

# QI + miscellaneous physics diary

Ethan Lake

## *Preface:*

This is a diary containing worked-out physics problems, mostly within the purview of QI theory, but also including some QM and CS stuff, as well as some more CMT-flavored things that ended up here since the CMT diary was getting too large.

## *Notation:*

- Usual QI notation for Paulis and common quantum gates holds
- $\zeta_d = d$ th root of unity
- In e.g. spectral representations of operators, states that look like  $|\psi_i\rangle$  will always denote norm-1 vectors which are not generically linearly independent, while states that look like  $|i\rangle$  will always denote orthonormal bases
- normalization factors for wavefunctions / density operators which look like  $1/\sqrt{N}$  will often be neglected

## QI

---

Two-site Hubbard models at half-filling and their entanglement entropies	5
Entanglement, modular flow, and algebraic entropies in mega-simple qubit systems	10
Simple heuristics for classical vs quantum probabilities	22
Algebraic entanglement entropy reminder	24
Entanglement for a harmonic oscillator	28
Intro to thermofield dynamics	30
Exercises on the Shannon entropy	36
Discrete Fourier transforms and generalized Pauli operators, with applications to scrambling and teleportation	39

---

Unitary equivalence of Kraus operators	45
Random quantum expanders	49
Minimal uncertainty states	68
Bounds on Pauli errors	78
Graphical CHSH proof	94
Page's theorem	103
Local complements in graph states	105
Bit commitment	107
Distinguishing states with measurements and some facts about dual norms	110
Channel fidelities	113
More on quantum compression	116
Data hiding with Werner states	118
Entanglement distillation with CSS codes	122
Quantum Pinsker	126
Dual unitary 2-qubit gates	132
The toric code as a homological product	133
Nice CSS codes	138
Absolutely stable ergodicity breaking cannot be achieved with unital dynamics	142
Global constraints on subsystem entanglement	146
Separable states have classical correlations (P10.5)	58
Reduced density matrices in typical states are maximally mixed	60
Quantum channels are invertible iff they describe closed-system time evolution	63
Minimal uncertainty states	68
Useful relations for Fock space bilinears	69

---

How Bogoliubov transformations act on states and normal ordering of squeeze operators	71
4th order perturbation theory	75
Bounds on Pauli errors	78
Codes for qudits	79
Local correlations define the state (P2.4)	82
Parameter counting and Schmidt decompositions (P2.9)	83
Non-contextuality of QM (P2.8)	85
Collision problem and Simon's algorithm	86
coNP trivialities	88
Understanding Grover's search adiabatically	89
One-way functions and P vs NP	92
Exact encryption requires big keys	93
Graphical CHSH proof	94
Random code ensemble basics	96
TDVP benchmarking with quantum quenches	100
Page's theorem	103
Local complements in graph states	105
Bit commitment	107
Distinguishing states with measurements and some facts about dual norms	110
Channel fidelities	113
More on quantum compression	116
Data hiding with Werner states	118
Entanglement distillation with CSS codes	122
Quantum Pinsker	126

---

One-axis twisting	128
Dual unitary 2-qubit gates	132
The toric code as a homological product	133
Nice CSS codes	138
Absolutely stable ergodicity breaking cannot be achieved with unital dynamics	142
Global constraints on subsystem entanglement	146
 Miscellaneous	
<hr/>	
Useful relations for Fock space bilinears	69
One-axis twisting	128
coNP trivialities	88
One-way functions and P vs NP	92
Exact encryption requires big keys	93
Random code ensemble basics	96
How Bogoliubov transformations act on states and normal ordering of squeeze operators	71
4th order perturbation theory	75
TDVP benchmarking with quantum quenches	100
Absolutely stable ergodicity breaking cannot be achieved with unital dynamics	142

## Two-site Hubbard models at half-filling and their entanglement entropies

---

Today we will be solving the two-site Hubbard model at half-filling, both for spinful fermions and spinful bosons. After finding the ground states we will compute the entanglement entropy in the ground state as a function of  $U/t$ . We will use conventions where the potential term is  $H_U = U(n_1^2 + n_2^2)$ , so that the Hamiltonian is

$$H = -t \sum_{\sigma} (c_{\sigma 1}^{\dagger} c_{\sigma 2} + h.c.) + U \sum_{i\sigma} n_{i\sigma}^2. \quad (1)$$

♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣

### Fermions

There are six states in the half-filled Hilbert space  $\mathcal{H}_{1/2}$ , which we label as

$$\mathcal{H}_{1/2} = \langle e_1, \dots, e_6 \rangle, \quad e_1 = |\uparrow, \uparrow\rangle, e_2 = |\downarrow, \downarrow\rangle, e_3 = |\uparrow\downarrow, 0\rangle, e_4 = |0, \uparrow\downarrow\rangle, e_5 = |\uparrow, \downarrow\rangle, e_6 = |\downarrow, \uparrow\rangle. \quad (2)$$

Note that  $|\uparrow\downarrow, 0\rangle$  and  $|\downarrow\uparrow, 0\rangle$  are both perfectly good basis vectors; we will therefore find it helpful to fix conventions whereby at a single site, up spins always appear to the left of down spins in basis vectors. We will also fix conventions where states are created by a series of creation operators are always ordered in the left-to-right order obtained from the bra-ket notation of the states. For example,

$$|\uparrow\downarrow, 0\rangle = c_{\uparrow 1}^{\dagger} c_{\downarrow 1}^{\dagger} |0, 0\rangle, \quad |\uparrow, \downarrow\rangle = c_{\uparrow 1}^{\dagger} c_{\downarrow 2}^{\dagger} |0, 0\rangle. \quad (3)$$

This pedantry is needed just to get fermion-ordering minus signs under control.

In this basis, the Hamiltonian is  $H = H_t + H_U$ , with

$$H_t = -t (0_{2 \times 2} \oplus P), \quad H_U = 2U[\mathbf{1}_2 \oplus (2\mathbf{1}_2) \oplus \mathbf{1}_2], \quad P = \begin{pmatrix} & 1 & -1 \\ & 1 & -1 \\ 1 & & \\ -1 & -1 & \end{pmatrix}. \quad (4)$$

The minus signs on  $H_t$  are super important, and come from keeping careful track about the ordering of creation operators in the second-quantized expressions of the various basis vectors.

Since  $H$  is diagonal in spin indices, it is  $SU(2)$ -symmetric and commutes with both  $S_{tot}^2$  and  $S_{tot}^z$ . In our basis, we find

$$S_{tot}^z = 2Z \oplus 0_{4 \times 4}, \quad S_{tot}^2 = 2\mathbf{1}_2 \oplus 0_{2 \times 2} \oplus (\mathbf{1}_2 + X). \quad (5)$$

The former is easy to see, while the latter can be found by noting that, restricted to the subspace  $V = (e_1, e_5, e_6, e_1)$ ,  $S_{tot}^2$  is

$$S_{tot}^2|_V = (S^i \otimes \mathbf{1} + \mathbf{1} \otimes S^i)^2 = \frac{3}{2}\mathbf{1}_4 + \frac{1}{2}(X \otimes X + Y \otimes Y + Z \otimes Z) = 2 \oplus (\mathbf{1} + X) \oplus 2. \quad (6)$$

Using this and using  $S_{tot}^2 e_3 = S_{tot}^2 e_4 = 0$ ,<sup>1</sup> we arrive at the above expression for  $S_{tot}^2$ .

$S_{tot}^z$  is already diagonal, but we'd like to go into a basis in which  $S_{tot}^2$  is diagonal as well. This is easy: defining  $e'_5 = (e_5 + e_6)/\sqrt{2}$  and  $e'_6 = (e_5 - e_6)/\sqrt{2}$ , we get, in the new basis,

$$S_{tot}^2 = 2\mathbf{1} \oplus 0_{2 \times 2} \oplus (\mathbf{1} + Z). \quad (7)$$

Therefore take  $H \mapsto SHS^{-1}$ , where

$$S = \mathbf{1}_4 \oplus \frac{1}{\sqrt{2}}(Z + X). \quad (8)$$

Therefore

$$H_t \mapsto -t(\mathbf{1}_4 \oplus \frac{Z + X}{\sqrt{2}})(0_{2 \times 2} \oplus P)(\mathbf{1}_4 \oplus \frac{Z + X}{\sqrt{2}}) = -t(0_{2 \times 2} \oplus M), \quad (9)$$

where

$$M = \sqrt{2} \begin{pmatrix} & & 1 \\ & & 1 \\ & & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}. \quad (10)$$

$H_U$  is invariant, since the Coulomb repulsion doesn't care about spin. To make things slightly nicer, define  $e_0 = e'_5$ , and change basis so that the basis vectors are ordered in sequence—this just moves the triplet which is annihilated by  $H_t$  up to the first basis vector. Then in this basis,

$$S_{tot}^2 = 2 \cdot \mathbf{1}_3 \oplus 0_{3 \times 3}, \quad S_{tot}^z = 0_{1 \times 1} \oplus Z \oplus 0_{3 \times 3}, \quad H_t = -t(0_{3 \times 3} \oplus M'), \quad H_U = 2U(\mathbf{1}_3 \oplus 2 \cdot \mathbf{1}_2 \oplus 1), \quad (11)$$

where  $M'$  is  $M$  with the 3rd row and 3rd column removed. Letting  $t' = \sqrt{2}t$ , we have

$$H = 2U\mathbf{1}_3 \oplus \begin{pmatrix} 4U & 0 & -t' \\ 0 & 4U & -t' \\ -t' & -t' & 2U \end{pmatrix}. \quad (12)$$

Let  $\mathcal{E} \equiv \sqrt{4t'^2 + U^2}$ . Then diagonalizing  $H$  gives

$$H = \mathcal{S}H_D\mathcal{S}^{-1}, \quad H_D = 2U \cdot \mathbf{1}_3 \oplus \begin{pmatrix} 3U + \mathcal{E} & & \\ & 4U & \\ & & 3U - \mathcal{E} \end{pmatrix}, \quad (13)$$

---

<sup>1</sup>Since  $S_{tot}^2 e_3 = |\uparrow\downarrow, 0\rangle + |\downarrow\uparrow, 0\rangle = 0$ , and likewise for  $S_{tot}^2 e_4$ .

where the transformation is accomplished with the matrix

$$\mathcal{S} = \mathbf{1}_3 \oplus \begin{pmatrix} t/(U - \mathcal{E}) & -1 & t/(U + \mathcal{E}) \\ t/(U - \mathcal{E}) & 1 & t/(U + \mathcal{E}) \\ 1 & 0 & 1 \end{pmatrix}. \quad (14)$$

The state with the lowest energy is  $e'_5$ , a singlet, which has energy

$$E_G = 3U - \mathcal{E}. \quad (15)$$

This is followed by the symmetric triplet  $e_0$  and the two “jammed” triplet states  $e_1, e_2$ , the three of which are triply degenerate in energy, with energy  $2U$ . From our expression for  $S_{tot}^2$ , we verify that all three of these states are triplets. The next two states up have energy  $4U$  and  $3U + \mathcal{E}$ , and are both singlets.

The energy difference between the ground state singlet and the excited triplet is, for the limit of  $t/U \ll 1$ ,

$$\Delta E = \mathcal{E} - U \approx 2t^2/U. \quad (16)$$

From the matrix  $\mathcal{S}$ , we see that the ground state wavefunction is (after normalizing)

$$\psi = \frac{U + \mathcal{E}}{\sqrt{4t^2 + (U + \mathcal{E})^2}} \left[ \frac{\sqrt{2}t}{U + \mathcal{E}} (c_{\uparrow 1}^\dagger c_{\downarrow 1}^\dagger + c_{\uparrow 2}^\dagger c_{\downarrow 2}^\dagger) + \frac{1}{\sqrt{2}} (c_{\uparrow 1}^\dagger c_{\downarrow 2}^\dagger - c_{\downarrow 1}^\dagger c_{\uparrow 2}^\dagger) \right] |0, 0\rangle. \quad (17)$$

When  $U \rightarrow \infty$  the doubly-occupied terms vanish as expected, and the singlet superposition becomes degenerate with the triplet superposition, since as  $U \rightarrow \infty$  the AF exchange interaction that is responsible for the singlet having lower energy goes away. Note that the  $\langle S_{tot}^z \rangle \neq 0$  basis vectors do not appear in the ground state wavefunction.

Now let us compute the entanglement entropy. We first find the reduced density matrix for the first site. Since the Hilbert space we’ve been working with has a global constraint, it is not separable in the form  $\mathcal{H}_{full} = \mathcal{H}_1 \otimes \mathcal{H}_2$ . We can however easily embed it into the (16-dimensional) space  $\mathcal{H}_{full}$ , simply by giving the wavefunction zero support on all the remaining 10 basis vectors. After doing the embedding,  $\mathcal{H}_2$  can then be traced out to yield  $\rho_1$  in the usual way. In the basis

$$\mathcal{H}_1 = \text{span}\{|0\rangle, |\uparrow\rangle, |\downarrow\rangle, |\uparrow\downarrow\rangle\}, \quad (18)$$

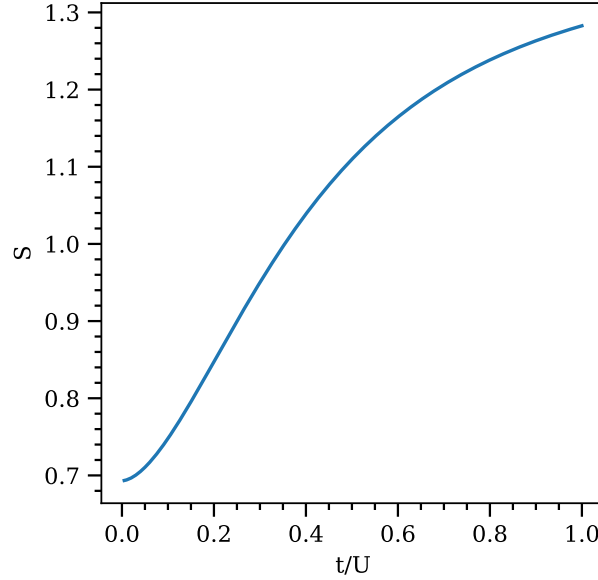
the reduced density matrix is

$$\begin{aligned} \rho_1 = \text{Tr}_{\mathcal{H}_2}[\rho] &= \begin{pmatrix} \langle 0, \uparrow\downarrow | \psi \rangle \langle \psi | 0, \uparrow\downarrow \rangle & & & \\ & \langle \uparrow, \downarrow | \psi \rangle \langle \psi | \uparrow, \downarrow \rangle & & \\ & & \langle \downarrow, \uparrow | \psi \rangle \langle \psi | \downarrow, \uparrow \rangle & \\ & & & \langle \uparrow\downarrow, 0 | \psi \rangle \langle \psi | \uparrow\downarrow, 0 \rangle \end{pmatrix} \\ &= \frac{(U + \mathcal{E})^2}{4t^2 + (U + \mathcal{E})^2} \begin{pmatrix} \frac{2t^2}{(U + \mathcal{E})^2} & & & \\ & 1/2 & & \\ & & 1/2 & \\ & & & \frac{2t^2}{(U + \mathcal{E})^2} \end{pmatrix} \end{aligned} \quad (19)$$

This is diagonal because the basis vectors appearing in the ground state wavefunction all have zero  $S_{tot}^z$  and an even number of particles: therefore the only terms that could contribute to the off-diagonal elements of  $\rho_1$  would need to come from elements of  $\rho$  off-diagonal in the  $\mathcal{H}_2$  factor, but these elements of course do not appear in the trace over  $\mathcal{H}_2$ . The entanglement entropy is thus easy to compute:

$$S = 2 \frac{(U + \mathcal{E})^2}{4t^2 + (U + \mathcal{E})^2} \left( \frac{2t^2}{(U + \mathcal{E})^2} \ln \left[ \frac{4t^2 + (U + \mathcal{E})^2}{2t^2} \right] + \frac{1}{2} \ln \left[ \frac{8t^2 + 2(U + \mathcal{E})^2}{(U + \mathcal{E})^2} \right] \right). \quad (20)$$

Plotting this as a function of  $t/U$ , we find



This passes the sanity checks at the two extremes: when  $t \rightarrow 0$  we know that we get a singlet from the superexchange interaction, and we see that the entropy accordingly goes to  $\ln 2$  in the  $t/U \rightarrow 0$  limit (we are using the natural log). On the other hand when  $t/U \rightarrow \infty$  all four basis states above will be populated evenly, and indeed we see that  $S(t/U \rightarrow \infty)$  asymptotes to  $\ln 4$ .

### Bosons

Now we consider the case of spinful bosons. We will be more more succinct, and won't go into great detail about how the diagonalization works. There are now ten states in the two-particle Hilbert space: we order the basis vectors in a way that makes the representation of the kinetic term easy:

$$\mathcal{H}_{2\text{-particle}} = \text{span}\{|\uparrow\uparrow, 0\rangle, |\uparrow, \uparrow\rangle, |0, \uparrow\uparrow\rangle, |\uparrow, \downarrow\rangle, |\downarrow, \uparrow\rangle, |0, \uparrow\downarrow\rangle, |\uparrow\downarrow, 0\rangle, |\downarrow\downarrow, 0\rangle, |\downarrow, \downarrow\rangle, |0, \downarrow\downarrow\rangle\} \quad (21)$$

In this basis the two parts of the Hamiltonian are

$$H_t = -t \left( \begin{pmatrix} & 1 & \\ \sqrt{2} & & \\ & 1 & \sqrt{2} \end{pmatrix} \oplus \begin{pmatrix} & 1 & 1 \\ & 1 & 1 \\ 1 & 1 & \end{pmatrix} \oplus \begin{pmatrix} & 1 & \\ \sqrt{2} & & \\ & 1 & \sqrt{2} \end{pmatrix} \right) \quad (22)$$



and

$$H_U = 2U (2 \oplus 1 \oplus 2 \oplus \mathbf{1}_2 \oplus 2\mathbf{1}_2 \oplus 2 \oplus 1 \oplus 2), \quad (23)$$

which admittedly is rather hard to look at when written like this.

Given that the symmetries are the same as the fermion problem, with the only difference coming in the minus signs in the hopping and the extra four states, we expect that the spectrum and ground state will look fairly similar to the fermion case. In particular, we expect the ground state to only be built out of basis vectors with  $\langle S_{tot}^z \rangle = 0$ , which gives us just the same set of four basis vectors as in the fermion problem. Without going into details, one finds that the ground state energy and ground state wavefunction are

$$E_G = 3U - \mathcal{E}, \quad (24)$$

which is the same as in the fermionic case, and

$$\psi = \frac{\mathcal{E} - U}{\sqrt{4t^2 + (\mathcal{E} - U)^2}} \left[ \frac{1}{\sqrt{2}}(b_{\uparrow 1}^\dagger b_{\downarrow 1}^\dagger + b_{\uparrow 2}^\dagger b_{\downarrow 2}^\dagger) + \frac{\sqrt{2}t}{\mathcal{E} - U}(b_{\uparrow 1}^\dagger b_{\downarrow 2}^\dagger + b_{\downarrow 1}^\dagger b_{\uparrow 2}^\dagger) \right] |0, 0\rangle, \quad (25)$$

which is the ground state wavefunction in the fermionic case, except that we have replaced  $\mathcal{E} \mapsto -\mathcal{E}$ , the second term has been properly symmetrized, and the prefactors of the two groups of creation operators in parenthesis have been swapped. Let us run a quick sanity check on this wavefunction: first, in the  $t/U \rightarrow \infty$  limit, we get the uniform  $\psi = (1, 1, 1, 1)^T/4$  as expected. More interesting is the  $t/U \rightarrow 0$  limit: here we have

$$\psi \xrightarrow{t/U \ll 1} \frac{1}{\sqrt{2}}(b_{\uparrow 1}^\dagger b_{\downarrow 1}^\dagger + b_{\uparrow 2}^\dagger b_{\downarrow 2}^\dagger), \quad (26)$$

which is the symmetrized version of the fermionic wavefunction in the same limit. This is telling us that the sign of the superexchange interaction is determined by the statistics of the particles involved: antiferromagnetic if the particles are fermions (so that the ground state is the singlet), and ferromagnetic if the particles are bosons (so that the ground state is the symmetric member of the spin-1 triplet, selected out from the other two for kinetic energy reasons). That the superexchange is ferromagnetic can also be checked by doing the algebra for the usual second-order perturbation theory calculation; we won't write it out here.

The computation of the density matrix and entanglement entropy for the ground state are then done in essentially the exact same way as for the fermionic case: if we again work in the basis (18), the density matrix is

$$\rho_1 = \frac{(U - \mathcal{E})^2}{4t^2 + (U - \mathcal{E})^2} \begin{pmatrix} 1/2 & & & \\ & \frac{2t^2}{(U - \mathcal{E})^2} & & \\ & & \frac{2t^2}{(U - \mathcal{E})^2} & \\ & & & 1/2 \end{pmatrix} \quad (27)$$

while the entanglement entropy is the same formula for the fermionic case, just with  $\mathcal{E} \mapsto -\mathcal{E}$ :

$$S = 2 \frac{(U - \mathcal{E})^2}{4t^2 + (U - \mathcal{E})^2} \left( \frac{2t^2}{(U - \mathcal{E})^2} \ln \left[ \frac{4t^2 + (U - \mathcal{E})^2}{2t^2} \right] + \frac{1}{2} \ln \left[ \frac{8t^2 + 2(U - \mathcal{E})^2}{(U - \mathcal{E})^2} \right] \right). \quad (28)$$

Interestingly enough, it turns out that  $S$  is actually an *even* function of  $\mathcal{E}$ , so that the entanglement entropy in the ground state is the exact same as the fermionic case! This is not too surprising given the above: in the  $t \rightarrow \infty$  limit we know we have to get the same  $\ln 4$  answer as we got for the fermions, while in the  $t \rightarrow 0$  limit we know we also need to get  $\ln 2$ , since the ground state is again a single Bell pair (just with a different symmetry compared to the fermionic case).



## Entanglement, modular flow, and algebraic entropies in mega-simple qubit systems

---

Today's diary entry is a rambling look at a few concepts in quantum information theory and algebraic qft applied to some very very simple examples. The impetus for this came from reading through Witten's notes on information theory and wanting to work out a few of the details myself.



We'll start by looking at the illustrative but very simple example of qubits. This begins with essentially the simplest possible example: a system of two qubits.

### Two qubits: entanglement entropy

Consider a two-site system consisting of two qubits, with the Ising Hamiltonian

$$H = -Z_L Z_R, \quad (29)$$

where  $Z_{L/R}$  are the third Pauli matrices acting on the left qubit and the right qubit, respectively. We have a global symmetry generated by  $X_L X_R$ , and so we expect that the ground state will be in the trivial representation of this  $\mathbb{Z}_2$  symmetry group.<sup>2</sup> Thus

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle). \quad (30)$$

The density matrix  $\rho$  has four non-zero entries, with a  $1/2$  in each corner. The reduced density matrices are  $\rho_L = \rho_R = \mathbf{1}/2$ , and so entanglement entropy of a single spin is easily checked to be  $S_L = S_R = \ln 2$ .

---

<sup>2</sup>For this contrived example of course all  $\alpha|00\rangle + \beta|11\rangle$  have the same energy; these states are indeed generated by states transforming in reps of  $\mathbb{Z}_2$ , viz.  $|00\rangle \pm |11\rangle$ . For a less pathological (but still symmetric) case when we have a nonzero transverse field, the trivial representation gets selected out.

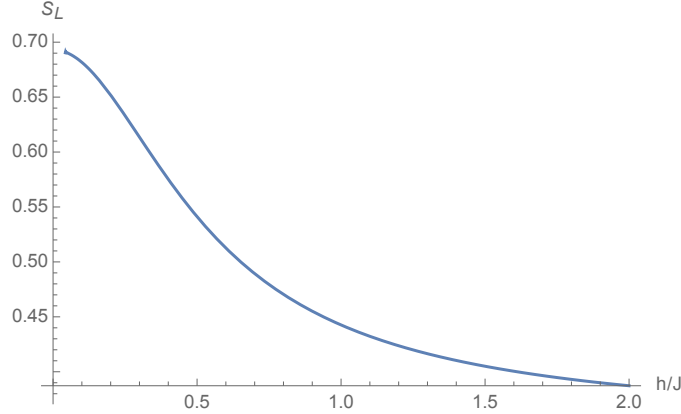


Figure 1: A hastily done plot showing the entanglement entropy  $S_L$  for the left spin as a function of the ratio of couplings  $h/J$ . As  $h \rightarrow 0$  we get the superposition  $(|00\rangle + |11\rangle)/\sqrt{2}$  which has (the maximal possible) entanglement of a Bell pair, namely  $\ln 2$ . As  $h \rightarrow \infty$  we get the product state  $|++\rangle$ , and so  $S_L \rightarrow 0$ .

This is boring, since the Hamiltonian is classical and has no dynamics. To fix this we can add a momentum term, which takes the form of a transverse field. We write

$$H = -h(X_L + X_R) - JZ_L Z_R. \quad (31)$$

Since this is such a simple system we can get the ground state wavefunction exactly, which due to the presence of the momentum term is now unique:

$$|\psi\rangle \propto (1, \gamma, \gamma, 1)^T, \quad \gamma \equiv \frac{-J + \sqrt{4h^2 + J^2}}{2J}, \quad (32)$$

where I haven't bothered to normalize it. Note that this is a linear combination of  $ZZ$  eigenstates and  $X_L, X_R$  eigenstates, and is symmetric under the global symmetry  $X_L \otimes X_R$ . As  $h \rightarrow \infty$  we get a product state  $|++\rangle$ , and so we expect  $S_L = S_R = 0$  in this limit. This is corroborated by a numerical calculation, shown in the first figure.

Now for a few more general comments that will be useful later. First, the entanglement entropy  $S_A$  for  $A \in \{L, R\}$  is invariant under unitary transformations on  $A$ . Indeed,

$$S_A = -\text{Tr}(\rho_A \ln \rho_A) \mapsto -\text{Tr}(U^\dagger \rho_A U \ln(U^\dagger \rho_A U)). \quad (33)$$

The matrix logarithm can be written as a series

$$\ln A = (A - \mathbf{1}) - \frac{1}{2}(A - \mathbf{1})^2 + \frac{1}{3}(A - \mathbf{1})^3 - \dots, \quad (34)$$

which converges provided that  $\|A - \mathbf{1}\| < 1$ . This holds for us since  $\text{Tr} \rho_a \leq 1$  and since  $\rho_A$  is positive semidefinite (the case where  $\|\rho_A - \mathbf{1}\| = 1$  happens when  $\rho_A$  is degenerate, but since  $0 \cdot \ln 0 = 0$  this case does not cause problems). From this series, we see that

$$-\text{Tr}(U^\dagger \rho_A U \ln(U^\dagger \rho_A U)) = -\text{Tr}(U^\dagger \rho_A \ln(\rho_A) U) = S_A, \quad (35)$$

and so the entanglement entropy is invariant under a unitary transformation supported on the spin  $A$ . Symmetrically, the entanglement entropy is also invariant under a transformation which has support only on the other spin  $\bar{A}$ .

However,  $S_A$  is (duh) not invariant under a general unitary transformation which has support on both  $A$  and  $B$ , since this will generically entangle  $A$  with  $B$ . Indeed, for the present two-site example, consider acting with the unitary

$$U = \mathbf{1} \oplus X. \quad (36)$$

This  $\otimes$  factorizes the wavefunction, leaving the  $L$  spin in an  $X$  eigenstate and the  $R$  spin in a  $Z$  eigenstate:

$$U|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle. \quad (37)$$

Then one can check that

$$U^\dagger \rho U = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \rho_L \otimes \rho_R. \quad (38)$$

Thus after applying the unitary,  $\rho$  becomes a product state; conjugating by  $U$  disentangles the two spins. Thus after applying  $U$ , we have  $S_L = S_R = 0$ .

To summarize, the entanglement entropy is preserved by unitaries of the form  $U = U_L \otimes U_R$ , but if  $U$  does not admit such a  $\otimes$  decomposition, the entanglement entropy is not invariant. This is intuitively quite obvious since operators of the form  $U_L \otimes U_R$  don't introduce any entanglement between  $L$  and  $R$ , while operators that cannot be factorized in this way do.

## Modular operators and algebraic properties

Now we'll look at how some algebraic QFT things are realized in this simple setting. The goal will be to see how we can use purely algebraic notions to construct a 1-parameter flow that we will identify as a sort of information-theoretic notion of time.

First, a word on notation: we'll use  $\mathcal{A}$  to refer to an algebra of operators, with a subscript specifying additional information. Thus e.g.  $\mathcal{A}_A$  will refer to the algebra of operators supported within the region  $A$ . These won't be the only algebras of interest though, e.g. one may consider the algebra  $\mathcal{A}_{Z_i, Z_j}$  of operators generated by the Pauli matrices  $Z_i, Z_j$  at two different sites  $i, j$ .

Since we are working with finite-dimensional Hilbert spaces, we can match dimensionalities of different spaces. A precondition for the state  $|\psi\rangle$  to be cyclic<sup>3</sup> for the algebra  $\mathcal{A}_A = \text{End}\mathcal{H}_A$  (here we assume that  $\mathcal{A}_A$  is a factor so that  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ , although this isn't really needed — in general,  $\mathcal{A}$  splits as a direct sum of  $\text{End}\mathcal{H}_\alpha$ 's; more on this later) is that  $\dim \mathcal{A} = \dim \mathcal{H}$ , that is we need

$$\dim(\text{End}\mathcal{H}_A) = \dim(\mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}). \quad (39)$$

But since

$$\dim(\text{End}\mathcal{H}_A) = \dim(\mathcal{H}_A \otimes \mathcal{H}_A^*) = \dim^2 \mathcal{H}_A, \quad (40)$$

---

<sup>3</sup>Recall that  $|\psi\rangle$  being cyclic for  $\mathcal{A}$  means that  $\mathcal{A}$  acting on  $|\psi\rangle$  generates the entire  $\mathcal{H}$  space.

we conclude that  $|\psi\rangle$  has a chance to be cyclic for  $\mathcal{A}_A$  only if

$$\dim \mathcal{H}_A = \dim \mathcal{H}_{\bar{A}}. \quad (41)$$

Thus in order for a state to be cyclic for a given algebra  $\mathcal{A}_A$ , we must have  $|A| = |\bar{A}|$ , i.e. the subsystem  $A$  must split the global system into two equally-sized chunks. This is not a contradiction to formal continuum QFT where we could usually choose  $A$  to be arbitrarily small, since in the continuum we have an infinite dimensional Hilbert space in any subregion. Note also that this makes the RL theorem in regular QFT seem kinda pathological, since it is as soon as you regulate the QFT with a lattice, the algebra you need to generate  $\mathcal{H}$  changes from being the operators in an arbitrarily small region to the operators in an entire half of spacetime). Also one should keep in mind that the condition on the dimension  $\dim \mathcal{H}_A = \dim \mathcal{H}_{\bar{A}}$  is just a necessary condition on the algebra, not a sufficient one:  $\mathcal{A}_A|\psi\rangle$  might fail to generate  $\mathcal{H}$  if  $|\psi\rangle$  is chosen to be some non-generic state (as a dumb example,  $|\psi\rangle$  with  $|\psi\rangle|_A = 0$  fails to be cyclic for  $\mathcal{A}_A$ ).

Assuming  $\dim \mathcal{H}_A = \dim \mathcal{H}_{\bar{A}}$  so that  $|\psi\rangle$  has a chance to be cyclic for  $\mathcal{A}_A$ , we use Schmidt decomposition to write

$$|\psi\rangle = \sum_i \lambda_i |i\rangle \otimes |i'\rangle, \quad (42)$$

where the kets on the RHS are bases for  $\mathcal{H}_A$  and  $\mathcal{H}_{\bar{A}}$  and where the  $\lambda_i$  are real and positive. Now if  $|\psi\rangle$  is cyclic for  $\mathcal{A}_A$  then it must be separating for  $\mathcal{A}_{\bar{A}}$ , and vice versa (since  $\mathcal{A}_A$  and  $\mathcal{A}_{\bar{A}}$  commute by the assumption that  $\mathcal{A}_A$  is a factor). It will fail to be separating if the Schmidt decomposition above has a nontrivial kernel, that is if the reduced density matrix

$$\rho_A = \sum_i |\lambda_i|^2 |i\rangle\langle i| \quad (43)$$

is not invertible (and likewise for  $\rho_{\bar{A}}$ ). Since  $\rho_A$  and  $\rho_{\bar{A}}$  share the same eigenvalues (since they came from a pure parent state  $\rho = |\psi\rangle\langle\psi|$ ),<sup>4</sup> if  $\rho_A$  is invertible then so is  $\rho_{\bar{A}}$ , and if  $\rho_A$  is degenerate, so is  $\rho_{\bar{A}}$ .

We have showed that if  $\rho_A$  is not invertible then  $|\psi\rangle$  is not separating for  $\mathcal{A}_{\bar{A}}$ , which means that it is not cyclic for  $\mathcal{A}_A$  (since being cyclic for  $\mathcal{A}_A$  implies being separating for  $\mathcal{A}_{\bar{A}}$ ). Thus if  $|\psi\rangle$  is cyclic for  $\mathcal{A}_A$ , then  $\det \rho_A \neq 0$ . In fact, the converse is also true. This is essentially because if  $\det \rho_A \neq 0, \det \rho_{\bar{A}} \neq 0$ , then every substate in the  $\bar{A}$  subsystem is entangled with the  $A$  subsystem, and so by acting only on the  $A$  we can still create states with arbitrary behavior in  $\bar{A}$ . More precisely, suppose we want to create the state

$$|\phi\rangle = \sum_{lm} \gamma_{lm} |l\rangle \otimes |m\rangle. \quad (44)$$

We can assume wolog that the above decomposition is taken with respect to the basis in which  $|\psi\rangle$  is Schmidt-decomposed. When we act on  $|\psi\rangle$  with some operator  $\mathcal{O} = \mathcal{O}_A \otimes \mathbf{1}_{\bar{A}}$ , we get

$$\mathcal{O}|\psi\rangle = \sum_{ab} [\mathcal{O}_A]_{ab} \lambda_b |a\rangle \otimes |b\rangle. \quad (45)$$

---

<sup>4</sup>The proof just uses the above Schmidt decomposition for  $|\psi\rangle$ : one sees from this that the eigenvalues of both reduced density matrices are  $\lambda_i^2$ , where  $\lambda_i$  are the coefficients in the Schmidt decomposition. In particular, this is how one shows  $S_A = S_{\bar{A}}$  for pure states.

Thus in order to reproduce the state  $|\phi\rangle$ , we need to choose

$$[\mathcal{O}_A]_{ab} = \gamma_{ab}/\lambda_b, \quad (46)$$

which we can do if  $\rho_A$  is invertible, since then all the  $\lambda_b$  are non-zero. Recapitulating, we have shown that  $|\psi\rangle$  is cyclic for  $\mathcal{A}_A$  iff  $\det \rho_A \neq 0$  (or equivalently, iff  $\det \rho_{\bar{A}} \neq 0$ ).

One may ask whether the ground states of the simple two-qubit Ising Hamiltonians are cyclic / separating with respect to one of the qubits. We expect “generic” states to be cyclic and separating for “generic” algebras, so we expect the answer to be yes. Since  $|\psi\rangle$  is cyclic for the qubit  $L$  if and only if  $\det \rho_L \neq 0$  (and hence  $\det \rho_R \neq 0$ ), this guess is easy to test. Putting the 2-qubit TFIM into Mathematica shows that indeed, for all finite values of  $h$ ,  $\det \rho_L \neq 0$ . When  $h \rightarrow \infty$  we get a product state, and in that case of course  $\det \rho_L = 0$ . Essentially,  $\det \rho_L$  decreases towards zero monotonically with  $h$  in same fashion that  $S_L$  does.

Now lets look at the modular operators. We will take  $|\psi\rangle$  to be cyclic for  $\mathcal{A}$ . In QFT this places comparatively few restrictions on  $\mathcal{A}$ , but as stated earlier in the present context we need  $\mathcal{A}$  to have the same (finite) dimension as  $\mathcal{H}$ . For now, we will assume that  $\mathcal{A}$  is a factor, with  $\mathcal{H} \cong \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ . Note that the cyclicity requirement on  $|\psi\rangle$  means that  $\rho \neq \rho_A \otimes \rho_{\bar{A}}$ .

We define the antilinear operator  $S_\psi$  (which we will call the “modular generator”) to be the operator which acts as  $\dagger$  for the algebra  $\mathcal{A}$ :

$$S_\psi \mathcal{O} |\psi\rangle = \mathcal{O}^\dagger |\psi\rangle, \quad (47)$$

for all  $\mathcal{O}$  which act as an element in  $\mathcal{A} = L(\mathcal{H}_A) \otimes \mathbf{1}_{\bar{A}}$ . Such an involution on  $\mathcal{A}$  exists because of the inner product on  $\mathcal{A}$  defined by using the trace and the density matrix  $\rho = |\psi\rangle\langle\psi|$ . Since  $|\psi\rangle$  is assumed to be cyclic for  $\mathcal{A}$ , specifying the action of the modular generator on elements of  $\mathcal{A}$  as above is sufficient to determine its action on all of  $\mathcal{H}$ .

To figure out what  $S_\psi$  is, we just need to know its matrix elements with respect to a basis in the matrix algebra  $\mathcal{A}$ . The canonical basis for the matrix algebra is of course  $a_{ij} = |i\rangle\langle j|$  (which is also a basis for  $\mathcal{A} \cong \mathcal{H}_A \otimes \mathcal{H}_A^*$  since  $|\psi\rangle$  is cyclic with respect to  $\mathcal{A}$ ). When acting on  $a_{ij}|\psi\rangle$ , we get

$$S_\psi a_{ij} |\psi\rangle = a_{ij}^\dagger \sum_k \lambda_k |kk\rangle = \lambda_i |ji\rangle, \quad (48)$$

where we have concised the notation by denoting  $|k\rangle_A \otimes |k\rangle_{\bar{A}} = |kk\rangle$ . But we also have

$$S_\psi a_{ij} |\psi\rangle = S_\psi \lambda_j |ij\rangle = \lambda_j^* S_\psi |ij\rangle, \quad (49)$$

and so comparing these two, the nonzero matrix elements of  $S_\psi$  are

$$\langle ji | S_\psi | ij \rangle = \frac{\lambda_i}{\lambda_j^*}. \quad (50)$$

Now for  $S_\psi^\dagger$ . Since  $S_\psi$  is anti-unitary by virtue of it implementing  $\dagger$ , we have

$$\langle \alpha | S_\psi^\dagger | \beta \rangle = \langle \beta | S_\psi | \alpha \rangle, \quad (51)$$

where  $S_\psi^\dagger$  is understood to act on the right. Note that this is different from the definition of an adjoint for a unitary operator by an application of complex conjugation, since we want

antiunitary operators to still satisfy  $U^\dagger = U^{-1}$ . So then the non-zero matrix elements of  $S_\psi^\dagger$  are

$$\langle ji|S_\psi^\dagger|ij\rangle = \frac{\lambda_j}{\lambda_i^*}. \quad (52)$$

Now define the modular operator (related to the modular Hamiltonian) as the “Laplacian”

$$\Delta_\psi = S_\psi^\dagger S_\psi. \quad (53)$$

Its matrix elements are calculated by using

$$\Delta_\psi a_{ij}|\psi\rangle = S_\psi^\dagger \lambda_i |ji\rangle = \lambda_i^* S_\psi^\dagger |ji\rangle. \quad (54)$$

But on the other hand, we also have

$$\Delta_\psi a_{ij}|\psi\rangle = \lambda_j \Delta_\psi |ij\rangle. \quad (55)$$

Then since we know the non-zero matrix elements of  $S_\psi^\dagger$ , we see that  $\Delta_\psi$  is diagonal, with matrix elements

$$\langle ij|\Delta_\psi|ij\rangle = \frac{|\lambda_i|^2}{|\lambda_j|^2}. \quad (56)$$

Or, taking advantage of the particularly simple form of  $|\psi\rangle$ ’s density matrices, we may write

$$\Delta_\psi = \rho_A \otimes \rho_{\bar{A}}^{-1}. \quad (57)$$

A picture to have in the back of one’s mind here is one where  $\Delta_\psi$  is the operator which generates “time evolution” in a way such that  $A$  flows forwards and  $\bar{A}$  flows backwards — think about Rindler coordinates and two-sided black holes and so on.

Sometimes we may want to work in a basis other than the one in which  $|\psi\rangle$  is Schmidt-decomposed. Writing  $|\psi\rangle = \sum_{kl} c_{kl} |kl\rangle$ , one checks that

$$\langle jk|\Delta_\psi|lm\rangle = \sum_{rs} [c^{-1}]_{mr} [c^{-1}]_{kr}^* c_{ls}^* c_{js}, \quad (58)$$

which also reads  $\Delta_\psi = \rho_A \otimes \rho_{\bar{A}}^{-1}$ . So, the form (57) is valid in any basis.

Modular flow is defined by evolving with the modular operator, and can be thought of a time evolution according to an emergent parameter  $t$  that comes out of the algebraic structure. For an operator  $\mathcal{O}$ , we write

$$\mathcal{O}_z = \Delta^{iz} \mathcal{O} \Delta^{-iz}. \quad (59)$$

Modular flow preserves expectation values of operators in  $\mathcal{A}$  and  $\mathcal{A}'$ : if  $\mathcal{O} = \mathcal{O}_A \otimes \mathbf{1}_{\bar{A}}$ , then

$$\langle \mathcal{O}_z \rangle = \text{Tr}(\rho(\rho_A^{iz} \mathcal{O}_A \rho_A^{-iz} \otimes \mathbf{1}_{\bar{A}})) = \text{Tr}_A(\rho_A^{iz+1} \mathcal{O}_A \rho_A^{-iz}) = \langle \mathcal{O}_0 \rangle, \quad (60)$$

and likewise for  $\mathcal{O} \in \mathcal{A}'$ . From the expression (57), we see that

$$\Delta^{iz} \mathcal{A} \Delta^{-iz} = \mathcal{A}, \quad \Delta^{iz} \mathcal{A}' \Delta^{-iz} = \mathcal{A}', \quad (61)$$

where as before  $\mathcal{A} = L(\mathcal{H}_A) \otimes \mathbf{1}_{\bar{A}}$ . For any two operators  $\mathcal{O}, \mathcal{O}'$ , an interesting function we will look at is a modular-flowed two-point function

$$f_{\mathcal{O}\mathcal{O}'}(z) \equiv \text{Tr}_{\mathcal{H}} (\rho \mathcal{O} \Delta_{\psi}^{iz} \mathcal{O}' \Delta_{\psi}^{-iz}), \quad (62)$$

which tells us how much  $\mathcal{O}$  overlaps with the “time-evolved” version of  $\mathcal{O}'$ . Note that the overlap of any operator with the identity is of course constant in time, viz.  $f_{\mathbf{1}\mathcal{O}}(z) = f_{\mathcal{O}\mathbf{1}}(z) = \langle \mathcal{O} \rangle$  for all  $z$ .

Now let’s return to the starting example of two qubits. Define the state

$$|\phi_{\theta}\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle. \quad (63)$$

Both reduced density matrices are  $\rho_A = \rho_{\bar{A}} = \cos^2 \theta \oplus \sin^2 \theta$ . The modular operator computed for the algebra  $\mathcal{A}_L$  of the left qubit is accordingly

$$\Delta_{\phi_{\theta}} = \begin{pmatrix} 1 & & & \\ & \cot^2 \theta & & \\ & & \tan^2 \theta & \\ & & & 1 \end{pmatrix}. \quad (64)$$

Of course, we would get the same modular operator if we used the algebra  $\mathcal{A}_R$ .

