Lie Algebras, Quantum Metrics, and Error Detecting Codes

UC Davis Math REU 2022

Ian Shors
under the direction of
Professor Greg Kuperberg

August 11, 2022

Table of Contents

Matrix Lie Algebras

In general an *algebra* is a set endowed with two operations thought of as addition and multiplication.

Definition

Let X and Y be two $n \times n$ matrices. The *Lie bracket* is given by

$$[X, Y] = XY - YX.$$

Matrix Lie Algebras

In general an *algebra* is a set endowed with two operations thought of as addition and multiplication.

Definition

Let X and Y be two $n \times n$ matrices. The *Lie bracket* is given by

$$[X, Y] = XY - YX.$$

Definition

Suppose $\mathfrak{g}$ is a vector subspace of $M_n(\mathbb{R})$ or $M_n(\mathbb{C})$ that is closed under the Lie bracket. The set $\mathfrak{g}$, endowed with the operations of $+$ and $[\cdot, \cdot]$, is said to be a *matrix Lie algebra*.

Note: There exists an abstract definition of a Lie algebra, but every (finite-dimensional) abstract Lie algebra is isomorphic to a matrix Lie algebra.

Matrix Lie Algebra Examples

- $\mathfrak{gl}(n, \mathbb{C}) = \{\text{all } n \times n \text{ complex matrices}\}$
- $\mathfrak{sl}(n, \mathbb{C}) = \{X \in \mathfrak{gl}(n, \mathbb{C}) \mid \mathrm{tr}(X) = 0\}$
- $\mathfrak{su}(n) = \{X \in \mathfrak{gl}(n, \mathbb{C}) \mid \mathrm{tr}(X) = 0 \text{ and } X^* = -X\}$

We are most interested in $\mathfrak{sl}(n, \mathbb{C})$ and $\mathfrak{su}(n)$ for small values of n.

Irreducible Representations

A *representation* of a Lie algebra $\mathfrak{g}$ is a vector space V together with a linear map $\rho : \mathfrak{g} \to \mathcal{L}(V)$. We can think of each $X \in \mathfrak{g}$ as being a linear operator on V, so we say $\mathfrak{g}$ *acts on* V.

This map must preserve the Lie algebra structure of $\mathfrak{g}$, so we require

$$\rho([X, Y]) = \rho(X)\rho(Y) - \rho(Y)\rho(X)$$

Irreducible Representations

A *representation* of a Lie algebra $\mathfrak{g}$ is a vector space V together with a linear map $\rho : \mathfrak{g} \to \mathcal{L}(V)$. We can think of each $X \in \mathfrak{g}$ as being a linear operator on V, so we say $\mathfrak{g}$ *acts on* V.

This map must preserve the Lie algebra structure of $\mathfrak{g}$, so we require

$$\rho([X, Y]) = \rho(X)\rho(Y) - \rho(Y)\rho(X)$$

Example

For a matrix Lie algebra $\mathfrak{g} \subseteq M_n(\mathbb{C})$, we can let $V = \mathbb{C}^n$ and $\rho(X) = X$. This is called the *defining representation* of $\mathfrak{g}$.

A representation is said to be *irreducible* if it has no non-trivial suprepresentations – i.e. subspaces W of V such that ρ restricted to W is a representation.

Some irreducible representations of $\mathfrak{sl}(d, \mathbb{C})$

Let $\mathcal{H}_k = \mathbb{C}[x_1, \ldots, x_d]_k$, the vector space of homogeneous polynomials in $x_1, \ldots, x_d$ of degree k.

Example

Taking $\mathfrak{sl}(3, \mathbb{C})$, we have

$$\mathcal{H}_1 = \operatorname{span}_{\mathbb{C}}\{x, y, z\}$$
$$\mathcal{H}_2 = \operatorname{span}_{\mathbb{C}}\{x^2, y^2, z^2, xy, xz, yz\}$$
$$\mathcal{H}_3 = \operatorname{span}_{\mathbb{C}}\{x^3, y^3, z^3, x^2y, xy^2, x^2z, xz^2, y^2z, yz^2, xyz\}$$

Some irreducible representations of $\mathfrak{sl}(d, \mathbb{C})$

Let $\mathcal{H}_k = \mathbb{C}[x_1, \ldots, x_d]_k$, the vector space of homogeneous polynomials in $x_1, \ldots, x_d$ of degree k.

