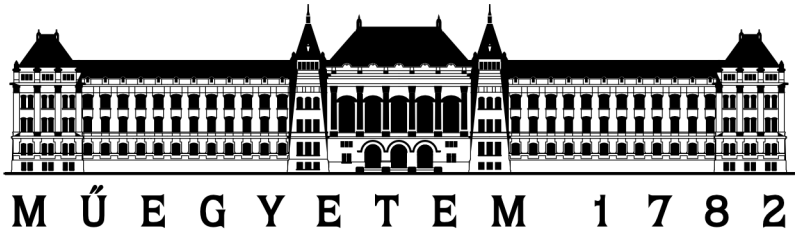


TDK DOLGOZAT

A Pauli-csoport és Veldkamp-egyenesei kombinatorikus megközelítésben

Szabó Zsolt

Konzulens: Dr. Lévay Péter
Tudományos főmunkatárs
BME Fizika Intézet
Elméleti Fizika Tanszék

BME

2016. november 2.

Tartalomjegyzék

1. Bevezetés

A kvantummechanika nemkontextuális rejtett-paraméter elméleteit kizáró konfigurációk iránt folyamatos az érdeklődés. Ez különösen igaz a Pauli-csoportból pont-egyenes geometriaként előbukkanó konfigurációkra, amelyek közül a legismertebbek a Mermin-négyzetek és a Mermin-pentagrammák [6].

Az ilyen konfigurációknak a vizsgálata során gyakran adódnak olyan esetek, amikor valamilyen $\{1, ..., n\}$ halmaznak a k-elemű részhalmazai bukkannak elő; lásd pl. [5]. A dolgozatban az eddigi módszereink és a kényelmes kombinatorikus módszerek kapcsolatának a matematikai hátterét szeretném tisztázni. Ebben a fizikusak által kevésbé ismert Veldkamp-egyenesek fontos szerepet kapnak. A kombinatorikus megközelítés nem teljesen új, de valamiért mégsem terjedt el a témával foglalkozó fizikusok között, pedig nyilvánvaló előnyei miatt jelentősen megkönnyíti a vizsgálódást, főleg ha viszonylag sok qubittel kell dolgoznunk.

Szeretnék köszönetet mondani *a családomnak* a megértésért és hogy megteremtik a lehetőséget, hogy a tudománnyal foglalkozhassak, *Vrana Péternek* a bírálói feladat elvállalásáért, végezetül pedig *Lévay Péter* konzulensemnek a kitartásáért és a támogatásáért.

2. A Pauli-csoport szimplektikus struktúrája

Ez a szakasz többnyire az [5] munkából merít, az egyes részek viszonylag kevés módosítással lettek átvéve; lásd még [4]. Tehát az ismertetett gondolatok nem újak, viszont a teljesség miatt itt kell lenniük, és az új megközelítéssel is érdemes őket összehasonlítani.

Egy véges dimenziós $\mathcal{H}$ Hilbert-tér által leírt kvantum rendszer *megfigyelhető mennyiségeit* a $\mathcal{H}$-n értelmezett önadjungált operátorok reprezentálják. Egy rögzített $\mathcal{H}$-beli bázisban minden ilyen operátornak a mátrixa hermitikus. Kétállapotú kvantum rendszer, vagy elterjedtebb nevén: *qubit* esetén 2×2-es mátrixokról van szó, és az általuk kifeszített vektortérnek egy bázisa $\{I, X, Z, Y\}$. Itt I a 2×2 egységmátrix, és X, Z és Y a három *Pauli spin mátrix*, melyek definíciója

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Y = \mathrm{i}XZ = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}. \tag{2.1}$$

A továbbiakban egy N darab qubitből álló kvantum rendszer megfigyelhető mennyiségei közül azok lesznek érdekesek, amelyek mátrixai az I, X, Z és Y mátrixok N-szeres Kronecker-szorzatai. Ezeket a $2^N \times 2^N$-es mátrixokat N-*qubit*

Pauli-operátoroknak hívom, és legtöbbször a kifejezésükből elhagyom a „$\otimes$” jelet, például $X \otimes I \otimes Z$ helyett csak annyit írok, hogy XIZ.

Az N-qubit Pauli-operátorok által generált csoport

$$\mathcal{P}_N = \{sA_1A_2...A_N |\, s = \pm 1, \pm \mathrm{i},\ A_i = I, X, Z, Y\}\,, \tag{2.2}$$

és ennek a neve: *N-qubit Pauli-csoport*. $\mathcal{P}_N$ centruma

$$Z(\mathcal{P}_N) = \{sI_N |\, s = \pm 1, \pm \mathrm{i}\} \tag{2.3}$$

ahol I_N a $2^N \times 2^N$-es egységmátrix. $Z(\mathcal{P}_N)$ megegyezik $\mathcal{P}_N$-nek a $[\mathcal{P}_N, \mathcal{P}_N]$ kommutátor-részcsoportjával, ezért a $\mathcal{P}_N/Z(\mathcal{P}_N)$ faktorcsoport Abel-féle. Ismert, hogy $\mathcal{P}_N/Z(\mathcal{P}_N)$ elemei

$$\{sA_1A_2...A_N |\, s = \pm 1, \pm \mathrm{i}\} \tag{2.4}$$

alakú ekvivalenciaosztályok. Mindegyik osztályból reprezentánsnak az $A_1A_2...A_N$ Pauli-operátort célszerű kiválasztani.

Következő lépésként nézzük $\mathcal{P}_N$ a szimplektikus vektortér struktúráját. (2.1) alapján, egy tetszőleges $A = sA_1...A_N \in \mathcal{P}_N$ csoportelem úgy írható, hogy

$$A = s\, \left(\mathrm{i}^{\sum_i a_i b_i}\right)^{-1} X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_N} Z^{b_N}, \tag{2.5}$$

ahol az X, illetve Z mátrixok kitevői 0 vagy 1 értéket vehetnek fel, és az i kitevőjében szereplő szumma a természetes számok $\mathbb{N}$ halmazán értelmezett szummát jelenti. (2.5) azt mutatja, hogy a

$$(s, a_1, ..., a_N, b_1, ..., b_N) \tag{2.6}$$

rendezett $2N+1$-es egyértelműen azonosítja az A csoportelemet. A $2N+1$-es első elemét, azaz s-et elhagyva egy

$$\boldsymbol{x} = (a_1, ..., a_N, b_1, ..., b_N) \in \mathbb{Z}_2^{2N} \tag{2.7}$$

vektor adódik. Ez az $\boldsymbol{x}$ vektor az $A_1...A_N$ Pauli-operátort azonosítja, így azonosítja az $A_1...A_N$-et tartalmazó $\mathcal{P}_N/Z(\mathcal{P}_N)$-beli ekvivalenciaosztályt is. Az utóbbit jelölje $(\boldsymbol{x})$. Gyakran a vektorokat, amilyen (2.7) is, szemléletesebb N-qubit Pauli-operátorokként kiírni 0-k és 1-ek $2N$ hosszú sorozata helyett. Például, a (2.5) formulával összhangban, $(1, 1, 0, 0, 1, 1)$ ekvivalens azzal, hogy XYZ.

Az X és Z Pauli-mátrixok teljesítik azt, hogy

$$ZX = -XZ \qquad \text{és} \qquad X^2 = Z^2 = I. \tag{2.8}$$

Emiatt, az $A, A' \in \mathcal{P}_N$ mátrixok AA' szorzatára (2.6) úgy néz ki, hogy

$$\left(ss' \, (-1)^{\sum_i a'_i b_i}, a_1 + a'_1, ..., b_N + b'_N\right), \tag{2.9}$$

ahol „+" a modulo 2 összeadást jelenti, ami nem más, mint a $\mathbb{Z}_2$-beli összeadás. A (2.9) formulából látszik, hogy *a $\mathcal{P}_N/Z(\mathcal{P}_N)$-beli csoportszorzás a $\mathbb{Z}_2^{2N}$-beli vektorösszeadást indukálja*: ha $A \in (\boldsymbol{x})$ és $A' \in (\boldsymbol{x}')$,

$$AA' \in (\boldsymbol{x} + \boldsymbol{x}'). \tag{2.10}$$

A (2.9) formulából az is látszik, hogy A és A' akkor és csak akkor kommutál, ha

$$\sum_{i=1}^{N} (a_i b'_i - a'_i b_i) = 0 \mod 2, \tag{2.11}$$

ellenkező esetben a két mátrix antikommutál. (2.11) bal oldala egy nemdegenerált, ferdén szimmetrikus bilineáris formát indukál a $\mathbb{Z}_2^{2N}$ vektortéren[1]:

$$\langle \cdot, \cdot \rangle : \mathbb{Z}_2^{2N} \times \mathbb{Z}_2^{2N} \to \mathbb{Z}_2, \qquad \langle \boldsymbol{x}, \boldsymbol{x}' \rangle = \sum_{i=1}^{N} (a_i b'_i + b_i a'_i) \tag{2.12}$$

Általánosan, egy nemdegenerált, ferdén szimmetrikus bilineáris formát *szimplektikus formának*, és egy ilyennel ellátott vektorteret *szimplektikus vektortérnek* hívnak. Tehát a $\mathbb{Z}_2^{2N}$ vektortér a (2.12) szimplektikus formával ellátva egy $\mathbb{Z}_2$ feletti szimplektikus vektorteret alkot, amit a továbbiakban V_N jelöl.

$\langle \cdot, \cdot \rangle$ azt jelenti, hogy ha adottak az $(\boldsymbol{x}), (\boldsymbol{x}') \in \mathcal{P}_N/Z(\mathcal{P}_N)$ ekvivalenciaosztályok, ahol $\boldsymbol{x}, \boldsymbol{x}' \in V_N$, egy tetszőleges $A \in (\boldsymbol{x})$ mátrix akkor és csak akkor kommutál egy tetszőleges $A' \in (\boldsymbol{x}')$ mátrixszal, ha $\langle \boldsymbol{x}, \boldsymbol{x}' \rangle = 0$, azaz, ha $\boldsymbol{x}$ és $\boldsymbol{x}'$ ortogonálisak.

Egy $\boldsymbol{y}$ vektorra ortogonális $\boldsymbol{x}$ vektorok halmazát $\boldsymbol{y}$ *perp-halmazának* hívom, és $C_{\boldsymbol{y}}$-nal jelölöm. $C_{\boldsymbol{y}}$ a V_N-t $\mathbb{Z}_2$-re képező $\boldsymbol{x} \mapsto \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ lineáris függvény magtere, emiatt, nemnulla $\boldsymbol{y}$ esetén, V_N-nek egy $2N-1$-dimenziós altere. $|C_{\boldsymbol{y}}|$ konkrét értékei megtalálhatók a C Függelékben.

3. Kvadratikus formák és kvadratikus felületek

Egy szimplektikus forma, például (2.12), a $Q : V_N \to \mathbb{Z}_2$ kvadratikus formához *asszociált bilineáris forma*, ha minden $\boldsymbol{x}, \boldsymbol{x}' \in V_N$-re teljesül, hogy

$$\langle \boldsymbol{x}, \boldsymbol{x}' \rangle = Q(\boldsymbol{x}) + Q(\boldsymbol{x}') + Q(\boldsymbol{x} + \boldsymbol{x}'). \tag{3.1}$$

[1] Emlékeztető: $-1 = +1 \mod 2$, vagyis $\mathbb{Z}_2$-ben. Emiatt a ferde szimmetria is szimmetriára redukálódik.

Ha (3.1) teljesül Q-ra, akkor az alábbi kvadratikus formára is teljesül:

$$Q_{\boldsymbol{y}}(\boldsymbol{x}) = Q(\boldsymbol{x}) + \langle \boldsymbol{x}, \boldsymbol{y} \rangle^2, \qquad \boldsymbol{y} \in V_N. \tag{3.2}$$

Mivel $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}_2$, a négyzetreemelés elhagyható.

3.1. Lemma. *Az $\boldsymbol{y} \mapsto Q_{\boldsymbol{y}}$ leképezés egy bijekció V_N és a (3.1) tulajdonságot kielégítő kvadratikus formák halmaza között.*

Bizonyítás. Ha egy Q' kvadratikus formára (3.1) igaz,

$$Q(\boldsymbol{x} + \boldsymbol{x}') + Q'(\boldsymbol{x} + \boldsymbol{x}') = Q(\boldsymbol{x}) + Q'(\boldsymbol{x}) + Q(\boldsymbol{x}') + Q'(\boldsymbol{x}'). \tag{3.3}$$

Ez azt sugallja, hogy érdemes a

$$\varphi : V_N \to \mathbb{Z}_2, \qquad \varphi(\boldsymbol{x}) = Q(\boldsymbol{x}) + Q'(\boldsymbol{x}), \tag{3.4}$$

vizsgálni, amely $Q \neq Q'$ esetén nemtriviális, és valamely nemnulla $\boldsymbol{y}$ vektorra $\varphi(\boldsymbol{x}) = \langle \boldsymbol{x}, \boldsymbol{y} \rangle$. Ezt behelyettesítve a (3.4) formulába adódik, hogy $Q' = Q_{\boldsymbol{y}}$. Nyilvánvalóan, $Q' = Q$ a $\mathbf{o}$ nullvektor képe az $\boldsymbol{y} \mapsto Q_{\boldsymbol{y}}$ leképezés szerint. □

A Q kvadratikus forma egy H *kvadratikus felületet* határoz meg, ami nem más, mint a $Q(\boldsymbol{x}) = 0$ egyenletet kielégítő $\boldsymbol{x}$ vektorok halmaza. (3.1) átrendezésével és (3.2) alkalmazásával adódik, hogy

$$Q_{\boldsymbol{y}}(\boldsymbol{x}) = Q(\boldsymbol{y}) + Q(\boldsymbol{x} + \boldsymbol{y}). \tag{3.5}$$

Ebből következik, hogy a $Q_{\boldsymbol{y}}$ által meghatározott $H_{\boldsymbol{y}}$ kvadratikus felület így írható:

$$H_{\boldsymbol{y}} = \begin{cases} \boldsymbol{y} + H & \text{ha } \boldsymbol{y} \in H, \\ \overline{\boldsymbol{y} + H} & \text{ha } \boldsymbol{y} \notin H. \end{cases} \tag{3.6}$$

Itt $\overline{S}$ az $S \subseteq V_N$ vektorhalmaz V_N-re vett komplementere, és

$$\boldsymbol{y} + S = \{\boldsymbol{y} + \boldsymbol{x} |\, \boldsymbol{x} \in S\}. \tag{3.7}$$

Az $S \mapsto \overline{S}$ és $S \mapsto \boldsymbol{y} + S$ függvények egymással felcserélhető involúciók, emellett

$$|\overline{S}| = 4^N - |S| \qquad \text{és} \qquad |\boldsymbol{y} + S| = |S|. \tag{3.8}$$

Mivel $Q(\boldsymbol{y}) = Q_{\boldsymbol{y}}(\boldsymbol{y})$, ami miatt $\boldsymbol{y} \in H \Leftrightarrow \boldsymbol{y} \in H_{\boldsymbol{y}}$, H kifejezhető úgy, hogy

$$H = \begin{cases} \boldsymbol{y} + H_{\boldsymbol{y}} & \text{ha } \boldsymbol{y} \in H_{\boldsymbol{y}}, \\ \overline{\boldsymbol{y} + H_{\boldsymbol{y}}} & \text{ha } \boldsymbol{y} \notin H_{\boldsymbol{y}}. \end{cases} \tag{3.9}$$

A 3.1. lemmából és a (3.6) és (3.8) formulákból következik, hogy számosság szerint osztályozva legfeljebb két típusú kvadratikus felület létezik. Az alábbiakban egy robusztusabb osztályozást fogalmazok meg, és ehhez felhasználom a maximális, páronként ortogonális vektorhalmazok, azaz a *Lagrange-alterek* fogalmát. Végül ki fog derülni, hogy a két osztályozás ekvivalens.

Mindenekelőtt bevezetek néhány fogalmat. Jelölje $W^\perp$ azoknak a vektoroknak az alterét, amelyek a W altér minden vektorára ortogonálisak:

$$W^\perp = \{\boldsymbol{x} | \, W \leq C_{\boldsymbol{x}}\}\,. \tag{3.10}$$

W *izotróp*, ha $W \subseteq W^\perp$, azaz ha a vektorai páronként ortogonálisak, és *Lagrange-altér*, ha $W^\perp = W$. A szimplektikus forma nemdegeneráltsága miatt

$$\dim W + \dim W^\perp = \dim V_N = 2N, \tag{3.11}$$

következésképpen minden Lagrange-altér N-dimenziós.

