Maximally nonlocal subspaces

ISNFQC-2018, SNBNCBS, Kolkata
Feb 1, 2018

R. Srikanth
Poornaprajna Institute of Scientific Research
Bengaluru, India.
with: Akshata Hejamadi Shenoy

Overview

- Nonlocal subspace $\mathcal{H}_{NS}$ is a subspace within the Hilbert space $\mathcal{H}$ of a multi-particle system s/t every $\psi \in \mathcal{H}_{NS}$ violates a given Bell inequality $\mathcal{B}$.
- Subspace $\mathcal{H}_{NS}$ is maximally nonlocal if each $\psi \in \mathcal{H}_{NS}$ violates $\mathcal{B}$ to its algebraic maximum.
- We propose ways by which states with a stabilizer structure can be used to construct maximally nonlocal subspaces (MNS's), essentially as a degenerate eigenspace $\mathcal{H}_{MNS}$ of Bell operators derived from the stabilizer generators.
- Applications to two tasks in quantum cryptography are discussed: (a) quantum secret sharing; (b) certifying graph states,

Graph states

- Class of highly entangled multi-qubit states representable by a graph. Given graph $G = (V, E)$, a graph state $|G\rangle$ is defined as:

$$|G\rangle = \Pi_{(j,k)\in E}\boxed{\text{C-Phase}}^{\{j,k\}}|+\rangle^{\otimes V}, \tag{1}$$

  Vertices represent spin systems, and edges Ising interactions.

- Various graph types with $V = 4$:

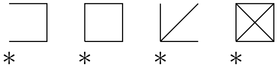

Figure : Graphs LC$_4$ (linear cluster, where underlying graph is connected subset of a d-dimensional lattice), RC$_4$ (ring cluster), ST$_4$ (star topology, rooted at vertex $*$), FC$_4$ (fully connected). Last two are related by graph theoretic operation called “local complementation” about vertex $*$.

Graph states and stabilizers

- For $1 \leq j \leq V$, define mutually commuting local observables (stabilizers):

$$g_j = X_j \bigotimes_{k \in \mathcal{N}(j)} Z_k. \tag{2}$$

  where $\mathcal{N}(j)$ denotes the vertex neighborhood of vertex j.

- $|G\rangle$ is the unique simultaneous $+1$ eigenstate of the V stabilizers g_j:

$$g_j \, |G\rangle = |G\rangle \, . \tag{3}$$

  Any graph state $\equiv$ a stabilizer state, up to local rotations (VDD 2004).

- The set of all 2^n possible products of the g_j's forms a group, called the stabilizer, denoted $\mathcal{S}$. Obviously, the graph state is stabilized by all elements $h_j \in \mathcal{S}$.

Graph basis

- A complete basis for the Hilbert space $\mathcal{H}_n$ of n qubits can be derived from $|G\rangle$ by all possible local applications of Pauli Z to the n vertices.
- Graph state basis consists of 2^n simultaneous eigenstates of stabilizer generators g_j:

$$|G_{\mathbf{x}}\rangle \equiv |G_{x_1 x_2 \cdots x_n}\rangle = \bigotimes_j (Z_j)^{x_j} |G_{000\cdots 0}\rangle, \tag{4}$$

where $|G_{000\cdots 0}\rangle \equiv |G\rangle$ and jth index $x_j \in \{0, 1\}$ of the n operators g_j, such that

$$g_j|G_{x_1 x_2 \cdots x_n}\rangle = (-1)^{x_j}|G_{x_1 x_2 \cdots x_n}\rangle. \tag{5}$$

- The *syndrome* of a graph basis state $((-1)^{x_1}, (-1)^{x_2}, \cdots, (-1)^{x_n}) \in \{\pm 1\}^{\otimes n}$ uniquely fixes the state.

Applications of graph states

- Cluster states in measurement-based quantum computing (MBQC) (RB 2001; MDF 2017). Verifiable MBQC (HM 2015; MK 2018);
- Brickwork states (underlying graph a "brickwork", requiring only X, Y-plane measurements) used in delegated quantum computation, specifically universal blind quantum computation (BFK 2008).
- Quantum secret sharing / information splitting (Markham and co-workers 2008, 2010, 2012; Sreraman, Panigrahi et al. 2008, 2009; and various others.
- Quantum error correction (SW 2001); quantum metrology (MK 2018);
- Studied extensively theoretically, and realized experimentally (Kiesen et al. 2005; Lu et al. 2007; Bell et al. 2014a,b)
- Graph states are robust against decoherence (Hein et al. 2005), which enhances their practical value.

