Latvijas Universitāte
Datorikas fakultāte

Kvantu dizaini: MUB un SIC-POVM

Maģistra darbs

Autors:
Aleksandrs Belovs
St. apl. nr.: DatZ020006

Vadītājs:
Juris Smotrovs
as. prof., Dr.dat.

Rīga, 2009

Anotācija

Kvantu dizaini ir simetriskas vektoru konfigurācijas daudzdimensiju telpā. Pazīstamākie no tiem ir MUBu pilnas sistēmas un SIC-POVMi. Tie tiek pielietoti kvantu stāvokļu mērīšanā (kvantu tomogrāfijā), kvantu kriptogrāfijā un citās jomās. Šie objekti veido tā saucamos kompleksos projektīvos 2-dizainus, tas ir, sasniedz vienādību Velča nevienādībā priekš k=2. To izmantojot, mēs izvedam nepieciešamu un pietiekamu nosacījumu, lai vektoru sistēma veidotu MUBu pilno sistēmu vai SIC-POVMu. Šis nosacījums der arī citiem kvantu dizainiem.

Atšķirībā no iepriekšējiem kritērijiem, mūsu kritērijs izmanto tikai vektoru ortogonalitāti. Mēs ievedam homogēnas sistēmas: vektoru sistēmas, kurām šis nosacījums pieņem ļoti vienkāršu formu. Mēs parādām, ka visas zināmās MUBu pilnās sistēmas un visi zināmie SIC-POVMi ir homogēnu sistēmu speciālgadījumi, kas varētu atvieglot šo objektu konstruēšanu.

Atslēgvārdi: Kompleksi projektīvi t-dizaini, Velča nevienādība, relatīvas starpību kopas, planāras funkcijas, kvantu tomogrāfija.

Abstract

We investigate complete systems of MUBs and SIC-POVMs in this thesis. These are highly symmetric sets of vectors in Hilbert space, interesting because of their applications in quantum information science and other areas. It is known that these objects form complex projective 2-designs, that is, they satisfy Welch bounds for $k = 2$ with equality. We derive a necessary and sufficient condition for a set of vectors to satisfy Welch bounds with equality. This condition uses the orthonormality of a specific set of vectors. In particular it gives a condition for a set of vectors to be a complete system of MUBs or a SIC-POVM.

We define *homogeneous systems*, as a special case of systems of vectors for which the condition takes an especially elegant form. It is notable that all known constructions of SIC-POVMs and complete systems of MUBs belong to this special case. We demonstrate this and show some new results following from this construction.

Key words: Complex projective t-designs, Welch bounds, relative difference sets, planar functions, quantum tomography.

Autoreferāts

Darbā tika izstrādāts kritērijs, kad vektoru sistēma sasniedz vienādību Velča nevienādībā. Šis kritērijs tika pielietots MUBiem un SIC-POVMiem, kuri, kā jau bija zināms, sasniedz vienādību pieminētajā nevienādībā. Balstoties uz šo kritēriju, tika ieviestas homogēnas sistēmas, kas ir MUBu un SIC-POVMu speciāls gadījums. Šis kritērijs palīdzēja iegūt alternatīvus pierādījumus jau zināmām MUBu un SIC-POVMu konstrukcijām, kā arī atrast elegantāku izskatu dažām no tām. Tika iezīmēti daži speciālie gadījumi, kuriem šie objekti pagaidām gandrīz nav pētīti, tātad ir cerības, ka ar mūsu kritērija palīdzību var no tiem iegūt jaunas, līdz šim nezināmas konstrukcijas.

Ja nav pateikts citādi tekstā, rezultāti no nodaļām 1—4 ir jau zināmi, rezultāti no nodaļām 5—7 ir jauni, maģistra darba autora izstrādāti. Dažviet jau zināmiem rezultātiem ir doti citi pierādījumi. Visvairāk tas attiecas uz sadaļām 3.2 un 7.2.3.

Saturs

Ievads

Kvantu mērījumi ir svarīga jebkura kvantu informācijas teorijas uzdevuma sastāvdaļa, jo, tikai, izmantojot mērījumus, ir iespējams iegūt informāciju par kvantu sistēmu, kuru pēc tam var interpretēt cilvēks. Daudzi kvantu informācijas teorijas protokoli un algoritmi izmanto tādas kvantu stāvokļa transformācijas, ka tikai viens speciāli izvēlēts mērījums dod daudz informācijas par risināmo uzdevumu. Atšķirībā no tādiem algoritmiem, kvantu stāvokļu tomogrāfija izmanto mērījumus vispārīgākos pieņēmumos — kad nekas vai gandrīz nekas par stāvokli netiek pieņemts. Speciāls gadījums šim ir kvantu sistēmu testēšana: vai stāvoklis, ko izdod sistēma, tiešām ir tāds, kādam tam ir jābūt. Šajā darbā mēs aplūkosim divus no šī viedokļa interesantus objektus: pilnās savstarpēji nenosliektu bāžu sistēmas (MUBus) un simetriskus informacionāli pilnus POVMus (SIC-POVMus).

Pilnās MUBu sistēmas unitārajā telpā $\mathbb{C}^n$ ir tāda $n+1$ ortonormētu bāžu sistēma, ka jebkuriem diviem vektoriem no dažādām bāzēm skalārais reizinājums pēc moduļa ir vienāds ar $\frac{1}{\sqrt{n}}$. SIC-POVMs telpā $\mathbb{C}^n$ ir tāda n^2 normētu vektoru kopa, ka jebkuriem diviem dažādiem vektoriem skalārais reizinājums pēc moduļa ir $\frac{1}{\sqrt{n+1}}$. Šie divi objekti dod labākos iespējamos mērījumus attiecīgajām mērījumu klasēm (atbilstoši projektīvajiem mērījumiem un POVMiem). MUBu pilnās sistēmas eksistē visās pirmskaitļu pakāpju dimensijās [74], un tiek uzskatīts, ka tie neeksistē citās dimensijās. SIC-POVMi ir skaitliski (aptuveni) konstruēti visās dimensijās līdz 67 [66] un dažas analītiskas (precīzas) konstrukcijas ir zināmas mazās dimensijās. Vispārpieņemta hipotēze ir, ka tie eksistē visās dimensijās. Neskatoties, ka daudzi darbi tika veltīti šai tematikai, abas šīs problēmas joprojām paliek atklātas.

Abas šīs konfigurācijas (MUBi un SIC-POVMi) veido tā saucamos kompleksos projektīvos 2-dizainus [47]. Tās ir vektoru kopas, kuras apmierina Velča nevienādību priekš $k = 2$ ar vienādību. Šajā darbā mēs formulējam nepieciešamo un pietiekamo nosacījumu, kad vektoru sistēma veido kompleksu projektīvu 2-dizainu. Šis nosacījums izmanto no-

teiktas vektoru sistēmas ortonormalitāti. Tas, pirmkārt, dod nepieciešamos nosacījumus dizaina vektoru komponenšu absolūtām vērtībām, kuras nav atkarīgas no fāzēm. Absolūto vērtību meklēšanu var uztvert kā uzdevumu reālajā vektoru telpā. Otrkārt, tas aizstāj neintuitīvo nosacījumu skalārajam reizinājumam pēc absolūtas vērtības būt vienādam ar $\frac{1}{\sqrt{n}}$ vai $\frac{1}{\sqrt{n+1}}$ ar nosacījumu uz vektoru ortogonalitāti, kas ir daudz skaidrākā vektoru attiecība.

Mēs definējam speciālu MUBu pilno sistēmu un SIC-POVMu gadījumu, ko mēs saucam par *homogēnām sistēmām.* Tas ir unificēts piegājiens gan MUBiem, gan SIC-POVMiem. Visas zināmās MUBu pilnās sistēmas un grupu kovariantie SIC-POVMi (SIC-POVMu speciāls gadījums, kas definēts darbos [76, 58]) ir šīs konstrukcijas speciāli gadījumi. Iemesls, kāpēc mēs definējam šo konstrukciju, ir tāds, ka jau pieminētajam kritērijam šajā gadījumā ir ļoti eleganta forma. Mēs demonstrējam piemēru, kad homogēna konstrukcija dod elegantāku SIC-POVMu nekā tie, kas jau bija zināmi. Šīs piegājiens arī izskaidro, kāpēc Furjē matricas ir tik ļoti noderīgas, konstruējot MUBus un SIC-POVMus.

Daļa no šī darba jau iepriekš ir tikusi publicēta darbos [9] un [10].

Darbs ir organizēts sekojoši. Dažas pirmās nodaļas ir ievadnodaļas. Pirmajā nodaļā mēs definējam dažus tehniskus jēdzienus, kurus mēs izmantosim tālāk darbā: kvantu stāvokļus un mērījumus, galīgas Ābela grupas raksturus, Furjē matricas, vispārināto Pauli grupu un Kliforda grupu. Otrajā nodaļā mēs definējām galvenos objektus, ar kuriem mēs taisāmies strādāt, — MUBus un SIC-POVMus, dodam dažus zināmus rezultātus, kā arī dažas hipotēzes. Trešajā nodaļā mēs iepazīstinām ar virknēm ar zemu savstarpēju korelāciju un parādām, ka tās ir līdzīgas otrajā nodaļā aplūkotajiem objektiem. Galvenais tehniskais līdzeklis, kuru mēs iegūstam no šīs iepazīšanas, ir Velča nevienādība — nevienādība, kas saista vektoru skaitu sistēmā ar to savstarpējām korelācijām. Izrādās, ka gan MUBi, gan SIC-POVMi apmierina Velča nevienādību priekš $k = 2$ ar vienādību. Ceturtajā nodaļā mēs parādām, ka tas nozīmē, ka tie ir kompleksie projektīvie 2-dizaini, kā arī iepazīstinām ar vispārīgāku dizaina jēdzienu.

Piektajā nodaļā mēs definējam mūsu kritēriju vienādības sasniegšanai Velča nevienādībā un pielietojam to MUBiem un SIC-POVMiem. Sadaļā 5.3. mēs ieviešam homogēnas sistēmas kā MUBu un SIC-POVMu speciālgadījumu. Lai uzdotu homogēnu MUBu pilno sistēmu vai SIC-POVMu telpā $\mathbb{C}^n$, pietiek definēt divas $n \times n$ matricas. Salīdzinājumam, lai uzdotu vispārīgu MUBu pilno sistēmu vai SIC-POVMu, vajadzīgi ar kārtu n^3 elementi. Izņemot matricu elementu absolūtās vērtības, mūs interesē tikai viena matricas funkcija — tas, ko mēs saucam par matricas L-grafu. Tas ir vienkāršs grafs, kura virsotnes

ir matricu rindiņu nesakārtoti pāri un divas virsotnes ir savienotas tad un tikai tad, ja pirmā pāra Adamāra reizinājums ir ortogonāls otrā pāra Adamāra reizinājumam. Rupji runājot, jo vairāk ir šķautņu L-grafā, jo labāk.

Sestajā nodaļā mēs pētām, kādas var būt absolūtās vērtības homogēnam SIC-POVMam. Mēs pierādām, ka tās var aprakstīt ar regulāru simpleksu, kas ir ievietots lielākā fiksētā simpleksā. Mēs arī pētām cirkulārus simpleksus, t.i., tādus, ka cirkulāra koordinātu maiņa neizmaina simpleksu. Tādi simpleksi rodas, aplūkojot, piemēram, grupu kovariantus SIC-POVMus, bet mēs parādām 7. nodaļā, ka arī vispārīgāks konteksts ir interesants.

Sadaļā 7.2 mēs aprakstām zināmās MUBu pilnās sistēmas, izmantojot mūsu kritēriju un parādām, ka no tā seko nesen iegūtie rezultāti par MUBu un dažu kombinatorisku objektu (tādu kā perfekti nelineāras funkcijas un relatīvas starpību kopas) saikni. Viena no mūsu pieejas īpatnībām ir tāda, ka mēs definējam Ābela grupas rakstura vērtības uz "neveseliem" elementiem. Piemēram, tas dod alternatīvu aprakstu relatīvām starpību kopām, kuras nav sadalāmas. Sadaļā 7.3 mēs aplūkojām SIC-POVMus dimensijā 2^k.

1. nodaļa

Pamatjēdzieni

1.1. Kvantu stāvokļu tomogrāfija

Šajā sadaļā mēs definēsim kvantu informācijas teorijas jēdzienus, kurus izmantosīm tālāk tekstā. Īpaša uzmanība tiks vēltīta kvantu mērījumiem kā kvantu tomogrāfijas pamatjēdzienam. Izklāstā visvairāk tiek izmantoti [42] un [53].

1.1.1. Statistiskā modeļa vispārīgs jēdziens

Kādas reālas parādības teorētiskais modelis, galu galā, ir balstīts uz eksperimentu datiem, kas veikti, pētot šo objektu. Jebkurā eksperimentā var izdalīt divas fāzes. Pirmajā, *sagatavošanas fāzē*, noteikta eksperimentāla situācija tiek izveidota. Nākamajā, *mērījuma fāzē*, eksperimentāla sistēma, sagatavota iepriekšējā solī, mijiedarbojas ar *mērījuma iekārtu*, kas izdod *mērījuma rezultātus*.

Katram zinātniskam eksperimentam ir jāapmierina tā saucamais *atkārtojamības nosacījums*. Tas ir, jābūt iespējamam atkārtot to pašu eksperimentu tajā pašā situācijā tik daudz reizes, cik nepieciešams. Kaut gan sistēma katru reizi tiek sagatavota identiskā veidā, mērījuma rezultāti parasti atšķirsies. Gandrīz vienmēr eksperimenta datos būs vērojamas fluktuācijas, un šo fluktuāciju amplitūda ir atkarīga no eksperimenta.

Daudzos fizikālos procesos fluktuācija ir tik maza, ka to var ignorēt. Piemēram, lielo objektu mehāniskai kustībai vai procesiem elektriskās ķēdēs piemīt tāda īpašība. Tādus procesus sauc par *determinististiskiem*, un atbilstošās fizikas nozares pieņem ka, vismaz teorētiski, var izdarīt perfektu mērījumu. Un tiešām, skrupulozi izdarīts mērījums parasti samazina fluktuācijas.

Bet eksistē tādi fizikāli procesi, kuros fluktuācijas paliek lielas, neatkarīgi no tā, cik pedantiski ir veikts mērījums. Tad tiek pieņemts, ka fluktuācijas ir ne no mērījuma iekārtu nepilnības, bet tāpēc, ka tie piemīt pašam pētāmajam objektam. Kā piemēru var minēt daļiņu izkliedes un kvantu mehāniskos procesus.

Kaut gan mērījumu rezultātu fluktuācijas tādos procesos nevar ignorēt, tiek pieņemts sekojošais *statistiskais postulāts*: mērījumu rezultāti, izdarot eksperimentu vairākas reizes, var būt dažādi, bet katra noteiktā mērījuma rezultāta iznākums pietiekoši ilgā eksperimentu virknē var tikt aprakstīts ar kaut kādu statistisku biežumu. No šī viedokļa, eksperimenta rezultāts (ar ko saprot vairāku identiski sagatavotu eksperimentu virkni, nevis vienu eksperimentu) var tikt teorētiski aprakstīts ar kaut kādu *varbūtību sadalījumu*.

Varbūtību sadalījums ir pāris $(\mathcal{X}, p)$, kur $\mathcal{X}$ ir kopa, saukta par *iznākumu telpu* un p ir funkcija, no $\mathcal{X}$ nenegatīvo reālo skaitļu kopā. Iepriekšējā paragrāfa kontekstā, $\mathcal{X}$ ir iespējamo mērījumu rezultātu kopa un p ir atbilstošais biežums. Šajā darbā mēs darbosimies tikai ar galīgām fāžu telpām, tāpēc pieņemsim, ka kopa $\mathcal{X}$ ir galīga. Šajā gadījumā funkcijai p jāapmierina nosacījums $\sum_{x\in\mathcal{X}} p_x = 1$.

Eksperimentāla sistēma pēc sagatavošanas fāzes ir aprakstāma ar kaut kādu stāvokli S. Mērījums M attēlo stāvokli S uz kaut kādu varbūtību sadalījumu μ_S^M. Iznākumu telpas visiem μ_S^M, kur M ir fiksēts un S mainās, ir vienādas. Ir iespējams veikt dažādus mērījumus uz vienas un tas pašas sistēmas, kuras attēlo stāvokli dažādos varbūtības sadalījumos, iespējams, ar dažādām iznākumu telpām. Ja stāvokļi S un S' ir tādi, ka visiem mērījumiem M attiecīgie varbūtību sadalījumi μ_S^M un $\mu_{S'}^M$ ir vienādi, tad šie divi stāvokļi ir neatšķirami, un parasti tas ir viens un tas pats stāvoklis.

Pieņemsim, ka mēs varam sagatavot stāvokļus S_α visiem $\alpha \in \mathcal{X}$, kur $\mathcal{X}$ ir iznākumu telpa kaut kādam varbūtību sadalījumam $(\mathcal{X}, p)$. Aplūkosim eksperimentu, kurā no sākuma nejauši tiek izvēlēts $\alpha \in \mathcal{X}$ saskaņā ar varbūtību sadalījumu $(\mathcal{X}, p)$, un tad sistēma tiek sagatavota stāvoklī S_α. Tādējādi sagatavotas sistēmas stāvokli sauc par stāvokļu S_α *maisījumu* atbilstoši varbūtību sadalījumam $(\mathcal{X}, p)$. Pieņemsim, ka M ir tāds mērījums, kas prot izmērīt visus stāvokļus S_α. Ir skaidrs, ka, neatkarīgi no mērījuma M izvēles, varbūtību sadalījumam μ_S^M jāapmierina

$$\mu_S^M(x) = \sum_{\alpha\in\mathcal{X}} p_\alpha \mu_{S_\alpha}^M(x)$$

visiem x no M iznākumu telpas. Izrādās, ka var identificēt sistēmas stāvokļus ar reālo vektoru telpas izliektas apakškopas punktiem tā, ka stāvokļu S_α maisījumu atbilstoši varbūtību sadalījumam $(\mathcal{X}, p)$ dod $\sum_{\alpha\in\mathcal{X}} p_\alpha S_\alpha$.

1.1.2. Kvantu stāvokļi un mērījumi

Pievērsīsimies tagad kvantu mērījumiem. No sākuma aprakstīsim, kā tiek uzdoti kvantu stāvokļi.

Apzīmēsim ar $\mathcal{H}$ galīgas dimensijas unitāru telpu. Mēs pieņemsim, ka tās elementi ir uzdoti kā vektori-stabiņi

$$\psi = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix},$$

ja $\mathcal{H}$ ir n-dimensionāla. Ja A ir patvaļīga kompleksa matrica, tad ar $\overline{A}$, A^T, A^* mēs apzīmēsim, atbilstoši, kompleksi saistīto, transponēto un saistīto matricu, t.i., $A^* = \overline{A^T}$. Skalāro reizinājumu telpā $\mathcal{H}$ mēs apzīmēsim ar

$$\langle \psi, \varphi \rangle = \psi^* \varphi = \sum_{i=1}^{n} \overline{\psi_i} \varphi_i.$$

Kvantu stāvokļi tiek uzdoti ar tā saucamām *blīvuma matricām*, t.i. ar operatoriem ρ, kas darbojās telpā $\mathcal{H}$ un apmierina $\rho \geq 0$ (ρ ir nenegatīvi definēta) un $\operatorname{Tr} \rho = 1$. Atgādināsim, ka matricu ρ sauc par *nenegatīvi definētu*, ja tā ir *Ermita* (**Hermite**), t.i., $\rho^* = \rho$, un visas ρ īpašvērtības ir nenegatīvi reāli skaitļi. Apzīmēsim ar $\mathcal{S}(\mathcal{H})$ visu blīvuma matricu kopu virs $\mathcal{H}$. Viegli redzēt, ka tā ir izliekta kopa: visiem $\rho_1, \rho_2 \in \mathcal{H}$ un visiem $0 \leq p \leq 1$ izpildās $p\rho_1 + (1-p)\rho_2 \in \mathcal{S}(\mathcal{H})$. Blīvuma matrica $p\rho_1 + (1-p)\rho_2$ atbilst maisījumam no sistēmām, sagatavotām stāvokļos ρ_1 un ρ_2 proporcijās p un $1-p$, atbilstoši.

Izliektās kopās ekstremāliem punktiem ir īpaša nozīme. Izliektas kopas *ekstremālais punkts* ir tāds punkts, kas nevar tikt izteikts kā divu dažādu šīs kopas punktu izliekta kombinācija. Kopā $\mathcal{S}(\mathcal{H})$ ekstremālie punkti ir tā saucamie *tīrie stāvokļi* (**pure state**). Tie ir viendimensionālie projektori $\rho_\psi = \psi\psi^*$, kur $\psi \in \mathcal{H}$. Tīrus stāvokļus mēdz uzdod, uzrādot tikai vektoru ψ. Šeit rodas neviennozīmība, jo vienu un to pašu tīro stāvokli $\psi\psi^*$ var uzdod ar jebkuru vektoru formā $\alpha\psi$, kur $\alpha \in \mathbb{C}$ un $|\alpha| = 1$. Visus šos stāvokļus pieņem par ekvivalentiem, un izsaka to tādā veidā, ka globāla fāze α kvantu mehānikā nav svārīga.

Stāvokļus, kuri nav tīrie, sauc par *jauktiem* (**mixed state**). Operatoru *spektrālais sadalījums*

$$\rho = \sum_i \lambda_i x_i x_i^*, \quad \lambda_i \geq 0, \quad \sum_i \lambda_i = 1,$$

kur λ_i ir ρ īpašvērtības un x_i ir atbilstoši īpašvektori, parāda, ka jebkurš jauktais stāvoklis var tikt izteikts kā ne vairāk kā $\dim \mathcal{H}$ tīru stāvokļu izliekta kombinācija.

Ja kvantu stāvoklis neiedarbojās ar ārpasauli, tad to evolūciju laikā var aprakstīt kā konjugāciju ar kaut kādu unitāru operatoru U, t.i., pielietojot izolētai kvantu sistēmai kaut kādu transformāciju, tās stāvoklis mainās kā $\rho \mapsto U\rho U^*$, kur U nav atkarīga no stāvokļa ρ. Ja ψ ir tīrais stāvoklis, tad tā evolūciju var uzdod ar $\psi \mapsto U\psi$.

Atgriezīsimies tagad pie mērījuma operatora. Tas transformē kvantu stāvokli $\rho \in \mathcal{S}(\mathcal{H})$ varbūtību sadalījumā $\mu_\rho^M(x)$ virs kaut kādas fāžu telpas $\mathcal{X}$. Kā tika minēts iepriekšējā sadaļā, katrs mērījums attēlo kvantu stāvokļu maisījumu attiecīgajā varbūtību sadalījumu maisījumā. Citiem vārdiem, μ_S^M, kā funkcijai no S, jābūt afīnai. Ar šo nosacījumu pietiek, lai pilnībā aprakstītu kvantu mērījuma operatorus.

Teorēma 1.1. *Pieņemsim, ka $\rho \mapsto \mu_\rho$ ir attēlojums no kvantu stāvokļu telpas $\mathcal{S}(\mathcal{H})$ varbūtību sadalījumos virs galīgas iznākumu telpas $\mathcal{X}$. Ja šīs attēlojums ir afīns, tad eksistē tādi Ermita operatori $\{M_x\}$ virs $\mathcal{H}$, ka*

$$M_x \geq 0, \quad \sum_{x \in \mathcal{X}} M_x = I \quad \textit{and} \quad \mu_\rho(x) = \mathrm{Tr}(\rho M_x).$$

Operatoru saime $\{M_x\}$ tiek saukta par *POVMu*, kas ir saīsinājums no angļu valodas 'Positive Operator-Valued Measure"; operatori M_x tiek saukti par *POVMa elementiem.*

Daudzas kvantu mehānikas klasiskas grāmatas nedefinē kvantu mērījumus tik vispārīgi, ierobežojoties ar *fon Neimana* (**von Neumann**), jeb *projektīviem* mērījumiem. POVMu $\{M_x\}$ sauc par projektīvu, ja tas sastāv no projektoriem, t.i., $M_x^2 = M_x$ visiem x, un tie ir savstarpēji ortogonāli: $M_x M_y = 0$ visiem $x \neq y$. Patiesībā, kā viegli pārbaudīt, katrs no šiem diviem nosacījumiem implicē otro.

Iemesls, kāpēc daudzi fiziķi neizmanto POVM formālismu, ir tāds, ka daudzas fizikālas sistēmas var tikt izmērītas tikai ļoti ierobežotos veidos, un ar projektīviem mērījumiem pietiek, lai pilnībā aprakstītu visus interesantos mērījumus, kas var tikt reāli izpildīti. No šī viedokļa, projektīvie mērījumi ir piemērotāki praktiskai realizācijai nekā POVMi. Turklāt jebkuru POVMu var implementēt, izmantojot projektīvus mērījumus, kā tas izriet no sekojošās Naimarka (**Наймарк**) teorēmas:

Teorēma 1.2. *Pieņemsim, ka $\{M_x\}_{x \in \mathcal{X}}$ ir POVMs unitārajā telpā $\mathcal{H}$,* $\dim \mathcal{H} = n$ *un* $|\mathcal{X}| = m$. *Tad eksistē unitārā telpa $\tilde{\mathcal{H}}$,* $\dim \tilde{\mathcal{H}} \leq nm$, *izometrija $V : \mathcal{H} \to \tilde{\mathcal{H}}$, un projektīvais mērījums $\{E_x\}$, tādi, ka*

$$M_x = V^* E_x V.$$

Citiem vārdiem, telpu $\mathcal{H}$ var iztēloties ielīktu lielākā telpā $\tilde{\mathcal{H}}$, un tas, kas izskatās kā POVMs telpā $\mathcal{H}$, patiesībā ir projektīvais mērījums telpā $\tilde{\mathcal{H}}$.

Daudzi kvantu skaitļošanas uzdevumi ir balstīti uz tāda stāvokļa sagatavošanu, ka pat viens vienīgs mērījums var dot daudz informācijas par atrisināmo problēmu. Bet dažos gadījumos maz, vai vispār nekas nav zināms par izmērāmo sistēmu. Šajā gadījuma sagatavo daudzas stāvokļa kopijas (izmantojot atkārtojamības postulāti) un tad mērā tos. Mērījumu sistēma $\{M_i\}$ tiek saukta par *informacionāli pilnu* (**informationally complete**) [57], ja stāvokli $\rho \in \mathcal{S}(\mathcal{H})$ var viennozīmīgi noteikt no $\mu_\rho^{M_i}$. Ja informacionāli pilna mērījumu sistēma tiek pielietota kvantu stāvoklim, tad no to statistikām var tuvināti dabūt stāvokli. Šo procesu sauc par *kvantu stāvokļa tomogrāfiju* (**quantum state tomography**).

Atzīmēsim, ka nav iespējams noteikt stāvokli precīzi, jo nav iespējams dabūt precīzas vērtības varbūtībām, izdarot tikai galīgu mērījumu skaitu. Kvantu tomogrāfijas galvenais mērķis ir novērst šo neprecizitāti līdz minimumam, izmantojot labākus mērījumus.

Pastāv divas kvantu tomogrāfijas paradigmas. Oriģinālajā paradigmā mērījumi var būt dažādi, un katrs no tiem ir projektīvs. Otrais piegājiens ir izmantot vienu un to pašu (neprojektīvu) mērījumu atkārtoti. Tādus mērījumus sauc par *IC-POVMiem*, kas atbilst "informacionāli pilniem POVMiem". Nākamajās nodaļās mēs dosim piemērus abām paradigmām: tie būs MUBu pilnās sistēmas un SIC-POVMi.

1.2. Furjē matricas

Par Furjē (**Fourier**) matricu sauc matricu, kas izdara galīgas Ābela (**Abel**) grupas Furjē transformāciju. Furjē transformācija tiek pielietota daudzās matemātikas, fizikas un informātikas nodaļās. Piemēram, Šora (**Shor**) kvantu algoritmi skaitļu sadalīšanai reizinātājos un diskrētā logaritma atrašanai izmanto Furjē transformāciju kā galveno soli [69]. Šajā darbā mūs vairāk interesēs dažas specifiskas Furjē matricu īpašības.

Paņemsim Ābela grupu

$$G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m} \tag{1.1}$$

ar kārtu $n = d_1 d_2 \cdots d_m$. Šeit ar $\mathbb{Z}_n$ tiek saprasta veselo skaitļu grupa pēc moduļa n: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Pēc Ābela grupu struktūru teorēmas jebkuru Ābela grupu var izteikt tādā formā (skat., piemēram, [39]). Mēs lietosim apzīmējumu G^* grupas G nenulles elementu kopai.

Furjē transformāciju definē, izmantojot *duālo grupu*. Ābela grupas G duālā grupa $\hat{G}$ sastāv no visiem grupas G raksturiem. Ābela grupas *raksturs* (**character**) ir tās morfisms multiplikatīvajā grupā, kas sastāv no visiem kompleksiem skaitļiem ar absolūto vērtību 1, t.i., raksturam χ jāapmierina nosacījums $\chi(a+b) = \chi(a)\chi(b)$, ja grupa ir aditīva. Duālas grupas operācija ir raksturu reizinājums kā funkciju ar kompleksām vērtībām, t.i., $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$, kur χ_1 un χ_2 ir divi grupas raksturi un a ir patvaļīgs grupas elements. Pastāv izomorfisms starp grupām G un $\hat{G}$, kas tiek uzdots ar

$$\chi_a(b) = \exp\left(\sum_{j=1}^{m} \frac{2\pi\mathbf{i}}{d_j} a_j b_j\right), \tag{1.2}$$

kur $a = (a_1, a_2, \ldots, a_m)$ un $b = (b_1, b_2, \ldots, b_m)$ ir grupas G elementi, χ_a ir grupas $\hat{G}$ elements, kas atbilst elementam a šajā izomorfismā, un $\mathbf{i} = \sqrt{-1}$. Atzīmēsim, ka izteiksme $\chi_a(b)$ ir simetriska pret a un b apmainīšanu vietām.