Let us now do some modular flows. For any two operators  $\mathcal{O}, \mathcal{O}' \in \text{End}(\mathcal{H}_L)$ , we write the function  $f_{\mathcal{O}\mathcal{O}'}(z)$  as

$$f_{\mathcal{O}\mathcal{O}'}(z) = \text{Tr}_{\mathcal{H}} (\rho_{\phi_{\theta}} (\mathcal{O} \otimes \mathbf{1}_R) \Delta_{\phi_{\theta}}^{iz} (\mathcal{O}' \otimes \mathbf{1}_R) \Delta_{\phi_{\theta}}^{-iz}) = \langle \phi_{\theta} | (\mathcal{O} \otimes \mathbf{1}_R) \Delta_{\phi_{\theta}}^{iz} (\mathcal{O}' \otimes \mathbf{1}_R) | \phi_{\theta} \rangle, \quad (65)$$

where we have used

$$\Delta_{\phi_{\theta}}^{iz} |\phi_{\theta}\rangle = |\phi_{\theta}\rangle, \quad (66)$$

which one can check either by the definition of the modular generator  $S$  and the definition  $\Delta = S^{\dagger} S$ , or by using (57) and Schmidt-decomposing  $|\phi_{\theta}\rangle$ . Intuitively this is because  $|\phi_{\theta}\rangle$  is (by construction) the ground state of the “Hamiltonian”  $\ln \Delta_{\phi_{\theta}}$ . In this case the expression for  $f$  simplifies to

$$f_{\mathcal{O}\mathcal{O}'}(z) = \text{Tr}_{\mathcal{H}_L} (\rho_{\phi_{\theta},L} \mathcal{O} \rho_{\phi_{\theta},L}^{iz} \mathcal{O}' \rho_{\phi_{\theta},L}^{-iz}). \quad (67)$$

We see that

$$f_{ZZ}(z) = 1, \quad f_{XZ}(z) = f_{ZX}(z) = 0, \quad (68)$$

which are a consequence of  $Z$  being invariant under the modular flow

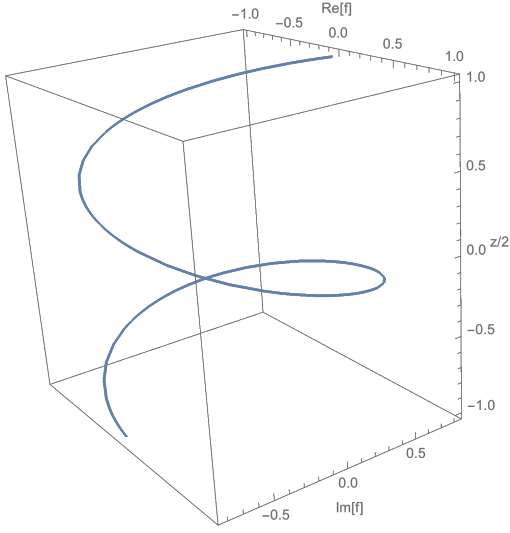
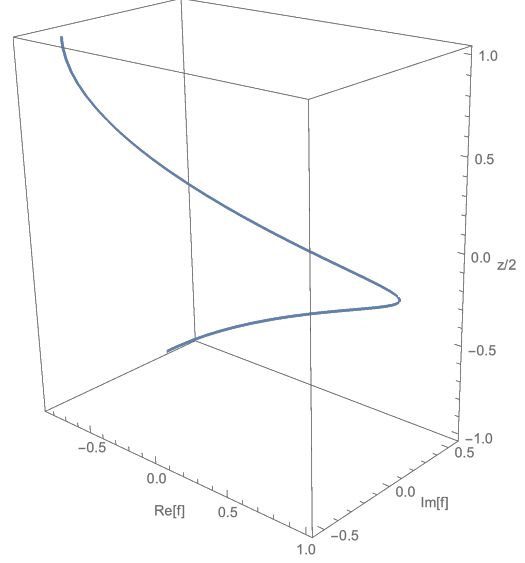
$$\Delta_{\phi_{\theta}}^{iz} (Z_L \otimes \mathbf{1}_R) \Delta_{\phi_{\theta}}^{-iz} = Z_L \otimes \mathbf{1}_R, \quad (69)$$

which is in turn a consequence of the fact that the state  $|\phi_{\theta}\rangle$  doesn’t mix the spins in the  $Z$  basis. Thus the only possible  $f$  that has a chance to actually evolve under the modular flow is  $f_{XX}(z)$ , which is

$$f_{XX}(z) = \cos^2 \theta (\tan^2 \theta)^{iz} + \sin^2 \theta (\cot^2 \theta)^{iz}. \quad (70)$$

At the symmetric point  $\theta = \pi/4$ ,  $f_{XX}(z) = 1$ . As we go further away from the symmetric point,  $f_{XX}(z)$  for  $z \in \mathbb{R}$  starts to spiral around the origin in the complex plane. The spirals become faster and faster, with a period that goes to zero as  $\theta$  approaches  $\pi$  or 0. The figures




 Figure 2: Here we take  $\theta = 0.3$ .

 Figure 3: Here we take  $\theta = \pi/4 - 0.3$ .

show the trajectory for  $z \in \mathbb{R}$  for two different  $\theta$  values. We can also examine the analytic structure of  $f_{XX}(z)$  when  $z \in \mathbb{C}$ , an example of this is shown in the next figure.

Suppose we instead used the Bell state  $\varphi_\theta = \cos\theta|01\rangle + \sin\theta|10\rangle$ . Working in the  $0,1$  basis (n.b. not Schmidt-decomposing  $\varphi_\theta$ ), we get

$$\Delta_{\varphi_\theta} = \begin{pmatrix} \cot^2 \theta & & & \\ & 1 & & \\ & & 1 & \\ & & & \tan^2 \theta \end{pmatrix}. \quad (71)$$

The reduced density matrices are

$$\rho_L = \begin{pmatrix} \cos^2 \theta & \\ & \sin^2 \theta \end{pmatrix}, \quad \rho_R = X \rho_L X. \quad (72)$$

Thus if  $\mathcal{O}, \mathcal{O}' \in \mathcal{A}_L$ , the modular flow function  $f_{\mathcal{O}\mathcal{O}'}(z)$  is the same as for the case with the  $\cos\theta|00\rangle + \sin\theta|11\rangle$  state. If  $\mathcal{O}, \mathcal{O}' \in \mathcal{A}_R$  then we take  $\theta \mapsto \theta + \pi/2$ , but the form of  $f_{\mathcal{O}\mathcal{O}'}(z)$  is the same.

We can also look at relative modular operators. Let  $\psi$  be a cyclic vector for the algebra  $\mathcal{A}_L$ , and let  $\phi$  be arbitrary. Let  $\rho$  and  $\sigma$  be the associated density matrices for these two states. For any  $\mathcal{O} \in \mathcal{A}_L$ , we define the relative modular generator as

$$S_{\psi|\phi} \mathcal{O} |\psi\rangle = \mathcal{O}^\dagger |\phi\rangle. \quad (73)$$

The relative modular operator is then defined in the expected way as

$$\Delta_{\psi|\phi} = S_{\psi|\phi}^\dagger S_{\psi|\phi}. \quad (74)$$

The matrix elements of these operators can be computed by Schmidt-decomposing both  $\psi$  and  $\phi$  in their respective Schmidt bases, which in general are not orthogonal (despite this,

it is better to do this than to Schmidt-decompose  $\psi$  and non-diagonally decompose  $\phi$  in the same basis). Following the same procedure that we did in the non-relative case, one gets

$$\Delta_{\psi|\phi} = \sigma_L \otimes \rho_R^{-1}. \quad (75)$$

Note that we don't require the reduced density matrices of  $\phi$  to be invertible, only those of  $\rho$  (that is, we only require  $\psi$  to be cyclic, not  $\phi$ ).

## Algebraic entropies

One advantage to formulating things algebraically is that we get a natural notion of entropy for algebras, which is a more general notion than the entropy associated to spatial regions. For example, we can compute the algebra of the  $X$ -spin operators, or the algebra of  $Z$ -spin operators, or the tensor product of a pair of Pauli algebras located at a pair of non-adjacent sites (thus computing an “entanglement correlation function”), and so on. A good mathematical take on this perspective is in Daniel's paper [?].

Given an algebra  $\mathcal{A}$ , we choose to work in a basis where the operators  $\mathcal{O} \in \mathcal{A}$  are orthogonal with respect to the Hilbert-Schmidt inner product

$$\langle \mathcal{O}_a | \mathcal{O}_b \rangle = \frac{1}{\text{Tr} \mathbf{1}_{\mathcal{A}}} \text{Tr}(\mathcal{O}_a^\dagger \mathcal{O}_b) = \delta_{ab}. \quad (76)$$

We will usually just drop the  $\dagger$  since we are really only interested in observables. Now in general we write the density matrix of the algebra as

$$\rho_{\mathcal{A}} = \frac{1}{\text{Tr} \mathbf{1}_{\mathcal{A}}} \sum_{\mathcal{O} \in \mathcal{A}} c_{\mathcal{O}} \mathcal{O}. \quad (77)$$

In the basis which is orthonormal under the above inner product, the coefficients are just the expectation values, and so

$$\rho_{\mathcal{A}} = \frac{1}{\text{Tr} \mathbf{1}_{\mathcal{A}}} \sum_{\mathcal{O} \in \mathcal{A}} \langle \mathcal{O} \rangle \mathcal{O}. \quad (78)$$

Tensor products of Pauli algebras are especially convenient algebras to work with since this property is already built-in, so no changing of bases is required.

Note the decomposition of the density matrix in this way is actually kind of cool, since it tells us that in order to figure out the reduced density matrix of e.g. a given spatial region  $A$ , we just need to know the correlation functions of operators entirely contained within  $A$  (note we are not assuming anything about  $\dim \mathcal{A}$  relative to  $\dim \mathcal{H}$ ). So, to figure out how entangled  $A$  is with the rest of the system, we actually don't need to know anything about the fields in the other part of the system at all!<sup>5</sup> We only need to know about local stuff going on in  $A$  (well, this is a slightly misleading way of phrasing it — we only need to know about correlation functions for operators supported in  $A$ , but those correlation functions still depend on stuff outside of  $A$  since the sum that goes into computing them will involve stuff

---

<sup>5</sup>Apart from the fact that we knew it was a pure state, which makes the result less surprising.

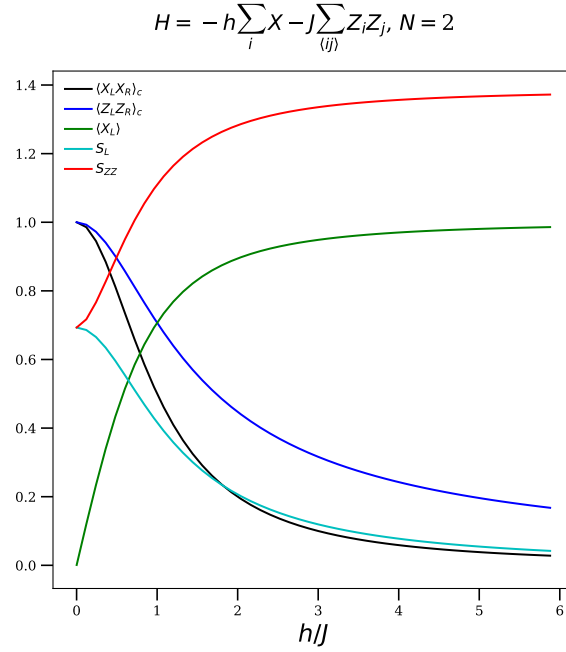


Figure 4: Various entanglement-related quantities for a two-site TFIM. Here  $S_{\mathcal{A}}$  denotes the algebraic entropy of the algebra  $\mathcal{A}$ . The entanglement entropy for a single site  $S_{P_i \in \{L, R\}}$  and the algebraic entropy for the  $X_L X_R$ -algebra are the same, as are the  $Z_L Z_R$  and  $Y_L Y_R$  two-point functions. The algebraic entropy of the  $Z_L Z_R$  algebra and the  $Y_L Y_R$  algebra are also identical. By symmetry,  $\langle Z_i \rangle = \langle Y_i \rangle = 0$ .

in  $\bar{A}$ ).<sup>6</sup> This is essentially because the entanglement present in generic ground states allows us to build up information in  $\bar{A}$  just from information in  $A$ .

In previous sections, we made use of the decomposition  $\mathcal{H} \cong \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ . While if we have in mind some collection of qubits then such a decomposition is always possible if  $A$  is associated to a spatial region, for algebras not tied to a particular region, this is not a convenient decomposition. In general, if  $Z(\mathcal{A}) = 0$  then  $\mathcal{A}$  induces a decomposition  $\mathcal{H} \cong \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$  (again  $A$  is not necessarily associated to a spatial region), on which  $\mathcal{A}$  acts as

$$L(\mathcal{H}_A) \otimes \mathbf{1}_{\bar{A}}. \quad (79)$$

Thus if  $Z(\mathcal{A}) = 0$  we can write  $|\psi\rangle = \sum_{ij} c_{ij} |ij\rangle$ , and use the strategy developed previously. If  $Z(\mathcal{A}) \neq 0$  however, we get the weaker

$$\mathcal{H} \cong \bigoplus_{\alpha} \mathcal{H}_{\alpha} \otimes \mathcal{H}_{\bar{\alpha}}, \quad (80)$$

where the sum runs over a complete set of orthogonal projectors  $\Pi_{\alpha} \in Z(\mathcal{A})$ , and on which  $\mathcal{A}$  acts as

$$\bigoplus_{\alpha} L(\mathcal{H}_{\alpha}) \otimes \mathbf{1}_{\bar{\alpha}}. \quad (81)$$

This just comes from simultaneously diagonalizing the elements of  $Z(\mathcal{A})$  and finding the minimal projectors in the center.

As an example, consider the algebra generated by  $X_L = X \otimes \mathbf{1}$  and  $X_R = \mathbf{1} \otimes X$ . In this case  $Z(\mathcal{A}) = \mathcal{A}$ , and so since  $\mathcal{A} \cong \mathbb{Z}_2^2$  has four irreps we get four projectors

$$\Pi_{\pm_L \pm_R} = \mathbf{1} \pm_L X_L \pm_R X_R + (\pm_L \cdot \pm_R) X_L X_R, \quad (82)$$

where  $\pm_L, \pm_R \in \{1, -1\}$ . Choosing the  $+$  ( $-$ ) sign for  $L/R$  projects onto the eigenspace of  $X_{L/R}$  with positive (negative) eigenvalue.

Continuing with this example, we can write a generic element in  $\mathcal{H}$  as

$$|\psi\rangle = a|++\rangle + b|+-\rangle + c|-+\rangle + d|--\rangle. \quad (83)$$

Suppose  $|\psi\rangle$  is an eigenstate of one of the operators in  $\mathcal{A}$ . Then by acting on  $|\psi\rangle$  with this operator, we see that two of the coefficients in the above decomposition must vanish. But as soon as at least one of the coefficients in the expansion vanishes, the associated density matrix  $|\psi\rangle\langle\psi|$  will not be invertible since it annihilates the ket whose coefficient in the decomposition in  $|\psi\rangle$  is zero. Thus, more generally we see that if  $|\psi\rangle$  is an eigenstate of any operator (other than  $\mathbf{1}$ ) in  $\mathcal{A}$  then  $\psi$  is not cyclic for  $\mathcal{A}$ . Equivalently, we can say that  $\psi$  will fail to be cyclic for  $\mathcal{A}$  if  $\langle\mathcal{O}\rangle = \pm 1$  for some  $\mathcal{O} \in \mathcal{A}$  (assuming we are still in the basis in which  $\text{Tr}(\mathcal{O}_a \mathcal{O}_b) \propto \delta_{ab}$ ).

Suppose we fix our state  $\psi$  to be the ground state of  $H$ . For simplicity, let's again work with the 2-qubit example. If the ground state is a tensor product  $\psi = \psi_L \otimes \psi_R$ , then it is not

---

<sup>6</sup>Think about e.g. spin-spin correlations in an Ising model: the correlator between two spins in some subregion  $A$  can be constructed from knowledge of other correlators contained within  $A$ , but at the same time it can also be computed by e.g. summing up paths connecting the locations of the two spins, and many of these paths will have support in  $\bar{A}$  and hence will depend on what's going on outside  $A$ .

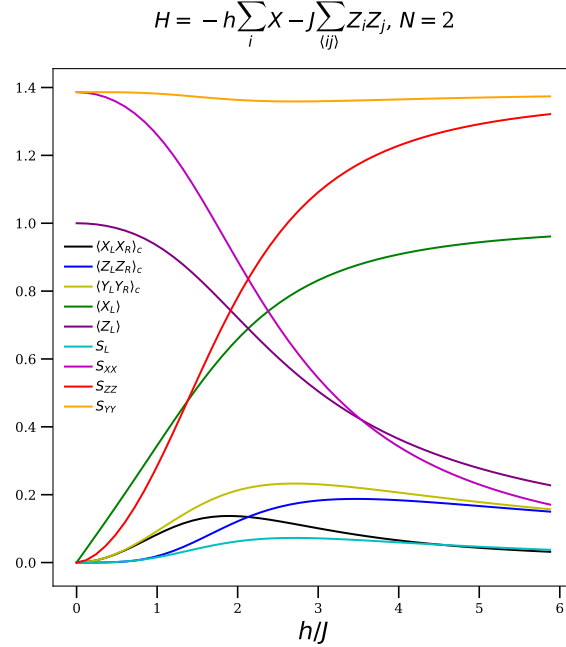


Figure 5: Just for fun, the chaos unleashed when we do a repetition of the previous plot but with a longitudinal field of strength  $J$  added (so the title of the plot is wrong, and a  $-J \sum_i Z_i$  should be added).

cyclic for  $\mathcal{A}_L$ . This is because the projector onto  $|\psi_L\rangle^\perp$  is in  $\mathcal{A}_L$ , and so  $\mathcal{A}_L$  is not separating for  $\psi$ , meaning that  $\mathcal{A}_R = \mathcal{A}'_L$  is not cyclic. But then  $\mathcal{A}_L$  is not cyclic either.

What about the algebras  $\mathcal{A}_X \ni \mathbf{1}, X_L, X_R, X_L X_R$  and  $\mathcal{A}_Z \ni \mathbf{1}, Z_L, Z_R, Z_L Z_R$ ? Let us work in a basis where all the elements of the algebra are diagonal. First, write the associated density matrix for the algebra as  $\rho \propto \sum_{\mathcal{O} \in \mathcal{A}} \langle \mathcal{O} \rangle \mathcal{O}$ . As discussed earlier,  $\mathcal{A}|\psi\rangle$  will be dense in  $\mathcal{H}$  iff  $\rho_{\mathcal{A}}$  is invertible. As we just saw, this fails if  $\psi$  is an eigenstate of any of the  $\mathcal{A} \in \mathcal{A}$  (other than  $\mathbf{1}$ ). This is in keeping with the general symmetry  $\iff$  degeneracy idea. Another way to see this result is to note that if  $\psi$  is an eigenstate of some  $\mathcal{O} \in \mathcal{A}$ , then  $\mathcal{O}$  acts as the identity on  $\psi$ , and thus doesn't contribute to the part of the Hilbert space generated by  $\mathcal{A}|\psi\rangle$ . Since there are only  $\dim \mathcal{H}$  operators in  $\mathcal{A}$ , this means that  $\mathcal{A}|\psi\rangle$  cannot generate all of  $\mathcal{H}$ , and so  $\psi$  is not cyclic for  $\mathcal{A}$ .

For example, for the TFIM model for 2 sites, the algebra  $\mathcal{A}_X$  is never cyclic for the ground state, since the symmetry generated by  $X_L X_R$  implies  $|\psi\rangle$  is a  $X_L X_R$  eigenstate. At  $h = 0$  we have the ground state  $(|00\rangle + |11\rangle)/\sqrt{2}$ , although if we instead had  $|00\rangle$  then the ground state would be cyclic for  $\mathcal{A}_X$ , since  $\langle \mathcal{O} \rangle_{|00\rangle} = 0 \forall \mathcal{O} \in \mathcal{A}_X$  implies  $\rho_{\mathcal{A}_X} \propto \mathbf{1}$  is invertible. By contrast,  $\psi$  is always cyclic for the  $\mathcal{A}_Z$  algebra, unless  $h = 0$  in which case  $|\psi\rangle \propto |00\rangle + |11\rangle$  is a  $Z_L Z_R$  eigenstate. When  $h \rightarrow \infty$  then  $|\psi\rangle = |++\rangle$  is not cyclic for  $\mathcal{A}_X$  since all the operators in  $\mathcal{A}_X$  have expectation value 1, but it is cyclic for  $\mathcal{A}_Z$ , for the same reason that  $\mathcal{A}_X$  is cyclic for  $|00\rangle$ .

The other natural algebras to look at are those of the form  $\mathcal{A}_i$ , the algebra of Pauli operators at a given site (or collection of sites)  $i$ .  $\psi$  will fail to be cyclic for these algebras precisely when  $\psi = \psi_i \otimes \psi_{\bar{i}}$ , since then  $\rho_i$  annihilates all vectors orthogonal to  $\psi_i$  in  $\mathcal{H}_i$ .

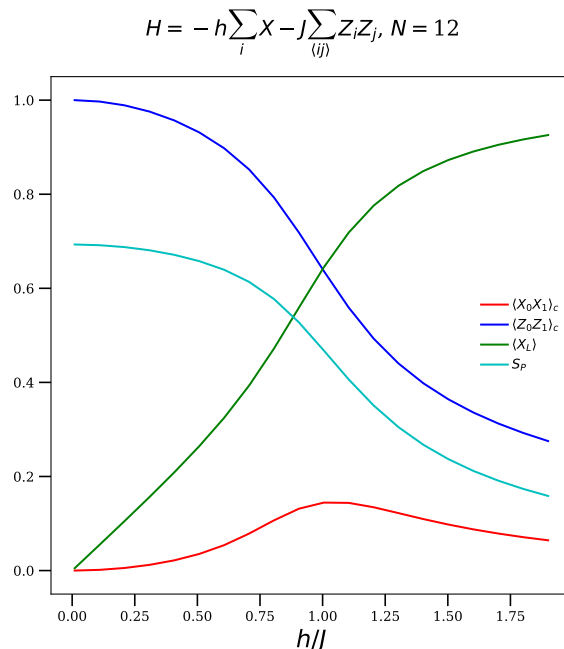


Figure 6: A 12-site TFIM chain. Note the evidence of the phase transition at  $h/J = 1$ .

Recapitulating, we see that if the wavefunction is a product state over different lattice sites this precludes it from being cyclic for algebras built from tensor products of Pauli algebras at different sites, it can still be cyclic for different types of algebras like  $\mathcal{A}_X$  and  $\mathcal{A}_Z$ .

Of course, a 2-qubit system, which is all that we've been focusing on so far since we wanted to do things analytically, is very simple. Less trivial is an  $N$ -qubit chain with periodic boundary conditions. My laptop can handle up to  $N \sim 12$  exactly; figure 6 shows various algebraic properties of interest for a length-12 chain.



## Simple heuristics for classical vs quantum probabilities

---

Today's entry is a very short and rather trivial comment on classical / quantum probability theory that I wanted to remember.

▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼

To discuss probability in quantum mechanics, we need to clarify what kind of things we are looking at probability distributions of. The most natural things to associate probabilities

to are projectors onto eigenstates of Hermitian operators (nevermind that one can never truly act with a projector in a closed quantum system).

Let  $P$  be such a projector. The probability of projecting into the image of  $P$  is given by  $\mu(P) = \text{Tr}[\rho P]$ . Since we can always diagonalize  $\rho$  in the eigenbasis of the observable associated to  $P$ , there is never anything quantum about probability distributions for single observables (the fact that the entries of  $\rho$  can be complex isn't key here, since  $\mu(P)$  is always real and can be captured by a completely classical probability distribution).

The difference with quantum mechanical probabilities only shows up when we look at joint probability distributions, since these can involve operators which don't commute. Consider two projectors  $P, Q$ , which project onto subspaces of the eigenbases of two different observables. In classical probabilities, the probability of  $P$  given  $Q$  would be

$$\mu(P|Q) = \frac{\mu(P \cap Q)}{\mu(Q)}. \quad (84)$$

On the other hand, in quantum mechanics, the probability of  $P$  given  $Q$  is computed by

$$\mu(P|Q) = \frac{\text{Tr}[\rho_Q P]}{\text{Tr}[\rho_Q]} = \frac{\text{Tr}[\rho Q P Q]}{\text{Tr}[\rho Q]}, \quad (85)$$

where  $\rho_Q = Q \rho Q$ . Now the probability distribution associated to the intersection of the images of  $P$  and  $Q$  is

$$\mu(P \cap Q) = \text{Tr}[\rho P Q], \quad (86)$$

Therefore the classical and quantum versions of  $\mu(P|Q)$  agree only when  $P$  and  $Q$  commute; this is the real difference between classical and quantum probabilities.

The fact that  $\mu(P \cap Q)$  is ill-defined (assuming that we want  $\mu(P \cap Q) = \mu(Q \cap P)$  in the quantum case when  $[P, Q] \neq 0$ ) is because in this case, one measurement disturbs this other. The failure of Bayes's theorem, which is the obstruction to defining  $\mu(P \cap Q)$ , is given by

$$\delta B(P, Q) = \mu(Q)\mu(P|Q) - \mu(P)\mu(Q|P) = \text{Tr}[\rho(Q P Q - P Q P)]. \quad (87)$$

As an example, consider the case when  $P = \Pi_{\uparrow}, Q = \Pi_{+}$ , where  $\Pi_{\uparrow}$  projects onto the largest eigenvalue of the  $\mathbb{Z}_N$  Pauli  $Z$  and  $\Pi_{+}$  projects onto the largest eigenvalue of the  $\mathbb{Z}_N$  Pauli  $X$ . Then  $P Q P = P/N$  and  $Q P Q = Q/N$ , so that in this case

$$\delta B(P, Q) = \frac{1}{N} \text{Tr}[\rho(Q - P)]. \quad (88)$$

One might think that this is non-vanishing if  $[P, Q] \neq 0$ , but this is not the case: for example, for  $N = 2$  with  $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , this will vanish provided that  $a = b + c + d$ .



## Algebraic entanglement entropy reminder

---

Today we will remind ourselves of how entanglement entropy is defined in gauge theories, focusing on lattice Abelian gauge theories to make things easy. We will recapitulate why the natural generalization of entanglement entropy is best called algebraic entropy and will explain how to define the entropy of an algebra of operators  $\mathcal{A}$ , especially when the center  $Z(\mathcal{A})$  is nontrivial. The appendix in Daniel Harlow’s paper on the RT formula and error correction is a good reference, and I learned most of what follows from Daniel himself.

❧ ❧

A word on notation:  $\mathcal{A}_A$  will denote the algebra of operators supported within a spatial region  $A$ . When we don’t have a particular spatial region in mind and are just referring to an algebra, we will just write  $\mathcal{A}$ . In an effort to use as many incarnations of the letter  $a$  as possible, we will also use the index  $a$  to label direct sum decompositions.

### Generalities on algebraic entropy and what to do about nontrivial centers

We first start with addressing how to view entanglement entropy from an algebraic point of view. The idea is to focus on the entanglement entropy of an algebra of operators more abstractly, rather than tying ourselves down by thinking of these operators are corresponding to a certain physical region of space (so really, we should be calling it algebraic entropy). This viewpoint is required if we are interested in gauge theories, but more generally we might want to deal with algebras other than the algebra of all operators supported within a certain region.

Although our focus is on the algebra rather than the Hilbert space, throughout we will assume a finite-dimensional Hilbert space (more importantly, a finite-dimensional representation of the algebra of interest), since we have lattice gauge theory in mind. Seeing to what extent the statements below hold in the infinite-dimensional case requires a bit more work but as a cmt person at heart I don’t really care too much.

Suppose we are given an algebra  $\mathcal{A}$ . If  $\mathcal{A}$  has trivial center (i.e. if  $Z_{\mathcal{A}} = \{\lambda \mathbf{1} \mid \lambda \in \mathbb{C}\}$ ), then it is a factor, meaning that it induces a tensor product decomposition  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ , on which it acts as  $L(\mathcal{H}_A) \otimes \mathbf{1}_{\bar{A}}$ , where  $L(\mathcal{H}_A)$  are the linear operators on  $\mathcal{H}_A$ .

In such a case, the algebraic entropy of the subalgebra  $\mathcal{A}_A$  (which we haven’t defined yet) is the same as the entanglement entropy of the region  $A$ , namely

$$S(\mathcal{A}_A) = -\text{Tr}(\rho_A \ln \rho_A). \quad (89)$$

If  $Z_{\mathcal{A}}$  is nontrivial, things change. In this case, we no longer have a simple  $\mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$  factorization. Schematically, this is because the tensor product  $U \otimes V$  of two vector spaces is defined to be “the freest possible bilinear product” between  $U$  and  $V$ , meaning that we impose  $U \otimes V \ni (au, v) = (u, av)$  for  $a \in \mathbb{C}$ , but no other relations. Thinking of  $\mathcal{A} = \mathcal{A}_A$  as the collection of operators supported within some spatial region  $A$ , then if  $Z_{\mathcal{A}}$  is nontrivial



we would have relations like  $(zu, v) = (u, zv)$  for  $z$  a central element and  $(u, v)$  an element of a putative tensor product. This only jives with the definition of  $\otimes$  if  $z$  is a scalar, i.e. if the center is trivial. If  $Z_{\mathcal{A}}$  is nontrivial one could imagine doing something like factoring  $\mathcal{H}$  as  $\mathcal{H} = \mathcal{H}_A \otimes_{Z_{\mathcal{A}}} \mathcal{H}_{\bar{A}}$  where  $Z_{\mathcal{A}}$  is treated as the tensor unit, but this is messy and I think is the wrong direction to go in.

Central elements typically come from non-local constraints, like gauge constraints. When the algebras in question are associated to the operators within a spatial region  $A$ , the central elements will usually correspond to degrees of freedom living on  $\partial A$ . We will see that elements in  $Z_{\mathcal{A}}$  contribute a Shannon term to the entanglement entropy, since they commute with everything and as such are “classical”. The Shannon term will usually manifest itself as the entropy associated to the boundary conditions on  $A$ .

Since stuff in  $Z_{\mathcal{A}}$  commutes with everything in  $\mathcal{A}$ , we can work in a representation in which all the elements in  $Z_{\mathcal{A}}$  are diagonalized. Thus we can write an element  $x \in Z_{\mathcal{A}}$  as

$$x = \bigoplus_a \lambda_a \mathbf{1}_{|a| \times |a|}, \quad (90)$$

where  $\lambda_a \in \mathbb{C}$  and  $|a|$  is the size of the  $a$ th block in the diagonalized representation of the center. The sum is an orthogonal direct sum since each generator of  $Z_{\mathcal{A}}$  corresponds to a single block, and if the different blocks overlapped, the generators would not commute with each other (and hence wouldn’t be generators of  $Z_{\mathcal{A}}$ ).

Let the projector  $\Pi_a$  be defined to project onto the  $a$ th block in the decomposition. They satisfy  $\Pi_a \Pi_b = \delta_{ab} \Pi_a$ . Since  $\dim \mathcal{H} < \infty$  we can and will always take the direct sum decomposition above to be complete, so that the  $\Pi_a$ s are minimal projectors (meaning that there are no projectors that map onto a subspace of an image of one of the  $\Pi_a$ s).

Since  $\mathcal{A}_a \equiv \Pi_a \mathcal{A} \Pi_a$  is the component of  $\mathcal{A}$  contained within a single block of the decomposition, all the elements in the center act on it either as 0 or as  $\lambda_a \mathbf{1}_{|a| \times |a|}$ . One can then check that  $\mathcal{A}_a$  is a von Neumann algebra with trivial center. Indeed, if  $Z_{\mathcal{A}_a}$  were non-trivial, we would diagonalize it as above and it would contain a projector  $\Pi_{\tilde{a}}$  which was represented as something other than  $\mathbf{1}$  on  $\Pi_a \mathcal{H}$ . Then we could form the projector  $\Pi_{\tilde{a}} \otimes 0_{(1-\Pi_{\tilde{a}})\mathcal{H}}$ , which is a central element of  $\mathcal{A}$  and a projector, contradicting the assumed completeness of the  $\Pi_a$ s.

Thus, while  $\mathcal{A}$  doesn’t induce a tensor factorization of  $\mathcal{H}$ , the upshot is that we can use the  $\mathcal{A}_a$ s to induce a tensor factorization on subspaces of  $\mathcal{H}$ . They won’t split the full Hilbert space, but they will split the subspaces  $\mathcal{H}_a \equiv \Pi_a \mathcal{H}$  on which they act. Since they are type I factors, we know that they induce a splitting

$$\mathcal{H}_a = \mathcal{H}_{A_a} \otimes \mathcal{H}_{\bar{A}_a}, \quad (91)$$

where  $A_a$  is some region associated to the factor  $\mathcal{A}_a$ . From their realizations as type I factors, they act on each  $\mathcal{H}_a$  as

$$\mathcal{A}_a = L(\mathcal{H}_{A_a}) \otimes \mathbf{1}_{\bar{A}_a}. \quad (92)$$

Since each  $\mathcal{A}_a$  induces a tensor product decomposition on each subspace  $\mathcal{H}_a$ , the full Hilbert space splits up into a sum of products according to the elements of the center:

$$\mathcal{H} = \bigoplus_a (\mathcal{H}_{A_a} \otimes \mathcal{H}_{\bar{A}_a}). \quad (93)$$

Given a global state  $\rho$  we want to construct a density matrix  $\rho_{\mathcal{A}}$  for  $\mathcal{A}$ , one which will faithfully reproduce expectation values of operators in  $\mathcal{A}$  but which will carry no information about what's going on in the commutant  $\mathcal{A}'$ . Since we have used the  $\Pi_a$  projectors to decompose  $\mathcal{A}$  into different von Neumann algebras, to get  $\rho_{\mathcal{A}}$  we need only to retain information about the diagonal components in the block decomposition. This is because any operator  $\mathcal{O} \in \mathcal{A}$  must have  $\mathcal{O}_{\alpha\beta} \propto \delta_{\alpha\beta}$  since  $\mathcal{O}$  commutes with everything in the center, and so as far as computing  $\langle \mathcal{O} \rangle$  goes, we only need to worry about the  $\rho_{aa}$  components. So we can write (this notation really is hilariously bad)

$$\rho_{\mathcal{A}} = \bigoplus_a p_a \rho_{A_a}, \quad (94)$$

where each component of the density matrix is taken to have unit trace on its parent tensor sub-factor:

$$\text{Tr}_{\mathcal{H}_a} \rho_{A_a} = 1. \quad (95)$$

Since the component density matrices have unit trace, the  $p_a$ s are

$$p_a = \text{Tr}_{\mathcal{H}_a} \rho_{\mathcal{A}}. \quad (96)$$

Thus  $\sum_a p_a = 1$ . There are some different ways to choose normalization factors and stuff for the different components of the density matrix, but I don't think the actual choice is too important.

So, the classical probabilities measure the traces of each part of the full density matrix, while each block of the density matrix has unit trace, allowing it to be defined as a bona fide density matrix on each superselection sector  $a$  (we call them superselection sectors since there are no operators with off-diagonal blocks which connect different  $\mathcal{H}_a$  subspaces, by virtue of the fact that all operators must commute with everything in  $Z_{\mathcal{A}}$ . The idea here is that the Hilbert space splits into a decomposition in terms of “boundary conditions”, which are given by the central elements in  $Z_{\mathcal{A}}$ . Of course, the individual probabilities  $p_a$  will have to be calculated on a case-by-case basis; they correspond to the probability of “getting” the superselection sector  $a$ .

We can then define an algebraic entropy for  $\mathcal{A}$  by taking the von Neumann entropy of  $\rho_{\mathcal{A}}$ :

$$S(\mathcal{A}) = - \sum_a p_a \ln p_a + \sum_a p_a S(\rho_a). \quad (97)$$

The first part is classical since it comes from elements of the center, which by virtue of their commutativity with everything, are effectively classical. Thus the probability distribution of the superselection sectors are responsible for the classical Shannon term. This is in-line with the idea that you can have states which are mixtures of different superselection sectors (you can have multiple  $p_a \neq 0$ ), but you cannot have superpositions of different sectors (by definition), and so their contribution to  $S(\mathcal{A})$  must be in the form of a Shannon term.

Note that the presence of a nontrivial center *reduces* the total entanglement entropy. This is not a very precise statement as it stands: roughly, we mean that if we imagine one algebra  $\mathcal{A}$  with nontrivial  $Z_{\mathcal{A}}$  and some  $\tilde{\mathcal{A}} = \mathcal{A} \cup \{\mathcal{O}_c\}$  with a few operators  $\mathcal{O}_c$  that have very small weights in the density matrix and are such that their inclusion forces  $Z_{\mathcal{A}}$  to become trivial

(think of very massive electric charges for Abelian gauge theory), then  $S(\tilde{\mathcal{A}}) > S(\mathcal{A})$ . This might seem not to be the case due to the presence of the positive classical Shannon entropy term, but the von Neumann  $S(\rho_a)$  contribution increases to more than account for the lack of the Shannon term. That the presence of a nontrivial center reduces the total entropy is of course physical: gauge constraints reduce the size of the effective Hilbert space, which after all is what entropy is designed to capture (or another way to say it — gauge constraints allow you to use gauge invariance to gain non-local information about the state by e.g. measuring electric fields and using Gauss's law; this increased information reduces the entropy).

### Lattice gauge theory examples

The basic variables for us are the holonomies  $\exp(i \int_l A)$  (the integral of  $A$  along a link  $l$ ) and the electric fields  $E_l^r$ , which measure the flux passing along  $l$  in a certain representation  $r$ . In the abelian case,  $E = i \frac{\delta}{\delta A}$ . When we are working with discrete gauge theories, the Hilbert space and algebra of operators are

$$\mathcal{H} = \bigotimes_l \mathbb{C}_l^N, \quad \mathcal{A} = \bigotimes_l \text{Gl}(N, \mathbb{C})_l. \quad (98)$$

Operators on different links thus commute. We will usually work in the basis where  $E_l^r$  is diagonalized on each link. The physical Hilbert space is spanned by the states created by loops of constant electric flux. A wilson loop of charge 1 around a plaquette is a creation operator for these states.

Using Gauss' law, we can write the electric field  $E_l$  on a boundary link as the product of  $E_k$ 's with  $k$  links all entirely outside of  $A$ . The electric flux variables on the boundary of the region are thus effectively classical because their conjugate variables  $e^{iA_l \in \partial A}$  aren't in  $\mathcal{A}_A$ . Also, we see that the operators in  $\mathcal{A}$ , namely  $\mathcal{A}_A$ , actually generate *more* than just themselves: they also generate electric field operators lying outside of  $A$ . This is in-line with a general result which says that the algebra of operators generated by  $\mathcal{A}_A$  is in fact the double commutant  $(\mathcal{A}_A)''$ . If  $\mathcal{A}_A$  is a von Neumann algebra then the operator algebra it generates is itself, but for gauge theory applications this is not the case.

Since  $Z_{\mathcal{A}_A}$  is non-trivial for generic choices of subregions in gauge theories, we need to follow the procedure of the previous section to be able to compute an algebraic entropy. What are the projectors  $\Pi_a$  in this case? They are simply the projectors onto electric flux configurations on  $\partial A$ . They are complete ( $\bigoplus_a \Pi_a = \mathbf{1}$ ) and they are orthogonal, since no gauge-invariant operator in  $\mathcal{A}_A$  can change the electric flux boundary conditions (the only operators that can are Wilson lines that end on the boundary). The gauge constraint means that physically, while we can form mixtures of states with different electric flux configurations, we are not allowed to take superpositions. Thus the density matrix must be diagonalized in the electric boundary flux basis, and we have seen that it indeed is. Also, of course not all electric flux configurations are allowed, since we require charge neutrality.



## Entanglement for a harmonic oscillator

Today we will find the entanglement entropy between two coupled harmonic oscillators as a function of their masses and the coupling strength. We will do this by explicitly tracing out one of the oscillators and finding the entropy of the reduced density matrix — even for this, the easiest possible example, the calculation is nontrivial. This calculation has of course been done a couple times in the literature (see e.g. Cassini’s paper or Srednicki’s one on black holes) — the goal here is just to understand it for myself and fill in the details that aren’t in the papers.

♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♣

If our oscillators are at positions  $\phi_1, \phi_2$ , have masses  $W_{11}, W_{22}$ , and interact with a coupling  $W_{12}$ , then the ground-state wavefunction is (here  $\phi^T = (\phi_1, \phi_2)$ )

$$\psi = \left( \frac{\det W}{\pi^2} \right)^{1/4} \exp \left( -\frac{1}{2} \phi^T W \phi \right). \quad (99)$$

Thus the full density matrix is

$$\langle \phi | \rho | \phi' \rangle = \sqrt{\frac{\det W}{\pi^2}} \exp \left( -\frac{1}{2} \phi^T W \phi - \frac{1}{2} \phi'^T W \phi' \right). \quad (100)$$

We get the reduced density matrix for the first oscillator by doing the trace over  $\phi_2$ , setting  $\phi_2 = \phi'_2$  and integrating out  $\phi_2$ . This gives

$$\langle \phi | \rho_1 | \phi' \rangle = \sqrt{\frac{\det W}{\pi W_{22}}} \exp \left( -\frac{1}{2} \left( W_{11} - \frac{W_{12}^2}{2W_{22}} \right) (\phi^2 + \phi'^2) + \frac{W_{12}^2}{2W_{22}} \phi \phi' \right). \quad (101)$$

We see that if  $W_{12} = 0$  then we have  $\rho_1 = |\psi_G\rangle\langle\psi_G|$ , where  $|\psi_G\rangle$  is a Gaussian. Since the reduced density matrix is a pure state the entanglement entropy is zero, which one can check by going into an occupation number representation where  $|\psi_G\rangle = |0\rangle$ . Despite the simple form of  $\rho_1$ , we aren’t really in a position to calculate the entanglement entropy: taking the trace is easy, but taking the logarithm of  $\rho_1$  is very difficult, since  $\rho_1$  is not diagonal.

In order to compute the entropy in the  $W_{12}$  case, we can either use the replica trick or go into a basis where  $\rho_1$  is diagonalized. We will go for the latter strategy. We need to figure out how to write the reduced density matrix in a simpler way. Experience teaches us that taking the modular Hamiltonian to look like a real Hamiltonian is a good choice (provided that the oscillators are coupled so that the reduced density matrix is likely to look thermal), and so we guess

$$\rho_1 = \frac{1}{Z_1} \exp(-\varepsilon a^\dagger a), \quad (102)$$

for some appropriate  $a^\dagger, a$ . Since we only have one oscillator to deal with, there is only one species of creation / annihilation operators.  $\varepsilon$  is some energy that we’ll compute later. The  $a$  operators are presumably in the form

$$\pi_1 = \lambda a + \lambda^* a^\dagger, \quad \phi_1 = i(\gamma a - \gamma^* a^\dagger) \quad (103)$$

for some coefficients  $\lambda, \gamma$ . By imposing  $\langle \phi_1 \pi_1 \rangle = i/2$ , we get the constraint

$$\gamma = \frac{1}{2\lambda^*}. \quad (104)$$

We then calculate the expectation values of  $\phi_1^2$  and  $\pi_1^2$  in this basis, which is easy to do since  $e^{-\epsilon a^\dagger a}$  is diagonal:

$$\langle \phi_1^2 \rangle = |\gamma|^2 (2\langle n \rangle + 1), \quad \langle \pi_1^2 \rangle = |\lambda|^2 (2\langle n \rangle + 1). \quad (105)$$

This means that if we know the 2-point functions we know  $\lambda$  and  $\gamma$ :

$$|\lambda|^2 = \frac{1}{2} \sqrt{\frac{\langle \phi_1^2 \rangle}{\langle \pi_1^2 \rangle}}, \quad |\gamma|^2 = \frac{1}{2} \sqrt{\frac{\langle \pi_1^2 \rangle}{\langle \phi_1^2 \rangle}}. \quad (106)$$

We would also know  $\langle n \rangle$ , since

$$2\langle n \rangle + 1 = 2\sqrt{\langle \pi_1^2 \rangle \langle \phi_1^2 \rangle}. \quad (107)$$

We can calculate  $\langle n \rangle$  explicitly since the density matrix is thermal, and we get

$$\tanh(\epsilon) = \frac{1}{2\sqrt{\langle \pi_1^2 \rangle \langle \phi_1^2 \rangle}}. \quad (108)$$

This means that if we can get the 2-point functions, we can get the entanglement entropy. Indeed, since we're in the occupation number basis the trace is now easy to carry out:

$$\begin{aligned} S &= -\text{Tr} \left( (1 - e^{-\epsilon}) e^{-\epsilon a^\dagger a} [\ln(1 - e^{-\epsilon}) - \epsilon a^\dagger a] \right) \\ &= \frac{\epsilon}{1 - e^{-\epsilon}} e^{-\epsilon} - \ln(1 - e^{-\epsilon}). \end{aligned} \quad (109)$$

Rephrasing this slightly,

$$S = \epsilon \langle n \rangle + \ln Z_1, \quad Z_1 = \frac{1}{1 - e^{-\epsilon}}. \quad (110)$$

Plugging in for  $\epsilon$  by inverting (108), we get an expression for  $S$  in terms of the 2-point functions.