Tegyük fel, hogy H a Q kvadratikus forma által meghatározott kvadratikus felület, és $U \subseteq H$ egy Lagrange-altér. Legyen $\boldsymbol{y} \notin U$, és legyen φ az $\boldsymbol{x} \mapsto \langle \boldsymbol{x}, \boldsymbol{y}\rangle$ leképezés U-ra vett megszorítása. Mivel $\boldsymbol{y}$ nemnulla és U maximális izotróp, φ nemtriviális, így a magtere,

$$\ker \varphi = U \cap C_{\boldsymbol{y}} \leq U, \tag{3.12}$$

egy $N-1$-dimenziós izotróp altér. Minden $\boldsymbol{x} \in U \setminus C_{\boldsymbol{y}}$-ra (3.1) úgy alakul, hogy

$$Q(\boldsymbol{x}+\boldsymbol{y}) = \underbrace{Q(\boldsymbol{x})}_{=0} + Q(\boldsymbol{y}) + \underbrace{\langle \boldsymbol{x}, \boldsymbol{y}\rangle}_{=1} = 1 + Q(\boldsymbol{y}). \tag{3.13}$$

Ezért minden $\boldsymbol{y} \notin H$-hoz tartozik 2^{N-1} darab $\boldsymbol{x}+\boldsymbol{y} \in H \setminus U$ vektor, és minden $\boldsymbol{y} \in H \setminus U$-hoz tartozik 2^{N-1} darab $\boldsymbol{x}+\boldsymbol{y} \notin H$ vektor. Mivel $U \subseteq H \subseteq V_N$, ebből következik, hogy

$$\underbrace{|V_N| - |H|}_{=|V_N \setminus H|} = \underbrace{|H| - |U|}_{=|H \setminus U|}\,. \tag{3.14}$$

Átrendezve és behelyettesítve az ismert számosságokat adódik, hogy

$$|H| = \frac{1}{2}(|V_N| + |U|) = \frac{1}{2}(2^{2N} + 2^N) = 2^{N-1}(2^N + 1). \tag{3.15}$$

Tekintsük ismét a H kvadratikus formát és az $U \subseteq H$ Lagrange-alteret. Legyen $\boldsymbol{y} \in H$. Ha $\boldsymbol{y} \in U$, mivel $\boldsymbol{y} + U = U$, $U \subseteq H_{\boldsymbol{y}}$. Ha $\boldsymbol{y} \notin U$, az $\boldsymbol{y}$ vektor és az $U \cap C_{\boldsymbol{y}}$ izotróp altér egy $\boldsymbol{y}$-t tartalmazó U' Lagrange-alteret feszít ki. Mint előbb,

$U' \subseteq H_{\boldsymbol{y}}$. Tehát, *ha* $\boldsymbol{y} \in H$, *létezik* $U' \subseteq H_{\boldsymbol{y}}$ *Lagrange-altér.* Az előző bekezdés eredményéből, de a (3.6) és (3.15) formulákból is következik, hogy

$$|H_{\boldsymbol{y}}| = 2^{N-1}(2^N + 1). \tag{3.16}$$

Továbbá, ha $\boldsymbol{z} \notin H$, egyetlen Lagrange-altér sem lehet $H_{\boldsymbol{z}}$ részhalmaza, mivel

$$|H_{\boldsymbol{z}}| = 2^{N-1}(2^N - 1). \tag{3.17}$$

Mindezekből az a következtetés vonható le, hogy *egy* H *kvadratikus felületnek valamely Lagrange-altér a részhalmaza akkor és csak akkor, ha* $|H| = 2^{N-1}(2^N+1)$. Ha az utóbbi igaz, a H kvadratikus felület *hiperbolikus*, különben *elliptikus*. A hiperbolikus, illetve az elliptikus felületeken lévő vektorok számát (3.16), illetve (3.17) adja meg. Konkrét értékek a C Függelékben találhatók.

Nem téveszthető szem elől, hogy a fenti megállapítás a H kvadratikus felület és az $U \subseteq H$ Lagrange-altér létezéséből következett. Többek közt a kételyek eloszlatása céljából is érdemes megvizsgálni egy olyan Q_0 kvadratikus formát, amely a Pauli-operátorok szimmetriájával van kapcsolatban [4].

Egy $(\boldsymbol{x}) \in \mathcal{P}_N/Z(\mathcal{P}_N)$ ekvivalenciaosztály négy, egyszerre szimmetrikus vagy antiszimmetrikus mátrixot tartalmaz. Mivel I, X és Z szimmetrikusak, és Y antiszimmetrikus, az $(\boldsymbol{x})$-beli mátrixok szimmetriája attól függ, hogy a reprezentáns Pauli-operátor tenzorszorzat alakjában lévő Y-ok száma páros vagy páratlan. Ezért, ha az összeget modulo 2 összegként értelmezzük, i kitevője a (2.5) formulában a négy mátrix szimmetriáját tükrözi. A kitevő a (3.1) tulajdonságot kielégítő Q_0 kvadratikus formát határozza meg:

$$Q_0 : V_N \to \mathbb{Z}_2, \qquad Q_0(\boldsymbol{x}) = \sum_{i=1}^{N} a_i b_i. \tag{3.18}$$

A fentiek értelmében az $(\boldsymbol{x})$ ekvivalenciaosztály akkor és csak akkor tartalmaz szimmetrikus mátrixokat, ha $Q_0(\boldsymbol{x}) = 0$.

A H_0 kvadratikus felület hiperbolikus, mivel tartalmazza az összes

$$\boldsymbol{x} = (a_1, ..., a_N, 0, ..., 0), \qquad a_i \in \mathbb{Z}_2 \tag{3.19}$$

alakú vektort, és ezek egy $U \subseteq H_0$ Lagrange-alteret feszítenek ki. A vektorokhoz tartozó $(\boldsymbol{x})$ ekvivalenciaosztályok elemeinek az alakja:

$$sX^{a_1} \otimes \cdots \otimes X^{a_N}, \qquad s = \pm 1, \pm \mathrm{i}. \tag{3.20}$$

Tehát, ha V_N szimplektikus formáját a $\mathcal{P}_N$-beli kommutációs relációk indukálják[2], $\mathcal{P}_N/Z(\mathcal{P}_N)$ *szerkezete garantálja*, hogy létezik olyan H kvadratikus felület, amelyhez létezik $U \subseteq H$ Lagrange-altér; ez a kvadratikus felületek osztályozásához kell. Hogy ez működjön, V_N és $\mathcal{P}_N/Z(\mathcal{P}_N)$ között alkalmas megfeleltetési szabályokra van szükség; a (2.5) és (2.7) formulák által leírt szabály ilyen.

4. Geometriák és geometriai hipersíkok

A pont-egyenes geometriák fogalmának az ismertetése elött összefoglalok néhány halmazelméleti eredményt. Legyen X egy nemüres halmaz. Egy $A \subseteq X$ halmaz *karakterisztikus függvényét* úgy definiálom, hogy

$$\chi_A : X \to \mathbb{Z}_2, \qquad \chi_A(x) = \begin{cases} 0 & \text{ha } x \in A, \\ 1 & \text{ha } x \notin A. \end{cases} \tag{4.1}$$

Például, a 3. szakaszban a Q kvadratikus forma a H felület karakterisztikus függvénye. Az X halmaz 2^X hatványhalmazán értelmezett halmazelméleti relációk és műveletek karakterisztikus függvényekkel az alábbi módon fejezhetők ki:

$$\overline{A}: \qquad \chi_{\overline{A}} = 1 + \chi_A, \tag{4.2a}$$
$$A \cup B: \qquad \chi_{A\cup B} = \chi_A \chi_B, \tag{4.2b}$$
$$A \cap B: \qquad \chi_{A\cap B} = \chi_A + \chi_B + \chi_A\chi_B, \tag{4.2c}$$
$$A \triangle B: \qquad \chi_{A\triangle B} = 1 + \chi_A + \chi_B, \tag{4.2d}$$
$$A \subseteq B: \qquad \chi_A\chi_B = \chi_B. \tag{4.2e}$$

2^X-en értelmezhető egy újabb függvény, amit [8] szerzői *Veldkamp-összegnek* hívnak:

$$A * B = \overline{A \triangle B} \qquad\qquad \chi_{A*B} = \chi_A + \chi_B. \tag{4.2f}$$

A második formulából látszik, hogy bármely $x \in X$ az A, B és $A * B$ halmazok közül vagy mind a háromban benne van, vagy pontosan az egyikben van benne. Ez X-nek egy felosztását határozza meg. Következésképpen, egyrészt,

$$A \cap B = A \cap (A * B) = B \cap (A * B) = A \cap B \cap (A * B), \tag{4.3}$$

másrészt pedig

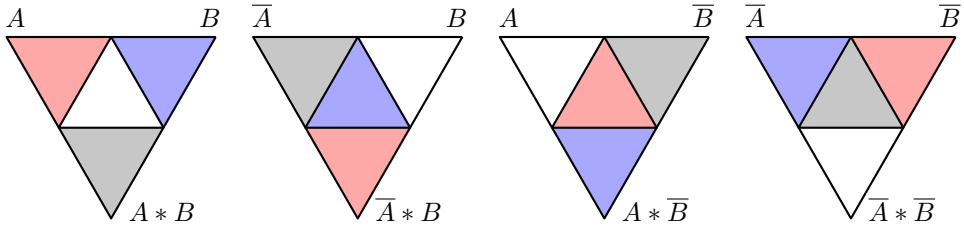
$$|A| + |B| + |A * B| = |X| + 2|A \cap B|. \tag{4.4}$$

[2]Lásd a 2. szakasz végét.

Ha $A, B \neq X$, $A \cap B \neq \emptyset$, és sem $A \subseteq B$, sem $B \subseteq A$ nem teljesül, a

$$A, B, A * B, \qquad \overline{A}, B, \overline{A} * B, \qquad A, \overline{B}, A * \overline{B}, \qquad \overline{A}, \overline{B}, \overline{A} * \overline{B} \tag{4.5}$$

vektor-hármasok X-nek ugyanazt a felosztását adják. A három halmaz metszetét *magnak* nevezem. Például, as első hármas esetében a mag $A \cap B$. A 4.1. ábra a felosztást és az osztályok szerepét mutatja mindegyik esetre. A színek az osztályokat azonosítják, a középső háromszögek pedig a magokat reprezentálják.



4.1. ábra. X-nek a Veldkamp-összeggel kapcsolatos felosztása

A továbbiakban két, $\mathbb{Z}_2$ feletti, 2^X alaphalmazú vektorteret fogok vizsgálni. Az első $(2^X, \triangle)$; ebben a vektorösszeg a $\triangle$ szimmetrikus differencia, és $\emptyset$ a nullvektor. A második $(2^X, *)$; ebben a vektorösszeg a $*$ Veldkamp-összeg, és X a nullvektor. Mi több, $A \mapsto \overline{A}$ egy bijektív lineáris leképezés a két vektortér között, ugyanis

$$\overline{A * B} = A \triangle B = \overline{A} \triangle \overline{B}. \tag{4.6}$$

Egy *pont-egyenes geometria*[3] egy $\Gamma = (P, L, I)$ hármas, ahol P a *pontok halmaza*, L az *egyenesek halmaza* és $I \subseteq P \times L$ az *incidenciareláció*. Egy $p \in P$ pont és egy $l \in L$ egyenes *illeszkedését* pIl fejezi ki. Az l egyenessel illeszkedő pontok $I(l)$ halmaza az l *pont-árnyéka*[4], és a p ponttal illeszkedő egyenesek $I(p)$ halmaza a p *egyenes-árnyéka*[5], amit *sugársornak*[6], is neveznek.

Egy pont-egyenes geometriában a következő axiómák teljesülnek:

1. *nincsenek kettőzött egyenesek*, azaz nincs két különböző l és k egyenes, amelyekre $I(l) = I(k)$. Emiatt minden l egyenes az $I(l)$ pont-árnyékával ekvivalens, és az L egyenesek halmaza 2^P részhalmazaként tekinthető. pIl tehát ugyanazt jelenti, mint $p \in l$.

2. minden $l \in L$-re $|l| \geq 2$.

[3] Az angol nyelvű elnevezések: *point-line geometry* [10] és *line space* [1].
[4] Angol nyelvű elnevezés: *point-shadow*.
[5] Angol nyelvű elnevezés: *line-shadow*.
[6] Angol nyelvű elnevezés: *pencil of lines centered at p*.

Két vagy több pont *kollineáris*, ha valamely $l \in L$ egyenessel mind illeszkednek, és *páronként kollineárisak*, ha bármely kettő közűlük kollineáris, de az összesükkel egyetlen $l \in L$ sem illeszkedik. Egy $p \in P$-vel kollineáris pontok halmazát, amelyet esetenként p *perp-halmazának* is neveznek [8], $p^\perp$ jelöli.

Az $A \subseteq P$ *által kifeszített* pont-egyenes geometria $\Gamma(A) = (A, L(A), \in)$, ahol

$$L(A) = \{l \cap A |\, l \in L,\ |l \cap A| \geq 2\}\,. \tag{4.7}$$

$\Gamma(A)$, vagy csak A, Γ-nak egy *altere*, ha $L(A) \subseteq P$, azaz, ha minden $l \in L$-re $|l \cap A| \geq 2$-ből következik, hogy $l \in L(A)$, és ennek megfelelően $l \subseteq A$. Γ-nak egy H *geometriai hipersíkja* egy (valódi) $H \neq P$ altere, amelyre minden $l \in L$ esetén igaz, hogy $l \cap H \neq \emptyset$. Vagyis minden $l \in L$ vagy egy pontban metszi H-t, vagy H-nak a részhalmaza.

Értelmezem az alábbi függvényt L-en:

$$\gamma_A : L \to \mathbb{Z}_2, \qquad \gamma_A(l) = \begin{cases} 0 & \text{ha } l \text{ egy pontban metszi } A\text{-t vagy } l \subseteq A, \\ 1 & \text{egyébként.} \end{cases} \tag{4.8}$$

Szemléletesen, $\gamma_A(l) = 1$ azt jelenti, hogy l „útjában áll" A-nak, hogy az geometriai hipersík legyen. γ_A egy $\lambda(A)$ egyeneshalmaz karakterisztikus függvénye, ami egy

$$\lambda : 2^P \to 2^L, \qquad \lambda(A) = \{l \in L |\, \gamma_A(l) = 0\} \tag{4.9}$$

leképezést definiál. Triviálisan, $\lambda(P) = L$ és $\lambda(\emptyset) = \emptyset$, és Γ minden H geometriai hipersíkjára $\lambda(H) = L$. Ha egy $A \neq P$ ponthalmazra és egy K egyeneshalmazra $K \subseteq \lambda(A)$ teljesül, A *egy geometriai hipersík* K*-ra nézve.*

Tegyük fel, hogy Γ minden egyenesével pontosan három pont illeszkedik, és ennek megfelelően az egyenesek $\{x, y, z\}$ alakúak. Ebben a speciális esetben γ_A úgy írható, hogy

$$\gamma_A(l) = \chi_A(x) + \chi_A(y) + \chi_A(z), \tag{4.10}$$

és könnyű belátni, hogy teljesülnek az alábbi relációk:

$$\lambda(\overline{A}) = \overline{\lambda(A)}, \tag{4.11a}$$

$$\lambda(A * B) = \lambda(A) * \lambda(B), \tag{4.11b}$$

$$\lambda(A \triangle B) = \lambda(A) \triangle \lambda(B). \tag{4.11c}$$

(4.11b), illetve (4.11c) alapján következik, hogy $\lambda : (2^P, *) \to (2^L, *)$, illetve $\lambda : (2^P, \triangle) \to (2^L, \triangle)$ lineáris leképezések. Az egyértelműség céljából az alábbi jelöléseket használom:

$$\ker_* \lambda = \{A \subseteq P |\, \lambda(A) = L\}\,, \qquad \ker_\triangle \lambda = \{A \subseteq P |\, \lambda(A) = \emptyset\}\,. \tag{4.12}$$

λ képtere esetén ez a probléma nem merül fel:

$$\lambda(2^P) \leq (2^L, *) \qquad \text{és} \qquad \lambda(2^P) \leq (2^L, \triangle). \tag{4.13}$$

Mivel a $\{p\}$ egyelemű halmazok bázist alkotnak $(2^P, \triangle)$-ban, az $I(p) = \lambda(\{p\})$ sugársorok halmaza $\lambda(2^P)$ bázisa $(2^L, \triangle)$-ban. Emellett, az $A \mapsto \overline{A}$ leképezés bijektív és lineáris $(2^P, \Delta)$ és $(2^P, *)$ között, valamint $(2^L, \Delta)$ és $(2^L, *)$ között. Következik, hogy a $\overline{\{p\}}$ szingleton-komplementerek halmaza $(2^P, *)$ bázisa, és az $\overline{I(p)}$ sugársor-komplementerek halmaza $\lambda(2^P)$ bázisa $(2^L, *)$-ban.

5. Az N-qubit Pauli-csoport Veldkamp-tere

Mivel ebben a szakaszban csak speciális esetek lesznek érintve, a *Veldkamp-tér* fogalma a következőképpen definiálható[7]. Legyen $\mathcal{H}$ egy $\Gamma = (P, L, I)$ pont-egyenes geometria geometriai hipersíkjainak a halmaza, és legyen $\mathcal{H}_2$ azoknak a $H_1 \cap H_2$, $H_1, H_2 \in \mathcal{H}$ metszeteknek a halmaza, amelyekre teljesül, hogy

$$H_1 \cap H_2 \subseteq H \;\Rightarrow\; H_1 \cap H_2 = H \cap H_1 = H \cap H_2, \qquad \forall H \in \mathcal{H}. \tag{5.1}$$

Γ *Veldkamp-tere* a $(\mathcal{H}, \mathcal{H}_2, \supseteq)$ pont-egyenes geometria, és ennek a pontjait, illetve egyeneseit *Veldkamp-pontoknak*, illetve *Veldkamp-egyeneseknek* nevezik.

