Rigidity and a common framework for mutually unbiased bases and k-nets

Sloan Nietert [1], Zsombor Szilágyi [2], and Mihály Weiner [3]

arXiv:1907.02469

Abstract

Many mysterious connections have been observed between collections of **mutually unbiased bases** (MUBs) and combinatorial designs called **k-nets** (particularly affine planes). We introduce the notion of a **k-net over an algebra**, providing a common framework for both objects, and derive a certain rigidity property which is new for MUBs. We specialize this result to a class of algebraically constructed MUBs and find as a corollary that certain large systems of this type cannot be completed.

What are MUBs?

Orthonormal bases $\mathcal{E}, \mathcal{F}$ of $\mathbb{C}^d$ are called ***unbiased*** if

$$|\langle \mathbf{e}, \mathbf{f} \rangle|^2 = 1/d \qquad \forall\, \mathbf{e} \in \mathcal{E}, \mathbf{f} \in \mathcal{F}.$$

A collection of r mutually unbiased bases (***MUBs***) is said to be ***complete*** if $r = d+1$ (as it is easy to prove that $r \leq d+1$).

MUBs arise naturally in several quantum information protocols and are of independent mathematical interest.

The eigenbases of the Pauli matrices $\sigma_1, \sigma_2, \sigma_3 \in \mathcal{L}(\mathbb{C}^2)$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \beta_1 := \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \beta_2 := \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \beta_3 := \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

form a complete collection of MUBs.

Conjecture: Complete sets of MUBs exist in $\mathbb{C}^d$ if and only if d is a prime power.

What are k-nets?

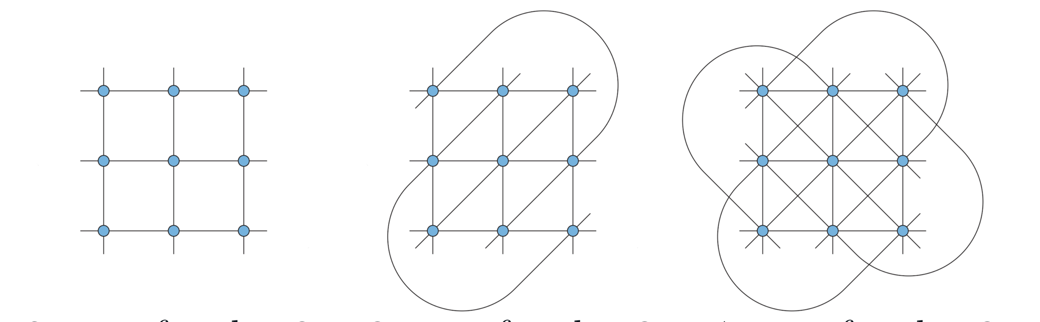
A ***k-net*** is an incidence structure consisting of a set X of *points* and a collection of subsets of X (called *lines*) such that

(i) the relation $||$ — where $\ell_1 || \ell_2$ means that $\ell_1 = \ell_2$ or $\ell_1 \cap \ell_2 = \emptyset$ — is an equivalence relation dividing the set of lines into k equivalence classes (called *parallel classes*);

(ii) any two lines are either parallel or intersect at a single point;

(iii) for any point p and line ℓ, $\exists$ a line parallel to ℓ containing p.

A *k-net of order d* consists of d^2 points and k parallel classes such that each class has exactly d lines and each line has exactly d points. A $(d+1)$-net of order d is called an *affine plane of order d*. Simple arguments show $k \leq d+1$ for all k-nets of order d, so one might say that affine planes are *complete* k-nets.



2-net of order 3   3-net of order 3   4-net of order 3 (complete 4-net) (affine plane of order 3)

Conjecture: Affine planes of order d exist if and only if d is a prime power.

C^*-algebra review

Recall that every C^*-algebra $\mathfrak{A}$ is $*$-isomorphic to the direct sum of full matrix algebras

$$\mathfrak{A} \cong \bigoplus_{j=1}^{k} M_{n_j}(\mathbb{C}),$$

for some $n_1, \ldots, n_k$ satisfying $\sum_{j=1}^k n_j^2 = \dim(\mathfrak{A})$, and all such $*$-isomorphisms are unitarily equivalent.

Generalized k-nets: a common framework

We now extend the notion of **classical k-nets** and **MUBs** to a more general setting.