All that remains is to get expressions for  $\langle \phi_1^2 \rangle$  and  $\langle \pi_1^2 \rangle$ . They are both easy to calculate. The first one is

$$\langle \phi_1^2 \rangle = \frac{W_{22}}{2 \det W}. \quad (111)$$

The second one is

$$\begin{aligned} \langle \pi_1^2 \rangle &= -\sqrt{\frac{\det W}{\pi W_{22}}} \int d\phi_1 \left( \frac{W_{12}^2 - 2W_{11}W_{22}}{2W_{22}} + 2\phi_1^2 \frac{\det^2 W}{W_{22}^2} \right) \exp(-\phi_1^2 [W_{11} - W_{12}^2/W_{22}]) \\ &= \frac{W_{11}}{2}. \end{aligned} \quad (112)$$

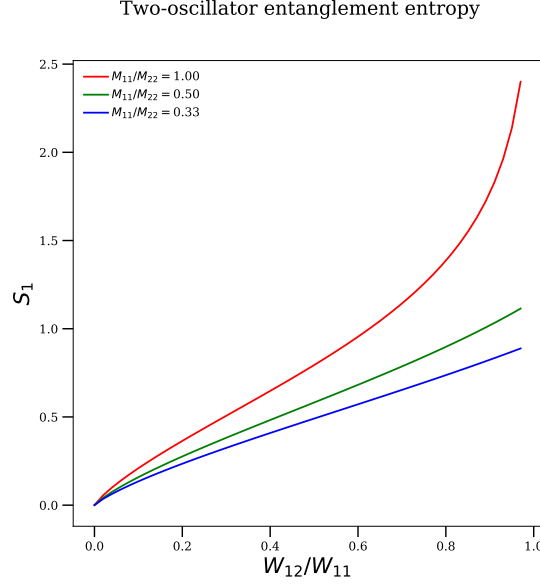


Figure 7: The entanglement entropy after tracing out one of the oscillators in a coupled pair of oscillators.

We get this simple result, the one for a pure Gaussian, since the coupling in the Hamiltonian takes place only in real space. Note that in order for this to work, we need to have  $\det W > 0$ .

So, we are finished! One sees that for  $W_{12} = 0$  we get the pure Gaussian result  $\langle \phi_1^2 \rangle = \langle \pi_1^2 \rangle / W_{11}^2 = 1/(2W_{11})$ . This leads to a vanishing entanglement entropy by way of (110), since for these 2-point functions we have the minimally-uncertain  $\langle \pi_1^2 \rangle \langle \phi_1^2 \rangle = 1/4$ , giving  $\varepsilon \rightarrow \infty$  (projecting onto the ground state), resulting in  $\langle n \rangle = 0$ ,  $Z_1 = 1$ , and hence  $S = 0$ .

In Figure 7 we plot the entanglement entropy as a function of  $W_{12}/W_{11}$  for a few different values of  $W_{11}/W_{22}$ . All the values we show have  $W_{11}/W_{22} < 1$ , but this is done wolog since the entanglement entropy is symmetric under swapping  $W_{11}$  and  $W_{22}$ . The divergence in  $S_1$  as  $W_{12} \rightarrow W_{11}$  for the  $W_{11} = W_{22}$  case is because at these values of the parameters  $W$  is singular.




---

## Intro to thermofield dynamics

Today we are going to be reading about thermofield dynamics and recapitulating some of the important parts. Our focus will be on harmonic oscillator-like systems for simplicity. We will try to explain the information theory meaning behind the thermofield double states

and how Tomita-Takesaki theory makes an appearance. A good reference for this problem is the book by Blasone, Jizba, and Vitiello.

❧ ❧

The basic problem with temperature is that it forces one to work with states that are not pure. This means that expectation values cannot be calculated by simply taking matrix elements of operators in the usual Fock basis. It also makes doing path integrals hard: there is no real concept of nontrivial asymptotic states for e.g. particle scattering processes, and it is no longer to use path integrals to calculate amplitudes for one thermal state  $|\Psi_{in}\rangle$  to evolve to another state  $|\Psi_{out}\rangle$ , since thermal states cannot be written as ket vectors. Indeed, suppose we had some pure state  $|s\rangle = \sum_n s_n |n\rangle$  expressible by transforming the usual Fock basis in some way. Then if  $\mathcal{O}$  is an operator with any nonzero off-diagonal components,

$$\langle s|\mathcal{O}|s\rangle = \sum_{m,n} s_n s_m^* \mathcal{O}_{mn} \neq \frac{1}{\text{Tr}[e^{-\beta H}]} \sum_n e^{-\beta E_n} \mathcal{O}_{nn}, \quad (113)$$

no matter what coefficients we choose. While the imaginary time formalism can be of help here, it is only really usable for studying equilibrium processes where we can do away with time, and doing the analytic continuation at the end can be a pain.

To fix these difficulties, we need to insist on having some “thermal pure state” that we can use to compute expectation values and compute transition amplitudes and stuff. This means we need to find some way to make the overall state pure. The way to do this is essentially to couple the system to a heat bath, so that the combined system+heat bath is in a pure state. Since the original thermal state’s density matrix is invertible — thermal states have “a lot” of entanglement and are far from being product states — the minimal way we can purify the thermal state is to just make a copy of it, so that together with its copy it becomes pure. Following convention, tildes will indicate things belonging to the copy, so that e.g. the full Hilbert space is  $\mathcal{H} \otimes \tilde{\mathcal{H}}$  and if we are interested in the operator algebra  $\mathcal{A}$  acting on the original  $\mathcal{H}$ , then we also have an associated algebra  $\tilde{\mathcal{A}}$  acting on  $\tilde{\mathcal{H}}$ . Recall that if our mixed density matrix is  $\rho = \text{diag}(p_1, \dots, p_n)$  in a basis  $\{|n\rangle\}$  for  $\mathcal{H}$ , then the purification is

$$\rho_p = \sum_{n,m} \sqrt{p_n p_m} |n \otimes \tilde{n}\rangle \langle m \otimes \tilde{m}| = |N\rangle \langle N|, \quad |N\rangle = \sum_n \sqrt{p_n} |n \otimes \tilde{n}\rangle. \quad (114)$$

When this is applied to our thermal density matrix  $\rho$ , we call the resulting purification the thermofield double:

$$|TFD\rangle = \frac{1}{\sqrt{\text{Tr}[e^{-\beta H}]}} \sum_n e^{-\beta E_n/2} |n \otimes \tilde{n}\rangle. \quad (115)$$

By construction, tracing out one of the tensor factors of the pure density matrix  $|TFD\rangle \langle TFD|$  gives a thermal state:

$$\text{Tr}_{\tilde{\mathcal{H}}}(|TFD\rangle \langle TFD|) = \frac{1}{\text{Tr}[e^{-\beta H}]} \sum_n e^{-\beta E_n} |n\rangle \langle n|. \quad (116)$$

We see that (again by construction) if  $\mathcal{O} = \mathcal{O}_A \otimes \mathbf{1}$  then  $\langle TFD | \mathcal{O} | TFD \rangle$  reproduces the correct thermal expectation value of  $\mathcal{O}$  (and likewise if  $\mathcal{O} = \mathbf{1} \otimes \mathcal{O}_{\tilde{A}}$ ). The  $|\tilde{n}\rangle$  states are the “heat bath” and represent coupling to a large “classical” system, since their purpose in life is to select out the diagonal elements of the density matrix when computing expectation values of operators.

Since the vectors in the tilde Fock basis are just a copy of the ones in the original Fock basis, we also see that  $|TFD\rangle$  is a ground state of the following Hamiltonian:

$$\mathcal{H}|TFD\rangle \equiv (H \otimes \mathbf{1} - \mathbf{1} \otimes H)|TFD\rangle = 0. \quad (117)$$

This “doubled system with the copy moving backwards in time” should remind you of either Rindler space or modular flow or both. More on this in a sec.

Let’s look briefly at the obligatory example of the harmonic oscillator in a heat bath. We can write

$$\begin{aligned} |TFD\rangle &= \frac{1}{\sqrt{\text{Tr}[e^{-\beta H}]}} \sum_n \frac{1}{\sqrt{n!}} \frac{1}{\sqrt{n!}} e^{-\beta\omega/4} e^{-\beta\omega n/2} (a^\dagger)^n (\tilde{a}^\dagger)^n |0 \otimes \tilde{0}\rangle \\ &= \frac{e^{-\beta\omega/4}}{\sqrt{\text{Tr}[e^{-\beta H}]}} \sum_n \exp(e^{-\beta\omega/2} a^\dagger \tilde{a}^\dagger) |0 \otimes \tilde{0}\rangle. \end{aligned} \quad (118)$$

Now a little algebra lets us write

$$\frac{1}{\sqrt{\text{Tr} \exp(-\beta H)}} = e^{\beta\omega/4} \sqrt{1 - e^{-\beta\omega}}, \quad (119)$$

so that the ground state is

$$|TFD\rangle = \sqrt{1 - e^{-\beta\omega}} \exp(e^{-\beta\omega/2} a^\dagger \tilde{a}^\dagger) |0 \otimes \tilde{0}\rangle. \quad (120)$$

We then want to make a suggestive (in terms of Rindler space and stuff) definition

$$\cosh \theta = \frac{1}{\sqrt{1 - e^{-\beta\omega}}}, \quad \sinh \theta = \frac{1}{\sqrt{e^{\beta\omega} - 1}}, \quad (121)$$

so that

$$\tanh \theta = e^{-\omega\beta/2}, \quad (122)$$

allowing us to write

$$|TFD\rangle = \frac{1}{\cosh \theta} \exp(\tanh \theta a^\dagger \tilde{a}^\dagger) |0 \otimes \tilde{0}\rangle. \quad (123)$$

Now some algebra lets us re-write this as

$$|TFD\rangle = \exp(\theta(a^\dagger \tilde{a}^\dagger - a \tilde{a})) |0 \otimes \tilde{0}\rangle, \quad (124)$$

from which we see that the TFD state is a bath of particles and antiparticles<sup>7</sup>. Note that in contrast to the imaginary time formalism, we can easily generalize to the non-equilibrium case simply by letting  $\theta$  depend on time.

<sup>7</sup>Showing this last step actually turned out to be kind of a pain in the ass! One first takes the logarithm of the prefactor and then exponentiates it, adds in the  $a\tilde{a}$  term with the aid of the BCH formula, and then does some algebra on the various numbers in the exponential. At the end one uses the identity

$$\cosh^{-1}(x) = \ln(x + \sqrt{(x+1)(x-1)}), \quad (125)$$

applied to  $x = (1 - e^{-\beta\omega})^{-1/2}$  (and so the LHS is equal to  $\theta$ ).



Thus let us define the operator  $U_\theta$  by

$$U_\theta = e^{\theta(a^\dagger \tilde{a}^\dagger - a \tilde{a})}, \quad (126)$$

so that  $U_\theta$  lets us map between the doubled Fock basis and the thermofield double. We see that the operators

$$a_\theta = U_\theta a U_\theta^{-1}, \quad \tilde{a}_\theta = U_\theta \tilde{a} U_\theta^{-1} \quad (127)$$

both annihilate  $|TFD\rangle$ . In terms of the original operators, some annoying algebra gives the Bogoliubov-esque representation

$$a_\theta = a \cosh(\theta) - \tilde{a}^\dagger \sinh(\theta), \quad (128)$$

and likewise for  $\tilde{a}_\theta$ .

One of the points of this whole thing is that in the thermodynamic limit (or in a finite system with infinitely many degrees of freedom allowed by e.g. free boundary conditions), different values of  $\theta$  (i.e. different temperatures) give rise to different operator algebras (different representations of the CCR) which are unitarily *inequivalent*, so that in some sense temperature is really fundamentally just a parameter that describes the way in which we represent the CCR. One can see this by taking the inner product of TFD states at different temperatures. Now simple algebra shows that

$$a^m (a^\dagger)^n |0\rangle = \frac{n!}{(n-m)!} (a^\dagger)^{n-m} |0\rangle. \quad (129)$$

When we take the inner product of this with  $\langle 0|$ , we then get  $\langle 0|a^m (a^\dagger)^n|0\rangle = \delta_{n,m} n!$ . Therefore when we expand the exponentials in the inner product, we have

$$\langle TFD_\theta | TFD_{\theta'} \rangle = \langle 0 \otimes \tilde{0} | \prod_k \frac{1}{\cosh \theta_k \cosh \theta'_k} \sum_{n,m} \frac{1}{n!m!} (a_k \tilde{a}_k)^n (a_k^\dagger \tilde{a}_k^\dagger)^m \tanh \theta_k \tanh \theta'_k |0 \otimes \tilde{0}\rangle, \quad (130)$$

which using the previous equation is

$$\begin{aligned} \langle TFD_\theta | TFD_{\theta'} \rangle &= \prod_k \frac{1}{\cosh \theta_k \cosh \theta'_k} \sum_n (\tanh \theta_k \tanh \theta'_k)^n \\ &= \prod_k \frac{1}{\cosh \theta_k \cosh \theta'_k (1 - \tanh \theta_k \tanh \theta'_k)} \\ &= \exp \left( -V \int_k \ln [\cosh \theta_k \cosh \theta'_k - \sinh \theta_k \sinh \theta'_k] \right) \end{aligned} \quad (131)$$

Now since the argument of the logarithm is greater than 1 unless  $\theta_k = \theta'_k$ , we get  $e^{-V\#} \rightarrow 0$  in the TDL unless  $\theta_k = \theta'_k$ , i.e. unless the two TFDs are at the same temperature. Hence

$$\langle TFD_\theta | TFD_{\theta'} \rangle = \delta_{\theta, \theta'}. \quad (132)$$

This can also be checked by directly writing down the TFD states as a sum over Boltzmann weights, with the orthogonality ultimately coming from the fact that the expectation value of

the energy is a monotonically increasing function of temperature (the maximum value of the overlap above occurs when  $\theta = \theta'$  as can be shown by differentiating the overlap wrt  $\beta$ ; in the TDL when infinitely many terms contribute to the sum the normalization makes us get zero unless  $\beta = \beta'$ ). Loosely speaking then the statement about the inequivalence of the operator algebras is that the operator algebras are built out of  $a_\theta$  and  $a_\theta^\dagger$  operators constructed from the specific states  $|TFD_\theta\rangle$ ; since these states are orthogonal in the TFD then the operator algebras they generate cannot have any "overlap", and are hence inequivalent. (note to self: come back and phrase this better)

We know that at finite temperature, Lorentz symmetry gets broken down to rotations + translations by the introduction of an energy scale. The boost symmetries are responsible for an  $SU(1,1)$  symmetry, since space and time have a relative minus sign in the metric. So we should expect to see the breaking of an  $SU(1,1)$  symmetry somewhere in this formalism.

This becomes most apparent if we define the thermal doublet (suppressing the momentum dependence from now)

$$\Psi_\theta = (a_\theta, \tilde{a}_\theta^\dagger)^T. \quad (133)$$

We define the doublet in this way since it is the object that transforms under changes in temperature by the Bogoliubov transformation identified above:

$$\Psi_\theta = B_\theta \Psi_0 \equiv \begin{pmatrix} \cosh \theta & -\sinh \theta \\ -\sinh \theta & \cosh \theta \end{pmatrix} \Psi_0. \quad (134)$$

One can quickly check that  $B_\theta \in SU(1,1)$ , i.e.  $B_\theta$  preserves the matrix  $Z$ . Note that when we put back in the momentum dependence, we actually have  $B_{\{\theta_k\}} \in \bigoplus_k SU(1,1)_k$ , with one copy of  $SU(1,1)$  for each mode. Thus the unitarity of this transformation in the thermodynamic limit fails, since as we saw earlier the different  $|TFD\rangle_\theta$  are not unitarily equivalent in the thermodynamic limit (this is the same as the statement that the charge operator  $Q = \int \star J$  in theories with a spontaneously broken continuous symmetry is not strictly speaking unitary since it has infinite norm).

Let us now rewrite the Hamiltonian  $\mathcal{H}$  in a more suggestive form. Since  $\mathcal{H} = H \otimes \mathbf{1} - \mathbf{1} \otimes H$ , we have, in terms of the original  $\theta = 0$  operators (which act on the original Fock space)

$$\mathcal{H} = \omega(a^\dagger a - \tilde{a}^\dagger \tilde{a}), \quad (135)$$

which we can write as

$$\mathcal{H} = \omega(\Psi_0^\dagger Z \Psi_0 + 1), \quad (136)$$

where  $Z$  as before is the third Pauli matrix. Since  $B_\theta \in SU(1,1)$ ,  $\mathcal{H}$  is actually independent of  $\theta$ , and so we might as well write

$$\mathcal{H} = \omega(\Psi_\theta^\dagger Z \Psi_\theta + 1). \quad (137)$$

This means that the Hamiltonian possesses the full  $SU(1,1)$  boost symmetry ( $\mathcal{H}$  annihilates  $|TFD\rangle_\theta$  for all  $\theta$ ). However, as we have just seen, the ground states of  $\mathcal{H}$  (the  $|TFD\rangle_\theta$  states) are *not* invariant under  $SU(1,1)$ : they are labelled by a particular  $\theta$  and permuted by the  $SU(1,1)$  action. Thus we have scenario like SSB, where the Hamiltonian is symmetric but the actual states that are chosen are not. Also like in SSB, in the thermodynamic limit,

distinct ground states are unitarily inequivalent because the operators which relate them are not normalizable.

Now for some more algebraic / informationy comments. As mentioned above, the operators in  $A$  commute with those in  $\tilde{A}$ , and vice versa. In fact, if  $A$  is a factor (i.e. has trivial center, which we can assume wolog after possibly doing a direct sum decomposition of an algebra with non-zero center by projectors onto central elements), we have

$$A' = \tilde{A}, \quad (138)$$

where  $A'$  is the commutant. We know that any von Neumann algebra is equal to its double-commutant, which we see here is reflected by the involutive nature of the tilde operation (which is true but which we haven't yet mentioned):

$$A'' = A \implies \tilde{\tilde{A}} = A. \quad (139)$$

One may think that since the Hamiltonian does not couple the  $\mathcal{H}$  and  $\tilde{\mathcal{H}}$  degrees of freedom, the two systems would be trivially decoupled. Of course this is not true since  $|TFD\rangle$  has a huge amount of entanglement between the  $A$  and  $\tilde{A}$  subsystems, and so even though the two systems do not talk to one another in the action we generically have correlations between the two subsystems:

$$\langle TFD | \mathcal{O} \otimes \tilde{\mathcal{O}} | TFD \rangle \neq 0. \quad (140)$$

In fact, the thermofield double is cyclic and separating for the algebras  $A$  and  $\tilde{A}$  (since they are each other's commutants, the fact that  $|TFD\rangle$  is cyclic and separating for one implies that it is also cyclic and separating for the other<sup>8</sup>). The cyclicity means that any state vector in  $\mathcal{H} \otimes \tilde{\mathcal{H}}$  can be constructed by acting on  $|TFD\rangle$  with an operator of either the form  $\mathcal{O} \otimes \mathbf{1}$  or of the form  $\mathbf{1} \otimes \tilde{\mathcal{O}}$ , which is made possible precisely because of the huge amount of entanglement between the  $A$  and  $\tilde{A}$  subsystems. The fact that states and operators can be in bijection like this in a finite system is allowed since

$$\dim \text{End}(\mathcal{H}) = \dim(\mathcal{H})^2 = \dim(\mathcal{H} \otimes \tilde{\mathcal{H}}), \quad (141)$$

as  $\dim(\tilde{\mathcal{H}}) = \dim(\mathcal{H})$  by construction. Note that when we say any state vector in  $\mathcal{H} \otimes \tilde{\mathcal{H}}$  can be created by acting on  $|TFD\rangle$  with an operator in either  $\text{End}(\mathcal{H})$  or  $\text{End}(\tilde{\mathcal{H}})$ , we are working with a *fixed* representation of the CCRs. As we saw earlier, we do have operators that take us between different CCRs (which change the temperature of the thermal state), but the image of this operator acting on  $|TFD\rangle$  is not included in  $\mathcal{H} \otimes \tilde{\mathcal{H}}$ , since the Hilbert space  $\mathcal{H} \otimes \tilde{\mathcal{H}}$  is the Hilbert space for a fixed representation of the CCRs. This is like considering the Hilbert space associated to a particular broken-symmetry sector in the case of SSB. The

---

<sup>8</sup>Proof: suppose  $\tilde{\mathcal{O}} \in \text{End}(\tilde{\mathcal{H}})$ . Then  $\tilde{\mathcal{O}}$  commutes with all  $\mathcal{O} \in \text{End}(\mathcal{H})$  since operators acting only on  $\mathcal{H}$  commute with those acting only on  $\tilde{\mathcal{H}}$ . Suppose  $\tilde{\mathcal{O}}|TFD\rangle = 0$ . Then  $\tilde{\mathcal{O}}\mathcal{O}|TFD\rangle = 0$  for any  $\mathcal{O} \in \text{End}(\mathcal{H})$ . But  $|TFD\rangle$  is cyclic for  $\text{End}(\mathcal{H})$  and so this means that  $\tilde{\mathcal{O}}$  annihilates all state vectors. Thus  $\tilde{\mathcal{O}} = 0$  and  $|TFD\rangle$  is separating for  $\text{End}(\tilde{\mathcal{H}})$ .

full Hilbert space, which includes all different symmetry-broken sectors, would in our case be something like  $\bigoplus_{\theta}(\mathcal{H} \otimes \tilde{\mathcal{H}})_{\theta}$ .

Note that the full time evolution operator for the system can be written suggestively as

$$\Delta_{TFD}^{is} = \exp(i(H \otimes \mathbf{1} - \mathbf{1} \otimes H)s), \quad (142)$$

where  $s$  is some real parameter. Connecting to Tomita-Takesaki theory, we see that the role of modular conjugation is played by the tilde involution which exchanges the  $A$  and  $\tilde{A}$  algebras:

$$\text{End}(\tilde{\mathcal{H}}) \ni J^{-1} \mathcal{O} J = \tilde{\mathcal{O}} \quad (143)$$

while the modular operator is

$$\Delta_{TFD} = e^{\mathcal{H}}. \quad (144)$$

This matches with the fact that for a Hilbert space split as  $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ , the modular operator  $\Delta_{\Psi}$  for a state  $\Psi$  which is cyclic and separating for  $\text{End}(\mathcal{H}_1)$  (and thus  $\text{End}(\mathcal{H}_2)$ ) is

$$\Delta_{\Psi} = \rho_1 \otimes \rho_2^{-1}, \quad (145)$$

where  $\rho_i$  are the reduced density matrices.



## Exercises on the Shannon entropy

---

Today we will do a few things relating to the Shannon entropy: proving weak and strong subadditivity is derived for the Shannon entropy.



We will first prove (weak) subadditivity (this is strictly speaking redundant as it follows from strong subadditivity which we will prove next, but we will prove it in a slightly different way). Recall the definition of the relative Shannon entropy:

$$H(p(x)||q(x)) = \sum_x p(x) \ln \frac{p(x)}{q(x)}, \quad (146)$$

which compares two different probability distributions on the same variables  $x$ . For the case of two random variables  $X, Y$  with outcomes enumerate by  $x, y$ , we see that the relative entropy between the joint distribution  $p(x, y)$  and the product of the two marginals  $p(x) = \sum_y p(x, y), p(y) = \sum_x p(x, y)$  is

$$I(X : Y) \equiv H(p(x, y)||p(x)p(y)) = -H(X, Y) + H(X) + H(Y), \quad (147)$$

which is also known as the mutual information. Weak subadditivity is the statement that  $H(X, Y) \leq H(X) + H(Y)$ , which from the above is true since  $I(X : Y) \geq 0$ . This follows from using  $\ln(x) \leq x - 1$  in the manner used to prove strong subadditivity below. The inequality is saturated only when  $p(x, y) = p(x)p(y)$ , i.e. when  $X$  and  $Y$  are independent random variables. This is of course totally in accordance with classical intuition.

Now for strong subadditivity, which is the statement that (using the notation of N&C)

$$H(X, Y, Z) + H(Y) \leq H(X, Y) + H(Y, Z). \quad (148)$$

This is proved by using  $\ln(x) \leq x - 1$ , with the inequality saturated only for  $x = 1$ . We use this on a combination of probabilities that produce LHS of the above inequality:

$$\begin{aligned} \sum_{x,y,z} p(x, y, z) \ln \left( \frac{p(x, y)p(y, z)}{p(x, y, z)p(y)} \right) &\leq \sum_{x,y,z} p(x, y, z) \left( \frac{p(x, y)p(y, z)}{p(x, y, z)p(y)} - 1 \right) \\ &= \sum_{x,y,z} \frac{p(x, y)p(y, z)}{p(y)} - 1 \\ &= \sum_y p(y) - 1 = 0. \end{aligned} \quad (149)$$

Since the LHS above is negative, strong subadditivity follows. Weak subadditivity then follows from this upon taking  $Y$  to be trivial.

We furthermore claim that the inequality is saturated iff  $Z \rightarrow Y \rightarrow X$  is a Markov chain. This is very reasonable: in this case  $H(X, Y) + H(Y, Z)$  contains all the information of all three variables (viz.  $H(X, Y, Z)$ ), but counts  $Y$  twice. Indeed, we see that the equality holds iff for all  $x, y, z$ ,

$$p(x, y)p(y, z) = p(x, y, z)p(y). \quad (150)$$

But then since  $p(xy) = p(x)p(y|x)$ , we can re-write the above after canceling a few factors as

$$p(x|y) = p(x|y, z) \quad (151)$$

The condition for this to hold for all  $x, y, z$  is indeed precisely the same statement as the one that  $Z \rightarrow Y \rightarrow X$  is a Markov chain.

We will now do two exercises from McGreevy's QI class exploring the properties of the conditional entropy and mutual information for an interesting but simple example. Recall that the conditional entropy is defined via (note that  $H(X||Y)$  and  $H(X|Y)$  mean different things — don't blame me)

$$H(X|Y) \equiv H(X, Y) - H(Y). \quad (152)$$

We will be considering a system with two variables  $x, y$  defined by the joint distribution

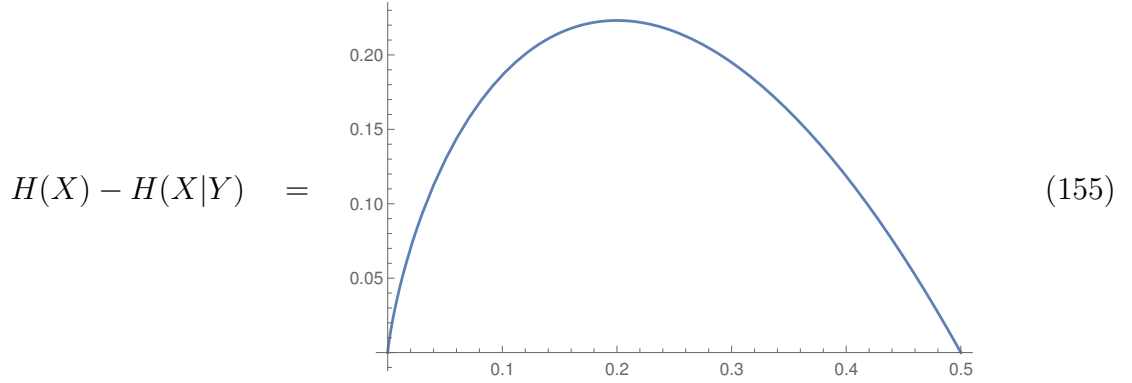
$$p(x, y) = \begin{pmatrix} 0 & a \\ b & b \end{pmatrix}_{yx}, \quad a \equiv 1 - 2b. \quad (153)$$

Here  $y = +, -$  is the row index and  $x$  is the column index, so that e.g.  $p(+, -) = a, p(-, -) = b$ , etc. Since the probabilities are all positive, we must have  $b \in [0, 1/2]$ .

We now go ahead and calculate all the entropic quantities of interest:

$$\begin{aligned}
 H(X, Y) &= -(1 - 2b) \ln(1 - 2b) - 2b \ln b \\
 H(X) &= -b \ln b - (1 - b) \ln(1 - b) \\
 H(Y) &= -(1 - 2b) \ln(1 - 2b) - 2b \ln(2b) \\
 H(X|Y) &= 2b \ln 2 \\
 H(Y|X) &= -(1 - 2b) \ln(1 - 2b) - b \ln b + (1 - b) \ln(1 - b).
 \end{aligned} \tag{154}$$

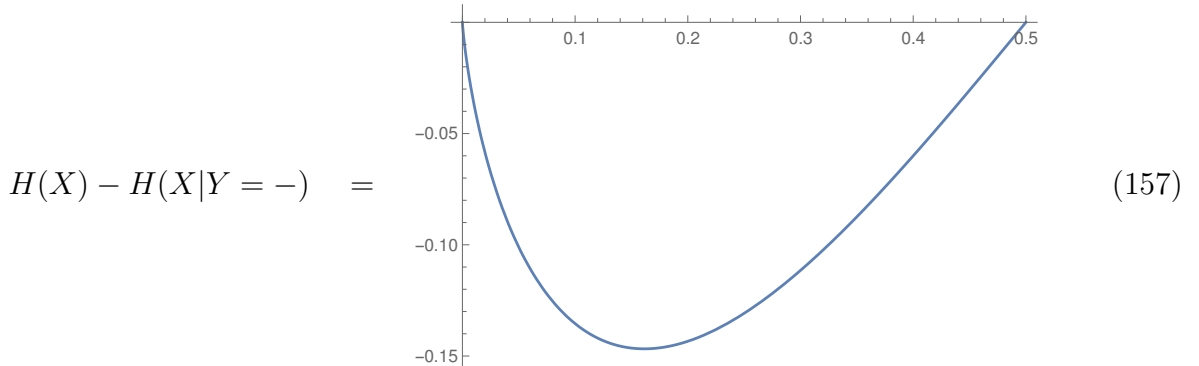
We can confirm that  $H(X) \geq H(X|Y)$  by plotting their difference as a function of  $b$  ( $H(Y) - H(Y|X)$  is exactly the same):



The positivity of this makes sense: learning about  $Y$  can only decrease your ignorance about  $X$ . However, this is true only on average: learning about *a particular value* of  $Y$  can actually *increase* our ignorance about  $X$ . This is true in this example: if we know that  $Y = -$ , then we find

$$H(X|Y = -) = -2b \ln b \implies H(X) - H(X|Y = -) = -b \ln b - (1 - b) \ln(1 - b) + 2b \ln b. \tag{156}$$

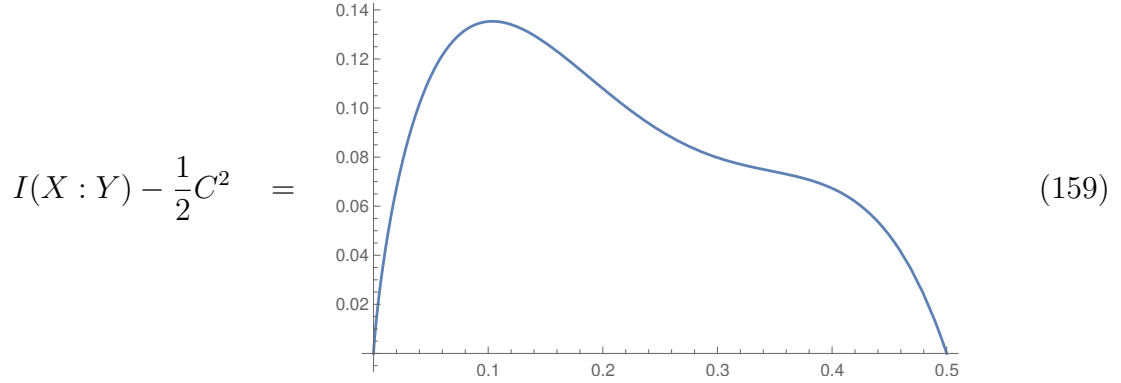
This is actually negative for all allowed values of  $b$ : we can prove this with concavity or by plotting:



We now compute the mutual information and the connected two-point function  $C = \langle xy \rangle_c$ . Classically  $I(X : Y) \geq \frac{1}{2} C^2$ , and our goal is to check this inequality in the present setting. This is straightforward enough: we find

$$C = 8b^2 - 4b, \quad I(X : Y) = (2b - 1) \ln(1 - b) - b \ln(2b) - b \ln(2(1 - b)), \tag{158}$$

We can then check that the inequality is satisfied by making a plot:



## Discrete Fourier transforms and generalized Pauli operators, with applications to scrambling and teleportation

---

Today we will explain properties of the  $\mathbb{Z}_N$  Pauli operators, show that they can be used to construct a nice basis on  $\text{End}(\mathbb{C}^d)$ , and give applications showing how they can be used to “scramble” operators and teleport qudits.



We will be discussing discrete Fourier transforms in what follows, so let us first fix some definitions. We define the Fourier transformation on  $\mathbb{C}^d$  by multiplying vectors by the following Hadamard-esque matrix:

$$\mathcal{F} : \mathbb{C}^d \rightarrow \mathbb{C}^d, \quad v \mapsto \mathcal{F}v, \quad \mathcal{F} = \sum_{ab} \zeta_d^{ab} |a\rangle\langle b|. \quad (160)$$

We can check that this satisfies the usual properties of the Fourier transform. For example,

$$\mathcal{F}^\dagger \mathcal{F} = \mathbf{1}, \quad \mathcal{F}^2 = [\mathcal{F}^\dagger]^2 = \sum_a |a\rangle\langle -a|, \quad (161)$$

with the last implying that  $\mathcal{F}^4 = \mathbf{1}$  but  $\mathcal{F}^2 = -\mathbf{1}$ , just like the usual Fourier transform on  $L^2(\mathbb{R}^d)$ . The Fourier transform of a vector  $|v\rangle$  is just  $\mathcal{F}|v\rangle$ , while that of an operator is  $\mathcal{F}(\mathcal{O}) = \mathcal{F}^\dagger \mathcal{O} \mathcal{F}$ , so that  $\mathcal{F}[\mathcal{O}\mathcal{O}'] = \mathcal{F}(\mathcal{O})\mathcal{F}(\mathcal{O}')$ .

We will define the matrix  $Z$  as the generalized Pauli matrix which returns a  $U(1)$  phase depending on which basis state it measures, i.e.  $Z_{ab} = \delta_{ab}\zeta_d^a$ . Then we see that  $\mathcal{F}(Z)$  is the generalized Pauli  $X$ :

$$\mathcal{F}(Z) = \sum_b |a\rangle\langle b| \zeta_d^{-ab+cb+b} = \sum_a |a+1\rangle\langle a| \equiv X. \quad (162)$$

Likewise,

$$\mathcal{F}(X) = Z^\dagger, \quad (163)$$

so that  $\mathcal{F}^2$  acts as  $\mathbb{C}$  conjugation on  $Z$  while  $\mathcal{F}^4$  acts as  $\mathbf{1}$ , as required. Similarly,  $\mathcal{F}^2(X) = X^\dagger$ . For a general operator  $\mathcal{O}$ , one checks that

$$\mathcal{F}^2(\mathcal{O}) = \sum_{ab} \mathcal{O}_{ab} | -a\rangle\langle -b|, \quad (164)$$

where  $| -a\rangle = |d-a\rangle$ .

$Z$  and  $X$  commute with one another as

$$ZX = \zeta_d XZ. \quad (165)$$

Complex conjugating this, we also have

$$Z^\dagger X = \zeta_d^{-1} X Z^\dagger, \quad ZX^\dagger = \zeta_d^{-1} X^\dagger Z \quad (166)$$

Note that this means charge-neutral  $\otimes$ s of  $Z$  operators ( $Z$  has charge 1,  $Z^\dagger$  has charge  $-1$ ) can be simultaneously diagonalized with products of  $X$  operators, e.g.

$$[Z \otimes Z^\dagger, X \otimes X] = 0. \quad (167)$$

All of this can essentially be summarized by thinking of  $Z$  as  $e^{2\pi i x/n}$  with  $x$  the position operator,<sup>9</sup> and  $X$  as  $e^{ip}$  with  $p$  the momentum operator.<sup>10</sup>

Let us now use these operators to define an orthogonal basis  $U_a$  on  $\text{End}(\mathbb{C}^d)$ , where orthogonality is defined wrt the Hilbert-Schmidt inner product:  $\text{Tr}[U_a^\dagger U_b] = d\delta_{a,b}$ . Our claim is that a set of  $d^2$  generators is given by

$$U_a = U_{mn} = X^m Z^n, \quad (168)$$

where  $a = (m, n) \in \mathbb{Z}_d \times \mathbb{Z}_d$  is a composite index.<sup>11</sup> Indeed, these matrices are all orthogonal under the HS inner product:

$$\langle U_a, U_b \rangle = \text{Tr}[(X^m Z^n)^\dagger X^k Z^l] = \sum_{ij} \zeta_d^{i(l-n)} \langle i|j\rangle \langle j+k-m|i\rangle = d\delta_{l,n}\delta_{k,m} = d\delta_{a,b}. \quad (169)$$

---

<sup>9</sup>Indeed, by taking the log,  $(2\pi i/d)^{-1} \ln Z = \sum_a a|a\rangle\langle a|$ .

<sup>10</sup>Indeed, this is the correct "translation operator" which "translates" by 1 along the  $\mathbb{Z}_d$  circle.

<sup>11</sup>Note that  $U_{mn}$  is not a matrix element! From now on matrix elements will always be denoted with bra-ket notation. Also note that now  $a$  is a composite index, whereas before it ran through elements of  $\mathbb{Z}_d$  — this is because I wrote the previous part of the diary entry at a different time than the present part. Apologies!



Since there are  $d^2 = \dim \text{End}(\mathcal{H}_A)$  of them and they are all orthogonal, they indeed constitute a basis.<sup>12</sup> Explicitly, we can write each of the standard basis vectors in  $\text{End}(\mathbb{C}^d)$  as

$$|a\rangle\langle b| = \frac{1}{d} \sum_n \zeta_d^{-bn} X^{a-b} Z^n. \quad (170)$$

Using the relations derived above, we see that these matrices commute as

$$U_{mn} U_{kl} = \zeta_d^{nk} U_{m+k, n+l} = \zeta_d^{nk-ml} U_{kl} U_{mn}. \quad (171)$$

Another useful property (which is just a special case of orthogonality) is that all but  $U_{00}$  are traceless:

$$\text{Tr}[U_{mn}] = d\delta_{m,0}\delta_{n,0}. \quad (172)$$

The moral reason why matrices of the form  $X^m Z^n$  constitute a basis is because  $\text{End}(\mathcal{H}_A) \cong \mathcal{H}_A^* \otimes \mathcal{H}_A$ , where the dual on the first tensor factor can be interpreted as the Fourier transform duality interchanging the  $X$ s and  $Z$ s: thus the  $X^m$  part is the basis for the  $\mathcal{H}_A^*$  factor and the  $Z^n$  part is the basis for the  $\mathcal{H}_A$  factor, and when tensored together they provide a basis for  $\text{End}(\mathcal{H}_A)$ .

### *Application to scrambling*

We will now show<sup>13</sup> that for any operator  $\mathcal{O} \in \text{End}(\mathcal{H}_A)$  with  $\mathcal{H}_A \cong \mathbb{C}^d$ , we can always find probabilities  $p_a$  and unitaries  $U_a$  such that there is an associated quantum channel  $\mathcal{E}$  which completely scrambles  $\mathcal{O}$ :

$$\mathcal{E}(\mathcal{O}) \equiv \sum_a p_a U_a \mathcal{O} U_a^\dagger = \frac{\text{Tr}[\mathcal{O}]}{d} \mathbf{1}_A, \quad (173)$$

where the sum runs over the basis elements for  $\text{End}(\mathcal{H}_A)$  defined above.

First we decompose  $\mathcal{O}$  in the  $U_a$  basis:

$$\mathcal{O} = \sum_{m,n} \alpha_{mn} U_{mn}, \quad (174)$$

where  $\alpha_{00} = \text{Tr}[\mathcal{O}]/d$ . The image of the quantum channel  $\mathcal{E}$  is then

$$\mathcal{E}(\mathcal{O}) = \sum_{klmn} p_{mn} \alpha_{kl} U_{mn} U_{kl} U_{mn}^\dagger = \sum_{klmn} p_{mn} \alpha_{kl} \zeta_d^{nk-ml} U_{kl}. \quad (175)$$

But now we see that we simply have to set  $p_{mn} = 1/d^2$  independent of  $m, n$ : the sums over  $m, n$  will then provide delta functions on  $k, l$ , and from  $\alpha_{00} = \text{Tr}[\mathcal{O}]/d$  we see that  $\mathcal{E}$  indeed scrambles  $\mathcal{O}$  in the way claimed.

---

<sup>12</sup>In the special case that  $d = 2^s$ , we can find a slightly nicer basis by taking all possible  $s$ -fold tensor powers of Pauli matrices; in this case not only are all the basis elements unitary, but they are also Hermitian and hence all square to 1. Checking orthogonality is easy.

<sup>13</sup>This comes from a nice exercise that John McGreevy assigned to his QI class.

Note that this result is one way to prove that the uniform state  $\rho = \mathbf{1}/d$  has the maximum possible vN entropy on  $\mathcal{H}_A$ : we use the concavity of the vN entropy to write, for any density matrix  $\rho$ ,

$$S(\mathcal{E}(\rho)) = S\left(\sum_a p_a U_a \rho U_a^\dagger\right) \geq \sum_a p_a S(U_a \rho U_a^\dagger) = \sum_a \frac{1}{d^2} S(\rho) = S(\rho), \quad (176)$$

so that the channel  $\mathcal{E}$  always increases  $S$ . On the other hand, the LHS is, since  $\rho$  is a density matrix,  $S(\mathcal{E}(\rho)) = S(\mathbf{1}/d)$ . Hence  $\mathbf{1}/d$  has the maximum possible vN entropy.

Also note that while in order to scramble a generic operator  $\mathcal{O}$  with this protocol we needed  $d^2$  matrices, if  $\mathcal{O}$  happens to be Hermitian we can do better. Indeed if  $\mathcal{O}$  is Hermitian, we can find a unitary  $U_{\mathcal{O}}$  which diagonalizes  $\mathcal{O}$ . Then we can define the quantum channel

$$\mathcal{E}(\mathcal{O}) = \sum_{n \in \mathbb{Z}_d} \frac{1}{d} (X^n U_{\mathcal{O}}) \mathcal{O} (X^n U_{\mathcal{O}})^\dagger. \quad (177)$$

The conjugation by  $U_{\mathcal{O}}$  diagonalizes  $\mathcal{O}$  and the conjugation by  $X^n$  cyclically permutes the entries of the resulting diagonal matrix. By summing over all cyclic permutations, each entry in  $\mathcal{E}(\mathcal{O})$  thus becomes  $\text{Tr}[\mathcal{O}]/d$ , and so in this case  $\mathcal{O}$  can be scrambled with only  $d$  matrices.

### *Application to encryption*

We can use the result of the previous subsection to give an encryption protocol for the communication of a quantum state. We consider the situation where two parties  $A, B$  want to encrypt and share a  $d$ -dimensional density matrix  $\rho$  through a quantum channel  $\mathcal{E}$ , with the encryption being done in a way such that an eavesdropper  $E$  is unable to gain any information about  $\rho$ . We assume that  $A$  and  $B$  share identical collections of random numbers  $a \in \mathbb{Z}_N$ , drawn from some distribution  $p_a$ . The goal is to find the smallest  $N$  (and an associated distribution  $p_a$ ) such that encryption is possible.