Feltételezem, hogy $H_1 \subseteq H_2$ semelyik $H_1, H_2 \in \mathcal{H}$-ra sem teljesül, és minden $H_1 \cap H_2 \in \mathcal{H}_2$ metszetre és p pontra *egyértelműen* létezik $H \in \mathcal{H}$ úgy, hogy $p \in H$ és $H_1 \cap H_2 \subseteq H$. Így minden Veldkamp-egyenes P-nek egy felosztását határozza meg, amelynek $H_1 \cap H_2$ egy osztálya. Az utóbbit *magnak* nevezem.

Ha $\mathcal{V} = \mathcal{H} \cup \{P\}$ zárt a $*$ Veldkamp-összegre, a Veldkamp-egyenesek halmaza egybeesik a $(\mathcal{V}, *)$ vektortér projektív egyeneseinek a halmazával. Ez azt jelenti, hogy minden $H_1, H_2 \in \mathcal{H}$-ra létezik egy Veldkamp-egyenes

$$\{H_1, H_2, H_1 * H_2\} \tag{5.2}$$

pont-árnyékkal, és más Veldkamp-egyenesek nincsenek.

Ezek után legyen $\mathcal{G}_N = (P, L, \in)$ az a pont-egyenes geometria, amelynek a pontjai, illetve az egyenesei V_N nemnulla vektorai, illetve projektív egyenesei. Az utóbbiak

$$l = \{\boldsymbol{x}, \boldsymbol{x}', \boldsymbol{x} + \boldsymbol{x}'\}, \qquad \boldsymbol{x} \neq \boldsymbol{x}', \qquad \boldsymbol{x}, \boldsymbol{x}' \in V_N \setminus \{\mathbf{o}\} \tag{5.3}$$

[7] Az Olvasó a teljes elméletet, az itteni feltételezések szükséges feltételeivel együtt, megtalálja az [1] vagy [10] műben. Ahogy [8] szerzői is kiemelik, [1] definíciói [10] definícióinál kevésbé korlátozók.

alakú halmazok. Mivel V_N-ből, és ennek megfelelően a $\mathcal{P}_N$ N-qubit Pauli-csoportból bukkan elő, $\mathcal{G}_N$-t $\mathcal{P}_N$ *pont-egyenes geometriájának* hívom.

Mivel három kollineáris vektor páronként ortogonális vagy páronként nemortogonális, *izotróp* és *hiperbólikus* egyenesek különböztethetők meg. Például, a fenti l egyenes $\langle \boldsymbol{x}, \boldsymbol{x}' \rangle = 0$ esetén izotróp, különben hiperbólikus. Az izotróp, illetve hiperbólikus egyenesek halmazát jelölje L_{iso}, illetve L_{hyp}. Természetesen, $L_{\mathrm{hyp}} = \overline{L}_{\mathrm{iso}}$, és ez fordítva is igaz.

Tekintsük a

$$\{\emptyset, L_{\mathrm{iso}}, L_{\mathrm{hyp}}, L\} \leq (2^L, *) \tag{5.4}$$

lineáris altér ősképét:

$$\mathcal{V} = \lambda^{-1}\{\emptyset, L_{\mathrm{iso}}, L_{\mathrm{hyp}}, L\} \leq (2^P, *), \tag{5.5}$$

ahol λ a (4.9) formulával definiált leképezés. Mivel $\mathcal{V}$ zárt $*$-ra, felépíthető belőle egy $\mathcal{V}_N$ pont-egyenes geometria, amelynek a ponthalmaza $\mathcal{V} \setminus \{P\}$, és az egyenesei $(\mathcal{V}, *)$ projektív egyenesei. Annak ellenére, hogy az így kapott $\mathcal{V}_N$-nek csak bizonyos pontjai geometriai hipersíkjai $\mathcal{G}_N$-nek, a tömörség kedvéért[8] $\mathcal{V}_N$-t $\mathcal{P}_N$ *Veldkamp-terének*, egyeneseit pedig $\mathcal{P}_N$ *Veldkamp-egyeneseinek* fogom hívni.

Leghamarabb a $\mathcal{V}$-beli ponthalmazokat határozom meg. Először is, egy $\lambda(A) = L$-et teljesítő $A \in \mathcal{V}$ halmaz χ_A karakterisztikus függvényére igaz, hogy

$$\chi_A(\boldsymbol{x}) + \chi_A(\boldsymbol{x}') + \chi_A(\boldsymbol{x} + \boldsymbol{x}') = 0, \qquad \boldsymbol{x}, \boldsymbol{x}' \in P = V_N \setminus \{\mathbf{o}\}. \tag{5.6}$$

Ebből látszik, hogy χ_A egy lineáris leképezés, és emiatt valamely[9] $\boldsymbol{y} \in V_N$-re

$$\chi_A(\boldsymbol{x}) = \langle \boldsymbol{x}, \boldsymbol{y} \rangle. \tag{5.7}$$

Következésképpen, $A = C_{\boldsymbol{y}}$. Másodszor, ha $\lambda(A) = L_{\mathrm{iso}}$,

$$\chi_A(\boldsymbol{x}) + \chi_A(\boldsymbol{x}') + \chi_A(\boldsymbol{x} + \boldsymbol{x}') = \langle \boldsymbol{x}, \boldsymbol{x}' \rangle, \qquad \boldsymbol{x}, \boldsymbol{x}' \in P. \tag{5.8}$$

$\boldsymbol{x}'$ helyébe $\boldsymbol{x}$-et helyettesítve adódik, hogy $\chi_A(\mathbf{o}) = 0$. Így χ_A egy, a (3.1) összefüggést kielégítő kvadratikus forma, és A az általa megadott kvadratikus felület. Harmadszor, (4.11a) alapján, ha $\lambda(A) = L_{\mathrm{hyp}}$, valamely H kvadratikus felületre $A = \overline{H}$. Végül, szintén (4.11a) alapján, ha $\lambda(A) = \emptyset$, valamely $\boldsymbol{y} \in V_N$-re $A = \overline{C}_{\boldsymbol{y}}$. Mivel ezeknek az állításoknak a fordítottja is igaz, $\lambda^{-1}(L)$, $\lambda^{-1}(L_{\mathrm{iso}})$, $\lambda^{-1}(L_{\mathrm{hyp}})$, *illetve* $\lambda^{-1}(\emptyset)$ *a perp-halmazok halmazával, a kvadratikus felületek halmazával, a kvadratikusfelület-komplementerek halmazával, illetve a perp-halmaz-komplementerek halmazával esik egybe.*

[8] A hasonlóságok ellenére ez a definíció *jelentősen* eltér a Veldkamp-tereknek és a Veldkamp-egyeneseknek [1] és [10] művekben található definícióitól.

[9] Vegyük észre, hogy $\boldsymbol{y} = \mathbf{o}$ *lehetséges*, mivel $\boldsymbol{y}$ most nem $\mathcal{G}_N$ pontjaként szerepel.

Ezután $\mathcal{P}_N$ Veldkamp-egyeneseit határozom meg. Mivel ezek $(\mathcal{V}, *)$ projektív egyenesei, és (5.2) alakúak, ehhez elég lesz a $\mathcal{V}$-beli $*$ vektorösszeadás szabályait lefektetni. (4.2f) és a szimplektikus forma bilinearitása alapján[10],

$$C_{\boldsymbol{x}} * C_{\boldsymbol{y}} = C_{\boldsymbol{x}+\boldsymbol{y}}. \tag{5.9}$$

Hasonlóképpen, (3.2) és (4.2f) összehasonlításából,

$$H_{\mathbf{o}} * C_{\boldsymbol{y}} = H_{\boldsymbol{y}}. \tag{5.10}$$

$H_{\mathbf{o}}$ egy önkényesen kiválasztott kvadratikus felület, például az, amelyet a Pauli-operátorok szimmetriája definiál (3. szakasz). Így a $*$-ra vonatkozó szabályok:

$$\begin{aligned} C_{\boldsymbol{x}} * C_{\boldsymbol{y}} = H_{\boldsymbol{x}} * H_{\boldsymbol{y}} = \overline{C}_{\boldsymbol{x}} * \overline{C}_{\boldsymbol{y}} = \overline{H}_{\boldsymbol{x}} * \overline{H}_{\boldsymbol{y}} = C_{\boldsymbol{x}+\boldsymbol{y}}, \\ C_{\boldsymbol{x}} * \overline{C}_{\boldsymbol{y}} = H_{\boldsymbol{x}} * \overline{H}_{\boldsymbol{y}} = \overline{C}_{\boldsymbol{x}+\boldsymbol{y}}. \end{aligned} \tag{5.11}$$

Ebből látszik, hogy $\lambda^{-1}(L_{\text{iso}})$, $\lambda^{-1}(L_{\text{hyp}})$ és $\lambda^{-1}(\emptyset)$ a

$$\ker{}_* \lambda = \lambda^{-1}(L) \tag{5.12}$$

altér három mellékosztálya $\mathcal{V}$-ben. Aszerint, hogy hogyan metszik ezt a négy halmazt, a Veldkamp-egyenesek öt típusba sorolhatók, és ezek reprezentánsai

$$\begin{aligned} &\{C_{\boldsymbol{x}}, C_{\boldsymbol{y}}, C_{\boldsymbol{x}+\boldsymbol{y}}\}, \quad \{H_{\boldsymbol{x}}, H_{\boldsymbol{y}}, C_{\boldsymbol{x}+\boldsymbol{y}}\}, \quad \{H_{\boldsymbol{x}}, \overline{H}_{\boldsymbol{y}}, \overline{C}_{\boldsymbol{x}+\boldsymbol{y}}\}, \\ &\{\overline{C}_{\boldsymbol{x}}, \overline{C}_{\boldsymbol{y}}, C_{\boldsymbol{x}+\boldsymbol{y}}\}, \quad \{\overline{H}_{\boldsymbol{x}}, \overline{H}_{\boldsymbol{y}}, C_{\boldsymbol{x}+\boldsymbol{y}}\} \end{aligned} \tag{5.13}$$

alakúak. $\lambda^{-1}(L_{\text{iso}})$ és $\lambda^{-1}(L_{\text{hyp}})$ a kvadratikus felületek típusa szerint tovább bontható (3. szakasz), és a kvadratikus felületeket is tartalmazó Veldkamp-egyenesek altípusokba sorolhatók. A későbbiekben részletesen tárgyalt altípusok:

$$\{H^+_{\boldsymbol{x}}, H^+_{\boldsymbol{y}}, C_{\boldsymbol{x}+\boldsymbol{y}}\}, \qquad \{H^-_{\boldsymbol{x}}, H^-_{\boldsymbol{y}}, C_{\boldsymbol{x}+\boldsymbol{y}}\}, \qquad \{H^+_{\boldsymbol{x}}, H^-_{\boldsymbol{y}}, C_{\boldsymbol{x}+\boldsymbol{y}}\}. \tag{5.14}$$

Néhány egyszerű, a $\mathcal{V} \setminus \{P\}$ elemei közt fennálló metszési viszonyokkal kapcsolatos tény megkapható a (4.4) és (5.11) formulákból. Például, a (4.4) formulát a $H_{\boldsymbol{x}} * H_{\boldsymbol{y}} = C_{\boldsymbol{x}+\boldsymbol{y}}$ összefüggésre alkalmazva adódik, hogy

$$|H_{\boldsymbol{x}}| + |H_{\boldsymbol{y}}| + |C_{\boldsymbol{x}+\boldsymbol{y}}| = |V_N| + 2|H_{\boldsymbol{x}} \cap H_{\boldsymbol{y}}|. \tag{5.15}$$

Már láttuk, hogy ha $\boldsymbol{x} \neq \boldsymbol{y}$,

$$|C_{\boldsymbol{x}+\boldsymbol{y}}| = \frac{1}{2}|V_N| = 2^{N-1}2^N. \tag{5.16a}$$

[10] Az (5.9) formulából látszik, hogy az $\boldsymbol{x} \mapsto C_{\boldsymbol{x}}$ leképezés egy $V_N \hookrightarrow \mathcal{V}$ beágyazás.

(3.16) és (3.17) alapján $H_{\boldsymbol{x}}$ és $H_{\boldsymbol{y}}$ elemszáma úgy írható, hogy

$$|H_{\boldsymbol{x}}| = 2^{N-1}(2^N + \alpha) = \frac{2^N + \alpha}{2^N}|C_{\boldsymbol{x}+\boldsymbol{y}}|, \tag{5.16b}$$

$$|H_{\boldsymbol{y}}| = 2^{N-1}(2^N + \beta) = \frac{2^N + \beta}{2^N}|C_{\boldsymbol{x}+\boldsymbol{y}}|, \tag{5.16c}$$

ahol $\alpha, \beta = \pm 1$. Ezeket az (5.15) formulába helyettesítve adódik, hogy

$$\begin{aligned} |H_{\boldsymbol{x}} \cap C_{\boldsymbol{x}+\boldsymbol{y}}| = |H_{\boldsymbol{x}} \cap H_{\boldsymbol{y}}| &= \frac{1}{2}\frac{2^N + \alpha + \beta}{2^N}|C_{\boldsymbol{x}+\boldsymbol{y}}| \\ &= \frac{1}{2}\frac{2^N + \alpha + \beta}{2^N + \alpha}|H_{\boldsymbol{x}}|. \end{aligned} \tag{5.17}$$

Az első egyenlőség (4.3) következménye. Vegyük észre, hogy

1. $|C_{\boldsymbol{x}+\boldsymbol{y}}|$ együtthatója akkor és csak akkor 1, ha $N = 1$ és $\alpha = \beta = 1$;
2. $|H_{\boldsymbol{x}}|$ együtthatója akkor és csak akkor 1, ha $N = 1$ és $\beta = -\alpha = 1$;
3. $|C_{\boldsymbol{x}+\boldsymbol{y}}|$ együtthatója akkor és csak akkor 0, ha $N = 1$ és $\alpha = \beta = -1$.

Ezek az alábbi módon értelmezhetők:

1. $C_{\boldsymbol{x}+\boldsymbol{y}} \subseteq H_{\boldsymbol{x}}$ akkor és csak akkor, ha $N = 1$, $H_{\boldsymbol{x}}$ hiperbólikus és $\boldsymbol{y} \in H_{\boldsymbol{x}}$.
2. $H_{\boldsymbol{x}} \subseteq H_{\boldsymbol{y}}$ akkor és csak akkor, ha $N = 1$ és $H_{\boldsymbol{x}}$ elliptikus. $H_{\boldsymbol{x}} \subseteq C_{\boldsymbol{x}+\boldsymbol{y}}$-ra ugyanez a feltétel érvényes. $H_{\boldsymbol{y}}$ szükségszerűen hiperbólikus, mivel $\boldsymbol{x} \neq \boldsymbol{y}$, és $N = 1$ esetén csak egy elliptikus kvadratikus felület létezik.
3. Az (5.17) formulában a két metszet akkor és csak akkor üres, ha $N = 1$, és $H_{\boldsymbol{x}}$ és $H_{\boldsymbol{y}}$ is elliptikusak. A fenti okok miatt az utóbbi lehetetlen.

A maradék metszési viszony ezekből azonnal következik. Végül azt lehet mondani, hogy, az $N = 1$ elfajult eset kivételével, *$\mathcal{V} \setminus \{P\}$-nek két különböző H_1 és H_2 eleme mindig metszi egymást, és H_1 soha nem részhalmaza H_2-nek.*

A 4. szakasz végén érintve volt, hogy $\lambda(2^P)$ nem a teljes 2^L. Ez az állítás $\mathcal{G}_N$-re tovább pontosítható: bármely $A \subseteq P$-re $\lambda(A)$

$$L_{\text{iso}} \subset \lambda(A) \subset L \qquad \text{és} \qquad L_{\text{hyp}} \subset \lambda(A) \subset L \tag{5.18}$$

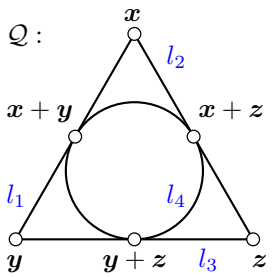
közül egyiket sem teljesíti. Ez a [11] munkában bizonyított, azonban most egy általánosabb eredményből következtetem, mégpedig abból, hogy

5.1. Tétel. *Ha γ_A rögzített L_{iso}-n, $\gamma_A(l)$ legfeljebb egy $l \in L_{\text{hyp}}$-re választható meg szabadon, és ugyanez L_{iso}-t és L_{hyp}-et felcserélve is igaz.*

Az 5.1. tétel bizonyítása felhasználja Pasch axiómáját, amely $N \geq 2$ esetén teljesül $\mathcal{G}_N$-ben, és amely miatt bármely három $\boldsymbol{x}$, $\boldsymbol{y}$ és $\boldsymbol{z}$ lineárisan független vektor egy $\mathcal{Q}$ *teljes négyoldalt* vagy *Pasch-konfigurációt* feszít ki (5.1. ábra). Az $\boldsymbol{x}$, $\boldsymbol{y}$ és $\boldsymbol{z}$ vektorok páronként kollineárisak, és rajtuk kívül még három, páronként kollineáris vektor-hármas található $\mathcal{Q}$-ban:

$$\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{z}, \qquad \boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{z} \qquad \boldsymbol{z}, \boldsymbol{x}+\boldsymbol{z}, \boldsymbol{y}+\boldsymbol{z}. \tag{5.19}$$

Ez a négy pont-hármas $\mathcal{Q}$-ban ekvivalens, és bármelyikük $\mathcal{Q}$-t feszíti ki.



