



## TDK DOLGOZAT

Rejtett paraméterek és véges geometriai  
módszerek a kvantummechanikában

Szabó Zsolt

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

BME

2015. november 4.

## Előszó, bevezetés

A kvantummechanika jellegzetességei közé tartozik, hogy a mérések nem egy meglévő értéket fednek fel, hanem eredményük a mérési folyamat során jön létre. A problémát, amire részben ez a válasz, Einstein, Podolsky és Rosen vetették fel híressé vált [9] cikkükben. A megoldásban döntő szerepe volt John Bell-nek, akinek a nevéhez a Bell- és a Bell–Kochen–Specker-tétel fűződik [10, 3, 4, 15, 16].

Az elmúlt pár évtizedben a Bell–KS-tétel azok számára is elérhetővé vált, akik „kevésbé hajlandók sivár bizonyításokat végigszenvedni” [15]. A középpontban 2 vagy annál több q bites, egymással speciálisan kommutáló vagy antikommutáló Pauli-operátorokból felépülő konfigurációk (*Bell–KS-konfigurációk*) állnak. A dolgozatban ezek közül vizsgálok meg néhányat, és miközben ismertetem az erre specializálódott módszereket, egy újabb konfigurációkhoz vezető utat is felvázolok.

Az első néhány részében bevezetem azokat a fogalmakat, amelyek segítségével a rejtett paraméterek és a kontextualitás problémája kényelmesen elmondható. Ezt úgy valósítom meg, hogy a BSc Kvantummechanika kurzusban megszokottnál szorosabbra fűzöm a kvantumelmélet és a valószínűségszámítás közti kapcsolatot. Habár hasonló elképzeléseim régóta vannak, a gondolatok jelen alakját, amelynek itt csak egy rövidített változatát ismertetem, legfőképp Asher Peres [18] és Rényi Alfréd [2] kiváló művei inspirálták.

A hátralevő részekben összefoglalom a matematikai apparátus lényeges elemeit, és így, remélhetőleg, sikerül kialakítanom a nyelvet, amivel az elért eredményeket érthetően el tudom mondani. A gondolatmenet folytonossága érdekében itt jegezném meg, hogy egyértelműen saját eredménynek az utolsó négy rész anyagát tekintem.

A vizsgálódás során használt programot és az ábrákhoz használt segédprogramot *Lazarus*-ban<sup>1</sup> írtam. Az előbbi fejlődése során alkalmam volt megfigyelni, hogy a programkódban milyen változások következnek be, amikor a sejtések elfogadott tényekké válnak, és ahogy a sejtések igazolására szánt kódrészleteket fokozatosan a sejtést *alkalmazó*, és majd újabb sejtésekhez vezető kódrészletek váltják fel.

A két program szorosan együttműködik. Az ábrázoló segédprogramban elkészítettem a kívánt konfiguráció diagramját, és az hozta létre a kódrészletet, amely a másik programban a diagramot és a pontokhoz tartozó operátorokat automatizáltan jeleníti meg. Máskor az automatizált diagramból született meg a szkript, amelyet az ábrázoló segédprogram képes értelmezni. A split Cayley hexagon diagramját is így készítettem el az Andreas Schroth-féle [22] ábrázolást véve alapul. A paramétereken változtattam, hogy a Heawood-gráf jobban látszodjon.

---

<sup>1</sup>URL: [lazarus.freepascal.hu](http://lazarus.freepascal.hu)

Köszönöm a családomnak a megértést és a támogatást.

Köszönöm *Dr. Orosz Lászlónak*, hogy a dolgozat bírálását elvállalta. A kvantummechanikát, és a fizikát általában, az ő előadásain szerettem meg.

Végezetül pedig köszönöm a konzulensemnek, *Dr. Lévy Péternek*, hogy a kezdetektől fogva támogatott, a nehézségek ellenére kitartott, mindig türelmes volt, és soha nem helyezett nyomást rám.

Szabó Zsolt  
Budapest, 2015. november 4.

# Tartalomjegyzék

<b>1. A kvantumelmélet elemei</b>	<b>1</b>
1.1. Kauzális, sztochasztikus és kvantum szkéma . . . . .	1
1.2. Valószínűségi változók és megfigyelhető mennyiségek . . . . .	6
1.3. Egy- és több-qubit rendszerek . . . . .	8
1.4. Bell–KS-konfigurációk . . . . .	10
<b>2. <math>GF(2)</math> feletti szimplektikus vektorterek tulajdonságai</b>	<b>12</b>
2.1. Pauli-csoport szimplektikus struktúrája . . . . .	12
2.2. Alterek, Gauss-együtthatók . . . . .	13
2.3. Izotróp és Lagrange-alterek . . . . .	14
2.4. Szimplektikus bázis, szimplektikus transzformáció . . . . .	16
<b>3. A véges geometria elemei</b>	<b>18</b>
3.1. Gráfelméleti alapfogalmak . . . . .	18
3.2. Illeszkedési rendszer és geometria . . . . .	20
3.3. Pont-egyenes geometria, általánosított $n$ -szög . . . . .	21
3.4. Néhány konkrét példa . . . . .	23
<b>4. Geometriák beágyazása és címkézése</b>	<b>28</b>
4.1. Szimplektikus poláris tér . . . . .	28
4.2. Ekvivalens és nemekvivalens címkézések . . . . .	29
4.3. $W(3, 2)$ és a doily izomorfája, Mermin-négyzetek . . . . .	30
4.4. A hexagon klasszikus beágyazása $W(5, 2)$ -be . . . . .	31
4.5. A $(10_2, 5_4)$ pentagramma $W(5, 2)$ -be képező címkézése . . . . .	32
4.6. A hexagon és a $(10_2, 5_4)$ pentagramma címkézéseinek a kapcsolata . . . . .	36
4.7. Pentagrammák címkézéseinek értelmezett műveletek . . . . .	38
4.8. 9+1-es geometria $W(5, 2)$ -be képező címkézése . . . . .	42
<b>Hivatkozások</b>	<b>43</b>

# 1. A kvantumelmélet elemei

## 1.1. Kauzális, sztochasztikus és kvantum szkéma

A stratégiát, hogy környezetünk valamely *megismétlődő* hatására minden alkalommal ugyanazt a választ adjuk, egyszerűsége miatt már ősidők óta használjuk. Szemben azzal, hogy alacsonyabb rendű szervezetek „egy, a kiváltó kauzalitás értelmében hatásos külső behatást, nevezetesen az *ingert* egy mozgási folyamattal vagy az anyagok kiválasztásával, szekrécióval válaszolnak meg”, „az ideg- és izomrendszer magasabb rendű állatoknál megjelenő munkamegosztása hozza magával, hogy ezek az élőlények anélkül képesek ingereket felvenni és értékelni, hogy azonos módú mozgásokkal reagálnának rájuk” [11]. Ez utóbbi speciális eseteként az ember, már tudatosan, *események bekövetkezéséről* beszél, ezeket vizsgálja és jóslgatja, és késleltetett reakcióit a velük kapcsolatos megállapításokra alapozza.

Definíciószerűen *kauzális szkémába* [2] tartoznak azok a szituációk, amikor bizonyos  $K$  feltételek teljesülése mellett valamilyen  $A$  esemény biztosan bekövetkezik (*szükségszerű esemény*). Ez a motívum megtalálható tudathoz nem kapcsolható mechanizmusok működésében, mint pl. a reflex, és a modern elméleti modellek olyan építőelemeiben, mint a *logikai következtetés* ( $K$  a premissza,  $A$  a konklúzió) vagy a *függvény* ( $K$  a paraméter,  $A$  a függvény szerinti kép).

A  $K$  feltételek megfigyelője nem egy kívülálló passzív szerepét tölti be, hanem  $K$  „létrehozásához” ő is hozzájárul. Vagyis a megfigyelő egy (a szokásosnál tágabb értelemben vett) *kísérletet* hajt végre, amitől a  $K$  feltételek elválaszthatatlanok. A továbbiakban a kísérletet és a feltételeket is ugyanaz a szimbólum jelöli.

Bizonyos esetekben a  $K$  kísérlet végrehajtásakor bekövetkezhet az  $A$  esemény, de  $A$ -tól különböző  $B$ ,  $C$ , ..., események is bekövetkezhetnek (*véletlen események*). Az ilyen jelenségek nem illenek a kauzális szkémába, ekkor ún. *sztochasztikus szkémáról* van szó. A kauzális szkémához hasonlóan ismét feltételezett, hogy a  $K$  körülmények *megismétlődően* vagy *megismételhetően* bukkannak elő, és ezért az egyes események *relatív gyakorisága* elvileg mérhető. Ha az  $A$  esemény relatív gyakorisága egy adott érték körül ingadozik, ez az érték  $A$  *valószínűsége* [2].

A sztochasztikus szkéma matematikai modellje a (*Kolmogorov-féle*) *valószínűségi mező*. A valószínűségi mező egy  $S = (\Omega, \mathcal{A}, \mathbf{P})$  hármas, ahol

- $\Omega$  az *eseménytér*;
- $\mathcal{A} \subseteq 2^\Omega$  az *eseményalgebra*, elemei az *események*;
- $\mathbf{P} : \mathcal{A} \rightarrow \mathbb{R}$  a *valószínűség*.

Az  $\mathcal{A}$  eseményalgebra egy  $\sigma$ -algebra, ami azt jelenti, hogy

1. az  $\Omega$  biztos esemény eleme  $\mathcal{A}$ -nak;
2. minden  $A \in \mathcal{A}$  esemény  $\bar{A} \equiv \Omega \setminus A$  ellentéte eleme  $\mathcal{A}$ -nak, azaz  $\mathcal{A}$  zárt a komplementer-képzésre;
3. megszámlálhatóan sok  $A_1, A_2, \dots \in \mathcal{A}$  esemény  $\bigcup_{i=1}^{\infty} A_i$  összege eleme  $\mathcal{A}$ -nak, azaz  $\mathcal{A}$  zárt a megszámlálható unióra.

Ezekből az axiómákból levezethető, hogy  $\mathcal{A}$  tartalmazza az  $\emptyset$  lehetetlen eseményt, két  $A, B \in \mathcal{A}$  esemény  $A \setminus B$  különbségét, és megszámlálhatóan sok esemény  $\bigcap_{i=1}^{\infty} A_i$  szorzatát ( $\mathcal{A}$  zárt a megszámlálható metszetre).

$A, B \in \mathcal{A}$  egymást kizáró események, ha  $A \cap B = \emptyset$ , és  $A$  maga után vonja  $B$ -t, ha  $A \subseteq B$ .  $A \in \mathcal{A}$  elemi esemény, ha nem írható fel két tőle különböző esemény összegeként, és ekkor minden  $B \in \mathcal{A}$  eseményre  $A \subseteq B$  vagy  $A \cap B = \emptyset$ .

A  $\mathbf{P}$  valószínűség egy halmazfüggvény, amelyre teljesülnek az alábbiak:

1. a biztos esemény valószínűsége egységnyi:  $\mathbf{P}(\Omega) = 1$ ;
2. ha  $A_1, A_2, \dots \in \mathcal{A}$  egymást páronként kizáró események,

$$\mathbf{P}\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mathbf{P}(A_i). \quad (1.1)$$

Ezekből következik, többek között, hogy a lehetetlen esemény valószínűsége 0,  $\bar{A}$  valószínűsége  $1 - \mathbf{P}(A)$ , és  $A \subseteq B$  esetén  $\mathbf{P}(A) \leq \mathbf{P}(B)$ . Az utóbbi alapján, ha egy  $A$  elemi esemény valószínűsége 1, akkor minden  $B \in \mathcal{A}$  esemény valószínűsége 1 (ha  $A$  maga után vonja  $B$ -t) vagy 0 (ha  $A$  és  $B$  egymást kizárják).

\* \* \*

A kvantumelmélet szempontjából érdekes sztochasztikus skémák  $K$  feltételei  $P$  előkészítésre és  $T$  tesztre bonthatók fel. Egy kvantum skémába<sup>2</sup> sorolható szituációban több, egy  $P$  előkészítés és egy  $T$  teszt párosításával megvalósuló  $K = (P, T)$  kísérlet lehetséges; ezek megismételhetősége és a figyelembe vett események valószínűségének a létezése most is elengedhetetlen kritérium.

A  $(P, T)$  kísérlethez tartozó valószínűségi mezőt jelölje  $S_{P,T}$ . Ennek az eseménytere és eseményalgebrája definíciószerűen csak a  $T$  tesztől függ (a  $P$  előkészítéstől

---

<sup>2</sup>Saját elnevezés.

független), ezért kényelmesebb  $T$  eseményeiről beszélni. Az elemi események  $T$  kimenetelei. Ha a  $P$  előkészítés a szövegkörnyezetből egyértelmű, vagy csak a megléte lényeges, az  $S_{P,T}$  valószínűségi mező  $T$ -hez tartozik, és  $T$  elvégzése a  $(P, T)$  kísérlet elvégzését jelenti.

A definíció következményeként, rögzített  $T$  mellett, az  $S_{P,T}$  és  $S_{P',T}$  valószínűségi mezők csak a valószínűségben térhetnek el. Ez alapján az előkészítéseken egy ekvivalencia-reláció értelmezhető:  $P$  és  $P'$  ekvivalens előkészítések, ha az  $S_{P,T}$  és  $S_{P',T}$  valószínűségi mezők minden figyelembe vett  $T$  tesztre megegyeznek. Az ekvivalencia kísérleti ellenőrzésének az elvi lehetősége adott, mivel az események valószínűsége a relatív gyakoriságok mérésével meghatározható.

A kvantumelméletben elterjedt szóhasználattal, az ekvivalens előkészítések adott állapotú rendszert állítanak elő, vagyis az állapotok az előkészítések ekvivalenciaosztályainak tekinthetők. A kifejezés által sugallt szemlélettel ellentétben az állapot *nem* a rendszer megfigyelőtől független objektív tulajdonsága, vagy más szavakkal: nem rendelkezik fizikai realitással.

Az állapot csak a megfigyelő képzeletében létezik, és újabb információk hatására pillanatszerűen változik meg abban a szintén képzeletbeli vonatkoztatási rendszerben, amelyben a megfigyelő a számításait elvégzi [17].

Egy  $T$  teszt *maximális*, ha minden kimenetelére igaz, hogy minden olyan állapotra, amelyre  $T$  adott kimenetele biztosan bekövetkezik, az összes többi teszt minden kimenetelének a valószínűsége az állapottól független<sup>3</sup>. Nem maximális tesztekkel olyan eseteket lehet kifejezni, amikor a kísérlet során használt mérőműszer felbontóképesége nem elég nagy ahhoz, hogy más tesztekkel megkülönböztethető eseményeket szétválasszon. A maximális teszt fogalma nem abszolút: hogy melyik kísérletben tekinthető a teszt maximálisnak, a rendelkezésre álló eszközöktől és a kísérlet céljától függ.

Az előállított rendszer *tiszta állapotban van*, ha valamely maximális teszt kimenetele meghatározott [18]. A továbbiakban *állapot* alatt mindig tiszta állapotot kell érteni, az ún. *kevert állapotok* ebben a dolgozatban nem lesznek érintve.

$T$  és  $T'$  *nem kompatibilis tesztek*, ha  $T$ -nek valamely  $A$  kimenetelére teljesül, hogy minden olyan állapotra (előkészítésre), amelyre  $A$  biztosan bekövetkezik,  $T'$  minden kimenetelének a valószínűsége 1-nél kisebb, és  $T'$ -re is hasonló igaz.

Speciális esetben minden olyan állapotra, amelyre  $T$  kimenetele meghatározott,  $T'$  kimenetelei „egyforma” valószínűségűek, és fordítva. Erre klasszikus példa a hely és az impulzus mérése. Niels Bohr EPR [9] cikkére adott [5] válaszában részletesen kifejti, hogy a kísérletező a helyméréssel hogyan fosztja meg magát

---

<sup>3</sup>Asher Peres [18] könyvében a maximális tesztek ettől különböző definíciója található. A dolgozat szerzője azt önkényesen egy kicsit átírta, hogy céljainak jobban megfeleljen.

az impulzusmérés lehetőségétől, és fordítva. Bohr erre a *komplementaritás* szót használja, és azt érti alatta, hogy a két leírás (hely és impulzus) kiegészíti egymást.

A kvantum szkéma tehát valószínűségi mezők gyűjteménye, és ezek között vannak olyanok is, amelyek nem kompatibilis tesztekhez tartoznak. Az  $S_{P,T}$  valószínűségi mezők, egymástól függetlenül kezelve, egyetlen  $S_0$  valószínűségi mezővel helyettesíthetők úgy, hogy ha  $S_0$ -nak valamelyik elemi eseménye bekövetkezik, minden  $S_{P,T}$  valószínűségi mezőben minden eseményre adott, hogy bekövetkezett vagy nem. Ekkor az előállított rendszer állapota az  $S_0$ -beli valószínűséget adja meg, és a mérési eredményeket reprodukáló,  $S_{P,T}$ -beli valószínűségek ebből csak közvetett módon származnak. Így a klasszikus statisztikus fizika leírásmódjával ekvivalens leírás adódik. Az ún. *kontextuális rejtett-paraméter elméletek* ezt valósítják meg.

A Bell–KS-tétel a *nem kontextuális rejtett-paraméter elméletek*<sup>4</sup> lehetőségét vizsgálja: megtehető az  $S_0$ -lal való helyettesítés akkor is, ha a valószínűségi mezők nem függetlenek, abban az értelemben, hogy az eseményalgebrák nem diszjunktak? Ekkor, ha  $A$  több valószínűségi mező eseménye, egyszerre kell bekövetkeznie az *összes* ilyen valószínűségi mezőben, és ezekben az  $A$  által kizárt események nem következhetnek be. A kérdésnek legfőképp a nem kompatibilis tesztek miatt van jelentősége, és a helyzet iróniája, hogy kísérletileg éppen ezek miatt nem eldönthető: nincs értelme azt feszegetni, hogy „*mi lett volna ha*”  $T$  helyett a vele nem kompatibilis  $T'$  teszt lett volna elvégezve.

A Bell–KS-tétel a kérdést egy logikai ellentmondással, azaz a matematikai apparátusra visszavezetve válaszolja meg. Ehhez viszont a nem kompatibilis tesztek eseményei közti kapcsolatok leírására is szükség van. Erre, és az események valószínűségének a kiszámítási módjára eszközöket a kvantum szkéma matematikai modellje biztosít. Ez a modell nem egyértelmű, pl. a „megszokott” modell komplex Hilbert-tere kvaterniók feletti Hilbert-térre általánosítható [1].

\* \* \*

Legyen  $\mathcal{H}$  egy Hilbert-tér, és az egyszerűség kedvéért legyen véges dimenziós.  $\mathcal{H}$  alkalmas arra, hogy egy kvantum szkéma matematikai modellje rá épüljön, mivel a vele kapcsolatos fogalmak segítségével valószínűségi mezők állíthatók elő, vagy röviden:  $\mathcal{H}$  *valószínűségi mezőket indukál*.

$\mathcal{H}$  minden valószínűségi mezője  $\Omega$  eseményterét  $\mathcal{H}$ -nak valamely ortonormált bázisa valósítja meg, amiből következik, hogy az eseményterek azonos elemszámúak. Az eseményalgebrák a  $\sigma$ -algebra axiómáinak betartása mellett tetszőlegesek lehetnek, rájuk  $\mathcal{H}$ -ból csak az a megkötés származik, hogy végesek. Az  $\Omega$  eseménytérhez

<sup>4</sup>A kifejezés pontos jelentését ld. később.



és  $\mathcal{A} \subseteq 2^\Omega$  eseményalgebrához tartozó teszt maximális, ha az elemi események egyelemű halmazok, azaz ha  $\mathcal{A} = 2^\Omega$ .