Example

Taking $\mathfrak{sl}(3, \mathbb{C})$, we have

$$\begin{aligned} \mathcal{H}_1 &= \mathrm{span}_{\mathbb{C}}\{x, y, z\} \\ \mathcal{H}_2 &= \mathrm{span}_{\mathbb{C}}\{x^2, y^2, z^2, xy, xz, yz\} \\ \mathcal{H}_3 &= \mathrm{span}_{\mathbb{C}}\{x^3, y^3, z^3, x^2y, xy^2, x^2z, xz^2, y^2z, yz^2, xyz\} \end{aligned}$$

$\mathcal{H}_k$ can be made into an irreducible representation of $\mathfrak{sl}(d, \mathbb{C})$ under the identification

$$\rho(E_{ij}) = x_j \frac{\partial}{\partial x_i}$$

This representation is isomorphic to the k^{th} symmetric power of the defining representation.

Example: $\mathcal{H}_3$ for $\mathfrak{sl}(3, \mathbb{C})$

The representation $\mathcal{H}_3$ of $\mathfrak{sl}(3, \mathbb{C})$ may be summarized in the following diagram.

$$\rho(E_{11}) = x\frac{\partial}{\partial x}$$

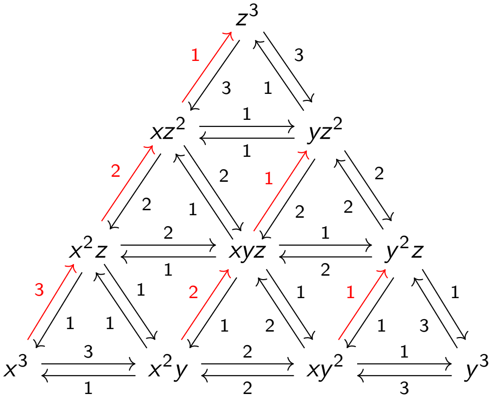
$$\rho(E_{12}) = y\frac{\partial}{\partial x}$$

$$\rho(E_{13}) = z\frac{\partial}{\partial x}$$

$$\rho(E_{21}) = x\frac{\partial}{\partial y}$$

$$\rho(E_{22}) = y\frac{\partial}{\partial y}$$

$$\vdots$$



Example: $\mathcal{H}_3$ for $\mathfrak{sl}(3, \mathbb{C})$

Rewriting $\mathcal{H}_3$ with basis vectors $|abc\rangle = \sqrt{\binom{k}{a,b,c}}\, x^a y^b z^c$, the diagram simplifies considerably.

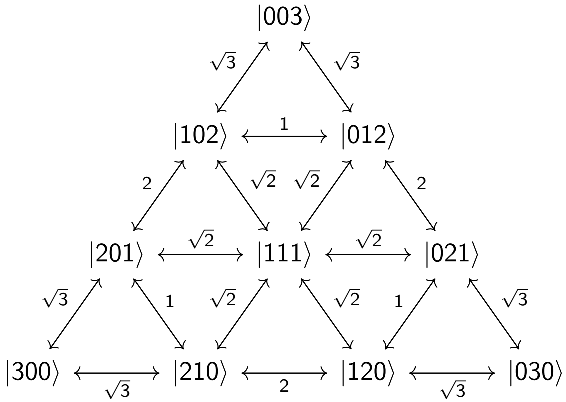


Table of Contents

Quantum Metric Spaces

Suppose $\mathcal{H} = \mathbb{C}^d$ is the state space of a quantum system. Let $\mathcal{L}(\mathcal{H}) = M_d(\mathbb{C})$ denote the set of linear operators from $\mathcal{H}$ to itself. Elements of $\mathcal{L}(\mathcal{H})$ are interpreted as errors on $\mathcal{H}$.

Quantum Metric Spaces

Suppose $\mathcal{H} = \mathbb{C}^d$ is the state space of a quantum system. Let $\mathcal{L}(\mathcal{H}) = M_d(\mathbb{C})$ denote the set of linear operators from $\mathcal{H}$ to itself. Elements of $\mathcal{L}(\mathcal{H})$ are interpreted as errors on $\mathcal{H}$.