Sekojošā lemma ir labi zināms rezultāts. Tā ir vispārīgākas Lemmas 7.2, kuru mēs pierādīsim Nodaļā 7., speciālgadījums.

Lemma 1.3. *Pieņemsim, ka x ir kopas G elements. Tad $\sum_{y\in G} \chi_y(x) = 0$ tajā un tikai tajā gadījumā, ja $x \in G^*$.*

Matricu ar vienāda moduļa kompleksiem elementiem sauc par *plakanu* (**flat**) matricu. Ja tā ir turklāt unitāra (ar precizitāti līdz reizināšanai ar skalāri), tad to sauc par *kompleksu Adamāra matricu* (**complex Hadamard matrix**). Ir pieņemts normalizēt plakanas matricas tā, ka katrs to elements pēc moduļa ir vienāds ar 1. Mēs to parasti pieņemsim. Kompleksas Adamāra $n \times n$-matricas gadījumā dažreiz ir izdevīgāk pieņemt, ka katra elementa absolūtā vērtība ir $\frac{1}{\sqrt{n}}$ (tad tā ir unitāra), dažreiz: 1. Atbilstoši situācijai mēs pieņemsim vienu vai otru, no konteksta būs skaidrs, kuru.

Kompleksā Adamāra matrica ir klasiskās Adamāra matricas vispārinājums. Klasiskā Adamāra matrica apmierina tos pašus nosacījumus, bet ar visiem elementiem reāliem (t.i., vienādiem ar ± 1, sk., piemēram, [11] Nodaļa I.9). Tālāk darbā mēs lietosim terminu Adamāra matrica lai apzīmētu kompleksas Adamāra matricas. Klasiskajām Adamāra matricām mēs lietosim nosaukumu "reāla Adamāra matrica".

Divas Adamāra matricas sauc par *ekvivalentām*, ja vienu var dabūt no otras, pareizinot rindiņas un kolonnas ar skalāriem un pārkārtojot tās. Dažas Adamāra matricu ekvivalences klases ir klasificētas [71]. Bet jau dimensijā 6 tas nav līdz galam klasificētas [12].

Tagad mēs esam devuši visas svarīgās definīcijas un varam noformulēt sekojošu svarīgu Lemmas 1.3 secinājumu:

Secinājums 1.4. *Matrica $F = (f_{i,j})$, kas ir indeksēta ar grupas G elementiem, un tāda, ka $f_{i,j} = \chi_j(i)$, ir Adamāra.*

Pierādījums. Acīmredzot, visiem matricas elementiem absolūtā vērtība ir 1. Skalārais reizinājums divām rindām ar indeksiem a un b ir

$$\sum_{y \in G} \overline{\chi_y(a)} \chi_y(b) = \sum_{y \in G} \chi_y(b-a) = 0,$$

ja $a \neq b$. Tātad, jebkuras divas dažādas matricas F rindiņas ir ortogonālas, un tā ir Adamāra. ■

Matricu F no iepriekšēja Secinājuma sauc par grupas G *Furjē matricu*. Piemēram, ja mēs paņemsim $G = \mathbb{Z}_n$, tad mēs dabūsim tādu matricu:

$$F_n = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \dots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \dots & \omega_n^{2n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \omega_n^{2n-2} & \dots & \omega_n^{n^2-2n+1} \end{pmatrix} \tag{1.3}$$

kur $\omega_n = e^{2\pi \mathbf{i}/n}$. Ja mēs gribam to uztvert kā unitāru operāciju, tad pietiek to pareizināt ar $\frac{1}{\sqrt{n}}$. Kvantu skaitļošanā ir pieņemts definēt F_n pareizinātu ar $\frac{1}{\sqrt{n}}$. Mēs pieturēsimies pie plašāk pieņemtās norunas, un definēsim F_n kā (1.3). Patvaļīga Furjē matrica ir vienāda ar tādu matricu tenzorreizinājumu, t.i., ja $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$, tad atbilstošā Furjē matrica būs $F = F_{d_1} \otimes F_{d_2} \otimes \cdots \otimes F_{d_m}$. Vektora x, kura komponentes ir indeksētas ar grupas G elementiem, *Furjē transformācija* ir definēta ar Fx.

Pieņemsim, ka $A = (a_{ij})$ un $B = (b_{ij})$ ir divas vienāda izmēra matricas. To *Adamāra reizinājums* (skat., piemēram, [43] Nodaļu 7) ir tāda paša izmēra matrica (apzīmēta ar $A \circ B$) ar (i,j)-to elementu vienādu ar $a_{ij} b_{ij}$. Citiem vārdiem, matricas tiek sareizinātas pa elementiem. Adamāra k-tā pakāpe atkal ir tāda paša izmēra matrica (apzīmējums $A^{(k)}$) ar (i,j)-to elementu vienādu ar a_{ij}^k. Sekojošais rezultāts ir acīmredzams.

Apgalvojums 1.5. *Grupas G Furjē matrica ir simetriska. Apzīmēsim ar R_i matricas rindu, kas atbilst elementam $i \in G$. Tad $R_i \circ R_j = R_{i+j}$, t.i., rindu kopa ar Adamāra reizinājuma operāciju veido grupu, kas ir izomorfa sākotnējai grupai G.*

1.3. Pauli un Kliforda Grupas

Atgādināsim, ka *unitārā grupa* $\mathrm{U}(n)$ (**unitary group**) ir grupa, kuru veido visas unitāras matricas telpā $\mathbb{C}^n$ ar matricu reizinājumu kā grupas operāciju. Aplūkosim grupu, kuru veido sekojošie divi operatori (to rindas un kolonnas ir sanumurētas ar $\mathbb{Z}_n$ elementiem, sākot no 0 un beidzot ar $n-1$):

$$X_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad Z_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega_n & 0 & \cdots & 0 \\ 0 & 0 & \omega_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega_n^{n-1} \end{pmatrix}. \tag{1.4}$$

Pirmais operators attēlo kanoniskās bāzes vektoru e_i par bāzes vektoru e_{i+1}, kur $i+1$ ir ņemts pēc moduļa n. Otrais operators pareizina bāzes vektoru e_i ar ω_n^i.

Pieminēsim dažas īpašības, kuras piemīt šiem diviem operatoriem. Pirmkārt, $Z_n X_n = \omega_n X_n Z_n$, jo

$$Z_n X_n e_i = Z_n e_{i+1} = \omega_n^{i+1} e_{i+1} = \omega_n X_n \omega_n^i e_i = \omega_n X_n Z_n e_i$$

visiem bāzes vektoriem e_i. Var arī viegli redzēt, ka $X_n^n = Z_n^n = I_n$, kur I_n ir vienības matrica.

Tātad, grupa, kuru veido X_n un Z_n, sastāv no n^3 elementiem $\{\omega_n^k X_n^i Z_n^j \mid 0 \leq k,i,j \leq n-1\}$. Bet kvantu mehānikā globālā fāze parasti nav svarīga, tāpēc mēs no sākuma definēsim $\mathrm{I}(n)$ kā $\{\alpha I \mid \alpha \in \mathbb{C}, |\alpha| = 1\}$, un tad definēsim *vispārināto Pauli grupu* $\mathrm{GP}(n)$ (**generalized Pauli group**) kā iepriekšējas grupas no n^3 elementiem faktorgrupu pēc tās šķēluma ar $\mathrm{I}(n)$. Vēl pēdējā grupa ir zināma kā *Veila-Heizenberga grupa* (**Weyl-Heisenberg group**). No pieminētām operatoru X_n un Z_n īpašībām seko, ka vispārinātā Pauli grupa $\mathrm{GP}(n)$ ir izomorfa ar grupu $\mathbb{Z}_n \times \mathbb{Z}_n$.

Mēs arī izmantosim vispārināto Pauli grupu tenzorreizinājumus, tāpēc definēsim $\mathrm{GP}(G)$, kur G ir galīga Ābela grupa kā formulā (1.1), sekojošajā veidā. Paņemsim $\mathrm{GP}(\mathbb{Z}_n) = \mathrm{GP}(n)$, un grupām G_1 un G_2 definēsim $\mathrm{GP}(G_1 \times G_2) = \{U_1 \otimes U_2 \mid U_1 \in \mathrm{GP}(G_1), U_2 \in \mathrm{GP}(G_2)\}$. Var viegli pārliecināties, ka $\mathrm{GP}(G) \cong G \times G$ un, tādējādi, $|\mathrm{GP}(G)| = |G|^2$.

Kliforda grupu $\mathrm{C}(n)$ (**Clifford group**) definē kā grupas $\mathrm{U}(n)/\mathrm{I}(n)$ apakšgrupu, kas normalizē vispārīgo Pauli grupu ar konjugāciju. Tas ir,

$$\mathrm{C}(n) = \{U \in \mathrm{U}(n)/\mathrm{I}(n) \mid U\,\mathrm{GP}(n)U^* = \mathrm{GP}(n)\}.$$

Atgriežoties pie operatoriem X_n un Z_n, operatoram X_n ir spēkā sekojošā acīmredzama īpašība:

Apgalvojums 1.6. *Operatoram X_n ir īpašvērtības $\lambda_k = \omega_n^{n-k}$ for $k = 0, 1, \ldots, n-1$ un atbilstošie īpašvektori ir*

$$t_k = (1, \omega_n^k, \omega_n^{2k}, \ldots, \omega_n^{(n-1)k}).$$

Furjē matricai F_n, kā tā ir definēta ar (1.3), ir tieši tādas kolonnas un matricai Z_n^{-1} ir tieši tādas pašas īpašvērtības uz diagonāles, tādējādi, $Z_n^{-1} = F_n^{-1} X_n F_n$. Aizvietojot F_n ar F_n^{-1}, mēs dabūjām līdzīgā veidā, ka $Z_n = F_n X_n F_n^{-1}$. No šim divām vienādībām seko, ka

Apgalvojums 1.7. *Furjē matrica $\frac{1}{\sqrt{n}} F_n$ pieder Kliforda grupai $\mathrm{C}(n)$.*

Šo rezultātu var pastiprināt sekojošajā veidā [35]. Izrādās, ka Furjē matrica, kopā ar matricām X_n un Z_n un matricu $P_n = (p_{ij})$, kur

$$p_{ij} = \begin{cases} 0, & i \neq j \\ \omega_n^{i^2/2}, & i = j \text{ un } n \text{ ir pāra} \\ \omega_n^{i(i-1)/2}, & i = j \text{ un } n \text{ ir nepāra} \end{cases},$$

viedo Kliforda grupu. Kliforda grupa arī ir zināma, īpaši skaitļu teorijā, kā *Jakobi grupa*. Skat., piemēram, [14].

Kvadrātisku matricu $C = (c_{ab})$, kuras rindas un kolonnas ir indeksētas ar Ābela grupas G elementiem, sauc par *cirkulāru* (**circulant**) par G, ja $c_{a+d,b+d} = c_{a,b}$ visiem $a, b, d \in G$. Ja $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$, tad, kā viegli redzēt, matrica ir cirkulāra tad un tikai tad, ja tā ir matricu

$$\{X_{d_1}^{a_1} \otimes X_{d_2}^{a_2} \otimes \cdots \otimes X_{d_m}^{a_m} \mid 0 \leq a_i < d_i\}. \tag{1.5}$$

lineāra kombinācija. Tā kā F_n diagonālizē X_n, tad grupas G Furjē matrica $F = F_{d_1} \otimes F_{d_2} \otimes \cdots \otimes F_{d_m}$ diagonālizē visas matricas no (1.5), tātad, arī visas cirkulāras matricas par G.

2. nodaļa

MUBi un SIC-POVMi

Šajā nodaļā mēs ieviesīsim objektus, ar kuriem mēs taisāmies strādāt līdz pat darba beigām: savstarpēji nenosliektas bāzes (MUBus) un simetriskus informacionāli pilnus POVMus (SIC-POVMus). Mēs dosim atbilstošas definīcijas, formulēsim galvenos rezultātus un šo objektu pielietojumus. Sadaļā 2.2. mēs formulēsim galvenās hipotēzes SIC-POVMu eksistencei.

2.1. Savstarpēji nenosliektas bāzes

Divus vektorus $x, y \in \mathbb{C}^n$ sauc par *nenosliektiem* (**unbiased**), ja to skalārā reizinājuma absolūtā vērtība $|\langle x, y\rangle|$ ir $\frac{1}{\sqrt{n}}$. Īsuma labad tālāk skalārā reizinājuma absolūtās vērtības kvadrātu sauksim par *leņķi* (**angle**) starp šiem vektoriem (tāda terminoloģija ir pieņemta, teiksim, darbā [47]). Tātad, divi vektori ir nenosliekti, ja leņķis starp tiem ir $\frac{1}{n}$.

Par *savstarpēji nenosliektu bāzu* (**mutually unbiased bases**) sistēmu unitārajā telpā $\mathbb{C}^n$ sauc šīs telpas ortonormētu bāzu sistēmu $\{B_0, B_1, \ldots, B_r\}$ tādu, ka jebkuri divi vektori no dažādām bāzēm ir nenosliekti. Mēs parasti lietosim saīsinājumu no angļu valodas, saucot tādu sistēmu par *MUBu sistēmu*. Mēs bieži grupēsim bāzes vektorus matricā, un teiksim, ka divas unitāras matricas ir savstarpēji nenosliektas, ja bāzes, ko veido tās kolonnas, ir savstarpēji nenosliektas. Pirmo reizi tādas bāzes aplūkoja Švingers (**Schwinger**) [63]. Nosaukumu "savstarpēji nenosliektas bāzes" piedāvāja Fīldss un Vūterss (**Fields, Wootters**) rakstā [74]. Piemēram, sekojošas trīs telpas $\mathbb{C}^2$ bāzes ir

savstarpēji nenosliektas:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ \mathbf{i} & -\mathbf{i} \end{pmatrix} \right\} \tag{2.1}$$

MUBu pielietojumi iekļauj kvantu stāvokļu tomogrāfiju [45, 74]. Var pierādīt, ka tie veido labāko mērījumu sistēmu, kas sastāv no $n+1$ ortonormētām bāzēm. Cits pielietojums ir kvantu kriptogrāfija. Piemēram, labi zināms protokols BB84, kuru piedāvāja Benets un Brasards (**Bennet, Brassard**) [13], izmanto pirmās divas bāzes no (2.1). Ideja šim pielietojumam ir tāda, ka mērījums vienā no bāzēm nedod absolūti nekādu informāciju par to, kāds būtu iznākums, ja mērījums tiktu izpildīts pirmajā bāzē. Vēl tos var pielietot Vīdēja Karaļa problēmā (**Mean King's problem**) [1] un konstruējot Vignēra (**Wigner**) funkcijas [75]. Jaunāko svarīgāko informāciju par MUBiem var atrast saitē [28].

Skaidrs, ka ja $n = 1$, tad jebkura vienības vektoru (patiesībā, skalāru) kopa dos MUBu sistēmu. Šis rezultāts nav pārāk interesants, tādēļ mēs tālāk pieņemsim, ka telpa ir n-dimensionāla, kur $n \geq 2$. Šajā gadījumā var pierādīt, ka telpā $\mathbb{C}^n$ neeksistē sistēma no vairāk kā $n+1$ savstarpēji nenosliektām bāzēm (sk. Teorēmu 3.3 tālāk tekstā). Ortonormētu bāžu sistēmu, kas sasniedz šo robežu, sauc par *pilno* (**complete**) MUBu sistēmu. Piemēram, trīs MUBi no (2.1) veido pilno MUBu sistēmu telpā $\mathbb{C}^2$. Interesants jautājums ir, vai tamlīdzīga sistēma eksistē katram dimensiju skaitam n. Atbilde ir pozitīva, ja n ir pirmskaitļa pakāpe [45, 74]. Atbilstošas konstrukcijas tiks aprakstītas Sadaļās 2.1.1. un 7.2.3. Visās citās dimensijās (pat, ja $n = 6$) jautājums ir joprojām atklāts par spīti daudzām pūlēm atrisināt šo problēmu (sk., piem., [12]).

Pieņemsim, ka mums ir dota MUBu sistēma: $\{B_0, B_1, \ldots, B_r\}$. Mēs vienmēr varam tos aprakstīt bāzē B_0 (t.i., pareizināt visas bāzes ar B_0^{-1} no kreisās puses). Tādēļ mēs varam pieņemt, ka pirmā bāze ir kanoniskā bāze (vienības matrica). Tad matricām, kas apraksta pārejas bāzes, visi elementi pēc absolūtas vērtības būs vienādi ar $\frac{1}{\sqrt{n}}$, t.i., tās būs Adamāra matricas.

Adamāra matricu sistēmu tādu, ka jebkuras divas no tām ir savstarpēji nenosliektas, sauc par *savstarpēji nenosliektu Adamāra matricu* (**Mutually Unbiased Hadamards**) sistēmu (MUHu sistēmu). Sekojošs rezultāts ir acīmredzams:

Apgalvojums 2.1. *Pilnā MUBu sistēma telpā $\mathbb{C}^n$ eksistē tajā un tikai tajā gadījuma, kad šajā telpā eksistē n MUHu sistēma.*

Sistēmu, kas sastāv no n MUHiem telpā $\mathbb{C}^n$, sauc par *pilno MUHu sistēmu*. Parasti ir ērtāk strādāt tieši ar MUHiem, un mēs pieturēsimies pie šī atlikušajā darba daļā.

Pilno MUBu sistēmu meklējumi ir sarežģīti gan liela meklēto bāzu skaita dēļ, gan tāpēc, ka leņķi $\frac{1}{n}$, kuru veido divi vektori no dažādām bāzēm, ir grūti iztēloties. Izmantojot Velča nevienādību, kā aprakstīts nākamajā nodaļā, mēs dosim pietiekamu un nepieciešamu nosacījumu, kas izmanto tikai vektoru ortogonalitāti. Skaidrs, ka tā ir daudz vairāk intuitīvāka un izpētītāka attiecība. Ir vērts pieminēt, ka tā nav pirmā reize, kad leņķi $\frac{1}{n}$ grib aizstāt ar nulli. Alternatīvo piegājienu, kur projicē attiecīgās blīvuma matricas un nulles pēdas Ermitu matricu telpu, ir aprakstīts rakstā [74].

Mūsu piegājiens ir citādāks. Izmantojot $n+1$ Adamāra matricu sistēmu telpā $\mathbb{C}^n$, mēs konstruējam n plakanus vektorus no $\mathbb{C}^{n^2}$, t.i., tādus, ka visiem šo vektoru elementiem ir vienādas absolūtas vērtības. Tālāk, no katriem diviem šādiem vektoriem mēs iegūstam jaunu šīs pašas telpas vektoru. Mēs pierādām, ka sākotnējās Adamāra matricas ir savstarpēji nenosliektas tad un tikai tad, ja šie vektori ir savstarpēji ortogonāli. Nav grūti atrast $\binom{n}{2}$ ortogonālus plakanus vektorus telpā $\mathbb{C}^{n^2}$, taču, vispār runājot, tos nevarēs sadalīt atpakaļ pāros.

Turklāt, ja mēs koncentrēsimies MUH homogēnām sistēmām, (skat., Sadaļu 5.3.), tad šo kritēriju var vienkāršot līdz divām matricām no $\mathbb{C}^n$ un līdzīgiem ortogonalitātes nosacījumiem. Lai parādītu šīs pieejas noderīgumu, mēs aprakstām jau zināmas MUHu konstrukcijas, izmantojot šo konstrukciju un pierādām, ka tie tiešam veido MUHu pilnās sistēmas.

Mēs arī parādam, kā šis piegājiens dabiski aizved pie dažu kombinatorisko struktūru pielietojumiem MUBu konstruēšanā, kuri tika atklāti nesen. Starp citu, mēs vispārinām atbilstību starp planārām funkcijām un sadalāmām semiregulārām relatīvām starpību kopām līdz nesadalāmo starpību kopu gadījumam (Sadaļa 7.2.4.).

2.1.1. Zināmas MUBu konstrukcijas

Šajā sadaļā mēs dosim zināmu konstrukciju MUHu pilnai sistēmai telpā $\mathbb{C}^{p^k}$, kur p ir nepāra pirmskaitlis. Šo konstrukciju gadījumā, kad $k=1$ ieguva Ivanovičs (**Ivanović**) [45] un tad tika vispārināta visiem k Vūtersa un Fīldsa rakstā [74]. Iemesls kāpēc ir nepieciešama pirmskaitļa pakāpe ir tāds, ka šī konstrukcija izmanto galīgus laukus, un tiem, kā labi zināms, ir tikai pirmskaitļa pakāpes izmēri. Kā tika teikts iepriekš, mēs aplūkosim tikai nepāra gadījumu. Gadījums, kad $p=2$, tiks aplūkots vēlāk, kopā ar citu pierādījumu nepāra pirmskaitļu gadījumā Sadaļā 7.2.3. Ar terminiem, kas saistīti ar galīgo lauku teoriju, var iepazīties jebkurā standarta grāmatā par šo tēmu, teiksim, iekš [51].

Pieņemsim, ka $GF(p^k)$ ir galīgs lauks ar p^k elementiem. Mēs lietosim ψ lai apzīmētu lauka aditīvas grupas raksturus un ϕ — lauka multiplikatīvas grupas raksturiem. Mēs arī pieņemsim, ka multiplikatīvie raksturi ir netriviālie, t.i., tie pieņem nevienības vērtību vismaz vienai argumenta vērtībai, un ka $\phi(0) = 0$.

Pastāv kanoniskais veids, kā var reprezentēt lauka aditīvus raksturus, izmantojot tā multiplikatīvu struktūru. Tas elementam $a \in GF(p^k)$ piekārto raksturu

$$\psi_a(x) = \omega_p^{\mathrm{Tr}(ax)}, \tag{2.2}$$

kur Tr ir *pēdas* (**trace**) funkcija $GF(p^k) \to GF(p)$. Tā ir definēta ar sakarību

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{k-1}}.$$

Pēda ir lineāra funkcija, un tas padara $\psi_a(x)$ par raksturu. Izmantojot šo atbilstību, var definēt funkcijas $f : GF(p^k) \to \mathbb{C}$ Furjē transformāciju kā funkciju $\hat{f} : GF(p^k) \to \mathbb{C}$ ar

$$\hat{f}(x) = \frac{1}{\sqrt{p^k}} \sum_{a \in GF(p^k)} \psi_a(x) f(a).$$

Ja $x \neq 0$, tad sekojošās transformācijas

$$\sum_{a \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax)} \phi(a) = \overline{\phi(x)} \sum_{a \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax)} \phi(ax) = \overline{\phi(x)} \sum_{a \in GF(p^k)} \psi_1(a)\phi(a)$$

dod elegantu identitāti

$$\hat{\phi}(x) = \overline{\phi(x)}\hat{\phi}(1). \tag{2.3}$$

Formula izpildās jebkuram netriviālam raksturam ϕ un jebkuram x (ja $x = 0$, tad šī identitāte seko no Lemmas 1.3). Izmantojot šo formulu, un to faktu, ka Furjē transformācija ir unitārs attēlojums, nav grūti pierādīt, ka $|\hat{\phi}(x)| = 1$ visiem $x \neq 0$, un ka $\hat{\phi}(0) = 0$.

Aplūkosim tagad sekojošu *kvadrātisku* (**quadratic**) multiplikatīvu raksturu:

$$\tau(a) = \begin{cases} 0 & , \quad a = 0; \\ 1 & , \quad a \neq 0 \text{ ir kvadrāts laukā } GF(p^k); \\ -1 & , \quad a \text{ nav kvadrāts laukā } GF(p^k). \end{cases}$$

un funkciju $\kappa_a(x) = \psi_a(x^2)$. Izmantojot šos divus objektus, nav grūti parādīt, ka

$$|\hat{\kappa}_a(b)| = 1 \tag{2.4}$$

visiem nenulles a. Tiešam, $|\hat{\kappa}_a(b)|$ ir vienāds ar

$$\left| \frac{1}{\sqrt{p^k}} \sum_{x \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax^2+bx)} \right| = \left| \frac{1}{\sqrt{p^k}} \sum_{x \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax^2)} \right| = \left| \frac{1}{\sqrt{p^k}} \sum_{y \in GF(p^k)} \omega_p^{\mathrm{Tr}(ay)} (1 + \tau(y)) \right|$$

$$= \left| \frac{1}{\sqrt{p^k}} \left(\sum_{y \in GF(p^k)} \omega_p^{\mathrm{Tr}(ay)} + \sum_{y \in GF(p^k)} \omega_p^{\mathrm{Tr}(ay)} \tau(y) \right) \right| = |\hat{\tau}(a)| = 1.$$

Otrajā vienādībā tiek pielietota transformācija $x \mapsto x - \frac{b}{2a}$. Trešajā solī tiek izmantots fakts, ka jebkuram nenulles kvadrātam laukā ar nepāra harakteristiku (t.i., ka p ir nepāra) ir tieši divas kvadrātsaknes. Piektajā solī mēs izmantojām Lemmu 1.3.

Teorēma 2.2. *Bāzes*

$$(v_b^{(r)})_\ell = \frac{1}{\sqrt{p^k}} \omega_p^{\mathrm{Tr}(r\ell^2 + b\ell)}$$

(kur r ir bāzes indekss, b ir vektora indekss un ℓ ir komponentes indekss, visi elementi no $GF(p^k)$ un p ir nepāra pirmskaitlis) dod pilno MUHu sistēmu telpā $\mathbb{C}^{p^k}$.

Pierādījums. Paņemsim divus vektorus no dažādām bāzēm, teiksim $v_{b_1}^{(r_1)}$ un $v_{b_2}^{(r_2)}$, $r_1 \neq r_2$. Var viegli redzēt, ka

$$\left| \langle v_{b_1}^{(r_1)}, v_{b_2}^{(r_2)} \rangle \right| = \left| \frac{1}{p^k} \sum_{\ell \in GF(p^k)} \omega_p^{\mathrm{Tr}((r_2 - r_1)\ell^2 + (b_2 - b_1)\ell)} \right| = \left| \frac{1}{\sqrt{p^k}} \hat{\kappa}_{r_2 - r_1}(b_2 - b_1) \right| = \frac{1}{\sqrt{p^k}}.$$

Pārējos skalārus reizinājumus var pārbaudīt līdzīgi. ■

2.2. Simetriskie informacionāli pilnie POVMi

Par *Simetrisku informacionāli pilno POVMu*, (**Symmetric Informationally Complete POVM**) jeb SIC-POVMu sauc kopu $\{x_i\}$, kas sastāv no n^2 vienības vektoriem unitarajā n-dimensionālajā telpā $\mathbb{C}^n$ tādiem, ka

$$|\langle x_i, x_j \rangle| = \frac{1}{\sqrt{n+1}}$$

dažādiem i un j. Tādējādi definēta, šī kopa, protams, nav POVMs. Lai uzbūvētu POVMu jāpaņem operatori $\{\frac{1}{n} x_i^* x_i\}$. Uzreiz nav acīmredzams, ka šī kopa ir POVMs, mēs to pierādīsim tālāk Sadaļā 5.1.. Bet ja tagad ir skaidrs, ka tā ir kopa no vektoriem, ka jebkuri divi dažādi no tiem veido vienu un to pašu leņķi. Kā tādi tie jau tika pētīti ārpus kvantu informācijas teorijas. Pirmais raksts, kur parādās tāds jēdziens ir [50].

Kvantu informācijas redzeslokā šis jēdziens pirmo reizi parādījās Caunerā (**Zauner**) doktora disertācijā [76]. Papildus kvantu tomogrāfijai [19], SIC-POVMi tiek pielietoti arī kvantu kriptogrāfijā [31] un kvantu mehānikas teorētiskajos pētījumos [32], kur tie veido "standarto kvantu mērījumu", līdzīgi standartizētajiem metram un kilogramam, kuri glabājas Francijā.

Lielākais daudzums no darbiem, kuri veltīti SIC-POVMiem, aplūko dažādus specālus gadījumus, kurus mēs tagad aprakstīsim.

2.2.1. Grupu kovarianti SIC-POVMi

Kontrastā ar MUBu gadījumu, skaitliskie SIC-POVMi tika atrasti visās dimensijās, kuras ir pietiekoši mazas, lai atļautu tādu pārlasi. Bet tikai daži analītiskie SIC-POVMi ir zināmi, un nav zināma neviena konstrukcija, kas darbotos priekš bezgalīgi daudziem n. Daudz pūļu tika veltīti cenšoties samazināt meklējuma apgabalu, t.i., dot stingrāku hipotēzi nekā vienkārši SIC-POVMu eksistence. Tāda hipotēze, ja tā izpildītos nelielās dimensijās, varētu izstrādāt intuīciju, lai atrastu paņēmienu, kā SIC-POVMu uzkonstruēt arī citās dimensijās. Turklāt, samazinot meklēšanas apgabalus, parasti atvieglojas datorpārlase, kas atļauj atrast SIC-POVMus ar datoru arī lielākajā dimensiju skaitā. Šajā nodaļā mēs dosim dažas no šīm hipotēzēm.