Nonlocality of graph states

- Graph states show nonlocal correlations (SAS+ 2005, GTH+ 2005, CGR 2008) through violation of Mermin-type inequalities (Mermin 1990) based on stabilizer measurements generating perfect correlations of GHZ type (GHZ 1989).
- Alternatively, graph states show nonlocal correlations (GC 2008, TGB 2006) through violation of Bell-Ardehali inequalities (Ardehali 1992) based on non-stabilizer measurements generating probabilistic correlations (Bell 1966; CHSH 1969).
- For nonlocal tests, one may consider various questions: optimal violation of classical/local-realist bound, all Bell-type inequalities violated by a graph state, only inequality violated maximally by a given graph state, etc.
- Here, we focus on Mermin inequalities, addressing the question: what are all graph states violating a given inequality?

Mermin inequality for graph states

From stabilizer $\mathcal{S}$, we construct (potential) Bell operator:

$$\mathcal{B} \equiv \sum_{j=1}^{m} h_j, \tag{6}$$

where h_j's are products of Pauli operators. In view of Eq. (3):

$$\mathcal{B}|G\rangle = m|G\rangle. \tag{7}$$

Let q denote the largest $\#h_j$'s in Eq. (6) that can assume a positive value $(+1)$ under LR value assignment to the individual Pauli operators. If $q < m$, Bell inequality:

$$\langle\mathcal{B}\rangle \leq \mathcal{L} \equiv 2q - m, \tag{8}$$

Degree of BI violation is $\mathcal{D} = \frac{m}{2q-m}$ (figure of merit that determines resistence of violation to noise and detection loophole.)

Mermin inequalities for graph states (contd.)

- The sum of all stabilizer elements h_j is a Bell operator, though not a maximal one (GTHB 2008). In fact:

$$2^{-n}\sum_{j=1}^{2^n} h_j = |G\rangle\langle G|, \tag{9}$$

  which is easily verified.
- Any graph state violates a BI, which can be shown using an inductive argument (GTHB 2005).
- There are 2^{2^V} potential Bell operators of type (6). For $3 \leq V \leq 6$, they are fully characterized into 14 equivalent classes (up to local rotations), among them the multiqubit GHZ states (corresponding to star graph).

Example of Bell-Mermin inequality

- Linear cluster state LC$_4$:

$$|G\rangle = \frac{1}{2}\left(|{+}0{+}0\rangle + |{+}0{-}1\rangle + |{-}1{-}0\rangle + |{-}1{+}1\rangle\right), \tag{10}$$

  stabilized by generators: $g_1 \equiv X_1Z_2, g_2 \equiv Z_1X_2Z_3, g_3 \equiv Z_2X_3Z_4$ and $g_4 \equiv Z_3X_4$.

- One constructs a GHZ-like contradiction:

$$\begin{aligned} g_1g_3 &= +X \quad I \quad X \quad Z \quad \to +1, \\ g_2g_3 &= +X \quad I \quad Y \quad Y \quad \to +1, \\ g_1g_3g_4 &= +Z \quad Y \quad Y \quad Z \quad \to +1, \\ g_2g_3g_4 &= -Z \quad Y \quad X \quad Y \quad \to +1, \end{aligned} \tag{11}$$

  Each column of Pauli operators has two copies of Pauli operator $\Rightarrow$ column product $= 1$. But, product on RHS $= -1$.

- Therefore, the sum

$$\mathcal{B} = XIXZ + XIYY + ZYYZ - ZYXY. \tag{12}$$

  provides a Bell operator.

From contradiction to inequality

- By design, $\langle G|\mathcal{B}|G\rangle = 4$ for $\mathcal{B}$ in Eq. (12), the number of summands m in the Bell operator.
- OTOH, only 3 terms in Eq. (12) can be simultaneously made positive, so that $q = 3$. from Eq. (8), $\mathcal{L} = 2q - m = 2$. We thus have the Bell-type inequality

$$\langle\mathcal{B}\rangle \leq 2, \tag{13}$$

  for the Bell operator in (12).
- For a large graph state, q can be derived by computer search. Some useful tips here: (a) LHV may assume $Z = +1$ (GTHB 2005). (b) Value of q invariant under local complementation. Thus, $\mathcal{B}(\mathrm{ST}_n)$ $= \mathcal{B}(\mathrm{FC}_n)$ for a given $\mathcal{B}$, etc.