A quantum metric assigns a real number to each error representing its severity. In particular, a quantum metric may be defined in terms of a function $D : M_d(\mathbb{C}) \to [0, \infty]$ satisfying

- $D(XY) \leq D(X) + D(Y)$
- $D(X + Y) \leq \max\{D(X), D(Y)\}$
- $D(X^*) = D(X)$
- $D(\alpha X) = D(X)$ for $\alpha \neq 0$
- $D(X) = 0$ if and only if $X = \alpha I$ for some $\alpha \in \mathbb{C}$

In error correction problems, we often assume that more severe errors are much less likely to occur.

Quantum Metric Spaces, Continued

Given such a function D, for each $t \in [0, \infty]$ we may define

$$\mathcal{V}_t = \{X \in M_d(\mathbb{C}) : D(X) \leq t\}$$

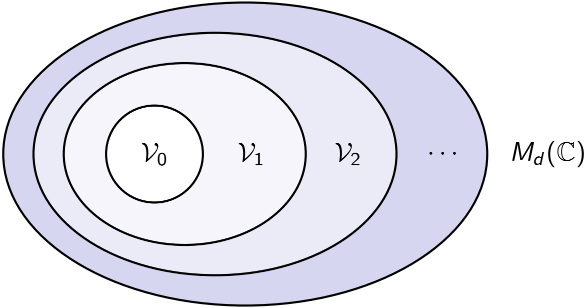
The collection $\{\mathcal{V}_t\}$ is called a $*$-algebra filtration of $M_d(\mathbb{C})$. A quantum metric may be equivalently defined in terms of this filtration.

Quantum Metric Spaces, Continued

Given such a function D, for each $t \in [0, \infty]$ we may define

$$\mathcal{V}_t = \{X \in M_d(\mathbb{C}) : D(X) \leq t\}$$

The collection $\{\mathcal{V}_t\}$ is called a $*$-algebra filtration of $M_d(\mathbb{C})$. A quantum metric may be equivalently defined in terms of this filtration.



Quantum Metric Spaces of Lie Type

Example

Let $\mathcal{E}$ be any subspace of $M_d(\mathbb{C})$ such that $I \in \mathcal{E}$ and $\mathcal{E}^* = \mathcal{E}$. We can build a quantum metric as follows:

$$\mathcal{V}_0 = \operatorname{span}_{\mathbb{C}}\{I\}, \qquad \mathcal{V}_1 = \mathcal{E}, \qquad \mathcal{V}_n = \operatorname{span}_{\mathbb{C}} \mathcal{E}^n \text{ for } n = 2, 3, 4, \ldots$$

Quantum metrics constructed in this way are called *quantum graph metrics*.

Quantum Metric Spaces of Lie Type

Example

Let $\mathcal{E}$ be any subspace of $M_d(\mathbb{C})$ such that $I \in \mathcal{E}$ and $\mathcal{E}^* = \mathcal{E}$. We can build a quantum metric as follows:

$$\mathcal{V}_0 = \operatorname{span}_{\mathbb{C}}\{I\}, \qquad \mathcal{V}_1 = \mathcal{E}, \qquad \mathcal{V}_n = \operatorname{span}_{\mathbb{C}} \mathcal{E}^n \text{ for } n = 2, 3, 4, \ldots$$

Quantum metrics constructed in this way are called *quantum graph metrics*.

Suppose $\mathcal{H} \cong \mathbb{C}^n$ is a representation of $\mathfrak{g}$ with representation map $\rho : \mathfrak{g} \to M_n(\mathbb{C})$. If we construct a quantum graph metric with $\mathcal{E} = \operatorname{span}_{\mathbb{C}}\{I\} \oplus \rho(\mathfrak{g})$, then the resulting quantum metric space has many nice properties. We say quantum metric spaces of this form are of *Lie type*.

$\mathfrak{sl}(3,\mathbb{C})$ Quantum Metric Spaces

Recall the diagram for the representation $\mathcal{H}_3$ of $\mathfrak{sl}(3,\mathbb{C})$:

In the corresponding quantum metric, distance one errors take vectors to adjacent ones in the diagram.