Vektoru $\psi \in \mathbb{C}^n$ sauc par *fiduciāro vektoru attiecībā pret* K (**fiducial**), kur K ir $\mathrm{U}(n)/\mathrm{I}(n)$ apakšgrupa, ja kopa $\{U\psi \mid U \in K\}$ veido SIC-POVMu (sk. Sadaļu 1.3. priekš grupu $\mathrm{U}(n)$, $\mathrm{I}(n)$ un tamlīdzīgu definīcijām). SIC-POVMu, kuru var tādā veidā uzbūvēt sauc par *grupu-kovariantu attiecībā pret* K (**group covariant**). Šis nosaukums atspoguļo to, ka katrs grupas K elements permutē, ar precizitāti līdz fāzei, SIC-POVMa elementus.

Parasti šo jēdzienu pielieto ar $K = \mathrm{GP}(n)$. Tādējādi, ja grupa K netiks specificēta, tad tas nozīmē, ka tā ir vispārināta Pauli grupa. Piemērām, telpā $\mathbb{C}^2$ fiduciāri vektori ir

$$\frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{3+\sqrt{3}}\\ \omega_8\sqrt{3-\sqrt{3}}\end{pmatrix} \qquad \text{un} \qquad \frac{1}{\sqrt{6}}\begin{pmatrix}-\sqrt{3-\sqrt{3}}\\ \omega_8\sqrt{3+\sqrt{3}}\end{pmatrix}. \tag{2.5}$$

Mēs dosim vairāk piemērus Nodaļā 7.. Dažreiz mēs izvēlēsimies K lomai grupu $\mathrm{GP}(G)$, kur G ir galīga Abela grupa.

Grup kovarianta SIC-POVMa jēdziens pieder Renesam (**Renes**) un līdzautoriem [58]. Sekojošā hipotēze arī pieder viņiem:

Neatrisināta Problema 2.3. *Vai grupu kovariantie SIC-POVMi eksistē visās dimensijās?*

Tajā pašā rakstā viņi dod skaitliski atrastus SIC-POVMus visās dimensijās līdz pat 45. Šo sarakstu var atrast saitē [59]. Piemēram, priekš $n = 5$ šajā saitē ir dots sekojšs fiduciārais vektors:

$$\begin{pmatrix}0.1630948960 - 0.3554098551\mathbf{i}\\ 0.3048387097 + 0.0113254913\mathbf{i}\\ 0.2784270686 + 0.3836760386\mathbf{i}\\ 0.6479623659 - 0.2829656308\mathbf{i}\\ 0.1544552195 - 0.0742890175\mathbf{i}\end{pmatrix}. \tag{2.6}$$

Var atzīmēt arī saiti [66], kur var atrast skaitliskas izteiksmes fiduciāriem vektoriem līdz dimensijai 67.

Analītiskas izteiksmes fiduciāriem vektoriem ir zināmas sekojošām n vērtībām: 2,3,4,5 [76], 6 [35], 7, 19 [6], 8, 9, 10, 12, 13 [36], 11 un 15 [37].

Svarīgs jautājums ir: kādas operācijas saglabā "fiduciārumu". Pirmā atbilde uz šo jautājumu varētu būt:

Apgalvojums 2.4. *Ja C ir Kliforda grupas $\mathrm{C}(n)$ elements un $\psi \in \mathbb{C}^n$ ir fiduciārs vektors, tad $C\psi$ arī ir fiduciārais vektors.*

Pierādījums. Tiešam, katram $U \in \mathrm{GP}(n)$ tādam, ka $U \notin \mathrm{I}(n)$, izpildās:

$$|\langle C\psi, UC\psi\rangle| = |\langle C\psi, CU'\psi\rangle| = |\langle \psi, \alpha U'\psi\rangle|,$$

kādam $U' \in \mathrm{GP}(n)$. Svarīgi pārliecināties, ka $U' \notin \mathrm{I}(n)$, bet tas tā ir, jo citādi izpildītos $U = CU'C^* \in \mathrm{I}(n)$, kas nav iespējams. Tātad, skalārais reizinājums ir vienāds ar $\frac{1}{\sqrt{n+1}}$. ■

Pirmo reizi šim rezultātam pievērsa uzmanību Grasls (**Grassl**) [35]. Piemēram, ja x ir fiduciārs vektors un $a, b \in \mathbb{Z}_n$, turklāt a ir savstarpējais pirmskaitlis ar n, tad vektors y ar komponentēm $y_j = x_{aj+b}$ arī ir fiduciārs. Citiem vārdiem, permutējot fiduciāra vektora komponentes ar apgriežamo afīno operāciju (kas darbojās indeksu kopā $\mathbb{Z}_n$) saglāba "fiduciārumu". Šī operācija iekrīt Apgalvojuma 2.4 aplūkojamo gadījumu skaitā, jo tāda permutācija pieder Kliforda grupai.

Bet eksistē viena svarīga operācija, kurai Apgalvojums 2.4 nestrādā. Tik tiešam, viegli redzēt, ka, ja $\psi \in \mathbb{C}^n$ ir fiduciārs vektors, tad

$$|\langle \overline{\psi}, X_n^i Z_n^j \overline{\psi}\rangle| = \overline{|\langle \psi, X_n^i Z_n^{n-j}\psi\rangle|} = \frac{1}{\sqrt{n+1}}$$

visiem veseliem $0 \leq i, j < n$, kas nav vienādi ar nulli vienlaicīgi. Tādējādi, kompleksā saistīta ņemšana, saglabā "fiduciārumu".

Tas uzvedināja Epelbeju (**Appleby**) definēt paplašinātu Kliforda grupu rakstā [6] sekojošajā veidā. Definēsim *anti-lineāru* (**anti-linear**) operatoru $L : \mathbb{C}^n \to \mathbb{C}^n$ kā lineāru operatoru virs $\mathbb{R}$ ar papildus īpašību $L(\alpha\psi) = \bar{\alpha}L\psi$ visiem vektoriem ψ un skalāriem α. Anti-lineāru operatoru L sauc par *anti-unitāru* (**anti-unitary**), ja tas ir apgriežams, un tā apgrieztais operators L^{-1} apmierina nosacījumu $\langle \varphi, L^{-1}\psi\rangle = \langle \psi, L\varphi\rangle$ visiem $\varphi, \psi \in \mathbb{C}^n$.

Paplašinātu Kliforda grupu (**extended Clifford group**) $\mathrm{EC}(n)$ definē kā grupu, kas sastāv no visiem unitāriem un anti-unitāriem operatoriem U tādiem, ka $U\,\mathrm{GP}(n)U^{-1} = \mathrm{GP}(n)$. Apgalvojumu 2.4 var precizēt sekojošajā veidā:

Apgalvojums 2.5. *Ja C ir paplašinātas Kliforda grupas* $\mathrm{EC}(n)$ *elements un $\psi \in \mathbb{C}^n$ ir fiduciārs vektors, tad $C\psi$ arī ir fiduciārs vektors.*

2.2.2. Caunera hipotēze

Kā mēs redzējām iepriekšējā punktā, katrs Kliforda grupas elements attēlo fiduciāro vektoru uz fiduciāro vektoru. Tā kā fiduciāro vektoru nav tik daudz, iespējams, ka kāds Kliforda grupas elements U attēlo fiduciāro vektoru pašu uz sevi ar precizitāti līdz skalāram, t.i., ka fiduciārs vektors ir operatora U īpašvektors.

Kaut ko tamlīdzīgu piedāvāja Cauners savā doktora darbā [76]. Aplūkosim unitāro $n \times n$-matricu $S = (s_{ij})$, kas definēta ar

$$s_{ij} = \frac{\omega_{24}^{n-1}}{\sqrt{n}} \omega_{2n}^{2ij+(n+1)j^2}.$$

Tā pieder Kliforda grupai, jo

$$S^{-1}XS = Z^{-1} \quad \text{un} \quad S^{-1}ZS = \omega_{2n}^{n-1} XZ^{-1}.$$

Bieži šo operatoru apzīmē ar Z, mēs nelietojām šo apzīmējumu, lai nesajauktu šo operatoru ar operatoru Z_n, kas definēts ar (1.4).

Hipotēze A. *Katrā galīgā dimensijā eksistē fiduciārs vektors, kas ir operatora S īpašvektors.*

Šo hipotēzi nav triviāli pārbaudīt, jo operatoram S ir ārkārtīgi deģenerēts spektrs. Var pārbaudīt, ka $S^3 = I$, tātad tam ir trīs iespējamas īpašvērtības: $1, \omega_3$ un ω_3^2. Atbilstošām īpaštelpām ir sekojošas dimensijas:

n	1	ω_3	ω_3^2
$3m$	$m+1$	m	$m-1$
$3m+1$	$m+1$	m	m
$3m+2$	$m+1$	$m+1$	m

Arī ir vērts atzīmēt, ka ja ψ ir fiduciārs vektors un vienlaicīgi ir operatora $U \in \mathrm{EC}(n)$ īpašvektors, un U' ir operatoram U konjugēts operators grupā $\mathrm{EC}(n)$ (teiksim, $U' = VUV^{-1}$, $V \in \mathrm{EC}(n)$), tad $V\psi$ ir operatora U' īpašvektors, kā arī fiduciārs vektors Apgalvojuma 2.5 dēļ.

Epelbejs rakstā [6], rūpīgi analizējot rakstā [58] skaitliski atrastus fiduciārus vektorus, definēja speciālu klāsi, kas sastāv no trešās kārtas elementiem no $\mathrm{C}(n)$, un kuru

viņš nosauca par *kanoniskiem trešās kārtas unitāriem operatoriem* (**canonical order 3 unitary**). Balstoties uz šo klasi, viņš izvirzīja divas hipotēzes:

Hipotēze B. *Fiduciārs vektors eksistē katrā galīgā dimensijā. Katrs fiduciārs vektors ir kanoniskā trešās kārtas unitāra operatora īpašvektors.*

Hipotēze C. *Fiduciārs vektors eksistē katrā galīgā dimensijā. Katrs fiduciārs vektors ir operatora $U \in \mathrm{C}(n)$ īpašvektors, kur U ir operatoram S konjugēts operators.*

Patiesībā, S ir kanoniskais trešās kārtas unitārs operators, un katrs operators, kas ir konjugēts kanoniskajam trešās kārtas unitāram operatoram arī ir kanoniskais trešās kārtas unitārs operators. Tādējādi, Hipotēze C implicē abas Hipotēzes A un B. Pagaidām neviens pretpiemērs Hipotēzēm A un B netika atrasts. Grasls [36] uzkonstruēja pretpiemēru Hipotēzei C telpā $\mathbb{C}^{12}$, taču ja n ir pirmskaitlis, kas ir lielāks par 3, tad Hipotēzes A, B un C ir ekvivalentas [29].

Var redzēt, ka galvenais virziens sastāv tajā, lai sašaurinātu SIC-POVMu klasi pēc iespējas vairāk. Mēs, savukārt, definēsim Nodaļā 5.3. nedaudz plašāku SIC-POVMu klasi nekā grupu kovarianti SIC-POVMi. Šai konstrukcijai ir daudz kas kopīgs ar MUHu pilno sistēmu konstrukcijām, un dažreiz tā atļauj uzkonstruēt elegantākus SIC-POVMus nekā tie, kas ir zināmi.

3. nodaļa

Velča nevienādība

Šajā nodaļā mēs dosim nelielu apskatu virknēm ar zemu korelāciju, jo tām ir daudz kas kopīgs ar objektiem, kurus mēs definējām iepriekšējā nodaļā. Galvenais, ko mēs iegūsim no šī apskata, ir Velča nevienādības — nevienādības, kas saista vektoru skaitu noteiktā sistēmā ar to korelāciju.

Velča nevienādības var pielietot arī mūsu problēmai. Izrādās, ka MUBu pilnās sistēmas un SIC-POVMi apmierina šo nevienādību priekš $k = 2$ ar vienādību. Kā mēs parādīsim nākamajā nodaļā, tas nozīmē, ka tie veido komplekso projektīvo 2-dizainu.

3.1. Velča nevienādība un korelācijas

Par *Velča nevienādību* sauc nevienādību no sekojošas teorēmas:

Teorēma 3.1. *Katrai galīgai vektoru virknei* $\{x_i\}$ *no unitārās telpas* $\mathbb{C}^n$ *un katram naturālam* $k \geq 1$ *izpildās sekojoša nevienādība*

$$\binom{n+k-1}{k} \sum_{i,j} |\langle x_i, x_j \rangle|^{2k} \geq \left(\sum_i \langle x_i, x_i \rangle^k \right)^2. \tag{3.1}$$

Pierādījums tiks dots Sadaļā 5.1.. Sākotnēji šo nevienādību (gadījumā, kad visiem vektoriem ir vienāda norma) pierādīja Velčs [73]. Ir vērts iepazīties ar viņa motivāciju.

Lai to izdarītu, mums vajadzēsies definēt virknes ar zemu korelāciju. Sistemātiskāk ar šo tematu var iepazīties iekš [40]. Pieņemsim, ka u un v ir divas kompleksas periodiskas virknes ar periodu n. Parasti šīs sekvences tiek definētas ar $u_i = \omega_q^{a_i}$, kur $a_i \in \mathbb{Z}_q$. Binārais gadījums, kad $q = 2$, sastopas visbiežāk. Par virkņu u un v *(periodisku) korelāciju* (**periodic correlation**) definē kā (kur L ir kreisās nobīdes funkcija)

$$\theta_{u,v}(\tau) = \langle L^\tau(u), v \rangle = \sum_{i=1}^{n} \overline{u_i} v_{i+\tau}.$$

Virknes korelāciju pašai ar sevi sauc par tās *autokorelāciju* (**autocorrelation**) $\theta_u(\tau) = \langle L^\tau(u), u\rangle$. Divu tādu virkņu, ka vienu nevar dabūt no otrās, izmantojot nobīdi, parasti sauc par *savstarpēju korelāciju* (**crosscorrelation**).

Divu bināru virkņu korelācija ir vienāda ar to pozīciju skaitu, kur divas virknes sakrīt, mīnus to pozīciju skaits, kur šīs virknes atšķiras. Korelācija ir zema, ja tās absolūtā vērtība ir maza. Korelāciju sauc par *ideālu* (**ideal**), ja tā ir tik maza, cik tas ir iespējams, tas ir, 0 vai ± 1. To sauc par zemu, ja tā ir $O(\sqrt{n})$. Tā ir vidējā sagaidāma vērtība nejaušām virknēm. Tātad šīs parametrs dod vienu no virkņu nejaušības novērtēšanas kritērijiem.

Piemēram, *m-virknēm* (**m-sequences**), tas ir, maksimālā iespējamā garuma virknes, kurus ģenerē LFSR (**linear feedback shift register**) ir ideāla autokorelācija, jo tiem $\theta(\tau) = -1$ visiem $\tau \not\equiv 0 \pmod{n}$ [61]. Tas, kopā ar citiem šo virkņu īpašībām, izskaidro, kāpēc tie tiek pielietoti klasiskajā kriptogrāfijā (kā galvenā sastāvdaļa gandrīz katram plūsmas šifrētajam) un elektroniskajā inženierijā (piem., radaros).

Virkņu sistēmas ar mazu savstarpēju korelāciju arī ir labi izpētītas. Jaukā šo virkņu īpašība ir tā, ka tās var vienlaicīgi sūtīti pa vienu un to pašu kanālu, tā kā tās nerāda traucējumus viena otrai. Laikā, kad Velčs rakstīja savu rakstu, bija zināmas daudzas virkņu sistēmas ar mazu korelāciju, un jautājums bija izstrādāt novērtējumus no augšas virkņu skaitām tādā sistēmā.

Piemēram, vienu no visvairāk zināmajām virkņu sistēmām uzkonstruēja Golds (**Gold**) rakstā [33]. Katram $k \in \mathbb{N}$ viņš uzkonstruēja sistēmu no $2^k + 1$ virknēm ar periodu $2^k - 1$ un ar korelāciju starp jebkurām divām no tām no kopas $\{-1, -(2^{(k+1)/2} + 1), 2^{(k+1)/2} - 1\}$.

Šīs sistēmas un MUBu pilnās sistēmas līdzība ir labi saskatāma. Abas sastāv no vektoriem no $\mathbb{C}^n$, vektori tiek sagrupēti blokos ar izmēru n (Golda virkņu gadījumā šos blokus veido viena virkne kopā ar visām savām cikliskām nobīdēm), bloku skaits un atbilstoši skalārie reizinājumi arī gandrīz sakrīt. Tādējādi, ideja izmantot Velča nevienādības, pētot MUBu sistēmas, izskatās diezgan dabiski.

Pat vairāk, izrādās, ka Altops (**Alltop**) savā darbā [2], kas uzrakstīts 1980. gadā (t.i., vienu gadu pirms Ivanoviča darba [45] of Ivanović), visiem pirmskaitļiem $p \geq 5$ uzkonstruēja sistēmu no p virknēm ar periodu p, kuru katrs elements ir ar absolūtu vērtību

$\frac{1}{\sqrt{p}}$ un tādu, ka savstarpēja korelācija ir vienāda ar

$$|\theta_{uv}(\tau)| = \begin{cases} 1 & , \quad u = v \text{ un } \tau = 0; \\ 0 & , \quad u \neq v \text{ un } \tau = 0; \\ \frac{1}{\sqrt{p}} & , \quad \tau \neq 0. \end{cases}$$

Atbilstošas virknes ir definētas ar

$$b_\ell^{(r)} = \frac{1}{\sqrt{p}} \omega_p^{\ell^3 + r\ell}$$

(šeit r ir virknes numurs un ℓ ir komponentes indekss). Pierādījums ir līdzīgs Teorēmas 2.2 pierādījumam. Šīs virknes kopā ar savām cikliskām nobīdēm un kanonisko bāzi dod MUBu pilno sistēmu telpā $\mathbb{C}^p$. Cits veids kā to izteikt ir teikt, ka vektors $\{\omega_p^{\ell^3}\}_{\ell \in \mathbb{Z}_p}$ ir "fiduciārs vektors", kas dod MUHu pilno sistēmu, līdzīgi SIC-POVMiem, kurus mēs aplūkojām Sadaļā 2.2.1..

Šo rezultātu vispārināja pirmskaitļu pakāpju dimensijām rakstā [48] līdzīgi kā Vūters un Fīlds [74] vispārināja Ivanoviča rezultātu.

Teorēma 3.2. *Pieņemsim, ka $p \geq 5$ ir pirmskaitlis. Ortonormētas bāzes*

$$(v_b^{(r)})_\ell = \frac{1}{\sqrt{p^k}} \omega_p^{\mathrm{Tr}((\ell-b)^3 + r(\ell-b))},$$

kur $r, b, \ell \in GF(p^k)$, r ir bāzes indekss, b ir vektora indekss un ℓ ir komponentes indekss, veido MUHu pilno sistēmu telpā $\mathbb{C}^{p^k}$.

Šīs bāzes nedod virknes, kā Altopa konstrukcijā, ja $k > 1$, tā kā ℓ vairs nav vesels skaitlis. Taču katra Adamāra matrica joprojām ir cirkulāra, tikai attiecībā pret $\mathbb{Z}_p^k$.

3.2. Saiknes starp MUBiem un Velča nevienādību

Kā mūsu pirmo pielietojumu Velča nevienādībai priekš MUBiem, mēs izmantosim Velča sākotnēju pieeju jaunajā situācijā. Var viegli pārbaudīt, ka ortonormētu bāžu apvienojums apmierina Velča nevienādību priekš $k = 1$ (ar vienādību). To var pārbaudīt vai nu tiešā veidā izmantojot (3.1), vai arī pielietojot Teorēmu 5.1 tālāk tekstā. Tātad būs jāpielieto Velča nevienādību priekš $k = 2$.

Teorēma 3.3. *Pieņemsim, ka $n \geq 2$ un $B_0, B_1 \ldots, B_n$ ir savstarpēji nenosliektas bāzes telpā $\mathbb{C}^n$. Tad neeksistē neviens vienības vektors, kas būtu nenosliekts attiecībā pret visām šīm bāzēm.*

Pierādījums. Pieņemsim, ka eksistē vektors ψ kas ir nenosliekts pret visiem vektoriem no $B_0, B_1, \ldots, B_n$. Apvienosim visus vektorus no B_i un vektoru ψ vienā vektoru sekvencē $\{x_i\}$ ar izmēru $n(n+1)+1$. Paņemsim $k=2$ un aprēķināsim kreiso nevienādības (3.1) pusi. Katrs no n^2+n+1 vektoriem dod skalāro reizinājumu ar sevi 1; vektori no B_i dod n^2+1 skalārus reizinājumus ar citiem vektoriem pēc moduļa vienādiem ar $\frac{1}{\sqrt{n}}$. Vektors ψ dod n^2+n tādu skalārus reizinājumus ar citiem vektoriem. Saskaitot to visu kopā mēs iegūstam:

$$\binom{n+1}{2}\sum_{i,j}|\langle x_i,x_j\rangle|^4 = \frac{n(n+1)}{2}\left[(n^2+n+1)\cdot 1+(n^2+n)(n^2+2)\cdot\frac{1}{n^2}\right]$$

$$= n^4+2n^3+\frac{5}{2}n^2+\frac{5}{2}n+1.$$

Labajai pusei mēs iegūstam:

$$\left(\sum_i\langle x_i,x_i\rangle^2\right)^2 = (n^2+n+1)^2 > n^4+2n^3+\frac{5}{2}n^2+\frac{5}{2}n+1,$$

ja $n\geq 2$, kas ir prētrunā ar Velča nevienādību priekš $k=2$. ■

Pirmo reizi šis rezultāts tika pierādīts rakstā [74] izmantojot pavisam citu tehniku: attēlojumu $x\mapsto x^*x-I/n$.

Ja mēs izmetīsim vektoru ψ, tad mēs neiegūsim tiešu pretrunu. Tomēr, pat šajā gadījuma Velča nevienādība izrādās noderīga. Lieta ir tāda, ka šajā gadījumā vektoru sistēmu apmierina Velča nevienādību ar vienādību. Īsumā labad tālāk tekstā mēs teiksim, ka vektoru sistēmu $\{x_i\}$ apmierina *Velča vienādību*, ja nevienādība (3.1) izpildās ar vienādību.

Teorēma 3.4. *Pieņemsim, ka $\{B_i\}$ ir $n+1$ ortonormētu bāžu sistēma n-dimensionālajā unitarajā telpā $\mathbb{C}^n$. Apzīmēsim ar X šo bāžu apvienojumu, t.i., vektoru sekvence, kur katrs no tiem parādās tik daudz reižu, cik tas ir sastopams bāzēs $\{B_i\}$. Tad X apmierina Velča vienādību priekš $k=2$ tad un tikai tad, ja $\{B_i\}$ ir pilnā MUBu sistēma.*

Pierādījums. Ja $\{B_i\}$ ir pilnā MUBu sistēma un $X=\{x_i\}$ ir šo bāžu apvienojums, tad līdzīgi skaitot kā iepriekšējas teorēmas pierādījumā, mēs iegūstam:

$$\binom{n+1}{2}\sum_{i,j}|\langle x_i,x_j\rangle|^4 = \frac{n(n+1)}{2}\left[n(n+1)\left(1+n^2\cdot\frac{1}{n^2}\right)\right] = n^2(n+1)^2$$

un

$$\left(\sum_i\langle x_i,x_i\rangle^2\right)^2 = n^2(n+1)^2.$$

Un otrādi, ja X, kas ir ortonormētu bāžu apvienojums, apmierina Velča vienādību priekš $k = 2$, tad $|\langle x, x\rangle|^4 = 1$ visiem $x \in X$, $|\langle x, y\rangle|^4 = 0$ diviem dažādiem vektoriem no vienas un tās pašas bāzes, un, izmantojot nevienādību starp vidējo kvadrātisko un vidējo aritmētisko, iegustam:

$$\sum_{x \in B_i} |\langle x, y\rangle|^4 \geq \frac{1}{n} \left(\sum_{x \in B_i} |\langle x, y\rangle|^2 \right)^2 = \frac{1}{n}.$$

katram vektoram y ar garumu 1. Lai sasniegtu vienādību Velča nevienādībā, šai nevienādībai jāizpildās ar vienādību, kur $y \in B_j \neq B_i$. Šī vienādība tiek sasniegta tikai tad, kad izteiksmei $|\langle x, y\rangle|^2$ ir viena un tā pati vērtība viesiem x no B_i. Un tas nozīmē, ka bāzes $\{B_i\}$ veido MUBu pilno sistēmu. ■

Saistību analīze starp MUBiem un SIC-POVMiem no vienas puses, un kompleksajiem projektīviem 2-dizainiem (kuri tiks definēti nākamajā nodaļā) aizsākās Caunera disertācijā [76]. Šis rezultāts tika noslīpēts Klapenekera un Rotelera darbā [47]. Starp citu, Teorēmas 3.4 "ja" daļa pieder viņiem. Viņi arī pierādīja, ka kopa no $n^2 + n$ vektoriem telpā $\mathbb{C}^n$, kas apmierina Velča vienādību un tāda, ka leņķis starp jebkuriem diviem elementiem ir no $\{0, \frac{1}{n}\}$, ir $n + 1$ MUBu apvienojums. Taču tas nav tieši tas rezultāts, kurā mēs esam ieinteresēti, jo, kā mēs teicām iepriekš, ar leņķi $\frac{1}{n}$ ir diezgan grūti strādāt. Izskatās, ka pirmo reizi Teorēmas "tikai tad" daļa parādās vēlāk, rakstā [60]. Var arī pieminēt Barnuma (**Barnum**) rakstu [8], kur Teorēma 3.4 parādījās pirmo reizi, taču ļoti speciālajā gadījumā.

3.3. Saiknes starp SIC-POVMiem ar Velča nevienādību

Izrādās, ka SIC-POVMi arī apmierina Velča vienādību. Patiesībā, izpildās pat nedaudz spēcīgāks apgalvojums.

Teorēma 3.5. *SIC-POVMa vektori apmierina Velča vienādību priekš $k = 1$ un $k = 2$. Un otrādi, katra telpas $\mathbb{C}^n$ normētu vektoru kopa X, kas apmierina Velča vienādību priekš $k = 2$, sastāv no nemazāk, ka n^2 elementiem, un, ja tā sastāv no n^2 elementiem, tad tas ir SIC-POVMs.*

Pierādījums. Teorēmas pirmo daļu var pierādīt vienkārši saskaitot attiecīgās vērtības. Pieņemsim, ka $\{x_i\}$ ir SIC-POVMs telpā $\mathbb{C}^n$. Tam ir n^2 vektori, katrs no kuriem

dod skalāro reizinājumu 1 pašam ar sevi un n^2-1 skalārus reizinājumus ar absolūto vērtību $\frac{1}{\sqrt{n+1}}$, reizinot ar citiem vektoriem. Saskaitot to visu, mēs dabūsim priekš $k=1$:

$$n\sum_{i,j}|\langle x_i,x_j\rangle|^2 = n\cdot n^2\left(1+(n^2-1)\frac{1}{n+1}\right) = n^4 = \left(\sum_i \langle x_i,x_i\rangle\right)^2.$$

Up priekš $k=2$:

$$\binom{n+1}{2}\sum_{i,j}|\langle x_i,x_j\rangle|^4 = \frac{n(n+1)}{2}n^2\left(1+(n^2-1)\frac{1}{(n+1)^2}\right) = n^4 = \left(\sum_i \langle x_i,x_i\rangle^2\right)^2.$$

Un otrādi, pieņemsim, ka kopa $X=\{x_i\}\subset\mathbb{C}^n$ apmierina Velča vienādību priekš $k=2$ un visiem vektoriem x_i norma ir viens. No Apgalvojuma 4.2 izriet, ka šī kopa apmierina Velča vienādību arī priekš $k=1$. Šīs divas vienādības dod

$$n\sum_{i,j}|\langle x_i,x_j\rangle|^2 = |X|^2 \quad\text{and}\quad \frac{n(n+1)}{2}\sum_{i,j}|\langle x_i,x_j\rangle|^4 = |X|^2.$$

Tādējādi:

$$\sum_{i\neq j}|\langle x_i,x_j\rangle|^2 = \frac{1}{n}|X|^2-|X| \quad\text{un}\quad \sum_{i\neq j}|\langle x_i,x_j\rangle|^4 = \frac{2}{n(n+1)}|X|^2-|X|. \tag{3.2}$$

Izmantojot nevienādību starp aritmētisko un kvadrātisko vidējiem, iegūstam:

$$\frac{2}{n(n+1)}|X|^2-|X| = \sum_{i\neq j}|\langle x_i,x_j\rangle|^4 \geq \frac{1}{|X|(|X|-1)}\left(\sum_{i\neq j}|\langle x_i,x_j\rangle|^2\right)^2 = \frac{(|X|^2-n|X|)^2}{n^2|X|(|X|-1)}. \tag{3.3}$$

No šīs nevienādības seko, ka, ja $|X|\geq n^2$ un $|X|=n^2$, tad nevienādībā (3.3) patiesībā pastāv vienādība. Tas ir iespējams tikai, ja visi $|\langle x_i,x_j\rangle|$ ir vienādi priekš $i\neq j$. Tad no (3.2) ir viegli dabūt, ka šie skalārie reizinājumi pēc absolūtas vērtības ir vienādi ar $\frac{1}{\sqrt{n+1}}$. ■

Piezīme 3.6. Šis pierādījums ir dots pēc līdzīga pierādījuma no [58] motīviem. Patiesībā, šis rezultāts izpildās arī ja mēs nepieprasīsim, ka katrs elements no X ar vienības normu. Šajā gadījumā, ja X ir kopa, kas apmierina Velča vienādību priekš $k=2$ ar n^2 elementiem, tad tā ir SIC-POVMa skalārais daudzkārtnis [64].