A rendszer állapotát egy  $|\psi\rangle \in \mathcal{H}$  egységvektor reprezentálja, és ebből az egyes események valószínűsége a következő szabállyal számolható. Minden  $A$  esemény (páronként ortogonális) vektorokból álló halmaz lévén  $\mathcal{H}$ -nak egy  $\langle A \rangle$  alterét feszíti ki, amelyhez egyértelműen tartozik egy  $\hat{P}_{\langle A \rangle}$  ortogonális projektor. Az  $A$  esemény valószínűsége ekkor

$$\mathbf{P}(A) = \|\hat{P}_{\langle A \rangle}|\psi\rangle\|^2. \quad (1.2)$$

Ez a halmazfüggvény teljesíti a valószínűség axiómáit:

1. Mivel  $\langle \Omega \rangle = \mathcal{H}$ ,  $\hat{P}_{\mathcal{H}}$  az egységoperátor, így  $\mathbf{P}(\Omega) = \|\psi\|^2 = 1$ .
2. Mivel  $\Omega$  és  $\mathcal{A}$  véges, a (1.1) kifejezésnek csak véges sok, egymást kizáró  $A_1, \dots, A_n \in \mathcal{A}$  eseményre való teljesülését kell ellenőrizni. Tetszőleges  $A_1, \dots, A_n$  vektorhalmazokra igaz, hogy

$$\langle A_1 \cup \dots \cup A_n \rangle = \langle A_1 \rangle + \dots + \langle A_n \rangle.$$

Felhasználva, hogy az  $\langle A_i \rangle$  alterek ortodiszjunktak<sup>5</sup>,

$$\hat{P}_{\langle A_1 \rangle + \dots + \langle A_n \rangle} = \hat{P}_{\langle A_1 \rangle} + \dots + \hat{P}_{\langle A_n \rangle}.$$

Következik, hogy

$$\begin{aligned} \mathbf{P}(A_1 \cup \dots \cup A_n) &= \|\hat{P}_{\langle A_1 \cup \dots \cup A_n \rangle}|\psi\rangle\|^2 = \|\hat{P}_{\langle A_1 \rangle + \dots + \langle A_n \rangle}|\psi\rangle\|^2 \\ &= \|\hat{P}_{\langle A_1 \rangle}|\psi\rangle + \dots + \hat{P}_{\langle A_n \rangle}|\psi\rangle\|^2 \\ &= \|\hat{P}_{\langle A_1 \rangle}|\psi\rangle\|^2 + \dots + \|\hat{P}_{\langle A_n \rangle}|\psi\rangle\|^2 \\ &= \mathbf{P}(A_1) + \dots + \mathbf{P}(A_n). \end{aligned}$$

Az utolsó előtti egyenlőség a Pitagorasz-tétel<sup>6</sup>, amely alkalmazható, mivel a  $\hat{P}_{\langle A_i \rangle}|\psi\rangle$  vektorok páronként ortogonálisak.

A tapasztalattal csak az események valószínűségei vethetők össze. Az (1.2) kifejezésből látható, hogy  $|\psi\rangle$ -t és az  $A$ -beli vektorokat egységnyi abszolút értékű skalárral szorozva  $\mathbf{P}(A)$  nem változik. Emiatt akárhányszor egységvektorról van szó, hacsak az ellenkezője nincs külön jelezve, mindig egy  $e^{i\varphi}$ ,  $\varphi \in \mathbb{R}$  faktor

<sup>5</sup>Az  $U, V \leq \mathcal{H}$  alterek *ortodiszjunktak*, ha bármely nemnulla  $|u\rangle \in U$ -ra és  $|v\rangle \in V$ -re  $\langle u | v \rangle = 0$ . Ebből következik, hogy  $U \cap V = \{\mathbf{0}\}$ .

<sup>6</sup>A véges eseménytér és eseményalgebra nem jelent lényegi megkötést, hanem csak kényelmi célokat szolgál, hogy ne kelljen határértékekkel számolni.

erejéig rögzített egységvektort, vagy ami ezzel ekvivalens, az egységvektor által kifeszített 1-dimenziós alteret, *sugarat* kell érteni, és az indukált valószínűségi mezők eseményterét is ennek a figyelembevételével kell összehasonlítani.

Következik, hogy  $\mathcal{H}$  ortonormált bázisai maximális tesztek reprezentálnak, és a valószínűség (1.2) kifejezése alapján a különböző bázisokhoz tartozó maximális tesztek nem kompatibilisek.

A bevezetett fogalmakkal a Bell–KS-tétel kérdésfeltevése szemléletesen így hangzik: kifesthetők a maximális tesztek elemi eseményei, vagy ezzel ekvivalens módon, a Hilbert-tér egységvektorai, pirosra vagy zöldre úgy, hogy a zöld vektorokra ortogonális vektorok pirosak legyenek [18]?

A zöld, illetve piros szín az elemi események bekövetkezését, illetve be nem következését jelenti, a piros vektorok zöldekre való ortogonalitása pedig azt, hogy egy elemi esemény bekövetkezése minden valószínűségi mezőben, amelynek eseménye, az összes többi elemi esemény bekövetkezését kizárja.

Kétdimenziós Hilbert-térben a kifestés lehetséges, de ekkor a  $\mathcal{H}$ -beli valószínűségi mezők eseményalgebrái alaphól diszjunktak. Egy  $\dim \mathcal{H} > 2$ -re vonatkozó nemleges választ elsőként Kochen és Specker [10] adtak úgy – és itt a módszer a fontos, ugyanis John Bell, Andrew Gleason eredményét felhasználva, már előttük megoldotta a feladatot [4] –, hogy összeállítottak egy 117 vektorból álló halmazt, amelynek a fenti feltételekkel való kiszínezése lehetetlen. Az évek során egyre kevesebb vektorból álló halmazok születtek, és mára sikerült erre a geometriai problémára adott választ algebrai ellentmondásként megfogalmazni.

## 1.2. Valószínűségi változók és megfigyelhető mennyiségek

A megfogalmazásban fontos szerepet játszanak az önadjungált operátorok, vagy *megfigyelhető mennyiségek*. Míg a sztochasztikus szkéma méréssel kapcsolatos fogalma, a valószínűségi változó, pusztán csak leképezi az egyetlen valószínűségi mező eseményterét, a vele analóg kvantum szkémabeli fogalom, az önadjungált operátor, már arra vonatkozó információt is tartalmaz, hogy *melyik* valószínűségi mezőben viselkedik valószínűségi változóként. A részletek a következők.

Legyen  $S_A = (\Omega, \mathcal{A}, \mathbf{P})$  és  $S_B = (\Theta, \mathcal{A}', \mathbf{Q})$  két valószínűségi mező. A  $\xi : \Omega \rightarrow \Theta$  függvény valószínűségi mezők közti homomorfizmus, ha

1. minden  $B \in \mathcal{B}$ -re  $\xi^{-1}(B) \in \mathcal{A}$ ;
2.  $\mathbf{Q}(B) = \mathbf{P}(\xi^{-1}(B))$ .

Ha speciálisan  $\Theta = \mathbb{R}$  és  $\mathcal{A}' = \mathcal{B}$ , ahol  $\mathcal{B}$  a Borel-féle  $\sigma$ -algebra<sup>7</sup>,  $\xi$  egy *valószínűségi*

<sup>7</sup>A legszűkebb  $\sigma$ -algebra, amely az  $(a, b] \subseteq \mathbb{R}$  intervallumokat tartalmazza.

változó.  $\xi$  diszkrét valószínűségi változó, ha értékkészlete megszámlálható. A diszkrét valószínűségi változóknak egy fontos speciális esete az  $A \in \mathcal{A}$ ,  $A \neq \emptyset$  esemény indikátor valószínűségi változója:

$$\xi_A(\omega) = \begin{cases} 0, & \text{ha } \omega \notin A, \\ 1, & \text{ha } \omega \in A. \end{cases}$$

A  $\xi$  és  $\zeta$  valószínűségi változókból összeadással és szorzással újabb valószínűségi változók állíthatók elő: minden  $\omega \in \Omega$ -ra

$$\begin{aligned} (\xi + \zeta)(\omega) &= \xi(\omega) + \zeta(\omega), \\ (\xi \cdot \zeta)(\omega) &= \xi(\omega)\zeta(\omega). \end{aligned}$$

Egy  $\hat{A}$  önadjungált operátor sajátértékei valósak, és különböző sajátértékekhez ortogonális sajátvektorok tartoznak. Emiatt, minden olyan  $\Omega$  ortonormált bázisra, amelyben diagonális<sup>8</sup>,  $\hat{A}$  egy  $\alpha : \Omega \rightarrow \mathbb{R}$  leképezést határoz meg: az  $|\omega\rangle \in \Omega$  bázisvektorhoz  $\alpha$  hozzárendeli  $\hat{A}$ -nak az  $|\omega\rangle$ -hoz tartozó sajátértékét. Ha  $S$  egy  $\Omega$  eseményterű valószínűségi mező, és eseményalgebrája minden  $B \in \mathcal{B}$ -re  $\alpha^{-1}(B)$ -t tartalmazza,  $\alpha$  az  $\hat{A}$  által  $S$ -ben indukált valószínűségi változó. Ha  $\hat{A}$  egy projektor,  $\alpha$  egy indikátor valószínűségi változó.

Ha  $\hat{A}$  degenerált, azaz van többszörös sajátértéke, az  $\Omega$  bázis, amelyben  $\hat{A}$  diagonális, nem egyértelmű. Ekkor a valószínűségi mezők, amelyekben  $\hat{A}$  valószínűségi változót indukál, akár nem kompatibilis tesztekhez is tartozhatnak. Ezek a valószínűségi változók különböző kísérleti elrendezésben elvégzett méréseket jelentenek, és a köztük lévő kapcsolat a kvantum szkéma matematikai modelljének a szintjén reprezentált: minden elrendezésben „ $\hat{A}$  mérése” történik.

Egy nem kontextuális rejtett-paraméter elmélet szerint, ha  $\hat{A}$ -nak valamely  $\lambda$  sajátértékéhez tartozó sajátvektora zöldre van festve, minden  $\mu \neq \lambda$ -hoz tartozó sajátvektor piros kell, hogy legyen. Ez azt jelenti, hogy a kifestés minden  $\hat{A}$  által indukált valószínűségi változó értékét  $\lambda$ -ra rögzíti, ami úgy is mondható, hogy „az  $\hat{A}$  megfigyelhető mennyiség értéke rögzített” (ld. pl. [15]). A kifestés ekvivalens a  $\mathcal{H}$  sugaraihoz tartozó projektorok értékének a rögzítésével úgy, hogy ha egy projektor értéke 1, minden, vele kommutáló projektor értéke 0.

Egy nemdegenerált  $\hat{A}$  önadjungált operátor meghatározza azt a maximális teszt-hez tartozó valószínűségi mezőt, amelyben valószínűségi változóként viselkedik. Emiatt egy nemkontextuális rejtett-paraméter elmélet létjogosultsága kísérletileg csak degenerált  $\hat{A}$  operátor méréssel dönthető el. Mivel  $\hat{A}$  értékének a rögzítését

<sup>8</sup>Pontosabban, ha a mátrixa diagonális a bázisban, de ettől a precízkedéstől a tömörség kedvéért érdemes eltekinteni.

nem kompatibilis tesztek elvégzésével kellene kimutatni, ilyen kísérlet nem létezik:  $\hat{A}$  ugyanazon az előállított rendszeren csak az egyik elrendezésben mérhető. Így a rejtett-paraméter elmélet azon állítása – ugyanis csak így lehet azt értelmezni –, hogy  $\hat{A}$ -t másik elrendezésben mérve az eredmény *ugyanaz lett volna*, értelmetlen.

Több önadjungált operátor szimultán mérése olyan  $T$  teszt elvégzésével történik, amelyre az  $S_{P,T}$  valószínűségi mezőben mindegyikük valószínűségi változót indukál. Ahhoz, hogy ilyen tesztről egyáltalán beszélni lehessen, szükséges, hogy az operátorok páronként kommutáljanak, különben  $\mathcal{H}$ -nak egyetlen ortonormált bázisa sem diagonalizálja mindannyiukat.

A „nem kontextuális rejtett-paraméter elmélet” kifejezésben a „nem kontextuális” jelentése a következő. Egy  $\hat{A}$  önadjungált operátor mérésének a *kontextusa* azoknak az  $\hat{A}$ -val, és egymás közt is, kommutáló operátoroknak a halmaza, amelyek mérése  $\hat{A}$  mérésével szimultán történik.  $\hat{A}$ -nak a  $\hat{B}_1, \hat{B}_2, \dots$  és a  $\hat{C}_1, \hat{C}_2, \dots$  operátorokkal való szimultán mérése, ha  $\hat{B}_i$  és  $\hat{C}_j$  nem feltétlenül kommutálnak, két különböző elrendezésben való mérést jelent.

Ha egy nem kontextuális rejtett-paraméter elmélet az  $\hat{A}, \hat{B}_1, \hat{B}_2, \dots$  operátoroknak egy közös  $|\lambda\rangle$  sajátvektorát zöldre festi, és ez  $\hat{A}$ -nak a  $\lambda$  sajátértékéhez tartozó sajátvektora, az  $\hat{A}, \hat{C}_1, \hat{C}_2, \dots$  operátoroknak a közös  $|\mu\rangle$  sajátvektora nem festhető zöldre, ha  $\hat{A}|\mu\rangle = \mu|\mu\rangle$  és  $\mu \neq \lambda$ , mivel ekkor  $|\lambda\rangle$  és  $|\mu\rangle$  ortogonálisak. Következik, hogy az elmélet szerint  $\hat{A}$  értéke a *kontextustól független*.

Ha egy  $S$  valószínűségi mezőben  $\hat{A}$ , illetve  $\hat{B}$  az  $\alpha$ , illetve  $\beta$  valószínűségi változókat indukálják,  $\hat{A} + \hat{B}$  és  $\hat{A}\hat{B}$  újabb valószínűségi változókat indukálnak  $S$ -ben, nevezetesen  $\alpha + \beta$ -t és  $\alpha\beta$ -t. Az állítás a négy operátor diagonális alakjából azonnal látszik, és csak kommutáló  $\hat{A}$  és  $\hat{B}$  operátorokra igaz; általában  $\hat{A} + \hat{B}$ , illetve  $\hat{A}\hat{B}$  teljesen más elrendezésben mérhető, mint  $\hat{A}$  vagy  $\hat{B}$ .

Egy nem kontextuális rejtett-paraméter elmélet, azáltal, hogy  $S$  eseményteréből valamelyik  $|\omega\rangle$  vektort zöldre festi, a négy operátorhoz hozzárendeli valamelyik sajátértékét úgy, hogy ha  $\hat{A}$ -hoz  $v(\hat{A})$  és  $\hat{B}$ -hez  $v(\hat{B})$  tartozik, akkor  $\hat{A} + \hat{B}$  és  $\hat{A}\hat{B}$  kiválasztott sajátértéke rendre [16, 15]

$$v(\hat{A} + \hat{B}) = v(\hat{A}) + v(\hat{B}), \quad (1.3a)$$

$$v(\hat{A}\hat{B}) = v(\hat{A})v(\hat{B}). \quad (1.3b)$$

### 1.3. Egy- és több-qubit rendszerek

A valószínűségi mező és a valószínűségi változó absztrakt fogalma csak egy keretrendszert alkot, konkrét problémák megoldásához további feltételezések, a problémát leíró *modellek* kellenek. Ezek megadják az eseményeket és azok valószínűségeit,

esetleg valószínűségi változókat is bevezetnek (ld. pl. binomiális eloszlás, Poisson-eloszlás stb.). Ugyanez a kvantumelméletre is igaz.

A lehető legegyszerűbb modell arra az esetre vonatkozik, amikor egy maximálisnak tekintett  $T$  tesztnek két lehetséges kimenetele van. Ekkor az előállított rendszer, elterjedt néven *qubit*, kétállapotú, és az őt leíró  $\mathcal{H}_2$  Hilbert-tér 2-dimenziós.

A  $T$  tesztet  $\mathcal{H}_2$ -nek egy kitüntetett bázisa reprezentálja, és az önadjungált operátorok erre a bázisra vonatkozó mátrix alakban írhatók:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad a_{11}, a_{22} \in \mathbb{R}, \quad a_{12} = a_{21}^*.$$

Ami  $\mathbf{A}$  sajátértékeit illeti, a modell egyszerűségéből adódóan, csak két lehetőség létezik. A triviális esetben  $\mathbf{A}$ -nak kétszeres sajátértéke van, és az egységmátrixszal arányos. Amikor a sajátértékei különböznek,  $\mathbf{A}$  arra vonatkozó információt is tartalmaz, hogy melyik ortonormált bázisban diagonális, vagyis hogy melyik valószínűségi mezőben tekinthető valószínűségi változónak.

A sajátértékeket az utóbbtól elválasztva,  $\mathbf{A}$  úgy írható, hogy

$$\mathbf{A} = a_0 \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} + a \left( n_x \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} + n_z \begin{bmatrix} 1 & \\ & -1 \end{bmatrix} + n_y \begin{bmatrix} & -i \\ i & \end{bmatrix} \right),$$

ahol  $(n_x, n_y, n_z) \in \mathbb{R}^3$  egy egységvektor, amely az említett bázist azonosítja. A zárójelbeli lévő mátrixok az ún. *Pauli-mátrixok*, és jelölésük rendre  $X$ ,  $Z$  és  $Y$ . A továbbiakban a  $2 \times 2$ -es egységmátrixot  $I$  jelöli.

A Pauli-mátrixok különböző ortonormált bázisban diagonálisak, és sajátértékük  $\pm 1$ . Közülük egyedül  $Z$  nemtriviális valószínűségi változó a  $T$  teszthez tartozó valószínűségi mezőben. A  $Z$  által reprezentált mérés minden extra információt nélkülöző számértékekkel fejezi ki a rendszer két állapotának a különbségét: a rendszer egyik állapotában a mérés eredménye  $+1$ , a másikban  $-1$ .

Egy másik fontos modell az  $N$  darab qubitből álló rendszerek modellje. Ekkor a Hilbert-tér a  $\mathcal{H}_2$  terek  $N$ -szeres tenzorszorzata:

$$\mathcal{H} = \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2.$$

A továbbiakban a  $\mathcal{H}$ -n értelmezett önadjungált operátorok közül csak az  $I$  egységmátrix és a Pauli-mátrixok  $N$ -szeres tenzorszorzatai, az  *$N$ -qubit Pauli-operátorok* kapnak lényeges szerepet. Az általuk generált csoport az  *$N$ -qubit Pauli-csoport*:

$$G_P = \{ i^k A_1 \otimes \cdots \otimes A_N \mid k = 0, \dots, 3, A_i = I, X, Y, Z \}.$$

Az egységoperátort leszámítva a Pauli-operátorok sajátértékei  $\pm 1$ , és kommutálásukat illetően csak két lehetőség van: kommutálnak vagy antikommutálnak. A továbbiakban a Pauli-operátorok a „ $\otimes$ ” jel nélkül lesznek kiírva.

## 1.4. Bell–KS-konfigurációk

A dolgozat főszereplői, a Bell–KS-konfigurációk, egymással speciálisan kommutáló, illetve antikommutáló Pauli-operátorokból épülnek fel. A nem kontextuális rejtett-paraméter elméletek kérdése, mint geometriai probléma, egy Bell–KS-konfiguráció segítségével egy jóval könnyebben tárgyalható algebrai problémára redukálódik: lehetetlen a konfiguráció operátoraihoz valamelyik sajátértéküket, azaz  $\pm 1$ -et hozzárendelni az (1.3b) összefüggés értelemszerű teljesülése mellett.