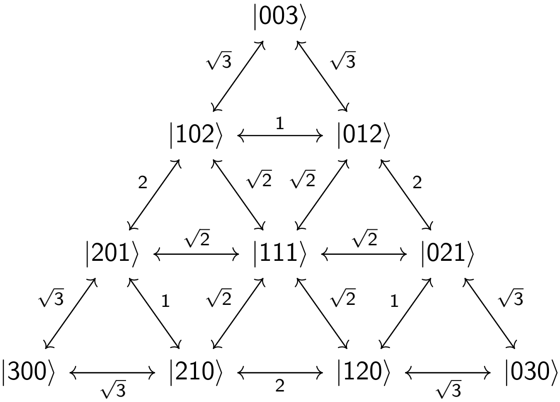


Table of Contents

Quantum Error Detecting Codes

A *quantum code* is a subspace $\mathcal{C}$ of $\mathcal{H}$.

Suppose we wish to send the message $|\psi\rangle \in \mathcal{C}$ and an error E occurs, meaning $E|\psi\rangle$ is received. This is fine if

- $E|\psi\rangle = \varepsilon|\psi\rangle$ (in which case the error E is *inconsequential*), or
- $E|\psi\rangle \perp \mathcal{C}$, (in which case the error is *detectable*).

Quantum Error Detecting Codes

A *quantum code* is a subspace $\mathcal{C}$ of $\mathcal{H}$.

Suppose we wish to send the message $|\psi\rangle \in \mathcal{C}$ and an error E occurs, meaning $E|\psi\rangle$ is received. This is fine if

- $E|\psi\rangle = \varepsilon|\psi\rangle$ (in which case the error E is *inconsequential*), or
- $E|\psi\rangle \perp \mathcal{C}$, (in which case the error is *detectable*).

An operator equation that encapsulates both of these scenarios is

$$P_{\mathcal{C}} E P_{\mathcal{C}} = \varepsilon P_{\mathcal{C}},$$

where $P_{\mathcal{C}}$ denotes the orthogonal projection onto $\mathcal{C}$. Hence, we say a code $\mathcal{C}$ can detect errors of distance t if $P_{\mathcal{C}} E P_{\mathcal{C}} = \varepsilon(E) P_{\mathcal{C}}$ for all E in $\mathcal{V}_t$. This ε is called the *slope* of the code.

KLV codes

In their 1999 paper, Knill, LaFlamme and Viola (KLV) gave a procedure for constructing quantum codes in general quantum metric spaces.

KLV codes

In their 1999 paper, Knill, LaFlamme and Viola (KLV) gave a procedure for constructing quantum codes in general quantum metric spaces.

Suppose we wish to detect errors from $\mathcal{V}_t$ for some t.

1. Find a subspace $\mathcal{B}$ of $\mathcal{H}$ such that $\mathcal{V}_t$ restricted to $\mathcal{B}$ is commutative.

KLV codes

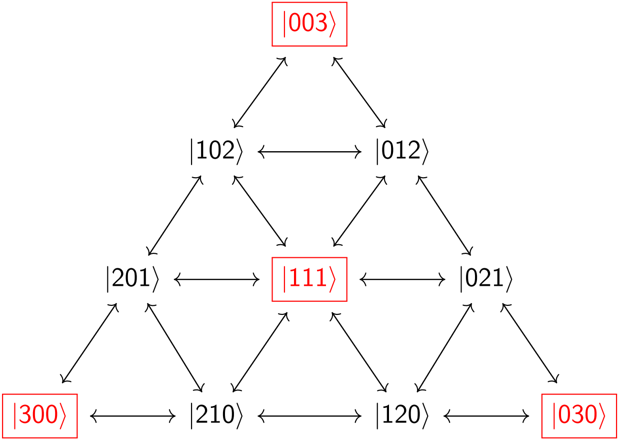
In their 1999 paper, Knill, LaFlamme and Viola (KLV) gave a procedure for constructing quantum codes in general quantum metric spaces.

Suppose we wish to detect errors from $\mathcal{V}_t$ for some t.

1. Find a subspace $\mathcal{B}$ of $\mathcal{H}$ such that $\mathcal{V}_t$ restricted to $\mathcal{B}$ is commutative.
2. Find a subspace $\mathcal{C}$ of $\mathcal{B}$ that detects those commutative errors. This reduces to a convex geometry problem.

In their original paper, KLV used a greedy algorithm for step 1, and cited Tverberg's theorem for step 2. With knowledge of the structure of the $\mathfrak{sl}(3, \mathbb{C})$ quantum metric spaces, both of these can be improved!