4. nodaļa

Dizaini

Iepriekšējā nodaļā mēs redzējām, ka vektori no MUBu pilnās sistēmas un SIC-POVMa apmierina Velča vienādības priekš $k = 1$ un $k = 2$. Patiesībā daudzos rakstos tādas sistēmas, kas apmierina Velča vienādības priekš $k = t$, sauc par *kompleksiem projektīviem t-dizainiem* (**complex projective t-design**). Šī iemesla dēļ ir vērts iepazīties ar šo jēdzienu, kā arī ar vispārīgāku dizaina jēdzienu. Turklāt tas arī dod papildu pielietojumus objektiem, kurus mēs pētām šajā darbā.

4.1. Dizaina definīcija un piemēri

Terminam "dizains" ir vairākas nozīmes dažādos matemātikas novirzienos, bet daudziem no tiem ir kopīgā īpašība: tie aizvieto lielāko objektu A ar to mazāku apakšobjektu B tā, ka kaut kādā veidā šie objekti kļūst par ekvivalentiem. Parasti gan lielais, gan mazais objekti ir telpas ar mēru, un ekvivalenti tie ir tādā ziņā, ka, integrējot funkcijas no zināmās klases (teiksim, polinomus ar nelielu pakāpi), iznākums abiem objektiem sakrīt.

Mēs nodarbosimies tikai ar kompaktām telpām un tikai ar nepārtrauktām funkcijām, tādēļ *telpu ar mēru* ir viegli definēt. Mūsu gadījumā tā ir kompakta topoloģiska telpa X kopā ar nepārtrauktu lineāru attēlojumu

$$\mu : f \mapsto \int_X f(x)\, d\mu(x),$$

ko sauc pār *mēru*, un kas darbojas no nepārtrauktu reālu funkciju kopas virs X reālo skaitļu kopā [16].

Ja telpa X vienlaicīgi ir topoloģiskā grupa, tad var definēt vienu īpašu mēru, ko sauc par Hāra (**Haar**) mēru. *(Kreisais) Hāra mērs* ir nenulles mērs μ, kas ir invariants

attiecībā pret X elementu pielietojumu, t.i.:

$$\int_X f(x)d\mu(x) = \int_X f(gx)d\mu(x)$$

visiem elementiem $g \in X$ un visām nepārtrauktām funkcijām f. Hāra mērs eksistē un ir viens vienīgs ar precizitāti līdz reizinājumam ar konstanti. Kompaktu telpu gadījumā parasti izvēlas tādu mēru μ, ka integrālis pa visu telpu X ir vienāds ar 1.

Aplūkosim dažus dizainu piemērus:

Kvadratūras formulas Pieņemsim, ka A ir telpa $[-1,1]$ ar parasto Lebega (**Lebesgue**) mēru dx, t.i., nepārtraukta funkcija f tiek attēlota uz $\int_{-1}^{1} f(x)\,dx$, kur $\int$ ir parastais Rīmaņa (**Riemann**) integrālis. Telpa B, savukārt, ir galīga, un sastāv no viena vienīga punkta $B = \{0\}$, un mērs μ attēlo funkciju f uz divkāršotu šīs funkcijas vērtību punktā 0: $f \overset{\mu}{\mapsto} 2f(0)$. To parasti izsaka ar frāzi, ka mēra μ *svars* punktā 0 ir 2.

Ja $f : [-1,1] \to \mathbb{R}$ ir patvaļīga lineāra funkcija, tad izpildās vienādība:

$$\int_{-1}^{1} f(x)dx = 2f(0) \quad \left(= \int_B f(x)d\mu(x)\right).$$

Ja mēs izvēlēsimies apakštelpu $B' = \{-1, 0, 1\}$ ar mēru μ', kura svars punktos -1 un 1 ir 1/3 un svars punktā 0 ir 4/3, mēs iegūsim sekojošu sakarību:

$$\int_{-1}^{1} f(x)dx = \frac{1}{3}f(-1) + \frac{4}{3}f(0) + \frac{1}{3}f(1) \quad \left(= \int_{B'} f(x)d\mu'\right),$$

kas izpildās jau visiem polinomiem f ar pakāpi, ne lielāku par 3.

Tamlīdzīgas formulas sauc par *kvadratūras formulām*. Tās aizstāj funkcijas integrāļa aprēķināšanu ar izteiksmes aprēķināšanu, kas satur tikai galīgu funkcijas vērtību skaitu. Pirmo sauc par *taisnstūru formulu* un otro — par *Simpsona* (**Simpson**), vai *parabolu* formulu. Šīs funkcijas ir ārkārtīgi noderīgas skaitliskajā integrēšanā. Ideja ir tāda, ka, kaut gan šīs vienādības, vispār runājot, neizpildās patvaļīgām funkcijām, patvaļīgu, samērā gludu funkciju pietiekoši īsā intervālā var diezgan labi aproksimēt ar nelielas pakāpes polinomu, kuram formula jau būs precīza. Kvadratūras formulas, kas izmanto šo pieeju, sauc par *interpolācijas kvadratūras formulām*. Tas nozīmē, ka patvaļīgai funkcijai formula dos kļūdu, bet šī kļūda parasti būs neliela. Intuitīvi, jo lielākas pakāpes polinomiem izpildās vienādība tamlīdzīgajā formulā, jo mazāka būs kļūda. Tādēļ, Simpsona formula ir piemērotāka skaitlisko integrāļu rēķināšanai, nekā taisnstūru formula.

Klasiskie Dizaini Par klasisko t-(v,k,λ)-dizainu [11] sauc pāri (V,U), kur V ir galīga *punktu* kopa un U ir *bloku* kopa, kas apmierina sekojošas prasības: V izmērs ir v, katrs

bloks ir V apakškopa un tā izmērs ir k, un katra V apakškopa ar izmēru t ieiet kā apakškopa tieši λ blokos no U.

Lai parādītu, kā tas saskan ar iepriekšējo piemēru, aplūkosim daudzu mainīgo polinomus $f : \mathbb{R}^v \to \mathbb{R}$ ar pakāpi, ne lielāku par t. Definēsim A kā visu to $\{0,1\}$-virkņu garumā v kopu, kas satur tieši k vieniniekus. Apveltīsim A ar homogēnu mēru μ ar kopējo svaru 1 (tas ir, katrs A elements ir ar svaru $\binom{v}{k}^{-1}$). Ja sanumurē V elementus, tad katru A elementu var uzskatīt kā k-apakškopas no V raksturīgo virkni. Uzbūvēsim B no visiem A elementiem, kas atbilst U elementu raksturīgajām virknēm. Apveltīsim arī to ar vienmērīgu mēru ν ar kopējo svaru 1. Tad var pierādīt [67], ka

$$\int_A f(x)d\mu = \int_B f(x)d\nu$$

visiem polinomiem ar pakāpi, kas nepārsniedz t.

Sfēriskie Dizaini Šajā gadījumā pieņemsim, ka telpa A ir vienības sfēra reālā vektoru telpā $\mathbb{R}^n$. Un σ ir šīs sfēras virsmas laukuma mērs. Tad, līdzīgi, kā iepriekšējos gadījumos, par *sfērisku t-dizainu* sauc tādu galīgu kopas A apakškopu B kopā ar funkciju $p : B \to [0,1]$, ka

$$\frac{1}{\sigma(A)} \int_A f(x)d\sigma(x) = \sum_{x \in B} p(x)f(x)$$

visām funkcijām f no kādas klases. Dažās definīcijās šī klase ir visi polinomi ar pakāpi, ne lielāku par t, citās šī klase ir visi homogēnie polinomi ar pakāpi t. Pēc būtības abas šīs definīcijas sakrīt. Turklāt parasti tiek pieņemts, ka visi svari $p(x)$ ir vienādi ar $\frac{1}{|B|}$. Vienu no piemēriem dod ikosaedra divpadsmit virsotnes, kuras veido sfērisku 5-dizainu telpā $\mathbb{R}^3$ [68].

Par šīs nozares pamatus likušo rakstu parasti uzskata [23], kaut gan šī problēma tika aplūkota arī agrāk. Piemēram, jau pieminētā grāmata [49] satur nodaļu, kas veltīta šim tematam.

4.2. Kvantu dizaini

Šajā sadaļā mēs aplūkosim dizainus, kas ir interesanti no kvantu informācijas teorijas viedokļa.

4.2.1. Kompleksie projektīvie dizaini

Ir labi zināms, ka kvantu stāvokļus apraksta ar punktiem kompleksajā sfērā $\mathbb{C}S^{n-1}$, kas ir sfēra unitārajā telpā $\mathbb{C}^n$ ar rādiusu 1 un centru koordināšu sākumpunktā. Bet īstenībā, kvantu stāvokļi, kas atšķiras tikai ar fāzi, ir neatšķirami savā starpā, tādēļ ir vērts ievest ekvivalences attiecību kopā $\mathbb{C}S^{n-1}$, uzskatot, ka divi vektori $x, y \in \mathbb{C}S^{n-1}$ ir ekvivalenti ($x \equiv y$), ja eksistē tāds skalārs $\alpha \in \mathbb{C}$, ka $x = \alpha y$. Ekvivalences klase izgriež riņķi sfērā $\mathbb{C}S^{n-1}$. Faktorizējot pēc šīs attiecības, mēs iegūstam *komplekso projektīvo telpu* $\mathbb{C}P^{n-1} = \mathbb{C}S^{n-1}/\equiv$. Skaidrs, ka mēs iegūstam to pašu telpu, faktorizējot pēc tās pašas attiecības visu nenulles vektoru kopu $\mathbb{C}P^{n-1} = (\mathbb{C}^n \setminus \{0\})/\equiv$. Šajā gadījumā ekvivalences klases ir 1-dimensionālas telpas $\mathbb{C}^n$ apakštelpas. Tas ir vispārpieņemts veids, kā definēt projektīvu telpu.

Tā kā katrs unitārs operators telpā $\mathbb{C}^n$ transformē 1-dimensionālu apakštelpu 1-dimensionālā apakštelpā, mēs varam uzskatīt, ka unitārie operatori darbojas telpā $\mathbb{C}P^{n-1}$. Eksistē viens vienīgs normalizēts mērs μ telpā $\mathbb{C}P^{n-1}$, kas paliek invariants visu unitāru operatoru iedarbībā. Šo mēru sauc par *Fubini-Stadi mēru* (**Fubini-Study**). Kaut gan tas neatbilst Hāra mēra klasiskai definīcijai, to bieži sauc arī par Hāra mēru šajā telpā. Katrai nepārtrauktai funkcijai $f : \mathbb{C}P^{n-1} \to \mathbb{R}$ tas var tikt definēts kā

$$\int_{\mathbb{C}P^{n-1}} f(x) d\mu(x) = \frac{1}{\sigma(\mathbb{C}S^{n-1})} \int_{\mathbb{C}S^{n-1}} \tilde{f}(y) d\sigma(y)$$

kur σ ir $(n-1)$-dimensionālais laukums uz $\mathbb{C}S^{n-1}$ un $\tilde{f} : \mathbb{C}S^{n-1} \to \mathbb{R}$ ir funkcija, vienāda ar $f(x)$ visos punktos no $\mathbb{C}S^{n-1} \cap x$.

Aplūkosim visus polinomus $f(x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n)$ ar kompleksiem koeficientiem, kuri ir homogēni mainīgajos $x_1, x_2 \ldots, x_n$ ar pakāpi t un homogēni mainīgajos $y_1, y_2, \ldots, y_n$ ar to pašu pakāpi. Mēs apzīmēsim šo kopu ar $\hom(t, t)$. Definēsim šī polinoma vērtību uz $x \in \mathbb{C}P^{n-1}$ ar $f_\circ(x) = f(x_\circ, \bar{x}_\circ)$, kur $x_\circ$ ir patvaļīgs punkts no x. Tā ir korekta definīcija, jo šī vērtība nav atkarīga no $x_\circ$ izvēles.

Tad, līdzīgi, kā sfērisko dizainu gadījumā, var definēt *komplekso projektīvo t-dizainu* kā tādu galīgu $\mathbb{C}P^{n-1}$ apakškopu ar mēru, ka, integrējot jebkuru polinomu no $\hom(t, t)$ pa visu $\mathbb{C}P^{n-1}$ ar Fubini-Stadi mēru vai pa t-dizainu, rezultāti sakrīt. Ja dizainu veidojošais mērs ir vienmērīgs, dizainu sauc par *nesvērtu* (**unweighted**), citādi to sauc par *svērtu* (**weighted**). Nesvērtais gadījums ir izplatītāks. Tā definēti, kompleksie projektīvie t-dizaini pirmo reizi tika aplūkoti darbā [54] kā sfērisko dizainu vispārinājums.

Sekojošais rezultāts izskaidro, kāpēc kompleksie projektīvie t-dizaini ietilpst mūsu darba tematikā.

Teorēma 4.1. *Galīga kopa ar mēru* (X, p), $X \subset \mathbb{C}P^{n-1}$, $p : X \to [0, 1]$ *ir svērts kompleksais projektīvais* t*-dizains tad un tikai tad, ja kopa* $\{ \sqrt[2t]{p(x)}x_\circ \mid x \in X\} \in \mathbb{C}^n$ *apmierina Velča vienādību priekš* $k = t$*, kur* $x_\circ$ *ir patvaļīgs vektors no* $\mathbb{C}S^{n-1} \cap x$*.*

Sekojošais rezultāts arī ir interesants un to ir vieglāk formulēt (un pierādīt) dizainu terminoloģijā:

Apgalvojums 4.2. *Jebkurš svērts kompleksais projektīvais* t*-dizains ir arī kompleksais projektīvais* $(t-1)$*-dizains.*

Šo divu rezultātu pierādījumus var atrast, piemērām, darbā [64].

Var redzēt, ka nesvērtie kompleksie projektīvie t-dizaini ir tieši normētu vektoru kopas, kuras apmierina Velča vienādību priekš $k = t$ (normalizācijas reizinātāju $\sqrt[2t]{p(x)}$ var, acīmredzot, izlaist). Svērto t-dizainu gadījums ir nedaudz sarežģītāks. Normalizācijas reizinātājs $\sqrt[2t]{p(x)}$ ir atkarīgs no t un, cita starpā, tas nozīmē arī to, ka no Apgalvojuma 4.2 nevar izsecināt, ka, ja $X \subset \mathbb{C}^n$ apmierina Velča vienādību priekš $k = t$, tad tas apmierina to arī priekš $k = t-1$. Lai dabūtu līdzīgu rezultātu, vektori jāpārnormalizē atbilstoši Teorēmas 4.1 prasībām. No šī skatpunkta, svērtie kompleksie t-dizaini ir dabiskāks jēdziens, taču nesvērto dizainu gadījumā šī atšķirība pazūd. Mēs šajā darbā nodarbosimies vairāk ar nesvērtiem dizainiem.

Kompleksus projektīvus t-dizainus var pielietot, kā tas izriet no definīcijas, aizstājot nejaušu stāvokli, paņemtu pēc Fubini-Stadi mēra, ar stāvokli, nejauši paņemtu no dizaina (skat., piemēram, [4]). Tā kā uzģenerēt nejaušo stāvokli pēc Fubini-Stadi mēra nav viegli, šādi varam iegūt tam labu aizstājēju. Cits pielietojums, kurā mēs esam vairāk ieinteresēti, ir kvantu mērījumos. Piemēram, var pierādīt (Apgalvojums 5.2), ka kompleksie projektīvie 1-dizaini pēc būtības ir nekas cits kā POVMi. Kompleksie projektīvie 2-dizaini veido "labus" POVMus, tādus kā MUBi un SIC-POVMi.

Kompleksie projektīvie t-dizaini ir labi izpētīts objekts, tādēļ ir vērts ar to iepazīties, īpaši no Teorēmas 4.1 viedokļa. Mums vairāk patīk strādāt ar Velča vienādību tāpēc, ka arī tā ir labi (iespējams, arī labāk) zināms jēdziens, it īpaši inženieru literatūrā. Otrkārt, tas ir elementārāks, jo neprasa zināšanas no mēru teorijas un ir adekvāts mūsu pielietojumiem. Turklāt parasti ir grūti pierādīt, ka vektoru sistēma veido kompleksu projektīvu t-dizainu, izejot no tā definīcijas, un parastais veids, kā tas tiek izdarīts, ir tieši ar Velča vienādību (skat., piemēram, [47]).

4.2.2. Unitārie dizaini

Pilnības dēļ mēs arī pieminēsim unitāros t-dizainus (**unitary t-designs**). Ja kvantu stāvokļi ir aprakstāmi ar punktiem kompleksajā projektīvajā telpā, operācijas ar kvantu stāvokļiem, kas neiesaista ārpasauli, ir aprakstāmas ar unitāriem operatoriem. Aplūkosim unitāro grupu $\mathrm{U}(n)/\mathrm{I}(n)$ kopā ar Hāra mēru uz tās.

Tad (projektīvs) unitārs t-dizains [22, 65] ir tāda galīga unitāru operatoru kopa X ar svariem p, ka

$$\int_{\mathrm{U}(n)/\mathrm{I}(n)} f(U)d\mu(U) = \sum_{U\in X} p(U)f(U)$$

visiem polinomiem f no matricas U elementiem un to kompleksi saistītajiem, kas ir homogēni ar pakāpi t gan pēc elementiem, gan pēc to kompleksi saistītajiem (līdzīgi, kā kompleksiem projektīviem dizainiem).

Unitārie dizaini ir noderīgi, derandomizējot kvantu algoritmus, kuri savā sākotnējā analīzē izmanto nejauši un vienmērīgi izvēlētu unitāru operāciju. Rakstā [22] ir pieminēti vairāki tamlīdzīgi pielietojumi.

Viens no ilustratīvākiem unitāro dizainu pielietojumiem ir kvantu kriptogrāfija. Iedomāsimies, ka viena persona grib aizsūtīt otrai kvantu stāvokli tā, lai, ja kāds ļaundaris pārķertu šo stāvokli, tad viņš nevarētu neko uzzināt par pārsūtāmo stāvokli. Lai to panāktu, abām pusēm ir pieejama slepena nejauši uzģenerēta bitu virkne — atslēga.

Klasiskajā gadījumā to var panākt ar *Vernama šifru* (**Vernam**) jeb *vienreizējo bloknotu* (**one-time pad**). Gadījumā, kad jāpārsūta n-bitu garš ziņojums M un slepenā atslēga K arī ir vismaz n bitu gara, tad ziņojumu var nošifrēt, paņemot izslēdzošo vai ar atslēgu: $C = M \oplus K$. Saņēmējs varēs to atšifrēt, pielietojot atslēgu vēlreiz: $M = C \oplus K$. Šenons (**Shannon**) bija pirmais, kas pierādīja, ka šī shēma ir pilnīgi droša un ka ar mazāka bitu skaita atslēgu pilnīgu drošību panākt nav iespējams [62].

Kvantu gadījumā var pielietot līdzīgu ideju [3, 17]. Ja paņem unitāru matricu U nejauši attiecībā pret Hāra mēru un pielieto to stāvoklim ρ, tad rezultātā iznāk pilnībā jauktais stāvoklis

$$\rho \mapsto \int_{\mathrm{U}(n)} U\rho U^* d\mu(U) = \frac{I}{n}, \tag{4.1}$$

neatkarīgi no stāvokļa ρ. To var viegli pārbaudīt, jo, pirmkārt, šīs attēlojums saglabā operatora pēdu un, otrkārt, rezultāts paliek invariants visu unitāro operatoru iedarbībā.

Bet nav iespējams iekodēt patvaļīgu unitāru operatoru ar galīgu bitu skaitu, kas veido slepeno atslēgu. Atrisināt šo problēmu palīdz unitārie 1-dizaini, jo tieši tas, ka tie nav atšķirami no Hāra mēra (4.1)-līdzīgos attēlojumos, veido unitāro 1-dizainu prasības.

Nav grūti pārbaudīt, ka jebkura ortogonāla unitāru operatoru bāze Ermita operatoru telpā veido unitāru 1-dizainu. Piemēram, vispārinātā Pauli grupa $\mathrm{GP}(n)$ veido unitāru 1-dizainu. Mazliet sarežģītāk ir pierādīt, ka Kliforda grupa $\mathrm{C}(n)$ veido unitāru 2-dizainu [22].

Arī unitāros 2-dizainus var pielietot šifrēšanas uzdevumā. Lieta ir tāda, ka iepriekš aprakstītās sistēmas, kaut arī skaitās "pilnīgi drošas", neatrisina visas iespējamas problēmas. Pieņemsim, ka mēs lietojam Vernama šifru. Kaut arī ļaundaris nevar iemācīties neko par pārsūtāmo ziņojumu, izņemot tā garumu, viņš tam var pielietot noteiktu operāciju, neatšifrējot to. Piemēram, paņemot nošifrēto ziņojumu, veicot izslēdzošo vai ar kādu bitu virkni un aizsūtot rezultātu tālāk, viņš, tādējādi, pielieto to pašu operāciju arī sākotnējiem, nenošifrētiem datiem. Līdzīgi var ietekmēt arī kvantu stāvokli, nošifrētu ar unitāru 1-dizainu. Dažreiz tas nav vēlams. Šo problēmu atrisina *izmaiņu-droša šifrēšana* (**tamper-resistant encryption**). Izrādās, ka, aizvietojot iepriekšējā shēmā unitāro 1-dizainu ar unitāro 2-dizainu, var dabūt tieši tādu shēmu [5].

Līdzīgi kā kompleksos projektīvos dizainus, arī unitāros dizainus var pielietot kvantu tomogrāfijā. Šoreiz kvantu procesu tomogrāfijā [65].

5. nodaļa

Kritērijs

Šajā nodaļā mēs definēsim kritēriju, kad vektoru kopa ir ekstremāla priekš Velča nevienādības un pielietosim to MUBiem un SIC-POVMiem. Tālāk mēs definēsim šo divu objektu speciālo gadījumu — homogēnas sistēmas, kurām šis kritērijs ir vispiemērotākais. Lai uzdotu homogēnu MUBU sistēmu vai SIC-POVMu telpā $\mathbb{C}^n$ pietiek ar divām $n \times n$-matricām. Abām šīm matricām var definēt L-grafu, kas apraksta, cik piemērota ir šī matrica homogēnu sistēmu uzbūvēšanai. Mēs parādīsim, ka Furjē matricām ir ļoti labi (savā ziņā labākie) L-grafi. Tas, līdz zināmai robežai, izskaidro, kāpēc Furjē matricas tiek pielietotas MUBu un SIC-POVMu konstruēšanā.

5.1. Vienādības sasniegšana Velča nevienādībā

No sākuma mēs dosim Velča nevienādības pierādījumu, tad formulēsim nosacījumus, kad patiesībā izpildās vienādība.

Teorēmas 3.1 pierādījums. Konstruēsim *Grama* (**Gram**) matricu $G = (a_{ij})$, kur $a_{ij} = \langle x_i, x_j \rangle$ un aplūkosim tās k-to Adamāra pakāpi $G^{(k)}$ (kur k ir naturāls skaitlis).

Atgādināsim, ka matricas *Eiklīda normu* (**Euclidean norm**) (skat., [43] 5. nodaļa, arī ir zināma, ka *Frobeniusa* (**Frobenius**) norma) definē ar $\|A\|_E = \sqrt{\mathrm{Tr}(A^*A)}$. Tā ir vienāda ar Eiklīda normu vektoram, kas veidots no visiem matricas elementiem. Var viegli redzēt, ka reizinot matricu ar unitāru matricu no kreisās vai labās puses, matricas norma nemainās. Tātad, izmantojot matricas singulāro dekompozīciju, var dabūt, ka $\|A\|_E$ ir vienāda ar $\sqrt{\sum_i \sigma_i^2}$, kur $\{\sigma_i\}$ ir matricas A singulāras vērtības. Ermīta matricām tie, protams, sakrīt ar īpašvērtību absolūtām vērtībām.

Pielietojot to matricai G, iegūstām, ka tās Eiklīda normas kvadrāts ir vienāds ar

$$\left(\|G^{(k)}\|_E\right)^2 = \sum_{i,j} |\langle x_i, x_j\rangle|^{2k} = \sum_{\lambda\in\sigma(G^{(k)})} \lambda^2, \tag{5.1}$$

kur σ ir spektrs (matricas īpašvērtību multikopa). Izmantojot nevienādību starp kvadrātisko un aritmētisko vidējo, mēs iegūstam (atgādināsim, ka matricas rangs ir vienāds ar tās nenulles īpašvērtību skaitu):

$$\sum_{\lambda\in\sigma(G^{(k)})} \lambda^2 \geq \frac{1}{\operatorname{rank}(G^{(k)})}(\operatorname{Tr} G^{(k)})^2 \geq \frac{1}{\binom{n+k-1}{k}} \left(\sum_i \langle x_i, x_i\rangle^k\right)^2. \tag{5.2}$$

Izmantoto novērtējumu uz matricas $G^{(k)}$ rangu mēs dosim Teorēmas 5.1 pierādījumā. ■

Teorēma 5.1. *Pieņemsim, ka B ir matrica un $X \subset \mathbb{C}^n$ ir tās kolonnu virkne. Apzīmēsim ar $w_1, w_2, \ldots, w_n$ tās rindas. Tad X sasniedz Velča vienādību priekš fiksēta k tad un tikai tad, ja visi vektori no*

$$W = \left\{ \sqrt{\binom{k}{k_1,\ldots,k_n}} w_1^{(k_1)} \circ w_2^{(k_2)} \circ \cdots \circ w_n^{(k_n)} \mid k_i \in \mathbb{N}_0, k_1 + \cdots + k_n = k \right\}$$

ir ar vienādu garumu un savstarpēji perpendikulāri.

Citiem vārdiem, katrs kopas W vektors ir k-multikopas no B Adamāra reizinājums ar koeficientu, kas ir vienāds ar attiecīgā multinomināla koeficienta

$$\binom{k}{k_1,\ldots,k_n} = \frac{k!}{k_1!k_2!\cdots k_n!}$$

kvadrātsakni.

Pierādījums. Sākumam, atzīmēsim, ka matrica G formulā (5.1) ir vienāda ar B^*B. Tātad, ja katru w_i uzskatīt par rindas vektoru:

$$G = w_1^* w_1 + w_2^* w_2 \cdots + w_n^* w_n.$$

Pielietojot formulu summas pakāpei, iegūstam:

$$G^{(k)} = \sum_{k_1+\cdots+k_n=k} \binom{k}{k_1,\ldots,k_n} \left(w_1^{(k_1)} \circ \cdots \circ w_n^{(k_n)}\right)^* \left(w_1^{(k_1)} \circ \cdots \circ w_n^{(k_n)}\right).$$

Citiem vārdiem, $G^{(k)} = C^*C$, kur matricas C rindas ir tieši vektori no W. Tas arī dod novērtējumu matricas $G^{(k)}$ rangam, kas tika lietots formulā (5.2), tā kā kopai ar n elementiem ir tieši $\binom{n+k-1}{k}$ apakšmultikopas ar izmēru n ([70], Nodaļa 1.2).

Aplūkojot nevienādību starp (5.1) un (5.2), redzam, ka multikopa X apmierina Velča vienādību fiksētam k tad un tikai tad, ja matricai $G^{(k)}$ ir $\binom{n+k-1}{k}$ vienādas nenulles

īpašvērtības (visas pārējās īpašvērtības ir vienādas ar nulli, kas seko no ranga novērtējuma).

Ir labi zināms, ka jebkurām divām matricām P un Q, nenulles īpašvērtību multikopa matricām PQ un QP ir vienādas, ja šo matricu reizinājumi ir definēti ([43], Nodaļa 1.3). Tātad matricai CC^* ir $\binom{n+k-1}{k}$ vienādas nenulles īpašvērtības, un tā kā tā ir Ermita matrica ar tādu pašu izmēru, tad tā ir vienības matricas skalārais daudzkārtnis. Un pēdējais ir ekvivalents ar nosacījumiem uz kopu W. ■

Mēs neesam redzējuši Teorēmu 3.1 un 5.1 pāru formulējumu tādā vispārīgā formā, taču visas idejas no pierādījuma parādījās arī agrāk. Kā jau tika teikts, Velčs bija pirmais, kas pierādīja nevienādību (3.1) gadījumā, kad visiem vektoriem norma ir viens un k ir patvaļīgs [73]. Teorēmas 5.1 variants, kur $k = 1$ un visi vektori ir ar vienādu garumu pirmo reizi parādījās rakstā [52]. Mūsu pierādījums ir eleganta pierādījuma no [72] vispārinājums. Pēdējā rakstā Velča nevienādība ir formulēta dažādu garumu vektoru gadījumā, taču tas ierobežojas tikai ar gadījumu $k = 1$. Atzīmēsim arī, ka kompleksa projektīva dizaina definīcijai no [64] arī ir daudz kopīga ar mūsu kritēriju.

