ISBN-10 -järjestelmä. Nämä molemmat toimivat kertalukuun 10 perustuvia järjestelmiä paremmin.

Taulukon 7.3 viimeisessä sarakkeessa kohdissa 1) toistuvat samat luvut, mikä ei ole sattumaa. Tätä ominaisuutta käsitellään seuraavassa luvussa.

Luku 8

Useampi tarkistusmerkki

Lukujen 4 ja 5 pohjalta tiedetään paremmin, millaisia ryhmiä kannattaa tarkastella uusia järjestelmiä rakennettaessa. Edellisen luvun kokeelliset tulokset näyttivät, että mikään yhden tarkistusmerkin järjestelmä ei kykene tunnistamaan kahta yksittäisvirhettä. Tässä luvussa tutkitaan tätä rajoitetta hieman tarkemmin, sekä konstruoidaan uusia esimerkkejä tarkistusmerkkijärjestelmille, joilla tämä rajoite voidaan ohittaa.

8.1 Graafien värityksistä

Tarkistusmerkkijärjestelmän ominaisuuksia voidaan tarkastella elementaarisen graafiteorian avulla. Tämä mahdollistaa kaikkiin tarkistusmerkkijärjestelmiin liittyvien tiettyjen rajoitteiden tunnistamisen.

Määritelmä 8.1. *Graafi on pari (V, E), missä V on joukko, jonka alkioita sanotaan graafin solmuiksi ja $E \subseteq V \times V$ on joukko, jonka alkioita sanotaan graafin viivoiksi. Joukolle E pätee ehto $\forall\, v_1, v_2 \in V : (v_1, v_2) \in E \Rightarrow (v_2, v_1) \in E$.*

Tarkistusmerkkijärjestelmää kuvataan seuraavan ongelman kautta.

Määritelmä 8.2. *Graafin $R = (V, E)$ väritys on funktio $c : V \mapsto C$. Joukkoa C sanotaan graafin väreiksi.*

Olkoon $G(V, E)$ graafi ja c sen väritys. Tällöin tämän graafin viivat voidaan jaotella *oikein väritettyjen* viivojen joukkoon

$$O = \big\{(v_1, v_2) \in E : c(v_1) \neq c(v_2)\big\}$$

ja *väärin väritettyjen* viivojen joukkoon $H = E \setminus O$. Jos graafin väritykselle c on voimassa $|H| = 0$, niin sanotaan, että graafi on *hyvin väritetty*.

Huomaa, että tämä käsitteistö eroaa hieman joistakin teksteistä, joissa käsitellään vain hyviä värityksistä käyttäen pelkästään termiä väritys. Lisäksi on mahdollista, joukon C valinnasta riippuen, että kaikilla graafeilla ei välttämättä ole olemassa hyvää väritystä.

Ryhmän G päälle rakennettua tarkistusmerkkijärjestelmää, jossa tarkisteen määrittää funktio $f : G^{n-1} \mapsto G$ voidaan mallintaa graafina $R = (V, E)$ seuraavasti. Määritellään graafin solmut asettamalla $V = \{a_1 a_2 \dots a_{n-1} \in G^{n-1} : a_i \in G\}$. Tehdään valinta taulukoissa 3.1, 3.2 ja 3.3 mainituista virheluokista, joita halutaan havaita ja määritellään graafin viivajoukko E siten, että $(v_1, v_2) \in E$, jos ja vain jos merkkijono v_1 saadaan merkkijonosta v_2 jollakin valittujen virheiden tyyppisellä muunnoksella. Valittujen virhetyyppien ehdot täyttävän tarkistusmerkkijärjestelmän olemassaolo määräytyy graafin R avulla kysymällä, onko olemassa sellaista funktiota $f : G^{n-1} \mapsto G$, joka on graafin R hyvä väritys? Funktion f pitäisi siis värittää jokainen graafin solmu hyvin jollakin joukon G alkiolla. Jos $(v_1, v_2) \in E$ ja $f(v_1) = f(v_2)$, niin tällöin tarkistusmerkkijärjestelmä ei kykene erottelemaan virhettä, joka aiheutti muutoksen $v_1 \rightsquigarrow v_2$.

Tästä analogiasta on hyötyä tutkittaessa tarkistusmerkkijärjestelmien rajoitteita.

Määritelmä 8.3. *Täydellinen graafi on graafi (V, E), jolle $(v_1, v_2) \in E$ aina, kun $v_1, v_2 \in V$.*

Luonnollisesti n solmua sisältävän täydellisen graafin hyvin värittämiseen tarvitaan n väriä.

Määritelmä 8.4. *Kahden merkkijonon $a_1 a_2 \dots a_n$ ja $b_1 b_2 \dots b_n$ Hamming-etäisyys on niiden indeksien i lukumäärä, joilla alkiot a_i ja b_i eroavat toisistaan.*

Syötemerkkijonossa tapahtuva yksittäisvirhe tuottaa merkkijonon, jonka Hamming-etäisyys alkuperäiseen merkkijonoon on yksi. Kaksi yksittäisvirhettä tuottavat merkkijonon, jonka Hamming-etäisyys on kaksi, ja niin edelleen.

Yksi taulukossa 3.2 esitetyistä virheluokista oli kaksi yksittäisvirhettä. Tällainen virhe tarkoittaa syötejonossa muutosta

$$\dots a_i \dots a_j \dots \rightsquigarrow \dots a'_i \dots a'_j \dots .$$

Keskitytään jatkossa tämän virheluokan käsittelyyn. Graafianalogian kautta tästä virheluokasta voidaan päätellä seuraavaa.