The method for scrambling a generic matrix demonstrated above can immediately be applied to show that perfect encryption is possible if both parties have access to identical collections of random numbers drawn from the uniform distribution on  $\mathbb{Z}_{d^2}$ . Encrypted communication happens by  $A$  selecting from her list of random numbers the first number  $a \in \mathbb{Z}_{d^2}$  and sending  $B$  the matrix  $U_a \rho U_a^\dagger$ , where  $U_a$  is the  $a$ th element of a unitary orthogonal basis of  $\text{End}(\mathbb{C}^d)$ , given as in the previous diary entry by  $X^m Z^n$  for  $m = (a \bmod d)$ ,  $n = \lfloor a/d \rfloor$ . Since  $E$  does not know the value of  $a$ ,  $E$  only has access to the state

$$\mathcal{E}(\rho) = \frac{1}{d^2} \sum_a U_a \rho U_a^\dagger. \quad (178)$$

However, we showed above that  $\mathcal{E}(\rho) = \mathbf{1} \text{Tr}[\rho]/d = \mathbf{1}/d$ . Therefore  $\mathcal{E}(\rho)$  is independent of  $\rho$ , and  $E$  cannot possibly learn anything about  $\rho$ . When  $B$  receives the state from  $A$ , he need only act on it by conjugation with  $U_a^\dagger$  to recover  $\rho$ .

This means that e.g. shared access to a repository of random length  $2n$  bit strings is always sufficient for encrypted communication of a quantum  $n$ -qbit state: basically because

$\dim \text{End}(\mathbb{C}^d) = d^2$ , so that turning an arbitrary operator in  $\text{End}(\mathbb{C}^d)$  into a particular one (one proportional to  $\mathbf{1}$ ) can be done by choosing  $d^2$  parameters.

The next question to ask is whether encrypted communication can be achieved with shared access to random numbers drawn from a distribution on  $\mathbb{Z}_N$ , with generic  $N$  (obviously  $N > d^2$  will always work, but we will work with generic  $N$  for now). In such a circumstance,  $A$  and  $B$  would be able to choose a set of  $N$  unitaries  $U_i$  and a probability distribution  $p_i$  such that the associated quantum channel is identical to  $\mathcal{E}(\rho)$ , viz. the channel which sends any density matrix to the maximally mixed state  $\mathbf{1}/d$ . In symbols, this means that we have

$$\mathcal{E}(\rho) = \sum_{a \in \mathbb{Z}_N} p_a U_a \rho U_a^\dagger. \quad (179)$$

We will want to use the same index set  $a$  to label both the  $U$  and  $\mathbf{U}$  operators. Therefore in both representations of the quantum channel we will let  $a$  run over values in  $\mathbb{Z}_{\max(d^2, N)}$ , with the understanding that if  $N < d^2$  then  $U_{a > N} = 0$ , while if  $N > d^2$  then  $U_{a > d^2} = 0$ . We will prove in another diary entry that since the Kraus operators  $U_a/d$  and  $\sqrt{p_a}U_a$  construct the same quantum channel, they must then be related through a unitary matrix  $\mathcal{V}$  via

$$U_a = \frac{1}{d\sqrt{p_a}} \sum_b [\mathcal{V}]_{ab} U_b, \quad \mathcal{V} \in \text{End}(\mathbb{C}^{\max(d^2, N)}). \quad (180)$$

Now consider  $p_a = p_a \cdot 1 = \frac{p_a}{d} \text{Tr}[U_a U_a^\dagger]$ , where  $a \leq N$  so that the RHS is non-zero. Using the relation between the  $U_a$  and the  $\mathbf{U}_a$ , we can use the orthogonality of the  $U_a$ s to write

$$p_a \text{Tr}[U_a U_a^\dagger] = \frac{1}{d^2} \sum_{bc} [\mathcal{V}]_{ab} \text{Tr}[U_b U_c^\dagger] [\mathcal{V}^*]_{ca} \leq \frac{1}{d^2} \sum_{bc} [\mathcal{V}]_{ab} \text{Tr}[\mathbf{1}_d] [\mathcal{V}^*]_{ba} = \frac{1}{d}, \quad (181)$$

where the  $\leq$  appeared because if  $N > d^2$ , some of the  $U_a$  will be zero (the inequality is saturated if  $N \leq d^2$ ). Therefore

$$p_a \leq \frac{1}{d^2}, \quad (182)$$

with equality if  $N \leq d^2$ .

Now we see that while choosing  $N \geq d^2$  unitaries is (obviously) sufficient for encrypted communication, no choice of  $N < d^2$  unitaries can work, since then  $\sum_a p_a < 1$  which contradicts the assumption that the  $p_a$ s are a probability distribution on  $\mathbb{Z}_N$ . Evidently encryption with the uniform distribution on  $\mathbb{Z}_{d^2}$  using the  $U_a$ s is the best we can do.<sup>14</sup>

### *Application to teleportation*

We can also use these operators to conveniently discuss teleportation for qdits. Teleportation is the process whereby party  $A$  “sends” a quantum state to party  $B$ , and can be accomplished

---

<sup>14</sup>Note that above we showed that if  $\mathcal{O} \in \text{End}(\mathbb{C}^d)$  is Hermitian, there exist a set of  $d$  matrices which “scramble”  $\mathcal{O}$ . Since  $\rho$  is Hermitian, isn't this in contradiction with the above proof? The answer is no, since the channel scrambling  $\mathcal{O}$  depended on  $\mathcal{O}$  through the unitary diagonalizing  $\mathcal{O}$ . For the present problem, we want a quantum channel that does encryption for arbitrary density matrices, i.e. we want the Kraus operators for  $\mathcal{E}$  to be independent of  $\rho$ .

provided that both  $A$  and  $B$  have access to some shared entanglement, as well as a classical communication channel.

First, we will need some notation. For any  $\mathcal{O} \in \text{End}(\mathcal{H}_A)$  (with  $\mathcal{H}_A \cong \mathbb{C}^d$  as before), we will denote the image of the isomorphism with  $\mathcal{H}_A^{\otimes 2}$  as the state

$$|\mathcal{O}\rangle = \sum_{ab} \mathcal{O}_{ab} |ab\rangle. \quad (183)$$

The Hilbert-Schmidt norm coming from tracing maps to the inner product of the associated states:

$$\langle \mathcal{O}, \mathcal{O}' \rangle = \text{Tr}[\mathcal{O}^\dagger \mathcal{O}'] = \langle \mathcal{O} | \mathcal{O}' \rangle. \quad (184)$$

Note that if  $\mathcal{O}$  is unitary the state  $|\mathcal{O}\rangle_{AB}$  is maximally entangled, since in this case the reduced density matrix is (as before, we are neglecting to write normalization factors)

$$\rho_A = \sum_{abcd} \text{Tr}_B [\mathcal{O}_{ab} \mathcal{O}_{cd}^* |ab\rangle \langle cd|] = \sum_{abc} \mathcal{O}_{ab} \mathcal{O}_{cb}^* |a\rangle \langle c| = \mathbf{1}_A. \quad (185)$$

The basis operators  $X^m Z^n$ , being unitary, give us a full  $d^2$ 's worth of maximally entangled states, which are

$$|X^m Z^n\rangle = \sum_a \zeta_d^{na} |a+m\rangle \otimes |a\rangle. \quad (186)$$

Since the  $X^m Z^n$  form a unitary orthogonal set of basis operators for  $\text{End}(\mathcal{H}_A)$ , the states  $|X^m Z^n\rangle$  form a maximally entangled set of orthogonal basis vectors for  $\mathcal{H}_A^{\otimes 2}$ . From the discussion above, we see that (yes, still not writing normalization factors)

$$|ab\rangle = \sum_n \zeta_d^{-bn} |X^{a-b} Z^n\rangle, \quad (187)$$

which makes sense from the Fourier transformation perspective discussed earlier.

Now we can see how to set up a teleportation protocol. Suppose for simplicity that the shared entanglement that  $A$  and  $B$  have access to is in the form of the state  $|\mathbf{1}\rangle_{AB}$  (it doesn't have to be  $\mathbf{1}$ ; we could choose any other  $|X^m Z^n\rangle$  to serve as the shared resource, but this just complicates notation). Suppose also that  $A$  possesses a quantum state  $|\psi\rangle_C$ , so that the full state of the system is

$$|\Psi\rangle_{CAB} = \sum_{ab} \psi_a |abb\rangle_{CAB}. \quad (188)$$

We then use the above result to write

$$|\Psi\rangle_{CAB} = \sum_{abn} \psi_a \zeta_d^{-bn} |X^{a-b} Z^n\rangle_{CA} \otimes |b\rangle_B. \quad (189)$$

Now suppose  $A$  does a projective measurement  $\mathcal{M}$  in the  $|X^m Z^n\rangle$  basis on the system  $\mathcal{H}_C \otimes \mathcal{H}_A$ , and obtains the state  $|X^k Z^l\rangle$ . The state  $|\psi_{\mathcal{M}}\rangle_B$  that  $B$  has after the measurement is

$$|\psi_{\mathcal{M}}\rangle_B = \sum_a \psi_a \zeta^{(k-a)l} |a-k\rangle_B = \sum_a \psi_a X^{-k} Z^{-l} |a\rangle_B = Z^{-l} X^{-k} |\psi\rangle_B. \quad (190)$$

Therefore if  $A$  sends the result of her measurement to  $B$  (so that  $B$  knows  $k, l$ ),  $B$  can simply apply  $X^k Z^l$  to his state and thereby obtain a "teleported copy" of  $|\psi\rangle$ .



## Unitary equivalence of Kraus operators

---

Today we will go over the proof that any two Kraus representations implementing a given quantum channel are necessarily related by a unitary matrix. This proof is in Preskill's notes (and probably many other places), but it took me a while to understand and I wanted to have a record here for posterity's sake.



First we will need an auxiliary result:

**Lemma 1.** Any two purifications  $|\Psi\rangle_{AB}, |\tilde{\Psi}\rangle_{AB}$  of a mixed state  $\rho_A$  are related by a unitary  $\mathbf{1}_A \otimes U_B$ , which acts nontrivially only on  $\mathcal{H}_B$ .

This makes sense because the only ambiguity that comes up when purifying is the map  $\mathcal{H}_A^* \hookrightarrow \mathcal{H}_B$ , which can be composed with unitary changes of basis on  $\mathcal{H}_B$  to yield different purifications without affecting the physics.

*Proof.* Formally, this follows by picking a fixed realization of  $\rho_A$  as a sum of pure states and using this to compare the two purifications via Schmidt decomposition. Indeed, since both purifications yield  $\rho_A$  when  $\mathcal{H}_B$  is traced out, their Schmidt decompositions must be of the form

$$|\tilde{\Psi}\rangle_{AB} = \sum_i \sqrt{\lambda_i} |i\rangle_A |i\rangle_B, \quad |\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |i\rangle_A |\tilde{i}\rangle_B, \quad (191)$$

for  $\{|i\rangle_B\}$  and  $\{|\tilde{i}\rangle_B\}$  two different orthonormal bases on  $\mathcal{H}_B$ . These two bases must be related by a unitary  $U_B$ , from which it follows that  $|\Psi\rangle_{AB} = (\mathbf{1}_A \otimes U_B)|\tilde{\Psi}\rangle_{AB}$  as claimed. Note that by padding either of the bases with zero vectors, we can easily extend the result to the case where the two purifications are accomplished with Hilbert spaces of different dimensions.

□

The proof of the unitary equivalence of Kraus operators is morally the same as the above proof for the unitary equivalence of purifications. In both cases, the problem is to figure out

the ambiguity in going along each arrow of the "purification sequence" (this is schematic; the exact meaning of e.g. the second arrow will be shown explicitly shortly)

$$\cdots \rightarrow \text{quantum channels} \rightarrow \text{density matrices} \rightarrow \text{state vectors}, \quad (192)$$

which is basically a specialization of the sequence (each arrow is the duality  $\mathcal{H} \rightarrow \mathcal{H}^*$ , assuming wolog that we purify by tensor-squaring each Hilbert space)

$$\cdots \rightarrow \text{superoperators} \rightarrow \text{operators} \rightarrow \text{vectors} \quad (193)$$

to the case where each entry has appropriate positivity properties (normalized wavefunction, unit trace positive, trace-preserving completely positive). Just as the ambiguity when purifying is a unitary operator acting on the auxiliary space, the ambiguity when determining Kraus operators is a unitary operator acting on the auxiliary space, where in this case the auxiliary space  $\mathcal{H}_E$  is usually thought of as an environment for the system in question. The environment is introduced to "purify" the sum over Kraus operators by writing their combined action as the action of a single unitary acting on the system  $\otimes \mathcal{H}_E$ , just as how the purification of density matrices is done to write the sum over operators in the spectral representation of  $\rho_A$  as a single operator acting on the system  $\otimes \mathcal{H}_E$  (with  $\mathcal{H}_E$  conventionally taken to be a copy of the original Hilbert space).

Let us first recall how to construct one set of Kraus operators for a given quantum channel  $\mathcal{E} : \text{End}(\mathcal{H}_A) \rightarrow \text{End}(\mathcal{H}_B)$ . The basic idea is that writing the action of  $\mathcal{E}$  in terms of a set of Kraus operators is completely analogous to writing a density matrix as an ensemble of pure states. Just as any density matrix can be decomposed (in many different ways) as  $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ , so too can any quantum channel be composed (in many different ways) as  $\mathcal{E}(\cdot) = \sum_i \mathcal{K}_i(\cdot) \mathcal{K}_i^\dagger$ .<sup>15</sup> In pictures, we should be thinking of

$$\begin{array}{c} A \\ | \\ \boxed{\rho} \\ | \\ A \end{array} = \sum_i p_i \begin{array}{c} | \\ \boxed{\psi} \\ | \\ \boxed{\psi} \\ | \end{array} \qquad \begin{array}{c} B \quad B^* \\ | \quad | \\ \boxed{\mathcal{E}} \\ | \quad | \\ A \quad A^* \end{array} = \sum_i \begin{array}{c} B \quad B^* \\ | \quad | \\ \boxed{\mathcal{K}} \quad \boxed{\mathcal{K}^\dagger} \\ | \quad | \\ A \quad A^* \end{array} \quad (194)$$

Here on the RHS we have written  $\mathcal{E}$  an operator which maps  $\mathcal{H}_A \otimes \mathcal{H}_A^*$  to  $\mathcal{H}_B \otimes \mathcal{H}_B^*$ ; in this

---

<sup>15</sup>The reason why these two equations don't look more similar is because we are accustomed to absorbing the  $p_i$ s into the definition of the  $\mathcal{K}_i$ s, and because of our notational bias in distinguishing between vectors and matrices (even though matrices are also vectors acting on larger Hilbert spaces).

notation the action of  $\mathcal{E}$  on  $\rho$  is

$$\mathcal{E}(\rho) = \begin{array}{c} \begin{array}{cc} B & B^* \\ \hline \boxed{\mathcal{E}} \\ \hline \end{array} \\ \begin{array}{cc} A & A^* \\ \diagup & \diagdown \\ \boxed{\rho} \end{array} \end{array} \quad (195)$$

Let's now see how this works more formally. For notational simplicity we will specialize to the case where  $\mathcal{E}$  maps  $\text{End}(\mathcal{H}_A)$  to itself;<sup>16</sup> the case where the Hilbert space on which density operators act is changed under  $\mathcal{E}$  can be analyzed in essentially the same way.

First of all, using the linearity of  $\mathcal{E}$  and a decomposition of  $\rho$  into an ensemble of pure states, we have

$$\mathcal{E}(\rho) = \sum_i p_i \mathcal{E}(|\psi_i\rangle_A \langle \psi_i|_A). \quad (196)$$

We will now dualize the  $|\psi_i\rangle_A$  vectors using a maximally entangled state  $|\Phi\rangle_{AB} = \sum_i |i\rangle_A |i'\rangle_B$ , where  $\{|i\rangle_A\}, \{|i'\rangle_B\}$  are some chosen orthonormal bases of  $\mathcal{H}_A, \mathcal{H}_B$  (with  $\mathcal{H}_B \cong \mathcal{H}_A$ , but with the notation as is because we want an easy way of distinguishing between the two tensor factors)

$$\mathcal{E}(\rho) = \sum_i p_i \langle \psi_i^* |_B (\mathcal{E} \otimes \mathbf{1}_B) (|\Phi\rangle_{AB} \langle \Phi|_{AB}) |\psi_i^*\rangle_B, \quad (197)$$

where as mentioned in the preface we are ignoring normalization issues, and where  $\mathbf{1}_B$  is the identity superoperator on  $\text{End}(\mathcal{H}_B)$ .

Since  $\mathcal{E}$  is completely positive and trace-preserving, the image of  $\mathcal{E} \otimes \mathbf{1}_B$  is a density matrix on  $\mathcal{H}_A \otimes \mathcal{H}_B$ . This density matrix can then be decomposed as an ensemble of pure states in many different ways; choosing one of them, we can write

$$\mathcal{E}(\rho) = \sum_{i,a} p_i q_a \langle \psi_i^* |_B (|\Gamma^a\rangle_{AB} \langle \Gamma^a|_{AB}) |\psi_i^*\rangle_B, \quad (198)$$

where  $\sum_a q_a = 1$ . Here the number of summands in the sum over  $a$  is at minimum the rank of the image under  $\mathcal{E} \otimes \mathbf{1}_B$ , but may also be greater than this. We now define the (Kraus) operators

$$\text{End}(\mathcal{H}_A) \ni \mathcal{K}_a : |\psi_i\rangle_A \mapsto \sqrt{q_a} |\psi_i^*| \Gamma^a\rangle_{AB}, \quad (199)$$

in terms of which

$$\mathcal{E}(\rho) = \sum_{a,i} p_i \mathcal{K}_a \rho \mathcal{K}_a^\dagger. \quad (200)$$

---

<sup>16</sup>This does not mean that  $\mathcal{E} \in \text{End}(\text{End}(\mathcal{H}_A))$ ! Indeed, one can show (see diary entry on invertible quantum channels) that any  $\mathcal{E}$  which is a homomorphism on  $\text{End}(\mathcal{H}_A)$  is necessarily realized by Hamiltonian time evolution.

One can check that since  $\mathcal{E}$  is trace-preserving, the  $\mathcal{K}_a$  satisfy the expected  $\sum_a \mathcal{K}_a^\dagger \mathcal{K}_a = \mathbf{1}_A$ .

The same sort of ambiguity which arises when decomposing a density matrix as an ensemble of pure states arises here when determining the Kraus operators. Indeed, there are both many different ways of decomposing  $\rho_A$  into ensembles of pure states on  $\mathcal{H}_A$ , and many different ways of decomposing the image of  $\mathcal{E} \otimes \mathbf{1}_B$  into ensembles of pure states on  $\mathcal{H}_A \otimes \mathcal{H}_B$ . Just as with the case of decomposing density matrices, the ambiguity can be determined by doing a purification: for the representation in terms of  $\Gamma^a$ s above,

$$\mathcal{E}(\rho) = \sum_i p_i \langle \psi_i^* |_B \text{Tr}_E [|\Gamma\rangle_{ABE} \langle \Gamma|_{ABE}] |\psi_i^*\rangle_B, \quad (201)$$

where

$$|\Gamma\rangle_{ABE} = \sum_a \sqrt{q_a} |\Gamma^a\rangle_{AB} |a\rangle_E, \quad (202)$$

and where the environment  $\mathcal{H}_E$  has a dimension at least as large as the number of Kraus operators.

Now suppose we write  $\mathcal{E}(\rho)$  using a different ensemble of pure states

$$\mathcal{E}(\rho) = \sum_{i,\mu} p_i q_\mu \langle \psi_i^* |_B (|\tilde{\Gamma}^\mu\rangle_{AB} \langle \tilde{\Gamma}^\mu|_{AB}) |\psi_i^*\rangle_B, \quad (203)$$

where we have used greek indices to emphasize that the number of pure states appearing in the ensemble may not be the same as in the representation in terms of the  $|\Gamma^a\rangle_{AB}$ s. The Kraus operators in this representation are evidently defined by

$$\tilde{\mathcal{K}}_\mu : |\psi_i\rangle_A \mapsto \sqrt{q_\mu} \langle \psi_i^* |_B |\tilde{\Gamma}^\mu\rangle_{AB}. \quad (204)$$

We can similarly purify this representation as

$$\mathcal{E}(\rho) = \sum_i p_i \langle \psi_i^* |_B \text{Tr}_E [|\tilde{\Gamma}\rangle_{ABE} \langle \tilde{\Gamma}|_{ABE}] |\psi_i^*\rangle_B, \quad |\tilde{\Gamma}\rangle_{ABE} = \sum_\mu \sqrt{q_\mu} |\tilde{\Gamma}^\mu\rangle_{AB} |\mu\rangle_E. \quad (205)$$

Now both  $|\Gamma\rangle_{ABE}$  and  $|\tilde{\Gamma}\rangle_{ABE}$  are purifications of the density matrix  $(\mathcal{E} \otimes \mathbf{1}_B)(|\Phi\rangle_{AB} \langle \Phi|_{AB})$ . Therefore using the result we proved above,

$$|\Gamma\rangle_{ABE} = (\mathbf{1}_{AB} \otimes U_E) |\tilde{\Gamma}\rangle_{ABE} = (\mathbf{1}_{AB} \otimes U_E) \sum_{\mu,b} \sqrt{q_\mu} [U_{a \rightarrow \mu}]_{\mu b} |\tilde{\Gamma}^\mu\rangle_{AB} |b\rangle_E, \quad (206)$$

where  $U_{a \rightarrow \mu}$  is the unitary implementing the change of basis between the  $\{|\mu\rangle_E\}$  and  $\{|a\rangle_E\}$  bases (if the number of states in the ensemble sum over  $a$  is not the same as the number in the sum over  $\mu$ , we simply add some new  $q_\mu$  or  $q_a$ s which take the value zero, allowing the sizes of the environments in both purifications to be identical wolog). We therefore find

$$\sqrt{q_a} |\Gamma^a\rangle_{AB} = \sum_\mu [\mathcal{U}]_{a\mu} \sqrt{q_\mu} |\tilde{\Gamma}^\mu\rangle_{AB}, \quad \mathcal{U} = U_E U_{a \rightarrow \mu}. \quad (207)$$

Then by definition,

$$\mathcal{K} = \mathcal{U} \tilde{\mathcal{K}}, \quad (208)$$



with the  $\mathcal{H}_E$  indices suppressed.



## Random quantum expanders

---

Today's entry is inspired by a problem assigned by John McGreevy to his QI class. We consider a family of quantum channels  $\mathcal{E}_N$  which act as

$$\mathcal{E}_N : \text{End}(\mathbb{C}^d) \rightarrow \text{End}(\mathbb{C}^d), \quad \mathcal{E}_N : \rho \mapsto \sum_{a=1}^N \frac{1}{N} U_a \rho U_a^\dagger, \quad (209)$$

where the  $U_a$  are drawn from a particular sampling of the Haar measure on  $U(d)$ . We will be looking at what happens under repeated application of this channel, by computing the vN entropy

$$S(N, n) = -\langle \text{Tr}[\mathcal{E}_N^n(\rho_0) \ln \mathcal{E}_N^n(\rho_0)] \rangle, \quad (210)$$

where the brackets denote the Haar average, and where  $\rho_0$  is some initial pure state (we will take  $\rho = |0\rangle\langle 0|$ ).



First, note that as  $n \rightarrow \infty$ , we expect that regardless of  $N$  and  $r$ , we will have (this intuitively obvious fact will be proved below)

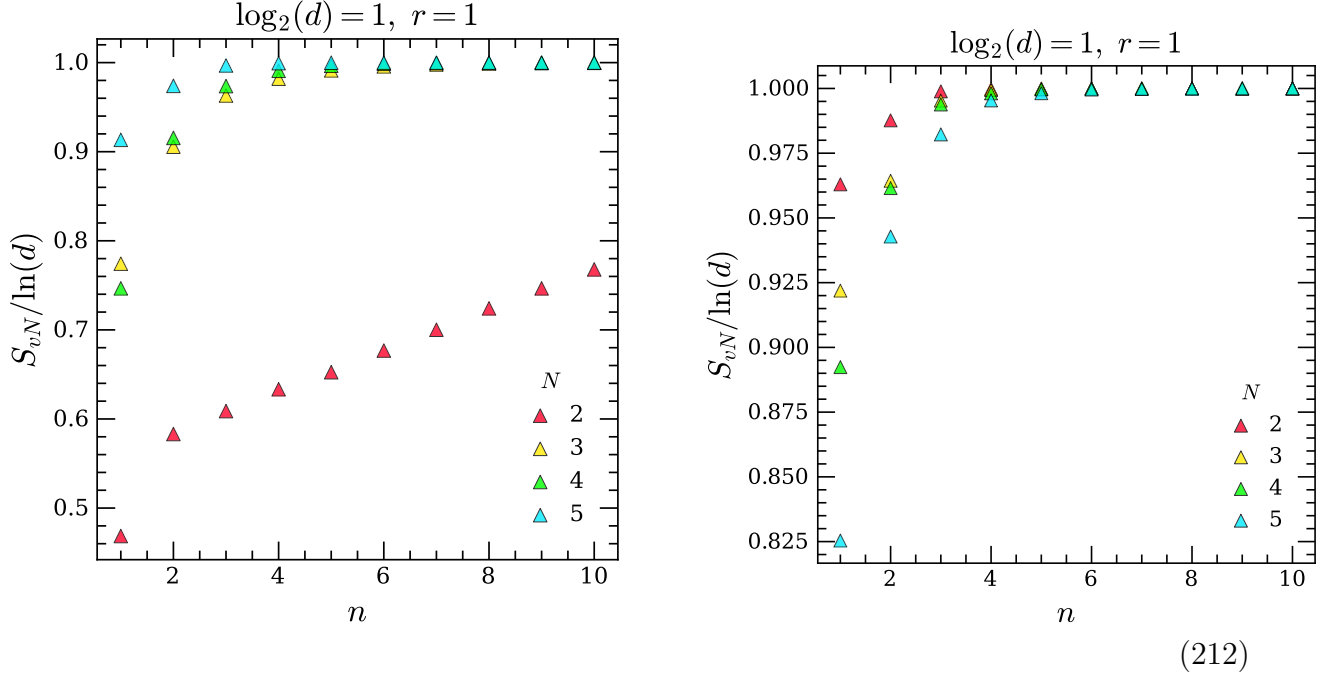
$$\mathcal{E}_N^n(\rho) \xrightarrow{n \rightarrow \infty} \mathbf{1}. \quad (211)$$

Therefore in all of the plots which follow, we will compute the difference between the vN entropy of  $\mathcal{E}_N^n(\rho)$  and  $\ln d$ , with  $d$  the Hilbert space dimension.

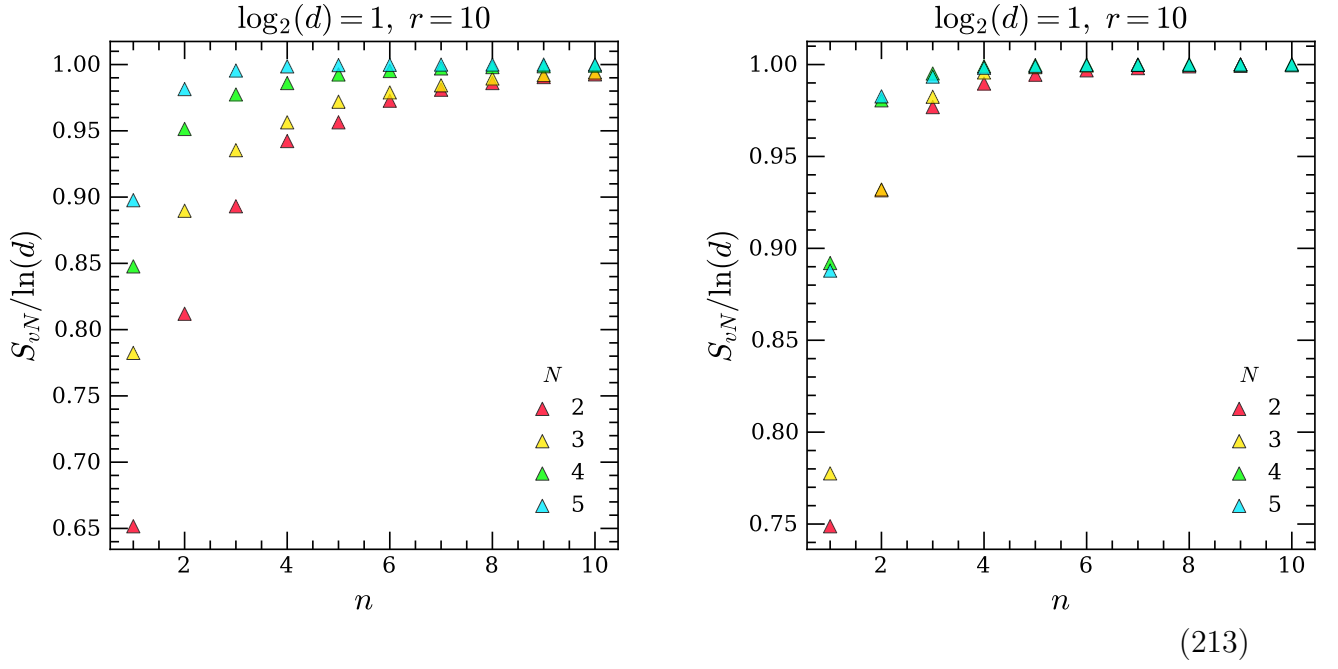
To compute the vN entropy of  $\mathcal{E}_N^n(\rho)$  numerically, we approximate the Haar average by averaging over  $r \in \mathbb{N}$  instances of the vN entropies computed for fixed realizations of the  $U_a$ s, with  $r \rightarrow \infty$  being the Haar average.

Let us first look at a single qubit. The variations in each realization of the sampling from  $U(2)$  are huge. For example, two such one-shot realizations give (here the matrices used in

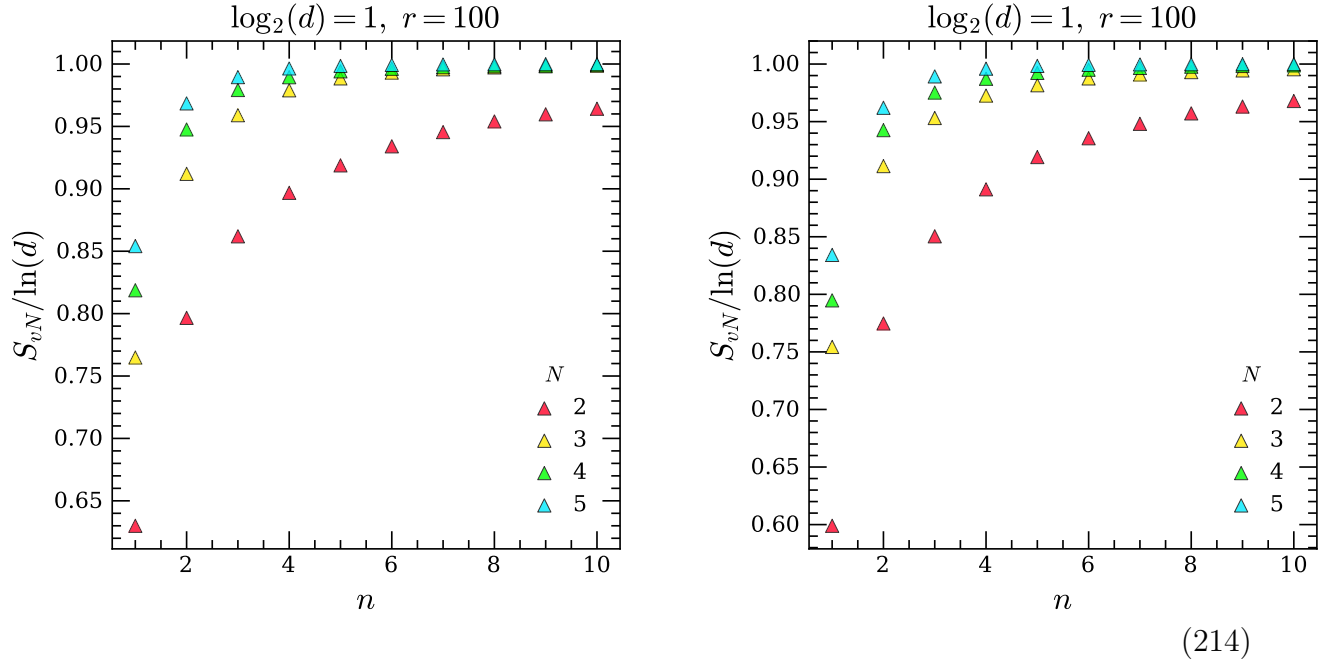
each sampling for  $N = k$  are a subset of those for  $N > k$ )



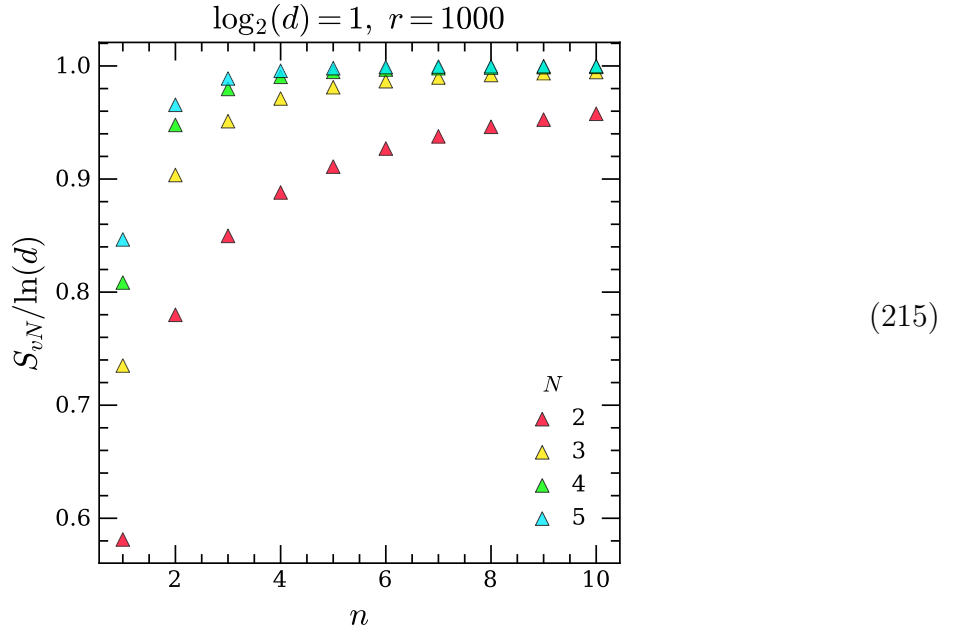
$r = 10$  is not enough large enough to effectively implement the average:



For  $r = 100$ , we have

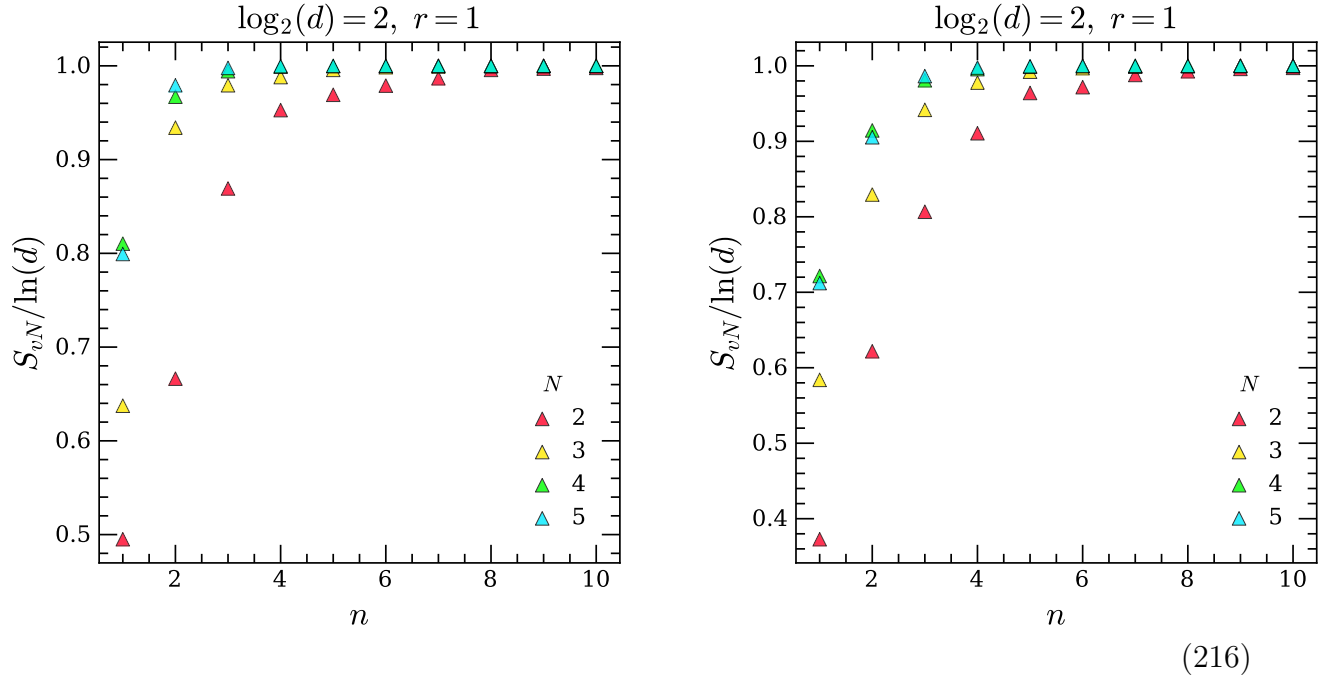


Therefore for 1 qubit,  $r = 100$  comes pretty close to implementing the full Haar average. Indeed, increasing by another factor of 10 doesn't change the plots appreciably:

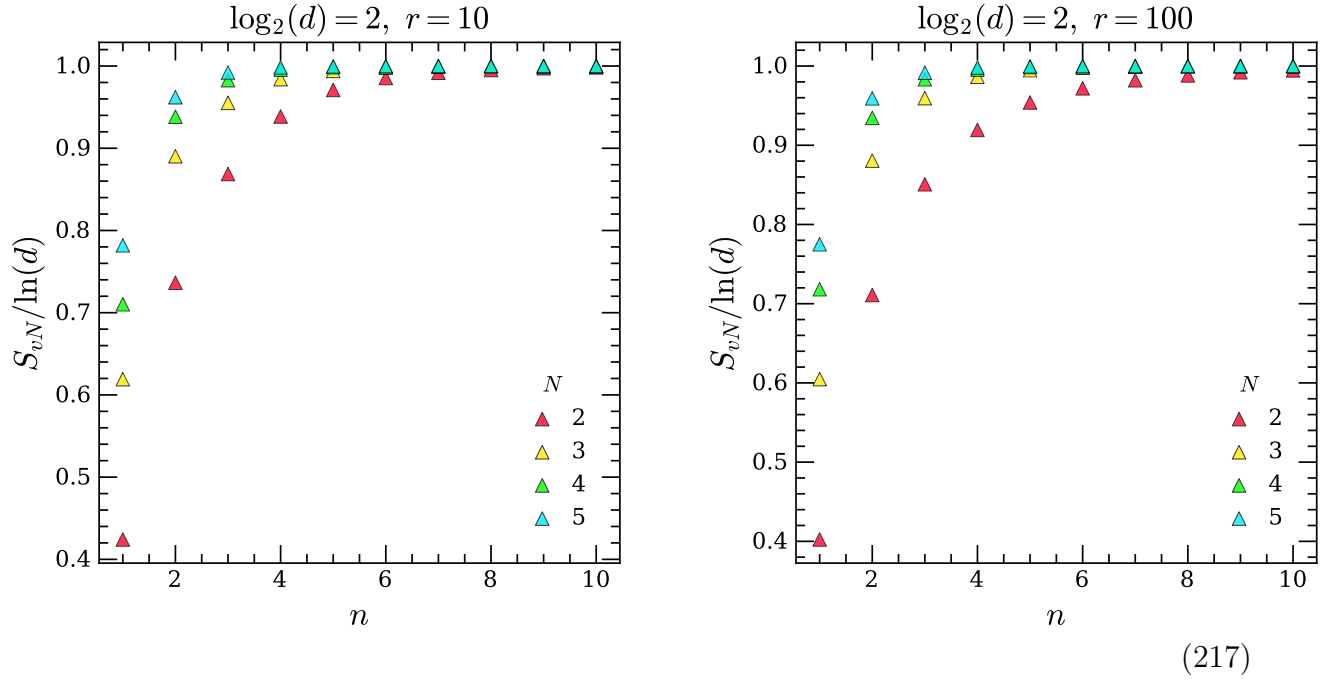


Now let us look at what happens when we increase the number of qubits. For two qubits,

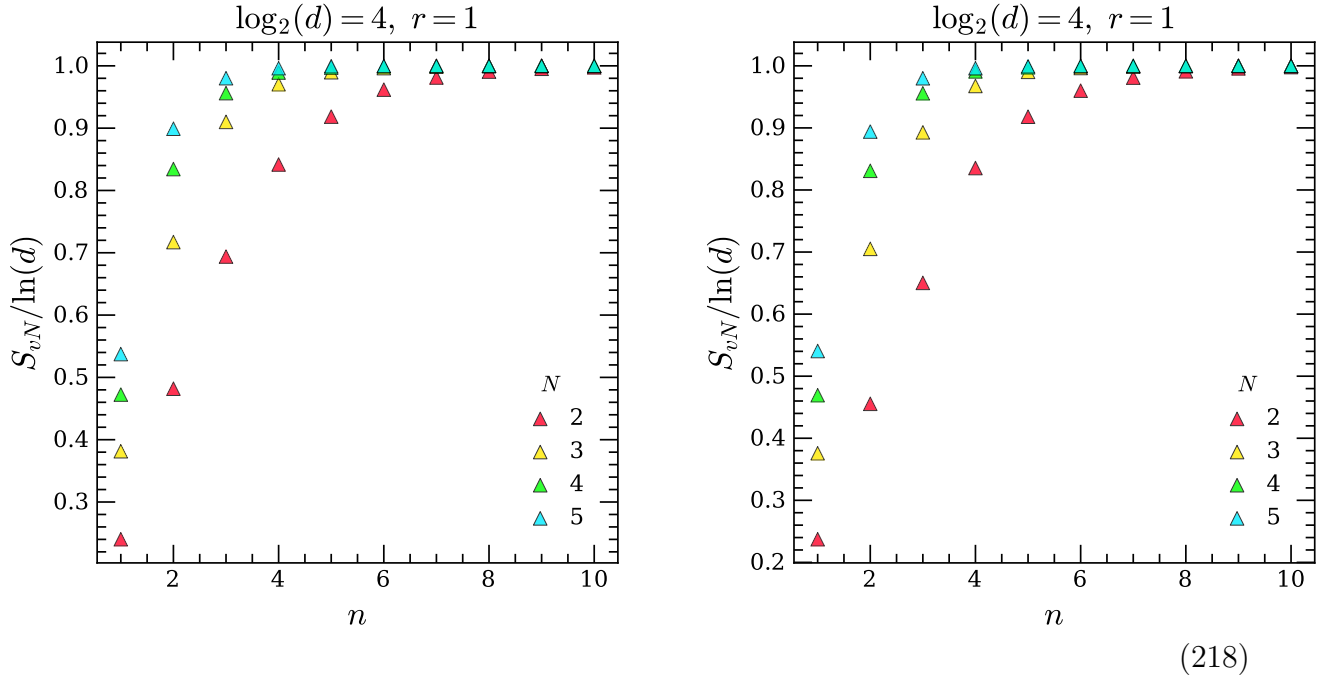
we still have appreciable variations between single-shot realizations of the unitaries:



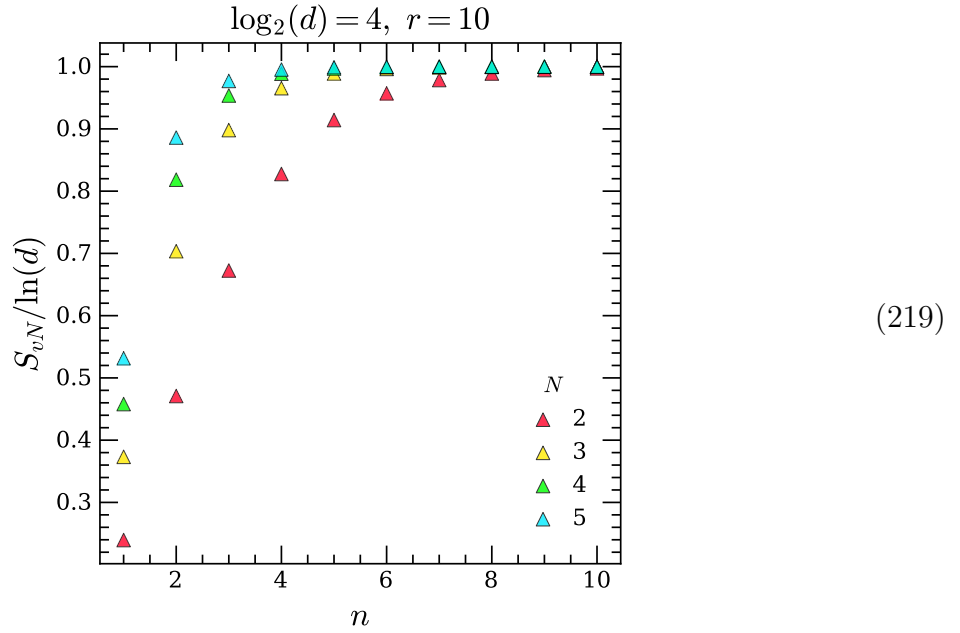
However, the convergence to the full Haar average is rather quick, with the  $r = 10, 100$  plots looking almost identical:



For four qubits, even two different  $r = 1$  realizations look very similar:

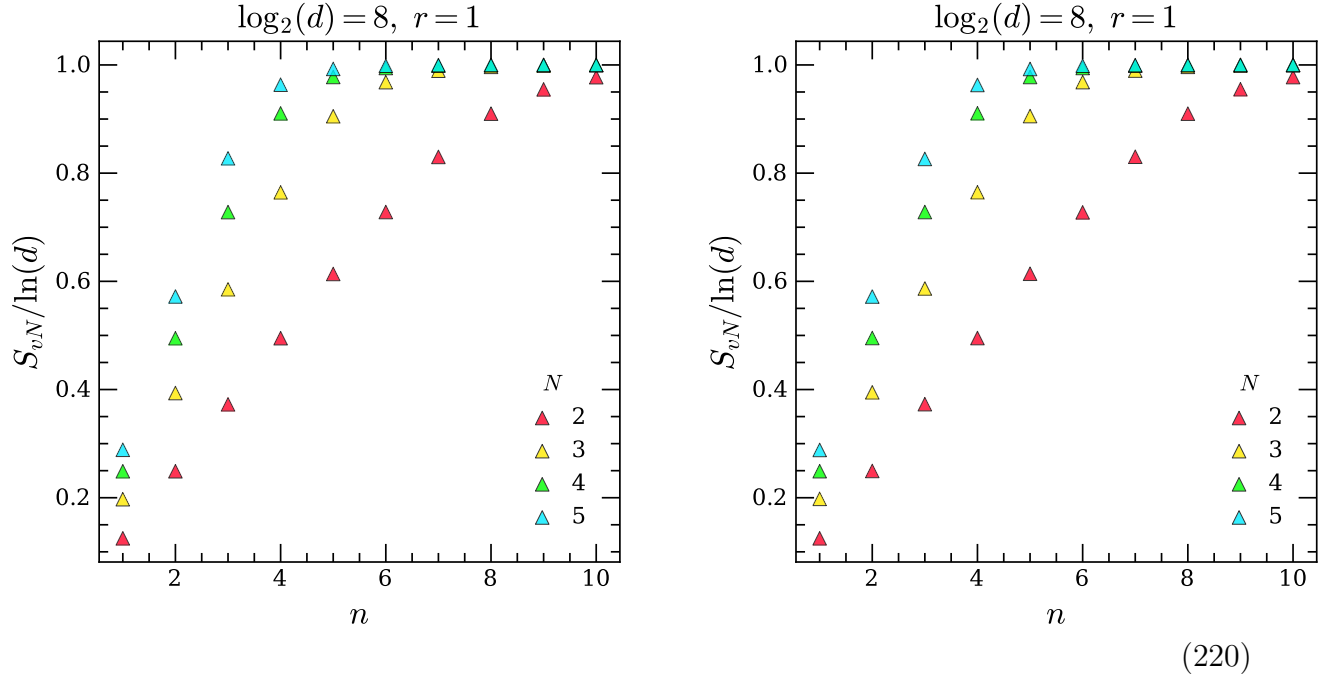


For  $r = 10$ ,



where there is no real reason to go beyond  $r = 10$  due to the fast convergence. Two different

one-shot realizations for eight qubits gives



with the two plots being essentially indistinguishable.