Vektoru $\{x_i\}$ sistēmu no $\mathbb{C}^n$ sauc par *ciešo rāmi* (**tight frame**), ja $\sum_i x_i x_i^* = aI$ kādam $a \in \mathbb{R}$. Ņemot abu pušu pēdu, kļūst skaidrs, ka a jābūt vienādam ar $\frac{1}{n}\sum_i \|x_i\|^2$. Patiesībā, mēs esam redzējuši šo objektu iepriekš: kopa $\{\frac{1}{a}x_i x_i^*\}$ ir POVMs, kas sastāv no projektoriem ar rangu 1.

Apgalvojums 5.2. *Vektoru kopa $\{x_i\} \subset \mathbb{C}^n$, kas apmierina Velča nevienādību priekš $k = 1$ ir ciešais rāmis.*

Pierādījums. Izmantojot Teorēmas 5.1 apzīmējumus, iegūstam, ka $CC^* = BB^* = aI$ kādam $a \in \mathbb{R}$. Atliek tikai pamanīt, ka $BB^* = \sum_i x_i x_i^*$. ■

No šī apgalvojuma un Teorēmas 3.5 var dabūt sekojošas sekas, kuras mēs iepriekš apsolījām pierādīt:

Secinājums 5.3. *Ja $\{x_i\}$ ir SIC-POVMs telpā $\mathbb{C}^n$, tad $\{\frac{1}{n}x_i x_i^*\}$ ir POVMs.*

5.2. Kritērija pielietojums MUBu sistēmām

Pirmkārt, dosim sekojošu vieglu Teorēmas 5.1 secinājumu:

Secinājums 5.4. *Pieņemsim, ka B ir matrica un $X \subset \mathbb{C}^n$ ir tās kolonnu kopa. Apzīmēsim ar $w_1, w_2, \ldots, w_n$ matricas rindas. Tad X sasniedz Velča vienādību priekš $k = 2$ tad un tikai tad, ja visi vektori no $W = \{w_i^{(2)}\} \cup \{\sqrt{2} w_i \circ w_j \mid \ 1 \leq i < j \leq n\}$ ir*

- *ar vienādu garumu (garumu nosacījums) un*
- *savstarpēji ortogonāli (ortogonalitātes nosacījums).*

Tagad mēs esam spējīgi pierādīt sekojošu teorēmu:

Teorēma 5.5. *Pieņemsim, ka $\{B_i\}$ $(i = 1, 2 \ldots, n)$ ir n Adamāra matricu kolekcija telpā $\mathbb{C}^n$ un B ir šo matricu konkatenācija, t.i., $n \times n^2$-matrica ar visām kolonnām, kas parādās matricās $\{B_i\}$). Tad $\{B_i\}$ veido MUHu pilno sistēmu tajā un tikai tajā gadījumā, kad visi vektori no $W' = \{w_i \circ w_j \mid \ 1 \leq i \leq j \leq n\}$ ir savstarpēji ortogonāli, kur $\{w_i\}$ ir matricas B rindas.*

Pierādījums. Apzīmēsim $n \times n$ vienības matricu ar B_0. Tad no Teorēmas 3.4 seko, ka kopa $\{B_0, B_1, \ldots, B_n\}$ ir pilnā MUBu sistēma tad un tikai tad, ja šo matricu kolonnu kopa sasniedz Velča vienādību priekš $k = 2$. Tagad, ņemot vērā Secinājumu 5.4, atliek pierādīt, ka vektori no W, ka tie definēti Secinājuma 5.4, ir ar vienādu garumu un ortogonāli, ja vektori no W' ir ortogonāli.

Ja vektors no kopas W tiek reizināts ar sevi, izmantojot Adamāra reizinājumu, tad rezultāts saturēs

- daļā, kas atbilst B_0: vienu vieninieku, un visas pārējās komponentes — nulles;
- visur citur: katras komponentes absolūtā vērtība ir vienāda ar $\frac{1}{n}$.

Tātad vektora garums ir $\sqrt{1 + n^2 \frac{1}{n^2}} = \sqrt{2}$.

Ja divi dažādi vektori tiek reizināti ar Adamāra reizinājumu, tad rezultāts saturēs tikai nulles daļā, kas atbilst B_0 matricai, un tā garums būs $\sqrt{n^2 \frac{1}{n^2}} = 1$. Tātad, garumu nosacījums no Secinājuma 5.4 ir apmierināts.

Turklāt, B_0 daļa dod nulli divu dažādu vektoru no W skalārajam reizinājumam, tātad vektori no W ir savstarpēji ortogonāli tad un tikai tad, ja vektori no W' ir savstarpēji ortogonāli. ■

Iepriekšējo teorēmu var pārfrāzēt. Pieņemsim, ka B ir plakana $n \times n$-matrica. Konstruēsim grafu $K(B)$ ar svariem sekojošajā veidā. Tā virsotnes ir visi nesakārtoti pāri no $\{1, ..., n\}$, pāris var saturēt divus vienādus elementus. Semantiski, virsotne $\{i, j\}$ apzīmē

i-tās un j-tās matricas B rindiņu Adamāra reizinājumu. Šķautnes svars ir skalārais reizinājums no diviem vektoriem, kuri atbilst virsotnēm, ko savieno šī šķautne (tā definēts, svars ir atkarīgs no virsotņu secības, bet mēs pieņemsim, ka visām šķautnēm šī secība ir kaut kā izvēlēta). Tad Teorēmu 5.5 var pārformulēt, pasakot, ka Adamāra matricas $B_1, \ldots, B_n$ veido MUHu pilno sistēmu tad un tikai tad, ja katrai šķautnei tai piekārtoto svaru summa grafos $K(B_1), \ldots, K(B_n)$ ir vienāda ar nulli. Patiesībā nav jēgas aplūkot šķautnes starp virsotnēm, kurām sakrīt viena rindiņa, jo tām būs svars 0 visos grafos $K(B_i)$.

Šīs kritērijs izskatās diezgan komplicēts, taču nākamajā sadaļā mēs definēsim MUHu speciālo gadījumu, kuram šīs kritērijs stipri vienkāršosies.

5.3. Homogēnas sistēmas

Šajā nodaļā mēs dosim MUHu un SIC-POVMu speciālgadījumu, kuram kritēriju no Secinājuma 5.4 var stipri vienkāršot. SIC-POVMiem šī konstrukcija ir grupu kovarianta SIC-POVMa vispārinājums. Pēdējo mēs aplūkojām Nodaļā 2.2.1..

Pieņemsim mums ir divas $n \times n$-matricas $A = (a_{i,j})$ un $B = (b_{i,j})$. Aplūkosim sekojošu matricu sistēmu:

$$(v_k^{(r)})_\ell = a_{\ell,r} b_{\ell,k}, \tag{5.3}$$

kur r ir matricas indekss, k ir kolonnas indekss un ℓ ir rindas indekss ($r, k, \ell \in \{1, \ldots, n\}$). Citiem vārdiem, sistēmas i-tā matrica ir $\mathrm{diag}(v_i)B$, kur v_i ir matricas A i-tā kolonna. Tādu matricu sistēmu mēs sauksim par *homogēnu sistēmu*. MUHu gadījumā katra matrica ir Adamāra matrica. SIC-POVMu gadījumā katra matrica ir n SIC-POVMa elementu apvienojums, kur katrs vektors ir matricas kolonna. Šis nosaukums ir paņemts no [12], kur MUHu sistēma, kas uzbūvēta no ekvivalentām Adamāra matricām tiek saukta par MUHu homogēnām sistēmām.

Var pamanīt, ka MUHu sistēmas, kuras mēs definējām Teorēmā 2.2, visas ir homogēnas, kā arī grupu kovarianti SIC-POVMi. Visos tajos viena no matricām A, B ir Furjē matrica. Tas dod motivāciju šo sistēmu izpētei.

Pielietosim tagad Secinājuma 5.4 rezultātu. Aizmirsīsim uz mirkli par garumu nosacījumu, un aplūkosim ortogonalitātes nosacījumu. No tā izriet, ka

$$\langle w_{\ell_1} \circ w_{\ell_2}, w_{\ell_3} \circ w_{\ell_4} \rangle = \frac{1}{n} \sum_{r,k} \overline{a_{\ell_1,r} b_{\ell_1,k} a_{\ell_2,r} b_{\ell_2,k}} a_{\ell_3,r} b_{\ell_3,k} a_{\ell_4,r} b_{\ell_4,k} =$$

$$= \frac{1}{n}\left(\sum_r \overline{a_{\ell_1,r}a_{\ell_2,r}}a_{\ell_3,r}a_{\ell_4,r}\right)\left(\sum_k \overline{b_{\ell_1,k}b_{\ell_2,k}}b_{\ell_3,k}b_{\ell_4,k}\right) \tag{5.4}$$

jābūt vienādam ar nulli visiem ℓ_1, ℓ_2, ℓ_3 un ℓ_4 tādiem, ka $\{\ell_1, \ell_2\} \neq \{\ell_3, \ell_4\}$.

Definēsim matricas A *L-grafu* (apzīmējums: $L(A)$) sekojošā veidā. Tas ir vienkāršs grafs, katra tā virsotne ir divu rindiņu no A nesakārtotais pāris, pāris var sastāvēt no vienas rindiņas saskaitītas divas reizes. Mēs apzīmēsim $L(A)$ virsotnes ar nesakārtotiem indeksu pāriem. Divas virsotnes $\{a, b\}$ un $\{c, d\}$ ir savienotas tad un tikai tad, ja $R_a \circ R_b \perp R_c \circ R_d$, kur R_a ir matricas A rinda ar indeksu a.

Mēs sauksim divus L-grafus $L(A)$ un $L(B)$ par *izomorfiem*, ja eksistē tāda bijekcija σ no matricas A rindiņu kopas un matricas B rindu kopu tāda, ka visiem a, b, c, d, virsotnes $\{a, b\}$ un $\{c, d\}$ grafā $L(A)$ ir savienotas tādā un tikai tādā gadījumā, kad virsotnes$\{\sigma(a), \sigma(b)\}$ un $\{\sigma(c), \sigma(d)\}$ ir savienotas grafā $L(B)$.

No vienādojuma (5.4) izriet sekojošais

Apgalvojums 5.6. *Homogēna sistēma, uzdotā ar (5.3), apmierina Secinājuma 5.4 ortogonalitātes nosacījumu tad un tikai tad, ja grafi $L(A)$ un $L(B)$ kopā pārklāj pilno grafu.*

Ja mēs aplūkojam MUHu pilnās sistēmas, tad no Teorēmas 5.5 var dabūt papildus nosacījumus matricām A un B. Mēs pieprasīsim, lai B būtu kompleksa Adamāra matrica, un A būtu plakana matrica. Tad no Teorēmas 5.5 un Apgalvojuma 5.6 seko, ka matricu sistēma (5.3) ir MUHu pilnā sistēma tad un tikai tad, kad $L(A)$ un $L(B)$ kopā pārklāj pilno grafu.

SIC-POVMu gadījumā tāds ierobežojums nepastāv, tomēr mēs pieņemsim ka matrica B ir plakana. Mēs izstrādāsim nosacījumus matricai A nākamajā nodaļā.

Dažreiz ir ērtāk strādāt ar grafu $\tilde{L}(A)$ grafa $L(A)$ vietā. Tā virsotnes ir *sakārtoti* rindiņu pāri, un divas virsotnes ir savienotas tad un tikai tad, ja pirmā pāra Adamāra reizinājums ir ortogonāls otrā pāra Adamāra reizinājumam. Grafu-teorētiski, grafu $\tilde{L}(A)$ var dabūt no grafa $L(A)$ sašķeļot katru virsotni $\{a, b\}$ ar dažādiem a un b divās nesavienotās virsotnēs: (a, b) un (b, a).

Ja matricas A un B apmierina Apgalvojuma 5.6 nosacījumus, un A' un B' ir tādas matricas, ka $L(A)$ ir grafa $L(A')$ apakšgrafs un tas pats ir spēkā arī $L(B)$ un $L(B')$, tad A' un B' arī apmierinā Apgalvojuma 5.6 nosacījumus. Tātad, ja garuma nosacījumi no Secinājuma 5.4 ir apmierināti, tad mēs varām apskatīt tikai matricas ar maksimāliem L-grafiem. Mēs tos sauksim par *L-maksimālām matricām.* Mēs lietosim arī nosaukumu *L-maksimāla Adamāra matrica* (*L-maksimāla plakana matrica*) matricai, kura ir Adamāra

(atbilstoši, plakana) un tāda, ka $L(A)$ nav stingrs $L(B)$ apakšgrafs kaut kādai Adamāra (atbilstoši, plakanai) matricai B.

Skaidrs, ka matrica A ir L-maksimāla tad un tikai tad, ja grafs $\tilde{L}(A)$ ir maksimāls. Homogēnu sistēmu pētīšanā sekojošs jautājums liekas svarīgs:

Neatrisināta Problema 5.7. *Aprakstīt visas L-maksimālas plakanas un Adamāra matricas, kā arī atbilstošus grafus.*

Neatkarīgi no atbildes uz šo jautājumu, ir skaidrs, ka L-maksimālas matricas pārklāj L-maksimālas plakanas matricas, kuras, savukārt, pārklāj L-maksimālas Adamāra matricas. Tas ir tāpēc, ka katra Adamāra matrica ir plakanas matricas speciālgadījums, kas ir vispārīgas matricas speciālgadījums.

Eksistē svarīga L-maksimālu Adamāru (un pat vispārīgu) matricu klase. Tās ir Furjē matricas, kuras mēs definējām Sadaļā 1.2..

5.4. Furjē matricas homogēnajās sistēmās

Pieņemsim, ka A ir $n \times n$-matrica un $L(A)$ ir tās L-grafs. Grafa virsotnes atbilst īpašā veidā dabūtiem vektoriem no $\mathbb{C}^n$ un divas virsotnes ir savienotas tad un tikai tad, ja atbilstoši vektori ir ortogonāli. Vispārīgāks jēdziens, kuru mēs arī izmantosim, būtu grafs T, kura virsotnes ir *patvaļīgi* vektori no $\mathbb{C}^n$ un, atkal, divas virsotnes ir savienotas tad un tikai tad, ja atbilstoši vektori ir ortogonāli.

Mēs atgādināsim dažus jēdzienus no grafu teorijas (skat., piem., [25]). Par grafa G *neatkarīgu kopu* (**independent set**) sauc inducētu apakšgrafu bez šķautnēm, t.i., tādu virsotņu kopas apakškopu, ka nevienas divas virsotnes tajā nav savienotas ar šķautni. Un otrādi, par *kliķi* (**clique**) sauc inducētu pilno apakšgrafi, jeb tādu virsotņu kopas apakškopu, ka jebkuras divas tās virsotnes ir savienotas ar šķautni. Par grafa G *neatkarības skaitli* (**independence number**) $\alpha(G)$ sauc lielākas neatkarīgas kopas izmēru, un par grafa G *blīvumu* (**clique number**) $\omega(G)$ sauc lielākās grafa kliķes izmēru.

Minimālu krāsu skaitu, kurā var izkrāsot grafa G virsotnes tā, ka jebkuras divas kaimiņvirsotnes ir nokrāsotas dažādās krāsās, sauc par grafa *hromatisko skaitli* (**chromatic number**) $\chi(G)$. Viegli redzēt, ka $\chi(G) \geq \omega(G)$, tā kā visām virsotnēm kliķē jābūt nokrāsotiem dažādās krāsās.

Sekojošā lemma ir acīmredzama.

Lemma 5.8. *Pieņemsim, ka T ir grafs, kura virsotnes ir patvaļīgi vektori no $\mathbb{C}^n$ un divi vektori ir savienoti tad un tikai tad, ja tie ir ortogonāli. Tad $\omega(G) \leq n$.*

Pieņemsim, ka F ir grupas G Furjē matrica un $\{R_i\}$ ir tās rindu kopa. Atgādināsim (Apgalvojums 1.5), ka matricas F ir pa pāriem ortogonālas un veido grupu attiecībā pret Adamāra reizinājumu, un šī grupa ir izomorfa ar G. Tātad, grafā $L(F)$ virsotnes $\{a, b\}$ un $\{c, d\}$ ir savienotas tad un tikai tad, ja $a + b \neq c + d$.

Teorēma 5.9. *Furjē matrica F ir L-maksimāla matrica,* a fortiori, *tā ir L-maksimāla Adamāra matrica. Turklāt, grafam $\tilde{L}(F)$ ir maksimālais šķautņu skaits starp visiem grafiem formā $\tilde{L}(A)$, kur A ir $n \times n$-matrica.*

Katra Adamāra $n \times n$-matrica H tāda, ka grafam $\tilde{L}(H)$ ir tik pat daudz šķautņu kā $\tilde{L}(F)$, grafs $L(H)$ ir izomorfs Furjē matricas L-grafam.

Pierādījums. Pieņemsim, ka A ir patvaļīga $n \times n$-matrica un F ir Furjē $n \times n$-matrica. No Lemmas 5.8 seko, ka $\omega(\tilde{L}(A)) \leq n$. Atradināsim, ka *Turāna grafs* (**Turán graph**) $T^r(n)$ (skat. Sadaļu 7.1 no [25]) ir vienīgais (ar precizitāti līdz izomorfismam) pilnais r-daļains grafs ar n virsotnēm, kura daļas atšķīrās izmēros lielākais par 1. Speciālajā gadījumā, kad r dala n, visas daļas ir ar izmēru $\frac{n}{r}$. Turāna grafs $T^r(n)$ ir svarīgs ar to, ka tam ir lielākais šķautņu skaits starp visiem grafiem ar izmēru n un blīvumu r.

Tātad, Furjē matricas L-maksimalitāte seko no viegli pārbaudāma fakta, ka $\tilde{L}(F)$ ir Turāna grafs $T^n(n^2)$.

Pieņemsim, ka H ir Adamāra $n \times n$-matrica. Apzīmēsim H rindas ar $\{R_i\}$, $i = 0, 1, \ldots, n-1$. Pareizinot matricas kolonnas ar kompleksu skaitli ar moduli 1 nemaina L-grafu, tātad, mēs varām pieņemt, ka R_0 sastāv tikai no vieniniekiem.

Priekš fiksēta i kopa $\{R_i \circ R_j \mid j = 0, \ldots, n-1\}$ ir telpas $\mathbb{C}^n$ ortonormēta bāze. Tātad, katrs vektors $R_a \circ R_b$ nav ortogonāls vismaz vienam elementam no $\{R_i \circ R_j \mid j = 0, \ldots, n-1\}$. Atzīmēsim, ka, ja H ir Furjē matrica, tad $R_a \circ R_b$ nav ortogonāla tieši vienam šīs kopas elementam — tādam, ka $i + j = a + b$.

Ja grafam $\tilde{L}(H)$ ir maksimālais iespējamais šķautņu skaits, tad tas ir Turāna grafs $T^n(n^2)$, tādējādi, katra virsotne nav savienota ar tieši n virsotnēm, ieskaitot viņu pašu. Tādējādi, katrs $R_a \circ R_b$ nav ortogonāls tieši vienam elementam no $\{R_i \circ R_j \mid j = 0, \ldots, n-1\}$ priekš katra i, un, starp citu, nav ortogonāls tieši vienam no $\{R_i\}$ (tā kā R_0 sastāv tikai no vieniniekiem). Tas nozīmē, ka $R_a \circ R_b = \alpha R_i$ kādam i un kādam $\alpha \in \mathbb{C}^*$.

Pieņemsim, ka G ir $\mathbb{C}P^{n-1}$ apakškopa, kuru veido H rindiņas un aplūkosim Adamāra reizinājuma operāciju un šīs kopas. Kopa ir galīga, tā ir slēgta attiecībā pret operāciju,

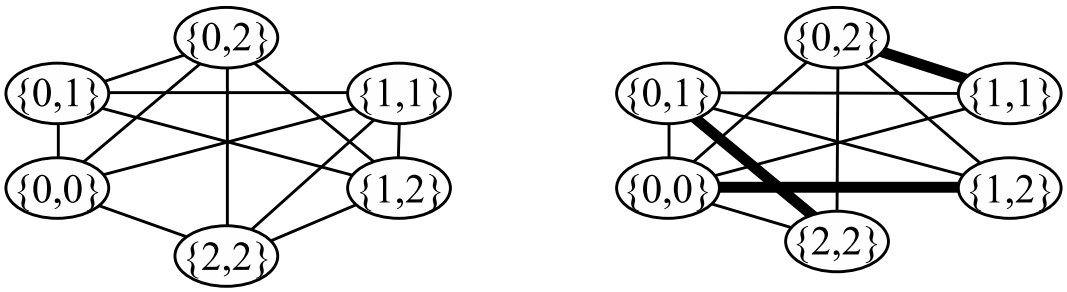
R_0 ir vienības elements, operācija ir komutatīva un asociatīva, un katram i atbilstība $R_j \mapsto R_i \circ R_j$ ir bijekcija. No tā visa seko, ka G ir galīga Ābela grupa un $L(H)$ ir izomorfs ar grupas G Furjē matricas L-grafu. ■

Šis rezultāts izskaidro, kāpēc Furjē matricas ir tik noderīgas konstruējot MUBus un SIC-POVMus. Tiešām, Furjē matricas L-grafs pārklāj rupji $\frac{n-1}{n}$ no visām pilnā grafa šķautnēm, tātad, atliek tikai atrast otru matricu A , kuras L-grafs pārklāj atlikušo daļu no $\frac{1}{n}$ šķautnēm. Priekš MUBiem šis uzdevums izskatās pavisam viegli, jo matrica A, pretēji matricai H, drīkst pat nebūt Adamāra, pietiek ar to, ka tā ir plakana. Diemžēl, šis uzdevums īstenībā neizskatās nemaz tik viegls.

Var izteikt hipotēzi, ka Furjē matricas ir vienīgās L-maksimālās Adamāra matricas. Bet var viegli pārliecināties, ka pastāv arī citas L-maksimālās plakanas matricas. Piemēram, aplūkosim sekojošas divas matricas: Furjē matricu F un plakano matricu A telpā $\mathbb{C}^3$, kas ir uzdotas ar

$$F = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3^2 & \omega_3 \end{pmatrix} \quad A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3 & \omega_3^2 \end{pmatrix}. \tag{5.5}$$

Atbilstoši L-grafi ir uzzīmēti Zīmējumā 5.1.. Otrajā grafā ir izceltas tās šķautnes, kurus



5.1. zīm.: Matricu F (pa kreisi) un A (pa labi) L-grafi. Matricas ir uzdotas ar (5.5).

nepārklāj $L(F)$. Tādējādi, šie divi grafi kopā pārklāj pilno grafu. Atzīmēsim, ka neviena no izceltām šķautnēm nevar piederēt Adamāra matricas L-grafam. Tiešām, pieņemsim, ka šķautne $\{0,0\}\{1,2\}$ pieder Adamāra matricas L-grafam. Tad šīs divas virsotnēs kopā ar $\{0,1\}$ un $\{0,2\}$ veido K_4 — pilno grafu ar četrām virsotnēm, bet tas nav iespējams.

Šajā gadījumā $L(F)$ pats ir Turāna grafs, tomēr, tas tā nebūs vienmēr. Piemēram, grafs $L(F_2^{\otimes k})$, kur F_2 ir definēts ar (1.3), satur neatkarīgu kopu ar izmēru 2^k. Tas ir iemesls tam, ka mēs aplūkojam grafu $\tilde{L}(F)$, nevis $L(F)$ Teorēmas 5.9 pierādījumā.

Kā tika atzīmēts iepriekš, izskatās, ka atrast matricu A būs viegli, bet tā tas nav. Furjē matrica F ir ar īpašību, ka $\chi(L(F)) = n$ (virsotnes $\{a,b\}$ krāsa ir $a+b$). Starp citu,

tas nozīmē, ka ja izdosies atrast $n \times n$ Adamāra matricu H tādu, ka $\chi(L(H)) > n$, tad to nepārklās neviena Furjē matrica, un hipotēze, ka Furjē matricas ir vienīgas L-maksimālas matricas, nebūs patiesa. Bet mēs pagaidām nezinām nevienu Adamāra matricu ar tādu īpašību.

Vispārīgam grafam G izpildās nevienādība $\alpha(G) \geq \frac{n(G)}{\chi(G)}$ (šeit $n(G)$ ir virsotņu skaits grafā G; nevienādība seko no tā fakta, ka vienas krāsas virsotnes veido neatkarīgu kopu). Tātad, mazs hromatiskais skaitlis implicē lielu neatkarības skaitli, un, tādējādi, otrajai matricai, lai apmierinātu Apgalvojuma 5.6 nosacījumus, jābūt ar lielu kliķes skaitli. Un tas var izpausties grūtībās meklējot otro matricu. Mēs šo apgalvojumu nedaudz precizēsim Apgalvojumā 5.10. Tātad, Adamāra matricas H ar lielu $\chi(L(H))$ un mazu $\alpha(L(H))$ (ja tādas eksistē) varētu būt interesantas konstruējot 2-dizainus.

Ir vērts pieminēt arī citas konstrukcijas, kas līdzīgi L-grafa jēdzienam, izmanto vektoru ortogonalitāti kā pazīmi, kad grafa virsotnes tiek savienotas ar šķautni. Viens piemērs ir tā saucamais *Adamāra grafs* (**Hadamard graph**) [44]. Adamāra grafa $S(n)$ ar kārtu n virsotņu kopa ir visu garumā n vektoru kopa, kuru elementi ir vienādi ar ± 1. Divi vektori ir savienoti ar šķautni tad un tikai tad, ja tie ir ortogonāli. Slavenā Adamāra hipotēze ir ekvivalenta ar apgalvojumu, ka $\omega(S(4n)) = 4n$ visiem naturāliem n. Papildus ir pierādīts [30], ka pastāv eksponenciāla sprauga starp $4n$ un $\chi(S(4n))$. Tā kā ir iespējams, ka kādai Adamāra matricai H pastāv stingra nevienādība $\chi(L(B)) > n$.

Labākas alternatīvas trūkuma dēļ, pieņemsim tālāk, ka B ir galīgas Ābela grupas G Furjē matrica. Šajā gadījumā var viegli pārliecināties, ka matricas A un B apmierina Apgalvojuma 5.6 nosacījumus tad un tikai tad, ja

$$\forall g_1, g_2, g_3, g_4 \in G : \left.\begin{array}{c} g_1 + g_2 = g_3 + g_4 \\ \{g_1, g_2\} \neq \{g_3, g_4\} \end{array}\right\} \Longrightarrow R_{g_1} \circ R_{g_2} \perp R_{g_3} \circ R_{g_4}, \tag{5.6}$$

kur R_i ir matricas A i-tā rindiņa. Šo nosacījumu var pārrakstīt sekojošajā veidā:

Apgalvojums 5.10. *Pieņemsim, ka B ir grupas G Furjē matrica un matrica A ir ar rindām $\{R_i\}_{i \in G}$. Tad šīs divas matricas apmierina Apgalvojuma 5.6 nosacījumus tad un tikai tad, ja priekš katra $\Delta \in G$ matricas D_Δ rindiņas*

$$\{R_{i+\Delta} \circ \overline{R_i} \mid i \in G\}$$

ir savstarpēji ortogonālas.

Pierādījums. Pieņemsim, ka A un B apmierina nosacījumus. Paņemsim divus G elementus $g_1 \neq g_3$. Tad

$$\langle R_{g_1+\Delta} \circ \overline{R_{g_1}}, R_{g_3+\Delta} \circ \overline{R_{g_3}} \rangle = \langle R_{g_1+\Delta} \circ R_{g_3}, R_{g_3+\Delta} \circ R_{g_1} \rangle.$$

Turklāt, $(g_1 + \Delta) + g_3 = (g_3 + \Delta) + g_1$, $g_3 \neq g_1$ un $g_3 \neq g_3 + \Delta$. Izmantojot (5.6) ar $g_2 = g_3 + \Delta$ un $g_4 = g_1 + \Delta$, iegūstam, ka $R_{g_1+\Delta} \circ \overline{R_{g_1}} \perp R_{g_2+\Delta} \circ \overline{R_{g_2}}$.

Pretējā apgalvojuma pierādījums ir līdzīgs. ■

Atzīmēsim, ka, ja matricai D_Δ ir savstarpēji ortogonālas rindiņas, tad matricai $D_{-\Delta}$ arī ir savstarpēji ortogonālas rindiņas. Šis novērojums atļauj dažreiz samazināt pārlasi.

6. nodaļa

Meklējot Moduļus

Šajā nodaļā mēs pētīsim, kādām jābūt formulā (5.3) ievesto matricu A un B elementu absolūtajām vērtībām, lai tās apmierinātu Secinājuma 5.4 garumu nosacījumu. Kā tika pieminēts iepriekšējā nodaļā, no Teorēmas 5.5 seko, ka homogēnu MUHu gadījumā pietiek pieņemt, ka A ir plakana un B ir kompleksa Adamāra matrica. Tas pilnībā apraksta A un B elementu moduļus MUHu gadījumā. Šajā nodaļā mēs mēģināsim atbildēt uz līdzīgu jautājumu SIC-POVMiem.