Lemma 8.5. *Mikään yhtä tarkistusmerkkiä käyttävä kaavaan 3.3 perustuva tarkistusmerkkijärjestelmä ei voi tunnistaa kaikkia kahden yksittäisvirheen tyyppistä virhettä.*

Todistus. Esitetään mahdolliset syötemerkkijonot graafina $R = (V, E)$. Tämä graafi sisältää solmut $\{\dots a_i \dots a_j \dots : a_i, a_j \in G\}$, jotka ovat kaikki keskenään yhdistettyjä viivoilla ja näitä solmuja on n^2 kappaletta. Siispä graafi R sisältää kokoa n^2 olevan täydellisen aligraafin. Tämä tarkoittaa sitä, että olisi löydettävä tarkistefunktio f, joka värittää kokoa n^2 olevan täydellisen

graafin hyvin käyttäen n:ää eri väriä, mikä on mahdotonta, sillä tähän tarvitaan n^2 väriä. □

Täydellinen kahden yksittäisvirheen tunnistaminen ei siis ole mahdollista, joten on luonnollista kysyä, kuinka permutaatio δ pitäisi valita, jotta saataisiin edes mahdollisimman hyvä kahden yksittäisvirheen tunnistamiskyky? Hieman merkillisesti osoittautuu, että permutaation δ valinnalla ei ole mitään väliä, sillä jokainen näistä toimii täsmälleen samalla tehokkuudella.

Lemma 8.6. *Olkoon G ryhmä, δ jokin sen permutaatio ja $x \in G$ jokin ryhmän G ennalta kiinnitetty alkio. Riippumatta permutaatiosta δ, kuvaus $f(a,b) := ax\delta(b)$ käy läpi kaikki ryhmän G n eri arvoa täsmälleen n kertaa, kun a ja b käyvät läpi kaikki alkiot ryhmässä G.*

Todistus. Koska permutaatiolla δ operoiminen sekä kiinnitetyllä alkiolla x kertominen ovat molemmat kuvauksina bijektioita, niin lauseke $x\delta(b)$ käy täsmälleen kerran läpi jokaisen ryhmän G alkion, kun b käy läpi ryhmän G alkiot. Siten $ax\delta(b) = aG$, jolloin jokaisella alkion a arvolla saadaan jokainen ryhmän G alkio täsmälleen kerran. □

Tämän lemman havaintona saadaan, että jokainen yhden tarkistusmerkin järjestelmä (G, δ) värittää kahden yksittäisvirheen tyyppisiä virheitä kuvaavan graafin kokoa n^2 olevan täydellisen aligraafin kaikilla väreillä "yhtä tasaisesti", eli käyttäen jokaista väriä n kertaa.

Lause 8.7. *Olkoon G ryhmä ja $|G| = n$. Jokainen kaavaan 3.3 perustuva ryhmän G tarkistusmerkkijärjestelmä, jossa syötemerkkijonon alkiot ovat ryhmästä G, tunnistaa täsmälleen $\frac{n}{n+1}$ osuuden kaikista kahden yksittäisvirheen tyyppisistä virheistä.*

Todistus. Tätä virheluokkaa kuvaava graafi on kokoa n^2 oleva täydellinen graafi ja edellisen lemman perusteella tiedetään, että jokainen tarkistusmerkkijärjestelmä värittää nämä n^2 solmua tasaisesti n eri värillä. Havaitsemattomat virheet ovat tämän graafin viivoja, joiden solmut ovat samanvärisiä. Nämä voidaan tarkalleen laskea. Graafissa on n^2 solmua ja jokaista solmua kohden on olemassa $n-1$ samanväristä solmua. Siten viivoja, joiden solmut ovat samanvärisiä on $\frac{n^2(n-1)}{2}$ kappaletta. Nimittäjässä esiintyy jakaja 2, koska muuten jokainen viiva laskettaisiin kahdesti, ensin järjestyksessä (a,b) ja sitten järjestyksessä (b,a).

Kokonaisuudessaan graafissa on $\binom{n^2}{2} = \frac{n^2(n^2-1)}{2}$ viivaa, joten kaikenkaikkiaan tarkistusmerkkijärjestelmä tunnistaa

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

kaikista kahden yksittäisvirheen tyyppisistä virheistä. □

Tämä tulos nähtiin kokeellisesti jo edellisessä kappaleessa esitetyn taulukon 7.3 kertalukua 10 olevien ryhmien kohdalta, joissa toistuvat luvut $\frac{10}{11} \approx 90.9\%$, sekä kertalukua 16 olevien ryhmien kohdalta, joiden kahden yksittäisvirheen tunnistuskyky on $\frac{16}{17} \approx 94.1\%$.

Yleisemmin täydellisen graafin värittämiselle on voimassa seuraava lemma.

Lemma 8.8. *Kokoa n olevalle täydelliselle graafille $G(V, E)$, joka väritetään mahdollisimman hyvin m:llä eri värillä, kun $m \mid n$, on voimassa yhtälö*

$$\frac{|O|}{|E|} = \frac{n(m-1)}{m(n-1)}.$$

Todistus. Tämän lauseen todistus etenee lähes kuten lauseessa 8.7. Koska graafi G on täydellinen, niin suurin määrä oikein väritettyjä viivoja saadaan, kun solmut väritetään tasaisesti jokaista väriä käyttäen. Tällöin jokaista väriä käytetään $\frac{n}{m}$ kertaa ja koska värejä on m kappaletta, niin väärin väritettyjä viivoja on yhteensä $|H| = m \cdot \binom{n/m}{2} = \frac{n(\frac{n}{m}-1)}{2}$ kappaletta. Tällöin

$$\frac{|O|}{|E|} = 1 - \frac{|H|}{|E|} = 1 - \frac{\frac{n(\frac{n}{m}-1)}{2}}{\frac{n(n-1)}{2}} = \frac{n(m-1)}{m(n-1)}$$

□

Edellisen ominaisuuden kannalta ei ole välttämätöntä, että $m|n$, mutta tämä oletus yksinkertaistaa saatua lauseketta huomattavasti. Tätä tulosta käytetään myöhemmin yleisemmän virheentunnistusrajan näyttämiseksi.