Let's now try to get an analytic understanding of these results. The basic fact that  $S(n \rightarrow \infty, N)$  monotonically increases with  $n$  and asymptotically approaches the maximal value of  $\ln d$  is a consequence of the result that the output of a unital channel is majorized by its input, i.e. that unital channels increase the mixed-ness of states on which they act. This statement is proved in a subsection below. Since  $\mathcal{E}_N$  is obviously unital, the limit as  $n \rightarrow \infty$  of  $\mathcal{E}_N^n$  will be the most mixed possible state, viz.  $\mathbf{1}/d$ .

Unfortunately since  $S_{vN}$  has a log, it is hard to make any more precise analytic statements about it directly. We can however make statements about e.g. things involving powers of  $\rho$ , like the Renyi entropies. For simplicity, we will look at the purity<sup>17</sup>  $\mathcal{P} = \text{Tr}[\rho^2]$ . Again for simplicity, we will just look at its average under a single application of the channel (we know that it must be monotonically decreasing as a function of  $n$  since  $\rho \prec \sigma$  implies that  $\mathcal{P}_\rho \leq \mathcal{P}_\sigma$ ). Therefore we would like to compute

$$\langle \mathcal{P} \rangle = \langle \text{Tr}[\mathcal{E}_N(\rho)^2] \rangle. \quad (221)$$

Now each  $U_a$  in the quantum channel is averaged over as an independent Haar unitary. Therefore

$$\langle \mathcal{E}_N(\rho)^2 \rangle = \frac{1}{N^2} \left( \sum_{a \neq b} \langle U_a \rho U_a^\dagger \rangle \langle U_b \rho U_b^\dagger \rangle + \sum_a \langle U_a \rho^2 U_a^\dagger \rangle \right). \quad (222)$$

The individual matrix elements of the square of the quantum channel are then

$$\langle [\mathcal{E}_N(\rho)^2]_{ad} \rangle = \frac{N-1}{N} \langle U_{aa'} U_{cc'}^* \rangle \langle U_{bb'} U_{dd'}^* \rangle \rho_{a'c'} \rho_{b'd'} \delta_{cb} + \frac{1}{N} \langle U_{aa'} U_{bb'}^* \rangle \rho_{a'e} \rho_{eb'} \quad (223)$$

<sup>17</sup>This is a simple measure of purity because it is 1 for pure states and minimal on maximally-mixed ones.

We know this will be proportional to the identity by Schur's lemma and shifting the Haar integral, but in order to get the coefficient we need to recall how to average over Haar unitaries. This is explained in gory detail in a separate diary entry; here we just need that

$$\int dU U_{ab} U_{cd}^* = \frac{1}{d} \delta_{ac} \delta_{bd}. \quad (224)$$

The above will work for computing the purity under one application of the channel; for larger values of  $n$  one also needs expressions like

$$\int dU [U_{a'a} U_{b'b} U_{c'c}^* U_{d'd}^*] = \frac{1}{d^2 - 1} \left( \delta_{a'a'} \delta_{b'b'} \delta_{ac} \delta_{bd} + \delta_{a'b'} \delta_{c'd'} \delta_{ad} \delta_{bc} - \frac{1}{d} (\delta_{a'a'} \delta_{b'b'} \delta_{ad} \delta_{bc} + \delta_{a'b'} \delta_{c'd'} \delta_{ac} \delta_{bd}) \right) \quad (225)$$

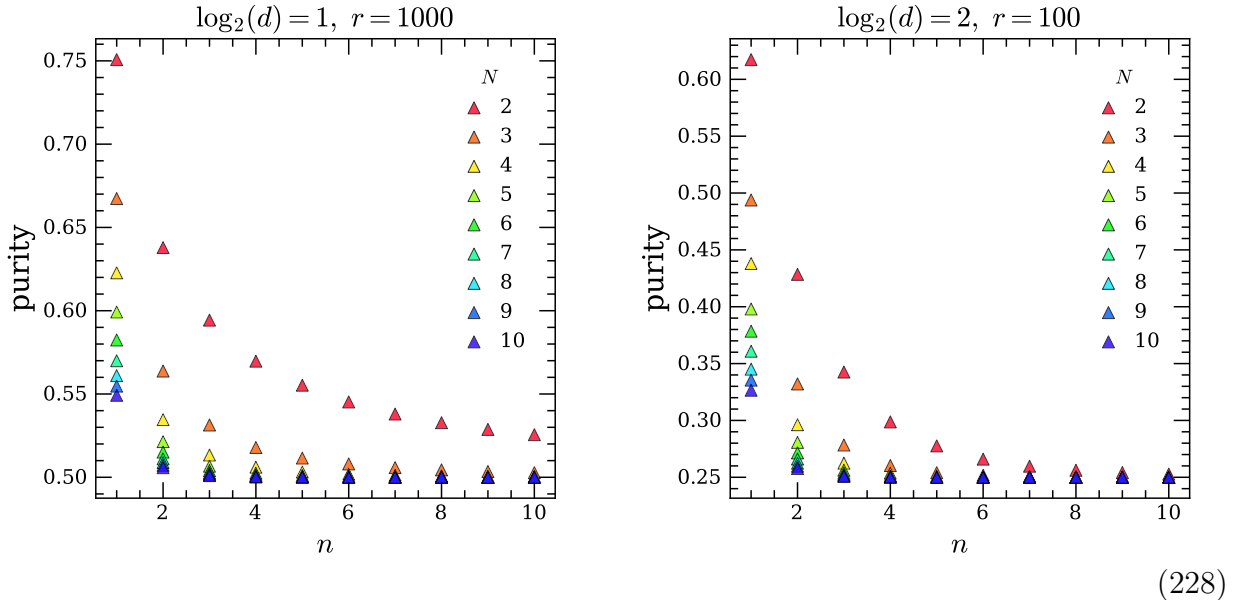
Using the above formula for the second moment, we find

$$\langle \mathcal{E}_N(\rho)^2 \rangle = \left( \frac{N-1}{d^2 N} \text{Tr}[\rho]^2 + \frac{1}{dN} \text{Tr}[\rho^2] \right) \mathbf{1}. \quad (226)$$

Since we are choosing an initial  $\rho$  which is pure, we obtain

$$\langle \mathcal{P} \rangle = \frac{N-1}{d^2 N} + \frac{1}{Nd}. \quad (227)$$

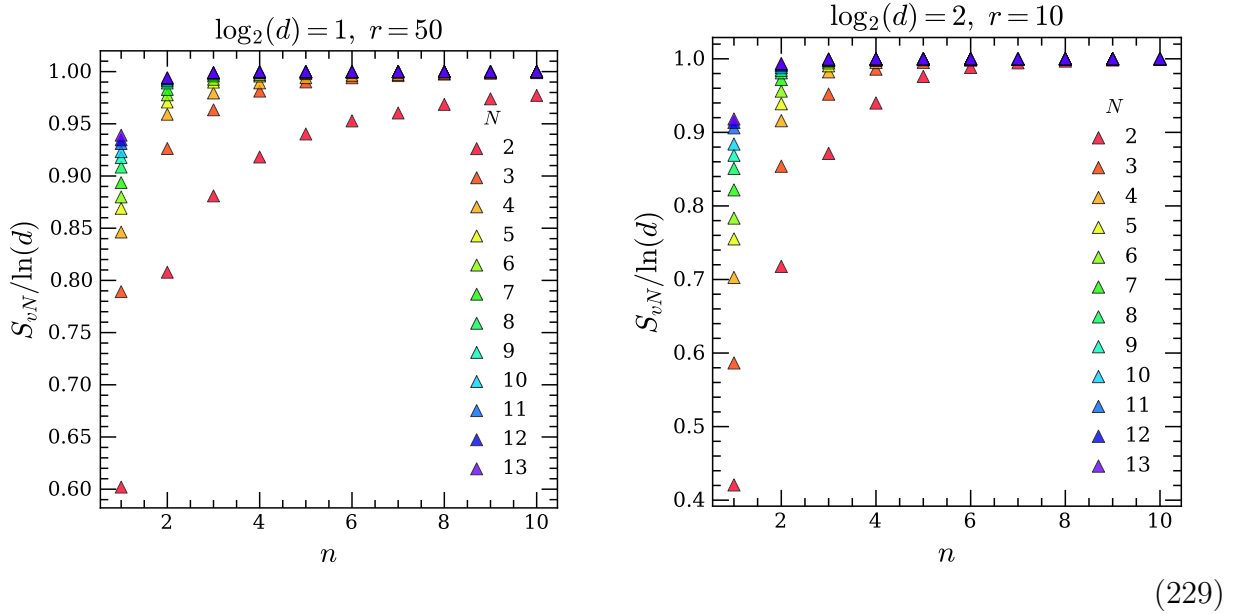
We can check this by computing the purities numerically: for one- and two-qubit systems, we find



Plugging in numbers to (227) verifies that this agrees exactly with the values obtained from the plots shown above.

Note that the purity (227) asymptotes to a fixed nonzero value of  $1/d^2$  as  $N \rightarrow \infty$ . We therefore expect that the vN entropy after one application of the channel should also asymptote as  $N \rightarrow \infty$  to some fixed value less than 1. This can be confirmed by increasing

the range of  $N$ : for one- and two-qubit systems, we have



### *Diversion on majorization and doubly stochastic maps*

We will now do a problem in Preskill's QI notes on unital channels and majorization (a channel  $\mathcal{C}$  is unital if  $\mathcal{C}(\mathbf{1}) = \mathbf{1}$ ; clearly the  $\mathcal{E}_N$  considered in today's diary entry are unital), which will give the result mentioned above on the increasing mixedness of  $\rho$  under application of  $\mathcal{E}_N$ .

**Theorem 1.** *If  $\mathcal{C}$  is a unital quantum channel, then for any density matrix  $\rho$ ,  $\mathcal{C}(\rho)$  is majorized by  $\rho$ :*

$$\mathcal{C}(\rho) \prec \rho. \quad (230)$$

Recall that this means that if  $\Delta_{\mathcal{C}(\rho)}, \Delta_\rho$  are the eigenvalues of  $\mathcal{C}(\rho), \rho$  respectively, then for all  $1 \leq n \leq \dim \Delta_\rho$ , we have

$$\mathcal{C}(\rho) \prec \rho \implies \sum_i^n [\Delta_{\mathcal{C}(\rho)}^\downarrow]_i \leq \sum_i^n [\Delta_\rho^\downarrow]_i, \quad (231)$$

where the  $\downarrow$  on each set of eigenvalues indicates that they are ordered from greatest to least.  $\mathcal{C}(\rho) \prec \rho$  is pronounced as “ $\mathcal{C}(\rho)$  is at least as mixed as  $\rho$ ”. Hence the claim is that if  $\mathcal{C}$  is unital, the purity of  $\rho$  decreases monotonically under repeated application of the channel.

*Proof.* The proof is pretty simple. Since  $\mathcal{C}(\rho)$  and  $\rho$  are both Hermitian, they are diagonalized by unitaries  $U$  and  $V$ , respectively. If  $\mathcal{C}$  has a representation in terms of Kraus operators  $\mathcal{K}_a$ , then

$$\Delta_{\mathcal{C}(\rho)} = \sum_a U^\dagger \mathcal{K}_a V \Delta_\rho V^\dagger \mathcal{K}_a^\dagger U, \quad (232)$$



where both  $\Delta$  matrices are diagonal. We can then write the RHS as

$$\sum_a U^\dagger \mathcal{K}_a V \Delta_\rho V^\dagger \mathcal{K}_a^\dagger U = \mathcal{M} \Delta_\rho \quad (233)$$

with the matrix  $\mathcal{M}$  given by

$$\mathcal{M}_{ij} = \sum_a [U^\dagger \mathcal{K}_a V]_{ij} [V^\dagger \mathcal{K}_a^\dagger U]_{ji} = \sum_a [U^\dagger \mathcal{K}_a V]_{ij} [U^T \mathcal{K}_a^* V^*]_{ij} = \sum_a |[V^\dagger \mathcal{K}_a^\dagger U]_{ji}|^2. \quad (234)$$

All the entries of  $\mathcal{M}$  are obviously positive. Furthermore all the rows of  $\mathcal{M}$  sum to 1:<sup>18</sup>

$$\sum_i \mathcal{M}_{ij} = \sum_a [V^\dagger \mathcal{K}_a^\dagger \mathcal{K}_a V]_{jj} = 1. \quad (235)$$

Since  $\mathcal{C}$  is unital, we must have  $\mathcal{C}(\mathbf{1}) = \sum_a \mathcal{K}_a \mathcal{K}_a^\dagger = \mathbf{1}$ . This implies that all the columns of  $\mathcal{M}$  sum to 1 as well:

$$\sum_j \mathcal{M}_{ij} = \sum_a [U^\dagger \mathcal{K}_a \mathcal{K}_a^\dagger U]_{ii} = 1. \quad (236)$$

Therefore we have  $\Delta_{\mathcal{C}(\rho)} = \mathcal{M} \Delta_\rho$ , with  $\mathcal{M}$  a doubly stochastic matrix.

The fact that the two vectors of eigenvalues are related by a doubly stochastic matrix means that the eigenvalues of  $\mathcal{C}(\rho)$  are convex combinations of the eigenvalues of  $\rho$ . This follows from the Birkhoff-von Neumann theorem, viz. that the set of doubly stochastic matrices is the convex hull<sup>19</sup> of the set of permutation matrices. Intuitively, this means that the eigenvalues of  $\mathcal{C}(\rho)$  are more "smoothed out" and "uniform" than those of  $\rho$ . The precise statement is of course that  $\mathcal{C}(\rho) \prec \rho$ , although we won't go into the details of the proof here. We won't show here that the double stochasticity of  $\mathcal{M}$  implies the majorization; this can be looked up in chapter 12 of N&C.

□



<sup>18</sup>If we have  $p = Dq$  for two probability distributions  $p, q$  (as we do here), then the rows of  $D$  generically sum to one — this is required if  $D$  is to preserve the normalization  $\sum_i q_i = 1$ , and hence is why proving it requires using  $\sum_a \mathcal{K}_a^\dagger \mathcal{K}_a = \mathbf{1}$ . The property of the columns of  $D$  summing to one is something extra, and is what determines the double stochasticity of  $D$ .

<sup>19</sup>The fact that convex combinations of doubly stochastic matrices are doubly stochastic is easy to see. The fact that the corners of this convex hull are given by the permutation matrices is also intuitively reasonable — taking convex combinations "smooths out" the eigenvalues while permutation matrices leave the eigenvalues unchanged, hence the permutation matrices cannot be formed from convex combinations of matrices which all "smooth out" the eigenvalues.

## Separable states have classical correlations (P10.5)

---

Today we will be doing a short exercise from Preskill's QI class, the goal of which is to check that the notion of separability provides a good definition of “unentangled” for mixed states.

☛ ☛

Consider a density matrix  $\rho_{AB}$  which is *separable*, i.e. which can be written in the form of an ensemble of  $\otimes$  states:

$$\rho_{AB} = \sum_a p_a |\psi_a\rangle\langle\psi_a| \otimes |\phi_a\rangle\langle\phi_a|. \quad (237)$$

The reduced density matrices generically have rank greater than 1, but the idea is that the nonzero vN entropy here is not really due to entanglement between  $A$  and  $B$ . This is basically because states of the above form are created from pure product states through LOCC (local operations + classical communication). These states are of the form  $\mathcal{E}_{LOCC}(|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|)$ , where the quantum channel is

$$\mathcal{E}_{LOCC} : \rho \mapsto \sum_a p_a U_{aA} \otimes U_{aB} \rho U_{aA}^\dagger \otimes U_{aB}^\dagger, \quad (238)$$

where the  $U_{aA/B}$  are (generically different) unitaries acting on  $A$  and  $B$ . The LOCC subscript here is due to how such a channel arises: an observer of the subsystem  $A$  does a local operation to their density matrix and sends the result via a classical communication channel to an observer of subsystem  $B$ , who then performs a local operation on their density matrix, with the operation chosen dependent on the classical communication from  $A$ . This process makes the density matrices on each subsystem mixed,<sup>20</sup> but since there are never any operators involved which act on both  $A$  and  $B$  simultaneously, no entanglement is created between  $A$  and  $B$ .

We will now check that separable states satisfy our intuition about classical probabilities, namely that subsystems of separable states are less disordered (mixed) than the full systems themselves.

To do this, we first write both  $\rho_{AB}$  and  $\rho_A$  in bases where they are diagonal (note that the  $|\psi\rangle$  [and  $|\phi\rangle$ ] states appearing in the expression for  $\rho_{AB}$  do not generically constitute an orthonormal basis; hence we still need to diagonalize  $\rho_A$ ):

$$\rho_{AB} = \sum_i q_i |e_i\rangle\langle e_i|, \quad \rho_A = \sum_\mu r_\mu |f_\mu\rangle\langle f_\mu|, \quad (239)$$

where the  $|e_i\rangle$  and  $|f_\mu\rangle$  are orthonormal bases for  $\mathcal{H}_{AB}$  and  $\mathcal{H}_A$ , respectively. Now consider purifications associated to the two different ways we have written  $\rho_{AB}$ :

$$|\Psi_e\rangle = \sum_i \sqrt{q_i} |e_i\rangle_{AB} \otimes |\gamma_i\rangle_C, \quad |\Psi_{\psi\phi}\rangle = \sum_a \sqrt{p_a} |\psi_a\phi_a\rangle_{AB} \otimes |\lambda_a\rangle_C, \quad (240)$$

---

<sup>20</sup>Indeed the mixedness of each reduced density matrix increases monotonically under the application of such channels. This is because on each reduced density matrix,  $\mathcal{E}_{LOCC}$  acts as a quantum expander (from the previous diary entry), which is unital and hence which is such that its output is majorized by its input.

where  $\mathcal{H}_C \cong \mathcal{H}_{AB}$  is the auxiliary space, with two different orthonormal bases  $|\gamma\rangle, |\lambda\rangle$ . These two purifications are then related by a unitary acting on  $\mathcal{H}_C$  as (proven by Schmidt-decomposing both purifications)

$$|\Psi_e\rangle = (\mathbf{1}_{AB} \otimes U_C) |\Psi_{\psi\phi}\rangle. \quad (241)$$

Taking the inner product of both sides with  $|\gamma_k\rangle$ , we find that

$$\sqrt{q_k} |e_k\rangle = \sum_a U_{ka} \sqrt{p_a} |\psi_a \phi_a\rangle. \quad (242)$$

Therefore

$$q_k = \sum_{ab} U_{ka} U_{kb}^* \sqrt{p_a p_b} \langle \psi_b | \psi_a \rangle \langle \phi_b | \phi_a \rangle \quad (243)$$

We now want to get an expression for the square root of  $p_a$ s in side the sum on the RHS. We do this by doing the same thing with the reduced density matrix  $\rho_A$ : it has the purifications

$$|\Psi_f\rangle = \sum_{\mu} \sqrt{r_{\mu}} |f_{\mu}\rangle_A \otimes |\beta_{\mu}\rangle_E, \quad |\Psi_{\psi}\rangle = \sum_a \sqrt{p_a} |\psi_a\rangle_A \otimes |\alpha_a\rangle_E, \quad (244)$$

which likewise are related via

$$|\Psi_{\psi}\rangle = (\mathbf{1}_A \otimes V_E) |\Psi_f\rangle. \quad (245)$$

Therefore

$$\sqrt{p_a p_b} \langle \psi_b | \psi_a \rangle = \sum_{\mu\nu} V_{a\mu} V_{b\nu}^* \sqrt{r_{\mu} r_{\nu}} \langle f_{\nu} | f_{\mu} \rangle = \sum_{\mu} V_{a\mu} V_{b\mu}^* r_{\mu}. \quad (246)$$

If we use this in our expression for  $q_k$  obtained above, we get

$$\mathbf{q} = \mathcal{D} \mathbf{r}, \quad \mathcal{D}_{k\mu} = \sum_{ab} U_{ka} U_{kb}^* V_{a\mu} V_{b\mu}^* \langle \phi_b | \phi_a \rangle = \left| \sum_a U_{ka} V_{a\mu} |\phi_a\rangle \right|^2. \quad (247)$$

The matrix  $\mathcal{D}$  is obviously positive. It is also easy to see by the normalization of the  $|\phi_a\rangle$ s and the unitarity of  $U, V$  that  $\sum_k \mathcal{D}_{k\mu} = 1, \sum_{\mu} \mathcal{D}_{k\mu} = 1$  for all  $k$  and all  $\mu$ . Therefore  $\mathcal{D}$  is a doubly-stochastic matrix. In accordance with the results from another diary entry, this means that the full density matrix is majorized by its marginals:

$$\rho_{AB} \prec \rho_A, \quad \rho_{AB} \prec \rho_B, \quad (248)$$

where by this we really mean that the matrix of eigenvalues of  $\rho_{AB}$  is majorized by the matrix of eigenvalues of  $\rho_A$  (and likewise for  $B$ ). Note that the statement about majorization here makes sense even though the two matrices involved are defined on different Hilbert spaces, since we have tacitly been extending the two reduced density matrices to  $\mathcal{H}_A \otimes \mathcal{H}_B$  by padding them with zeros.

Since the majorization symbol  $\rho \prec \sigma$  means ‘ $\sigma$  is less mixed than  $\rho$ ’, we conclude that in this case,  $\rho_{AB}$  is more mixed than either of its marginals. This is exactly what is expected classically, but is also exactly what *doesn't* happen in quantum mechanics when e.g. the

full density matrix is pure. Therefore we conclude that separable states are a good way of defining unentangled states in the mixed case.



## Reduced density matrices in typical states are maximally mixed

---

Today we have yet another short problem from Preskill's class. We will be showing that reduced density matrices associated to subsystems of generic pure states are very close to being maximally mixed, as long as the subsystem is smaller than  $\approx$  half the full system size.



We will be working in a Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$ , whose  $\otimes$  factors have dimensions  $d_A$  and  $d_B$ , respectively. To diagnose the expected mixedness of  $\rho_A$  when the full system is in a random pure state, we start by computing

$$\langle \|\rho_A - \mathbf{1}_A/d_A\|_2 \rangle_\phi, \quad (249)$$

where the average is over all pure density matrices  $\rho_{AB} = |\phi\rangle\langle\phi|$ . The norm here is  $\|\mathcal{O}\|_2 = \sqrt{\text{Tr}[\mathcal{O}^\dagger \mathcal{O}]}$ , which corresponds to the inner product of vectors when operators are mapped to vectors via  $\text{End}(\mathcal{H}) \cong \mathcal{H} \otimes \mathcal{H}^*$ . Since  $\langle \sqrt{f} \rangle \leq \sqrt{\langle f \rangle}$  for any positive function  $f$  (we will prove this simple fact below), we have

$$\langle \|\rho_A - \mathbf{1}_A/d_A\|_2 \rangle_\phi \leq \sqrt{\langle \|\rho_A - \mathbf{1}_A/d_A\|_2^2 \rangle_\phi}. \quad (250)$$

Now since  $\langle \rho_{AB} \rangle_\phi$  is in the center of  $GL(d_A d_B, \mathbb{C})$  and has unit trace, we have  $\langle \rho_{AB} \rangle_\phi = \mathbf{1}/d_A d_B \implies \langle \rho_A \rangle_\phi = \mathbf{1}_A/d_A$ . Therefore

$$\langle \|\rho_A - \mathbf{1}_A/d_A\|_2 \rangle_\phi \leq \sqrt{\langle \text{Tr}[\rho_A^2] \rangle - 1/d_A}. \quad (251)$$

We therefore need to calculate the average of the purity  $\mathcal{P}_A = \text{Tr} \rho_A^2$ . We will do this first by writing the purity as

$$\mathcal{P}_A = \text{Tr}_{ABA'B'}[\mathcal{S}_{AA'} \otimes \mathbf{1}_{BB'} \rho_{AB} \otimes \rho_{A'B'}], \quad (252)$$

where  $\mathcal{S}$  is the swap operator and  $\rho_{A'B'}$  is just a copy of  $\rho_{AB}$ . Proving the above equation is best done by drawing a picture:

$$\begin{aligned}
 & \text{Diagram 1} = \text{Diagram 2} \\
 & \text{Diagram 2} = \text{Diagram 3} \\
 & \text{Diagram 3} = \text{Diagram 4}
 \end{aligned}
 \tag{253}$$

We now want to average the purity using the above expression over all pure states  $\rho_{AB} = |\phi\rangle\langle\phi|$ :

$$\langle \mathcal{P}_A \rangle_\phi = \text{Tr}_{ABA'B'} [\mathcal{S}_{AA'} \otimes \mathbf{1}_{BB'} \langle |\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi| \rangle_\phi]
 \tag{254}$$

This can be done at the formal level by decomposing  $\mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$  into  $\oplus$ s of subspaces transforming under  $\otimes$ s of representations of  $\mathbb{Z}_2$  and  $GL(d_A d_B, \mathbb{C})$ , a decomposition made possible by Schur-Weyl duality (see the relevant entry in the math diary). Now we know that the average on the RHS of the above equation will only have support on the subspace corresponding to the trivial irrep of  $\mathbb{Z}_2$ , since it is invariant under  $\mathcal{S}_{AB, A'B'}$ . Furthermore we can implement the average by acting on  $|\phi\rangle$  with all possible unitaries; this implies that  $\langle |\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi| \rangle_\phi$  must be proportional to the identity. Since  $\langle |\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi| \rangle_\phi$  also has unit trace, we must have

$$\langle |\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi| \rangle_\phi = \frac{1}{\dim V_{\text{sym}}} \frac{\mathbf{1} + \mathcal{S}_{AA'} \mathcal{S}_{BB'}}{2} = \frac{1}{d(d+1)} (\mathbf{1} + \mathcal{S}_{AA'} \mathcal{S}_{BB'}),
 \tag{255}$$

where  $d = \dim \mathcal{H}_{AB} = d_A d_B$ . Therefore we find

$$\begin{aligned} \langle \mathcal{P}_A \rangle_\phi &= \frac{1}{d(d+1)} \text{Tr}_{ABA'B'} [\mathcal{S}_{AA'} \otimes \mathbf{1}_{BB'} + \mathbf{1}_{AA'} \otimes \mathcal{S}_{BB'}] \\ &= \frac{1}{d(d+1)} (d_A d_B^2 + d_A^2 d_B) \\ &= \frac{d_A + d_B}{d_A d_B + 1}. \end{aligned} \quad (256)$$

We can then put this into our inequality (251):

$$\begin{aligned} \langle \|\rho_A - \mathbf{1}_A/d_A\|_2 \rangle_\phi &\leq \left( \frac{d_A + d_B}{d_A d_B + 1} - \frac{1}{d_A} \right)^{1/2} \\ &< \frac{1}{\sqrt{d_B + 1/d_A}} \\ &< \frac{1}{\sqrt{d_B}}. \end{aligned} \quad (257)$$

The above provides an upper bound on the  $L^2$  distance of  $\rho_A$  from  $\mathbf{1}_A/d_A$ . We now want to calculate a bound on the  $L^1$  distance, where the norm now has the trace outside the square root, viz.  $\|\mathcal{O}\|_1 = \text{Tr}[\sqrt{\mathcal{O}^\dagger \mathcal{O}}]$ . We do this with the inequality

$$\|\mathcal{O}\|_1 \leq \sqrt{d_{\mathcal{O}}} \|\mathcal{O}\|_2, \quad (258)$$

which implies the inequality  $\langle \sqrt{f} \rangle \leq \sqrt{\langle f \rangle}$  that we used earlier (the inequality is saturated when  $\mathcal{O} = \mathbf{1}$ ). Indeed, in terms of the eigenvalues  $\lambda_a$  of  $\mathcal{O}$ , we have

$$\|\mathcal{O}\|_1 = \sum_a |\lambda_a|, \quad \|\mathcal{O}\|_2 = \sqrt{\sum_a |\lambda_a|^2}. \quad (259)$$

But then we see that the inequality (258) is just a special case of Cauchy-Schwarz: letting  $|\Lambda\rangle$  denote the vector  $(|\lambda_1|, \dots, |\lambda_{d_{\mathcal{O}}}|)^T$ , we have

$$\|\mathcal{O}\|_1 = \langle 1 | \Lambda \rangle \leq \langle 1 | 1 \rangle \langle \Lambda | \Lambda \rangle = \sqrt{d_{\mathcal{O}}} \|\mathcal{O}\|_2, \quad (260)$$

where  $|1\rangle = (1, \dots, 1)^T$ . Using this equality in (257), we then conclude that

$$\langle \|\rho_A - \mathbf{1}_A/d_A\|_1 \rangle_\phi \leq \sqrt{\frac{d_A}{d_B}}. \quad (261)$$

We then see that  $\rho_A$  is very close to being maximally mixed (and hence  $S_A$  is very close to being maximal) for large systems as soon as the size of  $A$  is less than half the system size, while it becomes very close to being pure as soon as the size of  $A$  is more than half the system size.



## Quantum channels are invertible iff they describe closed-system time evolution

---

Today we are doing an elaboration on an exercise found in John Preskill's QI notes — the goal is to prove the statement in the title. There are (at least) two approaches to tackling this problem; one in terms of Kraus operators (as in Preskill's exercise) and one which is rather more algebraic in character. A good reference for learning about stuff used in the algebraic part are the notes by Stephane Attal on quantum channels, available at his homepage.

▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼

We say that a quantum channel  $\mathcal{E} : \text{End}(\mathcal{H}_A) \rightarrow \text{End}(\mathcal{H}_A)$  is *invertible as a quantum channel* if there exists another quantum channel<sup>21</sup>  $\mathcal{E}^{-1}$  such that

$$(\mathcal{E}^{-1} \circ \mathcal{E})(\rho) = \rho \quad (262)$$

for any  $\rho \in \text{End}(\mathcal{H}_A)$ . Our goal is to prove that the existence of the quantum channel  $\mathcal{E}^{-1}$  implies that  $\mathcal{E}$  acts as conjugation by a single unitary, i.e. that all invertible quantum channels correspond to Hamiltonian time evolution.

Note that it is very important that we also require  $\mathcal{E}^{-1}$  to be a quantum channel (viz. completely positive and trace-preserving). Indeed, it is rather easy to construct quantum channels which are invertible *as linear operators*, but whose inverses are not CPTP.

Throughout, we will be restricting to quantum channels that map  $\text{End}(\mathcal{H}_A)$  to itself. If we instead consider maps between Hilbert spaces of different dimensions, the situation is slightly more complicated.

### Kraus operator approach

Consider an invertible quantum channel  $\mathcal{E}$  which acts in the Kraus representation as

$$\mathcal{E}(\rho) = \sum_a \mathcal{K}_a \rho \mathcal{K}_a^\dagger. \quad (263)$$

We will denote the Kraus operators of the inverse channel  $\mathcal{E}^{-1}$  as  $\tilde{\mathcal{K}}_\mu$ .

*Proof.* We will first want to show that  $\mathcal{K}_a \tilde{\mathcal{K}}_\mu = \lambda_{a\mu} \mathbf{1}_A$ ,  $\lambda_{a\mu} \in \mathbb{C}$  for all  $a, \mu$ . From the above remark, the constraint on  $\mathcal{E}^{-1}$  depends on our assumption that  $\mathcal{E}^{-1}$  is CPTP, and so to derive this we must use the normalization properties of the Kraus operators.

First, note that we can write the action of  $\mathcal{E}^{-1} \circ \mathcal{E}$  as

$$\mathcal{E}^{-1} \circ \mathcal{E}(\rho) = \sum_i \mathcal{K}_i \rho \mathcal{K}_i^\dagger, \quad (264)$$

---

<sup>21</sup>The inverse quantum channel will end up being unique if it exists, hence the notation  $\mathcal{E}^{-1}$  is justified.

where  $i$  runs over all tuples  $(a, \mu)$  and  $\mathcal{K}_{(a, \mu)} \equiv \tilde{\mathcal{K}}_\mu \mathcal{K}_a$  are Kraus operators due to the normalization conditions on  $\mathcal{K}_a, \tilde{\mathcal{K}}_\mu$ . Now  $\mathcal{E}^{-1} \circ \mathcal{E}$  can also obviously be written in terms of the single Kraus operator  $\mathbf{1}$ . Then because of the result of a previous diary entry showing that any two Kraus representations are unitarily related (i.e.  $\mathcal{K} = U\mathcal{K}_1$ , where  $\mathcal{K}$  and  $\mathcal{K}_1$  are both  $|a||\mu|$ -length vectors, with all but one of the entries in  $\mathcal{K}_1$  equal to zero, and with  $U$  unitary), we must have

$$\mathcal{K}_i \propto \mathbf{1} \ \forall i \implies \mathcal{K}_a \tilde{\mathcal{K}}_\mu = \lambda_{a\mu} \mathbf{1} \ \forall a, \mu, \quad \lambda_{a\mu} \in \mathbb{C}. \quad (265)$$

We can now use this to show that  $\mathcal{K}_a \mathcal{K}_b^\dagger \propto \mathbf{1}$  for all  $a, b$ . Indeed, we have

$$\mathcal{K}_a = \sum_\mu \tilde{\mathcal{K}}_\mu^\dagger \tilde{\mathcal{K}}_\mu \mathcal{K}_a = \sum_\mu \tilde{\mathcal{K}}_\mu^\dagger \lambda_{\mu a}. \quad (266)$$

Now multiply on both sides by  $\mathcal{K}_b^\dagger$  and use (265):

$$\mathcal{K}_a \mathcal{K}_b^\dagger = \sum_\mu \tilde{\mathcal{K}}_\mu^\dagger \mathcal{K}_b^\dagger \lambda_{\mu a} = \sum_\mu \lambda_{\mu a} \lambda_{\mu b}^* \mathbf{1}. \quad (267)$$

The same argument shows that  $\tilde{\mathcal{K}}_\mu \tilde{\mathcal{K}}_\nu^\dagger \propto \mathbf{1}$ . If we set  $a = b$  in the above, we get

$$\mathcal{K}_a \mathcal{K}_a^\dagger = c_a \mathbf{1}, \quad (268)$$

where  $c_a > 0$  is a positive constant (must be non-zero since  $\mathcal{K}_a \neq 0$  and  $\mathcal{K}_a \mathcal{K}_a^\dagger$  is positive). Therefore we must have  $\mathcal{K}_a = \sqrt{c_a} U_a$ , where  $U_a$  is unitary.

Now look at  $a \neq b$ . Since all the  $\mathcal{K}_a$ s are proportional to unitary matrices, we must have  $\mathcal{K}_a \mathcal{K}_b^\dagger \neq 0$ . But then we see that  $\mathcal{K}_b$  is proportional to  $U_a$  for any pair  $a, b$ . This is only possible if all of the  $\mathcal{K}_a$  are proportional to a single unitary matrix  $U$ . But then they are all linearly dependent, and hence there is really only a single Kraus operator given by  $U$ .

Hence any invertible quantum channel acts on density matrices by conjugating them with a unitary, as claimed. We will call such a channel a "unitary channel".<sup>22</sup>

□

Note that we have defined the inverse channel  $\mathcal{E}^{-1}$  by requiring that  $\mathcal{E}^{-1} \circ \mathcal{E}$  is the identity superoperator. With this definition, the only channels with inverses are unitary ones. However, it is certainly often possible to invert the action of a non-unitary channel on *specific* density matrices — that is, we can often construct a recovery channel (the Petz recovery map)  $\mathcal{R}_{\rho, \mathcal{E}}$  such that  $(\mathcal{R}_{\rho, \mathcal{E}} \circ \mathcal{E})(\rho) = \rho$ . Indeed, this is possible if  $\mathcal{E}(\rho)$  is invertible, for then we may take

$$\mathcal{R}_{\rho, \mathcal{E}}(\cdot) = \sum_a \mathcal{K}_a^{\mathcal{R}}(\cdot) (\mathcal{K}_a^{\mathcal{R}})^\dagger, \quad \mathcal{K}_a^{\mathcal{R}} = \sqrt{\rho} \mathcal{K}_a^\dagger \mathcal{E}(\rho)^{-1/2} \quad (269)$$

<sup>22</sup>This is standard but slightly misleading terminology — in particular, a channel whose Kraus operators are all unitary will generically not be a unitary channel (although we also wouldn't really want to call this kind of channel unitary, since we can generically always re-write the Kraus operators in a different non-unitary form).



where the  $\mathcal{K}_a^\dagger$ s are needed if we want to consider channels  $\mathcal{E} : \text{End}(\mathcal{H}_A) \rightarrow \text{End}(\mathcal{H}_B)$  with  $\mathcal{H}_A \not\cong \mathcal{H}_B$  (note that  $\mathcal{R}_{\rho, \mathcal{E}}$  is CPTP because of the above Kraus representation).

As mentioned above, it is possible to have quantum channels which are invertible as linear operators, but not as quantum channels. An example of this is the depolarizing channel  $\mathcal{D}_p$  on a single qubit, which conjugates by each Pauli matrix with probability  $p/3$  and acts as  $\mathbf{1}$  with probability  $1 - p$ :

$$\mathcal{D}_p : \rho \mapsto (1 - p)\rho + \frac{p}{3} \sum_j \sigma_j \rho \sigma_j, \quad (270)$$

where  $p \leq 3/4$  (for positivity reasons). Let us parametrize  $\rho$  as  $\rho = \frac{1}{2}(\mathbf{1} + \mathbf{v} \cdot \boldsymbol{\sigma})$ . Then some easy algebra shows that

$$\mathcal{D}_p(\rho) = \frac{1}{2}(\mathbf{1} + (1 - 4p/3)\mathbf{v} \cdot \boldsymbol{\sigma}). \quad (271)$$

This can therefore be inverted by the application of the map  $\mathcal{D}_q$ , where

$$q = \frac{p}{4p/3 - 1}. \quad (272)$$

Hence  $\mathcal{D}_p$  is invertible as a linear operator, in that  $\mathcal{D}_p \circ \mathcal{D}_q(\rho) = \rho$  for any  $\rho$ . However,  $\mathcal{D}_q$  is not positive. For example, take a density matrix which in the above parametrization has  $v = 1$ ; such a density matrix is positive. However, we see that the spectrum of  $\mathcal{D}_q(\rho)$  is

$$\text{Eig}(\mathcal{D}_q(\rho)) = \frac{1 \pm (1 - 4q/3)}{2}, \quad (273)$$

which is not positive since  $1 - 4q/3 = \frac{1}{1 - 4p/3} > 1$ . Hence  $\mathcal{D}_q$  is not a quantum channel.

The proof that  $\mathcal{D}_p$  is equivalent to unitary time evolution breaks down in this case because while  $\mathcal{D}_q = \mathcal{D}_p^{-1}$  is trace-preserving and has an operator-sum representation, its lack of complete positivity means that the operators in its operator sum representation can not be used to establish the unitary equivalence between  $\mathbf{1}$  and the  $\mathcal{K}_a \tilde{\mathcal{K}}_\mu$  operators which was used in the above proof.

## Abstract approach

This approach comes in two parts. First, we will prove that any  $\mathcal{E}$  which is invertible as a quantum channel is necessarily a homomorphism, so that  $\mathcal{E}$  is in fact an endomorphism of  $\text{End}(\mathcal{H}_A)$ . Next, we will show that all such endomorphisms can be realized by conjugating with a unitary matrix.

**Theorem 2.** *Suppose  $\mathcal{E}$  is invertible as a quantum channel. Then  $\mathcal{E}$  is a homomorphism on  $\text{End}(\mathcal{H}_A)$ .<sup>23</sup>*

<sup>23</sup>By homomorphism we really mean a  $*$ -homomorphism of  $C^*$  algebras, i.e. that

$$\mathcal{E}(X^\dagger Y) = \mathcal{E}(X)^\dagger \mathcal{E}(Y), \quad X, Y \in \text{End}(\mathcal{H}_A). \quad (274)$$

Note that a generic quantum channel will *not* satisfy this property. If we have written elsewhere in this diary that a generic quantum channel  $\mathcal{N}$  is an element of  $\text{Hom}(\text{End}(\mathcal{H}_A), \text{End}(\mathcal{H}_B))$ , the Hom is with respect to addition, i.e. it just means that  $\mathcal{N}$  is linear.