Teorēma 6.1. *Pieņemsim, ka mēs meklējam SIC-POVMus homogēnajā nostādnē (5.3), kur B ir grupas G Furjē matrica. Šajā gadījumā matricai A jāapmierina sekojošie nosacījumi:*

1. *katra matricas A kolonna ir ar normu 1;*
2. *katra rindiņa R_i ir ar normu 1;*
3. *visiem i, j, k, tādiem, ka $j \neq k$, izpildās $\|R_i^{(2)}\| = \sqrt{2}\|R_j \circ R_k\|$;*
4. *visiem $g_1, g_2, g_3, g_4 \in G$ tādiem, ka $g_1 + g_2 = g_3 + g_4$ un $\{g_1, g_2\} \neq \{g_3, g_4\}$, vektori $R_{g_1} \circ R_{g_2}$ un $R_{g_3} \circ R_{g_4}$ ir ortogonāli;*

kur, kā parasti, R_i apzīmē matricas A rindiņu, kas indeksēta ar elementu $i \in G$.

Pierādījums. Nosacījumam 1 jāizpildās pēc SIC-POVMu definīcijas. Secinājuma 5.4 apzīmējumos, w_i ir matricas B rindiņa, kas atbilst elementam $i \in G$. No (5.3), tā kā visi B elementi pēc absolūtās vērtības ir 1, seko, ka $\|w_i \circ w_j\| = \sqrt{n}\|R_i \circ R_j\|$ (katrs $R_i \circ R_j$ elements tiek atkārtots, ar precizitāti līdz fāzei, n reizes). Tad Secinājuma 5.4 garuma nosacījums implicē Nosacījumu 3. Nosacījums 4 ir formulas (5.6) parafrāze.

Nosacījums 2 prasa nedaudz vairāk komentāru. Kā seko no Teorēmas 3.5, SIC-POVMa vektori apmierina Velča vienādību priekš $k = 1$. No Teorēmas 5.1 seko, ka $\|w_i\| = \|w_j\|$ visiem $i, j \in G$. Tad, līdzīgi kā Nosacījumā 3, dabūjām $\|R_i\| = \|R_j\|$. Tā kā matricas A katras kolonnas norma ir 1, tad katras rindiņas norma arī ir 1. ■

Homogēnie SIC-POVMi ir parasti aplūkoto grupu kovarianto SIC-POVMu vispārinājums, kā tas seko no šīs piezīmes:

Piezīme 6.2. Ja matrica A apmierina Teorēmas 6.1 nosacījumus un ir cirkulāra attiecībā pret G, tad SIC-POVMs, kas aprakstīts ar (5.3), ir grupu kovariants attiecībā pret GP(G).

Kā jau tika teikts, šajā nodaļā mēs neaplūkojam Nosacījumu 4, atliekot to līdz nākamai nodaļai. Tā kā visi pārēji nosacījumi darbojas tikai ar vektoru normām, mēs varam aizvietot matricu $A = (a_{ij})$ ar matricu $M = (m_{ij})$, kas sastāv no matricas A elementu absolūtām vērtībām: $m_{ij} = |a_{ij}|$. Visi matricas M elementi ir nenegatīvi reāli skaitli.

No Piezīmes 3.6 un Secinājuma 5.4 var izvest, ka ar Nosacījumiem 3 un 4 pietiek, lai apgalvotu, ka konstruētā vektoru sistēma ir SIC-POVMa skalārais daudzkārtnis. Mēs pievienojām klāt Nosacījumus 1 un 2, lai pēc iespējas sašaurinātu iespējamo matricu M klāstu.

Sāksim problēmas izpēti. Apzīmēsim ar y_{ij} elementu ar indeksu (i, j) matricā $M^{(2)}$, t.i., $y_{ij} = m_{ij}^2$. Tad Teorēmas 6.1 Nosacījumi 1 un 2 dod, attiecīgi:

$$\sum_i y_{ij} = 1 \quad \text{un} \quad \sum_j y_{ij} = 1. \tag{6.1}$$

No Nosacījuma 3 izriet:

$$\sum_j y_{ij}^2 = 2 \sum_j y_{kj} y_{\ell j}$$

visiem i, k, ℓ tādiem, ka $k \neq \ell$. Saliekot kopā, mēs dabūjam:

$$n = \sum_j \left(\sum_i y_{ij} \right)^2 = \sum_{i,j} y_{ij}^2 + 2 \sum_{i<k} \sum_j y_{ij} y_{kj} = \left(n + \frac{n(n-1)}{2} \right) \sum_j y_{ij}^2. \tag{6.2}$$

Tātad,

$$\sum_j y_{ij}^2 = \frac{2}{n+1}, \quad \text{un} \quad \sum_j y_{kj} y_{\ell j} = \frac{1}{n+1}. \tag{6.3}$$

Apzīmējot vektoru $(y_{i1}, y_{i2}, \ldots, y_{in})$ ar y_i, definēsim vektorus $e = \left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right)$ un $\tilde{y}_i = y_i - e$. Viegli redzēt, ka (6.1) nozīmē, ka $\tilde{y}_i \perp e$ visiem i. Tātad

$$\frac{2}{n+1} = \langle y_i, y_i \rangle = \langle \tilde{y}_i + e, \tilde{y}_i + e \rangle = \langle \tilde{y}_i, \tilde{y}_i \rangle + \frac{1}{n}$$

visiem i. Un visiem $i \neq j$:

$$\frac{1}{n+1} = \langle y_i, y_j \rangle = \langle \tilde{y}_i + e, \tilde{y}_j + e \rangle = \langle \tilde{y}_i, \tilde{y}_j \rangle + \frac{1}{n}.$$

Tādējādi,

$$\langle \tilde{y}_i, \tilde{y}_i \rangle = \frac{n-1}{n(n+1)} \quad \text{un} \quad \langle \tilde{y}_i, \tilde{y}_j \rangle = -\frac{1}{n(n+1)} \quad \text{visiem } i \neq j.$$

Viegli redzēt, ka $\{\tilde{y}_i\}$ veido regulāra $(n-1)$-dimensionāla simpleksa virsotnes. Šis simplekss ir ievietots hiperplaknē, kas perpendikulāra vektoram e, un tā rādiuss ir $\sqrt{\frac{n-1}{n(n+1)}}$. Simplekss $\mathcal{Y}$, kuru veido vektori $\{y_i\}$, papildus ir pārnests par vektoru e. Tā kā visiem y_i jābūt nenegatīviem, $\mathcal{Y}$ atrodas lielākā simpleksā $\mathcal{S}$, kuru veido telpas $\mathbb{R}^n$ standartbāzes elementi. Pēdējais arī ir centrēts punktā e un tā rādiuss ir

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

Tā kā simplekss $\mathcal{Y}$ ir mazāks par $\mathcal{S}$, pirmo vienmēr var ievietot otrajā. Vieglākais veids, kā to izdarīt, ir homotēt $\mathcal{S}$ ar koeficientu $1/\sqrt{n+1}$ un centru e. Iegūto simpleksu veido vektors

$$\left(\frac{1}{n} + \frac{n-1}{n\sqrt{n+1}}, \frac{1}{n} - \frac{1}{n\sqrt{n+1}}, \frac{1}{n} - \frac{1}{n\sqrt{n+1}}, \ldots, \frac{1}{n} - \frac{1}{n\sqrt{n+1}}\right) \tag{6.4}$$

kopā ar tā cikliskām permutācijām.

Rūpīgi analizējot iepriekšējo spriedumu, var nonākt pie sekojošā rezultāta:

Teorēma 6.3. *Pieņemsim, ka M ir matrica, kas apmierina Teorēmas 6.1 Nosacījumus 1, 2 un 3. Tad $M^{(2)}$ rindiņas veido $(n-1)$-dimensionālu simpleksu $\mathcal{Y}$ ar rādiusu $\sqrt{\frac{n-1}{n(n+1)}}$ un centru $\left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right)$, kas ievietots $(n-1)$-dimensionālā simpleksā, ko veido standartbāzes elementi. Un otrādi, jebkurš tāds simplekss $\mathcal{Y}$ atbilst matricai M, kas apmierina nosacījumus 1, 2 un 3.*

Pierādījums. Mēs tikko pierādījām teorēmu vienā virzienā. Lai pierādītu apgriezto apgalvojumu, pamanām, ka Nosacījums 2 izriet no tā, ka visas $\mathcal{Y}$ virsotnes atrodas hiperplaknē $\sum_j y_j = 1$. Nosacījumu 3 var dabūt, apgriežot aprēķinus pēc formulas (6.3). Tad no (6.2) dabūjam, ka $\sum_j \left(\sum_i y_{ij}\right)^2 = n$. Pielietojot nevienādību starp kvadrātisko un aritmētisko vidējo, iegūstam:

$$\sum_j \left(\sum_i y_{ij}\right)^2 \geq \frac{1}{n}\left(\sum_{i,j} y_{ij}\right)^2 = n$$

ar vienādību tajā un tikai tajā gadījumā, kad visi $\sum_i y_{ij}$ ir vienādi. Tātad Nosacījums 1 arī izpildās. ■

Tagad mēs aplūkosim cirkulāras matricas M, kas apmierina Nosacījumus 1,2 un 3. Interese par cirkulārām matricām rodas tādēļ, ka tādas matricas tiek izmantotās grupu kovariantos SIC-POVMos. Vēl viens iemesls ir tas, ka tās atvieglo Nosacījuma 4 analīzi, ko mēs veiksim nākamajā nodaļā.

Aplūkosim grupu $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$. Mēs sauksim simpleksu $\mathcal{Y}$ par *cirkulāru pār* G, ja atbilstošā matrica M ir cirkulāra attiecībā pret G (mēs pieņemsim arī, ka M ir nenegatīva). Tādi simpleksi vienmēr eksistē. Piemēram, ar formulu (6.4) uzdotais simplekss ir cirkulārs attiecībā pret visām grupām G. Mēs tagad parādīsim, kā dabūt visus pārējos simpleksus no šī simpleksa.

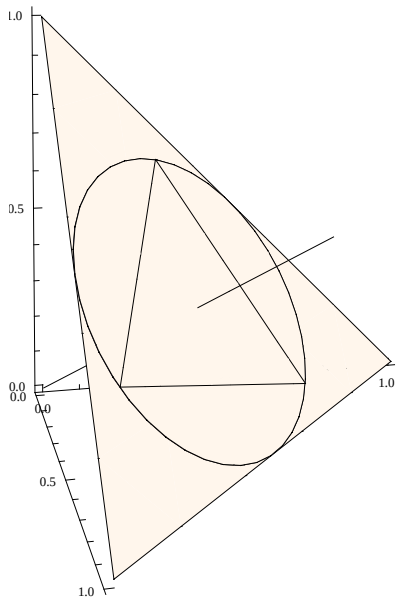
Matricas M rindas un kolonnas ir indeksētas ar G elementiem, tātad mēs varam pieņemt, ka arī telpas, kurā atrodas simplekss, kanoniskā bāze ir indeksēta ar elementiem no G. Apzīmēsim ar V_i lineāro transformāciju, kas attēlo kanoniskās bāzes elementu, kas atbilst elementam $(a_1, a_2, \ldots, a_m) \in G$, vektorā, kas atbilst elementam $(a_1, a_2, \ldots, a_{i-1}, a_i + 1, a_{i+1}, \ldots, a_m)$. Citiem vārdiem,

$$V_i = I_{d_1} \otimes I_{d_2} \otimes \cdots \otimes I_{d_{i-1}} \otimes X_{d_i} \otimes I_{d_{i+1}} \otimes \cdots \otimes I_{d_m} \tag{6.5}$$

kur I_n ir $n \times n$ vienības matricas un X_n ir definēta formulā (1.4). Atzīmēsim, ka visi V_i ir ortogonāli operatori un komutē savā starpā.

Pieņemsim, ka $\mathcal{Y}$ ir cirkulārs simplekss pār G (piemēram, (6.4)). Vienkāršības labad mēs aplūkosim simpleksus $\tilde{\mathcal{Y}} = \mathcal{Y} - e$ un $\tilde{\mathcal{S}} = \mathcal{S} - e$, kas abi centrēti nulles punktā (t.i., aplūkosim vektorus $\tilde{y}$ vektoru y vietā). Apzīmēsim ar $\mathcal{H}$ hiperplakni, kas perpendikulāra vektoram e. Visiem operatoriem V_i e ir īpašvektors ar īpašvērtību 1. Tātad $\mathcal{H}$ ir invarianta apakštelpa visiem V_i un mēs varam definēt inducētos operatorus $V_i|_{\mathcal{H}}$. Vienkāršības labad, tos mēs arī apzīmēsim ar V_i.

Fiksēsim patvaļīgu simpleksa $\tilde{\mathcal{Y}}$ virsotni v. Skaidrs, ka, pielietojot operatorus $V_1, V_2, \ldots, V_m$, to var attēlot uz jebkādu citu simpleksa virsotni. Tagad pieņemsim, ka w ir cita cirkulāra simpleksa $\tilde{\mathcal{Y}}' = \mathcal{Y}' - e$ virsotne. Apzīmēsim ar U lineāru operatoru, kas attēlo virsotni $V_1^{a_1} V_2^{a_2} \cdots V_m^{a_m} v$ virsotnē $V_1^{a_1} V_2^{a_2} \cdots V_m^{a_m} w$ visiem $(a_1, a_2, \ldots, a_m) \in G$. Tas ir ortogonāls operators un komutē ar visiem V_i. Un otrādi, ja U ir ortogonāls operators, kas komutē ar visiem V_i, tad $U\tilde{\mathcal{Y}}$ ir cirkulārs simplekss, ja vien tas iekļaujas simpleksā $\tilde{\mathcal{S}}$. Pietiek nodrošināt, ka vektora $Uv + e$ komponentes ir nenegatīvas, jo visu citu virsotņu koordinātas ir šī vektora komponenšu permutācijas. Turklāt, mēs varam vienmēr pieņemt, ka $Ue = e$. Tas dod sekojošu rezultātu:



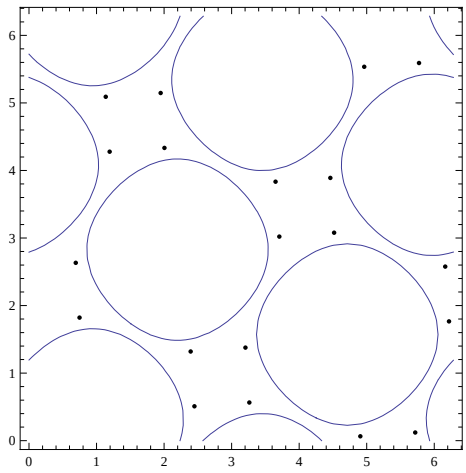
6.1. zīm.: Cirkulārais simplekss pār $G = \mathbb{Z}_3$. Tas atrodas simpleksa $\mathcal{S}$ iekšpusē. Simpleksu $\mathcal{Y}$ var griezt ap vektoru e par patvaļīgu leņķi, un tā virsotnes iezīmē riņķa līniju $\mathcal{C}$. Šajā gadījumā $\mathcal{Y}$ paliek simpleksā $\mathcal{S}$ pēc visām rotācijām, un katrs simplekss $\mathcal{Y}$ no teorēmas 6.3 ir cirkulārs.

Teorēma 6.4. *Pieņemsim, ka U ir ortogonāls operators telpā $\mathbb{R}^n$, tāds, ka $Ue = e$, un $\mathcal{Y}$ ir cirkulārs simplekss pār grupu G, kā tā definēta formulā (6.4). Tad $U\mathcal{Y}$ ir cirkulārs tad un tikai tad, ja tas atrodas $\mathcal{S}$ iekšpusē un U komutē ar visiem V_i, kas definēti ar (6.5).*

Aplūkosim gadījumu $G = \mathbb{Z}_n$, kas parādās visizplatītākajā grupu kovariantā SIC-POVMa gadījumā, t.i., attiecībā pret Veila-Heisenberga grupu $\mathrm{U}(n)$. Šajā gadījumā mums ir tikai viens operators $V_1 = X_n$. Labi zināms (to var arī viegli pārbaudīt, izmantojot Apgalvojuma 1.6 rezultātu), ka operators X_n veic rotāciju par leņķi $2\pi/k$ plaknēs, kuras veido vektori

$$\left(1, \cos\frac{2\pi k}{n}, \cos\frac{4\pi k}{n}, \ldots, \cos\frac{2(n-1)\pi k}{n}\right) \quad \text{un} \quad \left(0, \sin\frac{2\pi k}{k}, \sin\frac{4\pi k}{n}, \ldots, \sin\frac{2(n-1)\pi k}{n}\right)$$

visiem $k = 1, \ldots, \left\lfloor \frac{n-1}{2} \right\rfloor$. Ja n ir pāra, tad X_n arī veic atspoguļošanu uz taisnes, kuru veido vektors $(1, -1, 1, -1, \ldots, 1, -1)$. Vektors $e = (1, 1, \ldots, 1)$ ir šī operatora īpašvektors ar īpašvērtību 1. Tātad no Teorēmas 6.4 seko, ka simplekss $U\mathcal{Y}$, kas ievietojas $\mathcal{S}$ iekšpusē, ir cirkulārs visiem U, kas veic rotāciju par patvaļīgu leņķi tajās pašās plaknēs un, iespējams, ja n ir pāra, atspoguļošanu uz taisnes, kuru veido vektors $(1, -1, 1, -1, \ldots, 1, -1)$. Tātad, visi cirkulārie simpleksi pār $\mathbb{Z}_n$ var tikt parametrizēti ar $\left\lfloor \frac{n-1}{2} \right\rfloor$ reāliem parametriem. Gadījums $G = \mathbb{Z}_3$ ir attēlots Zīmējumā 6.1..



6.2. zīm.: Cirkulārais simplekss pār $G = \mathbb{Z}_5$. Šajā gadījumā visus cirkulārus simpleksus var aprakstīt ar diviem reāliem parametriem φ_1 un φ_2, kuri atbilst rotāciju leņķiem divās dažādās plaknēs. Asīs ir attēlotas φ_1 un φ_2 vērtības. Punkti, kas atrodās "riņķu" iekšpusē, atbilst simpleksiem, kas neievietojas simpleksā $\mathcal{S}$. Visi vektori, kas atbilst izejas vektoram (2.6) un tā afīnām permutācijām (sk. piemēru pēc Apgalvojuma 2.4 pierādījuma), ir atzīmēti ar punktiem.

Kad n aug, attiecība starp $\mathcal{S}$ un $\mathcal{Y}$ rādiusiem aug kā $O(\sqrt{n})$, bet attiecība starp $\mathcal{S}$ rādiusu un attālumu no $\mathcal{S}$ centra līdz tā robežai aug straujāk — kā $O(n)$. Tiešam, $(\frac{1}{n}, -\frac{1}{n}, 0, 0, \ldots, 0)$ ir īsākais vektors, kuru var pieskaitīt punktam e, lai iegūtu punktu uz $\mathcal{S}$ robežas. Tas nozīmē, ka lieliem n simpleksa $\mathcal{Y}$ rotācijas ne vienmēr ievietosies simpleksa $\mathcal{S}$ iekšpusē. Kā var redzēt no Zīmējuma 6.1., gadījumā $n = 3$ simplekss $\mathcal{Y}$ vienmēr atrodas $\mathcal{S}$ iekšpusē, bet ja $n = 5$, tas ne vienmēr ir taisnība. Sk. Zīmējumu 6.2.

Līdzīgā veidā var aprakstīt cirkulārus simpleksus attiecībā pret citām grupām.

7. nodaļa

Meklējot Fāzes

Šajā nodaļā mēs nodarbosimies ar sekojošu jautājumu. Pieņemsim, ka mums ir doti $n \times n$-matrica M, kuras elementi ir nenegatīvi reālie skaitļi, un galīga Ābela grupa G. Mēs gribam uzkonstruēt tādu plakanu matricu P, ka $A = M \circ P$ apmierina nosacījumu (5.6). Ja tāda matrica P eksistē, mēs sauksim matricu M par *apmierināmu* virs G. Turklāt, kā tas tika motivēts iepriekšējā nodaļā, mēs aplūkosim, galvenokārt, matricas M, kas ir cirkulāras attiecībā pret G. Šajā gadījumā matrica A būs cirkulāra tad un tikai tad, ja matrica P arī būs cirkulāra virs G. Tādējādi, ja mēs tālākajā tekstā teiksim, ka cirkulāra matrica M ir apmierināma virs G, mēs pieņemsim arī, ka matrica M ir cirkulāra *virs* G.

Motivācija šim ir sekojoša. Pieņemsim, ka mēs gribam konstruēt kompleksu projektīvu 2-dizainu, izmantojot homogēnu konstrukciju līdzīgu ar (5.3). Mēs izmantosim grupas G Furjē matricu kā matricu B, tās labo īpašību dēļ. Mēs pielietosim Secinājumu 5.4 lai dabūtu nosacījumus uz matricas A elementu absolūtām vērtībām (līdzīgi kā iepriekšējā nodaļā). Pieņemsim, ka M apmierina šos nosacījumus. Tad mēs gribam beigt šo konstrukciju, atrādot fāzes tādas, ka Secinājuma 5.4 nosacījumi izpildās pilnībā.

Konkrētā gadījumā, kad mēs paņemsim matricu M sastāvošu no visiem vieniniekiem, tad mēs dabūsim MUHu pilno sistēmu gadījumā, kad matrica M ir apmierināma. Ja M ir tāda kā Teorēmā 6.3, mēs dabūsim SIC-POVMu. Tātad, priekš MUHiem mēs dabūjam tikai vienu iespējamu matricu M, bet tai ir ļoti vienkārša struktūra. SIC-POVMiem, savukārt, matricu M izvēle ir daudz plašāka, taču tās nav tik vienkārši aprakstāmas. Tas viss ir saskaņā ar reālo situāciju: pilnās MUHu sistēmas ir atrastas visas dimensijās, kurās, ir pieņemts domāt, tādi eksistē; SIC-POVMi nav atrasti visās dimensijās, kur visi domā tie eksistē, taču izskatās, ka tie, atšķirībā no MUBiem, eksistē visās dimensijās.

Mēs iesāksim ar dažiem apmierināmo matricu piemēriem.

Apgalvojums 7.1. *Cirkulāra matrica ar pirmo rindu (a,b,c) ir apmierināma virs $\mathbb{Z}_3$ tad un tikai tad, ja vai nu viens no $\{a,b,c\}$ ir nulle, vai arī a,b,c apmierina trijstūra nevienādību, t.i., $2\max\{a,b,c\} \leq a+b+c$. Turklāt, šajā gadījumā, ja nosacījumi ir izpildīti, matricu P var izvēlēties cirkulāru.*

Pierādījums. Grupā G_3 nosacījumi $g_1+g_2 = g_3+g_4$ un $\{g_1,g_2\} \neq \{g_3,g_4\}$ izpildās vienlaicīgi tad un tikai tad, ja $g_1 = g_2$ un $\{g_3,g_4\} = \mathbb{Z}_3\backslash\{g_2\}$ vai otrādi. Matrica $A = M \circ P$ apmierina nosacījumu (5.6) tad un tikai tad, ja vektora $\overline{R_{g_1} \circ R_{g_2}} \circ R_{g_3} \circ R_{g_4}$ elementu summa ir nulle. Šī vektora elementu absolūtās vērtības, ar precizitāti līdz permutācijai, ir $abc(a,b,c)$.

Ja $abc = 0$, tad $M \circ P$ apmierina nosacījuma ar *jebkuru* plakanu matricu P.

Citādi, ja $abc \neq 0$, ir skaidrs, ka skaitļiem a,b,c jāapmierina trijstūra nevienādība. Pieņemsim, ka tie apmierina to. Šajā gadījumā pieņemsim, ka $\varphi_0, \varphi_1, \varphi_2 \in [0, 2\pi)$ ir tādi, ka $ae^{\mathbf{i}\varphi_0} + be^{\mathbf{i}\varphi_1} + ce^{\mathbf{i}\varphi_2} = 0$. Tagad var viegli pārbaudīt, ka cirkulāra matrica P ar pirmo rindu $(e^{\mathbf{i}\varphi_0/3}, e^{\mathbf{i}\varphi_1/3}, e^{\mathbf{i}\varphi_2/3})$ apmierina nosacījumus. Aplūkosim gadījumu, kad $g_1 = g_2 = 0$, $g_3 = 1$ un $g_4 = 2$. Tad

$$\langle R_0 \circ R_0, R_1 \circ R_2 \rangle = abc\left(ae^{(\mathbf{i}/3)(\varphi_1+\varphi_2-2\varphi_0)} + be^{(\mathbf{i}/3)(\varphi_0+\varphi_2-2\varphi_1)} + ce^{(\mathbf{i}/3)(\varphi_0+\varphi_1-2\varphi_2)}\right) =$$

$$= abce^{(\mathbf{i}/3)(\varphi_0+\varphi_1+\varphi_2)}\left(ae^{-\mathbf{i}\varphi_0} + be^{-\mathbf{i}\varphi_1} + ce^{-\mathbf{i}\varphi_2}\right) = 0.$$

Parējos gadījumus var pārbaudīt līdzīgi. ■

7.1. SIC-POVMi

Aplūkosim iesākumam grupu kovariantu SIC-POVMu gadījumu. Lai iegūtu grupu kovariantu SIC-POVMu, abām matricām M un P jābūt cirkulārām attiecībā pret vienu un to pašu grupu. Pieņemsim, ka x ir matricas $A = P \circ M$ nultā rinda. Apgriežot šo vektoru, mēs iegūstam matricas A pirmo kolonu, tātad, ja SIC-POVMs ir grupu kovariants, tad x ir fiduciārs vektors.

Apzīmējot Teorēmas 6.1 ceturtajā Nosacījumā $g_1 = j, g_2 = j+k+l, g_3 = j+k, g_4 = j+l$, nav grūti pierādīt, ka $x = (x_i)$ ir fiduciārs vektors tad un tikai tad, ja

$$\sum_{j=0}^{n-1} \overline{x_j} x_{j+k} x_{j+l} \overline{x_{j+k+l}} = \frac{1}{n+1}(\delta_{k,0} + \delta_{l,0})$$

kur $\delta_{a,b}$ ir Kronekera (**Kronecker**) delta, kas vienāda ar 1, ja $a = b$, un vienāda ar nulli pretējā gadījumā. Šis nosacījums tika pierādīts neatkarīgi rakstos [7] un [46], izmantojot citu tehniku.

Izmantojot Apgalvojumu 7.1 un analīzi iepriekšējās nodaļas beigās, ir iespējams uzkonstruēt dažus SIC-POVMus telpā $\mathbb{C}^3$. Kā mēs redzējām Zīmējumā 6.1., vektors, kuru veido matricas M pirmās rindas elementu moduļu kvadrāti atrodas uz riņķa līnijas $\mathcal{C}$ ar rādiusu $\frac{1}{\sqrt{6}}$, centru punktā $e = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ un kas ir perpendikulāra vektoram e. Turklāt, šī riņķa līnija pilnībā atrodas simpleksā $\mathcal{S}$, tātad, visiem punktiem un riņķa līnijas komponentes ir nenegatīvas. Tagad mēs parādīsim, ka riņķa līnija $\mathcal{C}$ sastāv tieši no ekstremāliem punktiem, kuru elementu kvadrātsaknes apmierina trijstūra nevienādību. Citiem vārdiem, visiem punktiem $(x, y, z) \in \mathcal{S}$, kas atrodas uz riņķa līnijas $\mathcal{C}$ vai tās iekšpusē, nevienādība $\sqrt{x} + \sqrt{y} + \sqrt{z} \geq 2\max\{\sqrt{x}, \sqrt{y}, \sqrt{z}\}$ ir apmierināta, visiem, kuri atrodas ārpus riņķa $\mathcal{C}$ — nav apmierināta.

Tiešām, no vienādības $\sqrt{x} + \sqrt{y} + \sqrt{z} = 2\max\{\sqrt{x}, \sqrt{y}, \sqrt{z}\}$ un $x + y + z = 1$ mēs iegūstām:

$$\sqrt{x} = \pm(\sqrt{y} \pm \sqrt{z}).$$

Paņemot kvadrātu, pārgrupējot locekļus, un paņemot kvadrātu vēl vienu reizi, mēs dabūjam:

$$\begin{aligned} & x - y - z = \pm 2\sqrt{yz} \\ \Longrightarrow \quad & x^2 + y^2 + z^2 = 2xy + 2xz + 2yz \\ \Longrightarrow \quad & 2x^2 + 2y^2 + 2z^2 = 1, \end{aligned}$$

tā kā $(x + y + z)^2 = 1$. Izdalot ar 2 un pārgrupējot, mēs iegūstam:

$$x^2 + y^2 + z^2 - \frac{2}{3}(x + y + z) + 3\frac{1}{9} = \frac{1}{6}$$
$$\left(x - \frac{1}{3}\right)^2 + \left(y - \frac{1}{3}\right)^2 + \left(z - \frac{1}{3}\right)^2 = \frac{1}{6}.$$

Tādējādi, mēs varam dabūt SIC-POVMu no jebkura punkta uz riņķa līnijas $\mathcal{C}$, izmantojot Apgalvojumu 7.1. Punktiem, kas atrodas uz $\mathcal{C}$ un $\mathcal{S}$ robežas krustpunktiem, var pat paņemt patvaļīgu P. Tā kā mēs vienmēr varam paņemt cirkulāru P, katrs punkts uz $\mathcal{C}$ dod fiduciāro vektoru.

Mēs atgriezīsimies SIC-POVMiem Sadaļā 7.3., bet tagad aplūkosim MUHu gadījumu.