Graafien värityksen ja tarkistusmerkkijärjestelmien yhteyden esitteli tiettävästi ensimmäisenä R. Carvajal [55] vuoden 1974 artikkelissaan, jossa konstruoitiin kaikki yksittäis- ja vaihtovirheet tunnistava tarkistusmerkkijärjestelmä ryhmässä $\mathbb{Z}_k$, missä k on pariton tai erikoistapauksessa $k = 4$.

8.2 Useamman tarkistusmerkin järjestelmät

Mikään edellisessä luvussa vertailluista järjestelmistä ei kykene havaitsemaan kaikkia kahden yksittäisvirheen tyyppisiä virheitä, mikä on lauseen 8.7 myötä ymmärrettävää. Tarkistusmerkkijärjestelmiä konstruoitaessa ei ole pakko rajoittua käyttämään vain yhtä tarkistusmerkkiä, vaan käyttämällä kahta tai useampaa tarkistusmerkkiä voidaan yksittäisvirheitäkin myös tunnistaa useampia.

Yhden tarkistusmerkin järjestelmät voidaan laajentaa usean tarkistusmerkin järjestelmiksi monella eri tavalla. Konkreettisia esimerkkejä tällaisista järjestelmistä on esitelty muunmuassa Eckerin ja Pochin [18] sekä Schulzin [56] artikkeleissa. Määritellään seuraavaksi yleinen rakenne moninkertaiselle tarkistusmerkkijärjestelmälle käyttäen lähtökohtana tarkisteyhtälöä 3.4.

Määritelmä 8.9. *Olkoot kuvaukset $\delta_1, \delta_2, \ldots, \delta_k$ ryhmän G permutaatioita ja $a_1, \ldots, a_n$ tarkistusmerkkijärjestelmän syötejono. Tällöin määrätään tarkistusmerkit $b_1, \ldots, b_k$ siten, että*

$$\begin{aligned} b_1 &= a_1\delta_1(a_2)\delta_1^2(a_3)\ldots\delta_1^{n-1}(a_n), \\ b_2 &= a_1\delta_2(a_2)\delta_2^2(a_3)\ldots\delta_2^{n-1}(a_n), \\ &\ldots \\ b_k &= a_1\delta_k(a_2)\delta_k^2(a_3)\ldots\delta_k^{n-1}(a_n). \end{aligned}$$

Tällaista järjestelmää sanotaan k-kertaiseksi tarkistusmerkkijärjestelmäksi.

Lähetystä varten merkkijono kirjoitetaan jonossa $a_1a_2\ldots a_nb_1b_2\ldots b_k$. Huomaa, että tässä menetelmässä kaikki tarkistusmerkit $b_1, \ldots, b_k$ lasketaan toisistaan erillään. Vaihtoehtoisessa määritelmässä nämä termit voitaisiin ketjuttaa siten, että alkiota b_i laskettaessa otettaisiin huomioon alkiot $b_1, \ldots, b_{i-1}$, mutta tällaisen menettelyn käyttäminen havaittiin vaikeuttavan järjestelmän analyysia.

Määritelmän 8.9 mukaisesti menettelemällä voidaan rakentaa k-kertaisia tarkistusmerkkijärjestelmiä, jotka tunnistavat useampia merkkijonossa tapahtuvia yksittäisvirheitä. Siihen tarvitaan automorfismeja, joilla on seuraava ominaisuus.

Määritelmä 8.10. *Ryhmän G automorfismia δ sanotaan kiintopistevapaaksi, jos se kiinnittää vain ryhmän G identiteettialkion, eli jos ehdosta $\delta(x) = x, x \in G$ seuraa, että $x = e$.*

Kiintopistevapailla automorfismeilla on seuraava helposti havaittava ominaisuus.

Propositio 8.11. *Jos kiintopistevapaan automorfismin δ lyhimmän ei-triviaalin radan pituus on k, niin automorfismit $\delta^2, \delta^3, \ldots, \delta^{k-1}$ ovat myös kiintopistevapaita.*

□

Seuraavat kappaleet esittelevät näihin ominaisuuksiin pohjautuvia esimerkkikonstruktioita.

8.2.1 Kaksinkertainen 10/16 -järjestelmä

Rakennetaan ryhmään $\mathbb{Z}_2^4$ perustuva kaksinkertainen tarkistusmerkkijärjestelmä käyttäen yhtä ryhmän $\mathbb{Z}_2^4$ kiintopistevapaata automorfismia δ, jonka lyhimmän ei-triviaalin radan pituus on s. Rajoitetaan järjestelmässä käytettävien syötemerkkijonojen $a_1a_2\ldots a_n$ pituutta n ehdolla $n \leq s$. Valitaan edellä $\delta_1 := \delta$ ja $\delta_2 := \delta^2$. Tällöin saadaan kaksi tarkisteyhtälöä

$$b_1 = a_1 + \delta(a_2) + \delta^2(a_3) + \ldots + \delta^{n-1}(a_n) \text{ ja} \quad (8.1)$$

$$b_2 = a_1 + \delta^2(a_2) + \delta^4(a_3) + \ldots + \delta^{2n-2}(a_n). \quad (8.2)$$

Lause 8.12. *Olkoon G ryhmä, kuvaus δ sen kiintopistevapaa automorfismi ja s kuvauksen δ lyhimmän ei-triviaalin radan pituus. Jos syötemerkkijonon pituus n on rajattu mittaan $n \leq s$, niin yhtälöihin 8.1 ja 8.2 perustuva kaksinkertainen tarkistusmerkkijärjestelmä tunnistaa kaikki kahden yksittäisvirheen muutokset.*

Todistus. Yhtälöt 8.1 ja 8.2 yksinään toimivat kahtena yhden merkin tarkistusmerkkijärjestelmänä, joten luonnollisesti yksi yksittäisvirhe tunnistetaan riippumatta siitä, tapahtuuko se missä tahansa merkissä a_i, b_1 tai b_2. Voidaan siis keskittyä kahden yksittäisvirheen tarkasteluun, joissa molempien merkkien muutos on oleellinen.