*Proof.* As pointed out above, the fact that both  $\mathcal{E}$  and  $\mathcal{E}^{-1}$  are quantum channels is crucial; without this assumption the theorem is not true. Therefore our proof must make use of the complete positivity of both  $\mathcal{E}$  and  $\mathcal{E}^{-1}$  (recall this means that both  $\mathcal{E}$  and  $\mathcal{E}^{-1}$  map positive operators to positive operators [but that e.g.  $\mathcal{E}(X)$  needn't be positive if  $X$  isn't]).

We will need to use a special case of the CS inequality on  $C^*$  algebras. This states that if  $\mathcal{M}$  is any completely positive linear functional of  $C^*$  algebras, then

$$|\mathcal{M}(X^\dagger Y)|^2 \leq \mathcal{M}(X^\dagger X) \mathcal{M}(Y^\dagger Y), \quad (275)$$

where here the  $\leq$  is in the sense of operators, i.e.

$$X \geq Y \implies \langle (X - Y)v | v \rangle \geq 0 \quad (276)$$

for all vectors  $v$ . This is proved in essentially the same way as normal CS; see e.g. [2]. If we take  $Y = \mathbf{1}$ , we get

$$\mathcal{M}(X^\dagger X) \geq \mathcal{M}(X)^\dagger \mathcal{M}(X), \quad (277)$$

for any completely positive unital  $\mathcal{M}$ . The assumption of unitality here is valid because of the following lemma:

**Lemma 2.** If  $\mathcal{E}$  is invertible as a quantum channel,  $\mathcal{E}$  is unital.

<proof of lemma>

This follows from the positivity of  $\mathcal{E}$  and  $\mathcal{E}^{-1}$ . Suppose  $\mathcal{E}(\mathbf{1}) = \sigma \neq \mathbf{1}$  for some density matrix  $\sigma$ . Then by invertibility, we must have  $\mathcal{E}^{-1}(\sigma) = \mathbf{1}$  as well as  $\mathcal{E}^{-1}(\mathbf{1}) \neq \mathbf{1}$ . If

</proof of lemma>

Now consider the action of  $\mathcal{E}^{-1} \circ \mathcal{E}$  on  $X^\dagger X$ : by (275), and since both  $\mathcal{E}$  and  $\mathcal{E}^{-1}$  are completely positive and unital,

$$X^\dagger X \geq \mathcal{E}(\mathcal{E}^{-1}(X)^\dagger \mathcal{E}^{-1}(X)) \geq \mathcal{E} \circ \mathcal{E}^{-1}(X)^\dagger \cdot \mathcal{E} \circ \mathcal{E}^{-1}(X) = X^\dagger X. \quad (278)$$

Hence the two  $\geq$ s are actually  $=$ s, and so  $\mathcal{E}$  at least acts as a homomorphism on certain elements in the image of  $\mathcal{E}^{-1}$ .

Now we make use of the positivity of  $\mathcal{E}^{-1}$ . Define the ‘coboundary’  $\delta\mathcal{E}$  by

$$\delta\mathcal{E}(X, Y) \equiv \mathcal{E}(X^* Y) - \mathcal{E}(X)^* \mathcal{E}(Y). \quad (279)$$

By (275),  $\delta\mathcal{E}(X, X)$  is a positive operator for any  $X$ . Therefore by the positivity of  $\mathcal{E}^{-1}$  we must have

$$0 \leq \text{Tr} [\mathcal{E}^{-1}(\delta\mathcal{E}(X, X))], \quad (280)$$

with equality only if  $\delta\mathcal{E}(X, X) = 0$  identically. But from (278) we see that the argument of the trace is indeed zero, and the inequality is saturated. Therefore we must in fact have  $\delta\mathcal{E}(X, X) = 0$  for all  $X$ .

Now we want to show that this implies  $\delta\mathcal{E}(X, Y) = 0$  for all  $X, Y$ . First, we use linearity to expand the equality  $\delta\mathcal{E}(X + iY, X + iY) = 0$ . Then using  $\delta\mathcal{E}(X, X) = \delta\mathcal{E}(Y, Y) = 0$ , we obtain

$$\delta\mathcal{E}(X, Y) = \delta\mathcal{E}(Y, X), \quad (281)$$

so that  $\delta\mathcal{E}$  is symmetric in its arguments. Now  $\delta\mathcal{E}$  is anti-linear in its first argument and linear in the second. Therefore we both have  $\delta\mathcal{E}(iX, Y) = -i\delta\mathcal{E}(X, Y)$  and  $\delta\mathcal{E}(iX, Y) = \delta\mathcal{E}(Y, iX) = i\delta\mathcal{E}(Y, X) = i\delta\mathcal{E}(X, Y)$ . This is only possible if in fact  $\delta\mathcal{E}(X, Y) = 0$ , completing the proof.  $\square$

Now for the second part of the proof; after proving this we clearly are done. The result we need is the following theorem:

**Theorem 3.** *Suppose  $\mathcal{E}$  is a homomorphism<sup>24</sup> on  $\text{End}(\mathcal{H}_A)$ . Then  $\mathcal{E}$  acts by conjugation with a unitary matrix:*

$$\mathcal{E} : X \mapsto UXU^\dagger, \quad (282)$$

for some  $U \in U(\dim \mathcal{H}_A)$ .

*Proof.* The proof proceeds by looking at the action of  $\mathcal{E}$  on the matrices  $E_{ij} = |i\rangle\langle j|$ . Define  $\mathbf{E}_{ij} = \mathcal{E}(E_{ij})$ . Then since  $\mathcal{E}$  is a homomorphism,

$$\mathbf{E}_{ij}\mathbf{E}_{kl} = \delta_{jk}\mathbf{E}_{il}. \quad (283)$$

Therefore  $\mathcal{E}$  maps the mutually orthogonal projectors  $E_{ii}$  to another set of mutually orthogonal projectors. Since the  $\mathbf{E}_{ii}$  are mutually orthogonal and since  $\mathcal{E}(\sum_i E_{ii}) = \mathbf{1} \implies \sum_i \mathbf{E}_{ii} = \mathbf{1}$ , if we can show that none of the  $\mathbf{E}_{ii}$  vanish, we will have shown that  $\mathbf{E}_{ii} = |\tilde{i}\rangle\langle\tilde{i}|$  for some orthonormal basis  $|\tilde{i}\rangle$ . In fact, we can easily argue that none of the  $\mathbf{E}_{ij}$  vanish. This is because we can write any given  $E_{ij}$  as a product which includes all the other  $E_{ij}$ s; for example  $E_{12} = E_{12}E_{22}E_{23}E_{33}E_{34}\cdots$ . Therefore if  $\mathbf{E}_{ij} = 0$  for any  $i, j$ , we must in fact have  $\mathbf{E}_{ij} = 0$  for *all*  $i, j$ , which is a contradiction. Hence all the  $\mathbf{E}_{ii}$  are indeed  $|\tilde{i}\rangle\langle\tilde{i}|$ . This means that we must have

$$\mathcal{E} : E_{ij} \mapsto UE_{ij}U^\dagger, \quad U = \sum_i |\tilde{i}\rangle\langle i|. \quad (284)$$

Since the matrix  $U$  is a change of basis between two orthonormal bases, it is a unitary.  $\square$

Note that it was important that we required  $\mathcal{E}$  to be a homomorphism on *all* the linear operators on  $\mathcal{H}_A$ . For example, suppose we restricted our attention just to the action of  $\mathcal{E}$  on e.g.  $GL(\dim \mathcal{H}_A, \mathbb{C})$ . Then it is no longer the case that  $\mathcal{E}$  being a homomorphism implies it is realized by unitary conjugation. As an example of such a homomorphism, consider the map

$$\mathcal{N} : \rho \mapsto (\rho^{-1})^T. \quad (285)$$

This is a homomorphism since

$$\mathcal{N}(\rho\sigma) = (\sigma^{-1}\rho^{-1})^T = (\rho^{-1})^T(\sigma^{-1})^T. \quad (286)$$

Furthermore it cannot be an inner automorphism, since it acts non-trivially on  $\lambda\mathbf{1}$  for  $\lambda \neq 1$ , and  $\lambda\mathbf{1} \in Z(GL(\dim \mathcal{H}_A, \mathbb{C}))$  (this is just an explicit way of saying that  $\text{Out}(GL(n, \mathbb{C}))$  is nontrivial).

<sup>24</sup>Again, here by ‘homomorphism’ we really mean ‘\*-homomorphism’.



## Minimal uncertainty states

Today we will be proving a very simple result that I don't remember seeing in my undergrad QM books. Let  $A$  and  $B$  be two self-adjoint operators. Then any state  $\psi$  for which the uncertainty relation between  $A$  and  $B$  is saturated is either an eigenstate of  $A$ , an eigenstate of  $B$ , or an eigenstate of the “annihilation operator”  $A - i\gamma B$  for some  $\gamma \in \mathbb{R}$ , and as such is a “coherent state”.



Recall how the proof of the uncertainty relation works. Define  $\bar{A} \equiv A - \langle A \rangle$ ,  $\bar{B} \equiv B - \langle B \rangle$ , where the expectation values are taken in the state  $\psi$ . Then from the CS inequality,

$$\begin{aligned}
 \sigma_A^2 \sigma_B^2 &= |\bar{A}|\psi\rangle| \cdot |\bar{B}|\psi\rangle| \\
 &\geq |\langle \psi | \bar{A} \bar{B} | \psi \rangle|^2 \\
 &\geq |\operatorname{Im} \langle \psi | \bar{A} \bar{B} | \psi \rangle|^2 \\
 &= \frac{1}{4} |\langle \psi | \bar{A} \bar{B} - \bar{B} \bar{A} | \psi \rangle|^2
 \end{aligned} \tag{287}$$

so that

$$\sigma_A \sigma_B \geq \frac{1}{2} |\langle \psi | [A, B] | \psi \rangle|. \tag{288}$$

Now consider what we would need to happen for the two inequalities above to be saturated. We claim that this happens iff  $\psi$  is an eigenstate of  $A$ ,  $B$ , or  $A - i\gamma B$ ,  $\gamma \in \mathbb{R}$ .

To prove the if part, suppose  $A|\psi\rangle = \lambda|\psi\rangle$ . Then  $\bar{A}|\psi\rangle = 0$ , and the inequalities are both trivially satisfied. The same thing holds if  $|\psi\rangle$  is an eigenstate of  $B$ . Suppose instead that  $(A - i\gamma B)|\psi\rangle = \lambda|\psi\rangle$ . We then see that

$$\bar{A}|\psi\rangle = i\gamma \bar{B}|\psi\rangle. \tag{289}$$

The CS inequality used in the second line is then saturated, since  $\bar{A}|\psi\rangle$  is parallel to  $\bar{B}|\psi\rangle$ . Since

$$\langle \psi | \bar{A} \bar{B} | \psi \rangle = i\gamma \langle \psi | \bar{B}^2 | \psi \rangle, \tag{290}$$

we see that the second inequality is saturated provided that  $\gamma \in \mathbb{R}$ .

The only if part is similarly easy. The CW inequality is saturated only if  $\bar{A}|\psi\rangle = \alpha \bar{B}|\psi\rangle$  for some  $\alpha \in \mathbb{C}$ . In order for the second inequality to be satisfied we must then have  $\alpha \in i\mathbb{R}$ , since  $\langle \psi | \bar{B} \bar{B} | \psi \rangle \in \mathbb{R}$  by virtue of the Hermiticity of  $\bar{B}$ . Letting  $\alpha = i\gamma$  for  $\gamma \in \mathbb{R}$ , this means that

$$\langle \psi | (\bar{A} - i\gamma \bar{B}) | \psi \rangle = 0 \implies (A - i\gamma B)|\psi\rangle = \lambda|\psi\rangle, \tag{291}$$

with  $\lambda = \langle A \rangle - i\gamma \langle B \rangle$ . Thus  $|\psi\rangle$  is an eigenstate of  $A - i\gamma B$  for  $\gamma \in \mathbb{R}$ . This argument breaks down only if  $\bar{A}$  or  $\bar{B}$  annihilate  $|\psi\rangle$ , in which case  $|\psi\rangle$  is an eigenstate of  $A$  or  $B$ . This is what we wanted to show.

The canonical example is the case where  $A = X$ ,  $B = P$ . Because of issues related to boundedness which we didn't get into above, eigenstates of  $X$  and  $P$  don't count as minimal uncertainty states. Eigenstates of  $a_\gamma \equiv X - i\gamma P$  do count, though. Now if  $\psi$  is an eigenstate of  $a_\gamma$ , then

$$a_\gamma \psi = (x - \gamma \partial_x) \psi = \lambda \psi \quad (292)$$

is satisfied if  $\psi$  is the Gaussian wavepacket

$$\psi(x) = e^{-(x-x_0)^2 \alpha/2} e^{ipx}, \quad (293)$$

with  $\alpha = -1/\gamma$  and  $\lambda = x_0 - ip\gamma$ .



## Useful relations for Fock space bilinears

---

Today's entry isn't anything special—we will just be listing a few useful relations involving creation / annihilation operators that will be useful to have for future reference. All derivations are done with simple algebra and as such will be omitted.



Throughout we will let  $a_i, a_j^\dagger$  denote creation / annihilation operators on some Fock space. We will mostly be interested in relations involving bilinears in the Fock space operators, which will not care about whether the  $a_i$  are bosonic or fermionic. Hats will denote operators, with uppercase letters being bilinears and lowercase being vectors, so that e.g.

$$\hat{A} = a_i^\dagger A_{ij} a_j, \quad \hat{v} = v \cdot a, \quad \hat{v}^\dagger = a^\dagger \cdot v, \quad (294)$$

etc. Note how the  $\dagger$  on  $\hat{v}$  only sends  $a \mapsto a^\dagger$ ; in this diary entry it will not act as  $\mathcal{K}$  on scalars. For  $\hat{A}, \hat{v}$  as above, one has

$$[\hat{A}, \hat{v}] = (v^T A) \cdot a, \quad [\hat{A}, \hat{v}^\dagger] = (Av) \cdot a^\dagger. \quad (295)$$

For two bilinears  $\hat{A} = a^\dagger A a$ ,  $\hat{B} = a^\dagger B a$  (in what follows the matrix  $A$  will always be Hermitian), one finds

$$[\hat{A}, \hat{B}] = a^\dagger [A, B] a. \quad (296)$$

Let  $\hat{\mathcal{B}} = a_i \mathcal{B}_{ij} a_j$  and  $\hat{\mathcal{B}}' = a_i^\dagger \mathcal{B}'_{ij} a_j^\dagger$ . Then we have

$$[\hat{A}, \hat{\mathcal{B}}] = -a^T (\mathcal{B}A + A^T \mathcal{B})a, \quad [\hat{A}, \hat{\mathcal{B}}'] = a^\dagger (A\mathcal{B}' + \mathcal{B}'A^T)(a^\dagger)^T. \quad (297)$$

We can also use these relations to find out how unitary conjugation acts on vectors / bilinears of second quantized operators. First recall that for any operators  $\mathcal{M}, \mathcal{N}$ ,

$$e^{\mathcal{M}} \mathcal{N} e^{-\mathcal{M}} = \mathcal{N} + [\mathcal{M}, \mathcal{N}] + \frac{1}{2}[\mathcal{M}, [\mathcal{M}, \mathcal{N}]] + \dots \quad (298)$$

One then shows that for  $\hat{U} = e^{i\theta_\alpha \hat{A}^\alpha}$  with  $\hat{A}^\alpha = a_i^\dagger A_{ij}^\alpha a_j$ ,

$$\hat{U} \hat{v} \hat{U}^\dagger = (v^T U) \cdot a, \quad \hat{U} \hat{v}^\dagger \hat{U}^\dagger = (Uv) \cdot a^\dagger, \quad (299)$$

while for  $\hat{B}$  as before,

$$\hat{U} \hat{B} \hat{U}^\dagger = a^\dagger (U B U^\dagger) a. \quad (300)$$

For  $\hat{\mathcal{B}}$  and  $\hat{\mathcal{B}}'$ ,

$$\hat{U} \hat{\mathcal{B}} \hat{U}^\dagger = a^T (e^{-iA^T} \mathcal{B} e^{-iA}) a, \quad \hat{U} \hat{\mathcal{B}}' \hat{U}^\dagger = a^\dagger (e^{iA} \mathcal{B}' e^{iA^T}) (a^\dagger)^T. \quad (301)$$

As an example of the utility of formula like the last one, consider the action of  $SU(2)$  spin rotations on the operator  $\hat{\mathcal{B}}' = c_{1\uparrow}^\dagger c_{2\downarrow}^\dagger + \eta c_{1\downarrow}^\dagger c_{2\uparrow}^\dagger$ , where  $\eta = \pm 1$  and 1, 2 label two sites. In the basis  $|\text{site} \otimes \text{spin}\rangle$ ,  $\mathcal{B}' = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}$ , where  $M = \begin{pmatrix} 0 & 1 \\ \eta & 0 \end{pmatrix}$ . Then for a spin rotation which acts as  $e^{i\theta_\alpha \sigma^\alpha / 2}$ , we have

$$\mathcal{B}' \mapsto (e^{i\theta_\alpha \sigma^\alpha / 2})^{\oplus 2} \mathcal{B}' (e^{i(\theta_\beta \sigma^\beta)^T / 2})^{\oplus 2} \equiv \begin{pmatrix} 0 & \widetilde{M} \\ 0 & 0 \end{pmatrix}. \quad (302)$$

For  $\eta = +1$ , we find

$$\widetilde{M}_{\eta=1} = e^{i\theta_x X + i\theta_y Y}, \quad (303)$$

while for  $\eta = -1$  we find

$$\widetilde{M}_{\eta=-1} = \widetilde{M}. \quad (304)$$

We therefore confirm that the state  $\hat{\mathcal{B}}'|0\rangle$  transforms as a vector if  $\eta = +1$  and as a scalar if  $\eta = -1$ .



## How Bogoliubov transformations act on states and normal ordering of squeeze operators

---

In today's entry we will discuss an aspect of Bogoliubov transformations (aka canonical transformations) that is not covered systematically in any of the books I own: how they act on states. Along the way we will get some practice with normal-ordering the operators that create squeezed states. These results are well-known in the quant-ph literature, but I was not able to find a sufficiently verbose derivation that I could understand anywhere. This diary entry should therefore just be viewed as a discussion explaining where the formulae quoted in the literature come from.

▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼

Suppose we are interested in a problem defined on a Hilbert space  $\mathcal{H}$ , which is acted on by the creation / annihilation operators  $a_\lambda^\dagger, a_\lambda$ , with  $\lambda$  a flavor index. Define the operator  $\mathbf{a} \equiv \bigoplus_\lambda (a_\lambda, a_\lambda^\dagger)^T$ , which is a vector of operators of length  $2|\{\lambda\}|$ . One part of a Bogoliubov transformation (BT) is a canonical transformation on  $\mathbf{a}$ , viz. one that sends

$$BT : \mathbf{a} \mapsto V \mathbf{a}, \quad V^\dagger (\mathbf{1} \otimes C) V = \mathbf{1} \otimes C, \quad (305)$$

where  $C = Z$  if the particles destroyed by  $a_\lambda$  are bosons, and  $C = \mathbf{1}_2$  if they are fermions (the condition on  $V$  ensures that the C(A)CR are preserved).

Now if  $V$  is of the form  $V_f \otimes \mathbf{1}_2$ , the BT acts on operators by unitary conjugation. However if it exchanges creation and annihilation operators then the action on operators *cannot* be that of conjugation by a unitary matrix. This then raises the question of how BTs act on states,<sup>25</sup> since we know that the action on states should be that of a unitary matrix.

To understand how to derive the action on states, we will restrict our attention to a single flavor of bosons, so that the allowed BTs are defined by a  $2 \times 2$  determinant-1 matrix  $V$  satisfying  $V^\dagger Z V = Z$ , viz. by the group  $SU(1, 1)$ . As with  $SU(2)$ , any matrix in  $SU(1, 1)$  can be parametrized in terms of two complex numbers  $z, w$ , with

$$V = \begin{pmatrix} z & w \\ w^* & z^* \end{pmatrix}, \quad |z|^2 - |w|^2 = 1. \quad (306)$$

Since the overall phase of  $V$  is redundant, we may thus write  $V$  in terms of a real number  $\theta$  and a  $U(1)$  phase  $\zeta$  as

$$V = \begin{pmatrix} \cosh \theta & \zeta \sinh \theta \\ \zeta^* \sinh \theta & \cosh \theta \end{pmatrix}. \quad (307)$$

---

<sup>25</sup>Of course we know how they act on states: states transform in the “adjoint representation”, viz.  $|\psi\rangle \mapsto \mathcal{U}|\psi\rangle$ , where  $\mathcal{U}^\dagger \mathbf{a} \mathcal{U} = V \mathbf{a}$ . The challenge is to find  $\mathcal{U}$  in terms of  $V$ .

### Action on the vacuum

Let us first ask how the vacuum is mapped under the BT  $V$ . The new vacuum  $|\tilde{0}\rangle$  should satisfy  $\tilde{a}|\tilde{0}\rangle = 0$ , where  $\tilde{a} \equiv c_\theta a + \zeta s_\theta a^\dagger$  is the transformed annihilation operator and  $c_\theta \equiv \cosh \theta$ ,  $s_\theta \equiv \sinh \theta$ . Writing  $|\tilde{0}\rangle = \sum_n \alpha_n |n\rangle$ , some algebra shows that

$$\frac{\alpha_{n+1}}{\alpha_{n-1}} = -\zeta t_\theta \sqrt{\frac{n}{n+1}}, \quad \alpha_1 = 0, \quad (308)$$

where  $t_\theta \equiv \tanh(\theta)$ . This gives

$$|\tilde{0}\rangle = \alpha_0 \sum_{n=0}^{\infty} (t_\theta \zeta)^n \sqrt{\frac{(2n-1)!!}{(2n)!!}} |2n\rangle. \quad (309)$$

Note in particular that the new vacuum is not built out of combinations of coherent states, and contains only states of *even* boson number (this can be anticipated by re-reading the diary entry on thermofield dynamics). Using  $(2n)!! = 2^n n!$  and  $|2n\rangle = (a^\dagger)^{2n} |0\rangle / \sqrt{(2n)!}$ , some algebra then lets us write

$$|\tilde{0}\rangle = \alpha_0 e^{\frac{\zeta t_\theta}{2} (a^\dagger)^2} |0\rangle, \quad (310)$$

with  $\alpha_0$  determined by normalization. We have

$$\begin{aligned} |\langle \tilde{0} | \tilde{0} \rangle|^2 &= \alpha_0^2 \sum_{n=0}^{\infty} (t_\theta/2)^{2n} \frac{(2n)!}{(n!)^2} \\ &= \alpha_0^2 \sum_{n=0}^{\infty} \frac{(t_\theta)^{2n}}{2^n} \frac{(2n-1)!!}{n!} \\ &= \frac{\alpha_0^2}{\sqrt{1 - (t_\theta)^2}}, \end{aligned} \quad (311)$$

so that

$$|\tilde{0}\rangle = c_\theta^{-1/2} e^{\frac{\zeta t_\theta}{2} a^\dagger a^\dagger} |0\rangle. \quad (312)$$

### General action

To determine the action on general states, strictly speaking one can proceed as above, by solving  $\tilde{a}^m |\tilde{m}\rangle = 0$ . This however involves rather heinous normal-ordering manipulations of the expansion of  $\tilde{a}^m$  and the commutation of these terms through the exponential in the above expression for  $|\tilde{0}\rangle$ .

A better strategy is to simply guess the form of the unitary based on the above expression for  $|\tilde{0}\rangle$ . To do this, it helps to first recall some things about coherent states. The usual way of writing down a coherent state on which  $a$  acts as  $\alpha$  is to write

$$(a - \alpha)|\alpha\rangle = 0 \implies \left( \frac{\delta}{\delta a^\dagger} - \alpha \right) |\alpha\rangle = 0 \implies |\alpha\rangle = e^{\alpha a^\dagger - |\alpha|^2/2} |0\rangle, \quad (313)$$



where the  $e^{-|\alpha|^2/2}$  comes from normalization. This is just how one obtains the coherent state  $|\alpha\rangle$ , but in the present context it is more helpful to think of this as a shift map which sends  $a \mapsto a - \alpha$ ,  $a^\dagger \mapsto a^\dagger - \alpha^*$  (which of course preserves the CCR).

How should this shift map be extended to an action on all states? Of course it cannot simply be via the operator  $e^{\alpha a^\dagger - |\alpha|^2/2}$ , which is not unitary. However, using the BCH formula we may write

$$e^{\alpha a^\dagger - |\alpha|^2/2} |0\rangle = e^{\alpha a^\dagger - \alpha^* a} |0\rangle \equiv D(\alpha), \quad (314)$$

where  $D(\alpha)$  is known as the “displacement operator”.  $D(\alpha)$  is unitary, and it is natural to guess that  $D(\alpha)$  is the correct unitary action on all states. This can be checked by observing that conjugation by  $D(\alpha)$  implements the desired shift on  $a$ :

$$D(\alpha) a D(\alpha)^\dagger = e^{\alpha a^\dagger} a e^{-\alpha a^\dagger} = a + e^{\alpha a^\dagger} [a, e^{-\alpha a^\dagger}] = a - \alpha. \quad (315)$$

The reason why the above comments about coherent states are useful is that the Bogoliubov ground state is essentially a coherent state of boson pairs (think about the BCS wavefunction), and we can use essentially the same strategy as above to guess the unitary that acts on the states. In particular, a bit of playing around shows that the natural guess<sup>26</sup> is the unitary

$$\mathcal{U}_{\theta, \zeta} = e^{\frac{\theta}{2}(\zeta a^\dagger a^\dagger - \zeta^* a a)}, \quad (317)$$

which is basically a coherent state of boson pairs (a “squeezed state”, because the matrix  $V$  implements a squeezing of phase space). The first sanity check on this is that it obeys the composition law

$$\mathcal{U}_{\theta, \zeta} \mathcal{U}_{\theta', \zeta} = \mathcal{U}_{\theta+\theta', \zeta} \quad (318)$$

which is a requirement based on the multiplication law of the matrices in (307).

As another sanity check (the only other one we will perform), we can see whether or not the action of  $\mathcal{U}_{\theta, \zeta}$  reduces to that of  $c_\theta^{-1/2} e^{t_\theta \zeta a^\dagger a^\dagger}$  when acting on  $|0\rangle$ . To do this, we need to normal-order  $\mathcal{U}_{\theta, \zeta}$ , which is a fun exercise whose solution turns out to be useful in other contexts.

### Normal-ordering $\mathcal{U}_{\theta, \zeta}$

The easiest way to normal-order  $\mathcal{U}_{\theta, \zeta}$  seems to be as follows. First, note that  $[aa, a^\dagger a^\dagger] = 4a^\dagger a + 2$  implies that the operators

$$\sigma^+ \equiv \frac{a^\dagger a^\dagger}{2}, \quad \sigma^- \equiv (\sigma^+)^\dagger, \quad \sigma^z \equiv a^\dagger a - \frac{1}{2} \quad (319)$$

satisfy the commutation relations

$$[\sigma^+, \sigma^-] = -\sigma^z, \quad [\sigma^z, \sigma^\pm] = 2\sigma^\pm, \quad (320)$$

<sup>26</sup>Since we want to send  $a$  to  $c_\theta a + \zeta s_\theta a^\dagger$ , we want something like

$$\exp \left( [(c_\theta - 1)a + \zeta s_\theta a^\dagger] \frac{\delta}{\delta a} + [(c_\theta - 1)a^\dagger + \zeta^* s_\theta a] \frac{\delta}{\delta a^\dagger} \right), \quad (316)$$

which is close in spirit to the above guess.

which are those of the  $su(1, 1)$  Lie algebra.<sup>27</sup> As usual in these kinds of problems, it helps to realize that Lie group multiplication rules can be worked out using any representation of the Lie algebra. This means that when manipulating exponentials of  $\sigma^\pm$  and  $\sigma^z$ , we are free to use any matrix representation of the  $su(1, 1)$  Lie algebra — in particular, we may simply use the spin 1/2 representation (obtained from the spin 1/2 representation of  $su(2)$  simply by multiplying  $X, Y$  by  $i$ ), where the exponentials are easy to work out.<sup>28</sup>

We will first massage our guess for  $\mathcal{U}_{\theta, \zeta}$  into a form that seems to appear most often in the literature, writing

$$\mathcal{U}_{\theta, \zeta} = e^{\alpha \sigma^-} e^{\Lambda \sigma^z} e^{-\alpha^* \sigma^+}, \quad (321)$$

where  $\alpha, \Lambda$  are constants to be determined. We relate these constants to  $\theta, \zeta$  by using the Pauli matrix relation

$$e^{\mathbf{u} \cdot \boldsymbol{\sigma}} = \cosh(u) + \frac{\mathbf{u} \cdot \boldsymbol{\sigma}}{u} \sinh(u), \quad (322)$$

where  $u = \sqrt{\mathbf{u} \cdot \mathbf{u}}$ . Using this relation on (317) and on the above ansatz, with the representation  $\sigma^\pm = (iX \mp Y)/2$ , we obtain the requirement that both

$$\mathcal{U}_{\theta, \zeta} = c_\theta - (X \operatorname{Im} \zeta + Y \operatorname{Re} \zeta) s_\theta \quad (323)$$

and

$$\mathcal{U}_{\theta, \zeta} = e^{\Lambda Z} + \frac{i}{2} e^{-\Lambda Z} (\alpha - \alpha^*) X - \frac{1}{2} e^{-\Lambda Z} (\alpha + \alpha^*) Y. \quad (324)$$

Matching these two expressions, some algebra yields

$$\Lambda = -\ln c_\theta, \quad |\alpha| = t_\theta, \quad \arg(\alpha) = \arg(\zeta). \quad (325)$$

Therefore we obtain the relation

$$e^{\frac{\theta}{2}(\zeta a^\dagger a^\dagger - \zeta^* a a)} = e^{\frac{\tanh(\theta)}{2} \zeta a^\dagger a^\dagger} [\operatorname{sech}(\theta)]^{a^\dagger a + 1/2} e^{-\frac{\tanh(\theta)}{2} \zeta^* a a}. \quad (326)$$

The RHS is still not normal-ordered due to the middle factor, but this is easy to rectify. Since the middle factor acts diagonally on the Hilbert space, we know that

$$[\operatorname{sech}(\theta)]^{a^\dagger a + 1/2} = \sum_{n=0}^{\infty} C_n (a^\dagger)^n a^n \quad (327)$$

for some coefficients  $C_n$ . These coefficients can be obtained by computing the commutator of both sides with  $a$ . The commutator with the LHS is

$$[a, e^{\Lambda(a^\dagger a + 1/2)}] = e^{\Lambda(a^\dagger a + 1/2)} (e^\Lambda - 1) a, \quad (328)$$

<sup>27</sup>It is very important here that the Lie algebra is  $su(1, 1)$  and not  $su(2)$ ; if we represent things with  $su(2)$  matrices all of the hyperbolic functions appearing in the following turn into regular trig functions. Note that we cannot just swap  $\sigma^+$  with  $\sigma^-$  to change the sign on  $[\sigma^+, \sigma^-]$ , as the definitions of  $\sigma^\pm$  are fixed from their commutation relations with  $\sigma^z$ .

<sup>28</sup>Of course we are actually interested in an infinite-dimensional representation, since e.g.  $(aa)^n$  is nontrivial for all  $n$ . Perhaps there could be some subtlety about using a finite-dimensional representation to manipulate the group elements, but since we are doing physics we will not worry about such things.

which follows from the fact that  $a$  carries a charge of negative 1, viz. from

$$e^{-\Lambda n} a e^{\Lambda n} = e^{\Lambda} a. \quad (329)$$

The commutator with the RHS on the other hand is

$$[a, \sum_{n=0} C_n (a^\dagger)^n a^n] = \left( \sum_{n=0} C_{n+1} (n+1) (a^\dagger)^n a^n \right) a. \quad (330)$$

This relation together with (328) imposes the consistency condition that

$$C_{n+1} (n+1) = (e^{\Lambda} - 1) C_n, \quad (331)$$

with the initial condition  $C_0 = e^{\Lambda/2}$ . Solving for the  $C_n$ , we then finally obtain the normal-ordered form

$$e^{\frac{\theta}{2}(\zeta a^\dagger a^\dagger - \zeta^* a a)} = e^{\frac{\tanh(\theta)}{2} \zeta a^\dagger a^\dagger} \left( \sum_{n=0}^{\infty} \frac{(\operatorname{sech}(\theta) - 1)^n}{n!} (a^\dagger)^n a^n \right) e^{-\frac{\tanh(\theta)}{2} \zeta^* a a}, \quad (332)$$

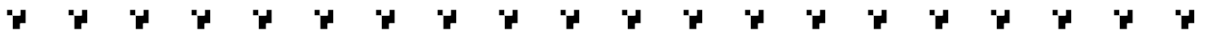
which agrees with the expression quoted in [5]. Note in particular that when evaluated on the vacuum, we recover the Bogoliubov vacuum of (312).



## 4th order perturbation theory

---

Today we will work out the expression for the 4th order correction to the ground state energy of a Hamiltonian perturbed by a Hermitian operator  $\mathcal{O}$ , where  $\mathcal{O}$  does not act in the ground state,  $\langle 0 | \mathcal{O} | 0 \rangle = 0$ . The expression we will derive can actually be found on Wikipedia, but I was not able to find a derivation. Therefore to be safe, we will work things out ourselves.



The way I like to organize perturbation theory is via a path integral flavored approach. Consider the imaginary time evolution of the perturbed system for an imaginary time  $T \rightarrow \infty$ . We may then write

$$e^{-T \sum_{i=1} E_i} = \langle e^{-\int d\tau \mathcal{O}(\tau)} \rangle, \quad (333)$$

where  $E_i$  is the  $i$ th order correction to the ground state energy, working perturbatively in powers of  $\mathcal{O}$ . By expanding both exponentials, we find to fourth order

$$\begin{aligned}\chi_1 &= E_1 T \\ \frac{1}{2}\chi_2 &= \frac{1}{2}E_1^2 T^2 - E_2 T \\ \frac{1}{6}\chi_3 &= \frac{1}{6}E_1^3 T^3 - E_1 E_2 T^2 + E_3 T \\ \frac{1}{24}\chi_4 &= \frac{1}{24}E_1^4 T^4 - \frac{1}{2}E_1^2 E_2 T^3 + E_1 E_3 T^2 + \frac{1}{2}E_2^2 T^2 - E_4 T,\end{aligned}\tag{334}$$

where we have defined

$$\chi_n \equiv \int_{\mathbb{R}} \prod_{i=1}^n d\tau_i \langle \mathcal{T}[\prod_{j=1}^n \mathcal{O}(\tau_j)] \rangle,\tag{335}$$

with  $\mathcal{T}$  denoting time ordering.

All that remains is to calculate the  $\chi_n$ . In most situations we are interested in,  $\chi_1 = 0$ .  $\chi_2$  is the familiar

$$\begin{aligned}\chi_2 &= T \sum_{l \neq 0} \int_{\mathbb{R}} d\tau (\Theta(\tau) e^{\tau E_{0l}} + \Theta(-\tau) e^{\tau E_{l0}}) |\mathcal{O}_{0l}|^2 \\ &= 2T \sum_{l \neq 0} \frac{|\mathcal{O}_{0l}|^2}{E_{0l}},\end{aligned}\tag{336}$$

where  $T$  appears as our way of regulating the integral over all times (viz.  $T = \int_{\mathbb{R}} d\tau$ ).

To derive  $\chi_3$  and  $\chi_4$ , it is helpful to define a more compact notation by writing

$$\int_{a_1}^{b_1} \cdots \int_{a_n}^{b_n} \langle p_1 \cdots p_n \rangle \equiv \int_{a_1}^{b_1} d\tau_1 \cdots \int_{a_n}^{b_n} d\tau_n \langle 0 | \mathcal{O}(\tau_{p_1}) \cdots \mathcal{O}(\tau_{p_n}) | 0 \rangle\tag{337}$$

We may then use this notation to write (after using time translation invariance to fix one of the times at 0)

$$\begin{aligned}\chi_3/T &= \int_{-\infty}^0 \left( \int_{-\infty}^1 \langle 012 \rangle + \int_1^0 \langle 021 \rangle + \int_0^\infty \langle 201 \rangle \right) + \int_0^\infty \left( \int_{-\infty}^0 \langle 102 \rangle + \int_0^1 \langle 120 \rangle + \int_1^\infty \langle 210 \rangle \right) \\ &\equiv \sum_{k,l \neq 0} \mathcal{O}_{0k} \mathcal{O}_{kl} \mathcal{O}_{l0} \sum_{i=1}^6 K_i\end{aligned}\tag{338}$$

where 1 in the integration limits means  $\tau_1$ , the integration variable of the outermost integral. In this case in fact all six terms are exactly the same:

$$K_i = \frac{1}{E_{0k} E_{0l}},\tag{339}$$

so that

$$\chi_3 = 6T \sum_{k,l \neq 0} \frac{\mathcal{O}_{0k} \mathcal{O}_{kl} \mathcal{O}_{l0}}{E_{0k} E_{0l}}.\tag{340}$$

The calculation of  $\chi_4$  is a bit more involved. There are a few easy symmetries of the integrations we can take advantage of to write

$$\begin{aligned}\chi_4/T &= 4 \int_0^\infty \left( \int_{-\infty}^0 \int_{-\infty}^2 \langle 1023 \rangle + \int_0^1 \int_{-\infty}^0 \langle 1203 \rangle + \int_0^1 \int_0^2 \langle 1230 \rangle \right. \\ &\quad \left. - \int_1^\infty \int_{-\infty}^0 \langle 2103 \rangle + \int_1^\infty \int_0^1 \langle 2130 \rangle + \int_1^\infty \int_1^2 \langle 2310 \rangle \right) \\ &\equiv 4 \sum_{k,l,m \neq 0} \mathcal{O}_{0k} \mathcal{O}_{km} \mathcal{O}_{ml} \mathcal{O}_{l0} \sum_{i=1}^6 L_i + 4 \sum_{k,l \neq 0} |\mathcal{O}_{0k}|^2 |\mathcal{O}_{0l}|^2 \sum_{i=1}^6 M_i.\end{aligned}\tag{341}$$

The  $L_i$  are in fact all the same; a straightforward calculation checks that

$$L_i = -\frac{1}{E_{0k} E_{0l} E_{0m}}.\tag{342}$$

For the  $M_i$ , we find (the subscripts defined in order of how the terms appear in the expression for  $\chi_4$  above)

$$\begin{aligned}M_1 &= M_4 = \frac{T}{2E_{0k} E_{0l}} \\ M_2 &= M_5 = \frac{1}{E_{0k} E_{0l}} \left( \frac{T}{2} + \frac{1}{E_{0k}} \right) \\ M_3 &= M_6 = \frac{T}{2E_{0l} E_{0k}} + \frac{2}{E_{0l} E_{0k}^2},\end{aligned}\tag{343}$$

where we have used symmetry in  $k \leftrightarrow l$ . Adding these up, we find

$$\chi_4 = 24T \sum_{k,l,m \neq 0} \frac{\mathcal{O}_{0k} \mathcal{O}_{km} \mathcal{O}_{ml} \mathcal{O}_{l0}}{E_{k0} E_{l0} E_{m0}} + 24T \sum_{k,l \neq 0} \frac{|\mathcal{O}_{0k}|^2 |\mathcal{O}_{0l}|^2}{E_{0k} E_{0l}} \left( \frac{1}{E_{0k}} + \frac{T}{2} \right).\tag{344}$$

Some simple algebra then leads to an expression for the energy shifts. As we are assuming  $E_1 = 0$ , we find

$$\begin{aligned}E_2 &= \sum_{l \neq 0} \frac{|\mathcal{O}_{0l}|^2}{E_{0l}} \\ E_3 &= \sum_{l,k \neq 0} \frac{\mathcal{O}_{0k} \mathcal{O}_{kl} \mathcal{O}_{l0}}{E_{0l} E_{0k}} \\ E_4 &= \sum_{k,l,m \neq 0} \frac{\mathcal{O}_{0k} \mathcal{O}_{km} \mathcal{O}_{ml} \mathcal{O}_{l0}}{E_{0k} E_{0m} E_{0l}} - E_2 \sum_{l \neq 0} \frac{|\mathcal{O}_{0l}|^2}{E_{0l}^2},\end{aligned}\tag{345}$$

which reassuringly matches the expressions on Wikipedia.



## Bounds on Pauli errors

---

In this entry we discuss some simple results about error correction schemes that are designed to protect against Pauli errors of a certain Hamming weight. (update: looks like the first part of this is just discussed in Preskill's notes — search for ‘quantum Hamming bound’)

⚡ ⚡

We will consider an error correcting code which maps  $k$  qubits into an  $n$ -qubit codeword state via the encoding map

$$\mathcal{C} : |s, 0^{n-k}\rangle \mapsto |C(s)\rangle, \quad (346)$$

where  $s \in \{0, 1\}^k$  is a binary string to be encoded and  $|C(s)\rangle$  is the appropriate codeword (which need not itself be a string in  $\{0, 1\}^n$ ). We will assume that there exists a unitary correction map  $\mathcal{S}$  on  $3n$  qubits which can identify all Pauli errors of weight  $\leq w$  (by ‘weight’ we mean Hamming weight of the operator string). Therefore we will assume that for all strings  $s \in \{0, 1\}^k$  and all weight  $w' < w$  Pauli errors  $E$ ,

$$\mathcal{S}(|EC(s)\rangle|0^{2n}\rangle) = |EC(s)\rangle|E\rangle, \quad (347)$$

where  $E$  means the binary encoding of the operator string associated with  $E$  (since the codewords are defined on  $n$  total qubits, we need  $2n$  ancillas for representing the operator strings, hence why  $\mathcal{S}$  operates on  $3n$  qubits).

If  $\mathcal{S}$  exists, then for any two errors  $E, F$ ,

$$\langle EC(s)|FC(s')\rangle = \delta_{E,F}\delta_{s,s'}. \quad (348)$$

To see this, we simply insert  $\mathcal{S}^\dagger\mathcal{S} = \mathbf{1}$  into the inner product:

$$\begin{aligned} \langle EC(s)|FC(s')\rangle &= \langle(s)|\mathcal{S}^\dagger\mathcal{S}|FC(s')\rangle \\ &= \langle F|E\rangle\langle EC(s)|FC(s')\rangle \\ &= \delta_{E,F}\langle C(s)|C(s')\rangle \\ &= \delta_{E,F}\delta_{s,s'} \end{aligned} \quad (349)$$

since the codewords of orthogonal states must themselves be orthogonal.

We can now place a lower bound on the number  $n$  of qubits needed to allow for this error correction scheme to work, as a function of  $\alpha \equiv w/n$ , the Hamming weight of the largest correctible operators as a fraction of the total system size.

We start by using the above fact (348). This says that every string  $s$  and every Pauli error of weight  $\leq w$  can be combined to yield an independent state. Since the number of states obtained in this way obviously cannot exceed  $2^n$ , we have

$$(\text{number of strings}) \cdot (\text{number of errors}) \leq 2^n, \quad (350)$$

which means that

$$n \ln 2 \geq k \ln 2 + \ln \left( \sum_{i=0}^w \binom{n}{i} 3^i \right). \quad (351)$$

Therefore we have a lower bound on  $n$  of

$$\begin{aligned} n &\geq k + \frac{1}{\ln 2} \ln \left( 3^w \binom{n}{w} \right) \\ &\approx k + n\alpha \frac{\ln 3}{\ln 2} + \frac{1}{\ln 2} (n\alpha \ln(1/\alpha - 1) - n \ln(1 - \alpha)), \end{aligned} \quad (352)$$

so that for large  $n$ ,

$$n \gtrsim \frac{k}{\ln(2 - 2\alpha) - \alpha \ln(3/\alpha - 3)}. \quad (353)$$

Note that this can be simplified in terms of the Shannon entropy  $H(\alpha)$ , but as of writing I'm not sure of the physical meaning of this.