7.2. Meklējot fāzes MUHiem

MUHu gadījumā mēs meklējām plakano matricu A, kas apmierina (5.6). Citiem vārdiem, mēs paņemsim M, kas pieminēta nodaļas sākumā ar visiem elementiem vienā-

diem ar 1. Ir vērts atzīmēt, ka visas matricas D_Δ no Apgalvojuma 5.10 šajā gadījumā ir kompleksas Adamāra matricas.

Adamāra matricas nav tik bieži sastopamas, un šajā gadījumā no vienas plakanas matricas ar iepriekš minēto konstrukciju sanāk $n-1$ Adamāra matricas. Tas, zināmā mērā, izskaidro, kapēc nav tik viegli atrast vajadzīgo matricu A. Iepriekšējās konstrukcijās, kā mēs paradīsim sadaļā 7.2.3., matricas D_Δ sanāk, līdz ekvivalencei, vienādas ar Furjē matricu.

7.2.1. Nepārtrauktas grupas

Lai aplūkotu sekojošus rezultātus pēc iespējas vispārīgākajā gadījumā, mēs pāriesim no diskrētas Ābela grupas (1.1) uz nepārtrauktu grupu

$$\tilde{G} = \mathbb{R}_{d_1} \times \mathbb{R}_{d_2} \times \cdots \times \mathbb{R}_{d_m},$$

kur $\mathbb{R}_a$ ir reālo skaitļu grupa pēc moduļa a ar saskaitīšanas operāciju, t.i., $\mathbb{R}_a = \mathbb{R}/a\mathbb{Z}$.

Viegli redzēt, ka G ir grupas $\tilde{G}$ apakšgrupa. Papildus jau ievēstam apzīmējumam G^* grupas G nenulles elementu kopai, mēs lietosim apzīmējumu $\tilde{G}^*$ to grupas $\tilde{G}$ elementu kopai, kuriem vismaz viena komponente ir nenulles vesels skaitlis. Šīs definīcijas nozīme kļūst skaidra pēc Lemmas 7.2. Skaidrs, ka $G^* = G \cap \tilde{G}^*$.

Mēs arī paplašināsim definīciju (1.2) visiem $b \in \tilde{G}$. Kaut gan mēs uzskatām šo definīciju par lietderīgu, tā jāpielieto uzmanīgi, jo, ja $b \notin G$, tad $\chi_a(b)$ nav viennozīmīgi definēts: izvēloties dažādus veselus skaitļus-reprezentantus atlikumiem $(\mathrm{mod}\, d)_i$, iegūstam dažādas $\chi_a(b)$ vērtības. Šo grūtību var atrisināt, ja pieņem, ka $0 \le a_i < d_i$, darbojoties ar neveseliem b. Atzīmēsim, ka mēs vienmēr lietosim tikai grupas G elementus kā rakstura indeksus a.

Pastāv arī sekojošais Lemmas 1.3 vispārinājums.

Lemma 7.2. *Pieņemsim, ka x ir kopas $\tilde{G}$ elements. Tad $\sum_{y \in G} \chi_y(x) = 0$ tajā un tikai tajā gadījumā, ja $x \in \tilde{G}^*$.*

Pierādījums. Uzrakstām $x = (x_1, x_2, \ldots, x_m)$. Tad:

$$\sum_{y \in G} \chi_y(x) = \prod_{j=1}^{m} \sum_{k=0}^{d_j - 1} \exp\left(\frac{2\pi \mathbf{i}}{d_j} x_j k\right).$$

Lemma seko no fakta, ka vienādojuma $\sum_{k=0}^{d_j-1} \omega^k = 0$ pret ω saknes ir tieši vienīnieka saknes $\exp(\frac{2\pi \mathbf{i}}{d_j} x_j)$, kur x_j ir vesels skaitlis, $0 < x_j < d_j$. ■

Atzīmēsim, ka $G_1 \cong G_2$ ne vienmēr nozīme, ka $\tilde{G}_1 \cong \tilde{G}_2$. Tiešām, ja $G_1 = \mathbb{Z}_6$ un $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_3$, tad $G_1 \cong G_2$, bet $\tilde{G}_1 = \mathbb{R}_6$ un $\tilde{G}_2 = \mathbb{R}_2 \times \mathbb{R}_3$ nav izomorfas. Pirmā ir "viendimensionāla", kamēr otrā ir "divdimensionāla". Liekas skaidrs, ka jo vairāk grupai dimensiju, jo vairāk tajā ir iespējams paveikt. Šo novērojumu var padarīt precīzu.

Mēs tālāk strādāsim ar grupām $\tilde{G}$, kur G ir kaut kāda grupa, ko mēs varām brīvi izvēlēties, ar fiksēto izmēru n. Tādām grupām var ievēst "kanonisko grupu", ar kuru pietiek, lai pārsegt visus gadījumus.

Teorēma 7.3. *Pieņemsim, ka $n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_m^{\ell_m}$ ir skaitļa n sadalījums pirmreizinātājos. Ja G ir grupa ar izmēru n formā (1.1), tad grupu $\tilde{G}$ var ielikt grupā $\tilde{H}$, kur*

$$H = \mathbb{Z}_{p_1}^{\ell_1} \times \mathbb{Z}_{p_2}^{\ell_2} \times \cdots \times \mathbb{Z}_{p_m}^{\ell_m},$$

ar attēlojumu ψ, tā, ka $\psi(\tilde{G}^*) = \psi(\tilde{G}) \cap \tilde{H}^*$.

Pierādījums. Skaidrs, ka pietiek atrast tādu attēlojumu ψ divos gadījumos.

Pirmajā gadījumā $G = \mathbb{Z}_{ab}$, $H = \mathbb{Z}_a\mathbb{Z}_b$ un a un b ir relatīvi pirmskaitļi. Tad, attēlojumu ψ var definēt sekojoši: $\psi(x) = (x \bmod a, x \bmod b)$. Teorēmas apgalvojumi seko no Ķīniešu teorēmas par atlikumiem.

Otrais gadījums ir, kad $G = \mathbb{Z}_{p^k}$ un $H = \mathbb{Z}_p^k$, kur p ir pirmskaitlis. Šajā gadījumā ψ var definēt kā

$$\psi(x) = \left(x \bmod p, \frac{x}{p} \bmod p, \frac{x}{p^2} \bmod p, \ldots, \frac{x}{p^{k-1}} \bmod p \right).$$

Arī šajā gadījumā nav grūti pārbaudīt, ka visi nepieciešamie nosacījumi izpildās. ■

Beidzot atzīmēsim arī, ka Secinājumu 1.4 arī var vispārināt, izmantojot nepārtrauktas grupas $\tilde{G}$.

Apgalvojums 7.4. *Paņemsim jebkuru apakškopu $X \subset \tilde{G}$ izmērā $|G|$, tādu, ka jebkuriem diviem dažādiem $a, b \in X$ ir spēkā $a - b \in \tilde{G}^*$. Tad matrica $F = (f_{xj})$ ($x \in X$, $j \in G$), kas definēta ar $f_{xj} = \chi_j(x)$, ir Adamāra.*

Pierādījums ir līdzīgs Teorēmas 1.4 pierādījumam. Piemēram, ja mēs paņemsim $G = \mathbb{Z}_3 \times \mathbb{Z}_2$ un $X = \{(0,0), (0,1), (1,a), (1,1+a), (2,b), (2,1+b)\}$, kur $0 \le a, b \le 1$ ir

patvaļīgi reāli skaitļi, tad mēs dabūjam matricu

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & z_1 & \omega_3 & \omega_3 z_1 & \omega_3^2 & \omega_3^2 z_1 \\ 1 & -z_1 & \omega_3 & \omega_6^5 z_1 & \omega_3^2 & \omega_6 z_1 \\ 1 & z_2 & \omega_3^2 & \omega_3^2 z_2 & \omega_3 & \omega_3 z_2 \\ 1 & -z_2 & \omega_3^2 & \omega_6 z_2 & \omega_3 & \omega_6^5 z_2 \end{pmatrix},$$

kur $z_1 = e^{\mathbf{i}\pi a}$ un $z_2 = e^{\mathbf{i}\pi b}$. Šī matrica ir ekvivalenta ar vienādojuma (4) matricu rakstā [12]. Šajā rakstā arī tādas matricas tiek sauktas par Furjē matricām. Mēs, savukārt, rezervējam nosaukumu "Furjē matrica" matricām, kas veic galīgas Ābela grupas Furjē transformāciju.

7.2.2. Trīs gadījumi

Tagad mēs sāksim konstruēt MUHu pilnās sistēmas. Pieņemsim, ka matrica B (kā iekš (5.3)) ir grupas $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$ Furjē matrica un $N = \mathbb{Z}_{d'_1} \times \mathbb{Z}_{d'_2} \times \cdots \times \mathbb{Z}_{d'_{m'}}$ ir kāda grupa ar to pašu izmēru. Mēs tagad dosim trīs iespējamos ierobežojumus uz matricām D_Δ, kur katra nākama vispārina iepriekšējo, un aprakstīsim šīs konstrukcijas, izmantojot funkcijas, kas attēlo vienu Ābela grupu otrajā.

1. Pieņemsim, ka visas matricas D_Δ ir vienādas ar grupas N Furjē matricu *ar precizitāti līdz rindu permutācijām* un katra konstruējamas matricas A rindiņa ir arī matricas F rindiņa. Definēsim funkciju $f : G \to N$, kas attēlo matricas A rindas indeksu uz vienādas rindas no F indeksu. Var viegli redzēt, ka šī konstrukcija apmierina Apgalvojuma 5.6 nosacījumus tad un tikai tad, ja f apmierina

$$\forall g_1, g_2, g_3, g_4 \in G : \left.\begin{array}{r} g_1 + g_2 = g_3 + g_4 \\ f(g_1) + f(g_2) = f(g_3) + f(g_4) \end{array}\right\} \Longrightarrow \{g_1, g_2\} = \{g_3, g_4\}. \tag{7.1}$$

2. Tas nav vispārīgākais gadījums. Ja mēs atļausim matricām D_Δ būt vienādam ar Furjē matricu ar precizitāti līdz rindu permutācijām *un atļausim arī katrai kolonai tikt pareizinātai ar* $\chi_a(x_\Delta)$, kur a ir kolonas indekss un x_Δ ir kaut kāds elements no $\tilde{N}$, tad mēs varam paņemt matricu $A = (a_{\ell r})$, $(\ell \in G, r \in N)$ definētu ar

$a_{\ell r} = \chi_r(f(\ell))$, kur funkcija $f : G \to \tilde{N}$ apmierina

$$\forall g_1, g_2, g_3, g_4 \in G : \left.\begin{array}{c} g_1 + g_2 = g_3 + g_4 \\ \{g_1, g_2\} \neq \{g_3, g_4\} \end{array}\right\} \Longrightarrow f(g_1) + f(g_2) - f(g_3) - f(g_4) \in N^*. \tag{7.2}$$

3. Beidzot, no Lemmas 7.2 ir skaidrs, ka iepriekšējais piegājiens dod pilno MUHu sistēmu tad un tikai tad, ja funkcija $f : G \to \tilde{N}$ apmierina

$$\forall g_1, g_2, g_3, g_4 \in G : \left.\begin{array}{c} g_1 + g_2 = g_3 + g_4 \\ \{g_1, g_2\} \neq \{g_3, g_4\} \end{array}\right\} \Longrightarrow f(g_1) + f(g_2) - f(g_3) - f(g_4) \in \tilde{N}^*. \tag{7.3}$$

Taču šajā gadījumā matricas D_Δ vairs nav ekvivalentas ar Furjē matricām. Tie kļūst ekvivalenti ar vispārīgākām matricām no Apzīmējuma 7.4.

Saliekot visu kopā, mēs iegūstam tādu rezultātu:

Teorēma 7.5. *Nosacījums (7.3) ir vispārīgāks par nosacījumu (7.2), kas, savukārt, ir vispārīgāks par nosacījumu (7.1). Formula*

$$(v_k^{(r)})_\ell = \frac{1}{\sqrt{n}} \chi_k(\ell)\chi_r(f(\ell)), \tag{7.4}$$

(ar $k, \ell \in G$ un $r \in N$) dod pilno MUHu sistēmu tad un tikai tad, ja funkcija f, kas attēlo G iekš $\tilde{N}$, apmierina (7.3).

Līdzīgs, taču ne tik vispārīgs rezultāts ir atrodams rakstā [60]. Mēs atliksim saistītu rezultātu apskatu līdz Sadaļai 7.2.4.. Nākamajās sadaļās mēs dosim zināmus MUHu konstrukcijas no Sadaļas 2.1.1. no iepriekšējā piegājiena skatpunkta.

7.2.3. Zināmas konstrukcijas

Tagad mēs dosim divas zināmas MUHu pilno sistēmu konstrukcijas Teorēmas 7.5 terminos.

Konstrukciju, kas ir pēc būtības ekvivalenta ar nākamo, aprakstīja Ivanovičs rakstā [45] priekš $GF(p)$, vispārīgs gadījums pieder Fīldsam un Vūteram [74].

Lemma 7.6. *Ja $n = p^k$ ir nepāra pirmskaitļa pakāpe, tad funkcija $f(x) = x^2$, kur $G = N$ ir galīga lauka $GF(n)$ adītiva grupa (t.i., $\mathbb{Z}_p^k$) apmierina (7.1).*

Pierādījums. Pieņemsim, ka $g_1 + g_2 = g_3 + g_4$ un $g_1^2 + g_2^2 = g_3^2 + g_4^2$. Tad $g_1 - g_3 = g_4 - g_2$ un $(g_1 - g_3)(g_1 + g_3) = (g_4 - g_2)(g_4 + g_2)$. Ja $g_1 = g_3$, viss ir pierādīts.

Citādi mēs varam izdalīt iepriekšējo vienādību ar $g_1 - g_3$ (šeit mēs izmantojām to, ka $GF(n)$ ir lauks) un iegūst $g_1 + g_3 = g_4 + g_2$. Kopā ar iepriekšējo vienādību tas dod $2(g_2 - g_3) = 0$. Tā kā 2 ir relatīvs pirmskaitlis ar p, $g_2 = g_3$ un lemma ir pierādīta. ■

Šī konstrukcija dod gandrīz tādu pašu MUHu sistēmu kā Teorēmā 2.2, izņemot to, ka mēs neizmantojam raksturus definētus ar (2.2), bet raksturus definētus ar (1.2). Pirmā izmanto pēdas funkciju, kas ir $GF(p^k)$ aditīvu raksturu specifika; otrā izmanto "skalāro reizinājumu", kas ir specifisks grupas $\mathbb{Z}_p^k$ raksturiem. Šī izmaiņa neko neiespaido, jo raksturi paliek tie paši, izmainās tikai atbilstība starp grupas elementiem un raksturiem, un tas izpaužas tikai rindu permutācijā. Dažreiz identitātes līdzīgas (2.3) ir nepieciešamas (kā to pielietošanas kvantu skaitļošanā piemēru var minēt rakstu [21]), bet mūsu gadījumā mēs varam izvēlēties tādu raksturu reprezentāciju, kura mums vairāk patīk.

Piezīme 7.7. Tātad, ar iepriekšējo rezultātu mēs parādījām, ka virs grupas $G = \mathbb{Z}_p^k$, kur p ir nepāra pirmskaitlis, matrica M, kas sastāv tikai no vieniniekiem ir apmierināma. Patiesībā, no Teorēmas 3.2 izriet, ka šī matrica ir apmierināma arī ar cirkulāru P, ja $p \geq 5$.

Ja n ir pāra, mums jābūt viltīgākiem. Atgādināsim, ka parasta galīga lauka $GF(2^k)$ konstrukcija ir kā polinomu kopa, kur katrs polinoms ir ar pakāpi mazāku par k un ar koeficientiem no $\{0, 1\}$. Visas operācijas tiek veiktas pēc moduļa 2 un h, kur h ir polinoms ar pakāpi k, kas ir nesadalāms reizinātājos virs $GF(2)$. Mēs izturēsimies pret šiem polinomiem, kā pret polinomiem ar veseliem koeficientiem. No nākamas lemmas var dabūt MUHu konstrukciju, ko pirmo reizi dabūja Fīldss un Vūters rakstā [74].

Lemma 7.8. *Pieņemsim, ka G ir galīga lauka $GF(2^k)$ aditīva grupa. Tad funkcija $f : G \to \tilde{G}$, kas definēta ar*

$$f(x) = \frac{x^2}{2} \bmod (2, h)$$

apmierina (7.2) ar $N = G$.

Pierādījums. Pieņemsim, ka $g_1 + g_2 \equiv g_3 + g_4 \pmod{2, h}$. Tad $(g_1 + g_2)^2 \equiv (g_3 + g_4)^2 \pmod{2, h}$. Tādējādi, $g_1^2 + g_2^2 - g_3^2 - g_4^2 \equiv 0 \pmod{2, h}$. Tas nozīmē, ka

$$f(g_1) + f(g_2) - f(g_3) - f(g_4) = \frac{g_1^2 + g_2^2 - g_3^2 - g_4^2}{2} \bmod (2, h)$$

ir polinoms ar veseliem koeficientiem. Vienīgais veids, kā tas varētu nepiederēt N^* būtu, ja tas būtu vienāds ar 0. Pieņemsim, ka tas ir vienāds ar nulli un pierādīsim, ka šajā gadījumā $\{g_1, g_2\} = \{g_3, g_4\}$.

Definēsim $s = (g_1 + g_2) \bmod 2$. Tad arī $g_1^2 + g_2^2 \equiv s^2 \pmod 2$. Aplūkosim sekojošu vienādojumu mainīgā x:

$$\frac{g_1^2 + g_2^2 - x^2 - (s-x)^2}{2} \equiv 0 \pmod{h, 2}.$$

Abi g_1 un g_2 ir tā saknes. Šo polinomu var pārrakstīt kā $\frac{g_1^2+g_2^2-s^2}{2} + sx - x^2$. Var pamanīt, ka $\frac{g_1^2+g_2^2-s^2}{2}$ ir polinoms ar veseliem koeficientiem, tātad, paņemot to pēc moduļa h un 2, mēs iegūstam otrās pakāpes vienādojumu laukā $GF(2^k)$:

$$x^2 - sx - \frac{g_1^2 + g_2^2 - s^2}{2} = 0.$$

Ja $g_1 \neq g_2$, neviens cits elements izņemot tos nevar apmierināt šo vienādojumu. Ja $g_1 = g_2$, tad $s = 0$ un šīm vienādojumam ir tikai viena sakne, jo attēlojums $x \mapsto x^2$ ir kopas $GF(2^k)$ bijekcija pašai uz sevi (tā saucamais Frobeniusa attēlojums (**Frobenius map**)). Tātad, f apmierina (7.2). ■

Divas iepriekšējas lemmas var sakombinēt sekojošajā labi zināmajā rezultātā:

Teorēma 7.9. *Ja n ir pirmskaitļa pakāpe, tad telpā $\mathbb{C}^n$ eksistē pilna MUBu sistēma.*

Tālāk mums noderēs sekojošais novērojums:

Piezīme 7.10. Matricas A kolonu permutācija neiespaido nosacījuma (5.6) izpildi. Arī, laukā $GF(2^k)$ attēlojums $x \mapsto x^2$ ir bijekcija. Tātad, ja mēs definēsim $A = (a_{ij})$ ar

$$a_{ij} = \chi_{j^2}\left(\frac{i^2}{2} \bmod (2, h)\right),$$

mēs joprojām iegūstam matricu, kas apmierina (5.6).

Bet šai matricai ir papildus īpašība, ka $A^{(2)}$ ir simetriska reāla Adamāra matrica, jo

$$a_{ij}^2 = \chi_{j^2}(i^2) = \chi_{i^2}(j^2) = a_{ji}^2.$$

Piemēram, ja mēs paņemsim $k = 2$ un $h = x^2 + x + 1$, mēs iegūsim sekojošu matricu:

$$A' = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i} & \mathbf{i} & 1 \\ 1 & -\mathbf{i} & -1 & -\mathbf{i} \\ 1 & 1 & \mathbf{i} & \mathbf{i} \end{pmatrix}, \tag{7.5}$$

kur rindas un kolonas ir indeksētas ar $0, 1, x, x+1$. Mēs izmantosim šo matricu Sadaļā 7.3..

7.2.4. Saistītas kombinatoriskas struktūras

Aplūkojot formulas (7.1), (7.2) un (7.3) var secināt, ka tām, īpaši formulai (7.1), ir kombinatoriska daba. Izrādās, ka pastāv saite starp šīm funkcijām un dažiem labi izpētītiem kombinatoriskiem objektiem.

Pieņemsim, ka G un N ir galīgas Ābela grupas tādas, ka $|G| \leq |N|$. Funkcijas $f : G \to N$ tādas, ka vienādojumam $f(x+a)-f(x) = b$ ir ne vairāk kā viens atrisinājums visiem $a, b \in G$, nevienādiem ar nulli vienlaicīgi, sauc par *diferenciāli 1-vienmērīgam* (**differentially 1-uniform**) [55]. Ja N apmierina $|G|/|N| = m \in \mathbb{N}$ un funkcija $f : G \to N$ ir tāda, ka $|\{x \in G \mid f(x+a) - f(x) = b\}| = m$ visiem $b \in N$ un nenulles $a \in G$, tad funkciju sauc par *perfekti nelineāru* (**perfect non-linear**) [18]. Šīs funkcijas, atskaitot citus pielietojumus, izmanto arī kriptogrāfijā, lai konstruētu S-kastes (**S-boxes**), kas ir drošas pret diferenciālu kriptoanalīzi (**differential cryptanalysis**).

Ja $|G| = |N|$, ka formulā (7.1), tad šie divi jēdzieni sakrīt, un funkciju f dažreiz sauc par *planāru funkciju* (**planar function**). Šis nosaukums atspoguļo to, ka, izmantojot tādas funkcijas, var uzkonstruēt galīgu afīno plakni (**affine plane**) [24]. Funkcijām, kas apmierina nosacījumu (7.2) mēs lietosim nosaukumu *frakcionāli planāras*.

Sekojošas planāras funkcijas no kopas $GF(p^k)$, kur p ir nepāra pirmskaitlis, ir zināmas:

- $f(x) = x^{p^\alpha+1}$, kur α ir nenegatīvs vesels skaitlis tāds, ka $k/\gcd(k,\alpha)$ ir nepāra skaitlis [24].
- $f(x) = x^{(3^\alpha+1)/2}$ tikai, ja $p = 3$, α ir nepāra un $\gcd(k,\alpha) = 1$ [20].
- $f(x) = x^{10} - ux^6 - u^2x^2$ tikai, ja $p = 3$, k ir nepāra un u ir nenulles kopas $GF(p^k)$ elements. Šīs konstrukcijas speciālais gadījums $u = -1$ tika dabūts rakstā [20], vispārīgā konstrukcija ir no [26].

Konstrukcija ar $f(x) = x^2$, kuru mēs izmantojām iepriekšējā sadaļā ir no pirmās klases.

Pieņemsim, ka K ir Ābela grupa un N ir tās apakšgrupa. Apakškopu $R \subset K$ sauc par *relatīvu* (m, n, r, λ)*-starpību kopu* (**relative** (m, n, r, λ)**-difference set**), ja $|K| = nm$, $|N| = n$, $|R| = r$ un

$$|\{r_1, r_2 \in R \mid r_1 - r_2 = b\}| = \begin{cases} r & , \quad b = 0; \\ 0 & , \quad b \in N \setminus \{0\}; \\ \lambda & , \quad b \in K \setminus N. \end{cases}$$

Relatīvā starpību kopa ir klasiskas starpību kopas vispārinājums, un tika ievests rakstā [27]. Ja $r = m$, starpību kopu sauc par *semiregulāru* (**semiregular**). Relatīvu starpību kopu sauc par *sadalāmu* (**splitting**), ja $K = G \times N$, t.i., ja apakšgrupai N ir papildinājums grupā K.

Šis jēdziens ir interesants mums sekojoša viegla novērojuma dēļ (skat., piem., [56]). Pieņemsim, ka G un N ir patvaļīgas galīgas grupas un f ir funkcija no G grupā N. Kopa $\{(x, f(x)) \mid x \in G\}$ ir semiregulāra sadalāma $(|G|, |N|, |G|, |G|/|N|)$-starpību kopa grupā $G \times N$ relatīvi pret $\{1\} \times N$ tajā un tikai tajā gadījumā, kad f ir perfekti nelineāra. Tādējādi, planāras funkcijas atbilst sadalāmām relatīvām $(n, n, n, 1)$-starpību kopām. Mēs nedaudz vispārinām šo rezultātu:

Teorēma 7.11. *Pieņemsim, ka K ir Ābela grupa ar izmēru n^2 un ar apakšgrupu $N = \mathbb{Z}_{d'_1} \times \mathbb{Z}_{d'_2} \times \cdots \times \mathbb{Z}_{d'_{m'}}$ ar izmēru n. Sekojoši divi apgalvojumi ir ekvivalenti:*

(a) Eksistē semiregulāra $(n, n, n, 1)$-starpību kopa R grupā K relatīvi pret N.

(b) Eksistē frakcionāla planāra funkcija $f : G \to \tilde{N}$, kur $G \cong K/N$.

Pierādījums. Pieņemsim, ka eksistē relatīva starpību kopa. Fiksēsim kaut kādu $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$ tādu, ka $G \cong K/N$. Paņemsim tādus kopas K elementus k_i, $i = 1, \ldots, m$, ka faktorizējot pēc N un pielietojot izomorfismu tie tiek attēloti uz i-to grupas G bāzes elementu, t.i., elementu $(0, \ldots, 0, 1, 0, \ldots, 0)$, kur pirms vienīnieka stāv $i - 1$ nulle. Apzīmēsim ar $(s_{1i}, s_{2i}, \ldots, s_{m'i})$ elementu $d_i k_i \in N$, $i = 1, \ldots m$.

Definēsim Ābela grupu K' sekojošajā veidā. Tās elementu kopa ir Dekarta reizinājums $G \times N$ un elementu summa $(x_1, x_2, \ldots, x_m; y_1, y_2, \ldots, y_{m'})$ un $(z_1, z_2, \ldots, z_m; t_1, t_2, \ldots, t_{m'})$ tiek definēta kā $(a_1, a_2, \ldots, a_m; b_1, b_2, \ldots, b_{m'})$, kur $a_i = x_i + z_i$ un

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m'} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{m'} \end{pmatrix} + \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_{m'} \end{pmatrix} + \begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1m} \\ s_{21} & s_{22} & \cdots & s_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m'1} & s_{m'2} & \cdots & s_{m'm} \end{pmatrix} \begin{pmatrix} [x_1 + z_1 \geq d_1] \\ [x_2 + z_2 \geq d_2] \\ \vdots \\ [x_m + z_m \geq d_m] \end{pmatrix} \tag{7.6}$$

kur izteiksme $[x_i + z_i \geq d_i]$ ir vienāda ar 1, ja summa $x_i + z_i$, paņemot saskaitāmus, kā veselus skaitļus, ir lielāka vai vienāda ar d_i, un vienāda ar 0 pretējā gadījumā. Nav grūti pārbaudīt, ka attēlojums $\varphi : K' \to K$, kas definēts ar

$$(x_1, x_2, \ldots, x_m; y) \mapsto y + \sum_{i=1}^{m} x_i k_i,$$

ir grupu izomorfisms. Kā parasti, mēs identificējām G ar kopu $\{(x,0) \mid x \in G\}$ un N — ar kopu $\{(0;y) \mid y \in N\}$.

Definēsim S kā $m' \times m$-matricu, kuras (i,j)-ais elements ir vienāds ar s_{ij}/d_i. Skaidrs, ka $\psi : K' \to \tilde{N}$, kas definēts ar

$$\psi(x,y) = y + Sx$$

ir morfisms. Tā kā R ir semiregulāra relatīva starpību kopa, katram $x \in K/N$ var atrast vienu vienīgu elementu $r_x \in R$ ar projekciju uz K/N vienādu ar x. Definēsim $f(x) = \psi(\varphi^{-1}(r_x))$.

Mēs pierādīsim, ka f ir frakcionāli planāra. Pirmkārt, atzīmēsim, ka visiem $x \in G$ izpildās $\varphi^{-1}(r_x) = (x,y)$ kādam $y \in N$. Tad pieņemsim, ka $g_1, g_2, g_3, g_4 \in G$ ir tādi, ka $g_3 - g_1 = g_2 - g_4 \neq 0$ un $g_1 \neq g_4$. Apzīmēsim $(x_1, y_1) = \varphi^{-1}(r_{g_3} - r_{g_1})$ un $(x_2, y_2) = \varphi^{-1}(r_{g_2} - r_{g_4})$. Izpildās $x_1 = x_2$ (tā kā $g_3 - g_1 = g_2 - g_4$) un $y_1 \neq y_2$ (tā kā $r_{g_3} - r_{g_1} \neq r_{g_2} - r_{g_4}$). No funkcijas ψ definīcijas seko, ka $(f(g_3) - f(g_1)) - (f(g_2) - f(g_4)) \in N^*$.