Bell-degeneracy: Basic idea

- When acting on graph basis states, on account of Eq. (5), the maximal violation condition with Bell operator $\mathcal{B}$ can be considered, as a set of m constraints on the graph syndrome, of the form $h_j(\hat{g}_1, \hat{g}_2, \cdots, \hat{g}_n) = 1$, where $\hat{g}_j \in \{\pm 1\}$ is the jth index of the graph syndrome.
- If these constraints don't uniquely fix the graph state, then there will be other graph basis elements $|G_j\rangle$ consistent with Eq. (7), i.e., there are multiple syndrome solutions to eq. $\mathcal{B}(\hat{g}_1, \hat{g}_2, \cdots, \hat{g}_n) = m$, and hence with maximal violation of BI (8), thereby making the Bell operator $\mathcal{B}$ degenerate.
- By linearity, any normalized state $\sum_j \alpha_j |G_j\rangle$ also violates BI by reaching its algebraic maximum.
- Thus, the span of these $|G_j\rangle$ defines a subspace associated with maximal violation. Accordingly, this degenerate $+1$-eigenspace of $\mathcal{B}$ is called a "maximally nonlocal subspace", $\mathcal{H}_{MNS}$.
- Various ways to produce Bell degeneracy are exemplified below.

MNS with LC state

- For LC$_4$, characterized by Eq. (12), solving $\hat{g}_1\hat{g}_3 = \hat{g}_2\hat{g}_3 = \hat{g}_1\hat{g}_3\hat{g}_4 = \hat{g}_2\hat{g}_3\hat{g}_4 = 1$, we find syndromes $(\hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4) \rightarrow (\pm 1, \pm 1, \pm 1, 1)$.
- The first of these syndromes correspond to graph state $|G\rangle$, while the other state to

$$\begin{aligned} |G'\rangle &\equiv Z_1 Z_2 Z_3 |G\rangle \\ &= \frac{1}{2}\left(|{-0-0}\rangle + |{-0+1}\rangle - |{+1+0}\rangle - |{+1-1}\rangle\right). \end{aligned} \tag{14}$$

MNS via Common generators

- In a Bell operator $\mathcal{B}$, suppose l (> 1) stabilizer generators $g_1, g_2, \cdots, g_l$ appear in all the summands h_j ($1 \leq j \leq m$). Then, $\dim(\mathcal{H}_{MNS}) \geq 2^{l-1}$ (# value assignments to $(\hat{g}_1, \hat{g}_2, \cdots, \hat{g}_l)$ consistent with $\hat{g}_1 \hat{g}_2 \cdots \hat{g}_l = 1$.)
- Example: LC$_6$ (CGR 2008):

$$\mathcal{B} = g_2 g_5 (I + g_1)(I + g_3)(I + g_4)(I + g_6) \leq 4, \qquad (15)$$

where $g_1 = X_1 Z_2, g_6 = Z_5 X_6$ and $g_j = Z_{j-1} X_j Z_{j+1}$ for $j = 2, 3, 4, 5$.

- Here $l = 2$ and the two graph basis states spanning $\mathcal{H}_{MNS}$ are $(\hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4, \hat{g}_5, \hat{g}_6) \rightarrow (1, \pm 1, 1, 1, \pm 1, 1)$, with

$$|G'\rangle = Z_2 Z_5 \, |\mathrm{LC}_6\rangle \, ,$$

being the second state in addition to $|G\rangle$.

MNS with QEC codes

- Quantum error correcting (QEC) codes have a natural association with MNS.
- A $[[n, k]]$ encodes k qubits in n qubits, s/t code space is stabilized by $n - k$ commuting syndrome operators g_j (G 1997).
- Any $\mathcal{B}$ formed from these $(n - k)$ generators will obviously have a 2^k-fold degeneracy, since all states in the code space will produce maximal violation, by construction.
- Example: $|G_0\rangle$ and $|G_1\rangle$ be the 5-qubit 1-bit error correcting code words introduced by Bennett et al. (1996):

$$\begin{aligned}
|G_0\rangle &= \frac{1}{4}(-|00000\rangle - |11000\rangle - |01100\rangle - |00110\rangle \\
&- |00011\rangle - |10001\rangle + |10010\rangle + |10100\rangle + |01001\rangle \\
&+ |01010\rangle + |00101\rangle + |11110\rangle + |11101\rangle + |11011\rangle \\
&+ |10111\rangle + |01111\rangle) \\
|G_1\rangle &= X_1X_2X_3X_4X_5|G_0\rangle. \qquad (16)
\end{aligned}$$

MNS with QEC codes – contd.