## Codes for qudits

Today's diary entry is a compendium of solutions to a few problems in chapter 7 of Preskill's QI notes concerning stabilizer codes for qudits (we will use  $N$  rather than  $d$  for the local  $\mathcal{H}$  space dimension).

For this diary entry we will need to defined the usual suspects

$$X \equiv \sum_a |a+1\rangle\langle a|, \quad Z \equiv \sum_a \zeta^a |a\rangle\langle a|, \quad ZX = \zeta XZ, \quad (354)$$

where  $a \in \mathbb{Z}_N$  and  $\zeta \equiv e^{2\pi i/N}$ . We will also need to define

$$\mathcal{F} \equiv \sum_{a,b} \zeta^{ab} |a\rangle\langle b| \quad (355)$$

as the matrix which implements Fourier transforms.  $\mathcal{F}$  satisfies

$$Z\mathcal{F} = \mathcal{F}X, \quad X\mathcal{F} = \mathcal{F}Z^\dagger, \quad \mathcal{F}Z = X^\dagger\mathcal{F}, \quad \mathcal{F}X = Z\mathcal{F}. \quad (356)$$

As proved in an earlier diary entry, the

$$E_{a,b} \equiv X^a Z^b \quad (357)$$

form a complete basis for all unitary operators on  $\mathbb{C}^N$ , in that

$$\text{Tr}[E_{a,b}^\dagger E_{c,d}] = N \delta_{a,c} \delta_{b,d}. \quad (358)$$

The  $E_{a,b}$  satisfy

$$E_{a,b} E_{c,d} = \zeta^{(a,b) \times (c,d)} E_{c,d} E_{a,b}. \quad (359)$$

Let  $G_n^N$  be the Pauli group on  $n$  qudits. To construct a stabilizer code, we choose an Abelian subgroup  $\mathcal{S}_{n-k}$  of  $G_n^N$  with  $n-k$  generators; the encoded space is then the simultaneous  $+1$  eigenspace of all generators. If  $N$  is prime, then the number of encoded qudits is simply  $k$ . This changes however if  $N$  is composite, as then each added generator of  $\mathcal{S}_{n-k}$  need not cut down the dimension of the stabilized subspace by a factor of  $N$ . This is simply due to the fact that the degeneracy of the  $+1$  eigenvectors of a given  $E_{a,b}$  need to be 1, e.g.  $Z^2$  has two  $+1$  eigenvalues for  $N = 4$ .

Define the controlled  $X$  gates by

$$CX = \sum_a |a\rangle\langle a| \otimes X^a, \quad (360)$$

where the left  $\otimes$  factor is the control. By introducing an ancillae qudit in the state  $|0\rangle$ , an application of  $CX$  can be used to measure the operator  $Z$ . Measuring a general  $E_{a,b}$  can be done when  $N$  is prime. In this case, we claim that there exists a unitary  $U_{a,b}$  such that

$$U_{a,b} E_{a,b} U_{a,b}^\dagger = Z. \quad (361)$$

Indeed, when  $N$  is prime it is easy to see that the eigenvalues of  $E_{a,b}$  are the  $N$ th roots of unity, for all  $a, b$ . First look at the case where  $b = 0$ . We claim that (for  $a \neq 0$ )

$$U_{a,0} = \mathcal{F}_a \equiv \sum_{c,d} \zeta^{cd/a} |c\rangle\langle d|, \quad (362)$$

where the  $1/a$  is made possible due to the assumption that  $N$  is prime (note that  $\mathcal{F} = \mathcal{F}_1$ ). Indeed, it is easy to check that

$$\mathcal{F}_a X^c \mathcal{F}_a^\dagger = Z^{c/a}. \quad (363)$$

In the case where  $a = 0$  and  $b \neq 0$ , we can simply use  $\mathcal{F}_b$  together with an  $\mathcal{F}_1^\dagger = \mathcal{F}^\dagger$  to convert the  $Z^b$  into  $X^b$ :

$$\mathcal{F}_b \mathcal{F}_1^\dagger Z^b \mathcal{F}_1 \mathcal{F}_b^\dagger = \mathcal{F}_b X^b \mathcal{F}_b^\dagger = Z. \quad (364)$$

Therefore

$$U_{0,b} = \mathcal{F}_b \mathcal{F}_{-1} = \sum_c |c\rangle\langle c/b|. \quad (365)$$

We can now generalize to both  $a, b \neq 0$ , which we will do by finding an operator which maps  $X^a Z^b$  to  $Z^b$ . After a bit of experimentation, we see that the right choice is

$$\mathcal{U}_{a,b} = \sum_{l,m} \zeta^{-\frac{b}{2a}(l-m)^2 - \frac{b}{2}(l-m)} |l\rangle\langle m|. \quad (366)$$



Note that here we are dividing by 2 even though 2 is prime since we already understand how to find the  $U_{a,b}$  in the  $N = 2$  case. To check the above, we write

$$\begin{aligned} \mathcal{U}_{a,b} X^a Z^b \mathcal{U}_{a,b}^\dagger &= \sum_{l,l',m} \zeta^{\frac{b}{2a}[-(l-m)^2 + (l'-m+a)^2] + \frac{b}{2}(l'-l+a) + (m-a)b} |l\rangle\langle l'| \\ &= \sum_l \zeta^{bl} |l\rangle\langle l| \\ &= Z^b. \end{aligned} \quad (367)$$

Therefore

$$U_{a,b} = \mathcal{F}_b \mathcal{F}_{-1} \mathcal{U}_{a,b} = \sum_{l,m} \zeta^{-\frac{b}{2a}(l-m)^2 - \frac{b}{2}(l-m)} |bl\rangle\langle m|. \quad (368)$$

This means that we may measure  $E_{a,b}$  by using a gate  $CX_{a,b}$ , which is a  $CX$  gate modified by  $U_{a,b}$ :

$$CX_{a,b} \equiv \sum_c |c\rangle\langle c| \otimes U_{a,b} X^c U_{a,b}^\dagger. \quad (369)$$

Now we will go into a bit more detail for the case of  $N = 3$ . Consider a code of length  $n = 3$  with  $k = 1$  logical qutrits. We can encode this with the two commuting stabilizer generators

$$\mathcal{S} = \langle ZZZ, XXX \rangle. \quad (370)$$

Since there are two generators for  $\mathcal{S}$ , we indeed have  $k = 3 - 2 = 1$ . Vectors in the 3-dimensional code subspace must be built from linear combinations of states  $|abc\rangle$  such that a)  $a + b + c = 0 \pmod{3}$  and b) they are invariant under the permutation induced by  $XXX$ . An explicit basis is given by the three vectors  $|\psi_i\rangle$ , where

$$\begin{aligned} |\psi_1\rangle &= |000\rangle + |111\rangle + |222\rangle \\ |\psi_2\rangle &= |012\rangle + |120\rangle + |201\rangle \\ |\psi_3\rangle &= |021\rangle + |210\rangle + |102\rangle. \end{aligned} \quad (371)$$

By taking  $\otimes$ s of the above generators, we can construct a code with  $k = n - 2$  encoded logical bits. We can also easily generalize this code to any  $N$ , as nothing in this construction relies on  $N$  being prime ( $N$  not being prime gives us additional operators stabilized by  $Z^{\otimes N}$ , e.g.  $|2200\rangle$  in the case of  $N = 4$ , but since the action of  $X^{\otimes N}$  cycles through all elements of  $\mathbb{Z}_N$ , this doesn't matter).

Recall that the *distance*  $d$  of a code is defined as the upper bound on the weight of Pauli errors which can be detected by the code. That is, it is the integer  $d$  such that all Pauli operators of weight  $w < d$  either a) appear in  $\mathcal{S}$  or b) do not commute with at least one element of  $\mathcal{S}$ . It is clear for the above choice of  $\mathcal{S}$  that  $d > 1$ . Consider however operators of the form  $PP^\dagger I$ , where  $P$  is any Pauli operator. These operators are not in  $\mathcal{S}$ , but commute with all elements in  $\mathcal{S}$ . Therefore  $d = 2$ .

This code can *detect* errors on any single qutrit, since  $d = 2$ . The number of errors a code can *correct* against is given by the largest integer  $t$  such that  $2t + 1 \leq d$ . This is because if  $\mathcal{A}_i$  are errors of weight  $w_i \leq t$ , then  $\mathcal{A}_i^\dagger \mathcal{A}_j$  has weight  $w_{ij} \leq 2t$ . In order for error correction to

work, we need  $w_{ij} < d$ , giving the above condition. Therefore the  $k = 1$  code above cannot correct for even a single Pauli error, although it can correct for a single  $X$  or  $Z$  type error.

We now construct an  $n = 5, k = 1$  qudit stabilizer code that can correct a single error, which is just a  $\mathbb{Z}_N$  generalization of the famous 5-qubit code. We choose the stabilizer to be generated by

$$\mathcal{S} = \langle \mathcal{S}_1, \dots, \mathcal{S}_4 \rangle, \quad (372)$$

where

$$\begin{aligned} \mathcal{S}_1 &= XZZ^\dagger X^\dagger I \\ \mathcal{S}_2 &= IXZZ^\dagger X^\dagger \\ \mathcal{S}_3 &= X^\dagger IXZZ^\dagger \\ \mathcal{S}_4 &= Z^\dagger X^\dagger IXZ, \end{aligned} \quad (373)$$

which are obtained from one another by cyclic permutations of the  $\otimes$  factors. All generators are of order  $N$ , are independent, and commute. The remaining cyclic permutation  $\mathcal{S}_5$  is not independent, as  $\prod_{i=1}^4 \mathcal{S}_i = \mathcal{S}_5^\dagger$ .

What is the code distance? It is straightforward to check that no elements in  $G_5^N$  of weight  $\leq 2$  commute with  $\mathcal{S}$ . On the other hand, there are elements of weight 3 which *do* commute; an example is the operator  $XIZ^\dagger IX$ . Thus the code distance is  $d = 3$ , and the code is non-degenerate (recall that a code is non-degenerate if the stabilizer contains no elements of weight less than  $d$ ). This last fact follows because *all* of the nontrivial elements in  $\mathcal{S}$  — not just the generators — have weight 4. To prove this, consider e.g. making the operator on the first  $\otimes$  factor equal to  $I$ . Of the  $N^4 - 1$  nontrivial elements in  $\mathcal{S}$ , the ones with an  $I$  in the first slot are of the form  $\mathcal{S}_2^a \mathcal{S}_1^b \mathcal{S}_3^c$  for at least one of  $a, b$  nontrivial in  $\mathbb{Z}_N$ . It is then easy to check that all such elements have an  $I$  only in the first slot.

We can construct weight-3 logical operators  $x, z$  on the code subspace as

$$Z = X^\dagger I Z I X^\dagger, \quad X = I Z X Z I. \quad (374)$$

One can check that these commute with the generators of  $\mathcal{S}$ , and that  $ZX = \zeta XZ$  as required of  $\mathbb{Z}_N$  logical  $X, Z$  operators. Note that this construction works for any  $N$ .



## Local correlations define the state (P2.4)

---

Today we are doing a short problem from Preskill (2.4), in which we will show that for a state  $\rho$  on  $\mathcal{H}_A \otimes \mathcal{H}_B$ , knowledge of all expectation values of local observables in  $A$  and  $B$  — that is, of expectation values of operators of the form  $\mathcal{O}_A \otimes \mathcal{O}_B$  — is sufficient to completely reconstruct  $\rho$ .

⌘ ⌘

As in the problem statement, let  $\rho$  be an arbitrary state on  $\mathcal{G}_A \otimes \mathcal{H}_B$ . Alice, living in  $A$ , can only measure operators of the form  $\mathcal{O}_A \otimes \mathbf{1}_B$ , while Bob, living in  $B$ , can only measure  $\mathbf{1}_A \otimes \mathcal{O}_B$ . One might have thought that this would prevent Alice and Bob from working together to reconstruct  $\rho$  from knowledge of the correlation functions they can compute (provided  $\rho$  is entangled), but this is not the case.

First, suppose that  $\{M_a\}$  are set of  $d^2$  linearly independent Hermitian operators acting on some Hilbert space  $\mathcal{H}$  of dimension  $d$ . By Gram-Schmidt, we can wolog assume that the  $M_a$  are orthonormal wrt the usual norm:  $\text{Tr}[M_a M_b] = \delta_{a,b}$ . Since any density matrix  $\sigma$  on  $\mathcal{H}$  is Hermitian, we may write

$$\sigma = \sum_a \text{Tr}[\sigma M_a] M_a. \quad (375)$$

Therefore knowledge of the expectation values  $\langle M_a \rangle$  for all  $a$  lets us reconstruct  $\sigma$ .

Now suppose  $\{\mathcal{A}_a\}, \{\mathcal{B}_b\}$  are bases for Hermitian operators on  $\mathcal{H}_A$  and  $\mathcal{H}_B$ , respectively. Consider the operators  $\mathcal{O}_{ab} \equiv \mathcal{A}_a \otimes \mathcal{B}_b$ . They clearly satisfy

$$\text{Tr}[\mathcal{O}_{ab} \mathcal{O}_{cd}] = \delta_{ac} \delta_{bd}. \quad (376)$$

Furthermore, the number of  $\mathcal{O}_{ab}$  operators is equal to  $d_A d_B$ , where  $d_{A/B} = \dim \mathcal{H}_{A/B}$ . Since the number of independent Hermitian operators on  $\mathcal{H}$  is  $\dim \mathcal{H}$ , the  $\mathcal{O}_{ab}$  evidently provide a basis for the Hermitian operators on  $\mathcal{H}_A \otimes \mathcal{H}_B$ . Thus from the above, the knowledge of  $\langle \mathcal{O}_{ab} \rangle$  for all  $a, b$  is sufficient to reconstruct the full state  $\rho$ . This obviously generalizes to any number of  $\otimes$  factors.

Note that this would *not* be true if quantum mechanics operated in a real Hilbert space, as opposed to a complex one. In a real Hilbert space, observables would presumably correspond to symmetric operators. However, the number of independent symmetric operators on  $\mathcal{H}_A$  is only  $d_A(d_A + 1)/2$ . Since

$$\frac{(d_A d_B)(d_A d_B + 1)}{2} - \frac{d_A(d_A + 1)}{2} \frac{d_B(d_B + 1)}{2} = \frac{d_A d_B}{4} (d_A - 1)(d_B - 1) > 0, \quad (377)$$

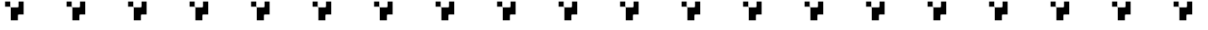
not all of the observables on  $\mathcal{H}_A \otimes \mathcal{H}_B$  can be generated by tensor products of local ones.



## Parameter counting and Schmidt decompositions (P2.9)

---

Today is a rather basic problem from Preskill which gives a simple reason for understanding what types of Schmidt decompositions are possible.



Consider first a bipartite system on  $\mathcal{H}_A \otimes \mathcal{H}_B$ , with  $\dim \mathcal{H}_A = \dim \mathcal{H}_B \equiv d$ . We want to know when we can put a state  $|\psi\rangle$  in the form

$$|\psi\rangle = \sum_{i=1}^d \sqrt{\lambda_i} |i\rangle_A |i\rangle_B. \quad (378)$$

Of course by using the SVD on the matrix  $\hat{\psi}$  obtained via  $\mathcal{H}_A \otimes \mathcal{H}_B \cong \mathcal{H}_A \otimes \mathcal{H}_B^*$ , we can get an explicit unitary  $U_A \otimes U_B$  which brings an arbitrary state into this form. Thus the Schmidt decomposition can always be accomplished by Alice and Bob acting with local unitaries in their respective subsystems.

That this is possible can be argued simply by counting degrees of freedom. The above Schmidt state  $|\psi\rangle$  is of course specified by  $d$  parameters. Consider the orbit obtained by acting on the Schmidt state with arbitrary *local* unitaries. We will find it helpful to parametrize local unitaries via their logarithms, using the Hermitian matrices  $H_A \otimes \mathbf{1}_B + \mathbf{1}_A \otimes H_B$ . Define the state

$$|\lambda\rangle \equiv \sum_i \sqrt{\lambda_i} |i\rangle. \quad (379)$$

Let  $\{|\mu\rangle\}$  be an orthonormal basis for  $\mathcal{H}_A$ , for which the  $\mu = 1$  basis state is  $|\lambda\rangle$ . Note that

$$(H_A \otimes \mathbf{1}_B)|\psi\rangle = \sum_{i,j} H_A^{ji} \sqrt{\lambda_i} |j\rangle |i\rangle \quad (380)$$

vanishes if  $|\lambda\rangle \in \ker H_A = \langle |\mu\rangle : \mu > 1 \rangle$ . Therefore the orbit of  $|\psi\rangle$  under local unitaries can be specified using only the first row and column of  $H_A, H_B$  in the  $|\mu\rangle$  basis. For determining the orbit, we may thus wolog parametrize

$$H_A = \sum_{\mu} \alpha_{\mu\lambda} |\mu\rangle \langle \lambda| + \alpha_{\mu\lambda}^* |\lambda\rangle \langle \mu|, \quad H_B = \sum_{\mu} \beta_{\mu\lambda} |\mu\rangle \langle \lambda| + \beta_{\mu\lambda}^* |\lambda\rangle \langle \mu| \quad (381)$$

for some complex coefficients  $\alpha_{\mu\lambda}, \beta_{\mu\lambda}$ . The number of (real) parameters needed to specify  $\alpha_{\mu\lambda}$  is  $2d - 1$ . However, not all choices of  $\alpha_{\mu\lambda}, \beta_{\mu\lambda}$  are non-degenerate in their action on  $|\psi\rangle$ . Indeed, writing  $H_A, H_B$  in the  $\{|i\rangle\}$  basis as (taking the generic case where all  $\lambda_i \neq 0$ )

$$H_A = \sum_{ij} \alpha_{ij} |i\rangle \langle j|, \quad H_B = \sum_{ij} \beta_{ji} \sqrt{\lambda_j / \lambda_i} |i\rangle \langle j|, \quad (382)$$

we have

$$(H_A \otimes \mathbf{1}_B + \mathbf{1}_A \otimes H_B)|\psi\rangle = \sum_{ij} \sqrt{\lambda_j} (\alpha^{ij} + \beta^{ij}) |ij\rangle, \quad (383)$$

so that really only the *symmetric* combination of  $\alpha$  and  $\beta$  contributes to the orbit. Since there are  $2d - 1$  independent parameters for both  $\alpha$  and  $\beta$ , the total number of parameters determining the orbit is

$$\frac{(2d - 1)(2d - 1 + 1)}{2} = 2d^2 - d. \quad (384)$$

Since there are  $d$  different  $\lambda_i$ , the total number of parameters needed to specify the Schmidt decomposition and its orbit under local unitaries is

$$2d^2 - d + d = 2d^2, \quad (385)$$

which is exactly the number of real parameters needed to specify the (un-normalized) wavefunction  $|\psi\rangle$ . Therefore any wavefunction can be specified by a Schmidt decomposition and a choice of local unitary in the orbit.

One can similarly ask whether the above counting goes through for  $k$ -partite systems when  $k > 2$ . Consider a wavefunction on  $\mathcal{H}^{\otimes k}$  of the form

$$|\psi\rangle = \sum_i \sqrt{\lambda_i} |i\rangle^{\otimes k}, \quad (386)$$

which is determined by  $d$  parameters. With the same parametrization as before, each Hermitian  $\otimes$  factor in the logarithm of a given local unitary is specified by  $2d - 1$  real parameters. The dimension of the orbit of  $|\psi\rangle$  under local unitaries is then determined by the dimension of the symmetric subspace of  $k$  tensor factors of the  $2d - 1$  Hermitian matrices, which is

$$\dim \text{Sym}^k = \binom{2d - k - 2}{k}. \quad (387)$$

In order for an arbitrary wavefunction in  $\mathcal{H}^{\otimes k}$  to admit a  $k$ -partite Schmidt decomposition, we need the dimension of the above space to be at least as large as  $2d^k$ . But in fact this is never satisfied as long as  $k > 2$ , meaning that Schmidt decompositions are possible *only* for 2-partite systems! A hasty way of justifying this is to consider the  $d \rightarrow \infty$  limit of

$$\lim_{d \rightarrow \infty} \frac{1}{2d^k} \binom{2d - k - 2}{k} = \frac{2^{k-1}}{k\Gamma(k)}, \quad (388)$$

which is equal to 1 when  $k = 2$  but goes rather quickly to zero when  $k > 2$ .



## Non-contextuality of QM (P2.8)

---

Today's entry is a short but cute problem from Preskill on something which is apparently known as Mermin's magic square.



Consider the following matrix of 9 operators acting on a 2-qubit system:

$$M = \begin{pmatrix} X \otimes \mathbf{1} & \mathbf{1} \otimes X & X \otimes X \\ \mathbf{1} \otimes Y & Y \otimes \mathbf{1} & Y \otimes Y \\ X \otimes Y & Y \otimes X & Z \otimes Z \end{pmatrix} \quad (389)$$

Notice that

$$\prod_j M_{ij} = \mathbf{1} \otimes \mathbf{1} \quad (390)$$

for all rows  $i$ , while

$$\prod_i M_{ij} = \begin{cases} \mathbf{1} \otimes \mathbf{1} & \text{if } i = 1, 2 \\ -\mathbf{1} \otimes \mathbf{1} & \text{if } i = 3 \end{cases} \quad (391)$$

Note furthermore that the three operators in each row and column are mutually commuting.

Consider a hidden variable theory in which a *noncontextual* assignment of classical values is made for the operators in the top  $2 \times 2$  subblock, say. This means here that if  $\mathcal{O}$  is assigned the value  $s_{\mathcal{O}}$  and  $\mathcal{O}'$  is assigned the value  $s_{\mathcal{O}'}$ , then  $\mathcal{O}\mathcal{O}'$  is assigned  $s_{\mathcal{O}}s_{\mathcal{O}'}$ . In such a theory, we would therefore require that  $\prod_j s_{M_{ij}} = 1$  and  $\prod_i s_{M_{ij}} = 1$  if  $i = 1, 2$  and  $-1$  if  $i = 3$ . But we see that noncontextuality forces

$$\prod_i \prod_{j=1,2} s_{M_{ij}} = \prod_i s_{M_{i3}}, \quad (392)$$

since all of the  $s_{M_{ij}} = \pm 1$ . Now the RHS must be 1, since all of the products on the LHS must be one. But in fact we also have that  $\prod_i M_{i3} = -\mathbf{1}$  — therefore the RHS must also be  $-1$ ; a contradiction. This is a simple disproof of noncontextual hidden variable theories.

A note to self is that this construction looks rather cohomological. Define a  $\mathbb{Z}_2$  ‘2-cochain’  $\alpha$  which assigns to each row / column of  $M$  the product of the elements of  $M$  along that row / column (which is always  $\pm \mathbf{1} \otimes \mathbf{1}$ ; hence the  $\mathbb{Z}_2$ ), via  $\prod_j M_{ij} = (-1)^{\alpha_{i,c}} \mathbf{1} \otimes \mathbf{1}$  and likewise for a product over the row index,  $\prod_i M_{ij} = (-1)^{\alpha_{j,r}} \mathbf{1} \otimes \mathbf{1}$ . Now  $\int \alpha = 1 \pmod 2$  (since only the product along the last column gives a nontrivial sign); therefore  $\alpha$  is not ‘exact’. But it is also ‘closed’, in that if we take the product over *all* rows and columns we just get  $0 \pmod 2$  (since every matrix element of  $M$  is counted twice). It remains to see whether or not this vagary can be made precise.




---

## Collision problem and Simon's algorithm

Today's entry is an elaboration on a problem from Xiaodi Wu's QI class, which serves as a simple illustration of the importance of periodic structure in getting quantum speedups.

✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂ ✂

Consider a function  $f(x)$  on some alphabet  $X$  of size  $N$ , which we are promised is 2:1. Our goal is to find a collision, i.e. a pair  $x, y$  such that  $f(x) = f(y)$ . We claim that classically, this takes  $\sqrt{N}$  queries to the function  $f$ . Indeed, after randomly choosing  $m$  values of  $x$ , the probability  $p_c$  that we get a collision looks like

$$p_c \sim 1 - \prod_{j=1}^m (1 - j/N) < 1 - \prod_{j=1}^m e^{-j/N} \approx 1 - e^{-m^2/2N}, \quad (393)$$

and so  $p_c$  is of order 1 when  $m \sim \sqrt{N}$ . This is the solution to the famous birthday problem.

How much better can we do with a quantum computer? One strategy is as follows:

- Randomly choose  $k$  different values of  $x$ , and compute  $f(x_i)$  for  $i = 1, \dots, k$ .
- If a collision exists among these  $k$  values, done.
- Else, perform a quantum search on the remaining  $N - k$  unchosen values, searching for  $x_l$  such that  $f(x_l)$  matches one of the  $f(x_{i=1,\dots,k})$ .

Now a quantum search of a database consisting of  $D$  values with  $M$  marked points runs in a number of queries scaling as  $\sqrt{D/M}$ . Therefore the total number  $q$  of queries needed by this approach goes as

$$q \sim k + \sqrt{N/k}, \quad (394)$$

where we have written  $\sqrt{(N-k)/k} \lesssim \sqrt{N/k}$ , under the assumption that the optimal value of  $k$  goes as  $N^\alpha$  for some  $\alpha < 1$ . Indeed, minimizing  $q$  gives  $k \sim N^{1/3}$ . The query complexity of this strategy therefore scales as  $N^{1/3}$ , narrowly beating out the  $\sqrt{N}$  required by the classical algorithm. Moreover, it has been proven that this speedup is actually optimal [1].

This result is interesting given the existence of Simon's algorithm, which for the sake of completeness we now briefly review. For simplicity we set  $X = \mathbb{Z}_2^n$ , and we are now promised that the 2:1 function  $f$  satisfies  $f(x) = f(x + s)$  for some secret string  $s$ , which can be determined from the unitary  $U_f : |x, y\rangle \mapsto |x, y + f(x)\rangle$  (both  $x, y \in \mathbb{Z}_2^n$ ) as follows.

First, we prepare the state  $|0\rangle^{\otimes 2n}$ , and then Fourier transform the first  $n$  bits using  $H^{\otimes n}$ . We then hit the resulting state with  $U_f$ , and again apply  $H^{\otimes n}$  on the first  $n$  bits. The result is the state

$$|\psi\rangle = \frac{1}{2^n} \sum_{x,y \in \mathbb{Z}_2^n} (-1)^{x \cdot y} |y, f(x)\rangle = \frac{1}{2^{n+1}} \sum_{x,y \in \mathbb{Z}_2^n} (-1)^{x \cdot y} (1 + (-1)^{s \cdot y}) |y, f(x)\rangle. \quad (395)$$

Now consider measuring the first  $n$  qubits. The reduced density matrix for the first  $n$  qubits is

$$\begin{aligned} \rho &= \frac{2^2}{2^{2n+2}} \sum_{x,y,x',y' \in \mathbb{Z}_2^n} (-1)^{x \cdot y + x' \cdot y'} (\delta_{x,x'} + \delta_{x,x'+s}) \mathcal{P}_s(y) \mathcal{P}_s(y') |y\rangle \langle y'| \\ &= \frac{1}{2^{n-1}} \sum_y \mathcal{P}_s(y) |y\rangle \langle y|, \end{aligned} \quad (396)$$

where we have let  $\mathcal{P}_s(y) \equiv (1 + (-1)^{s \cdot y})/2$  be the projector onto the  $2^{n-1}$ -dimensional subspace normal to  $s$ .  $\rho$  therefore gives the uniform distribution on strings normal to  $s$ . Consider sampling  $n - 1$  strings from this distribution. Since each string is normal to  $s$ , if all  $n - 1$  strings are linearly independent, they will tell us that either  $s$  is some particular nonzero string, or that  $s = 0$ . The probability that all  $n - 1$  strings are linearly independent is

$$p = \prod_{k=1}^{n-1} (1 - 2^{-k}) < \prod_{k=1}^{\infty} (1 - 2^{-k}) \approx 0.289, \quad (397)$$

according to Mathematica. Since  $p$  is  $O(1)$ , we need only  $O(n)$  queries to determine  $s$ .

Given this, we have consequently found all of the collisions in only  $O(n)$  queries, which is exponentially better than the  $2^{n/3}$  required from the Grover-assisted search algorithm described above. This serves to illustrate how important periodic structure is for quantum speedups: in the completely unstructured case (only the promise that  $f$  is 2:1) a brute-force search is necessary, affording only a modest speedup, while with the additional promise that the origin of the 2:1 behavior is due to a hidden periodicity, an exponential speedup a la Simon becomes possible.



## coNP trivialities

---

Today we will do some simple exercises from Arora + Boaz's book on complexity theory, meant to familiarize ourselves with coNP.



Let us first give two definitions of coNP:

**Definition 1.** A language  $L \in \text{coNP}$  if  $\bar{L} \in \text{NP}$ , where  $\bar{L} \equiv \{0, 1\}^* \setminus L$ .

The second is

**Definition 2.** A language  $L \in \text{coNP}$  if there is a polynomial TM  $M$  and a polynomial  $p : \mathbb{N} \rightarrow \mathbb{N}$  such that

$$x \in L \iff \forall u \in \{0, 1\}^{p(|x|)}, M(x, u) = 1. \quad (398)$$

Note that this latter definition is the exact same as the definition for a language being in NP, except that the  $\forall$  symbol is replaced by  $\exists$ .



**Proposition 1.** *The two definitions above are equivalent.*

*Proof.* Suppose  $L \in \text{coNP}$  according to the second definition. Define  $\widetilde{M}$  as the turing machine whose output on  $x, u$  is  $\neg M(x, u)$ . Then the converse of the property in definition 2 implies that  $\forall x \notin L$ , there must exist some  $u \in \{0, 1\}^{p(|x|)}$  such that  $\widetilde{M}(x, u) = 1$ . But then  $\widetilde{M}$  serves as a verifier for establishing that  $\bar{L} \in \text{NP}$ , implying that  $L \in \text{coNP}$  according to the first definition.

Suppose now that  $L \in \text{coNP}$  according to the first definition. Let  $N$  be the polynomial TM verifying  $\bar{L}$ . Thus  $\forall \bar{x} \in \bar{L}$ , there is a certificate  $u$  such that  $N(x, u) = 1$ . Thus if  $x \in L$ , there exists no such  $u$ , and  $N(x, u) = 0 \forall u$ . But then the TM  $\tilde{N}$  satisfies the properties of the second definition.  $\square$

**Proposition 2.**  $P \supseteq \text{NP} \cap \text{coNP}$ .

*Proof.*  $P \subseteq \text{NP}$  is pretty trivial: if a language  $L \in P$ , then there exists a poly-time TM  $N$  deciding  $L$  (this  $N$  is different than the TM appearing in the definition of  $\text{NP}$ , which only acts as a verifier, not as a decider). But then  $N$  can do the job of the TM in the definition of  $\text{NP}$  as well, with trivial certificate  $u = 0$  ( $N$  can decide on its own, without help from proof instructions).  $P \subseteq \text{coNP}$  is just as trivial: we just take the TM  $M$  in the second definition to be  $N$ , and independent of the (unneeded) certificate  $u$ .  $\square$

**Proposition 3.**  $P = \text{NP} \implies \text{NP} = \text{coNP}$

*Proof.* Suppose  $P = \text{NP}$ . Then for  $L \in \text{NP}$ , we can construct a poly-time decider  $N$  for  $L$ . Since  $N$  is a decider (i.e. it computes  $f(x) \in \mathbb{Z}_2$ , where  $f(x) = 1 \iff x \in L$ ),  $\tilde{N}$  is a decider for  $\bar{L}$ . Thus  $\tilde{N}$  provides the TM needed for showing that  $L \in \text{coNP}$ .  $\square$



## Understanding Grover's search adiabatically

---

Today's entry is a simple way of motivating why one gets a square-root speedup in unstructured search problems. I am not sure that this is really the best way of understanding things, and in any case am sure there is a more sophisticated treatment in the literature somewhere (update: Farhi and Gutmann unsurprisingly have a paper on this).



The basic idea is to perform the search using the adiabatic algorithm. Consider a system of  $n$  qubits, and let  $|m\rangle$  be the marked state we are searching for, assumed wolog to be a

computational basis state (this assumption is wolog since the runtime will only depends on the overlap between  $|m\rangle$  and a random state). Consider the Hamiltonian

$$H(\lambda) = \lambda \mathcal{P}_m^\perp + (1 - \lambda) \mathcal{P}_s^\perp, \quad (399)$$

where  $\mathcal{P}_a^\perp = \mathbf{1} - |a\rangle\langle a|$  and  $|s\rangle = |+\rangle^{\otimes n}$ , and  $\lambda$  sweeps from 0 to 1. Here  $\mathcal{P}_m^\perp$  is to be thought of as the time evolution provided by querying the oracle.

When  $\lambda = 0$  we are in the ‘paramagnet’ product state, and when  $\lambda = 1$  we have found the desired marked state. The running time for the adiabatic algorithm depends on the minimum gap size  $\Delta(\lambda)$  as a function of  $\lambda$ . Intuitively  $\Delta(\lambda \approx 1/2)$  is exponentially small in  $n$ : this is because

$$\|[\mathcal{P}_m^\perp, \mathcal{P}_s^\perp]\|_\infty = \frac{1}{2^{n/2}}, \quad (400)$$

so that the spectrum of  $H(\lambda)$  is almost just a weighted sum of the spectra for both terms, with the weighted sum vanishing at  $\lambda = 1/2$  (in fact the  $1/\sqrt{N}$ ,  $N = 2^n$  that appears in the norm above is exactly the right square root factor).

Since this problem is essentially just a 2-level system, we can compute  $\Delta(\lambda)$  exactly. Orthonormalizing by taking

$$|s'\rangle = \frac{|s\rangle - \frac{1}{2^{n/2}}|m\rangle}{\mathcal{N}}, \quad \mathcal{N} \equiv \sqrt{1 - 2^{-n}}, \quad (401)$$

we can write

$$H(\lambda) = \begin{pmatrix} -\lambda - (1 - \lambda)/2^n & 2^{-n/2}\mathcal{N} \\ 2^{-n/2}\mathcal{N} & -(1 - \lambda)\mathcal{N}^2 \end{pmatrix} \quad (402)$$

in the basis  $\{|m\rangle, |s'\rangle\}$ . The gap is then apparently

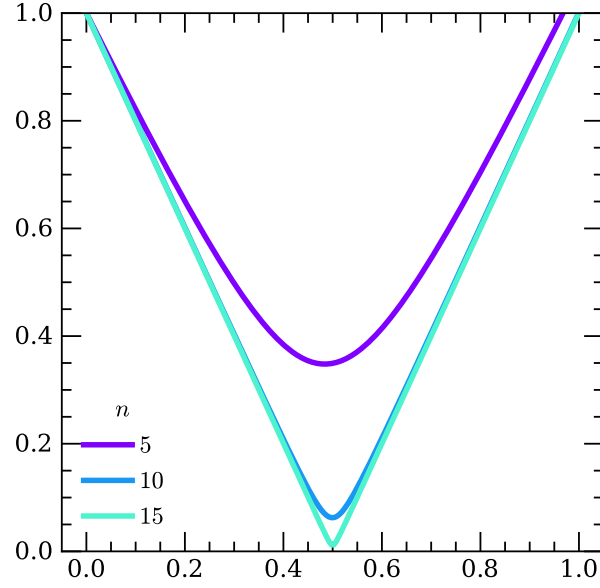
$$\Delta(\lambda) = \sqrt{((1 - \lambda)(1 - 2^{-n+1}) - \lambda)^2 + \mathcal{N}^2 2^{-n+2}}. \quad (403)$$

When  $\lambda \approx 1/2$  the first term goes as  $2^{-2n}$ , leaving the second term (going as  $2^{-n+2}$ ) to dominate. Thus

$$\Delta(1/2) = O(2^{-n/2}) \quad (404)$$

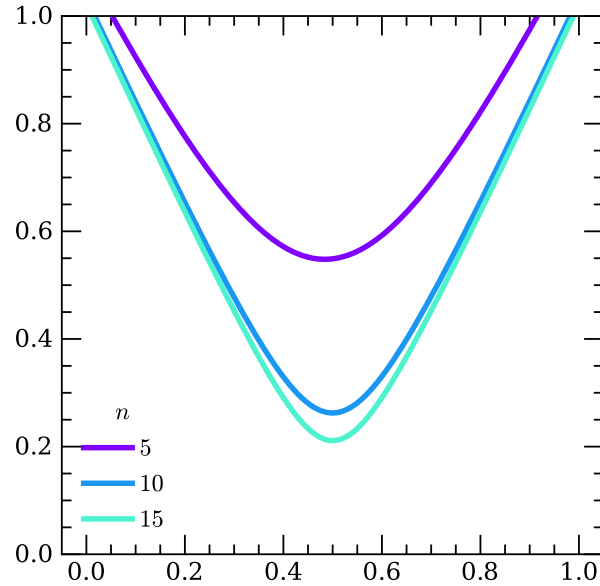
and so the time needed to run the adiabatic sweep scales as  $2^{n/2} = \sqrt{N}$ . Plotting  $\Delta(\lambda)$  for

a few values of  $n$  gives



(405)

While  $\Delta(\lambda)$  must close for the chosen path, we claim that any ‘reasonable’ path will also have  $\Delta(\lambda_*) \rightarrow 0$  for some  $\lambda_*$ . By ‘reasonable’ path, we mean one where  $H(\lambda)$  can always be modeled as alternating time evolution between a verifier and a black box, where the verifier does not know about  $|m\rangle$ , and the black box only provides  $\mathcal{P}_m^\perp$ . Indeed, since the above  $H(\lambda)$  goes from  $1 + Z$  to  $1 - Z$  in the space  $\{|m\rangle, |s'\rangle\}$  by moving along the  $z$  axis of the Bloch sphere defined in this space, we can make  $H(\lambda)$  fully gapped by taking e.g.  $H'(\lambda) = H(\lambda) + \delta\lambda(\lambda - 1)X$ , so that  $H'(\lambda)$  never passes through the center of the Bloch sphere. Indeed, taking  $\delta = 0.1$  changes the previous figure to



(406)

Doing this however requires adding the term  $X = |m\rangle\langle s'| + |s'\rangle\langle m|$ , which does not fit into

the above verifier / black box framework. The fact that  $\Delta(\lambda_*) \rightarrow 0$  is inevitable for some  $\lambda_*$  under these assumptions is essentially the proof that the  $\sqrt{N}$  Grover speedup is optimal.



## One-way functions and P vs NP

---

Today we are doing an exercise from Arora + Barak: showing that the existence of one-way functions (OWFs) imply  $P \neq NP$ .



We will prove the contrapositive: if  $P = NP$ , then OWFs cannot exist. Recall that a poly-time computable function  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  is said to be one-way if no poly-time algorithm exists which can compute pre-images of bit strings returned by  $f$ . That is, for all poly-time computable functions  $F$ ,

$$\mathbb{E}_{x \in \{0, 1\}^l} [f(F(f(x))) = f(x)] < \varepsilon(l), \quad (407)$$

where  $\varepsilon(l)$  is a negligible function (vanishing faster than any polynomial in  $1/l$  for  $l$  sufficiently large). Note that we need to average over  $x \in \{0, 1\}^l$  and then take  $f(x)$  (rather than just averaging over  $y \in \{0, 1\}^l$  and asking if  $f(F(y)) = y$ ), since we only want to average over strings where a pre-image exists, viz those of the form  $f(x)$  for some  $x$ .

Since we are assuming  $P = NP$ , we need to concoct a decision problem in  $NP$  which, when we assume it to be decided in poly time, lets us efficiently compute pre-images under  $f$  of any string, if they exist. The subtlety is that we cannot simply use the decision problem of deciding whether a pre-image of a given string  $y$  exists. For one, it may be the case that all pre-images of  $y$  are strings of length exponentially large in  $|y|$ ; in this case the problem as stated would not be in  $NP$ . This is easy to fix, though: instead of our input just being a string  $y$ , we input both a string and a length  $l$ , and ask if  $\exists$  a preimage of  $y$  of length at most  $l$ . We could thus define the language

$$L = \{(y, 1^l) \in \{0, 1\}^* \times \mathbb{N} : \exists x \in \{0, 1\}^{l' \leq l} \text{ s.t. } f(x) = y\}, \quad (408)$$

where we have done the usual trick of letting part of the input be in unary to allow for a witness, viz. an  $x$  such that  $f(x) = y$ , to be polynomially-sized in the input length. Clearly with this trick,  $L \in NP$ . However,  $L$  is not actually useful for this problem: we need to actually *find* a preimage of  $y$ ; simply knowing that one exists does not help. We thus need to incorporate more information about possible preimages into our input data. We will do

this by defining a decision problem that lets us improve on successive guesses for a candidate preimage.

Define the language

$$L' = \{(g, y, l') \in \{0, 1\}^{l' \leq l} \times \{0, 1\}^* \times \mathbb{N} : \exists x \in \{0, 1\}^l \text{ s.t. } f(x) = y \wedge g \subset x\}. \quad (409)$$

Here  $g$  is to be viewed as a guess for a possible preimage of  $y$ , and a tuple  $(g, y, l')$  is in  $L'$  if there exists a preimage  $x$  of  $y$  such that  $g$  is equal to the first  $l' \leq l$  characters of  $x$  (this is what we mean by  $g \subset x$ ). Clearly  $L' \in \mathbf{NP}$  since  $x$  again provides a certificate. But assuming  $\mathbf{P} = \mathbf{NP}$ , we can now use a poly-time TM  $N$  deciding  $L'$  to reconstruct a preimage. This works as follows:

1. Fix  $y$  and  $l$ , and initialize  $g = \varepsilon$  as the empty string.
2. Use  $N$  to decide if there are preimages of  $y$  beginning with  $a + g$ , where  $a \in \{0, 1\}$  and  $+$  denotes string concatenation. If  $N$  outputs YES only on one choice of  $a$ , send  $g \mapsto a + g$ . If  $N$  outputs YES on both choices, send  $g \mapsto 0 + g$  (for definiteness — we just care about finding a preimage). Finally, if  $N$  outputs NO on both choices, return  $\varepsilon$ .
3. Repeat the above step until  $|g| = l$ , at which point return  $g$ .

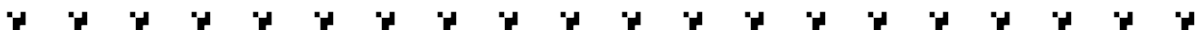
This algorithm will return a preimage of any  $y$  whenever one exists. It clearly runs in time polynomial in  $l$  (since there are only at most  $l$  steps in the loop and  $N$  runs in poly time). Therefore this algorithm provides an  $F$  for which (407) fails to hold.



## Exact encryption requires big keys

---

Today's entry is a brainwarmer on exact encryption with private keys.



Suppose we want to encrypt messages that take the form of  $n$ -length bit strings  $x \in \{0, 1\}^n$ , and suppose that the encryption is done using keys of length  $m$ . Then we claim

**Proposition 4.** *Exact encryption requires keys as long as the message length, i.e. requires  $m \geq n$ .*

Recall that an exact encryption scheme is a pair of maps  $(E_k, D_k)$ , where  $k$  is a length- $m$  key and

$$D_k \circ E_k(x) = x, \quad E_{U_m}(x) = E_{U_m}(x') \quad \forall x, x' \in \{0, 1\}^n, \quad (410)$$

where  $U_m$  is the uniform distribution on  $\{0, 1\}^m$ .

*Proof.* The proof is quite straightforward and just relies on dimension counting. In order for  $E_{U_m}(x) = E_{U_m}(x')$  for all  $x, x'$ , it is of course necessary that  $\text{Supp}(\cup_k E_k(x))$  be independent of  $x$ . Now for a fixed  $x$ ,  $\dim[\text{Supp}(\cup_k E_k(x))] \leq 2^m$ , the number of keys. But if this is independent of  $x$ , we can freely take a union over messages  $x$ , obtaining

$$\dim[\bigcup_k \text{Supp}(\bigcup_x E_k(x))] \leq 2^m. \quad (411)$$

This says that for each  $k$ , the size of  $\text{Supp}(\cup_x E_k(x))$  is upper-bounded by  $2^m$ . Since  $2^m < 2^n$  is less than the total number of message strings, it must be impossible to construct a decoder  $D_k$  which inverts  $E_k$ . Therefore our assumption that  $E_{U_m}(x) = E_{U_m}(x')$  for all  $x, x'$  must have been incorrect.  $\square$



## Graphical CHSH proof

---

Today's entry is a trivial graphical reminder of the quantum strategy for the CHSH game.