Let $\mathfrak{A}$ be a finite-dimensional C^*-algebra with canonical normalized trace τ. We say that a collection of orthogonal projections $\mathcal{N} \subset \{P \in \mathfrak{A} \mid P^2 = P^* = P\}$ is a ***k-net over $\mathfrak{A}$*** if

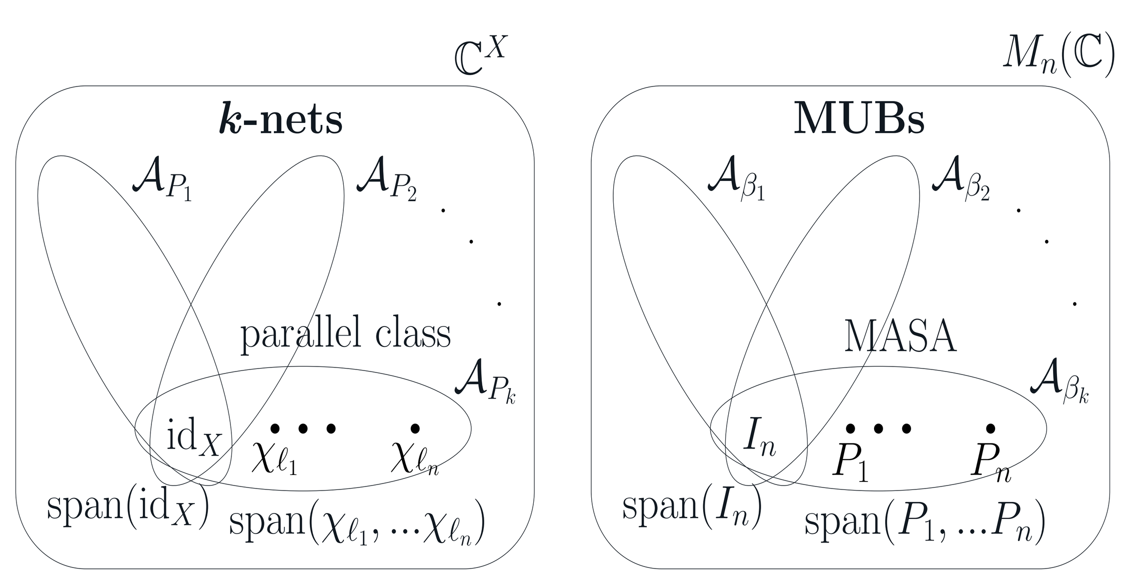
(i) the relation "$P = Q$ or $PQ = 0$" is an equivalence relation on $\mathcal{N}$ dividing $\mathcal{N}$ into k equivalence classes;

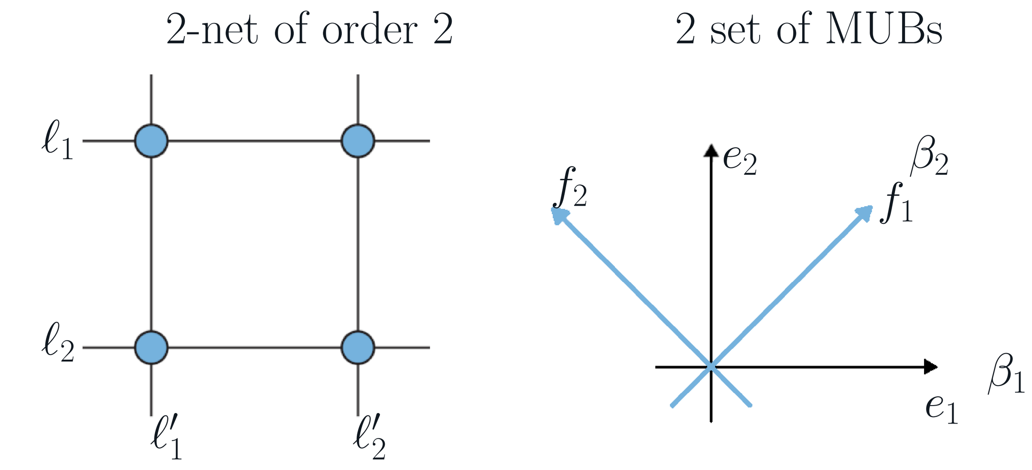
(ii) if $P, Q \in \mathcal{N}$ are not equivalent, then $\tau(PQ) = 1/\dim(\mathfrak{A})$;

(iii) the elements in each class sum to the identity I.