A konfiguráció bizonyos, páronként kommutáló operátorainak a közös sajátvektorait bárhogy színezve, mindig lesz köztük két ortogonális zöld vektor. Ez a két vektor valamelyik operátornak a két különböző sajátértékéhez tartozó sajátvektorai, ami azzal ekvivalens, hogy az operátor által reprezentált mennyiségnek egyszerre két különböző értéke van. Egyetlen rejtett-paraméter elméletnek sem engedhető meg, hogy ilyesmit állítson.

$$\begin{array}{cccc}
 & 4 & 5 & 6 \\
 1 & XI-IX-XX & & \\
 & | & | & | \\
 2 & IY-YI-YY & & \\
 & | & | & | \\
 3 & XY-YX-ZZ & & 
 \end{array}$$

1.1. ábra. Mermin–Peres-négyzet

Egy konkrét Bell–KS-konfiguráció, az ún. *Mermin–Peres-négyzet* [15, 18], az 1.1. ábrán látható. A négyzet 9 darab 2-qubit Pauli-operátorból áll, és ezek 6 darab, páronként kommutáló operátorokat tartalmazó halmazba szerveződnek. Egy ilyen halmazon belül az operátorok szorzata az egységoperátor  $\pm 1$ -szerese, ami alapján egy halmaz *pozitív* vagy *negatív*. Az 1.1. ábrán az 1, ..., 5 jelzésű halmazok pozitívak, a 6-os halmaz pedig negatív.

A kiszínezés, mint geometriai probléma a Mermin–Peres-négyzet segítségével a következőképpen tárgyalható. Adott halmaz operátorai valamely ortonormált bázisban egyszerre diagonalizálhatók, és a bázisvektorok közül valamelyiknek zöldnek kell lennie. Ez tehát halmazonként egy zöld vektort jelent. Az 1, ..., 5 halmazok zöld vektorait jelölje  $|a\rangle$ , ...,  $|e\rangle$ , és az egyszerűség kedvéért mindegyikük legyen a neki megfelelő halmaz összes operátorának a  $+1$ -hez tartozó sajátvektora.

Mivel  $|a\rangle$ -ra és  $|b\rangle$ -re nem lehet ortogonális, a 6-os halmaz  $|f\rangle$  zöld vektora  $XX$ -nek és  $YY$ -nek csak a  $+1$ -hez tartozó sajátvektora lehet. Viszont ekkor

$$ZZ|c\rangle = |c\rangle \quad \text{és} \quad ZZ|f\rangle = -|f\rangle,$$

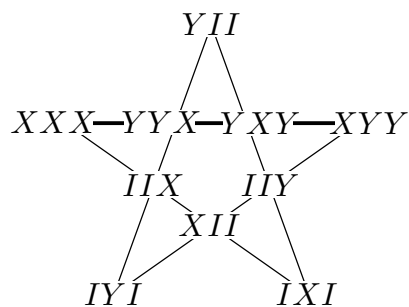
ezért  $|c\rangle$  és  $|f\rangle$  két ortogonális zöld vektor.

Az operátorok más sajátvektorainak a kiválasztásával is hasonló ellentmondásra lehet jutni. A Mermin–Peres-négyzet tehát 24, a kívánt módon nem kiszínezhető vektort rögzít.

Az algebrai érvelés szerint az operátorokhoz nem lehet hozzárendelni valamelyik sajátértéküket úgy, hogy (1.3b) értelemszerűen teljesüljön. Waegell és Aravind [27] az ehhez elégséges feltételeket a Mermin–Peres-négyzeten túlmutató általánossággal foglalta össze<sup>9</sup>:

1. mindegyik operátor páros számú halmaz eleme;
2. a negatív halmazok száma páratlan.

Az érvelés így hangzik. Egy halmazbeli operátorok értékeinek a szorzata  $+1$  vagy  $-1$  annak függvényében, hogy pozitív vagy negatív halmazról van szó. Az így kapott számokat minden halmazra összeszorozva, a 2. kritérium miatt  $-1$  adódik. Mivel egy operátor páros számú halmazban van, az értéke az előbbi szorzatban páros hatványon szerepel, így annak az eredménye  $+1$  kell, hogy legyen.



1.2. ábra. Mermin-pentagramma

Egy másik Bell–KS-konfiguráció az 1.2. ábrán látható *Mermin-pentagramma*. Mivel ennek csak a „vízszintes” halmaza negatív, a WA-kritériumok teljesülnek.

---

<sup>9</sup>Cikkükben néhány egészen egzotikus konfigurációt is mutatnak.

## 2. $GF(2)$ feletti szimplektikus vektorterek tulajdonságai

### 2.1. Pauli-csoport szimplektikus struktúrája

A Bell–KS-konfigurációk vizsgálatának első lépése az a felismerés, hogy az  $N$ -qubit Pauli-csoport egy  $GF(2)$  feletti szimplektikus vektortér struktúrájával rendelkezik. Pontosabban, létezik egy csoport-homomorfizmus  $G_N$  és  $GF(2)^{2N}$  között<sup>10</sup> úgy, hogy két operátor kommutálását, illetve antikommütálását egy, az utóbbin értelmezett alternáló bilineáris forma adja meg. Ez az irodalomban, a konzulensem nevével fémjelzett cikkekben is, számtalanszor megjelenik ( $N = 3$ -ra ld. pl. [12]).

A homomorfizmus alakja a következő: az  $i^k A_1 \otimes \cdots \otimes A_N \in G_N$  operátorhoz legyen hozzárendelve a  $GF(2)^{2N}$ -beli  $\mathbf{x} = x_1 \dots x_N x'_1 \dots x'_N$  vektor, ahol az  $A_i$  Pauli-mátrixot  $x_i x'_i$  azonosítja az alábbi szabály szerint:

$$I \leftrightarrow 00, \quad X \leftrightarrow 01, \quad Z \leftrightarrow 10, \quad Y \leftrightarrow 11.$$

Ekkor, ha két operátorhoz  $\mathbf{x}$ , illetve  $\mathbf{y}$  tartozik, a szorzatuk képe  $\mathbf{x} + \mathbf{y}$ , és az

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y'_1 + \cdots + x_N y'_N + x'_1 y_1 + \cdots + x'_N y_N \quad (2.1)$$

mennyiség 0, illetve 1 aszerint, hogy a két operátor kommutál vagy antikommütál.

A homomorfizmus magtere nem triviális, mivel a leképezés során az  $i^k$  tényezőre vonatkozó információ elveszlik, és a későbbiekben ez nem marad következmények nélkül.

Absztrakt szinten, egy  $F$  test feletti  $V$  vektortér *szimplektikus vektortér*, ha értelmezett rajta egy  $\langle \cdot, \cdot \rangle$  *szimplektikus formának* nevezett bilineáris forma, amely

1. *alternáló* vagy *totálisan izotróp*: minden  $\mathbf{x} \in V$ -re  $\langle \mathbf{x}, \mathbf{x} \rangle = 0$ ;
2. *nemdegenerált*: ha minden  $\mathbf{x} \in V$ -re  $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ , akkor  $\mathbf{y} = \mathbf{0}$ .

Az első axiómából következik, hogy

$$\begin{aligned} 0 &= \langle \mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle \\ &= \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{x} \rangle, \end{aligned}$$

tehát a szimplektikus forma ferdén szimmetrikus. A gondolatmenet szempontjából érdekes,  $GF(2)$  feletti vektorterek esetén ez szimmetriára egyszerűsödik, mivel  $GF(2)$ -ben  $-1 = 1$ .

Ismert tény, hogy minden szimplektikus vektortér dimenziószáma páros [14].

<sup>10</sup>Emlékeztető:  $GF(2)^{2N}$  a rajta értelmezett összeadással csoportot alkot.



## 2.2. Alterek, Gauss-együtthetők

Legyen  $V$  tetszőleges  $GF(2)$  feletti  $n$ -dimenziós vektortér.

**2.1. Lemma.** *A  $k$  darab lineárisan független vektorból álló halmazok száma*

$$\frac{1}{k!} 2^{1+\dots+(k-1)} (2^n - 1)(2^{n-1} - 1) \dots (2^{n-k+1} - 1). \quad (2.2)$$

*Bizonyítás.* A lineárisan független  $\mathbf{x}_1, \dots, \mathbf{x}_k$  vektorok egyenként választhatók ki. Első lépésként  $\mathbf{x}_1$  nem lehet a nullvektor. Feltéve, hogy az  $i$ -edik lépésben  $i - 1$  darab vektor már megvan, a lineáris függetlenség megőrzéséhez  $\mathbf{x}_i$  nem lehet benne az általuk kifeszített  $W_{i-1}$  altérben. Emiatt  $\mathbf{x}_i$

$$\nu_i = |V \setminus W_{i-1}| = 2^{i-1}(2^{n-i+1} - 1)$$

darab vektor közül választható. A vektorok sorrendje irreleváns, ezért a keresett szám  $\nu_1 \nu_2 \dots \nu_k / k!$ .  $\square$

$V$  bázisainak a száma a (2.2) formulából  $k := n$  helyettesítéssel adódik:

$$\frac{1}{n!} 2^{1+\dots+(n-1)} (2^n - 1)(2^{n-1} - 1) \dots (2^1 - 1). \quad (2.3)$$

A  $k$ -dimenziós  $V$ -alterek halmaza a  $\text{Gr}(n, k)$  *Grassmann-sokaság*, számukat a  $\begin{bmatrix} n \\ k \end{bmatrix}$  *Gauss-együtthetők* adják meg.

**2.2. Lemma.**

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{2^n - 1}{2^k - 1} \cdot \frac{2^{n-1} - 1}{2^{k-1} - 1} \dots \frac{2^{n-k+1} - 1}{2^1 - 1}. \quad (2.4)$$

*Bizonyítás.* A  $k$  darab lineárisan független vektorból álló halmazok (2.2) számát osztani kell egy ilyen halmaz által kifeszített altér bázisainak a (2.3) számával, és ebből  $\begin{bmatrix} n \\ k \end{bmatrix}$  adódik.  $\square$

A Gauss-együtthetőkre igazak az alábbi összefüggések:

$$\begin{bmatrix} n \\ n-k \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix}, \quad \begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1, \quad \begin{bmatrix} n+1 \\ k \end{bmatrix} = 2^k \begin{bmatrix} n \\ k \end{bmatrix} + \begin{bmatrix} n \\ k-1 \end{bmatrix}. \quad (2.5)$$

Legyen  $W \leq V$  egy altér. A  $V/W$  faktortérnek egy  $k$ -dimenziós altere olyan ekvivalenciaosztályokból áll, amelyek uniója  $V$ -nek egy  $k + \dim W$ -dimenziós,  $W$ -t tartalmazó altere. Így a  $W$ -t tartalmazó  $m > \dim W$ -dimenziós alterek száma

$$\begin{bmatrix} n - \dim W \\ m - \dim W \end{bmatrix}. \quad (2.6)$$

### 2.3. Izotróp és Lagrange-alterek

A továbbiakban  $V_N$  egy  $GF(2)$  feletti  $2N$ -dimenziós szimplektikus vektorteret jelöl. Egy  $W \leq V_N$  altér *ortogonális kiegészítője* az összes  $W$ -beli vektorra ortogonális vektorok  $W^\perp$  altere. Mivel a szimplektikus forma nem degenerált,

$$\dim W + \dim W^\perp = \dim V_N = 2N.$$

$W$  *izotróp*, ha  $W \leq W^\perp$ , azaz ha tetszőleges két vektora ortogonális.  $W$  *Lagrange-altér*, ha  $W^\perp = W$ . Következik, hogy minden Lagrange-altér  $N$ -dimenziós.  $V_N$  Lagrange-altereinek a  $\text{Lag } V_N$  halmaza a *Lagrange-Grassmann-sokaság*.

**2.3. Lemma.** *A  $k$  darab páronként ortogonális, lineárisan független vektorból álló halmazok száma:*

$$\frac{1}{k!} 2^{1+\dots+(k-1)} (2^{2N} - 1)(2^{2(N-1)} - 1) \dots (2^{2(N-k+1)} - 1). \quad (2.7)$$

*Bizonyítás.* A gondolatmenet (2.2) bizonyításához hasonló.  $\mathbf{x}_i$  most sem lehet a már kiválasztott  $\mathbf{x}_1, \dots, \mathbf{x}_{i-1}$  vektorok által kifeszített izotróp  $W_{i-1}$  altérben, de emellett a páronkénti ortogonalitásnak is meg kell maradnia. Ehhez az eddigi vektorokra  $\mathbf{x}_i$ -nek ortogonálisnak kell lennie, tehát  $\mathbf{x}_i \in W_{i-1}^\perp$ . Következik, hogy  $\mathbf{x}_i \in W_{i-1}^\perp \setminus W_{i-1}$ . Mivel  $W_{i-1}$  izotróp, a szóba jövő vektorok száma

$$\begin{aligned} v'_i &= |W_{i-1}^\perp \setminus W_{i-1}| = |W_{i-1}^\perp| - |W_{i-1}| \\ &= 2^{2N-(i-1)} - 2^{i-1} \\ &= 2^{i-1}(2^{2(N-i+1)-1} - 1). \quad \square \end{aligned}$$

$V_N$   $k$ -dimenziós izotróp altereinek a száma (2.7) és (2.3) hányadosa:

$$\left[ \begin{matrix} N \\ k \end{matrix} \right]_{\perp} \equiv \frac{2^{2N} - 1}{2^k - 1} \cdot \frac{2^{2(N-1)} - 1}{2^{k-1} - 1} \dots \frac{2^{2(N-k+1)} - 1}{2^1 - 1}. \quad (2.8)$$

Ebből,  $k := N$  helyettesítéssel,  $V_N$  Lagrange-altereinek a száma:

$$L(N) \equiv |\text{Lag } V_N| = (2^N + 1)(2^{N-1} + 1) \dots (2 + 1). \quad (2.9)$$

Egy  $W \leq V_N$  izotróp altér  $W^\perp/W$  *szimplektikus faktortere* egy  $2(N - \dim W)$ -dimenziós szimplektikus vektortér az alábbi szimplektikus formával:

$$\langle \mathbf{x} + W, \mathbf{y} + W \rangle_W = \langle \mathbf{x}, \mathbf{y} \rangle.$$

$W^\perp/W$  minden Lagrange-altere olyan ekvivalenciaosztályokból áll, amelyek uniója  $V_N$ -nek egy  $W$ -t tartalmazó Lagrange-altere adódik. Emellett, ha  $U$  egy Lagrange-altér  $V_N$ -ben,  $U/W$  Lagrange-altér  $W^\perp/W$ -ben. Következik, hogy a  $W$ -t tartalmazó Lagrange-alterek száma  $L(N - \dim W) = |\text{Lag } V_{N-\dim W}|$ .

**2.4. Lemma.**

$$\begin{bmatrix} N \\ k \end{bmatrix}_\perp = \frac{L(N)}{L(N-k)} \begin{bmatrix} N \\ k \end{bmatrix}.$$

*Bizonyítás.* Az összefüggés számolással is belátható, viszont egy szemléletesebb bizonyítás a következő. Minden  $k$ -dimenziós izotróp  $W$  altér benne van egy  $U$  Lagrange-altérben. Ez utóbbi  $L(N)$ -féleképpen választható, és a  $k$ -dimenziós altéreknek a száma  $\begin{bmatrix} N \\ k \end{bmatrix}$ .  $W$ -t összesen  $L(N-k)$  darab Lagrange-altér tartalmazza, ezért osztani kell ezzel a számmal.  $\square$

**2.5. Lemma.**

$$L(N) = \sum_{k=0}^N \begin{bmatrix} N \\ k \end{bmatrix} 2^{1+\dots+k}. \quad (2.10)$$

*Bizonyítás.* Indukcióval. Az állítás  $N = 1$ -re igaz:  $L(1) = 3$ . Az  $L(N)$ -re írható rekurziós összefüggés szerint

$$L(N) = (2^N + 1)L(N-1) = (2^N + 1) \sum_{k=0}^{N-1} \begin{bmatrix} N-1 \\ k \end{bmatrix} 2^{1+\dots+k}.$$

A jobb oldal algebrai átalakításokkal és a (2.5) azonosságok felhasználásával, kicsit hosszadalmasan, de a kívánt alakra hozható.  $\square$

**2.6. Lemma.** *Az  $U$  Lagrange-altérrel diszjunkt Lagrange-altérek száma*

$$I(N) \equiv 2^{1+\dots+N}.$$

$U$ -t egy  $W \leq U$  izotróp altérben metsző Lagrange-altérek száma  $I(N - \dim W)$ .

*Bizonyítás.* A második állításhoz, a konkrét ismerete nélkül, alkalmazni kell  $I$ -t a  $W^\perp/W$  szimplektikus faktortérre. Felhasználva a kapott kifejezést, és hogy minden Lagrange-altér  $U$ -t valamilyen  $W$  izotróp altérben metszi,

$$L(N) = \sum_{W \leq U} I(N - \dim W) = \sum_{k=0}^N \begin{bmatrix} N \\ k \end{bmatrix} I(N-k) = \sum_{k=0}^N \begin{bmatrix} N \\ k \end{bmatrix} I(k).$$

Egy  $k := N-k$  változócsere után az utolsó egyenlőség az  $\begin{bmatrix} N \\ k \end{bmatrix} = \begin{bmatrix} N \\ N-k \end{bmatrix}$  összefüggésből következik. A jobb oldalt a (2.10) formulával összehasonlítva,

$$0 = \sum_{k=0}^{N-1} \begin{bmatrix} N \\ k \end{bmatrix} [2^{1+\dots+k} - I(k)] + 2^{1+\dots+N} - I(N).$$

$V_1$  Lagrange-altéreknek a száma 3, és ezek csak a triviális altérben metszik egymást, ezért  $I(1) = 2^1$ . Indukciós feltevésésként, legyen  $I(k) = 2^{1+\dots+k}$  minden  $k < N$ -re. Ekkor a jobb oldalon a szumma eltűnik, és adódik az állítás.  $\square$

## 2.4. Szimplektikus bázis, szimplektikus transzformáció

**2.7. Lemma.** *Ha egy  $B \subseteq V_N$  vektorhalmazban minden vektor pontosan egy másik  $B$ -beli vektorra nem ortogonális,  $B$  elemei lineárisan függetlenek.*

*Bizonyítás.* Legyen  $\mathbf{x}$  a  $B$ -beli vektorok nemtriviális lineáris kombinációja úgy, hogy egyetlen  $B$ -beli vektorral sem egyenlő. Ha a lineáris kombinációban  $\mathbf{y}$  együtt-hatója nemnulla, egy olyan vektor, amely elvileg csak  $\mathbf{y}$ -ra nem ortogonális,  $\mathbf{x}$ -re sem lesz ortogonális. Ez már két vektor, tehát a feltétel nem teljesül.  $\square$

A fenti tulajdonsággal rendelkező vektorhalmazok szükségszerűen páros sok vektort tartalmaznak, és ezek nemortogonális párokba szerveződnek. Ha egy ilyen  $B$  vektorhalmaz kifeszíti  $V_N$ -t, akkor  $B$  *szimplektikus bázis*.

Nem ront az általánosságon, ha a  $B$  szimplektikus bázis elemeit  $\mathbf{a}_1, \dots, \mathbf{a}_N, \mathbf{b}_1, \dots, \mathbf{b}_N$  jelöli, ahol

$$\langle \mathbf{a}_i, \mathbf{a}_k \rangle = \langle \mathbf{b}_i, \mathbf{b}_k \rangle = 0, \quad \text{és} \quad \langle \mathbf{a}_i, \mathbf{b}_k \rangle = \delta_{ik}, \quad i, k = 1, \dots, N. \quad (2.11)$$

$B$ -nek a  $B_a = \{\mathbf{a}_1, \dots, \mathbf{a}_N\}$ , illetve  $B_b = \{\mathbf{b}_1, \dots, \mathbf{b}_N\}$  *partíciói* egy-egy Lagrange-alteret feszítenek ki, és ezeket jelölje  $U_a$ , illetve  $U_b$ . A két Lagrange-altér *diszjunkt*. Egy szimplektikus bázis  $2^{N-1}$ -féleképpen osztható fel  $B_a$  és  $B_b$  partíciókra úgy, hogy (2.11) teljesüljön.