Jos merkissä b_1 tapahtui muutos, niin yhtälössä 8.2 on tällöin voinut muuttua vain yksi merkki. Silloin tämä yhtälö tunnistaa virheen, sillä se tunnistaa kaikki yhden merkin muutokset. Vastaavasti, jos merkissä b_2 tapahtui muutos, niin yhtälössä 8.1 on tällöin tapahtunut vain yhden merkin virhe, joka tunnistetaan.

Voidaan siis olettaa, että on tapahtunut muutokset $a_i \rightsquigarrow a_i', a_i \neq a_i'$ ja $a_j \rightsquigarrow a_j', a_j \neq a_j', i \neq j$. Jos nämä muutokset jäisivät tunnistamatta, niin se tarkoittaisi, että

$$\begin{aligned}
a_1 + \ldots + \delta^{i-1}(a_i) + \ldots + \quad & \delta^{j-1}(a_j) \quad + \ldots + \delta^{n-1}(a_n) = \\
a_1 + \ldots + \delta^{i-1}(a_i') + \ldots + \quad & \delta^{j-1}(a_j') \quad + \ldots + \delta^{n-1}(a_n) \text{ ja} \\
a_1 + \ldots + \delta^{2i-2}(a_i) + \ldots + \quad & \delta^{2j-2}(a_j) \quad + \ldots + \delta^{2n-2}(a_n) = \\
a_1 + \ldots + \delta^{2i-2}(a_i') + \ldots + \quad & \delta^{2j-2}(a_j') \quad + \ldots + \delta^{2n-2}(a_n),
\end{aligned}$$

tai yhtäpitävästi

$$\begin{aligned}
\delta^{i-1}(a_i) + \delta^{j-1}(a_j) &= \delta^{i-1}(a_i') + \delta^{j-1}(a_j') \quad \text{sekä} \\
\delta^{2i-2}(a_i) + \delta^{2j-2}(a_j) &= \delta^{2i-2}(a_i') + \delta^{2j-2}(a_j').
\end{aligned}$$

Tehdään merkinnät $x := a_i - a_i'$ ja $y := a_j - a_j'$, jolloin saadaan yhtälöt

$$\begin{aligned}
\delta^{i-1}(x) &= \delta^{j-1}(y) \quad \text{ja} \\
\delta^{2i-2}(x) &= \delta^{2j-2}(y).
\end{aligned}$$

Näistä voidaan ratkaista muuttuja x ja saadaan

$$\delta^{j-i}(y) = \delta^{2j-2i}(y),$$

mikä tarkoittaa, että kuvaus δ^{j-i} kiinnittää alkion $a_j - a_j'$, mutta koska $j - i \leq n - 1 \leq s - 1 < s$, niin δ^{j-i} on kiintopistevapaa automorfismi ja kiinnittää vain ryhmän $\mathbb{Z}_2^4$ identiteettialkion. Tästä seuraisi, että $a_j = a_j'$, mikä ei ole mahdollista.

Siten yhtälöihin 8.1 ja 8.2 perustuva kaksinkertainen tarkistusmerkkijärjestelmä tunnistaa kaikki syötejonossa tapahtuvat kahden merkin muutokset. □

Huomaa, että edellisessä todistuksessa itse asiassa on oleellisempaa, että $s \nmid j - i$, eli että se indeksien etäisyys, jossa kaksi virhettä tapahtuvat, ei saa olla minkään automorfismin δ radan pituuden monikerta. Vertaa tätä ominaisuutta lauseeseen 7.3.

Tässä järjestelmässä merkkijonon pituuden rajoitus $n \leq s$ määrää järjestelmän käytännöllisyyden, joten on tärkeää valita automorfismi, jolle luku s on mahdollisimman suuri. Ryhmässä $\mathbb{Z}_2^4$ tällaisia ovat esimerkiksi kappaleessa 7.2.1 esitetyt automorfismit P ja Q sekä kappaleessa 7.2.2 esitetyt automorfismit δ_1, δ_2 ja δ_3. Kaikkien näiden automorfismien kertaluku on 15 ja koska ne kaikki koostuvat yhdestä 15:n alkion mittaisesta ei-triviaalista syklistä, niin näitä käytettäessä $s = 15$. Kappaleessa 7.2.3 esitetty automorfismi θ on kertalukua 31 ja koostuu myöskin vain yhdestä ei-triviaalista syklistä, joten sille $s = 31$. Nämä valinnat ovat parhaita mahdollisia kyseisissä ryhmissä, sillä $|\mathbb{Z}_2^4| = 16$ ja $|\mathbb{Z}_2^5| = 32$.

8.2.2 Kolminkertainen 10/16 -järjestelmä

Muokataan edellisen kappaleen konstruktiota seuraavasti. Käytetään kahden tarkisteyhtälön sijasta kolmea ja lasketaan alkiot b_1, b_2 ja b_3 kaavoilla

$$b_1 = a_1 + \delta(a_2) + \delta^2(a_3) + \ldots + \delta^{n-1}(a_n), \tag{8.3}$$
$$b_2 = a_1 + \delta^2(a_2) + \delta^4(a_3) + \ldots + \delta^{2n-2}(a_n), \tag{8.4}$$
$$b_3 = a_1 + \delta^3(a_2) + \delta^6(a_3) + \ldots + \delta^{3n-3}(a_n). \tag{8.5}$$

Tällä järjestelmällä voidaan tunnistaa syötteessä tapahtuvat kolme yksittäisvirhettä.