We refer to elements of $\mathcal{N}$ as ***lines*** and to the introduced equivalence classes as ***parallel classes***.

We can easily show (for $k \geq 3$) that each parallel class must have the same number d of lines (and $\tau(P) = 1/d$), so we say that $\mathcal{N}$ is a *k-net of order d*. This definition of k-nets over finite dimensional C^*-algebras generalizes the notions of both classical k-nets (case $\mathfrak{A} = \mathbb{C}^X$) and MUBs (case $\mathfrak{A} = M_d(\mathbb{C})$).





$\mathfrak{A} = \mathbb{C}^4$

$$\left.\begin{aligned} \chi_{\ell_1} &= (1,1,0,0) \\ \chi_{\ell_2} &= (0,0,1,1) \end{aligned}\right\} \mathcal{A}_{P_1} \qquad \left.\begin{aligned} \chi_{\ell'_1} &= (1,0,1,0) \\ \chi_{\ell'_2} &= (0,1,0,1) \end{aligned}\right\} \mathcal{A}_{P_2}$$

$\mathfrak{A} = M_2(\mathbb{C})$

$$\left.\begin{aligned} P_1 &= |e_1\rangle\langle e_1| \\ P_2 &= |e_2\rangle\langle e_2| \end{aligned}\right\} \mathcal{A}_{\beta_1} \qquad \left.\begin{aligned} Q_1 &= |f_1\rangle\langle f_1| \\ Q_2 &= |f_2\rangle\langle f_2| \end{aligned}\right\} \mathcal{A}_{\beta_2}$$

Rigidity Theorem

Our main result implies that generalized k-nets have a certain rigidity; they are determined by a proper subset of their parallel classes and cannot be "slightly modified" while retaining their defining properties.

Theorem 1. Let $\mathcal{N}$ be a k-net of order d over $\mathfrak{A}$, and suppose that $k \leq \sqrt{d}$. If $P = P^2 = P^* \in \mathrm{Span}(\mathcal{N})$ with $\tau(P) = \frac{1}{d}$, then $P \in \mathcal{N}$.

Corollary 1. Concretely, this means that sufficiently large combinatorial k-nets and sets of MUBs (of size $\geq d - \sqrt{d} + 1$) can be completed in at most one way.

References

[1] R. H. Bruck. "Finite nets II: uniqueness and imbedding". In: *Canad. J. Math.* **13**.2 (1963), pp. 421–457.

[2] Andreas Klappenecker and Martin Rötteler. "On the monomiality of nice error bases". In: *IEEE T. Inform. Theory* **51**.3 (2005), pp. 1084–1089.

[3] Prabha Mandayam et al. "Unextendible Mutually Unbiased Bases from Pauli Classes". In: *Quantum Inf. Comput.* 14.9&10 (2014), pp. 823–844. ISSN: 1533-7146.

[4] Koen Thas. "Unextendible mutually unbiased bases (after Mandayam, Bandyopadhyay, Grassl and Wootters)". In: *Entropy* **18**.11 (2016), p. 395.

Nice MUBs

In quantum information theory, orthonormal bases of unitary matrices are fundamental to error correction and super-dense coding and are often constructed algebraically [2]:

Let G a group of order d^2 with identity e. A ***nice error basis*** with index group G is a set $\mathcal{E} = \{U(g) \mid g \in G\}$ of unitary operators in $M_d(\mathbb{C})$ such that

(i) $U(e) = I$,

(ii) $\mathrm{Tr}(U(g)) = 0$ for $e \neq g \in G$,

(iii) $U(g)U(h) = \lambda(g,h)U(gh)$ for all $g, h \in G$,

where $\lambda(g,h)$ is a complex phase factor.

Fix $d \geq 2$, and let $\omega = e^{2\pi i/d}$. We define X_d to be the cyclic shift matrix $X_d \mathbf{e}_j = \mathbf{e}_{j+1} \pmod d$ and Z_d to be the diagonal matrix $Z_d \mathbf{e}_j = \omega^{j-1}\mathbf{e}_j$, where $\{\mathbf{e}_j\}_j$ is the standard basis. Then, the *discrete Weyl operators* $\{X_d^j Z_d^\ell \mid (j,\ell) \in \mathbb{Z}_d^2\}$ form a nice error basis with index group $\mathbb{Z}_d^2$.