**2.8. Lemma.** *Legyen  $U_a$  és  $U_b$  két diszjunkt Lagrange-altér. Ha  $U_a$  bázisa  $B_a$ ,  $U_b$ -nek egyértelműen létezik  $B_b$  bázisa úgy, hogy  $B_a \cup B_b$  szimplektikus bázis.*

*Bizonyítás.* Legyen  $B_a = \{\mathbf{a}_1, \dots, \mathbf{a}_N\}$ , és legyen  $B'_b = \{\mathbf{b}'_1, \dots, \mathbf{b}'_N\}$   $U_b$ -nek egy bázisa. Ha  $B'_b$  és a keresett  $B_b \subseteq U_b$  bázis közti transzformáció mátrixa  $\mathbf{B} = [B_{kj}]$ ,

$$\delta_{ik} = \langle \mathbf{a}_i, \mathbf{b}_k \rangle = \sum_{j=1}^N B_{kj} \langle \mathbf{a}_i, \mathbf{b}'_j \rangle, \quad \text{amiből} \quad \mathbf{B} = \mathbf{A}^{-1}, \quad \text{ahol} \quad A_{ij} = \langle \mathbf{a}_i, \mathbf{b}'_j \rangle.$$

Az egyértelműséghez felhasználható, hogy  $U_b$ -nek minden  $B_b$ -től különböző bázisában van olyan  $\mathbf{b}$  bázisvektor, amely két vagy több  $B_b$ -beli vektor összege, és amely így két vagy több  $B_a$ -beli vektorra nem ortogonális.  $\square$

**2.9. Lemma.**  *$V_N$  szimplektikus bázisainak a száma*

$$\frac{1}{4^N N!} 4^{1+\dots+N} (4^N - 1) \cdots (4^1 - 1). \quad (2.12)$$

*Bizonyítás.* Az előző lemma értelmében egy  $B$  szimplektikus bázis megválasztása  $U_a, U_b$  és  $B_a$  megválasztásával ekvivalens.  $U_a$   $L(N)$ -féleképpen,  $U_b$   $I(N)$ -féleképpen választható, a  $B_a \subseteq U_a$  bázisok számát pedig a (2.3) formula adja meg. Mivel  $U_a$  és  $U_b$  között nincs különbség, osztani kell 2-vel. A műveletek elvégzése és kisebb átrendezések után a kifejezés adódik.  $\square$

Az  $\hat{A} : V_N \rightarrow V_N$  lineáris transzformáció *szimplektikus transzformáció*, ha őrzi a szimplektikus formát, vagyis minden  $\mathbf{x}, \mathbf{y} \in V_N$ -re

$$\langle \hat{A}\mathbf{x}, \hat{A}\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle.$$

Ha  $V_N$ -ben rögzített egy szimplektikus bázis, a szimplektikus transzformációk mátrixa ún. *szimplektikus mátrix*. Ezek a mátrixok csoportot alkotnak, amelynek neve: *szimplektikus csoport*, és jelölése, általánosan,  $GF(q)$  feletti  $2N$ -dimenziós vektortér esetén:  $\text{Sp}(2N, q)$ .

Egy szimplektikus mátrix oszlopvektorai szimplektikus bázist alkotnak. Az anti-kommutáló párok permutációit és a párokon belüli cseréket összeszámolva, minden szimplektikus bázisból  $2^N N!$  darab szimplektikus mátrix hozható létre. (2.12) miatt

$$|\text{Sp}(2N, 2)| = \frac{1}{2^N} 4^{1+\dots+N} (4^N - 1) \dots (4^1 - 1). \quad (2.13)$$

Ismert, hogy a szimplektikus csoportot speciális szimplektikus transzformációk, ún. *transzvekciónak* generálják [7]. Az  $\mathbf{x}$  vektorhoz tartozó transzvekciónak

$$\hat{T}_{\mathbf{x}}(\mathbf{y}) = \mathbf{y} + \langle \mathbf{x}, \mathbf{y} \rangle \mathbf{y}.$$

A transzvekciónak kielégítik az alábbi, *Coxeter-relációknak* nevezett összefüggéseket:

$$\hat{T}_{\mathbf{x}}^2 = \hat{I} \quad \text{és} \quad \hat{T}_{\mathbf{x}}\hat{T}_{\mathbf{y}} = \begin{cases} \hat{T}_{\mathbf{y}}\hat{T}_{\mathbf{x}}, & \text{ha } \langle \mathbf{x}, \mathbf{y} \rangle = 0 \\ \hat{T}_{\mathbf{x}+\mathbf{y}}\hat{T}_{\mathbf{x}}, & \text{ha } \langle \mathbf{x}, \mathbf{y} \rangle = 1 \end{cases} \quad (2.14)$$

### 3. A véges geometria elemei

A szimplektikus vektorterek a Bell–KS-konfigurációkat csak az egyik oldalról képesek megvilágítani. A konfigurációk lényeges jellemzője, hogy az egyes, páronként kommutáló operátorokból álló halmazok hogyan metszik egymást, és ezt az információt a konfiguráció *geometriája* tartalmazza. Ennek a megragadásában a véges geometria módszerei segítenek.

A pont-egyenes geometriák kulcsfontosságú fogalmához, illetve azok előnyös tulajdonságokkal rendelkező speciális eseteihez a gráfokon és az illeszkedési rendszereken keresztül célszerű eljutni. Ez az összefoglaló is ezt a programot követi. Ahol nincs explicit módon forrás megjelölve, az összefoglaló többnyire a [8, 6, 19] művekből való szemezgetés eredménye.

#### 3.1. Gráfelméleti alapfogalmak

Egy  $G$  gráf, szemléletesen, *pontoknak* vagy *csúcsoknak* nevezett absztrakt objektumok gyűjteménye, amelyen belül bizonyos pontpárokat *élek* kötnek össze.  $G$  pont-halmazát  $V(G)$ , élhalmazát  $E(G)$  jelöli. Egy másik szokásos jelölés:  $G = (V, E)$ , ahol  $V$  a pontok halmaza és  $E$  az élek halmaza. „ $x \in G$ ” jelentése  $x \in V(G)$  vagy  $x \in E(G)$  aszerint, hogy a szöveggörnyezetben  $x$  pontot vagy élt jelöl.

A továbbiakban feltételezett, hogy  $G$  hurokmentes irányítatlan gráf, és az élei legfeljebb egyszeresek, azaz  $E(G)$  ekvivalens egy  $V(G)$ -n értelmezett szimmetrikus, irreflexív relációval.

A jelöléseket megkönnyíti, ha  $G$  élei  $V(G)$  kételemű részhalmazaként vannak kezelve. Egy  $v$  pont és egy  $e$  él *illeszkednek*, ha  $v \in e$ . Az  $e$ -vel illeszkedő pontok *végpontjai*. Az  $e = \{u, v\}$  élt a továbbiakban  $uv$  jelöli (természetesen  $uv = vu$ ).

Az  $u$  és  $v$  pontok *szomszédosak*, ha  $uv \in G$ ,  $v$  szomszédainak a halmaza  $v^*$ , és  $v$  *fokszáma* a szomszédainak a száma:  $\deg(v) = |v^*|$ . A  $G$  gráf  *$k$ -reguláris*, ha minden pontjának a fokszáma  $k$ , és *teljes*, ha pontjai páronként szomszédosak. Az  $n$  pontú teljes gráf jelölése:  $K_n$ . A  $G$  gráf  $\overline{G}$  *komplementer gráfjának* a ponthalmaza megegyezik  $V(G)$ -vel, és  $uv \in \overline{G}$  akkor és csak akkor, ha  $uv \notin G$ .

Az  $U \subseteq V(G)$  ponthalmaz *független*, ha  $G$  egyetlen élének sem tartalmazza mindkét végpontját. A  $G$  gráf  *$k$ -részes*, ha  $V(G)$ -nek létezik  $k$  elemű felosztása úgy, hogy minden partíció független, és nincs ugyanilyen  $k-1$  elemű felosztás. Ha a partíciók száma nem lényeges,  $G$  *többrészes*; ha speciálisan  $k = 2$ ,  $G$  *kétrészes*.

A  $\{v_0, \dots, v_k\}$  ponthalmazú,  $\{v_0v_1, \dots, v_{k-1}v_k\}$  élhalmazú  $P_k$  gráf egy  $v_0$  és  $v_k$  közti  *$k$ -hosszú út* ( $k$  az út *hossza*),  $v_0$  és  $v_k$  az út *végpontjai*, a többi  $v_i$  pedig *belső pont*.

Ha  $k \geq 3$ , egy  $k$ -hosszú út, amelynek a két végpontja megegyezik,  $k$ -hosszú kör. A  $k$ -hosszú utak, illetve körök kompakt jelölése:

$$P_k = (v_0, v_1, \dots, v_k), \quad \text{illetve} \quad C_k = (v_0, \dots, v_k = v_0).$$

A  $G'$  gráf *részgráfja*  $G$ -nek (jelölés:  $G' \leq G$ ), ha  $V(G') \subseteq V(G)$  és  $E(G') \subseteq E(G)$ .  $G'$  *feszített részgráf*, ha élhalmaza a  $G' \leq G$  feltétel teljesülése mellett maximális, azaz ha  $E(G')$  pontosan azoknak az  $uv \in G$  éleknek a halmaza, amelyekre teljesül, hogy  $u, v \in G'$ . Az  $U \subseteq V(G)$  *ponthalmaz által kifeszített részgráf* az egyetlen  $G' \leq G$  feszített részgráf, amelyre  $V(G') = U$ .

Az  $u, v \in G$  pontok  $d(u, v)$  *távolsága*<sup>11</sup> a legrövidebb  $u$  és  $v$  közti  $P \leq G$  út hossza, vagy  $d(u, v) = \infty$ , ha ilyen nem létezik.  $G$  *derékbősége* (vagy „*girth* paramétere”) a legrövidebb  $C \leq G$  kör hossza, és *átmérője* a két legtávolabbi pontjának a távolsága:  $D(G) = \max_{u, v \in G} d(u, v)$ .  $G$  *összefüggő*, ha bármely két pontja között létezik út, azaz ha  $D(G) \leq \infty$ .

Egy  $k$ -reguláris,  $g$  derékbőségű gráf, amelynek ezekkel a megkötésekkel minimális számú pontja van,  $(k, g)$ -*cage*. A  $(3, 5)$ -cage a jól ismert *Petersen-gráf* (3.1. ábra), a  $(3, 6)$ -cage pedig a *Heawood-gráf* (3.2. ábra).

Legyen  $\varphi : V(G) \rightarrow V(G')$  a  $G$  és  $G'$  gráfok pontthalmazai közti leképezés (alternatív jelölés:  $\varphi : G \rightarrow G'$ ). A halmazok szokásos elemenkénti leképezésével  $\varphi$  az  $E(G)$ -beli éleket (kételemű halmazokat)  $V(G')$  egy- vagy kételemű részthalmazaira képezi. Az érdekes leképezés-osztályok a következők:

- *homomorfizmus*: minden  $e \in G$  élre  $\varphi(e) \in G'$ ; ez kizárja, hogy  $\varphi(e)$  egyelemű halmaz legyen, tehát minden  $v' \in G'$  pont  $\varphi$  szerinti ősképe független pontthalmaz  $G$ -ben.
- *izomorfizmus*: bijektív homomorfizmus, amelynek a  $\varphi^{-1}$  inverze is homomorfizmus;
- *automorfizmus*: izomorfizmus, amikor  $G = G'$ ;

A  $G$  és  $G'$  közti homomorfizmusok halmaza  $\text{Hom}(G, G')$ , és  $G$  automorfizmusainak a halmaza  $\text{Aut}(G)$ . Az utóbbi a függvénykompozícióval csoportot alkot. A  $G$  és  $G'$  gráfok *izomorfak* (jelölés:  $G \cong G'$ ), ha létezik köztük izomorfizmus.

<sup>11</sup> $d(u, v)$  teljesíti a távolság axiómáit: (1)  $d(u, v) = 0$  akkor és csak akkor, ha  $u = v$ ; (2) *szimmetria*:  $d(u, v) = d(v, u)$ ; (3) *háromszög-egyenlőtlenség*:  $d(u, w) \leq d(u, v) + d(v, w)$ .

## 3.2. Illeszkedési rendszer és geometria

Egy  $\Gamma$  illeszkedési rendszer *elemek* gyűjteménye, amelyen belül bizonyos, különböző *típusú* elemek *illeszkednek* egymásra. Formálisan a  $\Gamma = (X, \sim, \tau)$  hármas egy  $I$  *típushalmaz feletti illeszkedési rendszer*, ahol  $X$  az *elemhalmaz*,  $\sim$  egy  $X$ -en értelmezett bináris reláció, az ún. *illeszkedési reláció*, és  $\tau : X \rightarrow I$  a *típusfüggvény*.  $x \in \Gamma$  szinonímája annak, hogy  $x \in X$ ,  $x \sim y$  az  $x$  és  $y$  elemek illeszkedését jelenti, és  $\tau(x)$  az  $x \in X$  elem *típusa*. Ha  $i \in I$ , az  *$i$ -elemek* halmaza  $\tau^{-1}(i)$ .

Az  $U \subseteq X$  elemhalmaz *típusa*  $\tau(U) \subseteq I$ ,  $U$  *rangja* a típusának a számossága, és  $\Gamma$  *rangja* az  $X$  elemhalmaz rangja. Ha a vizsgált szituáció az ellenkezőjét nem igényeli, a  $\tau$  típusfüggvény mindig szürjektív, azaz  $\tau(X) = I$ , mivel többnyire értelmetlen  $X$ -beli elemek által nem képviselt típusokat figyelembe venni.

A  $\Gamma$  illeszkedési rendszerre a következő axiómák teljesülnek:

1.  $\sim$  reflexív és szimmetrikus;
2. minden  $x, y \in \Gamma$ -ra, ha  $\tau(x) = \tau(y)$  és  $x \neq y$ , akkor  $x \approx y$ .

A  $\Gamma$  illeszkedési rendszer  $G(\Gamma)$  *illeszkedési gráfjának* a ponthalmaza  $X$ , és  $xy \in G(\Gamma)$  akkor és csak akkor, ha  $x \sim y$  (ennek csak  $x \neq y$  esetén van értelme). A 2. axióma értelmében  $G(\Gamma)$  egy többrésű gráf, amelyben bármely  $i \in I$ -re az  $i$ -elemek halmaza független.  $\Gamma$  két elemének a *távolsága* a  $G(\Gamma)$ -ban értelmezett távolság, és  $\Gamma$  *összefüggő*, ha  $G(\Gamma)$  összefüggő.

Legyen egy  $I$  feletti  $\Gamma = (X, \sim, \tau)$  és egy  $I'$  feletti  $\Gamma' = (X', \sim', \tau')$  illeszkedési rendszer.  $\Gamma'$  *részrendszere*  $\Gamma$ -nak (vagy  $\Gamma$  *tartalmazza*  $\Gamma'$ -t; jelölés:  $\Gamma' \leq \Gamma$ ), ha  $X' \subseteq X$ , és  $\sim'$  a  $\sim$  reláció,  $\tau'$  pedig a  $\tau$  függvény  $X'$ -re vett megszorítása. Ugyanezt az illeszkedési gráfok szemszögéből nézve,  $G(\Gamma') \leq G(\Gamma)$  az  $X'$  által kifizített részgráf.  $\Gamma'$ -t az  $X'$  halmaz által  $\Gamma$ -ban *indukált* illeszkedési rendszernek is hívják.

Legyen  $\varphi : X \rightarrow X'$  a két elemhalmaz közti leképezés (alternatív jelölés:  $\varphi : \Gamma \rightarrow \Gamma'$ ). Az alábbi leképezés-osztályokat érdemes definiálni:

- *gyenge homomorfizmus*: ha  $x, y \in X$  illeszkednek,  $\varphi(x), \varphi(y) \in X'$  is illeszkednek, emellett  $\tau'(\varphi x) = \tau'(\varphi y)$  akkor és csak akkor, ha  $\tau(x) = \tau(y)$ ;
- *korreláció*: bijektív gyenge homomorfizmus, amelynek a  $\varphi^{-1}$  inverze is gyenge homomorfizmus; egy  $\Gamma \rightarrow \Gamma'$  korreláció létezéséből következik, hogy a  $G(\Gamma)$  és  $G(\Gamma')$  illeszkedési gráfok izomorfak.
- *autokorreláció*: korreláció, amikor  $\Gamma = \Gamma'$ ;
- *homomorfizmus*: gyenge homomorfizmus,  $I = I'$  és  $\tau'(\varphi x) = \tau(x), \forall x \in X$ ;



- *izomorfizmus*, bijektív homomorfizmus, amelynek a  $\varphi^{-1}$  inverze is homomorfizmus; összehasonlítva a korrelációval, egy  $x \in X$  elem és  $x$  izomorfizmus szerinti képének a típusa megegyezik.
- *automorfizmus*: izomorfizmus, amikor  $\Gamma = \Gamma'$ ;
- *beágyazás*: injektív homomorfizmus.

A gráfokhoz hasonlóan a  $\Gamma$  és  $\Gamma'$  illeszkedési rendszerek közti homomorfizmusok halmaza  $\text{Hom}(\Gamma, \Gamma')$ , és  $\Gamma$  automorfizmusainak az  $\text{Aut}(\Gamma)$  halmaza csoportot alkot. A gráfokhoz képest most egy újabb csoport,  $\Gamma$  autokorrelációinak a  $\text{Cor}(\Gamma)$  csoportja is megjelenik, amelynek  $\text{Aut}(\Gamma)$  normális részcsoportja.  $\Gamma$  és  $\Gamma'$  *izomorfak* (jelölés:  $\Gamma \cong \Gamma'$ ), ha létezik köztük izomorfizmus.

$\Gamma$  *beágyazható*  $\Gamma'$ -be, ha létezik  $\Gamma \rightarrow \Gamma'$  beágyazás, és ekkor  $\Gamma$  a *beágyazott* illeszkedési rendszer. A beágyazás megengedi, hogy nem illeszkedő elemek képe illeszkedjen, ezért  $\Gamma$  beágyazhatóságából nem következik, hogy  $\Gamma'$ -nek van  $\Gamma$ -val izomorf részrendszere. Ha az utóbbi feltétel fennáll, kényelmesebb a  $\Gamma'$  által tartalmazott  $\Gamma$  rendszerről, vagy még rövidebben, „ $\Gamma'$ -nek a  $\Gamma$ -járól” beszélni annak ellenére, hogy szigorú értelemben  $\Gamma$  nem részrendszere  $\Gamma'$ -nek. Nem kizárt, hogy ilyen értelemben  $\Gamma'$ -nek „több  $\Gamma$ -ja is van”.

A  $\varphi$  autokorreláció és a  $\tau$  típusfüggvény egy  $\alpha(\varphi) : I \rightarrow I$  bijekciót határoz meg, és az  $\alpha : \text{Cor}(\Gamma) \rightarrow S_I$  leképezés magterét  $\Gamma$  automorfizmusai alkotják.  $\varphi$  egy *polaritás*, ha  $\varphi$  és  $\alpha(\varphi)$  rendje<sup>12</sup> 2, illetve *trialitás*, ha a két bijekció rendje 3.

Az  $f \subseteq X$  halmaz *zászló*, ha páronként illeszkedő elemeket tartalmaz. Az  $f$  zászló *kamra*, ha  $\tau(f) = I$ , és valamely  $i \in I$ -re  *$i$ -panel*, ha  $\tau(f) = I \setminus \{i\}$ . A 2. axióma miatt a zászlók elemei különböző típusúak, és a kamrákban minden lehetséges típusú elemből pontosan egy van. Az  $I$  feletti  $\Gamma$  illeszkedési rendszer  $I$  feletti *geometria*, ha minden maximális zászlója kamra.

A geometriák fontos tulajdonsága, hogy az  $I$ -től különböző zászlókat hány kamra tartalmazza. Ha ez a szám legalább 2, a geometria *rögzített*, ha legalább 3, a geometria *sűrű*. Ha minden panelt pontosan 2 kamra tartalmaz, a geometria *vékony*<sup>13</sup>. A  $\Gamma$  geometria *véges*, ha  $X$  véges halmaz.