Lause 8.13. *Olkoon G ryhmä, kuvaus δ sen kiintopistevapaa automorfismi ja s kuvauksen δ lyhimmän ei-triviaalin radan pituus. Jos syötemerkkijonon pituus n on rajattu mittaan $n \leq s$, niin yhtälöihin 8.3-8.5 perustuva tarkistusmerkkijärjestelmä tunnistaa kolme syötteessä tapahtuvaa yksittäisvirhettä.*

Todistus. Jos syötteessä tapahtuu kaksi tai vähemmän yksittäisvirhettä, niin lauseen 8.12 nojalla nämä virheet tunnistetaan. Jos yksi virheistä on tapahtunut alkiossa b_1, niin yhtälöissä 8.4 ja 8.5 on tällöin tapahtunut vain kaksi virhettä, jolloin lausetta 8.12 voidaan taas soveltaa. Samaa päättelyä voidaan soveltaa, jos virhe on tapahtunut alkiossa b_2 tai b_3.

Voidaan siis olettaa, että kaikki kolme virhettä ovat tapahtuneet alkioissa $a_i \rightsquigarrow a_i', a_j \rightsquigarrow a_j'$ ja $a_k \rightsquigarrow a_k'$, missä $i \neq j, j \neq k, k \neq i, a_i \neq a_i', a_j \neq a_j'$ ja $a_k \neq a_k'$.

Tällöin jos virhe jäisi tunnistamatta, täytyy olla voimassa seuraavat yhtälöt:

$$\begin{aligned} a_i + \delta^{j-i}(a_j) + \delta^{k-i}(a_k) &= a_i' + \delta^{j-i}(a_j') + \delta^{k-i}(a_k'), \\ a_i + \delta^{2(j-i)}(a_j) + \delta^{2(k-i)}(a_k) &= a_i' + \delta^{2(j-i)}(a_j') + \delta^{2(k-i)}(a_k') \quad \text{ja} \\ a_i + \delta^{3(j-i)}(a_j) + \delta^{3(k-i)}(a_k) &= a_i' + \delta^{3(j-i)}(a_j') + \delta^{3(k-i)}(a_k'), \end{aligned}$$

mistä saadaan muotoiltua ehdot

$$\begin{aligned}\delta^{j-i}(a'_j - a_j) + \delta^{k-i}(a'_k - a_k) &= \\ \delta^{2(j-i)}(a'_j - a_j) + \delta^{2(k-i)}(a'_k - a_k) &= \\ \delta^{3(j-i)}(a'_j - a_j) + \delta^{3(k-i)}(a'_k - a_k).&\end{aligned}$$

Merkitään $x := a'_j - a_j$ ja $y := a'_k - a_k$, ja käsitellään ensimmäistä ja toista yhtälöä erikseen sekä poistetaan automorfismin δ operoinnit, jolloin saadaan

$$\begin{aligned} x + \delta^{k-j}(y) &= \delta^{j-i}(x) + \delta^{2k-j-i}(y) \text{ ja} \\ x + \delta^{2(k-j)}(y) &= \delta^{j-i}(x) + \delta^{3k-2j-i}(y), \end{aligned}$$

josta yhdistelemällä samanmuotoiset termit vasemmalle puolelle saadaan ehto

$$\delta^{3k-2j-i}(y) - \delta^{2(k-j)}(y) = \delta^{2k-j-i}(y) - \delta^{k-j}(y).$$

Tämä yhtälö sievenee muotoon

$$\delta^{k-j}\big(\delta^{k-i}(y) - y\big) = \delta^{k-i}(y) - y.$$

Siispä automorfismi δ^{k-j} kiinnittää alkion $\delta^{k-i}(y) - y$, mikä on mahdollista vain, jos $\delta^{k-i}(y) - y = e$, sillä $k-j \leq n-1 < s$. Siten $\delta^{k-i}(y) = y$, mutta tämä on mahdotonta, koska myös $k-i < s$. Siten tämä tarkistusmerkkijärjestelmä tunnistaa kolme syötteessä tapahtuvaa yksittäisvirhettä. □

Edellisen lauseen todistus on jo hieman mittava ja nelinkertaisen tai sitä vahvemman järjestelmän varmuutta on vielä työläämpi todistaa. Tällaisten järjestelmien toimivuutta kokeiltiin tietokonepohjaisesti käytännössä ja tulokset tukevat seuraavaa teoriaa.

Propositio 8.14. *Olkoon G ryhmä, kuvaus δ sen kiintopistevapaa automorfismi ja s kuvauksen δ lyhimmän ei-triviaalin radan pituus. Jos syötemerkkijonon pituus n on rajattu mittaan $n \leq s$, niin käyttämällä tarkisteyhtälöryhmää*

$$\begin{aligned} b_1 &= a_1 + \delta(a_2) + \delta^2(a_3) + \ldots + \delta^{n-1}(a_n), \\ b_2 &= a_1 + \delta^2(a_2) + \delta^4(a_3) + \ldots + \delta^{2(n-1)}(a_n), \\ b_3 &= a_1 + \delta^3(a_2) + \delta^6(a_3) + \ldots + \delta^{3(n-1)}(a_n), \\ &\ldots \\ b_k &= a_1 + \delta^k(a_2) + \delta^{2k}(a_3) + \ldots + \delta^{k(n-1)}(a_n), \end{aligned}$$

missä $k < s$, havaitaan kaikki syötemerkkijonon muutokset

$$a_1 a_2 \ldots a_n b_1 b_2 \ldots b_k \rightsquigarrow a'_1 a'_2 \ldots a'_n b'_1 b'_2 \ldots b'_k,$$

kunhan näiden kahden merkkijonon Hammingin etäisyys on korkeintaan k.

□

Yllä on syytä tehdä rajoitus $k < s$, koska muuten voisi olla $\delta^s = id$, minkä jälkeen sama tarkisteyhtälö alkaisi toistaa itseään, kun $\delta^{s+1} = \delta$.

Moninkertaisille tarkistusmerkkijärjestelmille voidaan lemmasta 8.8 päätellä seuraavaa.