5.1. ábra. Az x, y és z által kifeszített $\mathcal{G}_N$-beli Pasch-konfiguráció

A Pasch-konfigurációkból adódó $\mathcal{G}_N$-beli megszorítások a következők. Egy $\mathcal{Q}$ Pasch-konfiguráció l_1, ..., l_4 egyeneseire igaz, hogy

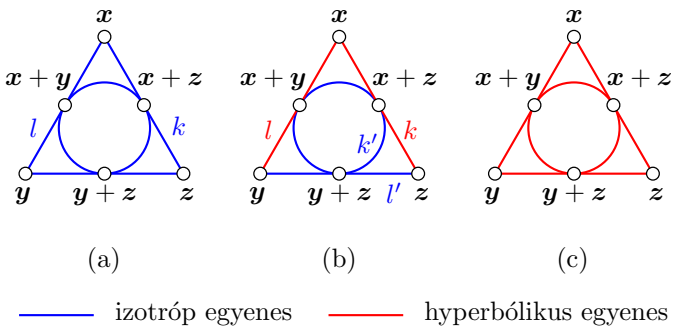
$$\sum_{i=1}^{4} \gamma_A(l_i) = 0, \qquad A \subseteq P, \tag{5.20}$$

mivel $\mathcal{Q}$ minden $\boldsymbol{p}$ pontja két egyenesre illeszkedik, és így minden $\chi_A(\boldsymbol{p})$ kétszer szerepel a szummában; lásd (4.10). Egy másik fontos kérdés az izotróp és hiperbólikus egyenesek $\mathcal{Q}$-beli eloszlása. A három lehetséges esetet az 5.2. ábra mutatja.

Legyen két izotróp (hiperbólikus) egyenes, l és k, *szomszédos*, és fejezze ezt ki $l \sim k$, ha l és k olyan $\mathcal{Q}$ Pasch-konfiguráció egyenesei, amelynek a másik két egyenese hiperbólikus (izotróp). Például, az 5.2 (b) ábrán $l \sim k$ és $l' \sim k'$. l és k *kapcsolódnak*, ha létezik izotróp (hiperbólikus) egyenesekből álló

$$l = l_0,\ l_1,\ \ldots,\ l_n = k \tag{5.21}$$

sorozat úgy, hogy $l_{i-1} \sim l_i$, $i = 1, \ldots, n$. Kissé visszaélve a jelöléssel, ugyancsak $l \sim k$-val fejezem ki azt is, hogy l és k kapcsolódnak. Triviális, hogy $\sim$ egy tranzitív reláció L-en.



5.2. ábra. Izotróp és hiperbólikus egyenesek Pasch-konfigurációkban

Legyen valamely $l \in L_{\text{hyp}}$-re γ_A rögzített az $\{l\} \cup L_{\text{iso}}$ halmazon, és legyen $l \sim k \in L_{\text{hyp}}$. Az (5.20) formulát alkalmazva arra a Pasch-konfigurációra, amely miatt az (5.21) formulában $l = l_0$ és l_1 szomszédosak, adódik, hogy $\gamma_A(l_1)$ rögzített. Ez $\gamma_A(l_2)$-re is megismételhető, és így tovább, egészen $\gamma_A(l_n = k)$-ig. Levonható az a következtetés, hogy minden $k \sim l$-re $\gamma_A(k)$ rögzített. Az érvelés L_{iso} és L_{hyp} felcserélése után is érvényes. Ezért, az 5.1. tétel bizonyításához elég annyit megmutatni, hogy bármely két izotróp (hiperbólikus) egyenes kapcsolódik.

5.2. Lemma. *Bármely két különböző, de egy közös ponttal illeszkedő izotróp (hiperbólikus) egyenes kapcsolódik.*

Bizonyítás. Legyen a két egyenes l és k, és legyen $\boldsymbol{x} \in l \cap k$. Ha l és k hiperbólikusak, a szimplektikus forma bilinearitása miatt létezik $\boldsymbol{y} \in l$ és $\boldsymbol{z} \in k$ úgy, hogy $\langle \boldsymbol{y}, \boldsymbol{z} \rangle = 0$. Ekkor $\boldsymbol{x}$, $\boldsymbol{y}$ és $\boldsymbol{z}$ egy olyan Pasch-konfigurációt feszítenek ki, amilyen az 5.2 (b) ábrán is látható. Következésképpen, $l \sim k$.

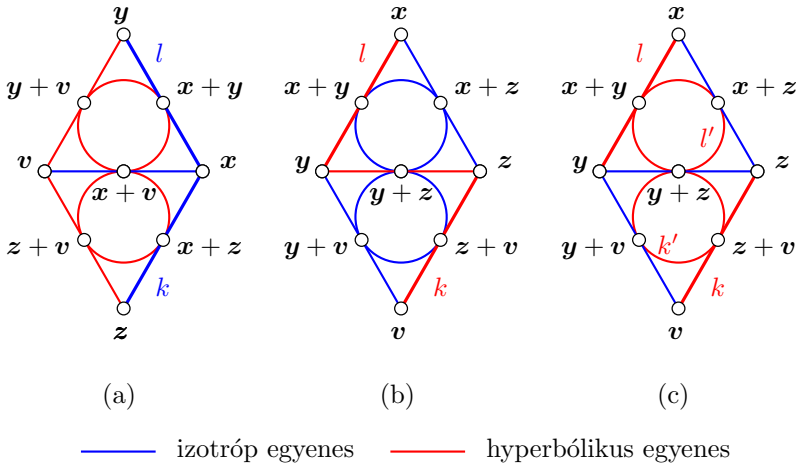
A két izotróp egyenes esete csak akkor problémásabb, ha $N \geq 3$, és minden $\boldsymbol{y} \in l$-re és $\boldsymbol{z} \in k$-ra $\langle \boldsymbol{y}, \boldsymbol{z} \rangle = 0$. Ekkor $\boldsymbol{x}$ és bármely $\boldsymbol{y} \in l \setminus \{\boldsymbol{x}\}$ és $\boldsymbol{z} \in k \setminus \{\boldsymbol{x}\}$ az 5.2 (a) ábrán látható Pasch-konfigurációt feszítik ki, amelynek a pontjai páronként ortogonálisak.

Mivel $C_{\boldsymbol{x}} \cap C_{\boldsymbol{y}}$ és $C_{\boldsymbol{x}} \cap C_{\boldsymbol{z}}$ a $2N-1$-dimenziós $C_{\boldsymbol{x}}$ altérnek $2N-2$-dimenziós alterei, $C_{\boldsymbol{x}} \cap C_{\boldsymbol{y}} \cap C_{\boldsymbol{z}}$ dimenziószáma $2N-3$, és emiatt három mellékosztálya van $C_{\boldsymbol{x}}$-ben. Ezen mellékosztályok valamelyike nem metszi sem $C_{\boldsymbol{y}}$-t, sem $C_{\boldsymbol{z}}$-t, így a belőle választott $\boldsymbol{v}$ vektor teljesíti azt, hogy

$$\langle \boldsymbol{y}, \boldsymbol{v} \rangle = \langle \boldsymbol{z}, \boldsymbol{v} \rangle = 1 \qquad \text{és} \qquad \langle \boldsymbol{x}, \boldsymbol{v} \rangle = 0. \tag{5.22}$$

Kapjuk, hogy $l \sim \{\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{x}+\boldsymbol{v}\} \sim k$; lásd 5.3 (a) ábra. □

Namármost, ha l és k *diszjunkt* izotróp egyenesek, azaz nem illeszkednek egy közös ponttal, a szimplektikus forma bilinearitása miatt minden $\boldsymbol{x} \in l$-re létezik $\boldsymbol{y} \in k$ úgy, hogy $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$. Ekkor, az 5.2. lemma alapján, $l \sim \{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}\} \sim k$.



5.3. ábra. Kapcsolódó egyenesek speciális esetei

Ha l és k diszjunkt hiperbólikus egyenesek, két lehetőség állhat fenn. Ha valamely $\boldsymbol{y} \in l$-re és $\boldsymbol{z} \in k$-ra $\langle \boldsymbol{y}, \boldsymbol{z} \rangle = 1$, az 5.2. lemma alapján $l \sim \{\boldsymbol{y}, \boldsymbol{z}, \boldsymbol{y}+\boldsymbol{z}\} \sim k$; lásd 5.3 (b) ábra. Az ellenkező eset az 5.3 (c) ábrán látható, ahol $l \sim l' \sim k' \sim k$.

Ezzel az 5.1. tétel bizonyítása véget is ért, mivel az elkerült $\mathcal{G}_1$-nek csupán egyetlen hiperbólikus egyenese van.

6. A Pauli-csoport szimplektikus struktúrája egy másik szemszögből

A 2. szakaszban láttuk, hogy a $\mathbb{Z}_2$ feletti $2N$-dimenziós V_N szimplektikus vektortér az N-qubit Pauli-csoport sok tulajdonságát képes megragadni. Mostantól az $\boldsymbol{x} \in \mathbb{Z}_2^{2N}$ vektorok a $[2N] = \{1, 2, ..., 2N\}$ halmaz részhalmazaiként lesznek kezelve, és $i \in \boldsymbol{x}$ azt fogja jelenteni, hogy $\boldsymbol{x}$-nek az i-edik komponense, x_i, egyenlő 1-el. Így az $\boldsymbol{x} \cup \boldsymbol{y}$ uniót, az $\boldsymbol{x} \cap \boldsymbol{y}$ metszetet, az $\boldsymbol{x} \setminus \boldsymbol{y}$ különbséget, az $\boldsymbol{x} + \boldsymbol{y}$ szimmetrikus differenciát és a $[2N]$ halmazra vett $\boldsymbol{x}^{\mathrm{c}}$ komplementert minden $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_2^{2N}$-re a szokásos, halmazelméleti módon kell érteni. Vegyük észre, hogy a szimmetrikus differencia egyben a $\mathbb{Z}_2^{2N}$-beli vektorösszeadás.

Amennyiben nem okoz zavart, érdemes az

$$ij...k \equiv \{i, j, ..., k\} \subseteq [2N] \tag{6.1}$$

rövidített jelölést használni. Ha hangsúlyozni kell, hogy a csupa 1 komponensű vektorról van szó, $[2N]$ helyett $\mathbf{1}_N$-et írok, és ha a szövegkörnyezet alapján N

egyértelmű, az alsó indexet elhagyom. Nyilvánvaló, hogy minden $\boldsymbol{x} \in \mathbb{Z}_2^{2N}$ komplementere kifejezhető úgy, hogy

$$\boldsymbol{x}^{\mathrm{c}} = \mathbf{1} + \boldsymbol{x}. \tag{6.2}$$

$[2N]$ részhalmazaként tekintve minden $\boldsymbol{x} \in \mathbb{Z}_2^{2N}$ vektornak van egy $|\boldsymbol{x}|$-el jelölt „mérete", ami éppen a nemnulla komponensek száma. Például, $|ijk| = 3$. A

$$|\cdot| : \mathbb{Z}_2^{2N} \to \mathbb{N} \subseteq \mathbb{R} \tag{6.3}$$

leképezés egy $\mathbb{Z}_2^{2N}$-n értelmezett norma[11] és egy $[2N]$-en értelmezett mérték. A mértékelméletből ismert, hogy

$$|\boldsymbol{x} + \boldsymbol{y}| = |\boldsymbol{x}| + |\boldsymbol{y}| - 2|\boldsymbol{x} \cap \boldsymbol{y}|. \tag{6.4}$$

A 2. szakaszban ismertetett, és a [4, 5] munkákban is átvett, megközelítés és a hamarosan bemutatásra kerülő megközelítés közötti különbségek abból erednek, hogy $\mathbb{Z}_2^{2N}$-t most, (2.12) helyett, a

$$\langle\cdot,\cdot\rangle : \mathbb{Z}_2^{2N} \times \mathbb{Z}_2^{2N} \to \mathbb{Z}_2, \qquad \langle \boldsymbol{x}, \boldsymbol{y}\rangle = |\boldsymbol{x}||\boldsymbol{y}| + |\boldsymbol{x} \cap \boldsymbol{y}| \mod 2 \tag{6.5}$$

leképezéssel látom el. Ez a formula [7]-ben is szerepel. Az utolsó tag egyenlő azzal, hogy $\boldsymbol{x} \cdot \boldsymbol{y} = \sum_{i=1}^{2N} x_i y_i$, ami az $\mathbb{R}^{2N}$-en értelmezett „szokásos" skalárszorzat. Következik, hogy

$$f : \mathbb{Z}_2^{2N} \times \mathbb{Z}_2^{2N} \to \mathbb{Z}_2, \qquad f(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x} \cap \boldsymbol{y}| \mod 2 \tag{6.6}$$

egy szimmetrikus bilineáris forma. (6.4) alapján ugyanez igaz a

$$g : \mathbb{Z}_2^{2N} \times \mathbb{Z}_2^{2N} \to \mathbb{Z}_2, \qquad g(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x}||\boldsymbol{y}| \mod 2 \tag{6.7}$$

leképezésre is. Tehát $\langle\cdot,\cdot\rangle$ szimmetrikus és bilineáris. A (6.5) formulából triviálisan következik, hogy $\langle \boldsymbol{x}, \boldsymbol{x}\rangle = 0$. Ha $\boldsymbol{x}$ nemnulla, páros $|\boldsymbol{x}|$ esetében választható $i \in \boldsymbol{x}$, és páratlan $|\boldsymbol{x}|$ esetében választható $i \notin \boldsymbol{x}$ úgy, hogy $\langle i, \boldsymbol{x}\rangle = 1$ teljesüljön. Emiatt $\langle\cdot,\cdot\rangle$ nemdegenerált[12]. Összegezve: $\langle\cdot,\cdot\rangle$ *szimplektikus forma*.

Megjegyzendő, hogy a (6.5) szimplektikus formával ellátott $\mathbb{Z}_2^{2N}$-nek *ugyanaz* a szimplektikus struktúrája, mint a (2.12) formával ellátott $\mathbb{Z}_2^{2N}$-é, mivel a (6.5) és (2.12) közti választás csupán egy bázisválasztással ekvivalens. (6.5) fontos előnye,

[11] A $|\cdot|$ norma által indukált távolság a kódoláselméletben jól ismert $d_{\mathrm{H}}(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x} - \boldsymbol{y}|$ *Hamming-távolság*.

[12] Fontos, hogy $\langle\cdot,\cdot\rangle$ nemdegeneráltsága megköveteli, hogy V_N páros dimenziós legyen, különben $|\mathbf{1}|$ páratlan, és ekkor nem létezik $i \notin \mathbf{1}$.

hogy V_N kanonikus bázisvektorai, amelyek most szingletonokként vannak tekintve, ekvivalensek. Hadd fejtsem ki. A „régi", (2.12) szimplektikus formával V_N kanonikus bázisa úgy írható, hogy

$$\{\boldsymbol{e}_1, ..., \boldsymbol{e}_N, \boldsymbol{f}_1, ..., \boldsymbol{f}_N\}, \tag{6.8}$$

ahol a bázisvektorokra teljesül, hogy

$$\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle = \langle \boldsymbol{f}_i, \boldsymbol{f}_j \rangle = 0 \qquad \text{és} \qquad \langle \boldsymbol{e}_i, \boldsymbol{f}_j \rangle = \delta_{ij}, \qquad i, j = 1, ..., N. \tag{6.9}$$

Más szavakkal, a (2.12) formával a kanonikus bázis egy *szimplektikus bázis*. Lásd még a (2.7) formulában a vektorkomponensek megkülönböztető jelöléseit. A fentiekkel ellentétben, a (6.5) formával a kanonikus bázisnak, amely most úgy ítható, hogy

$$\{\{1\}, \{2\}, ..., \{2N\}\}, \tag{6.10}$$

nincsenek megkülönböztetett részhalmazai, és a bázisvektorok az egységes

$$\langle i, j \rangle = 1 - \delta_{ij}, \qquad i, j = 1, ..., 2N \tag{6.11}$$

tulajdonságot elégítik ki.

Shaw [9] munkáját követve, V_N-nek egy bázisa *off-diagonális*[13], ha a bázisvektorok a kanonikus bázisvektorokhoz hasonlóan páronként nemortogonálisak. A (6.5) szimplektikus forma kanonikus bázisra vett $\mathbf{J}$ mátrixa egyértelművé teszi az elnevezés mögötti motivációt:

$$\mathbf{J} = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix} \in \mathbb{Z}_2^{2N \times 2N}, \qquad J_{ij} = \langle i, j \rangle = 1 - \delta_{ij}. \tag{6.12}$$

(6.8) alapján, a (2.12) szimplektikus forma mátrixa

$$\mathbf{J}' = \begin{bmatrix} & I_N \\ I_N & \end{bmatrix} \in \mathbb{Z}_2^{2N \times 2N}, \tag{6.13}$$

ahol I_N az $N \times N$-es egységmátrix. Azonnal következik, hogy a bázisvektorokat permutáló permutációs mátrixok közül nem mindegyik őrzi a (2.12) szimplektikus formát. Ezzel szemben, a (6.5) formát mindegyik permutációs mátrix őrzi. Erről a 8. szakaszban bővebben lesz szó.

[13] Angol nyelvű elnevezés: *off-diagonal*.