### 3.3. Pont-egyenes geometria, általánosított $n$ -szög

Ha a típusalmaznak nincs túl sok eleme, az illeszkedési rendszer vagy geometria megadásában a különböző típusú elemek halmaza explicit módon jelölhető, és ekkor

<sup>12</sup>Emlékeztető: egy  $a$  csoportelem *rendje* a legkisebb  $k$  szám, amelyre  $a^k = e$ .

<sup>13</sup>Az angol nyelvű terminológia rendre *firm*, *thick* és *thin* (ld. pl. [6], 1. fejezet).

a típusfüggvény magától értetődővé válik. Például az  $I = \{1, \dots, n\}$  feletti  $n$  rangú  $\Gamma = (X_1, \dots, X_n, \sim)$  illeszkedési rendszer  $X_i$ -beli elemeinek a típusa  $i$ . Ilyenkor az  $x \in \Gamma$  kifejezés pontos jelentése, azaz hogy  $x$  melyik  $X_i$  halmazba tartozik, a szövegkörnyezetre van bízva.

A geometriák speciális esete a  $\Gamma = (P, L, \sim)$  *pont-egyenes geometria*, ahol  $P$  a *pontok*,  $L$  pedig az *egyenesek* halmaza.  $\Gamma$  zászlói egy pontot és egy vele illeszkedő egyenest tartalmaznak, ezért triviálisan kamrák. Két nem illeszkedő elem halmaza egy *anti-zászló*. Ha az ellenkezője nincs jelezve, a továbbiakban geometria alatt pont-egyenes geometriát kell érteni. Esetenként hasznos egy gráfot is geometriaként tekinteni.

Annak a megfogalmazása, hogy a  $\Gamma$  geometria rögzített (sűrű), így egyszerűsödik: minden egyenessel legalább két (három) pontnak, és minden ponttal legalább két (három) egyenesnek kell illeszkednie.  $\Gamma$  vékony, ha minden egyenessel pontosan két pont, és minden ponttal pontosan két egyenes illeszkedik.

$\Gamma = (P, L, \sim)$  *duálisa*  $\Gamma^* = (L, P, \sim^{-1})$ , vagyis  $\Gamma^*$  ponthalmaza  $L$ , egyeneshalmaza  $P$ , és illeszkedési relációja  $\Gamma$  illeszkedési relációjának az inverze. A duálisképzés általában *nem* polaritás (pl. amikor  $|P| \neq |L|$ ), emellett meglévő zászlókat nem ront el, és újabb zászlókat sem teremt. Mivel a duálisképzés lényegében az elemek típusainak a felcserélése,  $\text{Aut}(\Gamma^*) \cong \text{Aut}(\Gamma)$ .  $\Gamma$  *önduális*, ha  $\Gamma \cong \Gamma^*$ .

$\Gamma$  *reguláris, típusa*  $(|P|_t |L|_s)$ , és *rendje*  $(s-1, t-1)$ , ha minden egyenessel  $s$  darab pont, és minden ponttal  $t$  darab egyenes illeszkedik. Az  $(n_t n_t)$  típus, illetve az  $(s, s)$  rend szokásos rövidítése:  $(n_t)$ , illetve  $s$ . Ha  $\Gamma$  rendje  $s = 1, 2, 3, \dots$ , akkor  $\Gamma$  *elsőrendű, másodrendű, harmadrendű* stb. geometria. Ha  $\Gamma$  típusa  $(|P|_t |L|_s)$ ,  $\Gamma^*$  típusa  $(|L|_s |P|_t)$ . Egy  $k$ -reguláris  $G = (V, E)$  gráf típusa  $(|V|_k |E|_2)$ .

A  $p, p' \in \Gamma$  pontok *kollineárisak*, ha egy közös egyenessel illeszkednek; ha az egyenes egyértelmű,  $pp'$ -vel jelölhető. A különböző  $l, l' \in \Gamma$  egyenesek a mindkettőjükre illeszkedő pontokban *metszik egymást*, ha ilyen létezik, egyébként *párhuzamosak*. Definíciószerűen egy egyenes párhuzamos önmagával. Az egyértelmű közös pont  $ll'$ -vel jelölhető. A duális geometriában az egymást metsző egyeneseknek kollineáris pontok felelnek meg.

A pontok halmazán a kollinearitás egy szimmetrikus bináris reláció, ezért van értelme a  $\Gamma$  geometria *kollinearitási gráfjáról* beszélni. A  $p \in \Gamma$  ponttal kollineáris pontok halmaza  $p$  *perp-halmaza* (jelölés:  $p^\perp$ ). Az  $A \subseteq P$  ponthalmaz *perp-halmaza* azokat a pontokat tartalmazza, amelyek minden  $A$ -beli ponttal kollineárisak:  $A^\perp = \bigcap_{p \in A} p^\perp$ . Egy egyenes perp-halmaza az öt metsző egyenesek halmaza.

Ha  $\Gamma$ -nak nincs két egyenese, amelyre ugyanazok a pontok illeszkednek,  $\Gamma$  minden egyenese a vele illeszkedő pontok halmazaként tekinthető. Ez a szemlélet előnyös, mert értelmet ad a halmazműveletek egyenesekre való alkalmazásának. Egy ilyen

geometria abban különbözik a 3.1 részben definiált gráfoktól, hogy az egyenesekkel illeszkedő pontok száma nincs 2-re korlátozva.

Egy  $\Gamma$  geometria *általánosított  $n$ -szög*, vagy,  $n$ -re való explicit utalás nélkül, *általánosított sokszög*, ha [13, 22]

1. bármely  $x, y \in \Gamma$  elemekre  $\Gamma$ -nak van  $x$ -et és  $y$ -t tartalmazó  $n$ -hosszú köre. Egy ilyen kör  $\Gamma$ -nak egy *apartmanja*<sup>14</sup>.
2.  $\Gamma$ -nak nincs  $k$ -hosszú köre, ha  $2 \leq k < n$ .

Az  $n$ -hosszú körök ezt a két axiómát triviálisan teljesítik, ezért *hagyományos  $n$ -szögeknek*<sup>15</sup> is szokták őket nevezni. Ők tehát elsőrendű általánosított  $n$ -szögek. A  $GQ(s, t)$  szimbólum egy  $(s, t)$  rendű általánosított négyszöget jelent.

Ismert eredmény, hogy egy általánosított  $n$ -szög duálisa is általánosított  $n$ -szög, és hogy egy általánosított  $n$ -szög akkor és csak akkor sűrű, ha tartalmaz  $n + 1$ -hosszú kört. Egy általánosított  $n$ -szög illeszkedési gráfjának a derékbősége  $2n$  és átmérője  $n$ ; az egymástól (maximális)  $n$  távolságra lévő elemek *szembenállnak egymással*<sup>16</sup> [13].

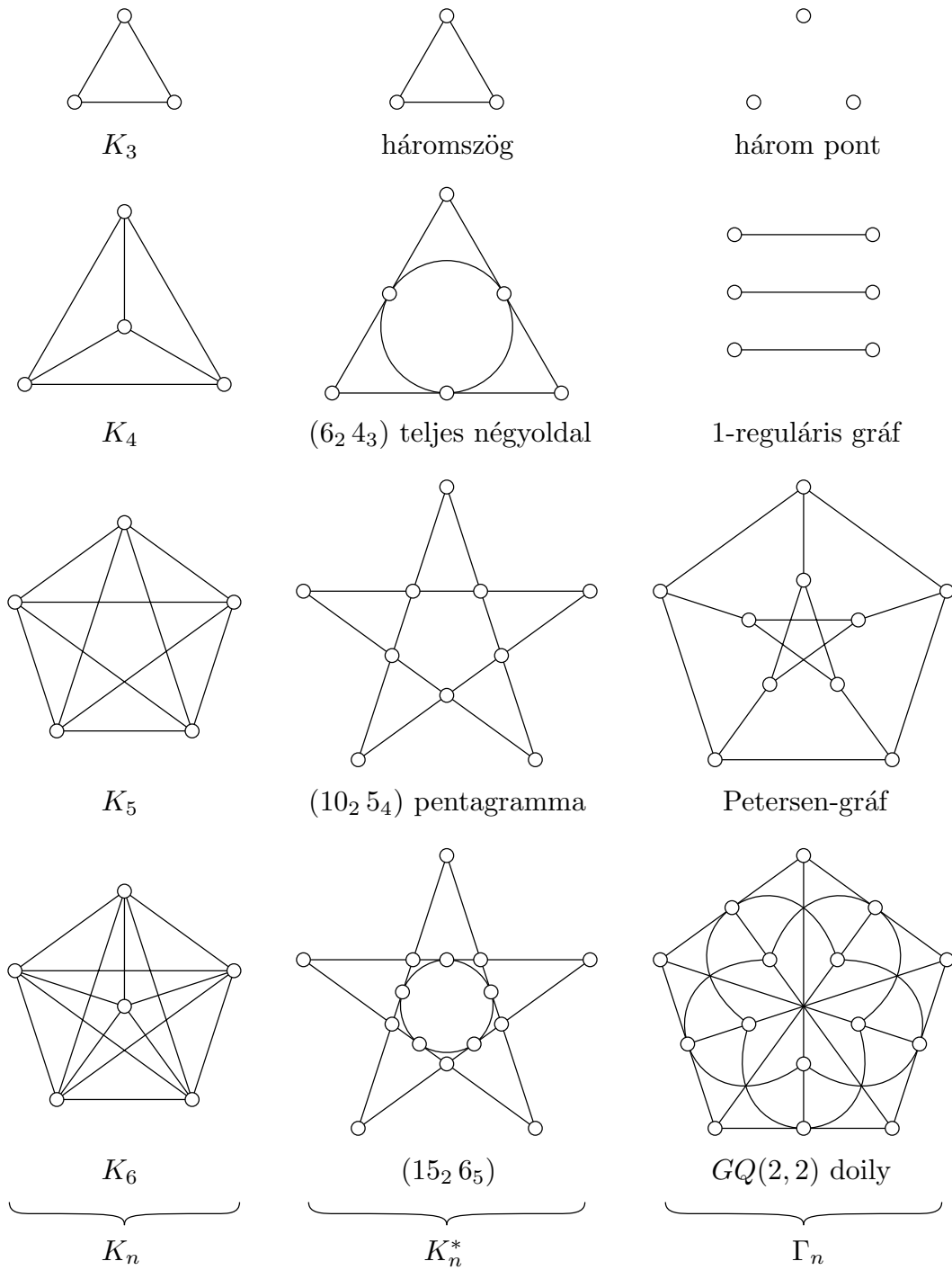
### 3.4. Néhány konkrét példa

A későbbiekben releváns geometriák egy része a  $K_n$ ,  $n = 3, 4, 5, 6$  teljes gráfból felépíthető (3.1. ábra). A teljes gráf  $K_n^*$  duálisa és a tőle jobbra lévő  $\Gamma_n$  geometria kapcsolata a következő:  $\Gamma_n$  pontthalmaza megegyezik  $K_n^*$  pontthalmazával, egyenesei pedig a  $K_n^*$ -ban maximális, páronként nem kollineáris pontokat tartalmazó  $S$  halmazok közül azok, amelyek elemszáma a lehető legnagyobb.

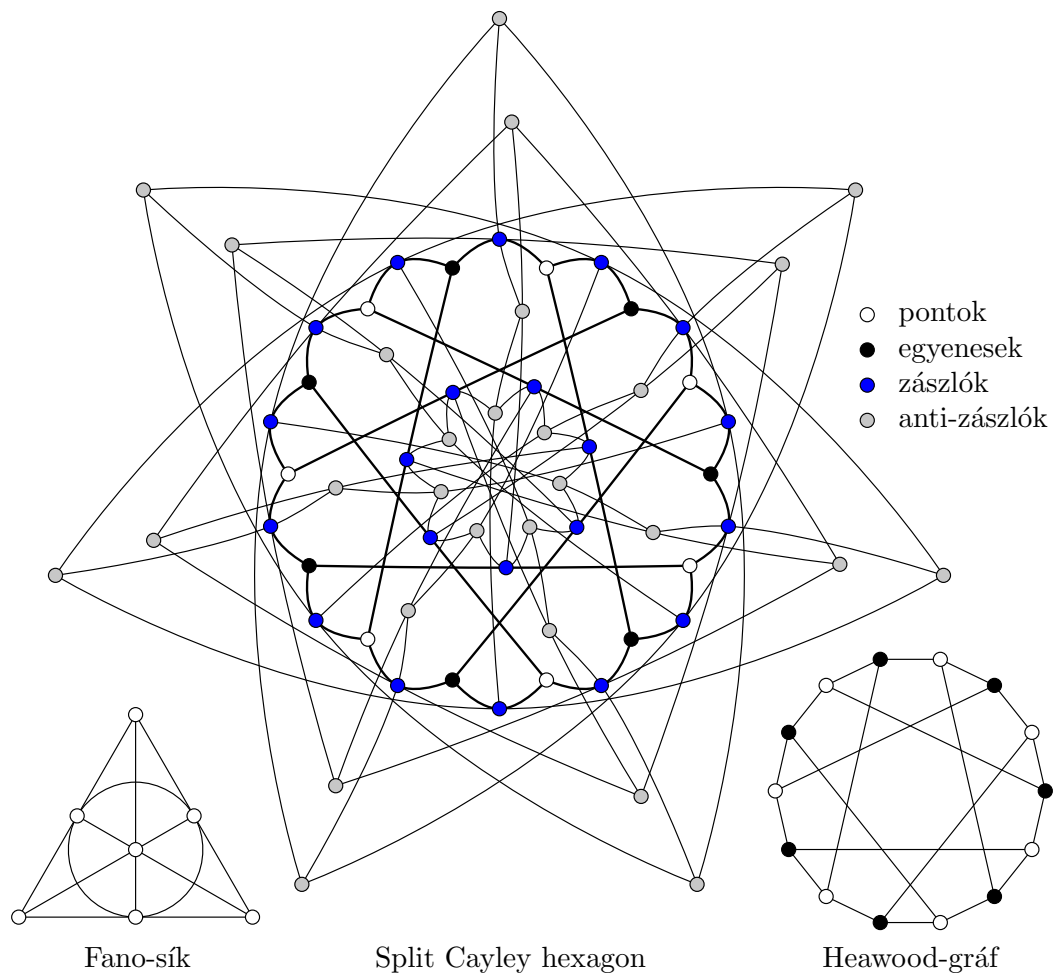
Speciálisan  $K_n^*$ -ban az  $S$  halmazok egyforma elemszámúak, ezért egyrészt mindegyikük  $\Gamma_n$  egyenese lesz, másrészt a  $\gamma : K_n^* \mapsto \Gamma_n$  leképezés nem kollineáris pontokhoz kollineáris pontokat rendel, és fordítva.

$K_n^*$  páronként kollineáris pontjainak a maximális halmazai két osztályba sorolhatók aszerint, hogy a pontok illeszkednek egy közös egyenessel vagy nem. Az előbbiek elemszáma  $n - 1$ , az utóbbiaké pedig 3, amiből következik, hogy a teljes gráfok duálisán értelmezett  $\gamma$  akkor és csak akkor invertálható (és inverze önmaga), ha  $n > 4$ , mivel ez kell ahhoz, hogy  $\Gamma_n$ -ben a két osztály ne mosódjon össze (vö:  $\Gamma_4$  esete, 3.1. ábra). Ha az invertálhatóság fennáll,  $\text{Aut}(\Gamma_n) \cong \text{Aut}(K_n)$ .

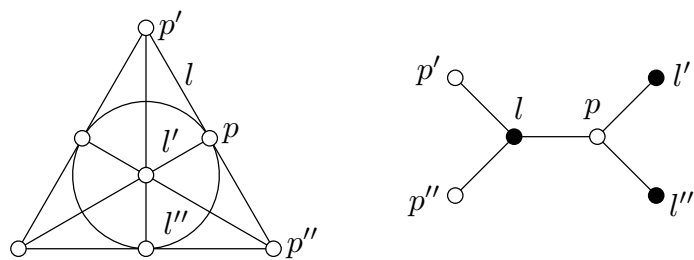
Az így kapott geometriákon kívül fontos még a *Fano-sík* és két, belőle felépíthető geometria, a *Heawood-gráf* és a *split Cayley-hexagon* (3.2. ábra).



3.1. ábra. Teljes gráfból felépíthető geometriák



3.2. ábra. Fano-síkból felépíthető geometriák



3.3. ábra. Fano-sík zászlója és illeszkedő elemek

A Fano-sík egy másodrendű általánosított háromszög, 7 pontja és 7 egyenese van, pontjai páronként kollineárisak, és apartmanjainak a száma<sup>17</sup> 28. A Fano-sík pontjainak, egyeneseinek, zászlóinak és anti-zászlóinak a száma, összesen, 63.

A Heawood-gráf a Fano-sík illeszkedési gráfja, ezért kétrésztű, 14 pontja van és 3-reguláris, így éleinek a száma 21. Minden él a Fano-sík egy zászlójának felel meg. A Heawood-gráf, mint geometria, egy (2, 1) rendű általánosított hatszög, és az előzőek alapján apartmanjainak a száma 28.

A split Cayley-hexagon (a továbbiakban csak *hexagon*) egy másodrendű általánosított hatszög 63 ponttal és 63 egyenessel. A pontok a Fano sík valamely pontjához, egyeneséhez, zászlójához vagy anti-zászlójához egyértelműen hozzárendelhetők [22] (3.2. ábra). Az egyenesek megkonstruálásához legyen  $\{p, l\}$  a Fano-sík zászlója. Az  $l$  egyenessel illeszkedő másik két pont legyen  $p'$  és  $p''$ , és a  $p$  ponttal illeszkedő másik két egyenes legyen  $l'$  és  $l''$  (3.3. ábra). Ekkor a  $\{p, l\}$  zászlóhoz rendelt hexagon-ponttal illeszkedő három egyenes alakja a pontokhoz tartozó Fano-sík-objektumokkal kifejezve

$$\{p, l, \{p, l\}\}, \quad \{\{p, l\}, \{p', l'\}, \{p'', l''\}\}, \quad \{\{p, l\}, \{p', l''\}, \{p'', l'\}\}. \quad (3.1)$$

Mivel a Fano-síknak 21 zászlója van, ez a konstrukció a 63 egyenest lefedi.

A hexagon 36 Heawood-gráfot tartalmaz. Ezek közül egy a 3.2. ábrán, a diagramon 7-edrendű forgási szimmetriával nem rendelkezők pedig a 3.4. ábrán láthatók. A hexagon apartmanjai egyértelműen valamelyik Heawood-gráfhoz tartoznak, ezért a számuk  $36 \cdot 28 = 1008$ .

A Fano-sík, a doily és a hexagon közös tulajdonsága, hogy másodrendű, azaz a lehető legkevesebb elemmel rendelkező sűrű általánosított sokszögek (a doily általánosított négyszög). A Fano-sík és a doily önduálisak, de a hexagon már nem az; duálisa a másik lehetséges másodrendű általánosított hatszög [21].