Lause 8.15. *Olkoon (G, δ) l-kertainen tarkistusmerkkijärjestelmä, jonka syötemerkkijonoissa käytetään vain osajoukkoa $S \subseteq G$ ryhmästä G, mutta jonka tarkistusmerkit saavat olla mitä tahansa ryhmän G alkioita. Merkitään $|G| = n, |S| = m$. Tällöin (G, δ) havaitsee syötemerkkijonossa korkeintaan Hamming-etäisyydeltään $k \in \mathbb{Z}_+$ tapahtuvista virheistä osuuden*

$$\frac{m^k(n^l - 1)}{n^l(m^k - 1)}, \text{ olettaen, että } m^k \mid n^l.$$

Todistus. Syötemerkkijonon virheet, jotka tapahtuvat Hamming-etäisyydellä k muodostavat kokoa m^k olevan täydellisen graafin. Tarkistusmerkkijärjestelmän tarkistusfunktion on väritettävä tämä graafi n^l eri värillä. Lemma 8.8 kertoo, kuinka tämä väritys on tehtävä ja se antaa myös oikein väritettyjen viivojen lukumäärän. Sijoittamalla tähän kaavaan $n \leftarrow m^k$ ja $m \leftarrow n^l$, saadaan virheentunnistukselle lauseessa väitetty muoto. □

Kirjallisuutta

[1] M. Niemenmaa, *(80033A) Algebra.* Oulun yliopistopaino, 2004.

[2] M. Niemenmaa, *(80043A) Algebra 2.* Oulun yliopistopaino, 1998.

[3] S. Lang, *Algebra.* Springer-Verlag, 3rd ed., 2005.

[4] J. Rotman, *An Introduction to the Theory of Groups.* Springer, 4th ed., 1994.

[5] M. Niemenmaa, *(80060S) Ryhmäteoria.* Oulun yliopistopaino, 1997.

[6] ISO, *ISO 2108:1978. Documentation – International standard book numbering (ISBN)*, 1978.

[7] R.-H. Schulz, "On check digit systems using anti-symmetric mappings," *Numbers, Information and Complexity*, pp. 295–310, Helmikuu 2000.

[8] International ISBN Agency, Berlin, *ISBN Users' Manual*, 5th ed., 2005.

[9] Oikeusministeriö, *Valtioneuvoston asetus yritys- ja yhteisötietojärjestelmästä 29.3.2001/288*, Maaliskuu 2001.

[10] Verohallinto, *Arvonlisäverotunniste (Alv-numero, Vat number) ja sen käyttö, Julkaisu 200.10*, Tammikuu 2010.

[11] Väestörekisterikeskus, "Henkilötunnus." Internet-julkaisu, 2006. Haettu 19.8.2010. http://www.intermin.fi/vrk/home.nsf/wLatest/2575C011A439C3ACC22571FB00248CA2.

[12] European Committee for Banking Standards, *EBS204. IBAN: International Bank Account Number v3.2*, Elokuu 2003.

[13] International Civil Aviation Organization, *ICAO Doc 9303. Machine Readable Travel Documents. Part 1. Machine Readable Passports.*, 6th ed., 2006.

[14] International Civil Aviation Organization, *ICAO Doc 9303. Machine Readable Travel Documents. Part 2. Machine Readable Visas.*, 6th ed., 2006.

[15] ISO/IEC, *International Standard ISO/IEC 7812*, Syyskuu 2009.

[16] J. Verhoeff, *Error detecting decimal codes*, vol. 29. Math. Centre Tracts, 1969.

[17] D. F. Beckley, "An optimum system with modulus 11," *The Computer Bulletin*, vol. 11, pp. 213–215, 1967.

[18] A. Ecker and G. Poch, "Check character systems," *Computing*, vol. 37, no. 4, pp. 277–301, 1986.

[19] F. J. Damerau, "A technique for computer detection and correction of spelling errors," *Commun. ACM*, vol. 7, no. 3, pp. 171–176, 1964.

[20] J. A. Gallian and M. D. Mullin, "Groups wih anti-symmetric mappings," *Archiv der Mathematik*, vol. 65, pp. 273–280, Lokakuu 1995.

[21] L. J. Paige, "A note on finite abelian groups," *Bulletin of the American Mathematical Society*, vol. 53, no. 6, pp. 590–593, 1947.

[22] H. B. Mann, "The construction of orthogonal latin squares," *The Annals of Mathematical Statistics*, vol. 13, pp. 418–423, Joulukuu 1942.

[23] P. T. Bateman, "A remark on infinite groups," *The American Mathematical Monthly*, vol. 57, no. 9, pp. 623–624, 1950.

[24] M. Hall and L. J. Paige, "Complete mappings of finite groups," *Pacific Journal of Mathematics*, vol. 5, no. 4, pp. 541–549, 1955.

[25] L. J. Paige, "Complete mappings of finite groups," *Pacific Journal of Mathematics*, vol. 1, no. 1, pp. 111–116, 1951.

[26] M. Vaughan-Lee and I. Wanless, "Latin squares and the hall-paige conjecture," *Bulletin London Mathematical Society*, vol. 35, pp. 191–195, Maaliskuu 2003.

[27] S. Wilcox, "Reduction of the hall-paige conjecture to sporadic simple groups," *Journal of Algebra*, vol. 321, no. 5, pp. 1407 – 1428, 2009.

[28] R. L. Daniel Gorenstein and R. Solomon, *The Classification of the Finite Simple Groups*. American Mathematical Society, 1994.

[29] A. B. Evans, "The admissibility of sporadic simple groups," *Journal of Algebra*, vol. 321, no. 1, pp. 105 – 116, 2009.

[30] H. J. Zassenhaus, *The Theory of Groups*. Dover Publications, 2 ed., 1999.

[31] S. Heiss, "Antisymmetric mappings for finite solvable groups," *Archiv der Mathematik*, vol. 69, pp. 445–454, Joulukuu 1997.