$\mathbf{J}$ segítségével a (6.5) szimplektikus forma úgy fejezhető ki, hogy

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = |\boldsymbol{x} \cap \mathbf{J}\boldsymbol{y}| = |\mathbf{J}\boldsymbol{x} \cap \boldsymbol{y}| \mod 2. \tag{6.14}$$

$\mathbf{J}$ minden i kanonikus bázisvektort az i^{c} komplementerére képez, ezért

$$\mathbf{J}\boldsymbol{x} = \sum_{i \in \boldsymbol{x}} (i + \mathbf{1}) = \boldsymbol{x} + |\boldsymbol{x}|\mathbf{1} = \begin{cases} \boldsymbol{x} & \text{ha } |\boldsymbol{x}| \text{ páros,} \\ \boldsymbol{x}^{\mathrm{c}} & \text{ha } |\boldsymbol{x}| \text{ páratlan.} \end{cases} \tag{6.15}$$

Mivel $|\boldsymbol{x}^{\mathrm{c}}|$ és $|\boldsymbol{x}|$ paritása megegyezik, egyrészt $\mathbf{J}$ egy involúció:

$$\mathbf{J}^{-1} = \mathbf{J}, \tag{6.16}$$

másrészt pedig a $\mathbf{J}$ és $(\cdot)^{\mathrm{c}}$ leképezések felcserélhetők:

$$(\mathbf{J}\boldsymbol{x})^{\mathrm{c}} = \mathbf{J}\boldsymbol{x}^{\mathrm{c}} = \begin{cases} \boldsymbol{x}^{\mathrm{c}} & \text{ha } |\boldsymbol{x}| \text{ páros,} \\ \boldsymbol{x} & \text{ha } |\boldsymbol{x}| \text{ páratlan.} \end{cases} \tag{6.17}$$

Ahhoz, hogy a (6.5) szimplektikus formát a $\mathcal{P}_N/Z(\mathcal{P}_N)$-beli kommutációs relációk indukálják a 2. szakasz végén részletezett módon, V_N páronként nemortogonális kanonikus bázisvektoraihoz $\mathcal{P}_N/Z(\mathcal{P}_N)$ olyan ekvivalenciaosztályait kell rendelni, amelyeket *páronként antikommutáló* N-qubit Pauli-operátorok adnak meg. Ezzel lemondunk a V_N és $\mathcal{P}_N/Z(\mathcal{P}_N)$ közti, (2.5) és (2.7) által leírt intim megfeleltetési szabályról. Egy több szempontból is kényelmes megfeleltetési szabály a következő:

$$\begin{array}{ll} 1 \leftrightarrow YIII...II, & 2 \leftrightarrow XIII...II, \\ 3 \leftrightarrow ZYII...II, & 4 \leftrightarrow ZXII...II, \\ 5 \leftrightarrow ZZYI...II, & 6 \leftrightarrow ZZXI...II, \\ \vdots & \vdots \\ 2N-1 \leftrightarrow ZZZZ...ZY, & 2N \leftrightarrow ZZZZ...ZX. \end{array} \tag{6.18}$$

A $\mathcal{P}_N$-beli mátrixok szimmetriái ismét egy V_N-en értelmezett Q_0 kvadratikus formát indukálnak úgy, hogy (6.5) az asszociált bilineáris forma, vagyis a (3.1)-hez hasonló összefüggés teljesül.

7. Kvadratikus formák és egy kanonikus Veldkamp-egyenes

Ebben a szakaszban egy *kanonikus* Veldkamp-egyenes lesz megkonstruálva az alábbi kvadratikus formák segítségével:

$$P(\boldsymbol{x}) = \binom{|\boldsymbol{x}|}{2} \bmod 2 = \begin{cases} 0 & \text{ha } |\boldsymbol{x}| \bmod 4 \in \{0,1\}, \\ 1 & \text{ha } |\boldsymbol{x}| \bmod 4 \in \{2,3\}, \end{cases} \tag{7.1a}$$

$$Q(\boldsymbol{x}) = \binom{|\boldsymbol{x}|+1}{2} \bmod 2 = \begin{cases} 0 & \text{ha } |\boldsymbol{x}| \bmod 4 \in \{0,3\}, \\ 1 & \text{ha } |\boldsymbol{x}| \bmod 4 \in \{2,1\}. \end{cases} \tag{7.1b}$$

Először be kell látni, hogy a (6.5) szimplektikus forma P-hez és Q-hoz asszociált bilineáris forma. Az $f(n) = \binom{n}{2} \bmod 2$ függvény releváns tulajdonságai az A. függelékben vannak összegyűjtve. Javasolt, hogy az Olvasó nézze át őket, mivel a további levezetésekben, a tömörség kedvéért, akár külön hivatkozás nélkül is alkalmazva lesznek.

Kezdjük azzal, hogy

$$\begin{aligned} P(\boldsymbol{x}+\boldsymbol{y}) = \binom{|\boldsymbol{x}+\boldsymbol{y}|}{2} &= \binom{|\boldsymbol{x}| + |\boldsymbol{y}| - 2|\boldsymbol{x} \cap \boldsymbol{y}|}{2} \mod 2 \\ &= \binom{|\boldsymbol{x}| + |\boldsymbol{y}|}{2} + |\boldsymbol{x} \cap \boldsymbol{y}| \mod 2 \\ &= \binom{|\boldsymbol{x}|}{2} + \binom{|\boldsymbol{y}|}{2} + |\boldsymbol{x}||\boldsymbol{y}| + |\boldsymbol{x} \cap \boldsymbol{y}| \mod 2 \\ &= P(\boldsymbol{x}) + P(\boldsymbol{y}) + \langle \boldsymbol{x}, \boldsymbol{y} \rangle. \end{aligned} \tag{7.2}$$

Q esetében ezt az eredményt, és a P és Q közti

$$Q(\boldsymbol{x}) = P(\boldsymbol{x}) + |\boldsymbol{x}| \mod 2 \tag{7.3}$$

összefüggést felhasználva,

$$\begin{aligned} Q(\boldsymbol{x}+\boldsymbol{y}) &= P(\boldsymbol{x}+\boldsymbol{y}) + |\boldsymbol{x}+\boldsymbol{y}| \mod 2 \\ &= P(\boldsymbol{x}) + P(\boldsymbol{y}) + \langle \boldsymbol{x}, \boldsymbol{y} \rangle + |\boldsymbol{x}| + |\boldsymbol{y}| \mod 2 \\ &= Q(\boldsymbol{x}) + Q(\boldsymbol{y}) + \langle \boldsymbol{x}, \boldsymbol{y} \rangle. \end{aligned} \tag{7.4}$$

P, illetve Q az alábbi kvadratikus felületeket definiálja:

$$H_P = \{\boldsymbol{x} \in V_N \,|\, |\boldsymbol{x}| \bmod 4 \in \{0,1\}\}, \qquad \text{illetve} \tag{7.5a}$$

$$H_Q = \{\boldsymbol{x} \in V_N \,|\, |\boldsymbol{x}| \bmod 4 \in \{0,3\}\}. \tag{7.5b}$$

A kívánt Veldkamp-egyenes harmadik pontja a

$$C_{\mathbf{1}} = H_P * H_Q = \{\boldsymbol{x} \in V_N \,|\, |\boldsymbol{x}| \bmod 4 \in \{0, 2\}\} \tag{7.5c}$$

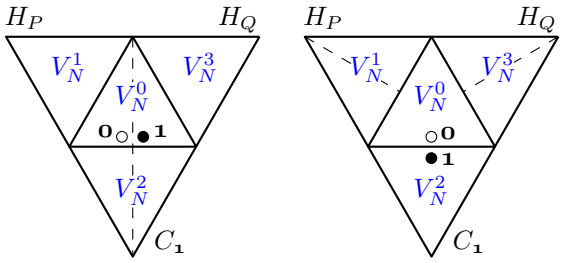
perp-halmaz. Ez összhangban van a (7.3) formulával, amiből következik, hogy

$$P(\boldsymbol{x}) + Q(\boldsymbol{x}) = |\boldsymbol{x}| = \langle \boldsymbol{x}, \mathbf{1} \rangle \mod 2. \tag{7.6}$$

A $\{H_P, H_Q, C_{\mathbf{1}}\}$ kanonikus Veldkamp-egyenes kéz a kézben jár V_N-nek a vektorméretek modulo 4 kongruenciaosztályokba való sorolása szerinti felosztásával; lásd (7.5a), (7.5b) és (7.5c). Ez a felosztás a 7.1. ábrán látható. A kis körök a $\mathbf{0} = (0, ..., 0)$ nullvektort, a kis fekete pontok pedig az $\mathbf{1} = (1, ..., 1)$ vektort reprezentálják. H_P és H_Q akkor és csak akkor ugyanolyan típusúak, ha $\mathbf{1} \in H_P \cap H_Q$ (részletekért lásd 3. szakasz), akkor és csak akkor, ha

$$|\mathbf{1}| \bmod 4 = 2N \bmod 4 = 2(N \bmod 2) = 0. \tag{7.7}$$

Az osztályt, amely az $|\boldsymbol{x}| \bmod 4 = k$-t teljesítő $\boldsymbol{x}$ vektorokat tartalmazza, V_N^k jelöli. Azt mondom, hogy V_N^k a *k-adrendű osztály*, elemei a *k-adrendű vektorok*, és a részhalmazai *k-adrendűek*. Például, a $H_P \cap H_Q$ mag a nulladrendű osztály.



7.1. ábra. V_N felosztásának a függése N mod 2-től

A 7.1. ábrán a szaggatott vonalak azt jelentik, hogy egy osztály két egyforma méretű részhalmazra bontható úgy, hogy $\boldsymbol{x}$ és $\boldsymbol{x}^{\mathrm{c}} = \boldsymbol{x} + \mathbf{1}$ mindig különböző részhalmazokba essenek. Ez a felbontás nem egyértelmű, azonban az $(N+2)$ mod 4-edrendű osztály esetében lehet olyan, hogy ha $\boldsymbol{x}$ és $\boldsymbol{y}$ különböző részhalmazok elemei, $|\boldsymbol{x}| \neq |\boldsymbol{y}|$. Az N mod 4-edrendű osztály esetében ez nem igaz az N méretű vektorok miatt, ugyanis ezek komplementerének a mérete szintén N.

A két nem felbontható osztály egyforma méretű, köztük $\boldsymbol{x} \mapsto \boldsymbol{x}^{\mathrm{c}}$ egy bijekció, és az uniójuk N paritásától függően $C_{\mathbf{1}}$ vagy $\overline{C}_{\mathbf{1}}$. Következésképpen, mindkettő 2^{2N-2} vektort tartalmaz. Kivonva 2^{2N-2}-t a (3.16) és (3.17) formulákból adódik,

hogy egy felbontott osztály mérete $2^{2N-2} \pm 2^{N-1}$. Legyen egy osztály A, B, illetve C *típusú*, ha a méretére a

$$2^{2N-2}, \qquad 2^{2N-2} + 2^{N-1}, \qquad \text{illetve} \qquad 2^{2N-2} - 2^{N-1} \tag{7.8}$$

képlet igaz. Konkrét értékek a C. függelékben találhatók. V_N felosztásában mindig van két A típusú, egy B típusú és egy C típusú osztály.

A H_P és H_Q kvadratikus felületek típusa megkapható $|H_P|$-nek és $|H_Q|$-nak a (3.16) és (3.17) formulákkal való összehasonlításából; az előbbiek függése N-től kombinatorikus módszerekkel meghatározható. Ezt azonban sokkal tanulságosabb másképp megtenni.

Tegyük fel, hogy Q_0 pillanatnyilag egy *tetszőleges* kvadratikus forma, amelyhez az asszociált bilineáris forma (6.5). (6.11) és matematikai indukció segítségével levezethető (lásd A. függelék), hogy

$$Q_0(\boldsymbol{x}) = \sum_{i \in \boldsymbol{x}} Q_0(i) + \binom{|\boldsymbol{x}|}{2} \mod 2, \tag{7.9}$$

ahol $Q_0(i)$ ugyanazt jelenti, mint $Q_0(\{i\})$. Bevezetve a

$$\boldsymbol{w} = \sum_{i=1}^{2N} Q_0(i)\, \{i\} \tag{7.10}$$

vektort, amelynek az i-edik komponense éppen $Q_0(i)$, (7.9) úgy írható, hogy

$$Q_0(\boldsymbol{x}) = |\boldsymbol{x} \cap \boldsymbol{w}| + P(\boldsymbol{x}) = \langle \boldsymbol{x}, \mathbf{J}\boldsymbol{w} \rangle + P(\boldsymbol{x}) \mod 2. \tag{7.11}$$

Definiálva a

$$\boldsymbol{p} = \mathbf{J}\boldsymbol{w} = \mathbf{J} \sum_{i=1}^{2N} Q_0(i)\, \{i\} \tag{7.12}$$

vektort és (3.2) segítségével átrendezve a (7.11) formulát adódik, hogy[14]

$$Q^0_{\boldsymbol{p}}(\boldsymbol{x}) = P(\boldsymbol{x}). \tag{7.13}$$

A P és Q közti (7.3) kapcsolat alapján kapjuk, hogy

$$\begin{aligned} Q(\boldsymbol{x}) = Q^0_{\boldsymbol{p}}(\boldsymbol{x}) + \langle \boldsymbol{x}, \mathbf{1} \rangle &= Q_0(\boldsymbol{x}) + \langle \boldsymbol{x}, \boldsymbol{p} \rangle + \langle \boldsymbol{x}, \mathbf{1} \rangle \\ &= Q_0(\boldsymbol{x}) + \langle \boldsymbol{x}, \boldsymbol{p}^{\mathrm{c}} \rangle. \end{aligned} \tag{7.14}$$

[14] A ‘0’ a felső indexben csak annyit jelez, hogy a kvadratikus forma Q_0-ból lett származtatva, nem pedig Q-ból.

Következésképpen, definiálva a

$$\boldsymbol{q} = \boldsymbol{p}^{\mathrm{c}} = \mathbf{J}\boldsymbol{w}^{\mathrm{c}} = \mathbf{J}\sum_{i=1}^{2N}[1 - Q_0(i)]\,\{i\} \tag{7.15}$$

vektort adódik, hogy

$$Q^0_{\boldsymbol{q}}(\boldsymbol{x}) = Q(\boldsymbol{x}). \tag{7.16}$$

Most tegyük fel, hogy Q_0 az a hiperbólikus kvadratikus forma, amit a Pauli-operátorok szimmetriái indukálnak (lásd a 3. szakasz végét). $Q_0(i)$-vel ellentétben, sem H_P típusa, sem H_Q típusa nem függ a V_N és $\mathcal{P}_N/Z(\mathcal{P}_N)$ közti megfeleltetési szabálytól. Következésképpen, $Q_0(\boldsymbol{p})$ és $Q_0(\boldsymbol{q})$ csak N-től függ, és ezek bármelyik alkalmas bázisvektor—ekvivalenciaosztály megfeleltetéséből meghatározhatók. A (6.18) megfeleltetést választva használható a kényelmes

$$Q_0(i) = i \bmod 2. \tag{7.17}$$

Ebből $|\boldsymbol{p}| = N$, és (7.13) felhasználásával adódik egy általánosan érvényes kifejezés:

$$Q_0(\boldsymbol{p}) = Q^0_{\boldsymbol{p}}(\boldsymbol{p}) = P(\boldsymbol{p}) = \binom{N}{2} \bmod 2 = \begin{cases} 0 & \text{ha } N \bmod 4 \in \{0,1\}, \\ 1 & \text{ha } N \bmod 4 \in \{2,3\}. \end{cases} \tag{7.18}$$

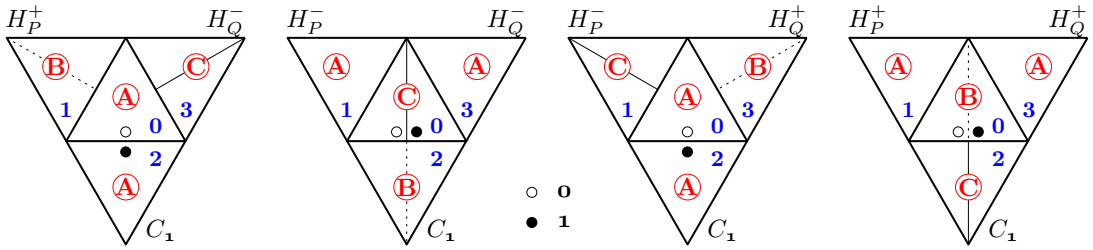
Felhívom a figyelmet, hogy ebből az érvelésből *nem* következik, hogy $|\boldsymbol{p}| = N$ általánosan igaz. Csak annyi következik belőle, hogy a bázisvektor—ekvivalencia-osztály megfeleltetéstől függetlenül

$$\binom{|\boldsymbol{p}|}{2} = \binom{N}{2} \mod 2. \tag{7.19}$$

Mivel $|\boldsymbol{q}| = 2N - |\boldsymbol{p}| = N$, a $Q_0(\boldsymbol{q})$-ra vonatkozó, (7.18) formulához hasonló kifejezés

$$Q_0(\boldsymbol{q}) = Q^0_{\boldsymbol{q}}(\boldsymbol{q}) = Q(\boldsymbol{q}) = \binom{N+1}{2} = \begin{cases} 0 & \text{ha } N \bmod 4 \in \{0,3\}, \\ 1 & \text{ha } N \bmod 4 \in \{2,1\}. \end{cases} \tag{7.20}$$

A H_P és H_Q kvadratikus felületek típusai, összevetve a korábbi megfigyelésekkel, a 7.2. ábrán láthatók. A piros bekarikázott betűk az osztályok típusát, a kis kék számok pedig az osztályok rendjét mutatják. Az N mod 4-edrendű osztályról kiderül, hogy mindig B típusú. A kis kör által reprezentált nullvektor mindig a magban van, ezzel szemben a kis fekete pont által reprezentált $\mathbf{1}$ csak akkor van a magban, ha N páros.