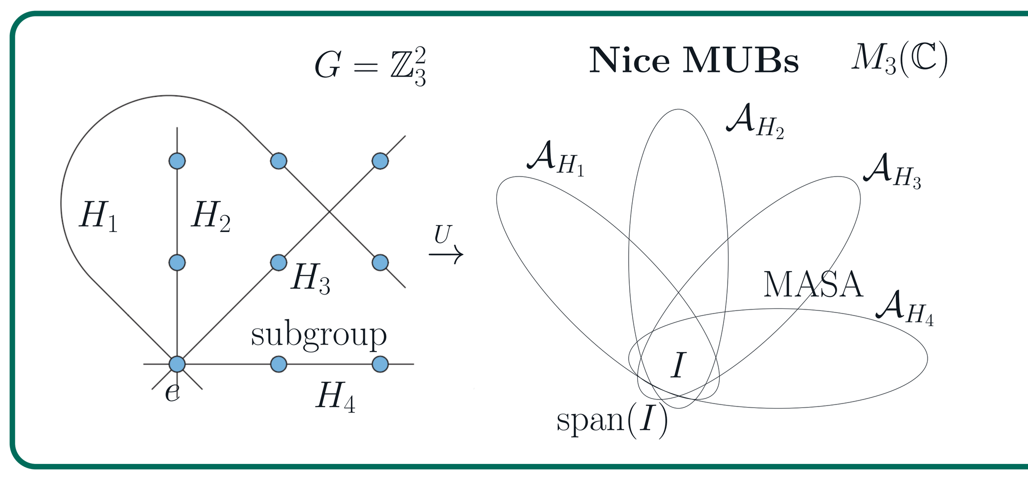
For each subgroup H of the index group G, define

$$\mathcal{A}_H := \mathrm{Span}\{U(h) \mid h \in H\}$$

to be the subspace of $M_d(\mathbb{C})$ spanned by the unitaries corresponding to H.

Proposition. Let $\mathcal{E}$ be a nice error basis for $M_d(\mathbb{C})$ with index group G, and take $H_1, \ldots, H_m$ to be subgroups of G of order d with pairwise trivial intersections. If, for each H_j, the associated unitaries of $\mathcal{E}$ are pairwise commuting, then $\mathcal{A}_{H_1}, \ldots, \mathcal{A}_{H_m}$ are quasi-orthogonal MASAs of $M_d(\mathbb{C})$, corresponding to a set of MUBs.

We call bases constructed from a nice error basis $\mathcal{E}$ in this way ***$\mathcal{E}$-nice mutually unbiased bases***, and can adapt Theorem 1 to this setting.



Theorem 2. Let $\mathcal{E}$ be a nice error basis for $M_d(\mathbb{C})$ with abelian index group. If an $\mathcal{E}$-nice set of at least $d+1-\sqrt{d}$ MUBs can be completed to a full set of $d+1$ MUBs, then this completion is unique and $\mathcal{E}$-nice.

Finally, we can use these rigidity results to prove that certain sets of MUBs cannot be completed.

Let $\mathcal{E}$ be a nice error basis for $M_d(\mathbb{C})$. A set of $\mathcal{E}$-nice MUBs in $\mathbb{C}^d$ is called ***weakly unextendible*** if there does not exist another mutually unbiased $\mathcal{E}$-nice basis.

Several examples of weakly unextendible MUBs are examined in [4, 3].

Corollary 2. A weakly unextendible set of at least $d+1-\sqrt{d}$ nice MUBs in $\mathbb{C}^d$ cannot be completed.

Concluding remarks

In [1], Bruck proved a uniqueness result which implies our rigidity theorem for classical k-nets. Moreover, he also proved an *existence result* stating that even larger k-nets automatically have a completion. Having examined uniqueness, we wonder whether one could derive such an existence result for MUBs using our framework.

Acknowledgements

The authors are grateful for the environment provided by Budapest Semesters in Mathematics and for fruitful discussions on finite geometry with Zsuzsa Weiner.

[1] Dept. of Computer Science, Cornell University
[2,3] MTA-BME Lendület Quantum Information Theory Research Group
[2] Dept. of Theoretical Physics, Budapest University of Technology & Economics (BME)
[3] Dept. of Analysis, Budapest University of Technology & Economics (BME)