[32] R.-H. Schulz, "Check character systems and anti-symmetric mappings," pp. 136–147, 2001.

[33] G. Belyavskaya and A. Diordiev, "On check character systems over groups.," 2004.

[34] G. B. Belyavskaya, V. I. Izbash, and V. A. Shcherbacov, "Check character systems over quasigroups and loops.," *Quasigroups Relat. Syst.*, vol. 10, pp. 1–28, 2003.

[35] S. Heiss, "Antisymmetric mappings for finite groups." 1999.

[36] R.-H. Schulz, "Yksityinen sähköpostikeskustelu," Elokuu 2010.

[37] S. Giese, "Äquivalenz von prüfzeichensystemen am beispiel der diedergruppe d_5. (theoretische und algorithmische behandlung). staatsexamenarbeit.," Tammikuu 1999.

[38] S. Ugan, "Prüfzeichensysteme über dizyklischen gruppen der ordnung 8 und 12," Master's thesis, FU Berlin, FB Mathematik und Informatik, 1999.

[39] R.-H. Schulz, "Equivalence of check digit systems over the dicyclic groups of order 8 and 12," 1999.

[40] R. Sedgewick, *Algorithms*. Addison-Wesley Publishing Company, 1st ed., 1984.

[41] D. E. Knuth, *The Art of Computer Programming, Volume 4, Fascicle 2: Generating All Tuples and Permutations (Art of Computer Programming)*. Boston, MA, USA: Addison-Wesley Professional, 2005.

[42] H. M. Damm, "Prüfziffersysteme über quasigruppen," Master's thesis, Fachbereich Mathematik und Informatik der Philipps-Universität Marburg, Maaliskuu 1998.

[43] J. Marshall Hall, "A combinatorial problem on abelian groups," *Proceedings of the American Mathematical Society*, vol. 3, pp. 584–587, Elokuu 1952.

[44] T. H. Cormen, C. Stein, R. L. Rivest, and C. E. Leiserson, *Introduction to Algorithms*. McGraw-Hill Higher Education, 2001.

[45] Finanssialan keskusliitto, Bulevardi 28, 00120 Helsinki, *Kotimaisen viitenumeron rakenneohje 1.11.2009*, Marraskuu 2009.

[46] H. P. Luhn, "Us patent 2950048. computer for verifying numbers," tech. rep., United States Patent and Trademark Office, 1954.

[47] Finanssialan keskusliitto, Bulevardi 28, 00120 Helsinki, *Suomalaisten tilinumeroiden rakenne ja tarkiste 1.11.2009*, Marraskuu 2009.

[48] 3GPP, *3GPP TS 23.003 v9.3.0. Numbering, addressing and identification*, Kesäkuu 2010.

[49] International Telecommunication Union, *ITU-T Rec. E.118. The international telecommunication charge card*, Toukokuu 2006.

[50] ISO/IEC, *International Standard ISO/IEC 7064*, 1st ed., Helmikuu 2003.

[51] "Banknotes.com." Internet-sivusto. Viitattu 14.1.2011.

[52] D. H. Joseph Gallian and S. Kennedy, "Math on money," *The Edge of the Universe: Celebrating Ten Years of Math Horizons*, pp. 38–39, 2006.

[53] *SNOMED CT Technical Reference Guide*, Tammikuu 2010.

[54] M. Niemenmaa, "A check digit system for hexadecimal numbers." Ilmestyy lehdessä Applicable Algebra in Engineering, Communication and Computing., 2010.

[55] P. Carvajal, "Modulus k check digits and the chromatic number problem," in *IFIP Congress*, pp. 521–523, 1974.

[56] R.-H. Schulz, "Check character systems over groups and orthogonal latin squares," *Applicable Algebra in Engineering, Communication and Computing*, pp. 125–132, 1996.

Liite A

Permutaatioiden listaus

Seuraavaa ohjelmakoodi toteuttaa B.R. Heapin algoritmin [41, pp. 49-52], jota voidaan käyttää yleisenä aliohjelmana kulkemaan kaikkien valittua kokoa olevien permutaatioden läpi nopeasti tietyt alipermutaatiot karsien.

```
/** Represents a fixed-size permutation of numbers
    [0, Size-1].*/
class Permutation
{
private:
   std::vector<int> image;

public:
   Permutation(){}
   Permutation(int size)
   {
      SetIdentity(size);
   }

   int Size() const { return image.size(); }

   /// Sets this permutation to the identity,
   /// [0  1  2  ...  Size-1]
   void SetIdentity(int size)
   {
      image.clear();
      image.reserve(size);
      for(int i = 0; i < size; ++i)
         image.push_back(i);
   }

   /// Helper structure that saves information about
```

```
/// the permutation's traversal state.
struct Traversal
{
   /// The factoradic number of the last-visited
   /// permutation.
   std::vector<int> c;
};

/// Starts a new traversal, the first permutation to
/// visit is the identity.
void BeginTraversal(Traversal &t)
{
   SetIdentity(Size());
   t.c.clear();
   t.c.reserve(Size());
   for(int i = 0; i < Size(); ++i)
      t.c.push_back(0);
}

/// Gets the next permutation where the first #change
/// items are not all the same.
/// @return The index of the smallest changed
///   element, or -1 if no permutation.
int NextPermutation(Traversal &t, int change)
{
   assert(change > 0);

   int k = 1;
   while(t.c[k-1] >= k)
   {
      t.c[k-1] = 0;
      ++k;
      if (k >= Size())
      {
         BeginTraversal(t);
         return -1;
      }
   }
   ++t.c[k-1];

   for(int i = 1; i < k; ++i)
      swap(image[Size()-1 - i], image[Size()-1]);
   swap(image[Size()-1 - k],
        image[Size()-1 - (k+1-t.c[k-1])]);
```

```
      swap(image[Size()-1 - k],
           image[Size()-1 - (k-t.c[k-1])]);

      int m = Size()-1-k;
      if (m < change || change <= 0)
         return m;

      k = 1;
      while(k < Size())
      {
         if (Size()-1-k < change)
         {
            return Size()-1-k;
         }
         else // skip this suffix
         {
            while(t.c[k-1] >= k)
            {
               // apply sigma-1
               swap(image[Size()-1 - k], image[Size()-1]);

               t.c[k-1] = 0;
               ++k;
               if (k >= Size())
               {
                  BeginTraversal(t);
                  return -1;
               }
            }
            ++t.c[k-1];

            // apply tau
            swap(image[Size()-1 - k],
                 image[Size()-1 - (k+1-t.c[k-1])]);
            swap(image[Size()-1 - k],
                 image[Size()-1 - (k-t.c[k-1])]);
         }
      }
      return 0;
   }
};
```