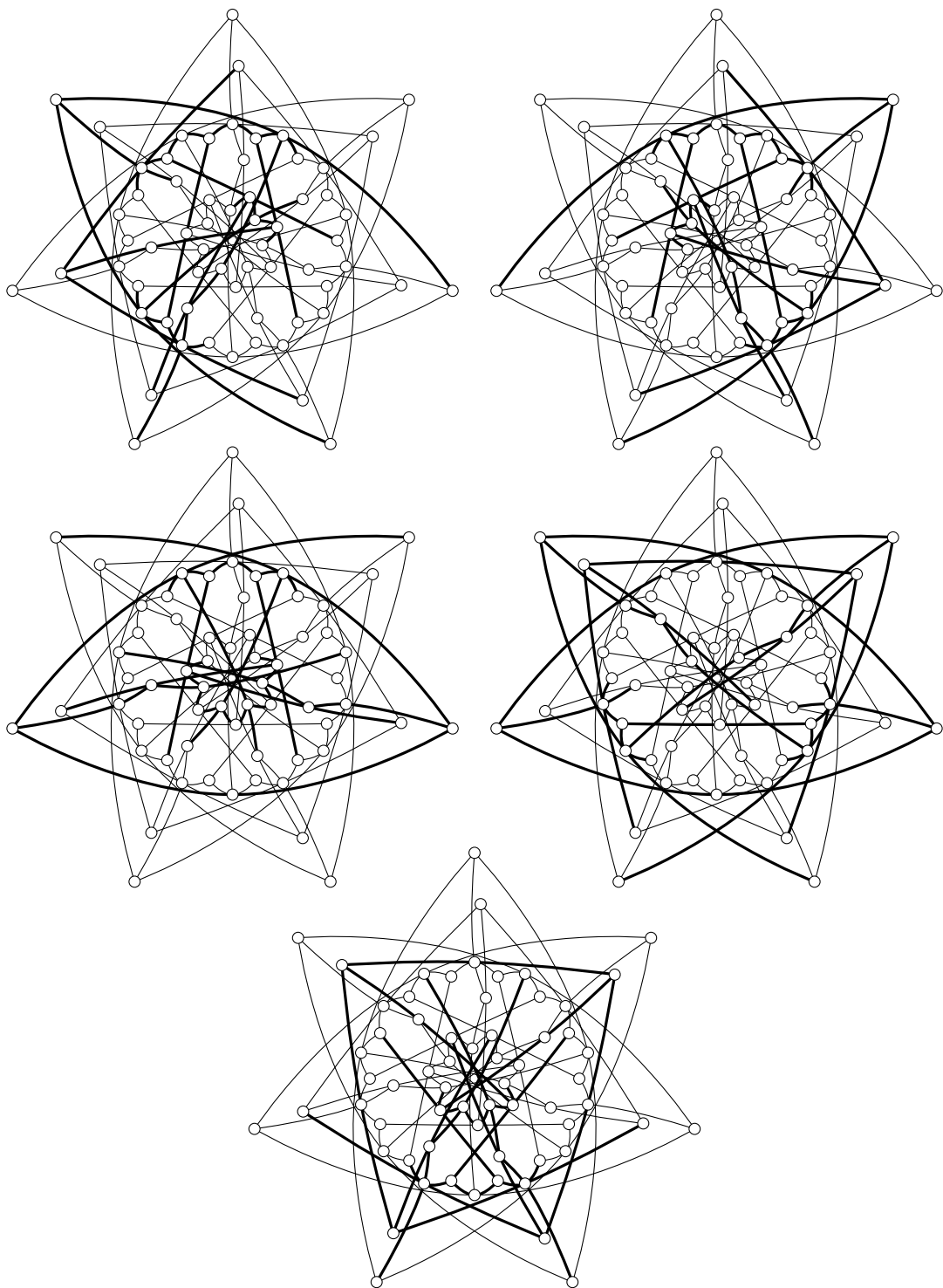
---

<sup>14</sup>Angol nyelvű terminológia: *apartment*.

<sup>15</sup>Angol nyelvű terminológia: *ordinary n-gon*

<sup>16</sup>Angol nyelvű terminológia: *opposites*.

<sup>17</sup>Azaz  $\binom{7}{3} - 7$ , mivel 7 darab közös egyenessel illeszkedő ponthármaszt nem kell számolni.



3.4. ábra. Nemtriviális Heawood-gráfok a hexagonban

## 4. Geometriák beágyazása és címkézése

### 4.1. Szimplektikus poláris tér

Absztrakt szinten, a 2.1. részben definiált szimplektikus vektorterek fontos geometriákat, ún. *szimplektikus poláris tereket* indukálnak [25]. Ha  $F = GF(q)$  és a vektortér  $2N$ -dimenziós, a szimplektikus poláris teret  $W(2N - 1, q)$  jelöli.  $W(2N - 1, q)$  elemei az indukáló vektortér izotróp alterei, két elem illeszkedik, ha valamelyik altér tartalmazza a másikat (a  $\sim$  illeszkedési reláció a szimmetrizált  $\leq$ ), és egy elem típusa az altér dimenziószáma. Az 1, 2, illetve 3 típusú elemek  $W(2N - 1, q)$  *pontjai*, *egyenesei*, illetve *síkjai*.  $W(2N - 1, q)$  rangja  $N$ .  $W(2N - 1, q)$  két pontja *kollineáris*, ha ugyanarra az egyenesre illeszkednek.

A kvantumelmélet és a szimplektikus poláris terek közti összefüggés a következő. Az  $N$ -qubit Pauli-csoport a (2.1) szimplektikus formával ellátott  $GF(2)^{2N}$  vektortérre képezhető (ld. 2.1. rész), vagyis adott egy *konkrét* szimplektikus vektortér, amely egy *konkrét*  $W(2N - 1, 2)$  szimplektikus poláris teret valósít meg. Ennek a térnek bármely pontját a megvalósító altér egyetlen nemnulla vektora, vagy a vektor által megadott Pauli-operátor egyértelműen azonosítja.

Módszertani érdekesség, hogy az  $N$ -qubit Pauli-csoport és  $W(2N - 1, 2)$  kapcsolatát [26] szerzői a szimplektikus vektortér megkerülésével építik fel. Természetesen ez az út rövidebb, de csak akkor járható, ha a gondolatmenet nélkülözheti a vektorterek által rendelkezésre bocsátott eszközöket.

A hátralevő részekben pont-egyenes geometriák  $W(2N - 1, 2)$ -be való beágyazásai lesznek megvizsgálva  $N = 2, 3$ -ra, illetve egy tágabb leképezés-osztályra, a *címkézésekre*<sup>18</sup> is szükség lesz. Ez utóbbiak speciális injektív gyenge homomorfizmusok, amelyek pontokhoz pontokat, de bizonyos esetekben egyenesekhez nem egyeneseket, hanem jól definiálható módon (ld. alább) síkokat<sup>19</sup> rendelnek. Bevezetésüket az motiválja, hogy  $W(2N - 1, 2)$ -be csak olyan geometriák ágyazhatók, amelyek egyenesekre legfeljebb három pont illeszkedik<sup>20</sup>.

Minden címkézést egy injektív  $\varphi$  *generátorfüggvény*<sup>21</sup> határoz meg, amely a vizsgált  $\Gamma$  geometria pontjait  $W(2N - 1, 2)$  pontjaira képezi úgy, hogy egy közös egyenessel illeszkedő pontok képei  $W(2N - 1, 2)$ -nek valamely, ponttól különböző típusú elemével illeszkednek. A  $\varphi$  által meghatározott címkézés képezze az  $l$  egyenest a legkisebb típusú ilyen elemre. A továbbiakban a  $\Gamma$  teljes elemhalmazán értelmezett címkézés és a generátorfüggvénye ugyanazzal a szimbólummal lesz jelölve.

<sup>18</sup>Átvett nemhivatalos elnevezés, saját definíció.

<sup>19</sup>vagy  $N > 3$  esetén akár még nagyobb típusú elemeket, de erre most nem lesz szükség

<sup>20</sup>Emlékeztető: egy beágyazás injektív, és őrzi az illeszkedéseket.

<sup>21</sup>Saját elnevezés.



A definícióból nem következik, de a vizsgált esetekben fennáll, hogy a fenti szabállyal a  $\varphi$  címkézés injektív, és az egyenesekhez ugyanolyan típusú elemeket rendel. Vagyis  $\varphi$  egy  $\Gamma \mapsto W(2N - 1, 2)$  injektív gyenge homomorfizmus.

Mivel  $W(2N - 1, 2)$  pontjait  $GF(2)^{2N}$  nemnulla vektorai egyértelműen azonosítják, könnyebb azt mondani, hogy  $\varphi$ , generátorfüggvény vagy címkézés,  $\Gamma$  kollineáris pontjaihoz ortogonális  $GF(2)^{2N}$ -beli vektorokat, és így, közvetetten, kommutáló  $N$ -qubit Pauli-operátorok rendel<sup>22</sup>. Konkrét címkézések ábrázolásában a geometria pontjai mellett az operátorok lesznek feltüntetve.

Ha a szöveggörnyezetből egyértelmű, hogy melyik címkézésről van szó, a rá való explicit utalást meg lehet spórolni egy olyan szóhasználattal, amely nem tesz különbséget  $\Gamma$  pontjai, a hozzájuk rendelt  $W(2N - 1, 2)$ -pontok, az utóbbiakat azonosító vektorok, és a vektorok által megadott  $N$ -qubit Pauli-operátorok között. Így van értelme azt mondani, hogy „ $\Gamma$  vektorai kollineárisak” vagy „az operátorok az  $l$  egyenessel illeszkednek”.

## 4.2. Ekvivalens és nemekvivalens címkézések

A Bell–KS-konfigurációk vizsgálata során fontos tudni, hogy két címkézés mikor határoz meg két *különböző* konfigurációt. Definíciószerűen, a  $\varphi$  és  $\varphi'$  címkézések *ekvivalensek* (jelölés:  $\varphi' \equiv \varphi$ ), ha valamely  $\alpha \in \text{Aut}(\Gamma)$ -ra  $\varphi' = \varphi\alpha$ .

$\Gamma$  nemekvivalens címkézéseinek a száma,  $|\text{Aut}(\Gamma)|$  és  $|\text{Sp}(2N, 2)|$  nem függetlenek. A  $GF(2)^{2N}$ -en értelmezett  $\mathbf{M}$  szimplektikus mátrix és egy  $\varphi$  generátorfüggvény kompozíciója egy újabb,  $\mathbf{M}\varphi$ -vel jelölhető címkézés generátorfüggvénye, és így  $\Gamma$  címkézéseinek a halmazán egy  $\text{Sp}(2N, 2)$  csoporthatás definiálható.

$\varphi$  stabilizátorát jelölje  $s(\varphi)$ , és a stabilizátor definíciójához hasonlóan legyen

$$S(\varphi) = \{\mathbf{M} \in \text{Sp}(2N, 2) \mid \mathbf{M}\varphi \equiv \varphi\}.$$

Ekkor  $s(\varphi)$  részcsoportja  $S(\varphi)$ -nek, és

$$\frac{|S(\varphi)|}{|s(\varphi)|} = |\text{Aut}(\Gamma)|.$$

Következik, hogy a  $\varphi$ -vel közös orbiton lévő nemekvivalens címkézések száma

$$\frac{|\text{Sp}(2N, 2)|}{|S(\varphi)|} = \frac{|\text{Sp}(2N, 2)|}{|s(\varphi)| \cdot |\text{Aut}(\Gamma)|}, \quad (4.1)$$

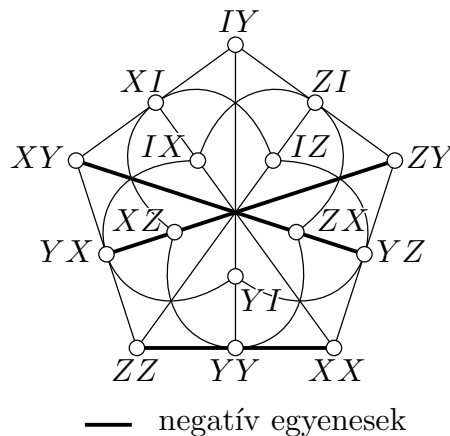
<sup>22</sup>Ezzel a szemlélettel az  $l \in \Gamma$  egyenes, mint pont-halmaz,  $\varphi$  szerinti képe páronként ortogonális vektorok halmaza, és mint olyan, egy izotróp alteret feszít ki. A  $\varphi$  címkézés  $l$ -t ezen alter által megvalósított  $W(2N - 1, 2)$ -beli elemre képezi.

Ahhoz, hogy  $\Gamma$  címkézései  $\Gamma$  geometriájú Bell–KS-konfigurációkat adjanak meg, a Waegell–Aravind-kritériumoknak teljesülniük kell. Az 1.4. részben leírtak alapján, az új fogalmakkal a WA-kritériumok így hangzanak:

1. adott címkézés esetén  $\Gamma$  minden egyenesére igaz, hogy a vele illeszkedő Pauli-operátorok szorzata az egységoperátor  $\pm 1$ -szerese (azaz a vele illeszkedő vektorok összege a nullvektor). Ekkor  $\Gamma$ -nak *pozitív*, illetve *negatív* egyenesei különböztethetők meg.
2.  $\Gamma$  minden pontja páros számú egyenessel illeszkedik;
3.  $\Gamma$ -nak páratlan számú negatív egyenesre van.

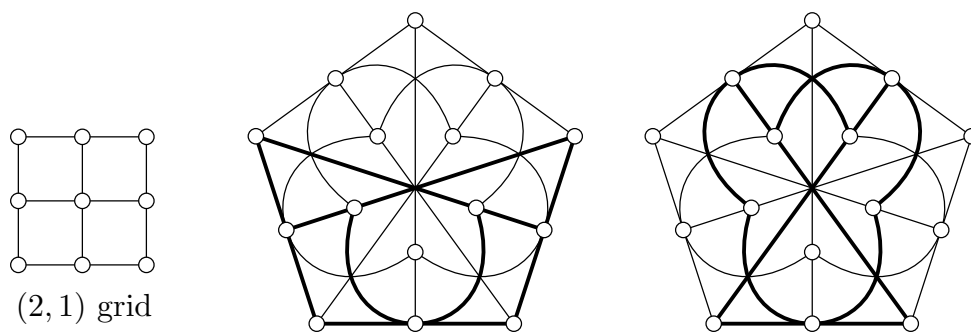
Ha az 1. kritérium a  $\varphi$  címkézésre teljesül, akkor tetszőleges  $\mathbf{M} \in \text{Sp}(2N, 2)$  esetén  $\mathbf{M}\varphi$ -re is teljesül. A 3. kritérium  $\mathbf{M}\varphi$ -re már nem garantált, mivel az egyenesek „előjelére” vonatkozó információt sem a  $GF(2)^{2N}$  vektortér, sem a  $W(2N - 1, 2)$  szimplektikus poláris tér nem tartalmazza; ez a Pauli-csoport leképezése során elveszett. Emiatt a  $\Gamma$  geometriájú Bell–KS-konfigurációk számát (4.1) nem adja meg, hanem csak felülről becsüli. A tényleges egyenlőség, jó esetben, számítógéppel ellenőrizhető (ld. pl. [20], Conclusion).

### 4.3. $W(3, 2)$ és a doily izomorfája, Mermin-négyzetek



4.1. ábra. Doily és  $W(3, 2)$  izomorfája

A (2.8) formula szerint  $GF(2)^4$ -nek 15 egydimenziós, és ugyanennyi kétdimenziós izotróp altere van. Az utóbbiak, a Lagrange-altér, 3 nemnulla vektort tartalmaznak, és ezek 3, az adott Lagrange-altérben lévő egydimenziós alteret feszítenek ki. A (2.8) formula utáni megjegyzések alapján minden egydimenziós, és egyben



4.2. ábra. (2,1) grid-ek a doily-ban

izotróp, alteret 3 Lagrange-altér tartalmaz. Tehát  $W(3,2)$  másodrendű geometria 15 ponttal és 15 egyenessel.

A 4.1. ábrán látszik, hogy a doily  $W(3,2)$ -vel izomorf (a kiemelt egyenesek negatívak). Az izomorfizmus, mint beágyazás stabilizátora triviális, és mivel (2.13) szerint  $\text{Sp}(4,2)$  rendje megegyezik a doily automorfizmus-csoportjának a rendjével, (4.1) alapján a csoportthatás újabb nemekvivalens beágyazásokat nem hoz létre.

A 4.2. ábrán a (2,1) grid (a Mermin-négyzetek geometriája) és a doily 10 darab grid-je látható, az utóbbiak egy ötödrendű forgási szimmetria erejéig. 9 grid-nek 1, 1-nek pedig 3 negatív egyenese van, ezért mind a 10 egy-egy Mermin-négyzetet határoz meg. Ez ismert eredmény, ld. pl. [23].

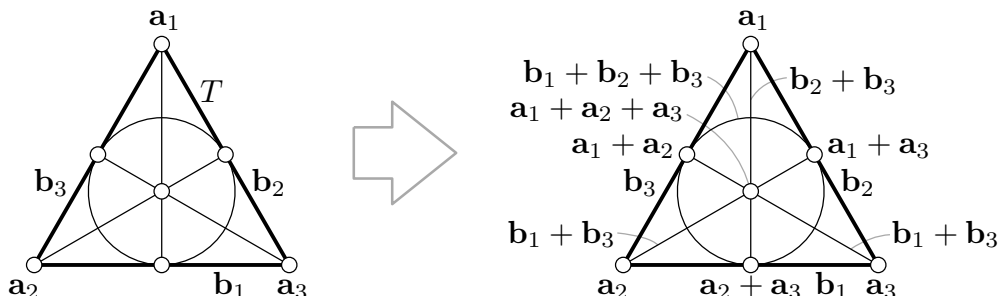
#### 4.4. A hexagon klasszikus beágyazása $W(5,2)$ -be

A hexagon  $W(5,2)$ -be való ún. *klasszikus* beágyazásai több okból is figyelemre méltók. Az egyik az, hogy csak a szembenálló vektorok nem ortogonálisak, amiből a 2.7. Lemma alapján következik, hogy az apartmanok (6-hosszú körök) vektorai szimplektikus bázist alkotnak. Ez a jelenség a doily beágyazásán is megfigyelhető. Miatta a hexagon minden klasszikus beágyazásának a stabilizátora triviális.

A klasszikus beágyazások másik fontos tulajdonsága, hogy tetszőleges apartman pontjainak a képe a teljes beágyazást meghatározza. Bármely apartman valamilyik hexagon-beli Haewood-gráf apartmanja, ezért egy Fano-sík háromszögének az illeszkedési gráfja.

A Fano-sík egy  $T$  háromszögének az elemei leképezhetők egy  $B \subseteq GF(2)^6$  szimplektikus bázis vektoraira úgy, hogy nemortogonális vektorok csak szembenálló, és így különböző típusú elemekhez tartozzanak (4.3. ábra, bal). Legyen  $U_1$ , illetve  $U_2$  a pontokhoz, illetve az egyenesekhez tartozó vektorok által kifeszített Lagrange-altér. A leképezés a teljes Fano-síkra kiterjeszthető úgy, hogy adott típusú ele-

mekhez ugyanannak az  $U_i$  Lagrange-altérnek a nemnulla vektorai tartoznak, és, továbbra is, csak a szembenálló elemekhez rendelt vektorok ne legyenek ortogonálisak (4.3. ábra, jobb).



4.3. ábra. Vektorok hozzárendelése a Fano-sík elemeihez

Rögzítve, hogy a Fano-sík bármely  $\{p, l\}$  zászlójához vagy anti-zászlójához a  $p$ -hez és  $l$ -hez rendelt vektorok összege tartozzon, a (3.1) konstrukció miatt egy hexagon-beágyazás generátorfüggvénye adódik (vö: [24], IV. rész). A  $GF(2)^6$  kanonikus bázisából így felépíthető hexagon-beágyazás a 4.4. ábrán látható.