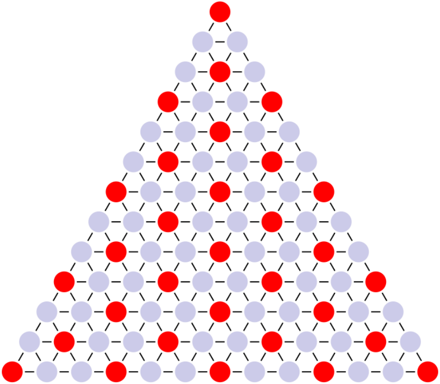
Finding a commutative subspace



If we choose a subspace spanned by vectors spaced out by distance $t+1$, then the only non-zero surviving errors of distance $\leq t$ will be diagonal.

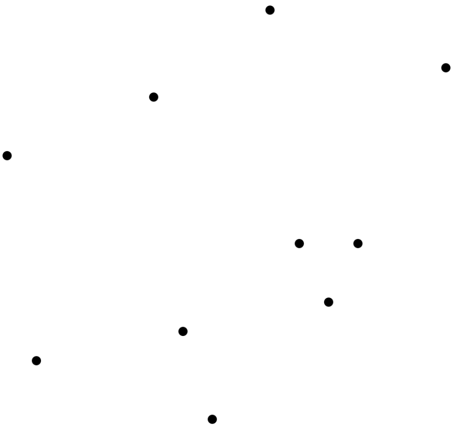
A larger example

$\mathcal{H}_{12}$ is shown below. Looking for subspaces $\mathcal{B}$ that diagonalize $\mathcal{V}_1$, we can achieve $\dim \mathcal{B} = \left\lceil \frac{\dim \mathcal{H}_k}{3} \right\rceil$. The greedy algorithm given by KLV gives $\dim \mathcal{B} \geq \left\lceil \frac{\dim \mathcal{H}_k}{8} \right\rceil$.



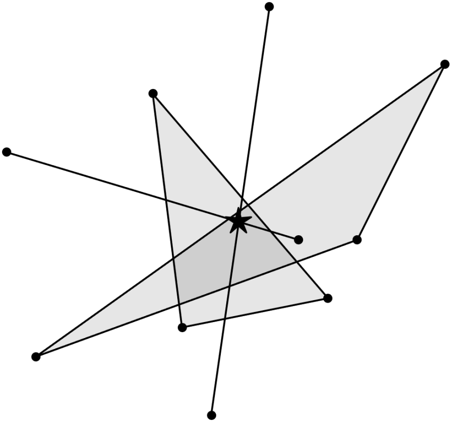
The Tverberg problem

Given n points in $\mathbb{R}^d$, we wish to partition them into subsets so that the intersection of the convex hull of each subset is nonempty.



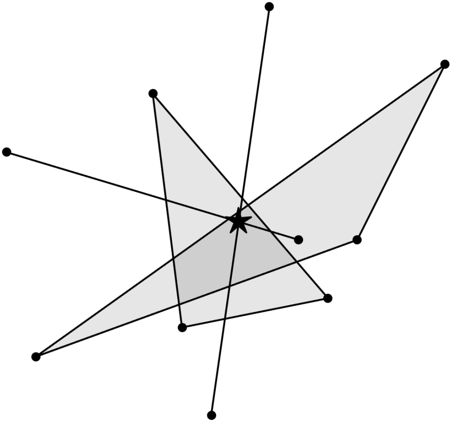
The Tverberg problem

Given n points in $\mathbb{R}^d$, we wish to partition them into subsets so that the intersection of the convex hull of each subset is nonempty.



The Tverberg problem

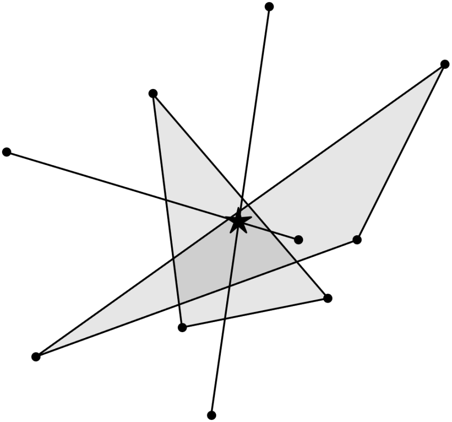
Given n points in $\mathbb{R}^d$, we wish to partition them into subsets so that the intersection of the convex hull of each subset is nonempty.