- The stabilizers are $g_1 = X_1 Y_2 Y_3 X_4$, $g_2 = X_2 Y_3 Y_4 X_5$, $g_3 = Z_1 Y_2 Y_4 Z_5$ and $g_4 = X_1 Y_2 Z_3 Y_4 X_5$, from which we construct Bell operator

  $$\mathcal{B} = g_1 g_4 (g_3 + 1) + g_2 (g_3 + g_1) + g_1 \leq 3. \tag{17}$$

  Our previous result entails that any encoded state in this QEC code will violate BI (17) maximally.
- In case of Eq. (17), from $\hat{g}_2 \hat{g}_3 = \hat{g}_2 \hat{g}_1 = 1$, we know that g_j ($j = 1, 2, 3$) have the same sign. Because of the first summand, $\hat{g}_3 = 1$ and thus $\hat{g}_4 = 1$. In other words, the "Bell conditions" fully fix the code space, and there is no further degeneracy. But this is not necessary, as we discuss with the Steane code.

MNS with Steane QEC code

- A BI with $m = 6$ for the 7-qubit Steane QEC code (1996):

$$\mathcal{B} = g_1 g_2(g_4 + g_4 g_5 + 1) + g_3 g_5(g_2 + g_1) + g_5 \leq 4 \tag{18}$$

  where Stabiliziers for the Steane code (Steane 1996) are $g_1 = X_4X_5X_6X_7, g_2 = X_2X_3X_6X_7, g_3 = X_1X_3X_5X_7, g_4 = Z_4Z_5Z_6Z_7, g_5 = Z_2Z_3Z_6Z_7$ and $g_6 = Z_1Z_3Z_5Z_7$.
- Generator g_6 doesn't appear in BI (18) $\Rightarrow \hat{g}_6$ is unrestricted.
- Solving the "Bell conditions" for $\hat{g}_j$ $(1 \leq j \leq 5)$ gives two solutions: $(\hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4, \hat{g}_5) \to (\pm 1, \pm 1, \pm 1, 1, 1)$.
- For BI (18), we thus find

$$\dim(\mathcal{H}_{MNS}) = 4 \times \dim(\text{code space}) = 8.$$

- Thus, not just states in QEC code space, but other states indicated by these graph syndromes would violate BI (18) maximally. Some of these may be correctible (when Hamming weight of corresponding error vector is at most 1, e.g., Z_7) or not (e.g., $Z_1Z_2Z_3$).

Applications

- MNS can be adapted to various situations where graph states are used with the key extension that not just a resource state, but a resource subspace is available: metrology, t-designs (MK 2018), quantum cryptography, measurement-based quantum computing (MBQC) (RB 2001; MDF 2017). Verifiable MBQC (HM 2015; MK 2018) and universal blind quantum computation (BFK 2008).
- Here: Applications to two tasks in quantum cryptography are discussed: (a) quantum secret sharing; (b) certifying graph states, which would be used as a resource for verifiable blind measurement-based quantum computing, etc.

QSS with Bennett et al. 5-qubit code

- Let Alice (secret dealer) have qubit 1, Bob qubits 2 and 3, Charlie qubit 4, while Rex (recoverer) have qubit 5. Secret is encoded in code space $\alpha |G\rangle + \beta |G'\rangle$.
- Step 1:

Alice's measurement	State obtained Bob, Charlie and Rex
$\|0\rangle$	$\alpha(-\|0000\rangle - \|1100\rangle - \|0110\rangle - \|0011\rangle + \|1001\rangle + \|1010\rangle + \|0101\rangle + \|1111\rangle)$ $+\beta(-\|0111\rangle - \|1110\rangle + \|1101\rangle + \|1011\rangle + \|0001\rangle + \|0010\rangle + \|0100\rangle + \|1000\rangle)$
$\|1\rangle$	$\alpha(-\|1000\rangle - \|0001\rangle + \|0010\rangle + \|0100\rangle + \|1110\rangle + \|1101\rangle + \|1011\rangle + \|0111\rangle)$ $+\beta(\|0110\rangle - \|1111\rangle - \|0011\rangle - \|1001\rangle - \|1100\rangle + \|0101\rangle + \|1010\rangle + \|0000\rangle)$

- Step 2:

Bob's measurement	State obtained by Charlie and Rex
$\|00\rangle$	$\alpha(-\|00\rangle - \|11\rangle) + \beta(\|01\rangle + \|10\rangle)$
$\|11\rangle$	$\alpha(-\|00\rangle + \|11\rangle) + \beta(\|01\rangle - \|10\rangle)$
$\|01\rangle$	$\alpha(\|01\rangle - \|10\rangle) + \beta(\|00\rangle - \|11\rangle)$
$\|10\rangle$	$\alpha(\|01\rangle + \|10\rangle) + \beta(\|00\rangle + \|11\rangle)$

- Charlie measures his qubit in the computational basis $\{|0\rangle, |1\rangle\}$. Rex recovers secret based on classical communication from Alice, Bob, Charlie.