Az említett két tulajdonság a következő észrevételt támasztja alá: a hexagon egy automorfizmusát egyértelműen jellemzi, hogy egy kiszemelt apartmant melyik másikra képezi, és hogyan. Az apartmanok száma 1 008, az apartman-apartman izomorfizmusoké pedig, a  $D_6$  diéder-csoport rendjével azonosan, 12. Következik, hogy a hexagon automorfizmus-csoportjának<sup>23</sup> a rendje 12 096. Mivel a klasszikus beágyazások stabilizátora triviális, a nemekvivalens beágyazások száma

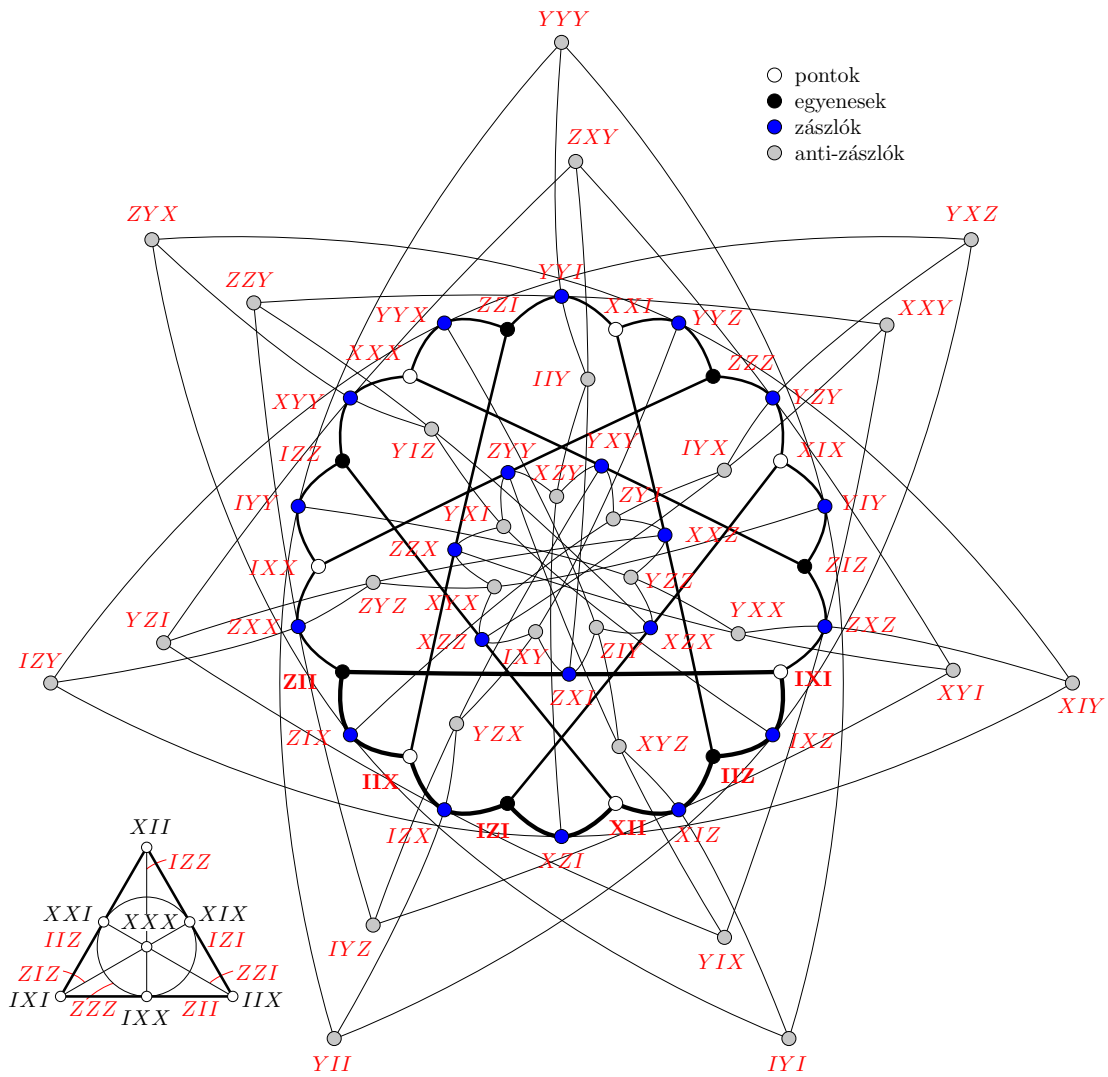
$$\frac{|\text{Sp}(6, 2)|}{12\,096} = 120.$$

A továbbiakban nem lesz különös jelentősége, de érdemes megjegyezni, hogy a hexagonnak ún. *ferde* beágyazása is létezik (konkrét példa: ld. [20], Figure 2), viszont a csoporthatás a klasszikus beágyazások halmazából nem vezet ki.

#### 4.5. A $(10_2 5_4)$ pentagramma $W(5, 2)$ -be képező címkézése

A hexagon és a  $(10_2 5_4)$  pentagramma egymás ellentétei abban az értelemben, hogy míg az előbbinek 12 096 automorfizmusa és 120 nemekvivalens beágyazása, az utóbbinak, pont fordítva, 120 automorfizmusa és 12 096 nemekvivalens címkézése

<sup>23</sup>Ez a csoport izomorf a  $G_2(2)$  Chevalley-csoporttal, ezért a split Cayley-hexagont  $G_2(2)$  hexagonnak is hívják [24].

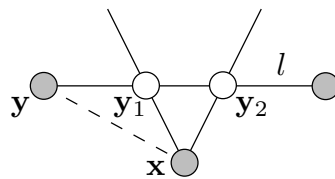


4.4. ábra. A  $GF(2)^6$  kanonikus bázisa által meghatározott hexagon-beágyazás

van. Az állítás a (4.1) formulából következik, de ehhez be kell látni, hogy a pentagramma címkézéseinek a stabilizátora triviális.

A címkézések az egyenesekhez  $W(5, 2)$  síkjait rendelik, és teljesítik az 1. WA-kritériumot. Ami a 3. WA-kritériumot illeti, számítógép segítségével ellenőriztem, hogy az 1, 3, illetve 5 negatív egyenest eredményező címkézések száma 7 884, 4 104, illetve 108. Ez nem teljesen új eredmény, ld. [20], Conclusion.

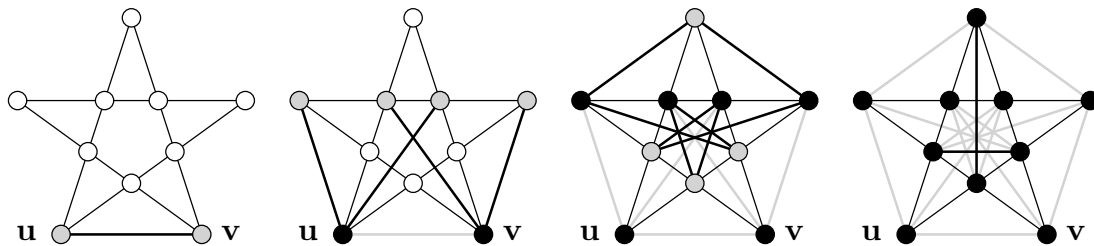
**4.1. Lemma.** *Ha a pentagramma két nemkollineáris  $\mathbf{x}$  és  $\mathbf{y}$  vektora ortogonális, akkor az összes  $\mathbf{y}$ -nal kollineáris vektor ortogonális  $\mathbf{x}$ -re.*



4.5. ábra. Segédábra a 4.1. Lemmához

*Bizonyítás.* Egy  $\mathbf{y}$ -nal illeszkedő  $l$  egyenes az  $\mathbf{x}$ -el illeszkedő egyenesektől különbözik, de metszi azokat, és a közös vektorokat jelölje  $\mathbf{y}_1$  és  $\mathbf{y}_2$  (4.5. ábra). A kollinearitások miatt  $\mathbf{x}$  ortogonális  $\mathbf{y}_1$ -re és  $\mathbf{y}_2$ -re. Ha  $\mathbf{x}$  ortogonális  $\mathbf{y}$ -ra, akkor az  $l$ -el illeszkedő negyedik vektorra,  $\mathbf{y} + \mathbf{y}_1 + \mathbf{y}_2$ -re is ortogonálisnak kell lennie.  $\square$

**4.2. Lemma.** *A pentagramma két vektora akkor és csak akkor ortogonális, ha kollineáris.*

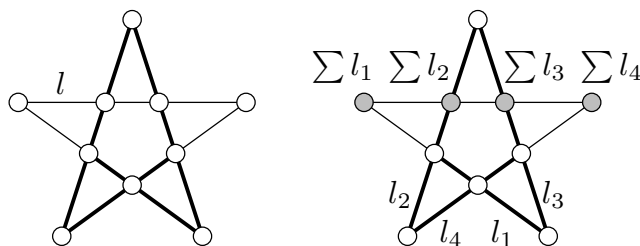


4.6. ábra. Segédábra a 4.2. Lemmához

*Bizonyítás.* A címkézések definíciója miatt csak azt kell belátni, hogy az ortogonalitás elégséges a kollinearitáshoz. Ez indirekt módon bizonyítható. Legyen  $\mathbf{u}$  és  $\mathbf{v}$  a pentagramma két nem kollineáris, de ortogonális vektora. Az ellentmondáshoz a 4.1. Lemma egymásutáni alkalmazása vezet, és ez a 4.6. ábrán látható. A szürke vektorok a lemmabeli  $\mathbf{x}$  szerepét töltik be, a vastag fekete vonalak az újonnan

megállapított ortogonalitások, és a fekete vektorok már biztosan minden vektorra ortogonálisak. A végén az adódik, hogy tíz különböző vektor páronként ortogonális.  $GF(2)^6$  maximális, páronként ortogonális vektorokat tartalmazó halmazai a Lagrange-alterek, és ezeknek csak 7 nemnulla vektoruk van.  $\square$

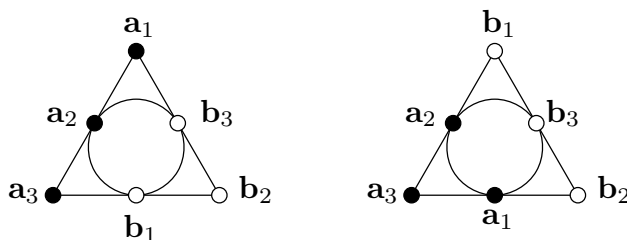
A pentagramma minden egyeneséhez egy teljes négyoldal tartozik (4.7. ábra, bal). A 4.2. és a 2.7. Lemmából következik, hogy mind az öt teljes négyoldal vektorai szimplektikus bázist alkotnak.



4.7. ábra. Az  $l$  egyeneshez tartozó teljes négyoldal

Mivel a pentagramma közös egyenessel illeszkedő vektorainak az összege a nullvektor, bármely teljes négyoldal címkézése a pentagramma címkézését is meghatározza. A generátorfüggvények közti összefüggés a 4.7. ábra jobb oldali digramján látható, ahol  $\sum l$  a teljes négyoldal  $l$  egyenesével illeszkedő vektorok összege. Mechanikusan belátható, hogy  $\sum_i \sum l_i = 0$ .

**4.3. Lemma.** *A teljes négyoldalnak két olyan  $W(5, 2)$ -be képező nem-ekvivalens címkézése van, amely generátorfüggvényének a képhalmaza ugyanaz a szimplektikus bázis.*



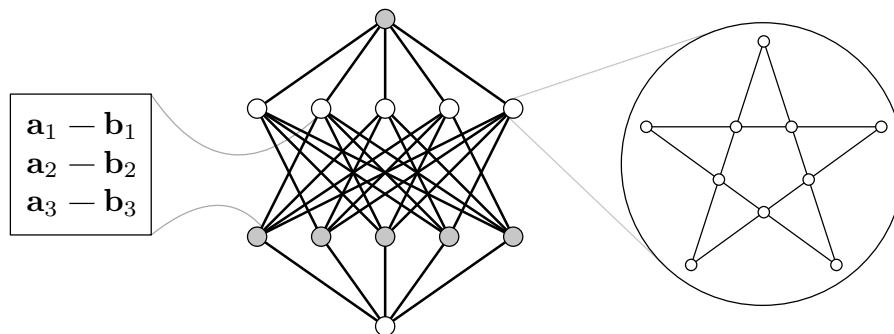
4.8. ábra. Segédábra a 4.3. Lemmához

*Bizonyítás.* A generátorfüggvény a teljes négyoldal nemkollineáris pontjait csak nemortogonális vektorokra képezheti. Három, páronként ortogonális bázisvektor az egyik címkézésben közös egyenesre illeszkedik, a másikban a teljes négyoldal valamely háromszögének a három vektora (4.8. ábra).  $\square$

Legyen a pentagramma címkézése  $\varphi$ . Ekkor tetszőleges  $l$  egyeneshez tartozó  $Q$  teljes négyoldal címkézése adott.  $Q$ -nak a 4.3. Lemma szerinti másik címkézéséből származó pentagramma-címkézés  $\varphi$ -nek az  $l$ -konjugáltja<sup>24</sup>.

Az  $l$ -konjugálás a definíció alapján önmaga inverze. A művelet megváltoztatja az  $l$  egyenesre illeszkedő vektorokat: a  $Q$  egyenseire illeszkedő vektorok összegét a  $Q$ -beli háromszögek vektorainak az összege váltja fel (vö: 4.7. ábra, jobb).

Egy adott pentagramma-címkézésnek 5 darab  $l$ -konjugáltja van. Számítógépet használva feltártam, hogy a pentagrammák 1008 darab 12-es csoportba, *dupla hatosokba*<sup>25</sup> szerveződnek, és egy dupla hatosból az  $l$ -konjugálás nem vezet ki.



4.9. ábra. Dupla hatosok és megvalósító objektumok

A dupla hatosok szerkezetét a 4.9. ábra szemlélteti. A gráf pontjai pentagramma-címkézéseket, az élek szimplektikus bázisokat, és a szomszédos pontok egymással  $l$ -konjugált kapcsolatban álló címkézéseket reprezentálnak. Az azonos árnyalatú pontok a kétrésű gráf azonos partíciójához tartoznak.

## 4.6. A hexagon és a $(10_2, 5_4)$ pentagramma címkézéseinek a kapcsolata

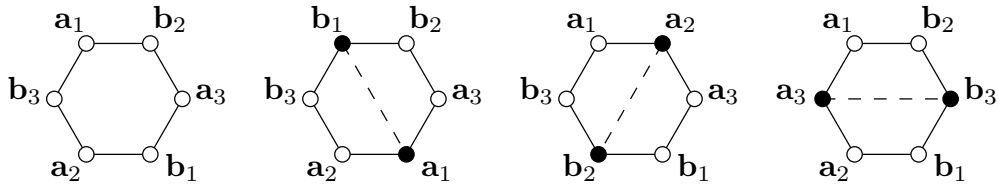
**4.4. Lemma.** *A 6-hosszú körnek négy olyan  $W(5,2)$ -be képező nemekvivalens beágyazása van, amely generátorfüggvényének a képhalmaza ugyanaz a szimplektikus bázis, és a szembenálló pontok képei nemortogonálisak.*

*Bizonyítás.* A négy beágyazás a 4.10. ábrán látható. Az első diagramhoz képest a többi háromban a kiemelt pontokhoz rendelt nemortogonális vektorpár fel van cserélve. A négy diagramot középpontosan tükrözve belátható, hogy többszörös cserével újabb nemekvivalens beágyazások nem hozhatók létre.  $\square$

<sup>24</sup>Saját elnevezés.

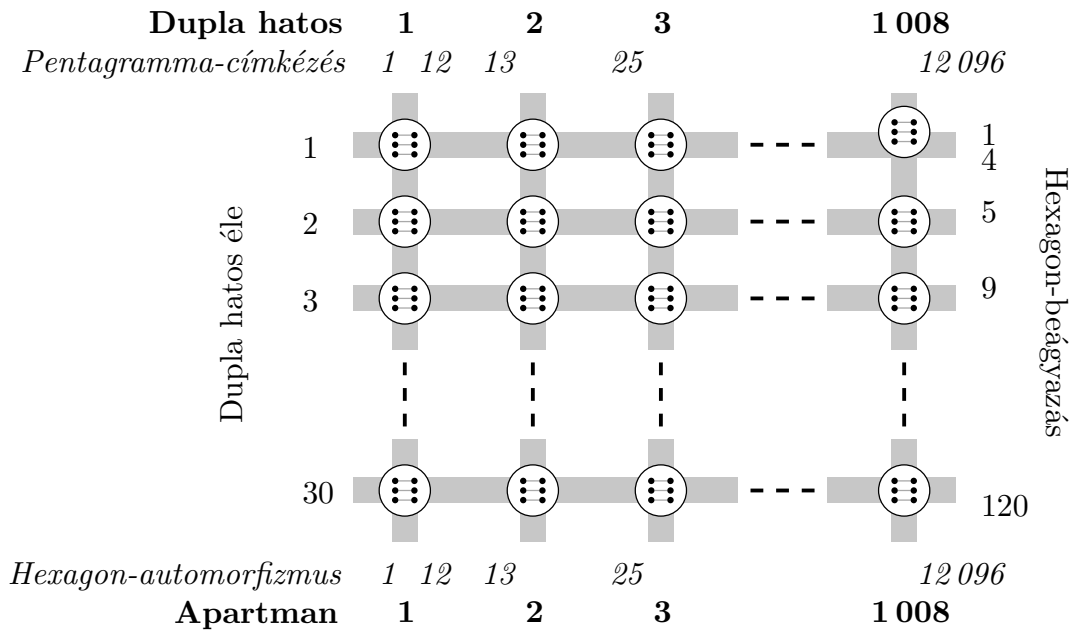
<sup>25</sup>Az elnevezés abból ered, hogy a gráf (ld. 4.9. ábra) a 30 pontból és 12 egyenesből álló Schläfli-féle dupla hatos konfiguráció duálisával izomorf.





4.10. ábra. Segédábra a 4.4. Lemmához

A pentagramma és a hexagon kapcsán előbukkanó 12 096 és 120 számokra [26] és [20] szerzői is felfigyeltek. Ennek a magyarázatát a 4.11. ábra foglalja össze, amit a következőképpen kell értelmezni.

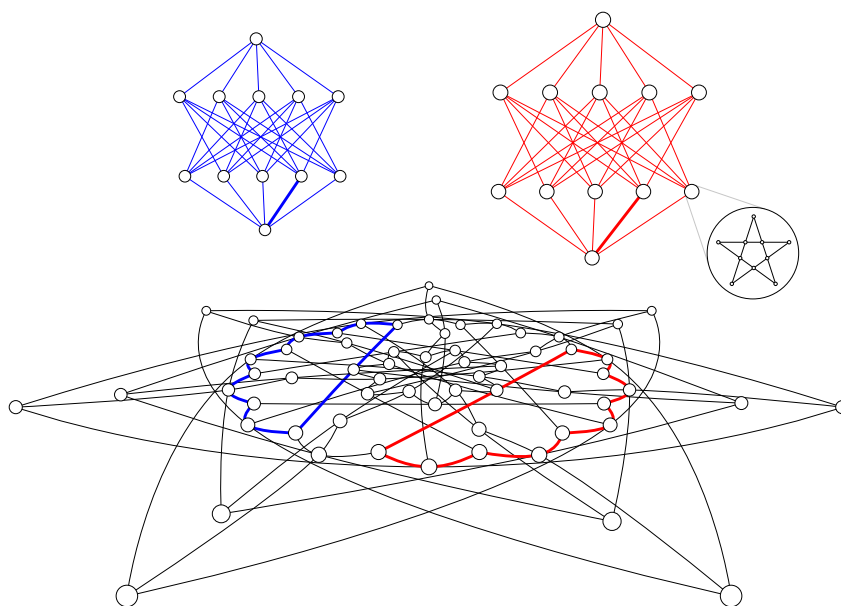


4.11. ábra. A többször is előbukkanó 12 096 szám magyarázata

A függőleges sávok kifejezik, hogy a dupla hatosok és a hexagon apartmanjai kölcsönösen egyértelműen megfeleltethetők egymásnak. Egy dupla hatos 12 pentagramma-címkézésből áll, egy apartmannak pedig 12 automorfizmusa van.

A vízszintes sávok a 120 nemekvivalens hexagon-beágyazás és a dupla hatosok 30 élének a kapcsolatát fejezik ki. Egy kiválasztott dupla hatos 30 szimplektikus bázis kiválasztását jelenti (ld. 4.9. ábra), és a 4.4. Lemma alapján a dupla hatoshoz tartozó hexagon-apartmannak ezekből 120 beágyazása készíthető el. Az utóbbiakat kiterjesztve a hexagonra, adódik a 120 klasszikus beágyazás.