7.2. ábra. V_N felosztásának a függése N mod 4-től

A többi, V_N-en értelmezett kvadratikus forma (3.2) előírásai szerint akár P, akár Q segítségével is kifejezhető. Mivel (7.6) összekapcsolja P-t és Q-t,

$$\begin{aligned} P_{\boldsymbol{y}}(\boldsymbol{x}) &= P(\boldsymbol{x}) + \langle \boldsymbol{x}, \boldsymbol{y} \rangle = Q(\boldsymbol{x}) + \langle \boldsymbol{x}, \mathbf{1} \rangle + \langle \boldsymbol{x}, \boldsymbol{y} \rangle \\ &= Q(\boldsymbol{x}) + \langle \boldsymbol{x}, \boldsymbol{y}^{\mathrm{c}} \rangle = Q_{\boldsymbol{y}^{\mathrm{c}}}(\boldsymbol{x}). \end{aligned} \tag{7.21}$$

(3.5), (7.1a) és (7.1b) alapján,

$$P_{\boldsymbol{y}}(\boldsymbol{x}) = P(\boldsymbol{y}) + P(\boldsymbol{x}+\boldsymbol{y}) = \binom{|\boldsymbol{y}|}{2} + \binom{|\boldsymbol{x}+\boldsymbol{y}|}{2} \bmod 2, \tag{7.22a}$$

$$Q_{\boldsymbol{y}}(\boldsymbol{x}) = Q(\boldsymbol{y}) + Q(\boldsymbol{x}+\boldsymbol{y}) = \binom{|\boldsymbol{y}|+1}{2} + \binom{|\boldsymbol{x}+\boldsymbol{y}|+1}{2} \bmod 2. \tag{7.22b}$$

8. A kanonikus Veldkamp-egyenes stabilizátor csoportja

Ebben a szakaszban azoknak a $\mathbb{Z}_2$-beli elemű, $2N \times 2N$-es mátrixok-nak a csoportja lesz megvizsgálva, amelyek úgy hatnak V_N-re, hogy őrzik a (6.5) szimplektikus formát és a vektorok rendjét, vagy, más szavakkal, a $\{H_P, H_Q, C_1\}$ kanonikus Veldkamp-egyenes a fixpontjuk. Ezt a csoportot *a kanonikus Veldkamp-egyenes stabilizátor csoportjának* nevezem, és L_{2N}-el jelölöm.

A (6.5) formát megtartó $\mathbf{M}$ mátrixok pontosan azok, amelyekre igaz, hogy

$$\mathbf{M}^{\mathrm{T}}\mathbf{J}\mathbf{M} = \mathbf{J}. \tag{8.1}$$

Ezek az $\mathbf{M}$ mátrixok az $\mathrm{Sp}(2N, 2)$ *szimplektikus csoportot* alkotják, és őket is *szimplektikusnak* mondják. (6.12) alapján, a permutációs mátrixok nyilvánvalóan kielégítik a (8.1) feltételt, és így $\mathrm{Sp}(2N, 2)$-nek egy, az S_{2N} szimmetrikus csoporttal

izomorf részcsoportját alkotják. Ezentúl, hacsak másképp nincs jelezve, S_{2N} mindig $\mathrm{Sp}(2N,2)$-nek ezt a részcsoportját[15] jelenti. A permutációs mátrixok a vektorok méreteit is megtartják, és így a rendeket sem változtatják. Következésképpen,

$$S_{2N} \leq L_{2N} \leq \mathrm{Sp}(2N,2). \tag{8.2}$$

Ismert [3], hogy V_N-nek egy speciális transzformáció-osztálya, a *transzvekciók* osztálya olyan elemeket tartalmaz, amelyek mátrixai generálják $\mathrm{Sp}(2N,2)$-t. Az $\boldsymbol{y} \in V_N$ vektorhoz tartozó transzvekció

$$T_{\boldsymbol{y}} : V_N \to V_N, \qquad T_{\boldsymbol{y}}(\boldsymbol{x}) = \boldsymbol{x} + \langle \boldsymbol{y}, \boldsymbol{x} \rangle \boldsymbol{y} = (\mathbf{I} + \boldsymbol{y} \circ \boldsymbol{y}^{\mathrm{T}} \mathbf{J})\boldsymbol{x}. \tag{8.3}$$

Ebből $T_{\boldsymbol{y}}$-nek a a kanonikus bázisra vett mátrixa:

$$\mathbf{T}_{\boldsymbol{y}} = \mathbf{I} + \boldsymbol{y} \circ \boldsymbol{y}^{\mathrm{T}} \mathbf{J}. \tag{8.4}$$

A továbbiakban transzvekciók alatt a $\mathbf{T}_{\boldsymbol{y}}$ mátrixokat kell érteni. Ezek teljesítik azt, hogy

$$\mathbf{T}_{\boldsymbol{y}}^2 = \mathbf{I}, \qquad \mathbf{T}_{\boldsymbol{y}} \mathbf{T}_{\boldsymbol{z}} \mathbf{T}_{\boldsymbol{y}} = \mathbf{T}_{\mathbf{T}_{\boldsymbol{y}} \boldsymbol{z}}. \tag{8.5}$$

Ha $\langle \boldsymbol{y}, \boldsymbol{z} \rangle = 1$, $\mathbf{T}_{\mathbf{T}_{\boldsymbol{y}} \boldsymbol{z}}$ úgy alakul, hogy $\mathbf{T}_{\boldsymbol{y}+\boldsymbol{z}}$, ami $\boldsymbol{y}$-ban és $\boldsymbol{z}$-ben szimmetrikus. Következésképpen,

$$\mathbf{T}_{\boldsymbol{y}} \mathbf{T}_{\boldsymbol{z}} \mathbf{T}_{\boldsymbol{y}} = \mathbf{T}_{\boldsymbol{z}} \mathbf{T}_{\boldsymbol{y}} \mathbf{T}_{\boldsymbol{z}} = \mathbf{T}_{\boldsymbol{y}+\boldsymbol{z}}. \tag{8.6}$$

A (8.4) formulában $\boldsymbol{y}$ helyébe $\mathbf{o}$-t, illetve $\mathbf{1}$-et helyettesítve adódik, hogy

$$\mathbf{T}_{\mathbf{o}} = \mathbf{I}, \qquad \text{illetve} \qquad \mathbf{T}_{\mathbf{1}} = \mathbf{I} + \mathbf{1} \circ \mathbf{1}^{\mathrm{T}} = \mathbf{J}. \tag{8.7}$$

A (8.5) azonosságok *Coxeter-relációk* néven ismertek [2]. A levezetés technikai részletei iránt érdeklődő Olvasó megtalálja őket a B. függelékben, ahol annak a bizonyítása is helyet kap, hogy a $\mathbf{T}_{\boldsymbol{y}}$ transzvekciók szimplektikusak.

$|\boldsymbol{y}| = 2$ esetén $\mathbf{T}_{\boldsymbol{y}}$ egy, a kanonikus bázison értelmezett transzpozíció. Nevezetesen, $\mathbf{T}_{ij}$ felcseréli az $\{i\}$ és $\{j\}$ bázisvektorokat, és minden $\{k\}$, $k \neq i, j$ a fixpontja. Ezek a transzpozíciók generálják S_{2N}-t, vagyis bármely $\mathbf{P}$ permutációs mátrix transzpozíciók $\mathbf{T}_{ij} \cdots \mathbf{T}_{kl}$ szorzataként írható. A (8.5) Coxeter-relációkból azt kapjuk, hogy

$$\begin{aligned} \mathbf{P}\mathbf{T}_{\boldsymbol{y}}\mathbf{P}^{-1} = (\mathbf{T}_{ij} \cdots \mathbf{T}_{kl})\mathbf{T}_{\boldsymbol{y}}(\mathbf{T}_{ij} \cdots \mathbf{T}_{kl})^{-1} &= (\mathbf{T}_{ij} \cdots \mathbf{T}_{kl})\mathbf{T}_{\boldsymbol{y}}(\mathbf{T}_{kl} \cdots \mathbf{T}_{ij}) \\ &= \mathbf{T}_{\mathbf{T}_{ij} \cdots \mathbf{T}_{kl} \boldsymbol{y}} \\ &= \mathbf{T}_{\mathbf{P}\boldsymbol{y}}. \end{aligned} \tag{8.8}$$

[15] $\mathrm{Sp}(2N,2)$-nek több olyan részcsoportja van, amely S_{2N}-nel izomorf, azonban S_{2N} mindig a permutációs mátrixok részcsoportjára utal.

Következésképpen, ha $\boldsymbol{y}$ fixpontja $\mathbf{P}$-nek,

$$\mathbf{P}\mathbf{T}_{\boldsymbol{y}} = \mathbf{T}_{\boldsymbol{y}}\mathbf{P}. \tag{8.9}$$

Ennek a szakasznak a fő eredménye a következő:

8.1. Tétel. *L_{2N}-t a másodrendű $\boldsymbol{y}$ vektorok szerinti $\mathbf{T}_{\boldsymbol{y}}$ transzvekciók generálják, vagyis azok a $\mathbf{T}_{\boldsymbol{y}}$-ok, amelyekre $|\boldsymbol{y}| \bmod 4 = 2$.*

A bizonyítás menete a következő. Először, a teljesség kedvéért, a 6. szakasz formalizmusában megmutatom, hogy a transzvekciók valóban generálják $\mathrm{Sp}(2N, 2)$-t. Ezután megmutatom, hogy ugyanez az érvelés hogyan és miért alkalmazható L_{2N}-re. Az érvelés egyes részei a [3] munkából lettek átvéve és egyszerűsítve.

Minden $\mathbf{M}$ szimplektikus mátrixhoz egyértelműen tartozik egy

$$B = \{\boldsymbol{e}_1, ..., \boldsymbol{e}_{2N}\} \tag{8.10}$$

off-diagonális bázis úgy, hogy $\mathbf{M}$ B-t V_N kanonikus bázisára képezi, ráadásul

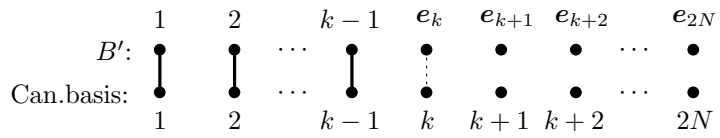
$$\mathbf{M}\boldsymbol{e}_i = \{i\} \equiv i, \qquad i = 1, ..., 2N. \tag{8.11}$$

Ha B és a kanonikus bázis diszjunktak, keresni kell a transzvekcióknak egy olyan szorzatát, amely B-t egy B' off-diagonális bázisra képezi úgy, hogy $\boldsymbol{e}_1$ képe 1. Ha $\langle 1, \boldsymbol{e}_1\rangle = 1$, $\mathbf{T}_{1+\boldsymbol{e}_1}$ erre alkalmas, de ha $\langle 1, \boldsymbol{e}_1\rangle = 0$, $\mathbf{T}_{1+\boldsymbol{e}_1}$ nem működik. (6.5) alapján, $\langle 1, \boldsymbol{e}_1\rangle = 0$ kétféleképpen fordulhat elő: vagy $|\boldsymbol{e}_1|$ páros és $1 \notin \boldsymbol{e}_1$, vagy $|\boldsymbol{e}_1|$ páratlan és $1 \in \boldsymbol{e}_1$. Az első esetben létezik $i \in \boldsymbol{e}_1$, a második esetben létezik $i \notin \boldsymbol{e}_1$, és mindkét esetben ez az i kielégíti azt, hogy

$$\langle i, 1\rangle = \langle i, \boldsymbol{e}_1\rangle = 1. \tag{8.12}$$

Következik, hogy

$$\mathbf{T}_{i+\boldsymbol{e}_1}\boldsymbol{e}_1 = i, \qquad \mathbf{T}_{i+1}i = 1 \qquad \text{és} \qquad \mathbf{T}_{i+1}\mathbf{T}_{i+\boldsymbol{e}_1}\boldsymbol{e}_1 = 1. \tag{8.13}$$



8.1. ábra. A két bázis kapcsolata

Ezután messe B a kanonikus bázist $k-1$ darab vektorban valamely $k \geq 2$-re. B-t megfelelő, $\mathbf{T}_{ij}$ és $\mathbf{T}_{\boldsymbol{e}_{i+j}}$ alakú transzvekciókkal képezve egy olyan off-diagonális

B' bázis kapható, amelynek az első $k-1$ bázisvektora 1, ... $k-1$ (8.1. ábra). Az előző bekezdéshez képest az érvelés kissé elbonyolódik, mivel most egy olyan transzvekció-szorzatot kell keresni, amely nem pusztán $\boldsymbol{e}_k$-t képezi k-ra, hanem minden $j<k$ a fixpontja. Mivel az utóbbiakra igaz, hogy

$$\langle j,k\rangle = \langle j,\boldsymbol{e}_k\rangle = 1, \tag{8.14}$$

ha $\langle k,\boldsymbol{e}_k\rangle = 1$, $\mathbf{T}_{k+\boldsymbol{e}_k}$ megteszi a szolgálatot. Mint előbb, $\mathbf{T}_{k+\boldsymbol{e}_k}$ nem működik, ha $\langle k,\boldsymbol{e}_k\rangle = 0$. Ekkor, ha $|\boldsymbol{e}_k|$ páros, (8.14) miatt $k\notin\boldsymbol{e}_k$ és minden $j<k$-ra $j\in\boldsymbol{e}_k$. Következik, hogy létezik olyan $i>k$, amelyre $i\in\boldsymbol{e}_k$, és így $\langle i,\boldsymbol{e}_k\rangle = 1$, különben $\boldsymbol{e}_k$ a $j<k$-t teljesítő j-k összege, sértve ezzel B' lineáris függetlenségét. Ez az i kielégíti azt is, hogy

$$\langle i,k\rangle = \langle i,j\rangle = 1, \qquad j<k. \tag{8.15}$$

Következésképpen,

$$\mathbf{T}_{i+k}\mathbf{T}_{i+\boldsymbol{e}_k}\boldsymbol{e}_k = k \qquad \text{és} \qquad \mathbf{T}_{i+k}\mathbf{T}_{i+\boldsymbol{e}_k}j = j, \qquad j<k. \tag{8.16}$$

Ha $\langle k,\boldsymbol{e}_k\rangle = 0$ és $|\boldsymbol{e}_k|$ páratlan, (8.14) miatt $k\in\boldsymbol{e}_k$ és minden $j<k$-ra $j\notin\boldsymbol{e}_k$. Namármost, ha k páros, belefuthatunk abba a szerencsétlen esetbe, amikor

$$\boldsymbol{e}_k = \{k,k+1,k+2,...,2N\}\,. \tag{8.17}$$

Ha k páratlan, vagy a (8.17) esetet sikerült másképp elkerülni, választható olyan $i>k$, amelyre $i\notin\boldsymbol{e}_k$, és így $\langle i,\boldsymbol{e}_k\rangle = 1$; ezek után (8.15) és (8.16) szerint kell eljárni. Ha (8.17) fennáll, választani kell egy olyan $\boldsymbol{e}_l\in B'$ bázisvektort, amelyre $l>k$, $\mathbf{T}_{\boldsymbol{e}_k+\boldsymbol{e}_l}$-lel képezni kell B'-t, hogy $\boldsymbol{e}_k$ és $\boldsymbol{e}_l$ felcserélődjön[16], majd $\boldsymbol{e}_l$-el újra kell kezdeni mindent a (8.14) formulától. Ezúttal (8.17) biztosan nem fordul elő, mivel ha $\langle k,\boldsymbol{e}_l\rangle = 0$ és $|\boldsymbol{e}_l|$ páratlan, $\boldsymbol{e}_l\subseteq\boldsymbol{e}_k$, és így $\langle\boldsymbol{e}_k,\boldsymbol{e}_l\rangle = 0$, ami ellentmondás.

Így, lépésről lépésre a (8.10)-beli B bázis a kanonikus bázisra képződik, és csak transzvekciók felhasználásával, amelyek szorzata nem lehet más, mint $\mathbf{M}$.

Mielőtt az érvelést L_{2N}-re alkalmaznám, észre kell venni a következőt:

8.2. Lemma. *k darab páronként nemortogonális, $\alpha=\pm1 \bmod 4$-edrendű $\boldsymbol{x}_1$, ..., $\boldsymbol{x}_k$ vektor összege $\alpha k \bmod 4$-edrendű.*

Bizonyítás. Ez k-ra vett indukcióval bizonyítható. Ha $k=1$, az állítás triviálisan igaz. Legyen

$$\boldsymbol{s}_k = \boldsymbol{x}_1+\cdots+\boldsymbol{x}_k. \tag{8.18}$$

Az induckiós hipotézis úgy hangzik, hogy

$$|\boldsymbol{s}_k| = \alpha k \mod 4. \tag{8.19}$$

[16]Emlékeztető: $\mathbf{T}_{\boldsymbol{e}_k+\boldsymbol{e}_l}$ felcseréli $\boldsymbol{e}_k$-t és $\boldsymbol{e}_l$-t, és B' többi eleme a fixpontja.