Security of 5-qubit-QECC-based QSS

- Suppose Eve, as part of eavesdropping, attacks 4th qubit of an encoded state of above 5-qubit QECC via interaction:

$$U(\theta) = \frac{1+Z}{2} \otimes \mathbb{I} + \frac{1-Z}{2} \otimes \left(\begin{array}{cc} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{array} \right), \qquad (19)$$

  where $\theta \in [0, \pi/2]$.

- One finds

$$\langle h_m \rangle = \left\{ \begin{array}{cc} 1 & (m = 2,3,4) \\ \cos(\theta) & (m = 1,5), \end{array} \right. \qquad (20)$$

  so that for BI (17)

$$\langle \mathcal{B} \rangle = 3 + 2\cos(\theta). \qquad (21)$$

- Basic idea is that any intervention by Eve diminishes violation from maximality by virtue of monogamy of entanglement.

Certification of graph states

- Given unknown system and uncharacterized measurement device, some features (say, system dimension or entanglement of state) may be inferrable from observed measurement statistics: self-testing. Makes no assumptions about preparations, channels and measurements.
- Tomographic methods (DPS 2003) or entanglement witnesses (JMG 2011) test states, assuming trusted preparation & measurement procedures.
- Certifying states requires an intermediate trust level, where measurements are trusted, but sources and channels aren't.
- Because graph basis states form a complete basis, stabilizer tests which admit a trivial MNS (i.e., $\dim(\mathcal{H}_{\rm MNS}) = 1$) can be used to certify the unique (graph) state that maximally violates $\mathcal{B}$.

Certification of graph states–contd.

- Two security criteria here (MK 2018): (Completeness) test accepts ideal preparation; (Soundness) acceptance indicates closeness to ideal preparation.
- Suppose $|G\rangle$ uniquely violates BI B maximally, but no other graph basis state does. Stabilizers g_j associated with B obviously accept $|G\rangle$– completeness. Because of uniqueness, any deviation from $|G\rangle$ will increase chances of rejection– soundness.
- In the context of verifiable MBQC, this idea can be extended to fault tolerance by having client (Alice) ask server (Bob) for resource graph state to be used;

Certification of graph states–contd.

- CGR (2008) list BI's for graph states of various families. Three 4-qubit inequalities listed for $|LC_4\rangle$ are:

$$\begin{aligned} \mathcal{B}_1 &= (I+g_1)g_2(I+g_3) \leq 2 \\ \mathcal{B}_2 &= (I+g_1)g_2(I+g_3g_4) \leq 2 \\ \mathcal{B}_3 &= (I+g_1)g_2(g_3+g_4) \leq 2 \end{aligned} \tag{22}$$

  with the quantum limit being 4 in each case. Here Here $g_1 = X_1Z_2, g_4 = Z_3X_4$ and $g_j = Z_{j-1}X_jZ_{j+1}$ $(j = 2, 3)$.

- By quick inspection, $\dim(\mathcal{H}^1_{MNS}) = \dim(\mathcal{H}^2_{MNS}) = 2$, since $(\hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4)^1 \rightarrow (1, 1, 1, \pm 1)$ and $(\hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4)^2 \rightarrow (1, 1, \pm 1, \pm 1)$ violate BI maximally.

- But linear cluster state $|LC_4\rangle$ is the unique solution to $(1+\hat{g}_1)\hat{g}_2(\hat{g}_3+\hat{g}_4) = 4 \Rightarrow$ trivial MNS and hence basis for self-testing (cf. MK 2018).

Conclusions and discussions

- The concept of a nonlocal subspace $\mathcal{N}$, as one where all states violate a given Bell inequality **B**, was introduced.
- We studied a particular type of nonlocal subspace $\mathcal{N}$, namely the maximal variety (MNS), where the violation is maximal.
- We proposed various ways by which graph states (characterized by stabilizer structure) can be used to construct MNS's, essentially as the degenerate eigenspaces of Bell operators derived from the stabilizer generators.
- Applications to quantum cryptography are discussed: in specific, DQIS and certification of resource graph states.
- A future direction would be: creating nonlocal subspaces for Bell-Ardehali-type inequalities (i.e., not based on stabilizer measurements) which may lead to stronger violations of BI (A 1992).
- Another direction would be: derive Svetlichny-type inequalities for graph states leading to *absolutely nonlocal subspaces.*
- Further: design secure protocols for certification for graph states, and extend this to self-testing.

Thank you!