A vízszintes és függőleges sávok találkozási pontjában egy-egy szimplektikus bázis áll. Ezek száma az ábra, és a (2.12) formula szerint is,  $1\,008 \cdot 30 = 30\,240$ . Ha a



4.12. ábra. Dupla hatosok és hexagon-apartmanok kapcsolata

hexagon beágyazása rögzített, egy sor az apartmanok által meghatározott szimp-  
plektikus bázisokat reprezentálja. Egy oszlop egy kiválasztott dupla hatos élét  
megvalósító bázisokat jelenti.

Az 4.12 ábra az elhangzottakat szemlélteti. A hexagon aktuális (az ábrán nem  
feltüntetett) beágyazása a dupla hatosok kiemelt éléhez tartozik.

## 4.7. Pentagrammák címkézésein értelmezett műveletek

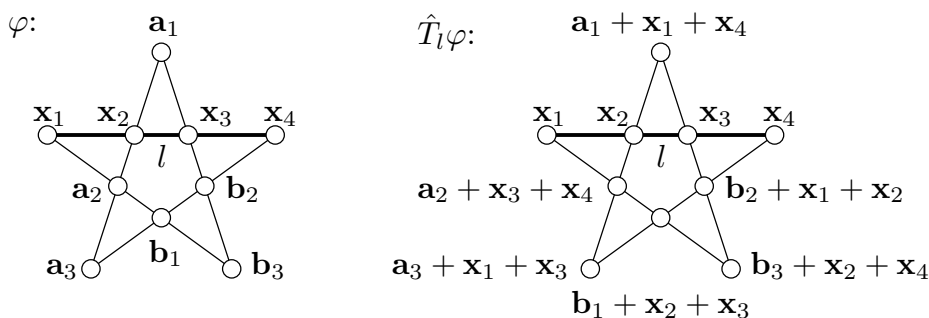
Az  $l$ -konjugálás nem az egyedüli, címkézésekre ható művelet, amely a dupla hatosokból nem vezet ki. Ebben a részben két újabb művelet lesz megvizsgálva, mivel ezek a dupla hatosokat egy másik irányból világítják meg, és ezzel, indirekt módon, a Bell–KS-konfigurációk egy osztályának a megtalálásához járulnak hozzá.

Legyen a pentagramma címkézése  $\varphi$ . Ha az  $l$  egyenessel illeszkedő vektorok  $\mathbf{x}$ ,  $\mathbf{y}$ ,  $\mathbf{z}$  és  $\mathbf{w}$ , a címkézésre ható  $l$ -transzvekcio<sup>26</sup>

$$\hat{T}_l\varphi := \hat{T}_x\hat{T}_y\hat{T}_z\hat{T}_w\varphi, \quad (4.2)$$

ahol  $\hat{T}_x$  az  $\mathbf{x}$  vektorhoz tartozó transzvekcio. Mivel a négy vektor páronként orto-  
gonális, a (2.14) Coxeter-relációk miatt a transzvekcio sorrendje lényegtelen.

<sup>26</sup>Saját elnevezés.



4.13. ábra. Címkezés  $l$ -transzvektáltja

A művelet hatását, az általánosság megsértése nélkül, a 4.13. ábra mutatja. Az, hogy a jobb oldalon valóban egy, az 1. WA-kritériumot teljesítő címkezés látható, néhány lépésben mechanikusan ellenőrizhető. Az  $l$  egyenesre illeszkedő pontokhoz  $\hat{T}_l\varphi$  ugyanazokat a  $W(5, 2)$ -pontokat rendeli, mint  $\varphi$ , ami tömören úgy mondható, hogy *a két címkezésnek van közös egyenese*.

Legyen  $\sum \varphi$  a pentagramma vektorainak az összege. Az 4.13. ábra mindkét oldalán a vektorokat összeadva, és felhasználva, hogy  $\sum_i \mathbf{x}_i = \mathbf{0}$ , adódik, hogy

$$\sum \varphi = \sum \hat{T}_l\varphi. \quad (= \mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3 + \mathbf{b}_1 + \mathbf{b}_2 + \mathbf{b}_3) \quad (4.3)$$

Pusztán a geometriát tekintve, a pentagramma bármely  $p$  pontja három egyenessel nem illeszkedik (jelölje őket  $l_1, l_2$  és  $l_3$ ), és három ponttal nem kollineáris (ezek  $l_1l_2, l_2l_3$  és  $l_1l_3$ ). Ez a hat elem egy  $T(p)$  háromszöget indukál. Ha adott egy  $\varphi$  címkezés, és  $\varphi(p) = \mathbf{x}$ , a  $T(p)$  és  $T(\mathbf{x})$  jelölések ekvivalensek.  $T(\mathbf{x})$  vektorainak az összegét jelölje  $\sum T(p)$ , vagy  $\sum T(\mathbf{x})$ . A  $p \mapsto \sum T(\mathbf{x})$  generátorfüggvényű,  $\varphi^*$ -gal jelölt címkezés  $\varphi$  konjugáltja<sup>27</sup>. Vagyis egy  $\varphi$  címkezés konjugáltját úgy kell elkészíteni, hogy egy adott  $p$  ponthoz a  $T(p)$  háromszög  $\varphi$  szerinti vektorainak az összegét kell rendelni.

A  $\varphi \mapsto \varphi^*$  leképezés transzvektációval is felírható.  $\sum \varphi$ -re a pentagramma egyetlen  $\mathbf{x}$  vektora sem ortogonális, mivel három vektor nem ortogonális  $\mathbf{x}$ -re, és így

$$\hat{T}_{\sum \varphi} \mathbf{x} = \mathbf{x} + \sum \varphi.$$

Az 1. WA-kritérium miatt az  $\mathbf{x}$  perp-halmazában lévő vektorok összege  $\mathbf{x}$ , ezért  $\sum \varphi = \mathbf{x} + \sum T(\mathbf{x})$ , amiből következik, hogy  $\hat{T}_{\sum \varphi} \mathbf{x} = \sum T(\mathbf{x})$ . Tehát

$$\varphi^* \equiv \hat{T}_{\sum \varphi} \varphi. \quad (4.4)$$

<sup>27</sup>Ismert szó, új fogalomra használva.

$\sum \varphi^*$  kiszámolása során felhasználható, hogy a pentagramma adott pontjával illeszkedő két egyenes a  $p$ -vel nem illeszkedő három egyenes mindegyikével egy-egy háromszöget határoz meg. Vagyis minden pont három darab háromszögnek a pontja. Következik, hogy  $\sum \varphi^*$ -ban minden pont  $\varphi$  szerinti vektora háromszorosan van figyelembe véve, ezért

$$\sum \varphi^* = \sum \varphi. \quad (4.5)$$

Mivel egy transzvektió önmaga inverze, a (4.4) és (4.5) formulákból látszik, hogy a konjugálás is önmaga inverze, azaz  $\varphi$  kétszeres konjugálása egy  $\varphi$ -vel ekvivalens címkézést eredményez.

A definíciókat felhasználva mechanikusan ellenőrizhető, hogy a már megismert  $l$ -konjugálás az  $l$ -transzvektió és a konjugálás szorzata. A két művelet felcserélhető:

$$(\hat{T}_l \varphi)^* = \hat{T}_{l^*} \varphi^*, \quad (4.6)$$

A  $\hat{T}_{l^*}$  szimbólumban a  $*$  azt jelenti, hogy az  $l$ -transzvektiót a  $\varphi^*$  címkézés szerinti vektorokkal kell elvégezni (ld. (4.2)).

Egy tetszőleges  $\varphi$  címkézésből kiindulva  $l$ -transzvektiókkal 5 másik címkézés hozható létre, és a művelet ennek a 6 címkézésnek a halmazából nem vezet ki. Ez a halmaz a 4.9. ábrán látható kétrészes gráf egy partíciója. Benne bármely két címkézésnek van közös egyenese. A partíciók közti átjáró művelet a konjugálás.

Az 4.14. ábra ezeket az észrevételeket szemlélteti arra az esetre, amikor a kiinduló címkézés a pentagramma valamelyik teljes négyoldalának a pontjaihoz a kanonikus bázisvektorokat rendeli (a hozzájuk tartozó Pauli-operátorok  $XII$ ,  $IXI$ ,  $IIX$ ,  $ZII$ ,  $IZI$ ,  $IIZ$ ).

Egy adott  $\hat{T}_l$   $l$ -transzvektió és a konjugálás a dupla hatos összes címkézésére a következőképpen hat. Legyen  $l$  az azonos partíciókhoz tartozó  $\varphi_1$  és  $\varphi_2$  címkézések közös egyenese<sup>28</sup>, és most, (4.6) szellemiségével ellentétben, hasson mind a 12 címkézésre *ugyanaz* a négy transzvektió. Az elhangzottak alapján  $\hat{T}_l$  felcseréli  $\varphi_1$ -et és  $\varphi_2$ -t. A többi címkézésekre az írható, hogy  $\hat{T}_l \varphi = \varphi \alpha_{12}$ , ahol  $\alpha_{12}$  egy pentagramma-automorfizmus, amely  $\varphi$ -nek a  $\varphi_1$ -el, illetve a  $\varphi_2$ -vel közös egyeneseit cseréli fel (vö: ekvivalens címkézések). (4.6) miatt a másik partícióban hasonló történik.

A konjugálás (4.3), (4.4) és (4.5) alapján a dupla hatos minden címkézésére ugyanaz a transzvektió. Ez a művelet a partíciókat cseréli fel.

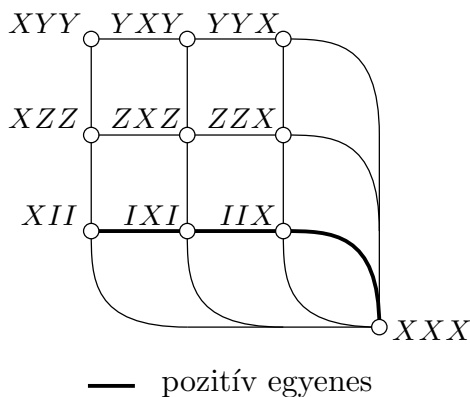
---

<sup>28</sup>Ez nem precíz, de szemléletes.



## 4.8. 9+1-es geometria $W(5, 2)$ -be képező címkézése

A 9+1-es konfigurációkhoz<sup>29</sup> az a kérdés vezetett, hogy egy kiszemelt operátor (vagy vektor), pl.  $XXX$ , egy adott dupla hatoson belüli címkézésekre, pl. a 4.14. ábrán lévőkre, milyen más operátorokkal együtt illeszkedik a pentagramma valamelyik egyenesével. Az  $XXX$ -et tartalmazó operátor-négyeseket külön választva, a 4.15. ábrán látható konfiguráció adódik. A geometriát jelölje  $\Gamma$ . A vastag görbével jelölt egyenes pozitív, így a WA-kritériumok teljesülnek.



4.15. ábra. 9+1-es Bell–KS-konfiguráció

Az eddigi geometriákhoz képest  $\Gamma$  kilóg a sorból, mivel nem reguláris, és a kitüntetett „10.” pontja minden egyenesével illeszkedik, továbbá vannak olyan egyenesei, amelyek két pontban metszik egymást.

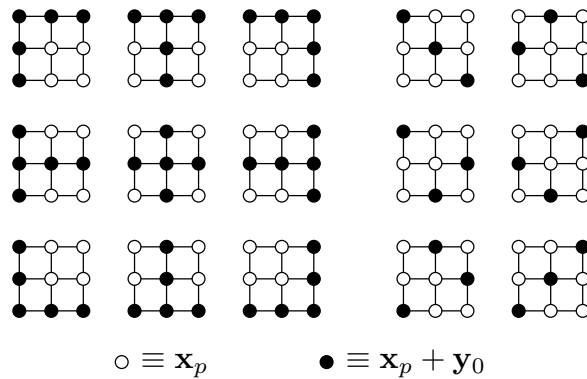
Utolsó nekifutásként  $\Gamma$ -nak a 4.15. ábrából általánosított címkézései lesznek megvizsgálva. Egy ilyen címkézés  $\Gamma$  egyeneseit  $W(5, 2)$  síkjaira, azaz  $GF(2)^6$  Lagrange-altereire képezi. Az érintett Lagrange-alterek  $Y$  metszete  $GF(2)^6$ -nak egydimenziós (izotróp) altere. Ennek a nemnulla vektora legyen  $\mathbf{y}_0$ .

A  $GF(2)/Y$  szimplektikus faktortér által indukált  $W_Y(3, 2)$  szimplektikus poláris tér pontjai  $\{C, Y\}$  alakúak, ahol  $C$  egy mellékszotály  $Y$ -nak valamely  $GF(2)^6$ -beli,  $Y$ -t tartalmazó, kétdimenziós altérben.  $C$  két darab nemnulla vektort tartalmaz, és ha az egyiket  $\mathbf{x}$  jelöli, a másik  $\mathbf{x} + \mathbf{y}_0$ .

$\Gamma$  nem kitüntetett pontjai a 6 egyenessel egy  $G$  grid-et indukálnak.  $W_Y(3, 2)$  a doily-val izomorf, és így 10 grid-et tartalmaz. Legyen ezek közül az egyik  $G_Y$ , és legyen egy izomorfizmus  $G$  és  $G_Y$  között. Ekkor  $G$  minden  $p$  pontjához hozzátartozik egy  $\{C_p, Y\}$  alakú  $G_Y$ -pont. A  $C_p$ -beli vektorok legyenek  $\mathbf{x}_p$  és  $\mathbf{x}_p + \mathbf{y}_0$ . Az  $\mathbf{x}_p$  vektorok megválaszthatók úgy, hogy  $G$  bármely  $l$  egyenesére  $\sum_{p \in l} \mathbf{x}_p$  eltűnjön (vö: Mermin–Peres-négyzet, 1.1. ábra).

<sup>29</sup>A névadó: Lévay Péter

Ezek után  $\Gamma$ -nak egy címkézése a következőképpen építhető fel. A generátorfüggvény rendelje a 10. ponthoz  $\mathbf{y}_0$ -t, a  $G$  grid  $p$  pontjaihoz pedig  $\mathbf{x}_p$ -t vagy  $\mathbf{x}_p + \mathbf{y}_0$ -t a 4.16. ábrán látható mintázatok szerint.



4.16. ábra. Mintázatok a címkézés konstrukciójához

A címkézések számának a becsléséhez fel kell használni, hogy  $\mathbf{y}_0$  63-féleképpen,  $G_Y$  10-féleképpen, a mintázat pedig 16-féleképpen választható. Ez összesen 10 080 nemekvivalens címkézés. Ugyanez az érték jön ki a (4.1) formula alapján is, viszont figyelembe kell venni, hogy a címkézések stabilizátora most nem triviális, hanem két szimplektikus mátrixot tartalmaz.

Számítógép segítségével azt kaptam, hogy  $\Gamma$  összes nemekvivalens címkézése Bell–KS-konfigurációt határoz meg. Pontosabban, az 1, 3, illetve 5 negatív egyenest eredményező címkézések száma 5 184, 4 464, illetve 432.

## Hivatkozások

- [1] Stephen L. Adler. *Quaternionic Quantum Mechanics and Quantum Fields*. The International Series of Monographs on Physics. Oxford University Press, 1995.
- [2] Rényi Alfréd. *Valószínűségszámítás*. Budapest: Tankönyvkiadó, 1954.
- [3] John S. Bell. “On The Einstein Podolsky Rosen Paradox”. In: *Physics* 1 (1964), pp. 195–200.
- [4] John S. Bell. “On the Problem of Hidden Variables in Quantum Mechanics”. In: *Reviews of Modern Physics* 38 (3 1966), pp. 447–452. DOI: 10.1103/RevModPhys.38.447. URL: <http://link.aps.org/doi/10.1103/RevModPhys.38.447>.
- [5] Niels Bohr. “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” In: *Physical Review* 48 (1935), pp. 696–702.
- [6] 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>.
- [7] Yaim Cooper. *Generators of the Symplectic Group*. 2005. URL: <http://www-math.mit.edu/~dav/sympgen.pdf>.
- [8] Reinhard Diestel. *Graph Theory*. Vol. 173. Graduate Texts in Mathematics. Springer-Verlag, 2005. URL: <http://diestel-graph-theory.com/>.
- [9] Albert Einstein, Boris Podolsky, and Nathan Rosen. “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” In: *Physical Review* 47 (1935), pp. 777–780.
- [10] Simon Kochen and E. P. Specker. “The Problem of Hidden Variables in Quantum Mechanics”. In: *Journal of Mathematics and Mechanics* 17 (1967), pp. 59–87.
- [11] Konrad Lorenz. *Die Rückseite des Spiegels*. (Magyar változat: Konrad Lorenz. A tükör hátoldala. Cartafilus Kiadó, Budapest 2000). München: R. Piper GmbH & Co. KG., 1973.
- [12] 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>.
- [13] Hendrik Van Maldeghem. *Generalized Polygons*. Modern Birkhäuser Classics. Birkhäuser, 1998.



- [14] Eckhard Meinrenken. *Symplectic Geometry*. 2000. URL: <http://www.math.toronto.edu/mein/teaching/symp1.pdf>.
- [15] 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>.
- [16] N. David Mermin. “Simple unified form for the major no-hidden-variables theorems”. In: *Physical Review Letters* 65 (27 1990), pp. 3373–3376. DOI: 10.1103/PhysRevLett.65.3373. URL: <http://link.aps.org/doi/10.1103/PhysRevLett.65.3373>.
- [17] Asher Peres. *Einstein, Podolsky, Rosen and Shannon*. 2003. URL: [arXiv: quant-ph/0310010](http://arxiv.org/abs/quant-ph/0310010).
- [18] Asher Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 2002.
- [19] Tomaz Pisanski and Brigitte Servatius. *Configurations from a Graphical Viewpoint*. Birkhäuser, 2013.
- [20] Michel Planat, Metod Saniga, and Frédéric Holweck. “Distinguished three-qubit ‘magicity’ via automorphisms of the split Cayley hexagon”. In: *Quantum Information Processing* Vol. 12 (7 2013), pp. 2535–2549. URL: <http://arxiv.org/abs/1212.2729v1>.
- [21] Burkard Polster. *A Geometrical Picture Book*. Springer, 1998.
- [22] Burkard Polster, Andreas E. Schroth, and Hendrik Van Maldeghem. “Generalized flatland.” eng. In: *MATHEMATICAL INTELLIGENCER* 23.4 (2001), pp. 33–47. ISSN: 0343-6993.
- [23] Lévy Péter. *Black Hole Entropy and Finite Geometry*. 2015. URL: [http://www.iip.ufrn.br/media/pdf/tfbhc\\_PeterLevy\\_06\\_2015\\_01.pdf](http://www.iip.ufrn.br/media/pdf/tfbhc_PeterLevy_06_2015_01.pdf).
- [24] Lévy Péter, Metod Saniga, and Peter Vrana. “Three-Qubit Operators, the Split Cayley Hexagon of Order Two and Black Holes”. In: *Physical Review D* Vol. 78, Iss. 12, 124022 (2008). URL: <http://arxiv.org/abs/0808.3849v2>.
- [25] Metod Saniga and Michel Planat. *Multiple Qubits as Symplectic Polar Spaces of Order Two*. 2006. URL: <http://arxiv.org/abs/quant-ph/0612179v1>.
- [26] Metod Saniga et al. “‘Magic’ Configurations of Three-Qubit Observables and Geometric Hyperplanes of the Smallest Split Cayley Hexagon”. In: *Symmetry, Integrability and Geometry: Methods and Applications (SIGMA)* 8 (2012) (2012), Article 83. URL: <http://arxiv.org/pdf/1206.3436v2.pdf>.

- [27] Mordecai Waegell and P. K. Aravind. “Proofs of the Kochen–Specker theorem based on a system of three qubits”. In: *Journal of Physics A: Mathematical and Theoretical* 45.40 (2012). URL: <http://arxiv.org/pdf/1205.5015.pdf>.