Mivel a vektorok páronként nemortogonálisak,

$$\langle \boldsymbol{s}_k, \boldsymbol{x}_{k+1} \rangle = \langle \boldsymbol{x}_1, \boldsymbol{x}_{k+1} \rangle + \cdots + \langle \boldsymbol{x}_k, \boldsymbol{x}_{k+1} \rangle = k \mod 2. \tag{8.20}$$

A bal oladalt (6.5) segítségével kiírva és az indukciós hipotézist felhasználva, a (8.19) formulából adódik, hogy

$$\langle \boldsymbol{s}_k, \boldsymbol{x}_{k+1} \rangle = |\boldsymbol{s}_k||\boldsymbol{x}_{k+1}| + |\boldsymbol{s}_k \cap \boldsymbol{x}_{k+1}| = k + |\boldsymbol{s}_k \cap \boldsymbol{x}_{k+1}| \mod 2. \tag{8.21}$$

A (8.21) és (8.20) formulákból látszik, hogy $|\boldsymbol{s}_k \cap \boldsymbol{x}_{k+1}|$ páros, tehát valamely nemnegatív m egészre egyenlő $2m$-mel. Következik, hogy

$$|\boldsymbol{s}_k + \boldsymbol{x}_{k+1}| = |\boldsymbol{s}_k| + |\boldsymbol{x}_{k+1}| - 4m = \alpha(k+1) \mod 4. \tag{8.22}$$

Vö: (6.4). Tehát, az $\boldsymbol{s}_{k+1} \equiv \boldsymbol{s}_k + \boldsymbol{x}_{k+1}$ vektor $\alpha(k+1)$-edrendű, ahogy vártuk. □

A 8.2. lemmából következik, és ez visz közelebb a fő eredményhez, hogy ha egy $\mathbf{M}$ szimplektikus mátrix a kanonikus bázist valamely elsőrendű off-diagonális bázisra képezi ($\alpha = 1$), $\mathbf{M}$ őrzi a vektorok rendjét, és így $\mathbf{M} \in L_{2N}$. Mivel az L_{2N}-beli mátrixok ezt definíciószerűen tudják, egy $\mathbf{M}$ szimplektikus mátrix akkor és csak akkor eleme L_{2N}-nek, ha a kanonikus bázist valamely elsőrendű off-diagonális bázisra képezi, vagy, ami ezzel ekvivalens, ha $\mathbf{M}$ valamely elsőrendű off-diagonális bázist a kanonikus bázisra képez.

Most ugorjunk vissza a (8.10) bázishoz, és tegyük fel, hogy az elsőrendű, ami azt jelenti, hogy $\mathbf{M} \in L_{2N}$. Gondosan megvizsgálva az ezután következő érvelést, látható, hogy benne szereplő transzvekciók $\mathbf{T}_{\boldsymbol{a}+\boldsymbol{b}}$ alakúak, ahol $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = 1$, $\boldsymbol{a}$ vagy szingleton, vagy $\boldsymbol{a} \in B \subseteq V_N^1$, és ugyanez igaz $\boldsymbol{b}$-re is. Következésképpen, a 8.2. lemma alapján, $\boldsymbol{a}+\boldsymbol{b}$ másodrendű. Ezeknek a transzvekcióknak a szorzata $\mathbf{M}$-mel egyenlő, és ezzel a 8.1. tétel bizonyításának vége.

9. Veldkamp-egyenesek a szimplektikus faktorterekben

A 7. szakaszban tárgyaltaknak megfelelően, V_N-nek a 6. szakaszban ismertetett formalizmusa a $\mathcal{P}_N$ N-qubit Pauli-csoportnak egy kanonikus Veldkamp-egyenesét emeli ki. Ez a Veldkamp-egyenes két kvadratikus felületből, H_P-ból és H_Q-ból, és a többiek közül kiváló $\mathbf{1}$ vektor $C_{\mathbf{1}}$ perp-halmazából áll. A 7. szakaszban láttuk, hogy H_P és H_Q típusa, és ezzel egyidőben a kanonikus Veldkamp-egyenes típusa hogyan függ N-től (7.2. ábra).

$\mathcal{P}_N$ maradék, az (5.14) típusok között lévő típusú Veldkamp-egyenesei szintén megközelíthetők kombinatorikusan. Triviális, hogy ezek megkonstruálhatók a $P_{\boldsymbol{y}}$ és $Q_{\boldsymbol{y}}$ kvadratikus formák kvadratikus felületeiből; lásd (7.22a) és (7.22b). Viszont kevésbé triviális megkonstruálni őket egy $W \subseteq V^0_{N+\dim W}$ izotróp altér $W^\perp/W$ *szimplektikus faktorterében* a P és Q által meghatározott kvadratikus felületekből. Ebben a szakaszban az lesz részletezve, hogy ez hogyan lehetséges.

Kezdésként érdemes átismételni néhány általános, a szimplektikus faktorterekre vonatkozó eredményt. Emlékezzünk vissza, hogy egy $W \leq V_N$ izotróp alteret az definiálja, hogy $W \leq W^\perp$. $W^\perp/W$ elemei

$$\boldsymbol{x} + W, \qquad \boldsymbol{x} \in W^\perp \tag{9.1}$$

alakú mellékosztályok, és $W^\perp/W$ vektorösszeadása

$$(\boldsymbol{x} + W) + (\boldsymbol{x}' + W) = (\boldsymbol{x} + \boldsymbol{x}') + W. \tag{9.2}$$

A V_N-en értelmezett $\langle \cdot, \cdot \rangle$ szimplektikus forma egy $W^\perp/W$-n értelmezett szimplektikus formát indukál:

$$\langle \cdot, \cdot \rangle_{\text{fs}} : (W^\perp/W) \times (W^\perp/W) \to \mathbb{Z}_2, \qquad \langle \boldsymbol{x} + W, \boldsymbol{x}' + W \rangle_{\text{fs}} = \langle \boldsymbol{x}, \boldsymbol{x}' \rangle. \tag{9.3}$$

Ez a definíció konzisztens: ha $\boldsymbol{w}, \boldsymbol{w}' \in W$,

$$\langle \boldsymbol{x} + \boldsymbol{w}, \boldsymbol{x}' + \boldsymbol{w}' \rangle = \langle \boldsymbol{x}, \boldsymbol{x}' \rangle + \underbrace{\langle \boldsymbol{w}, \boldsymbol{x}' \rangle}_{=0} + \underbrace{\langle \boldsymbol{x}, \boldsymbol{w}' \rangle}_{=0} + \underbrace{\langle \boldsymbol{w}, \boldsymbol{w}' \rangle}_{=0} = \langle \boldsymbol{x}, \boldsymbol{x}' \rangle. \tag{9.4}$$

(3.11) alapján,

$$\dim W^\perp/W = \dim W^\perp - \dim W = 2(N - \dim W). \tag{9.5}$$

Tehát, $W^\perp/W$ *egy szimplektikus vektortér, és* $V_{N-\dim W}$*-vel izomorf.*

Egy V_N-en értelmezett, W elemeit lenullázó Q kvadratikus forma egy $W^\perp/W$-n értelmezett kvadratikus formát indukál:

$$Q^{\text{fs}} : W^\perp/W \to \mathbb{Z}_2, \qquad Q^{\text{fs}}(\boldsymbol{x} + W) = Q(\boldsymbol{x}). \tag{9.6}$$

Ez a definíció is konzisztens: ha $\boldsymbol{w} \in W$,

$$Q(\boldsymbol{x} + \boldsymbol{w}) = Q(\boldsymbol{x}) + \underbrace{Q(\boldsymbol{w})}_{=0} + \underbrace{\langle \boldsymbol{x}, \boldsymbol{w} \rangle}_{=0} = Q(\boldsymbol{x}). \tag{9.7}$$

A $\langle \cdot, \cdot \rangle_{\text{fs}}$ szimplektikus forma a Q^{fs}-hez asszociált bilineáris forma: ha $\boldsymbol{x}, \boldsymbol{x}' \in W^\perp$,

$$\begin{aligned} Q^{\text{fs}}(\boldsymbol{x} + \boldsymbol{x}' + W) &= Q(\boldsymbol{x} + \boldsymbol{x}') = Q(\boldsymbol{x}) + Q(\boldsymbol{x}') + \langle \boldsymbol{x}, \boldsymbol{x}' \rangle \\ &= Q^{\text{fs}}(\boldsymbol{x} + W) + Q^{\text{fs}}(\boldsymbol{x}' + W) + \langle \boldsymbol{x} + W, \boldsymbol{x}' + W \rangle_{\text{fs}}. \end{aligned} \tag{9.8}$$

A többi, $W^\perp/W$-n értelmezett kvadratikus forma (3.2) szerint az alábbi módon írható: ha $\boldsymbol{x}, \boldsymbol{y} \in W^\perp$,

$$\begin{aligned} Q^{\mathrm{fs}}_{\boldsymbol{y}+W}(\boldsymbol{x}+W) &= Q^{\mathrm{fs}}(\boldsymbol{x}+W) + \langle \boldsymbol{x}+W, \boldsymbol{y}+W\rangle_{\mathrm{fs}} \\ &= Q(\boldsymbol{x}) + \langle \boldsymbol{x}, \boldsymbol{y}\rangle = Q_{\boldsymbol{y}}(\boldsymbol{x}). \end{aligned} \tag{9.9}$$

V_N-nek minden $U \geq W$ Lagrange-alteréhez egyértelműen tartozik $W^\perp/W$-nek egy U' Lagrange-altere: U' tartalmazza W-nek az U-ban lévő mellékosztályait, és az U'-beli W-mellékosztályok uniója U. Ezen alapszik V_N-beli és a $W^\perp/W$-beli kvadratikus felületek típusai közti kapcsolat.

9.1. Lemma. *Egy $H \subseteq V_N$ kvadratikus felület akkor és csak akkor hiperbólikus, ha bármely $W \subseteq H$ izotróp altér valamely $U \subseteq H$ Lagrange-altér része. Továbbá, ha H elliptikus, minden $W \subseteq H$ izotróp altér egy $N-1$-dimenziós $Y \subseteq H$ izotróp altérnek a részhalmaza.*

Bizonyítás. Legyen H a Q kvadratikus forma felülete, $W \subseteq H$ egy izotróp altér, és $M \subseteq H$ egy maximális izotróp altér úgy, hogy $W \subseteq M$. Az $M^\perp/M$-en értelmezett Q^{fs} kvadratikus forma egy $H^{\mathrm{fs}} \subseteq M^\perp/M$ kvadratikus felületet ad meg, és M maximalitásából következik, hogy $H^{\mathrm{fs}} = \{M\}$. Namármost, H^{fs} vagy hiperbólikus, vagy elliptikus. Feltéve, hogy az előbbi, a

$$2^{k-1}(2^k+1) = 1 \tag{9.10}$$

egyenletet megoldva k-ra adódik, hogy $k = \dim M^\perp/M = 0$. Következésképpen, M egy Lagrange-altér és H egy hiperbólikus kvadratikus felület. Ezután, feltéve, hogy H^{fs} elliptikus, a

$$2^{k-1}(2^k-1) = 1 \tag{9.11}$$

egyenletetből $k = \dim M^\perp/M = 1$. Mivel ekkor $M^\perp/M \cong V_1$,

$$M^\perp/M = \{M,\ \boldsymbol{x}+M,\ \boldsymbol{y}+M,\ \boldsymbol{z}+M\}, \tag{9.12}$$

és teljesülnek az alábbi összefüggések:

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \langle \boldsymbol{x}, \boldsymbol{z}\rangle = \langle \boldsymbol{y}, \boldsymbol{z}\rangle = 1 \qquad \text{és} \qquad \boldsymbol{z} = \boldsymbol{x}+\boldsymbol{y}. \tag{9.13}$$

Mivel $\boldsymbol{y}+M \notin H^{\mathrm{fs}}$, (3.6) alapján,

$$H^{\mathrm{fs}}_{\boldsymbol{y}+M} = \{M,\ \boldsymbol{x}+M,\ \boldsymbol{z}+M\}. \tag{9.14}$$

$H^{\mathrm{fs}}_{\boldsymbol{y}+M}$ egy hiperbólikus kvadratikus felület, mivel tartalmazza, például, az

$$\{M,\ \boldsymbol{x}+M\} \leq M^\perp/M \tag{9.15}$$

Lagrange-alteret. A $Q^{\mathrm{fs}}_{\boldsymbol{y}+M}$-et indukáló, V_N-et leképező $Q_{\boldsymbol{y}}$ kvadratikus forma a

$$M \cup (\boldsymbol{x} + M) \leq V_N \tag{9.16}$$

Lagrange-altéren eltűnik, ezért a $H_{\boldsymbol{y}} \subseteq V_N$ kvadratikus felület hiperbólikus. (9.6) alapján,

$$Q(\boldsymbol{y}) = Q^{\mathrm{fs}}(\boldsymbol{y} + M) = 1, \tag{9.17}$$

azaz $\boldsymbol{y} \notin H$. Következik, hogy a H kvadratikus felület elliptikus. □

9.2. Következmény. *A V_N-en értelmezett Q kvadratikus forma $H \subseteq V_N$ kvadratikus felülete ugyanolyan típusú, mint a $H^{\mathrm{fs}} \subseteq W^{\perp}/W$ indukált kvadratikus felület, amit a $W^{\perp}/W$-n értelmezett, Q által indukált Q^{fs} határoz meg.*

Ezekkel felfegyverkezve, tekintsük egy $W \subseteq V^0_{N+\dim W}$ izotróp altér $W^{\perp}/W$ szimplektikus faktorterét. A (7.1a) formulával megadott P kvadratikus forma egy $W^{\perp}/W$-n értelmezett P^{fs} kvadratikus formát indukál. (9.6) miatt P^{fs} akkor és csak akkor nullázza az $\boldsymbol{x} + W$ mellékosztályt, ha P minden $\boldsymbol{x}' \in \boldsymbol{x} + W$-re nulla. A (7.1b)-beli Q által indukált Q^{fs}-re ugyanez igaz. Következik, hogy

$$|\boldsymbol{x}_1| = |\boldsymbol{x}_2| \mod 4, \qquad \boldsymbol{x}_1, \boldsymbol{x}_2 \in \boldsymbol{x} + W \tag{9.18}$$

minden $\boldsymbol{x} + W \in W^{\perp}/W$ mellékosztályra fennáll, és ez lehetővé teszi a mellékosztályok „méretének” az értelmezését:

$$\|\cdot\| : W^{\perp}/W \to \{0, ..., 3\}, \qquad \|\boldsymbol{x} + W\| = |\boldsymbol{x}| \bmod 4. \tag{9.19}$$

Ezzel a leképezéssel P^{fs} és Q^{fs} kifejezhető úgy, hogy

$$P^{\mathrm{fs}}(\boldsymbol{x} + W) = \binom{\|\boldsymbol{x} + W\|}{2} \bmod 2 = \begin{cases} 0 & \text{ha } \|\boldsymbol{x} + W\| \in \{0, 1\}, \\ 1 & \text{ha } \|\boldsymbol{x} + W\| \in \{2, 3\}, \end{cases} \tag{9.20a}$$

$$Q^{\mathrm{fs}}(\boldsymbol{x} + W) = \binom{\|\boldsymbol{x} + W\| + 1}{2} \bmod 2 = \begin{cases} 0 & \text{ha } \|\boldsymbol{x} + W\| \in \{0, 3\}, \\ 1 & \text{ha } \|\boldsymbol{x} + W\| \in \{2, 1\}; \end{cases} \tag{9.20b}$$

vö: (7.1a) és (7.1b). Egy másik lényeges megfigyelés, hogy

$$\langle \boldsymbol{x} + W, \mathbf{1} + W \rangle_{\mathrm{fs}} = \begin{cases} 0 & \text{ha } \|\boldsymbol{x} + W\| \in \{0, 2\}, \\ 1 & \text{ha } \|\boldsymbol{x} + W\| \in \{1, 3\}. \end{cases} \tag{9.20c}$$

Tegyük fel, hogy $\mathbf{1} \in W$. Ekkor $\mathbf{1} + W = W$, és

$$C_{\mathbf{1}+W} = C_W = W^{\perp}/W, \tag{9.21}$$

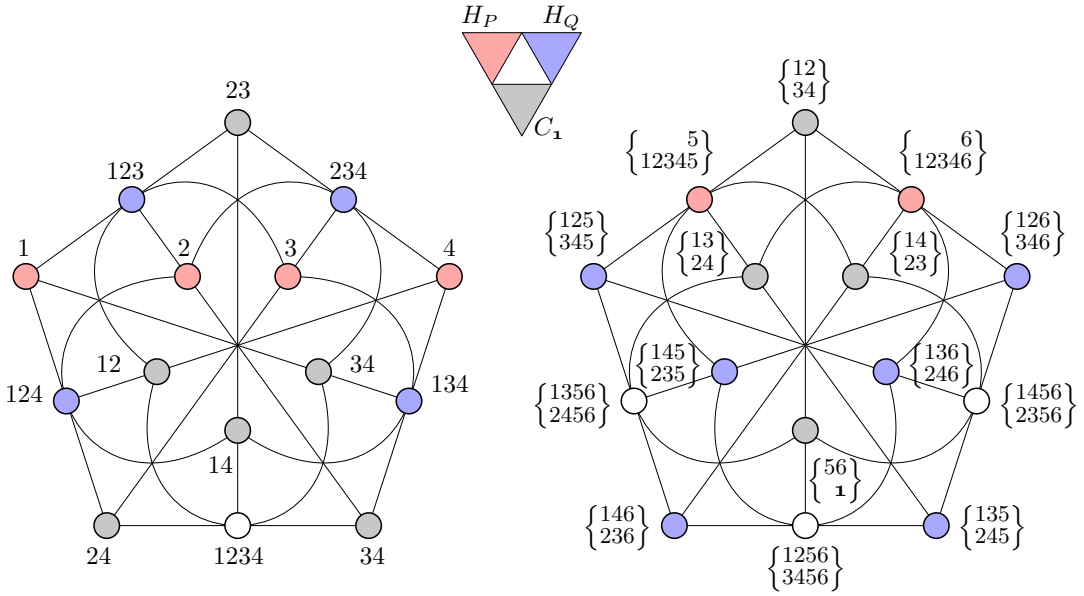
mivel W a $W^\perp/W$ faktortér nullvektora. (9.20c) miatt $\|\boldsymbol{x}+W\|$ minden $\boldsymbol{x}+W \in W^\perp/W$-re páros, és emiatt a P^{fs} által megadott H_P^{fs} és a Q^{fs} által megadott H_Q^{fs} kvadratikus felületek egybeesnek. Mivel $\mathbf{1} \in W$ csak páros $N + \dim W$ esetén fordulhat elő, és ekkor H_P és H_Q ugyanolyan típusúak, nincs ellentmondás: *H_P^{fs} és H_Q^{fs} ugyanolyan típusú, mint H_P vagy H_Q.*

Ha $\mathbf{1} \notin W$, lennie kell olyan $\boldsymbol{x}+W$ mellékosztálynak, amelyre $\|\boldsymbol{x}+W\|$ páratlan, különben minden $\boldsymbol{x} \in W^\perp$-re $|\boldsymbol{x}|$ páros. Emiatt $H_P^{\text{fs}} \neq H_Q^{\text{fs}}$, és *a $\{H_P, H_Q, C_{\mathbf{1}}\}$ kanonikus Veldkamp-egyenes egy*

$$\left\{H_P^{\text{fs}}, H_Q^{\text{fs}}, C_{\mathbf{1}+W}\right\} \tag{9.22}$$

Veldkamp-egyenest indukál, amely ugyanolyan típusú, mint az eredeti; lásd (5.14).