What is the maximal number of subsets we can take?

The Tverberg problem

Given n points in $\mathbb{R}^d$, we wish to partition them into subsets so that the intersection of the convex hull of each subset is nonempty.

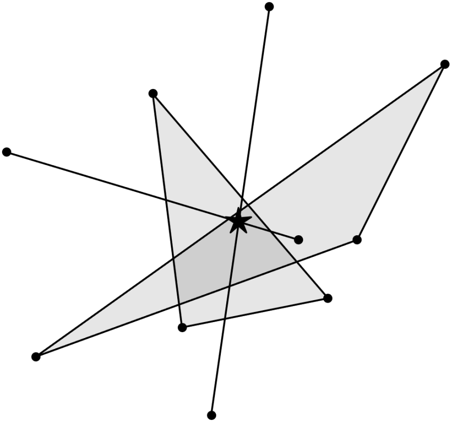


What is the maximal number of subsets we can take?

For points in general position, Tverberg's theorem says $\lceil n/(d+1) \rceil$.

The Tverberg problem

Given n points in $\mathbb{R}^d$, we wish to partition them into subsets so that the intersection of the convex hull of each subset is nonempty.



What is the maximal number of subsets we can take?

For points in general position, Tverberg's theorem says $\lceil n/(d+1) \rceil$.

However, for highly ordered sets of points, we can potentially do better!

KLV Construction, Step 2

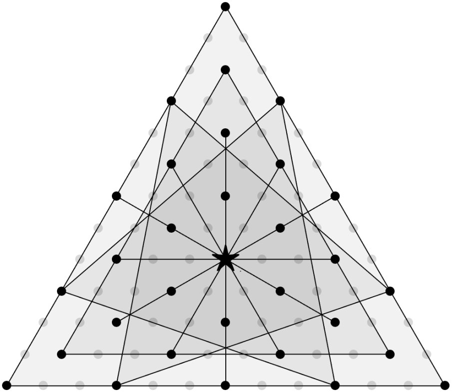
Suppose we have a set of commuting errors $\mathcal{F}$ with basis $\{F_1, \ldots, F_d\}$ on $\mathcal{B}$. Since they commute, there is a basis in which all are diagonal. To each basis vector $|m\rangle$, we can associate a vector $\vec{\lambda}_m = (\lambda_m^{(1)}, \ldots, \lambda_m^{(d)}) \in \mathbb{R}^d$, where $\lambda_m^{(j)}$ is the eigenvalue of $|m\rangle$ for the matrix F_j.

KLV Construction, Step 2

Suppose we have a set of commuting errors $\mathcal{F}$ with basis $\{F_1, \ldots, F_d\}$ on $\mathcal{B}$. Since they commute, there is a basis in which all are diagonal. To each basis vector $|m\rangle$, we can associate a vector $\vec{\lambda}_m = (\lambda_m^{(1)}, \ldots, \lambda_m^{(d)}) \in \mathbb{R}^d$, where $\lambda_m^{(j)}$ is the eigenvalue of $|m\rangle$ for the matrix F_j.

To find a code $\mathcal{C}$ inside $\mathcal{B}$, we find a Tverberg partition of the λ_i's. The Tverberg point, $\vec{\varepsilon}$ will become the slope of the code, and for each set in the partition, we can construct a corresponding vector $|\psi\rangle$ in $\mathcal{C}$ with $\langle\psi| F_j |\psi\rangle = \varepsilon_j$. Hence, the number of sets in the partition is the dimension of $\mathcal{C}$.

Super Tverberg points



For our earlier example of an subspace $\mathcal{B}$ of $\mathcal{H}_k$ for $\mathfrak{sl}(3, \mathbb{C})$, the collection of points is a triangular lattice. By pairing up points on opposite sides of the centroid, we can get approximately $4n/9$ sets. Hence,

$$\frac{\dim \mathcal{C}}{\dim \mathcal{B}} = \frac{4}{9} + O(1/k)$$

which implies

$$\frac{\dim \mathcal{C}}{\dim \mathcal{H}_k} = \frac{4}{27} + O(1/k).$$

Further questions

- The KLV construction can sometimes be modified to work with *block* diagonal error, not just diagonal error. This allows us to enlarge $\mathcal{B}$. How much advantage does this give?
- What about $\mathfrak{sl}(4)$ and beyond?

Thank you!