Tagad pieņemsim, ka mums ir dota frakcionāli planāra funkcija $f : G \to \tilde{N}$ ar tādām pašām izteiksmēm priekš G un N. Definēsim funkciju $\{\cdot\}$, kas paņem katras elementa no $\tilde{N}$ komponentes daļveida daļu. Definēsim arī funkciju $\tilde{f}(x) = \{f(x)\}$. Tad no (7.2) izriet, ka

$$(a + b = c + d) \Longrightarrow (\tilde{f}(a) + \tilde{f}(b) - \tilde{f}(c) - \tilde{f}(d) \in N).$$

Tā kā nosacījums uz f nemainās, pieskaitot funkcijai konstanti, mēs varam pieņemt, ka $\tilde{f}(0) = 0$. Tad $\tilde{f}(a+b) = \{\tilde{f}(a) + \tilde{f}(b)\}$. Tagad ir viegli pārliecināties, ka $\tilde{f}(x) = \{Sx\}$, kur S ir definēta līdzīgā veidā kā iepriekš kaut kādiem veseliem skaitļiem s_{ij}.

Definēsim K' kā formulā (7.6) un

$$R = \{(x; f(x) - Sx) \mid x \in G\}.$$

Līdzīgi kā iepriekš var pierādīt, ka R ir semiregurāla starpību kopa relatīvi pret N. ■

Tātad, mēs esam pierādījuši, ka ja matrica B no (5.3) ir Furjē matrica un visas matricas D_Δ ir ekvivalentas (zināmā mērā) Furjē matricām, tad pilnās MUHu sistēmas eksistence ir ekvivalenta relatīvas $(n,n,n,1)$-starpību kopas eksistencei. Patiesībā var pierādīt vispārīgāku rezultātu [34]: relatīvas (n,k,n,λ)-starpību kopas eksistence implicē k MUHu sistēmas eksistenci telpā $\mathbb{C}^n$. Visas zināmas pilno MUHu sistēmas konstrukcijas ir šīs konstrukcijas speciālie gadījumi.

Diemžēl ir pierādīts [15], ka relatīva $(n,n,n,1)$-starpību kopa eksistē tikai tajā gadījumā, kad n ir pirmskaitļa pakāpe. Tātad, izmantojot pieeju ar funkciju f, kas apmierina

nosacījumu (7.2), nav iespējams konstruēt pilno MUBu sistēmu kādā jaunā dimensijā. Bet vēl paliek iespējas ar vispārīgām Adamāra matricām D_Δ un, starp citu, arī gadījums, kad funkcija f apmierina nosacījumu (7.3).

7.3. SIC-POVMi dimensijā 2^k

Šajā sadaļā mēs aplūkosim SIC-POVMus dimensijā 2^k un parunāsim par dažām konstruēšanas idejām.

Kā jau tika pieminēts Sadaļā 2.2.1., analītiskas izteiksmes fiduciāriem vektoriem ir zināmas dimensijās 2, 4 un 8. Piemēram, telpā $\mathbb{C}^2$ tas ir vektors no (2.5). Šie, pieminētie Sadaļā 2.2.1. SIC-POVMi ir kovarianti pret grupām $\mathrm{GP}(\mathbb{Z}_2), \mathrm{GP}(\mathbb{Z}_4)$ un $\mathrm{GP}(\mathbb{Z}_8)$, attiecīgi. Telpā $\mathbb{C}^8$ vēl viens SIC-POVMs tika uzkonstruēts vēl pirms jau pieminētā [41], un tas ir kovariants attiecībā pret $\mathrm{GP}(\mathbb{Z}_2^3)$ [34]. Mēs dosim ekvivalenta SIC-POVMa aprakstu, izmantojot homogēnu konstrukciju. Paņemsim $G = \mathbb{Z}_2^3$ un

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}} I & \frac{1}{\sqrt{6}} A' \\ \frac{1}{\sqrt{6}} A' & \frac{i}{\sqrt{3}} I \end{pmatrix},$$

kur I ir 4×4 vienības matrica un A' ir matrica no (7.5). Mēs pierādīsim, ka matrica A apmierina visus Teorēmas 6.1 nosacījumus. Pieņemsim, ka A rindas un kolonas ir sanumurētas ar $(0,0,0), (0,0,1), \ldots, (1,1,0), (1,1,1)$.

Nosacījumu 1 un 2 pārbaude ir triviāla. Nosacījumam 3 jāpamana, ka

$$\|R_i^{(2)}\| = \sqrt{\frac{1}{9} + 4\frac{1}{36}} = \frac{\sqrt{2}}{3}$$

un

$$\|R_i \circ R_j\| = \begin{cases} \sqrt{4\frac{1}{36}} & , \quad i \text{ un } j \text{ ir no viena bloka} \\ \sqrt{2\left(\frac{1}{3}\right)\left(\frac{1}{6}\right)} & , \quad \text{citādi} \end{cases} = \frac{1}{3}.$$

Lai pierādītu, ka Nosacījums 4 arī izpildās, mēs aprakstīsim, kā izskatās vektors $R = \overline{R_{g_1} \circ R_{g_2}} \circ R_{g_3} \circ R_{g_4}$ un pierādīsim, ka tā elementu summa ir nulle. Pastāv divas iespējas:

- Ja visi g_1, g_2, g_3, g_4 ir no viena, teiksim, no pirmā bloka, tad R izskatās kā

  $$(0,0,0,0, a_{(0,0)}, a_{(0,1)}, a_{(1,0)}, a_{(1,1)})$$

  un nosacījums izpildās, jo matrica A' apmierina (5.6) priekš $\mathbb{Z}_2^2$. (Tas ir līdzīgi Teorēmas 5.5 pierādījumam).

- Pieņemsim, ka tie ir no dažādiem blokiem. Teiksim, g_1, g_2 ir no pirmā bloka un g_3, g_4 ir no otrā bloka. Izpildās vienādība $g_1 + g_2 = g_3 + g_4$. Apzīmēsim šo kopīgo vērtību ar d. Ja $d \neq 0$, tad R sastāv tikai no nullēm. Ja $g_1 = g_2$ un $g_3 = g_4$ tad vektoram R ir tieši divi nenulles elementi: viens pozīcijā g_1 ar vērtību $a^2_{g_3', g_1}$, un otrais — pozīcijā g_3 ar vērtību $-a^2_{g_1, g_3'}$, kur $A = (a_{ij})$ un $g_3' = g_3 + (1, 0, 0)$. Tad R elementu summa ir nulle, jo $A'^{(2)}$ ir simetriska.

Diemžēl, tāda redukcija no MUHiem uz SIC-POVMiem ir iespējāma tikai priekš $\mathbb{Z}_2^3$ Nosacījuma 3 dēļ. Arī, kā pierādīts rakstā [34], neeksistē SIC-POVMs kovariants pret $\mathrm{GP}(\mathbb{Z}_2^k)$, ja $k \neq 1$ un $k \neq 3$.

Tagad mēs nodarbosimies ar gadījumu $n = 4$. Teorēmā 7.1 tika doti nepieciešamie un pietiekamie nosacījumi, lai cirkulāra virs $\mathbb{Z}_3$ matrica būtu apmierināma. Grupu $G = \mathbb{Z}_2$ un $G = \mathbb{Z}_2^2$ gadījumā nosacījumi ir vēl vienkāršāki:

Apgalvojums 7.12. *Jebkura matrica M, cirkulāra virs $\mathbb{Z}_2$ vai $\mathbb{Z}_2^2$, ir apmierināma. Priekš $\mathbb{Z}_2$ matricu P var paņemt cirkulāru.*

Pierādījums. Jāizmanto matricas

$$P = \begin{pmatrix} 1 & \omega_8 \\ \omega_8 & 1 \end{pmatrix} \quad \text{un} \quad P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i} & 1 & \mathbf{i} \\ 1 & -\mathbf{i} & -\mathbf{i} & 1 \\ 1 & 1 & \mathbf{i} & -\mathbf{i} \end{pmatrix},$$

attbilstoši. Otrajā matricā rindas un kolonas ir sanumurētas ar $(0,0), (0,1), (1,0), (1,1) \in \mathbb{Z}_2^2$. Ar tiešo pārbaudi var pārliecināties, ka šīs matricas tiešām der. ■

Ja mēs paņemsim matricu M tādu kā formulā (6.4) priekš $n = 4$ un matricu P no iepriekšējā apgalvojuma, mēs dabūsim SIC-POVMu telpā $\mathbb{C}^4$. Tas sastāv no 16 vektoriem — sekojošas matricas kolonām:

$$\begin{pmatrix} b & a & a & a & b & a & a & a & b & a & a & a & b & a & a & a \\ a & \mathbf{i}b & a & \mathbf{i}a & -a & -\mathbf{i}b & -a & -\mathbf{i}a & a & \mathbf{i}b & a & \mathbf{i}a & -a & -\mathbf{i}b & -a & -\mathbf{i}a \\ a & -\mathbf{i}a & -\mathbf{i}b & a & a & -\mathbf{i}a & -\mathbf{i}b & a & -a & \mathbf{i}a & \mathbf{i}b & -a & -a & \mathbf{i}a & \mathbf{i}b & -a \\ a & a & \mathbf{i}a & -\mathbf{i}b & -a & -a & -\mathbf{i}a & \mathbf{i}b & -a & -a & -\mathbf{i}a & \mathbf{i}b & a & a & \mathbf{i}a & -\mathbf{i}b \end{pmatrix}$$

kur

$$a = \frac{1}{2}\sqrt{1 - \frac{1}{\sqrt{5}}} \qquad \text{un} \qquad b = \frac{1}{2}\sqrt{1 + \frac{3}{\sqrt{5}}}.$$

Šī izteiksme izskatās ārkārtīgi vienkārši, jo izmanto tikai četras fāzes — $1, \mathbf{i}, -1$ un $-\mathbf{i}$, kā arī tikai divus moduļus — a un b. Kā atzīmēja Grasls [38], pielietojot šīm SIC-POVMam unitāru matricu

$$\begin{pmatrix} 1 & 0 & 0 & -\omega_8 \\ 0 & -\omega_8^3 & 1 & 0 \\ 1 & 0 & 0 & \omega_8 \\ 0 & -\omega_8^3 & -1 & 0 \end{pmatrix},$$

var dabūt SIC-POVMu, kas, ar precizitāti līdz elementu permutācijai un elementu reizināšanai ar skalāriem, ir kovariants attiecībā pret $\mathrm{GP}(\mathbb{Z}_4)$.

Matricas P, kas nav atkarīgas no matricas M, kā Teorēmā 7.12 izskatās interesantas, jo tiem var būt ļoti vienkārši elementi, kā matricām no Apgalvojuma 7.12, pat ja matricai M ir komplicēti elementi. Teorētiski, tādas matricas varētu eksistēt grupām $G = \mathbb{Z}_2^k$. Iemesls šim ir sekojošs. Pieņemsim, ka M ir cirkulāra virs G matrica, $g_1, g_2, g_3, g_4 \in G$ ir tādi, ka $g_1 + g_2 = g_3 + g_4$ un d ir patvaļīgs grupas G elements. Aplūkosim matricas M 4×4-apakšmatricu M', kas atrodas rindu $\{g_1, g_2, g_3, g_4\}$ un kolonu $\{d, d+g_1+g_2, d+g_1+g_3, d+g_1+g_4\}$ krustojumā. Tā ir cirkulāra matrica virs $\mathbb{Z}_2^2$. Starp citu tas nozīmē, ka vektorā $\overline{R_{g_1} \circ R_{g_2}} \circ R_{g_3} \circ R_{g_4}$, kur R_i ir matricas $A = M \circ P$ i-tā rindiņa, visi elementi ar indeksiem $\{d, d+g_1+g_2, d+g_1+g_3, d+g_1+g_4\}$ ir ar vienādu absolūto vērtību. Ja P ir tāda, ka fāžu summa šajās četrās pozīcijās ir nulle, un tas izpildās visām g_1, g_2, g_3, g_4 un d vērtībām, tad matrica $A = M \circ P$ apmierina visus nosacījumus neatkarīgi no cirkulāras matricas M elementu vērtībām.

Diemžēl, var pierādīt, ka dimensijām lielākām par 4, tādas matricas neeksistē [10]. Šajā darbā ir pierādīts arī, ka tamlīdzīgas matricas neeksistē pat pieņēmumā, ka matricai M visas vērtības ārpus diagonāles ir vienādas savā starpā. Tādas matricas rodas, izmantojot simpleksu, uzdotu ar 6.4. Protams, tas nenozīmē, ka līdzīgas idejas nevar pielietot kombinācijā ar citām idejām.

Noslēgums

Šajā darbā mēs esam parādījuši, ka konstrukcijām, kas tiek pielietotas kvantu informācijas teorijā (piemēram, kvantu stāvokļu tomogrāfijā), ir daudz kopīga ar virknēm ar mazu savstarpēju korelāciju. Viens no šiem kopīgajiem jēdzieniem ir labi zināmais apakšējais novērtējums virkņu savstarpējai korelācijai — Velča nevienādība. Tā dod labu raksturojumu tādām sistēmām kā MUBu pilnās sistēmas un SIC-POVMi. Šī saistība ir zināma arī komplekso projektīvu dizainu terminos.

Mēs esam formulējuši kritēriju, kas reducē MUBu pilnās sistēmas vai SIC-POVMa (vai, vispārīgāk, patvaļīga kompleksā projektīvā t-dizaina) eksistenci uz nosacījumu, kas izmanto noteiktas vektoru sistēmas W ortonormalitāti. Mēs varam pieminēt sekojošas šī kritērija priekšrocības:

Ortogonalitāte Abas MUBu un SIC-POVMu definīcijas izmanto tādus leņķus, kā $\frac{1}{n}$ vai $\frac{1}{n+1}$. Mūsu kritērijs atļauj definēt šos objektus tikai vektoru ortogonalitātes terminos. Skaidrs, ka tā ir daudz vairāk izpētīta un skaidrāka vektoru attiecība.

Fāžu un moduļu atdalījums Problēmu var sadalīt divos posmos. Pirmajā jānodrošina, lai visiem vektoriem no W būtu vienāds garums. Šajā posmā mēs nosakām vektoru elementu absolūtās vērtības. Nākamajā posmā šīm vērtībām jāpiemeklē fāzes, lai izpildītos ortogonalitātes nosacījums. Ar pirmo uzdevumu parasti var diezgan viegli tikt galā (skat., piemēram, Nodaļu 6.). Otra problēma izrādās daudz sarežģītāka.

Modularitāte Mūsu piegājiens arī atļauj raksturot katras sistēmas daļas ieguldījumu konstrukcijā. Tas atļauj aizvietot dažas sistēmas daļas ar citām. Piemēram, MUHu pilnā sistēmā vienu Adamāra matricu var aizvietot ar citu, ja svari uz K-grafa šķautnēm abos grafos ir vienādi (skat. Sadaļu 5.2.).

Mēs arī definējām homogēnas sistēmas, kas ir gan MUHu, gan SIC-POVMu speciāls gadījums, kas raksturo katru no šīm sistēmām ar divām $n \times n$-matricām, kurām nosacījumi

ir ļoti līdzīgi nosacījumiem visai sistēmai. Mēs aprakstām šo nosacījumu ar L-grafu jēdzienu. Šajā piegājienā saglabājas tikko aprakstītās priekšrocības. Modularitāte kļūst vēl izteiktāka: vienu no šīm divām matricām var aizstāt ar citu matricu, ja jaunas matricas L-grafs pārklāj vecās matricas L-grafu.

Homogēnu sistēmu piegājiens arī izceļ Furjē matricas kā kompleksas Adamāra matricas, kurām L-grafā ir ļoti daudz šķautņu. Turklāt šīs matricas ir jaukas ar to, ka tās var ļoti viegli aprakstīt, kad L-grafam trūkst šķautne, izsakot to ar vienkāršo vienādību, kas iesaista attiecīgos grupu elementus. Ja, konstruējot MUHu pilno sistēmu, vienu no matricām izvēlas vienādu ar Furjē matricu, tad nosacījumi otrai matricai dabiski noved līdz planārām funkcijām un dažādiem to vispārinājumiem.

Galvenais mūsu piegājiena trūkums ir diezgan sarežģītas sakarības starp sākotnējiem vektoru sistēmas elementiem un W elementiem. Tas padara fāžu meklējumus par diezgan sarežģītu uzdevumu pat, ja visas matricas elementu absolūtās vērtības ir vienādas, kā MUHu gadījumā.

Mūsuprāt, perspektīvākie virzieni, kuros varētu meklēt jaunus SIC-POVMus un MUHus būtu, pirmkārt, homogēni SIC-POVMi, kuri nav grupu kovarianti, un, otrkārt, funkcijas, kuras apmierina (7.3), bet neapmierina (7.2). Abi šie gadījumi ir tuvi perspektīviem virzieniem, kuros ir atrasti daudz piemēri, taču tieši šiem gadījumiem īpaša uzmanība līdz šim netika veltīta. Varētu arī aplūkot sistēmas, kuras ir tuvas šīm.

No neeksistēšanas viedokļa būtu interesanti uzzināt, vai eksistē kādas citas L-maksimālas Adamāra matricas, izņemot Furjē matricas, un vai tās var kaut kā pielietot, konstruējot 2-dizainus. SIC-POVMu gadījumā var uzdot analoģisku jautājumu: vai ir iespējams uzkonstruēt homogēnu SIC-POVMu, kas izmanto L-maksimālu plakanu matricu, kura nav Furjē matrica.

Izmantotā literatūra un avoti

[1] Aharonov, Y., Englert, B.-G.: The mean kings problem: Spin 1. Zeitschrift für Naturforschung 56a, 16–19 (2001)

[2] Alltop, W.O.: Complex sequences with low periodic correlations. IEEE Transactions on Information Theory 26(3), 350–354 (1980)

[3] Ambainis, A., Mosca, M., Tapp, A., deWolf, R.: Private Quantum Channels. 41st Symposium on Foundations of Computer Science, 547—553 (2000)

[4] Ambainis, A., Emerson, J.: Quantum t-designs: t-wise independence in the quantum world. arXiv:quant-ph/0701126v2 (2007)

[5] Ambainis, A., Bouda, J., Winter, A.: Tamper-resistant encryption of quantum information. arXiv:0808.0353v1 (2008)

[6] Appleby, D.M.: SIC-POVMs and the Extended Clifford Group. Journal of Mathematical Physics 46, 052107, arXiv:quant-ph/0412001 (2004)

[7] Appleby, D.M., Dang, H.B., Fuchs, C.A.: Physical significance of symmetric informationally complete sets of quantum states. arXiv:0707.2071v1 (2007)

[8] Barnum, H.: Information-disturbance tradeoff in quantum measurement on the uniform ensemble. Proceedings of IEEE International Symposium on Information Theory 2001, 277, arXiv:quant-ph/0205155v1 (2002)

[9] Belovs, A., Smotrovs, J.: A Criterion for Attaining the Welch Bounds with Applications for Mutually Unbiased Bases. Mathematical Methods in Computer Science 2008, Lecture Notes in Computer Science 5393, 50—69. arXiv:0802.0855v2 (2008)

[10] Belovs, A.: Welch Bounds and Quantum State Tomography. Master's thesis, University of Waterloo, hdl.handle.net/10012/4159 (2008)

[11] Beth, T., Jungnickel, D., Lenz, H.: Design Theory (Second Edition). Cambridge University Press (1999)

[12] Bengtsson, I., Bruzda, W., Ericsson, A., Larsson, J.-A., Tadej, W., Zyczkowski, K.: MUBs and Hadamards of Order Six. arXiv:quant-ph/0610161 v1 (2006)

[13] Bennett, C.H., Brassard, G.: Quantum Cryptography : Public Key Distribution and Coin Tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, New York, 175–179 (1984)

[14] Berndt, R., Schmidt, R.: Elements of the Representation Theory of the Jacobi Group. Progress in mathematics 163, Birkhäuser, Basel (1998)

[15] Blokhuis, A., Jungnickel, D., Schmidt, B.: Proof of the Prime Power Conjecture for Projective Planes of Order n with Abelian Collineation Groups of Order n^2. Proceedings of AMS 130(5), 1473–1476 (2001)

[16] Bourbaki, N.: Éléments de mathématique VI, Intégration. Hermann, Paris (1956)

[17] Boykin, P.O.,Roychowdhury, V.: Optimal encryption of quantum bits. Physical Review A 67, 042317, arXiv:quant-ph/0003059 (2000)

[18] Carlet C., Ding C.: Highly nonlinear mappings. Journal of Complexity 20, 205–244 (2004)

[19] Caves, C.M., Fuchs, C.A., Schack R.: Unknown Quantum States: The Quantum de Finetti Representation. Journal of Mathematical Physics 43, 4537–4559, arXiv:quant-ph/0104088v1 (2002)

[20] Coulter, R.S., Matthews, R.W.: Planar functions and planes of Lenz-Barlotti class II. Designs, Codes and Cryptography 10, 167–184 (1997)

[21] van Dam, W., Hallgren, S., Ip, L.: Quantum algorithms for some hidden shift problems. Proceedings of the ACM-SIAM Symposium on Discrete Algorithms, 489–498, arXiv:quant-ph/0211140 (2003)

[22] Dankert, C., Cleve, R., Emerson, J., Livine, E.: Exact and approximate unitary 2-designs: Constructions and applications. arXiv:quant-ph/0606161 (2006)

[23] Delsarte, P., Goethals, J.M., Seidel, J.J.: Spherical codes and designs. Geometriae Dedicata 6, 363 (1977)

[24] Dembowski, P., Ostrom, T.G.: Planes of order n with collineation groups of order n^2. Mathematische Zeitschrift 103, 239–258 (1968)

[25] Diestel, R.: Graph theory (Third edition). Springer-Verlag (2005)

[26] Ding, C., Yuan J.: A family of skew Hadamard difference sets. Journal of Combinatorial Theory, Series A 113 1526–1535 (2006)

[27] Elliott, J.E.H., Butson, A.T.: Relative difference sets. Illinois Journal of Mathematics 10, 517–531 (1966)

[28] Englert, B.-G.: Mutually unbiased bases. Problem page in Quantum Information at TU Braunschweig [tiešsaite], http://www.imaph.tu-bs.de/qi/problems/13.html.

[29] Flammia, S.T.: On SIC-POVMs in Prime Dimensions. Journal of Physics A: Mathematical and General 39, 13483–-13493, arXiv:quant-ph/0605050v3 (2006)

[30] Frankl, P.: Orthogonal vectors in the n-dimensional cube and codes with missing distances. Combinatorica 6(3), 279–285 (1986)

[31] Fuchs, C.A., Sasaki, M. : Squeezing Quantum Information through a Classical Channel: Measuring the 'Quantumness' of a Set of Quantum States. Quantum Information & Computation 3(5), 377-404, arXiv:quant-ph/0302092v3 (2003)

[32] Fuchs, C.A.: Quantum Mechanics as Quantum Information (and only a little more). arXiv:quant-ph/0205039 (2002)

[33] Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Transactions on Information Theory, IT-14, 154–156 (1967)

[34] Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models. European Journal of Combinatorics 30(1), 246–262, arXiv:quant-ph/0511004 v2 (2005)

[35] Grassl, M.: On SIC-POVMs and MUBs in dimension 6. arXiv:quant-ph/0406175 (2004)

[36] Grassl, M.: Tomography of Quantum States in Small Dimensions. Electronic Notes in Discrete Mathematics 20, 151–164 (2005)

[37] Grassl, M.: Seeking symmetries of SIC-POVMs. Seeking SICs: A Workshop on Quantum Frames and Designs, Perimeter Institute, pirsa.org/08100069/ (2008)

[38] Grassl, M.: Personīga komunikācija.

[39] Hall, M. Jr: The theory of groups. The Macmillan Company (1968)

[40] Helleseth, T., Kumar, V.J.: Sequences with low correlation. in Handbook of Coding Theory, V. Pless, C. Huffman Eds., Elsevier (1998)

[41] Hoggar, S.G.: 64 lines from a quaternionic polytope. Geometriae Dedicata 69(3), 287–289 (1998)

[42] Холево, А.С.: Вероятностные и статистические аспекты квантовой теории. Москва, Наука (1980) [Holevo, A.S.: Kvantu mehānikas varbūtiskie un statistiskie aspekti] (krievu val.)

[43] Horn, R.A., Johnson, C.R.: Matrix Analysis. Cambridge University Press (1985)

[44] Ito, N.: Hadamard graphs. Graphs and Combinatorics 1, 57–64 (1985)

[45] Ivanović, I.D.: Geometrical description of quantal state determination. Journal of Physics A: Mathematical and General 14, 3241–3245 (1981)

[46] Khatirinejad, M.: On Weyl-Heisenberg orbits of equiangular lines. Journal of Algebraic Combinatorics 28(3), 333–349 (2007)

[47] Klappenecker, A., Rötteler, M.: Mutually Unbiased Bases are Complex Projective 2-Designs. Proceedings of ISIT International Symposium on Information Theory 2005, 1740–1744, arXiv:quant-ph/0502031 v2 (2005)

[48] Klappenecker, A., Rötteler, M.: Constructions of Mutually Unbiased Bases. Finite Fields and Applications 2004, Lecture Notes in Computer Science 2948, 262–266, arXiv:quant-ph/0309120 (2003)

[49] Крылов В.И.: Приближенное вычисление интегралов. Издание второе. Москва, Наука, 500 стр (1967) [Krilovs, V.I.: Integrāļu tuvināta aprēķināšana] (krievu val.)

[50] Lemmens, P.W.H., Seidel J.J.: Equiangular Lines. Journal of Algebra 24, 494-512 (1973)

[51] Lidl, R., Niederreiter, H.: Finite fields. 2nd ed. Cambridge University Press (1997)

[52] Massey, J.L., Mittelholzer, T.: Welch's bound and sequence sets for code-division multiple-access systems. Sequences II: Methods in Communication, Security and Computer Sciences. Springer-Verlag, 63–78 (1993)

[53] Nielsen, M.A., Chuang I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)

[54] Neumaier, A.: Combinatorial configurations in terms of distances. Departement of Mathematics Memorandum 81-09, Eindhoven University of Technology (1981)

[55] Nyberg, K.: Differentially uniform mappings for cryptography. Advances in cryptology EUROCRYPT 93 (Lofthus), Lecture Notes in Computer Science 765, 55–64 (1994)

[56] Pott, A.: Nonlinear functions in abelian groups and relative difference sets. Discrete Applied Mathematics 138, 177–193 (2004)

[57] Prugovečki, E.: Information-theoretic aspects of quantum measurement. International Journal of Theoretical Physics 16, 321–331 (1977)

[58] Renes, J., Blume-Kohout, R., Scott, A.J., Caves, C.: Symmetric Informationally Complete Quantum Measurements. Journal of Mathematical Physics 45, 2171–2180, quant-ph/0310075v1 (2003)

[59] Renes, J., Blume-Kohout, R., Scott, A.J., Caves, C.: A list of fiducial vector up to dimension 45. Available at http://info.phys.unm.edu/papers/reports/sicpovm.html.

[60] Roy, A., Scott, A.J.: Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements. Journal of Mathematical Physics 48, 072110, quant-ph/0703025v2 (2007)

[61] Rueppel, R.: Analysis and Design of Stream Ciphers. Springer-Verlag (1986)

[62] Shannon, C.E.: Communication theory of secrecy systems. Bell System Technical Journal 28, 656–715 (1949)

[63] Schwinger, J.: Unitary operator bases. Proceedings of the National Academy of Sciences USA 46, 570–579 (1960)

[64] Scott, A.J.: Tight informationally complete quantum measurements. Journal of Physics A: Mathematical and General 39, 13507-–13530, arXiv:quant-ph/0604049v6 (2006)

[65] Scott, A.J.: Optimizing quantum process tomography with unitary 2-designs. arXiv:0711.1017v2 (2008)

[66] Scott, A.J.: SIC-POVMs [tiešsaite]. www.cit.gu.edu.au/ ascott/sicpovms/

[67] Seidel, J.J.: Designs and approximations. Contemporary Mathematics 111, 179–186 (1990)

[68] Seidel, J.J.: Definitions for spherical designs. Journal of Statistical Planning and Inference 95, 307—313 (2001)

[69] Shor, P.W: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Scientific Computing 26, 1484–1509, arXiv:quant-ph/9508027v2 (1997)

[70] Stanley, R.: Enumerative Combinatorics. Volume 1. Cambridge University Press (1997)

[71] Tadey, W., Zyczkowski, K.: A concise guide to complex Hadamard matrices. Open Systems & Information Dynamics 13(2), 133–177, arXiv:quant-ph/0512154v2 (2006)

[72] Waldron, S.: Generalized Welch Bound Equality Sequences Are Tight Frames. IEEE Transactions on Information Theory 49(9), 2307–2309 (2003)

[73] Welch, L.R.: Lower bounds on the maximum cross correlations of signals. IEEE Transactions on Information Theory 20(3), 397–399 (1974)

[74] Wootters, W.K., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Annals of Physics 191, 363 – 381 (1989)

[75] Wootters, W.K.: Picturing qubits in phase space. IBM Journal of Research and Development 48(1), 99–110 (2004)

[76] Zauner, G.: Quantendesigns Grundzüge einer nichtkommutativen Designtheorie. PhD thesis, Universität Wien (1999)

Dokumentārā lapa

Maģistra darbs "Kvantu dizaini: MUB un SIC-POVM" izstrādāts LU Datorikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Aleksandrs Belovs .....

Rekomendēju darbu aizstavēšanai

Vadītājs: as. prof., Dr.dat. Juris Smotrovs .....

Recenzents: prof., Dr.sc.comp. Andris Ambainis

Darbs iesniegts Datorikas fakultātē .....

Metodiķe: .....

Darbs aizstāvēts Datorzinātņu maģistra gala pārbaudījuma komisijas sēdē .....prot. Nr. ....., vērtējums .....(.....).

Komisijas sekretārs: ....