Az elhangzott gondolatokat a 9.1. ábra szemlélteti. Ismert, hogy $\mathcal{G}_2$ pontosan a GQ(2, 2) általánosított négyszög. A bal oldali diagram $\mathcal{G}_2$-nek a V_2 vektortér felöli megközelítését mutatja, a jobb oldali pedig azt, hogy $\mathcal{G}_2$ hogyan néz ki a $W^\perp/W$ szimplektikus faktortér szemszögéből, ahol $W = \{\mathbf{o}, 1234\} \subseteq V_3^0$. Látszik, hogy a két diagramon lévő Veldkamp-egyenesek *különböző* típusúak.



9.1. ábra. Veldkamp-egyenes a szimplektikus faktortérben

A. Függelék: $\binom{n}{2} \bmod 2$ és Q_0 tulajdonságai

Először beássuk magunkat az $f(n) = \binom{n}{2} \bmod 2$ függvény rejtelmeibe, majd a (7.9) összefüggést is bizonyítjuk. $\binom{n}{2}$ egyszerűen csak egy rövidített jelölése annak, hogy

$\frac{1}{2}n(n-1)$, ahol n bármilyen egész szám lehet. Könnyen meg lehet győződni róla, hogy a mindkét irányban végtelen $f(n)$, $n \in \mathbb{Z}$ sorozat úgy néz ki, hogy

$$\ldots \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad \mathbf{0} \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad \ldots, \tag{A.1}$$

ahol a félkövér nulla $f(0)$-t jelöli, és n balról jobbra nő. Ez a sorozat tömören úgy írható, hogy

$$f(n) = \begin{cases} 0 & \text{ha } n \bmod 4 \in \{0,1\}, \\ 1 & \text{ha } n \bmod 4 \in \{2,3\}. \end{cases} \tag{A.2}$$

Számítógépen $f(n)$-et egy olyan függvény valósítja meg, amely az n egész szám kettes-komplemens reprezentációjának *a második legkisebb helyiértékű bitjét* adja vissza. Így minden k egészre

$$f(n+2k) = \binom{n+2k}{2} = \binom{n}{2} \pm k = f(n) \pm k \mod 2. \tag{A.3}$$

Elemi algebra alapján, tetszőleges m és n egészekre igaz, hogy

$$f(m+n) = \binom{m+n}{2} = \binom{m}{2} + \binom{n}{2} + mn = f(m) + f(n) + mn \mod 2. \tag{A.4}$$

A jobb oldalon a harmadik tag a legkisebb helyiértékű bitek összeadásából származó átvitel, feltéve, hogy m és n kettes-komplemens alakban van. Az (A.4) formulában m helyébe 1-et helyettesítve,

$$f(n+1) = \binom{n+1}{2} = \binom{n}{2} + n = f(n) + n \mod 2. \tag{A.5}$$

Az (A.3) összefüggést alkalmazva a jobb oldalon, kapjuk, hogy

$$f(n+1) = \binom{3n}{2} \bmod 2 = \binom{-n}{2} \bmod 2 = \begin{cases} 0 & \text{ha } n \bmod 4 \in \{0,3\}, \\ 1 & \text{ha } n \bmod 4 \in \{2,1\}, \end{cases} \tag{A.6}$$

mivel $3 = -1 \bmod 4$.

Most már nekifoghatunk (7.9) bizonyításának. Ha $|\boldsymbol{x}| = 2$, vagyis ha valamely $i, j \in [2N]$-re $\boldsymbol{x} = ij$, (3.1) és $\langle i, j \rangle = 1$ miatt (7.9) triviálisan igaz:

$$Q_0(ij) = Q_0(i) + Q_0(j) + 1 = Q_0(i) + Q_0(j) + \binom{2}{2} \mod 2. \tag{A.7}$$

Legyen $n \notin \boldsymbol{x}$. A (7.9) formulát, mint indukciós hipotézist $Q_0(\boldsymbol{x})$-re alkalmazva,

$$\begin{aligned} Q_0(\boldsymbol{x}+n) &= Q_0(\boldsymbol{x}) + Q_0(n) + \langle \boldsymbol{x}, n \rangle \\ &= \sum_{i \in \boldsymbol{x}} Q_0(i) + \binom{|\boldsymbol{x}|}{2} + Q_0(n) + \langle \boldsymbol{x}, n \rangle \mod 2. \end{aligned} \tag{A.8}$$

A jobb oldal utolsó tagja úgy írható, hogy

$$\langle \boldsymbol{x}, n\rangle = \sum_{i\in\boldsymbol{x}} \langle i, n\rangle = |\boldsymbol{x}| \mod 2. \tag{A.9}$$

Visszahelyettesítve az (A.8) formulába, éppen az $\boldsymbol{x}+n$-re vonatkozó (7.9) adódik:

$$\begin{aligned} Q_0(\boldsymbol{x}+n) &= \sum_{i\in\boldsymbol{x}+n} Q_0(i) + \binom{|\boldsymbol{x}|}{2} + |\boldsymbol{x}| \mod 2 \\ &= \sum_{i\in\boldsymbol{x}+n} Q_0(i) + \binom{|\boldsymbol{x}|+1}{2} \mod 2 \\ &= \sum_{i\in\boldsymbol{x}+n} Q_0(i) + \binom{|\boldsymbol{x}+n|}{2} \mod 2. \end{aligned} \tag{A.10}$$

B. Függelék: a transzvekciók tulajdonságai

Az első dolog, amit a $T_{\boldsymbol{y}}$ transzvekciókkal kapcsolatban tisztázni kell az, hogy a $\mathbf{T}_{\boldsymbol{y}}$ mátrixuk szimplektikus. Ahogy a 8. szakaszban is elhangzott, az *utóbbiak* fogom transzvekcióknak hívni. $\mathbf{M}$ helyébe $\mathbf{T}_{\boldsymbol{y}}$-t helyettesítve, (8.1) bal oldala így alakul:

$$\begin{aligned} \mathbf{T}_{\boldsymbol{y}}^{\mathrm{T}}\mathbf{J}\mathbf{T}_{\boldsymbol{y}} &= (\mathbf{I}+\mathbf{J}\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}})\mathbf{J}(\mathbf{I}+\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J}) \\ &= \mathbf{J}+(\mathbf{J}\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J})+(\mathbf{J}\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J})+(\mathbf{J}\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J}\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J}). \end{aligned} \tag{B.1}$$

A jobb oldal második és harmadik tagja kiejti egymást, és a negyedik tag eltűnik, mivel középen $\boldsymbol{y}^{\mathrm{T}}\mathbf{J}\boldsymbol{y} = \langle \boldsymbol{y}, \boldsymbol{y}\rangle$. Emiatt $\mathbf{T}_{\boldsymbol{y}}$-ra (8.1) igaz, tehát $\mathbf{T}_{\boldsymbol{y}} \in \mathrm{Sp}(2N, 2)$.

Ezután megmutatom, hogy a (8.5) azonosságok fennállnak. $\mathbf{T}_{\boldsymbol{y}}$ és $\mathbf{T}_{\boldsymbol{z}}$ szorzata:

$$\begin{aligned} \mathbf{T}_{\boldsymbol{y}}\mathbf{T}_{\boldsymbol{z}} &= (\mathbf{I}+\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J})(\mathbf{I}+\boldsymbol{z}\circ\boldsymbol{z}^{\mathrm{T}}\mathbf{J}) \\ &= \mathbf{I}+(\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J})+(\boldsymbol{z}\circ\boldsymbol{z}^{\mathrm{T}}\mathbf{J})+(\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J}\boldsymbol{z}\circ\boldsymbol{z}^{\mathrm{T}}\mathbf{J}). \end{aligned} \tag{B.2}$$

A jobb oldal utolsó tagjának a közepe $\boldsymbol{y}^{\mathrm{T}}\mathbf{J}\boldsymbol{z} = \langle \boldsymbol{y}, \boldsymbol{z}\rangle$. Következésképpen,

$$\mathbf{T}_{\boldsymbol{y}}\mathbf{T}_{\boldsymbol{z}} = \mathbf{I}+(\boldsymbol{y}\circ\boldsymbol{y}^{\mathrm{T}}\mathbf{J})+(\boldsymbol{z}\circ\boldsymbol{z}^{\mathrm{T}}\mathbf{J})+\langle \boldsymbol{y}, \boldsymbol{z}\rangle(\boldsymbol{y}\circ\boldsymbol{z}^{\mathrm{T}}\mathbf{J}). \tag{B.3}$$

Ennek két fontos következménye van. Egyrészt, ha $\boldsymbol{y} = \boldsymbol{z}$, a bal oldalon $\mathbf{T}_{\boldsymbol{y}}^2$ lesz, míg a jobb oldal második és harmadik tagja kiejti egymást, és a negyedik tag eltűnik. Ez igazolja, hogy $\mathbf{T}_{\boldsymbol{y}}$ egy involúció. Másrészt, ha $\langle \boldsymbol{y}, \boldsymbol{z}\rangle = 0$, (B.3) jobb oldala $\boldsymbol{y}$-ban és $\boldsymbol{z}$-ben szimmetrikus, és ekkor $\mathbf{T}_{\boldsymbol{y}}$ és $\mathbf{T}_{\boldsymbol{z}}$ kommutálnak:

$$\mathbf{T}_{\boldsymbol{y}}\mathbf{T}_{\boldsymbol{z}} = \mathbf{T}_{\boldsymbol{z}}\mathbf{T}_{\boldsymbol{y}}. \tag{B.4}$$

Most feltételezve, hogy $\langle \boldsymbol{y}, \boldsymbol{z} \rangle = \langle \boldsymbol{y}, \boldsymbol{y} + \boldsymbol{z} \rangle = 1$, és felhanszálva a (B.3) formulát,

$$\mathbf{T}_{\boldsymbol{y}+\boldsymbol{z}} \mathbf{T}_{\boldsymbol{y}} = \mathbf{I} + [(\boldsymbol{y} + \boldsymbol{z}) \circ (\boldsymbol{y} + \boldsymbol{z})^{\mathrm{T}} \mathbf{J}] + (\boldsymbol{y} \circ \boldsymbol{y}^{\mathrm{T}} \mathbf{J}) + [(\boldsymbol{y} + \boldsymbol{z}) \circ \boldsymbol{y}^{\mathrm{T}} \mathbf{J}] \tag{B.5}$$

A zárójelek felbontása és a kétszeres tagok elhagyása után (B.3) jobb oldala adódik. Következésképpen, ha $\langle \boldsymbol{y}, \boldsymbol{z} \rangle = 1$,

$$\mathbf{T}_{\boldsymbol{y}} \mathbf{T}_{\boldsymbol{z}} = \mathbf{T}_{\boldsymbol{y}+\boldsymbol{z}} \mathbf{T}_{\boldsymbol{y}}. \tag{B.6}$$

(B.4) és (B.6) összevonható:

$$\mathbf{T}_{\boldsymbol{y}} \mathbf{T}_{\boldsymbol{z}} = \mathbf{T}_{\mathbf{T}_{\boldsymbol{y}} \boldsymbol{z}} \mathbf{T}_{\boldsymbol{y}}. \tag{B.7}$$

Ezt jobb oldalról szorozva $\mathbf{T}_{\boldsymbol{y}}$-nal, megkapjuk (8.5) második azonosságát.

C. Függelék: számtáblázatok

A perp-halmazokban és a kvadratikus felületeken lévő vektorok száma. Lásd (3.16) és (3.17).

N	1	2	3	4	5	6	7	8	9	10	11
$\lvert C_{\boldsymbol{y}} \rvert$	2	8	32	128	512	2048	8192	32 768	131 072	524 288	2 097 152
$\lvert H \rvert$, hip	3	10	36	136	528	2080	8256	32 896	131 328	524 800	2 098 176
$\lvert H \rvert$, ell	1	6	28	120	496	2016	8128	32 640	130 816	523 776	2 096 128

Az osztályok elemszáma V_N felosztásában. Lásd (7.8) és 7.2. ábra.

N	1	2	3	4	5	6	7	8	9	10	11
A típus	1	4	16	64	256	1024	4096	16 384	65 536	262 144	1 048 576
B típus	2	6	20	72	272	1056	4160	16 512	65 792	262 656	1 049 600
C típus	0	2	12	56	240	992	4032	16 256	65 280	261 632	1 047 552

Hivatkozások

[1] Francis Buekenhout and Arjeh M. Cohen. *Diagram Geometry Related to Classical Groups and Buildings*. Vol. 57. A Series of Modern Surveys in Mathematics. Springer-Verlag, 2013. URL: http://www.win.tue.nl/~amc/buek/book1n2.pdf.

[2] Bianca Letizia Cerchiai and Bert van Geemen. "From qubits to E7". In: *Journal of Mathematical Physics* 51 (12 2010), p. 122203. DOI: 10.1063/1.3519379. URL: http://arxiv.org/abs/1003.4255v1.

[3] Yaim Cooper. *Generators of the Symplectic Group*. 2005. URL: http://www-math.mit.edu/~dav/sympgen.pdf.

[4] Péter Lévay, Michel Planat, and Metod Saniga. "Grassmannian connection between three- and four-qubit observables, Mermin's contextuality and black holes". In: *Journal of High Energy Physics* Volume 2013 (9 2013), Article:37. URL: http://arxiv.org/abs/1305.5689v2.

[5] Péter Lévay and Zsolt Szabó. "Mermin pentagrams arising from Veldkamp lines for three qubits". In: (2016). URL: https://arxiv.org/abs/1608.03400.

[6] N. David Mermin. "Hidden variables and the two theorems of John Bell". In: *Rev. Mod. Phys.* 65 (3 1993), pp. 803–815. DOI: 10.1103/RevModPhys.65.803. URL: http://link.aps.org/doi/10.1103/RevModPhys.65.803.

[7] David A. Richter. "Gosset's figure in a Clifford algebra". In: *Advances in Applied Clifford Algebras* 14 (2 2004), pp. 215–224. DOI: 10.1007/s00006-004-0014-4. URL: http://www.maths.ed.ac.uk/~aar/papers/richtere8.pdf.

[8] Metod Saniga et al. "The Veldkamp Space of GQ(2,4)". In: *International Journal of Geometric Methods in Modern Physics* 7 (2010), pp. 1133–1145. URL: http://arxiv.org/abs/0903.0715.

[9] Ron Shaw. "Finite Geometry, Dirac Groups and the Table of Real Clifford Algebras". In: *Clifford Algebras and Spinor Structures: A Special Volume Dedicated to the Memory of Albert Crumeyrolle (1919–1992)*. Ed. by Rafał Ablamowicz and Pertti Lounesto. Vol. 321. Mathematics and Its Applications. Dordrecht: Springer Netherlands, pp. 59–99. ISBN: 978-94-015-8422-7. DOI: 10.1007/978-94-015-8422-7_4. URL: http://www.hull.ac.uk/php/masrs/1995/Shaw261copy2b.pdf.

[10] Ernest E. Shult. *Points and Lines Characterizing the Classical Geometries*. Berlin Heidelberg: Springer-Verlag, 2011.

[11] Péter Vrana and Péter Lévay. "The Veldkamp space of multiple qubits". In: *Journal of Physics A: Mathematical and Theoretical* 43.12 (2010), p. 125303. URL: https://arxiv.org/abs/0906.3655v3.