Liite B

Täydellisten kuvausten konstruointi

Tässä liitteessä esitetty ohjelma toteuttaa Eckerin ja Pochin algoritmin 6.2, joka konstruoi täydellisiä kuvauksia Abelin ryhmästä.

```
class CompleteMap
{
private:
   QuasiGroup g;
   Permutation a;
   Permutation b;
   int numSolved;

public:
   explicit CompleteMap(QuasiGroup &group)
   :g(group) {}

   bool IsInSolvedRange(int e)
   {
      for(int i = 0; i < numSolved; ++i)
         if (g.Mul(a[i], b[i]) == e)
            return true;

      return false;
   }

   int FindNextIndexWithImage(int i, int e)
   {
      for(i = i+1; i < numSolved; ++i)
         if (g.Mul(a[i], b[i]) == e)
            return i;
```

```
   return -1;
}

bool Step1()
{
   for(int i = numSolved; i < g.NumElems(); ++i)
      for(int j = numSolved; j < g.NumElems(); ++j)
         if (!IsInSolvedRange(g.Mul(a[i], b[j])))
         {
            a.Swap(numSolved, i);
            b.Swap(numSolved, j);
            ++numSolved;
            return true;
         }
   return false;
}

bool Step2()
{
   for(int i = numSolved; i < g.NumElems(); ++i)
   {
      int j = FindNextIndexWithImage(-1, g.Mul(a[i], b[i]));
      while(j != -1)
      {
         for(int k = numSolved; k < g.NumElems(); ++k)
            if (k != i)
            {
               if (!IsInSolvedRange(g.Mul(a[j], b[k])))
               {
                  b.Swap(j, k);
                  a.Swap(numSolved, i);
                  b.Swap(numSolved, i);
                  ++numSolved;
                  return true;
               }
               if (!IsInSolvedRange(g.Mul(a[k], b[j])))
               {
                  a.Swap(j, k);
                  a.Swap(numSolved, i);
                  b.Swap(numSolved, i);
                  ++numSolved;
                  return true;
               }
            }
```

```
            j = FindNextIndexWithImage(j, g.Mul(a[i], b[i]));
         }
      }
      return false;
   }

   void RepeatStep1()
   {
      bool success = true;
      while(success)
         success = Step1();
   }

   void RepeatStep2()
   {
      bool success = true;
      while(success)
         success = Step2();
   }

   void RepeatStep3()
   {
      bool success = true;
      while(success)
         success = Step3();
   }

   bool Pivot(int e, int nPivoted)
   {
      for(int i = nPivoted; i < numSolved; ++i)
         if (g.Mul(a[i], b[i]) == e)
         {
            a.Swap(i, nPivoted);
            b.Swap(i, nPivoted);
            return true;
         }
      return false;
   }

   bool Step3()
   {
      if (numSolved+1 >= g.NumElems())
         return false;
```

```
    int nPivoted = 0;
    int e = g.Mul(a[numSolved], b[numSolved]);
    bool success = Pivot(e, nPivoted++);
    while(success)
    {
       if (nPivoted == 1)
          e = g.Mul(a[0], b[numSolved+1]);
       else
          e = g.Mul(a[nPivoted-1], b[nPivoted-2]);
       success = Pivot(e, nPivoted);
       if (success)
          ++nPivoted;
       if (nPivoted > numSolved)
          return false;
    }
    int bLast = b[nPivoted-1];
    for(int i = nPivoted-1; i > 0; --i)
       b[i] = b[i-1];
    b[0] = b[numSolved+1];
    b[numSolved+1] = bLast;
    ++numSolved;
    return true;
}

/// Starts from a random input permutation
/// and builds a complete map of it.
Permutation FindRandomCompleteMap(LCG &lcg)
{
    a.SetToRandom(lcg, g.NumElems());
    b.SetToRandom(lcg, g.NumElems());
    numSolved = 0;

    int nSolved = numSolved-1;
    while(nSolved != numSolved && numSolved < g.NumElems())
    {
       nSolved = numSolved;
       RepeatStep1();
       RepeatStep2();
       RepeatStep1();
       RepeatStep3();
    }

    Permutation final;
```

```
      final.SetIdentity(g.NumElems());
      for(int i = 0; i < g.NumElems(); ++i)
         final[a[i]] = b[i];

      if (numSolved == g.NumElems()-1)
      {
         ++numSolved;
         if (!IsSolvedRangeValid())
            --numSolved;
      }
      return final;
   }

   void PrintBar(int d, char c)
   {
      cout << "     ";
      for(int i = 0; i < d; ++i)
         cout << "   ";
      cout << c << endl;
   }

   void Print()
   {
      PrintBar(numSolved, '|');
      cout << "a: " << a << endl;
      cout << "b: " << b << endl;
      Permutation c;
      c.SetIdentity(g.NumElems());
      for(int i = 0; i < g.NumElems(); ++i)
         c[i] = g.Mul(a[i], b[i]);
      cout << "c: " << c << endl;
      cout << endl;
   }
};
```