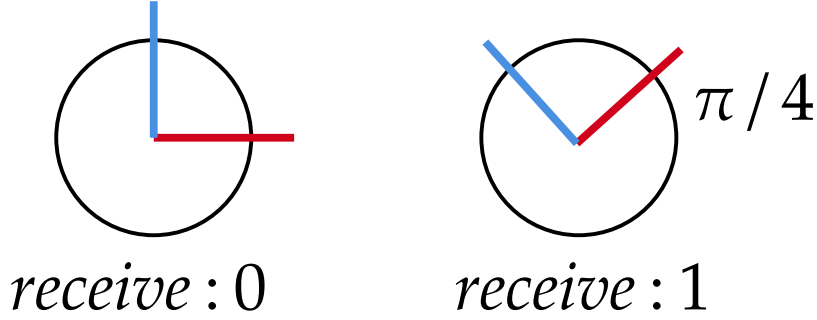
Recall the CHSH game. Alice and Bob share a Bell pair, which we will take to be  $|\Phi_0\rangle$ . They receive random bits  $s_A, s_B$  from a judge, and they each must respond with one bit each, which we denote  $r_A, r_B$ . Alice and Bob win if

$$r_A \oplus r_B = s_A \wedge s_B. \quad (412)$$

It is easy to show that any classical strategy can win at most  $3/4$  of the time. If Alice and Bob make use of the Bell pair, they can do better. In the optimal strategy, the responses  $r_A, r_B$  are chosen as the outcomes Alice and Bob get when performing measurements on their respective qubits in bases  $\mathcal{B}_A(s_A), \mathcal{B}_B(s_B)$  (note that with this strategy, both  $r_A$  and  $r_B$  separately are uniformly random!). The idea is to choose the bases in such a way that the basis vectors of  $\mathcal{B}_A(s_A), \mathcal{B}_B(s_B)$  are nearly aligned if  $s_A \wedge s_B$  is false, and are nearly orthogonal

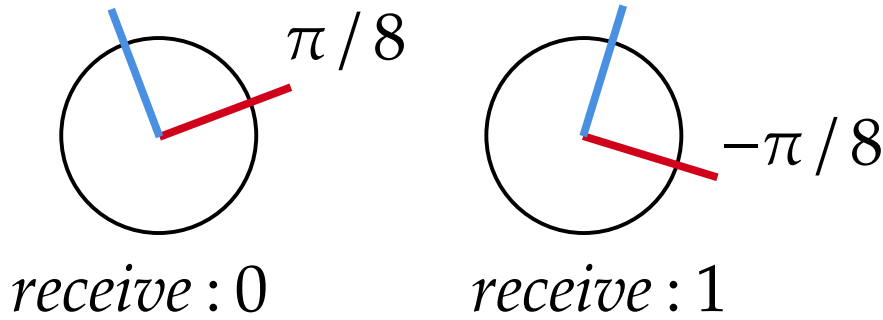
if  $s_A \wedge s_B$  is true. It turns out the best choice (which is fairly obvious geometrically) is to use the following bases:

*Alice :*



(413)

*Bob :*



Here the  $x$  axis in the plane of the page is  $|0\rangle$ , and the  $y$  axis is  $|1\rangle$  (if the Bloch sphere picture is preferred, just double all angles). A measurement of a red vector results in a reply of 0, while a measurement of a blue vector results in a reply of 1 — *i.e.* if Alice receives 0,  $r_A = 0/1$  if she measures  $|0/1\rangle$ , while if she receives 1,  $r_A = 0/1$  if she measures  $|+/-\rangle$ .

From the picture, it is easy to see that the bases of Alice and Bob are nearly aligned (rotated by  $\pm\pi/8$ ) if  $s_A \wedge s_B$  is false. On the other hand, they are nearly orthogonal (rotated by  $\pi/2 - \pi/8$ ) if  $s_A \wedge s_B$  is true. Therefore regardless of  $s_A, s_B$ , the response  $r_A, r_B$  wins with probability  $\cos^2(\pi/8) \approx 85\%$ .



## Random code ensemble basics

Today's entry is a discussion of some aspects of the random code ensemble and finite-temperature decoding, which proceeds following an elaboration on a few exercises posed in Mezard + Montanari's book.

❧ ❧

*Word MAP and Symbol MAP:* Consider a code where codewords of length  $M$  are encoded in messages of length  $N$ . We will focus on the random code ensemble, where for each string in  $\{0, 1\}^M$ , each possible codeword is chosen with uniform probability. Of course this may in general lead to collisions and non-injective coding, but the probability of this happening is (recall the Birthday problem)

$$p_{\text{coll}} = (1 - 2^{-N})^{\binom{M}{2}} \approx e^{-M(M-1)2^{-(N+1)}} \rightarrow 0. \quad (414)$$

Define the probability for the channel input to be  $x$  conditioned on a recieved message  $y$  as

$$\mu_y(x) \equiv \mathbb{P}(x|y) = \frac{1}{Z(y)} \prod_{i=1}^N Q(y_i|x_i) \mathbb{P}(x), \quad (415)$$

where  $Z(y)$  is a normalization constant,  $Q(y_i|x_i)$  are the transition probabilities for the channel, and  $\mathbb{P}(x)$  is the a priori probability of  $x$  being the transmitted message — we will always take the uniform distribution  $\mathbb{P}(x) = \frac{1}{|\mathfrak{c}|} \mathbb{I}(x \in \mathfrak{c})$ , where  $\mathfrak{c}$  is the codebook. Marginal probabilities will be denoted by

$$\mu_y^i(x_i) = \sum_{x_j \neq i} \mu_y(x). \quad (416)$$

Two common ways of decoding are to either aim to reconstruct full codewords, or else to get distributions of symbols which are close to those present in the codewords themselves. Given a channel output  $y$ , word MAP (maximum a posteriori) decoding outputs the most probable transmitted codeword:

$$x^w(y) = \arg \max_x \mu_y(x). \quad (417)$$

Symbol MAP on the other hand outputs the most probable transmitted bits:

$$x^s(y) = \left( \arg \max_{x_1} \mu_y^1(x_1), \dots, \arg \max_{x_N} \mu_y^N(x_N) \right). \quad (418)$$

**Example 1.** Word MAP and symbol MAP decoding obviously needn't give the same answers. For example, consider a code of length  $N = 3$  with four codewords  $x^1 = 001, x^2 = 101, x^3 = 110, x^4 = 111$ , which is used to communicate over a binary symmetric channel with error probability  $p$ . Suppose the channel output is  $y = 000$ . When  $p < 1/2$ , word MAP decoding always outputs 001, as

$$\mu_{000}(x^1) = p(1-p)^2, \quad \mu_{000}(x^{2,3}) = p^2(1-p), \quad \mu_{000}(x^4) = p^3, \quad (419)$$



so that  $x^1$  is always chosen by the decoder. To see that this does not always agree with symbol MAP, consider decoding just the first digit  $x_1$ . We have

$$\mu_{000}^1(0) = p(1-p)^2, \quad \mu_{000}^1(1) = 2p^2(1-p) + p^3. \quad (420)$$

The latter is greater than the former if  $p \gtrsim 1/3$ .

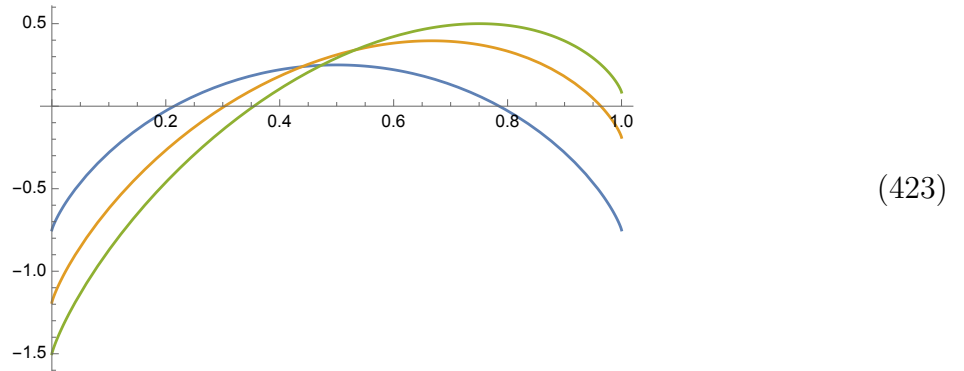
*Expected distance:* Consider random codes on an alphabet  $\mathcal{X}$  with  $q$  characters. What is the expected distance between codewords? We define this distance using the quantity  $\mathcal{N}_{x_*}(d)$ , the number of codewords a distance  $d$  from some (arbitrary) base codeword  $x_*$ , where the distance is measured using the Hamming distance  $d(x, x') = \sum_i (1 - \delta_{x_i, x'_i})$ . With  $M$  codewords on  $\mathcal{X}^N$ , the expected number of codewords at distance  $d$  is easily seen to be

$$\mathbb{E}\mathcal{N}_{x_*}(d) = (q^M - 1)q^{-M} \binom{N}{d} (q-1)^d. \quad (421)$$

Letting  $\delta \equiv d/N$  and  $R \equiv M/N$ , and sending  $M, N \rightarrow \infty$  with  $\delta, R$  fixed, we have

$$\mathbb{E}\mathcal{N}_{x_*}(\delta) = 2^{N[(R-1)\log_2 q + \delta\log_2(q-1) + H_2(\delta)]}, \quad (422)$$

where  $H_2(\delta)$  is the binary Shannon entropy and comes from using Stirling's approximation on  $\log_2 \binom{N}{d}$ . Note that  $\mathbb{E}\mathcal{N}_{x_*}(\delta)$  is maximized at  $\delta = 1/q$ , since this is the expected Hamming distance between random strings. Thus in the  $N \rightarrow \infty$  limit, almost all codewords are separated by a distance of  $N/q$ . Furthermore, there are almost *no* codewords with distances  $\delta < \delta_1(R)$  or  $\delta > \delta_2(R)$ , where  $\delta_{1,2}(R)$  are the roots of the exponent in (422). For  $q = 2$  we have  $\delta_2 = 1 - \delta_1$  as  $H_2(\delta) = H_2(1 - \delta)$ , but for  $q > 2$  this is no longer the case. The function  $\log(\mathbb{E}\mathcal{N}_{x_*}(\delta))/N$  is plotted below for  $q = 2, 3, 4$  and a fixed rate of  $R = 1/4$ :



Changing  $R$  just moves one up or down; for  $R = 1$  there are always an exponentially large number of codewords at arbitrarily small  $\delta$ , while for  $R \rightarrow 0$  all of the codewords are always far away. Decoding will succeed provided  $\delta < \delta_1$ .<sup>29</sup>

<sup>29</sup>Note that the naive guess might have been that decoding would succeed only if  $\delta < \delta_1/2$ , with the  $1/2$  coming from thinking of the codewords as defining spheres of radius  $\delta$  in the space of all strings. This is not correct, however: since the codewords are chosen randomly,  $y$  is uncorrelated with all of  $\mathfrak{c} \setminus x_*$ . Thus if  $\delta < \delta_1$ , no elements of  $\mathfrak{c} \setminus x_*$  will be within a distance of  $\delta$  of  $y$ ; hence  $y$  is closest to  $x_*$  and decoding will succeed.

*Finite-temperature decoding:* We now discuss a flexible physics-based approach to decoding the binary symmetric channel, which is focused on entropy rather than strictly on reproducing words / symbols. Define the 1-parameter family of distributions

$$\mu_y^\beta(x) = \frac{1}{Z_\beta} e^{-\beta \varepsilon_p d(y,x)} \mathbb{I}(x \in \mathfrak{c}), \quad (424)$$

where

$$\varepsilon_p \equiv \ln \left( \frac{1-p}{p} \right), \quad (425)$$

with the utility of this definition to become clear shortly. Note that  $\mu_y^{\beta \rightarrow \infty}(x)$  is localized on the closest codeword to  $y$ , thus when  $\beta \rightarrow \infty$  this decoding scheme is equivalent to word MAP. On the other hand, when  $\beta = 1$ ,  $\mu_y^{\beta=1}(x)$  is exactly the distribution of the channel input conditoinal on  $y$ , since the probability of getting a given string  $y$  by flipping bits of  $x$  is  $(1-p)^{N-d} p^d$ , whose  $d$ -dependent part is exactly  $e^{-\varepsilon_p d}$ .

To understand the performance of this decoding procedure in general, we need to estimate the ‘partition function’  $Z_\beta$ . As usual when analyzing condensation phenomena (BECs, the REM, etc.), we separate  $Z_\beta$  into a contribution coming from a ‘zero mode’ (here the *correct* codeword  $x_*$ ) and all of the reamining incorrect codewords:

$$Z_\beta = e^{-\beta \varepsilon_p d(x_*, y)} + \sum_{d=0} \mathcal{N}_y^{in}(d) e^{-\beta \varepsilon_p d} \equiv Z_{\beta, corr} + Z_{\beta, in}, \quad (426)$$

where  $\mathcal{N}_y^{in}(d)$  is the expected number of incorrect codewords at distance  $d$  from  $y$ .  $Z_{\beta, corr}$  is evaluated by using the expected distance  $d(x_*, y) = Np$ , so that

$$Z_{\beta, corr} = e^{-N f_{corr}}, \quad f_{corr} = \beta \varepsilon_p p. \quad (427)$$

Since  $y$  is uncorrelated with all of the incorrect codewords, at  $N \rightarrow \infty$  we may turn the sum over  $d$  into an integral and evaluate it using the saddle point method:

$$\sum_{d=0} \mathcal{N}_y^{in}(d) e^{-\beta \varepsilon_p d} \rightarrow e^{-N f_{in}}, \quad (428)$$

where the ‘free energy density’ of the incorrect codewords is

$$f_{in} = - \max_{\delta \in [\delta_1, \delta_2]} ((R-1) \ln(q) + \delta [\ln(q-1) - \varepsilon_p \beta] + H_2(\delta) \ln 2). \quad (429)$$

For simplicity we will specify to the case of bits ( $q = 2$ ), since that is the case our notation (viz. the definition of  $\varepsilon_p$ ) is best adapted to. In this case  $\delta_2 = 1 - \delta_1$ . If the above maximum is acheived on  $(\delta_1, 1 - \delta_1)$ , then using  $H'_2(\delta) = \log_2((1-\delta)/\delta)$  (so that  $\varepsilon_p = H'_2(p) \ln 2$ ), we find

$$\delta_* = n_F(\varepsilon_p) \quad (430)$$

with  $n_F$  the Fermi distribution at inverse temperature  $\beta$ . If  $\delta_* < \delta_1$ , then the maximum is instead realized at  $\delta_1$ . Expressing  $n_F(\varepsilon_p)$  in terms of  $p$ , the distinction between these two cases occurs at the probability

$$p_* = n_F \left( \frac{1}{\beta^2} \ln(1/\delta_1 - 1) \right). \quad (431)$$

Evaluating  $f_{in}$  in these two cases,

$$f_{in} = \begin{cases} \delta_1 \varepsilon_p \beta & p < p_*, \\ -[(R-1) + H_2(n_F(\varepsilon_p))] \ln 2 + \beta \varepsilon_p n_F(\varepsilon_p) & p \geq p_* \end{cases} \quad (432)$$

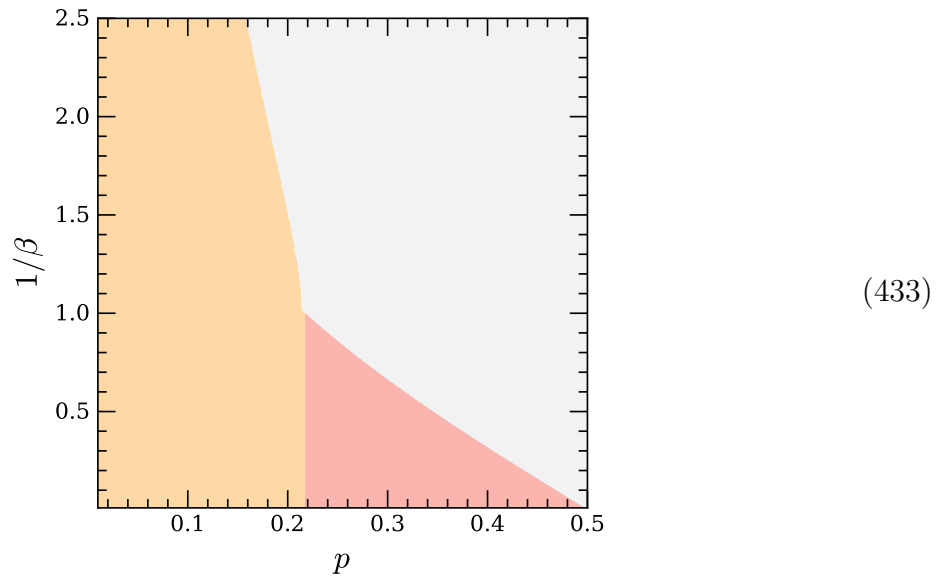
Note that at  $\beta = 1$  — where we reproduce symbol MAP decoding — things simplify on account of  $n_F(\varepsilon_p)|_{\beta=1} = p$  and  $p_* = \delta_1$ .

Decoding will fail if  $f_{in} < f_{corr}$ , for then all of the weight of the distribution  $\mu_y^\beta(x)$  is on the incorrect codewords ( $Z_{corr}/Z_{in} \rightarrow 0$ ). Let us write  $p_{corr}$  as the critical value of  $p$  beyond which  $f_{in} > f_{corr}$ ;  $p < p_{corr}(\beta)$  then defines the correctible phase of the model. In this phase the entropy  $H(\mu_y^\beta)$  vanishes.

Right at  $\beta = 1$ ,  $p < p_{corr}$  is the same as the condition that  $p < p_*$ , since for  $\beta = 1$ ,  $p_* = \delta$ , implying  $f_{in}(p_*) = f_{corr}(p_*)$ . Away from  $\beta = 1$ , this no longer holds, and  $p_*$  defines a separate phase boundary. When  $p_{corr} < p < p_*$ , the distribution is dominated by only the codewords closest to  $x_*$ , since the minimum of the free energy occurs when  $\delta$  is pinned at the lower end of the interval  $[\delta_1, 1 - \delta_1]$  — thus decoding fails, but it does so in the most minimal way possible. This is exactly the same ‘condensation’ phenomenon we saw in the glassy phase of the random energy model. In this regime the entropy  $H(\mu_y^\beta)$  is sublinear in  $N$ , since all of the weight of the partition function is codewords of distance  $\delta_1$ .

By contrast when  $p > p_*$ ,  $p_{corr}$  then not only does decoding fail, but the typical codeword chosen is at a distance  $N\delta_* = Nn_F(\varepsilon_p)$  away from  $x_*$ , which is much larger than the minimal distance — this is the ‘paramagnetic’ phase, and  $H(\mu_y^\beta)$  is linear in  $N$ . It is easy to show that  $p_{corr} > p_*$  when  $\beta < 1$  (large  $T$ ), but that  $p_{corr} < p_*$  when  $\beta > 1$  (small  $T$ ). Thus for symbol MAP decoding one transitions straight from the correctible phase to the paramagnetic phase, while for lower temperatures there is an intermediate glassy regime. Since  $p_*(\beta \rightarrow \infty) = 1/2$ , at zero temperature the glassy phase ends at  $p = 1/2$ , as expected.

The phase diagram extracted from the above analysis is (drawn with a code rate of  $R = 1/4$ )



where the orange region is the correctible phase, the gray region is the paramagnetic phase,

and the red region is the glassy phase (the  $p < p_*$  curve extends smoothly into the correctible phase).



## TDVP benchmarking with quantum quenches

---

In today’s diary entry, we benchmark some TDVP code by looking at its ability to reproduce the ‘dynamical quantum phase transition’ that occurs when quenching across the QCP in the TFIM. See e.g. the review [4] for a review on DQPTs.

⚡ ⚡

We will benchmark the use of TDVP to evolve a wavefunction  $|\psi\rangle$  by comparing it against what we get from directly applying trotterized gates to  $|\psi\rangle$  (TEBD).<sup>30</sup> Note that just like DMRG, TDVP can be done by simultaneously evolving either one or two MPS tensors. Evolving only a single MPS tensor has the advantage that it *exactly* conserves both energy and probability (i.e.  $|\psi\rangle$  remains normalized), but has the drawback that there is no way of adaptatively changing the bond dimension  $\chi$ , which is often needed when quenching since the initial and final states will usually have different amounts of entanglement. The two-site variant on the other hand lets one change  $\chi$  by doing SVDs on the two-site block, but has the problem that doing so will lead to energy and probability no longer being conserved. When doing quenches in practice, one approach is to use the two-site variant and dynamically increase  $\chi$  as needed until it hits some threshold  $\chi_*$ . At this point we switch over to the single-site variant, which lets us push to higher times while still conserving energy (of course pushing to higher  $t$  will lead to an inevitable loss of fidelity, but depending on what one is interested in calculating, this may not really matter). Another approach is to run the two-site variant until the deviations in norm / energy cross some threshold, at which point one switches to the single-site variant.

The concrete setting we will focus on is a TFIM of the form

$$H = - \sum_i Z_i Z_{i+1} + g(t) \sum_i X_i, \quad (434)$$

where

$$g(t) = g_i \Theta(-t) + g_f \Theta(t), \quad (435)$$

---

<sup>30</sup>We also benchmarked TDVP against ED at small system sizes, but the plots aren’t shown here.

with  $g_i < 1, g_f > 1$ . The DQPT manifests itself as a non-analyticity in the Loschmidt echo, which we will define as

$$\mathcal{L}(t) \equiv -\frac{1}{L} \log(|\langle \psi_i | e^{-iH_f t} | \psi_i \rangle|^2), \quad (436)$$

where  $L$  is the chain length,  $|\psi_i\rangle$  is the ground state of  $H_i \equiv H(t < 0)$ , and  $H_f \equiv H(t > 0)$ .

In the setting of the Ising model, the locations of the singularities in  $\mathcal{L}(t)$  can be worked out analytically (see e.g. the review cited above and references therein); in the TDL they occur at times

$$t_n^* = t^*(n + 1/2), \quad n \in \mathbb{N}, \quad (437)$$

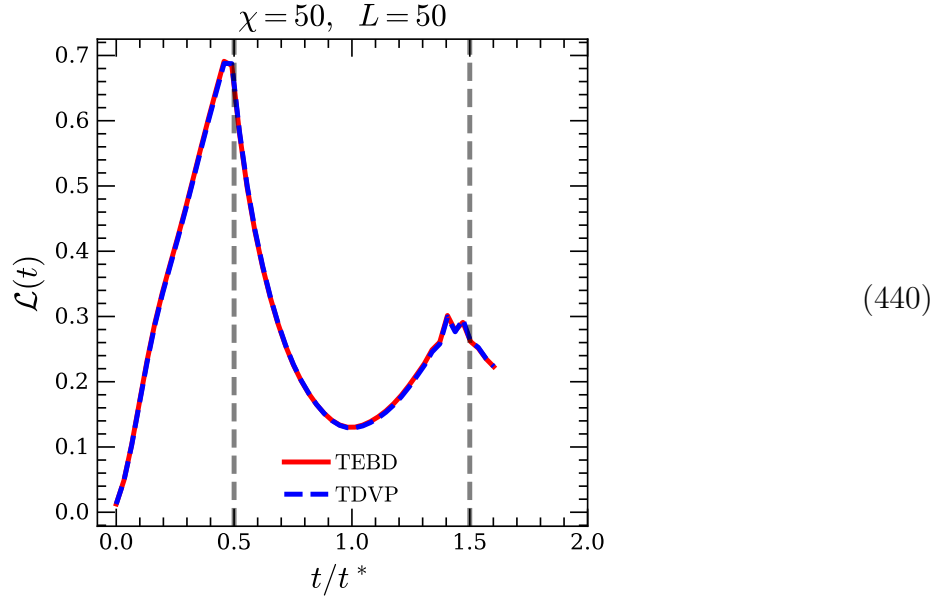
where

$$t^* = \frac{\pi}{\varepsilon_{k^*}(g_f)}, \quad k^* = \arccos\left(\frac{1 + g_i g_f}{g_i + g_f}\right) \quad (438)$$

and with the quasiparticle dispersion

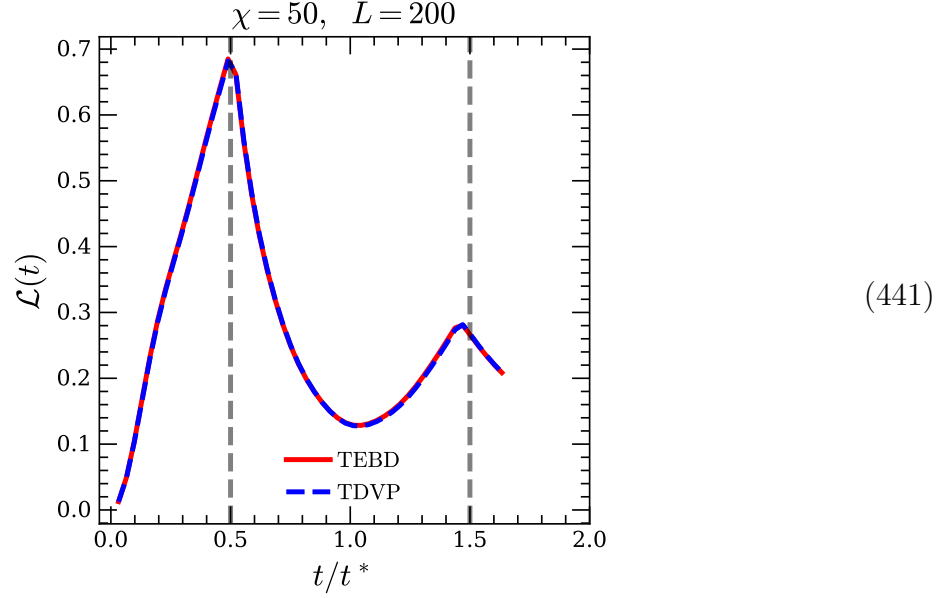
$$\varepsilon_k(g) = \sqrt{(g - \cos(k))^2 + \sin^2(k)}. \quad (439)$$

Below we use the two-site variant of TDVP until the bond dimension reaches  $\chi_* = 50$ , at which point we switch over to the one-site variant. This is compared against TEBD with the same cutoff on  $\chi$ . For a big quench from  $g_i = 1/2$  to  $g_f = 2$  (and step size  $\delta t = 0.075$ ), we get for  $L = 50$



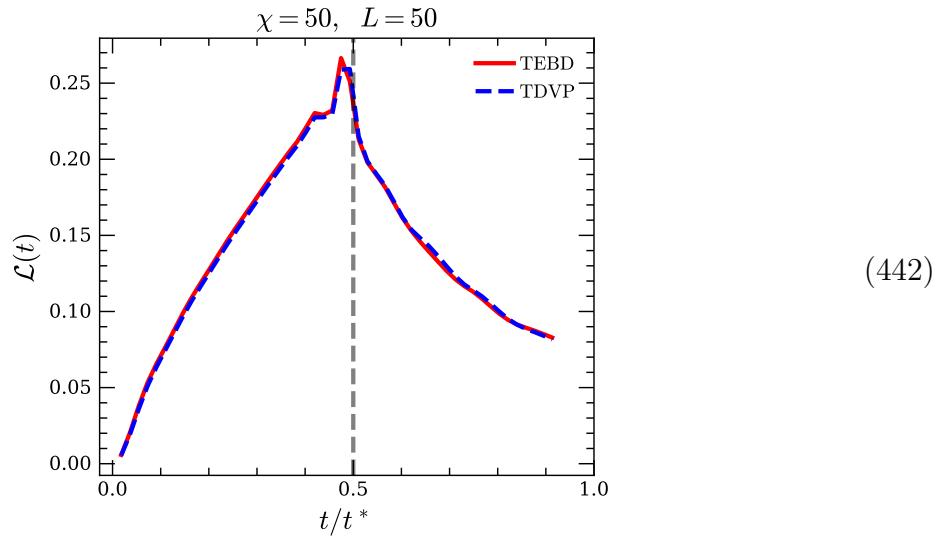
where things have basically the right shape, but with peaks that don't quite fall at the expected places. In this quench TDVP never actually saturated the bond dimension, while TEBD saturated at  $t \approx 1$ . The deviation of energy  $\delta E \equiv |(E_f - E_i)/E_i|$  (with  $E_i = \langle \psi_i | H_f | \psi_i \rangle$  and  $E_f = \langle \psi_f | H_f | \psi_f \rangle$ , where  $|\psi_f\rangle$  is the TDVP / TEBD - evolved wavefunction) was  $\delta E \sim 10^{-5}$  for TDVP, and  $\sim 10^{-3}$  for TEBD (which ran 3x faster). Increasing the

system size to  $L = 200$ ,

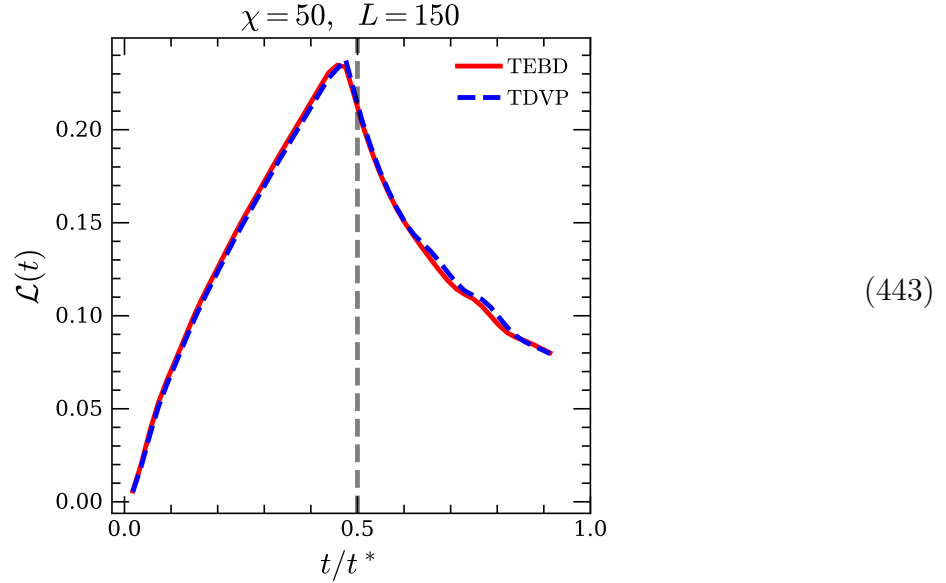


which looks pretty good (here  $\delta E$  is about the same as in the previous plot).

To get an example where the two algorithms noticeably differ, we can perform a quench which is narrower wrt the critical point. Taking  $g_i = 3/4$  and  $g_f = 5/4$  (for which  $t^* \approx 8$  is 4ish times larger than in the previous example), we find



Here TEBD has  $\delta E \sim 0.04$ . Going to  $L = 150$ ,



which took  $O(10)$  minutes on my laptop. Here  $\delta E \sim 0.2$  and  $|\psi_f| \sim 0.9$  for TEBD, while TDVP has basically no problems with this quantities (TDVP also gets a sharper kink at the DQPT but this is hard to see in the present plot).



## Page's theorem

---

This entry is devoted to a quick proof of Page's theorem, or rather of a morally equivalent (but easier to prove) result pertaining to the trace distance between a random reduced density matrix and the maximally mixed state. Incidentally Page's original paper [6] is actually worth a read, if only for a lesson in how to *not* write a PRL.



First recall the intuitive argument for the theorem: for a random bipartite state, entanglement is spread out equally across Hilbert space (after all, how else could it be spread out?). Consider then a Hilbert space  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$  and let  $d = \dim \mathcal{H}$ ,  $d_\alpha = \dim(\mathcal{H}_\alpha)$ ,  $|\alpha| = \log \dim(\mathcal{H}_\alpha)$ . Suppose wolog that  $|B| \leq |A|$ . Then  $d_B/d_A$  is exponentially tiny in  $2^{-|A|/|B|} \rightarrow 0$ . Since entanglement is spread out uniformly in a random pure state, this means that the degrees of freedom in  $B$  are essentially all entangled with those in  $A$ , rather than

with other dof in  $B$ . This then means that  $\rho_A$  is very close to  $\mathbf{1}_A/d_A$ , in a sense that we will quantify shortly. Note that if one does not care about making ‘very close’ precise, this statement is essentially trivial and not in need of proof. Nevertheless it is perhaps good to go through the mechanics of the calculation.

To this end let  $|\psi\rangle$  be any state in  $\mathcal{H}$ , and define

$$\rho_A(U) \equiv \text{Tr}_B[U|\psi\rangle\langle\psi|U^\dagger], \quad (444)$$

where  $U$  is a unitary in  $L^2(\mathcal{H})$ . We are interested in computing

$$\delta \equiv \mathbb{E}_U[||\rho_A(U) - \mathbf{1}/d_A||_1] \quad (445)$$

where  $U$  is drawn from the Haar measure. We first bound the expectation of the 1-norm as

$$\begin{aligned} \delta &\leq \sqrt{\mathbb{E}_U[||\rho_A(U) - \mathbf{1}/d_A||_1^2]} \\ &\leq \sqrt{d_A \mathbb{E}_U[||\rho_A(U) - \mathbf{1}/d_A||_2^2]}, \end{aligned} \quad (446)$$

where we used Jensen's inequality<sup>31</sup> to write  $\mathbb{E}[X]^2 \leq \mathbb{E}[X^2]$  and used  $||X||_1 \leq \sqrt{d}||X||_2$  for  $X \in L^2(\mathbb{C}^d)$ . The expectation of the squared 2-norm can be expanded in terms of the average purity as

$$\mathbb{E}_U[||\rho_A(U) - \mathbf{1}/d_A||_2^2] = \mathbb{E}_U[\text{Tr}[\rho_A(U)]^2] - 1/d_A. \quad (447)$$

We now directly calculate the average purity using

$$\mathbb{E}_U[U_{ij}U_{kl}U_{mn}^\dagger U_{op}^\dagger] = \frac{1}{d^2 - 1} \left( \delta_{in}\delta_{jm}\delta_{kp}\delta_{lo} + \delta_{ip}\delta_{jo}\delta_{kn}\delta_{lm} - \frac{1}{d}(\delta_{in}\delta_{jo}\delta_{kp}\delta_{lm} + \delta_{ip}\delta_{kn}\delta_{jm}\delta_{lo}) \right). \quad (448)$$

Using composite indices  $I = (i, i')$  to index bases of  $\mathcal{H}$  (with  $|i\rangle$  a basis of  $\mathcal{H}_A$  and  $|i'\rangle$  a basis of  $\mathcal{H}_B$ ), the average purity is

$$\begin{aligned} \mathbb{E}_U[\text{Tr}[\rho_A(U)]^2] &= \mathbb{E}_U[U_{IJ}U_{KL}U_{MN}^\dagger U_{OP}^\dagger \psi_J \psi_M^* \psi_L \psi_O^* \delta_{i'n'} \delta_{k'p'} \delta_{nk} \delta_{pi}] \\ &= \sum_{I K J L} \frac{1}{d^2 - 1} \psi_J \psi_J^* \psi_L \psi_L^* (\delta_{ik} + \delta_{i'k'}) (1 - 1/d) \\ &= \frac{d_A + d_B}{d + 1} \end{aligned} \quad (449)$$

where we wrote  $|\psi\rangle = \sum_I \psi_I |I\rangle$ ; note that the dependence on  $\psi$  is removed by normalization as required. Some easy algebra then gives

$$\delta \leq \sqrt{\frac{d_A^2 - 1}{d_A d_B + 1}} \approx \sqrt{\frac{d_A}{d_B}}. \quad (450)$$

Thus  $\rho_A$  is on average exponentially close to  $\mathbf{1}/d_A$  as soon as  $A$  gets smaller than  $B$ .

---

<sup>31</sup>Recall that Jensen's inequality says that if  $f$  is any convex (positive second derivative) function (such as  $f(X) = X^2$  in the present example), then  $f(\mathbb{E}[X]) \leq \mathbb{E}[f(X)]$ .



Given this starting point, it is also easy to e.g. derive things like the average entropy, which for  $d_A/d_B \ll 1$  is

$$\mathbb{E}_U(S(\rho_A(U))) \approx |A| - \frac{d_A}{2d_B}, \quad (451)$$

so that  $\rho_A$  is exponentially close to having a volume law.



## Local complements in graph states

---

Today we will be proving a simple fact about graph states stated (without proof) in an appendix of [3].



Fix a graph  $G = (E, V)$  and let  $|G\rangle$  denote the graph state

$$|G\rangle \equiv \prod_{l \in E} CZ_l \bigotimes_{v \in V} |+\rangle_v. \quad (452)$$

For a vertex  $v \in V$ , we define the graph  $G_{\bar{v}}$  — the local complement of  $G$  at  $v$  — by replacing the subgraph  $N_v \subset G$  defined by the neighbors of  $v$  with its complement  $\bar{N}_v$ . To say this in a clearer way, define

$$\mathbf{E}_G(u, w) = \begin{cases} 1 & (u, w) \in E(G) \\ 0 & (u, w) \notin E(G) \end{cases} \quad (453)$$

Then  $\mathbf{E}_{G_{\bar{v}}}(u, w) = \mathbf{E}_G(u, w)$  if at most one of  $(u, w)$  belong to  $N_v$ , while  $\mathbf{E}_{G_{\bar{v}}}(u, w) = \neg \mathbf{E}_G(u, w)$  if both  $u, w \in N_v$ .

Our goal is to prove the following fact:

**Proposition 5.** *The local complement operation can be implemented (up to a phase) by acting on  $|G\rangle$  with the single-site unitary*

$$U_v \equiv \exp\left(-i\frac{\pi}{4}X_v\right) \prod_{u \in V(N_v)} \exp\left(i\frac{\pi}{4}Z_u\right). \quad (454)$$

That is,  $|G_{\bar{v}}\rangle \propto U_v|G\rangle$ , where the proportionality constant is a  $U(1)$  phase.

This immediately implies

**Corollary 1.** *Taking local complements does not modify the entanglement entropy of graph states.*

Note that the full graph complement cannot be obtained in general from taking successive local complements (just consider the triangle graph to see why).

At face value this proposition is perhaps quasi-surprising. The most obvious way of turning  $|G\rangle$  into  $|G_{\bar{v}}\rangle$  is via the unitary

$$\mathcal{C}_v \equiv \prod_{(u,w) \in E(N_v)} CZ_{(u,w)}. \quad (455)$$

Applying random CZ gates to  $|G\rangle$  will of course generically change the state's entanglement, and thus the proposition can hold only by virtue of the geometric structure present in the local complement operation.

*Proof.* One way of proving this is to simply re-write the action of  $U_v$  on  $|G\rangle$  in terms of only  $Z_u$  operators, and to then show that the resulting expression matches the expansion of the control gates in  $\mathcal{C}_v$  in terms of  $Z_u$  operators. Using that

$$X_v|G\rangle = \prod_{u \in V(N_v)} Z_u|G\rangle, \quad (456)$$

we find

$$U_v \approx 2^{-(|N_v|+1)/2} \sum_{\mathbf{s} \in \mathbb{Z}_2^{|N_v|}} i^{|\mathbf{s}|} (Z^{\mathbf{s}} - iZ^{-\mathbf{s}}), \quad (457)$$

where  $\approx$  means equivalence when acting on  $|G\rangle$ ,  $|N_v|$  means the number of vertices in the subgraph  $N_v$ , and  $Z^{\mathbf{s}}$  denotes a  $\otimes$  of  $Z_u$  operators over the vertices in  $V(N_v)$ . As the simplest example, consider the case when  $G$  is a 1d lattice. Then if  $l, r$  are the vertices to the left and right of  $v$ , the unitary which implements the local complement at  $v$  is clearly just  $CZ_{(l,r)}$ . On the other hand, in this case the above formula gives

$$U_v \approx 2^{-3/2} (1 - iZ_l Z_r + i(Z_l + Z_r - iZ_l - iZ_r) - (Z_l Z_r - i)) = \frac{1+i}{\sqrt{2}} \frac{1 + Z_l + Z_r - Z_l Z_r}{2}, \quad (458)$$

which is indeed proportional to  $CZ_{(l,r)}$ .

Proving that the signs always work out in this way is slightly annoying, and instead it is easier to simply check that the stabilizers of  $U_v|G\rangle$  match with those of  $|G_{\bar{v}}\rangle$ . Define the  $|G\rangle$  stabilizers

$$\mathcal{S}_u \equiv X_u \prod_{w \in V(N_u)} Z_w. \quad (459)$$

We now look for a set of stabilizers  $\mathcal{S}_u^{\bar{v}}$  for the state  $|G_{\bar{v}}\rangle$ . We take

$$\mathcal{S}_u^{\bar{v}} = X_u \prod_{w \in S_u} Z_w \quad (460)$$

for some as-yet-undetermined set of vertices  $S_u$ , with  $u \notin S_u$ .

Consider first the case when  $u \notin V(N_v)$ . We see first that  $\mathcal{S}_v^{\bar{v}} = \mathcal{S}_v$ , on account of

$$[\mathcal{S}_v^{\bar{v}}, U_v] = 0. \quad (461)$$

If  $u \notin V(N_v)$  and  $u \neq v$ ,

$$\mathcal{S}_u^{\bar{v}} U_v = U_v (iZ_v)^{v \in S_u} \mathcal{S}_u^{\bar{v}}, \quad (462)$$

where  $\mathcal{O}^{a \in X}$  is equal to  $\mathcal{O}$  if  $a \in X$  and equal to  $\mathbf{1}$  else. The operator  $(iZ_v)^{v \in S_u} \mathcal{S}_u^{\bar{v}}$  will only stabilize  $|G\rangle$  if  $v \notin S_u$  and  $\mathcal{S}_u^{\bar{v}} = \mathcal{S}_u$ . Thus if  $u \notin V(N_v)$ , then  $\mathcal{S}_u^{\bar{v}} = \mathcal{S}_u$ , and the only change in the stabilizers can occur for those centered on vertices of  $N_v$ .

Thus consider the case when  $u \in N_v$ . A similar argument as in the previous paragraph shows that in this case we must require  $v \in S_u$ . Taking  $v \in S_u$  then, we have

$$\mathcal{S}_u^{\bar{v}} U_v = U_v (-iZ_u) (-iX_v) X_u \prod_{w \in S_u} Z_w. \quad (463)$$

When acting on  $|G\rangle$ , the RHS becomes

$$(-iZ_u) (-iX_v) X_u \prod_{w \in S_u} Z_w |G\rangle = \prod_{p \in V(N_u)} Z_p \prod_{q \in V(N_v) \setminus \{u\}} Z_q \prod_{w \in S_u} Z_w |G\rangle. \quad (464)$$

Therefore if  $\mathcal{S}_u^{\bar{v}}$  is to stabilize  $U_v |G\rangle$ , we need  $S_u$  to be the symmetric difference between the neighbors of  $v$  and those of  $u$  (minus  $u$ ), viz.

$$S_u = [(V(N_v) \cup V(N_u)) \setminus (V(N_v) \cap V(N_u))] \setminus \{u\} \quad (465)$$

A moments thought shows that this is precisely equal to the neighbors of  $u$  in the local complement graph  $G^{\bar{v}}$ . Thus the stabilizers of  $U_v |G\rangle$  are the same as those of  $|G^{\bar{v}}\rangle$ , proving the claim. □



## Bit commitment

---

In this diary entry we consider two parties  $A, B$  who wish to engage in bit commitment by exchanging quantum states. We will see that this is impossible without any extra assumptions, and provide one possible physically-motivated work around.



### *first attempt at a protocol*

Suppose  $A$  transmits  $b$  by sending  $B$  the state  $H^b|r\rangle$ , where  $r \in \{0, 1\}$  is uniformly random. During the reveal phase,  $A$  sends  $(b, r)$  to  $B$ , who then checks if the state  $|\mathcal{R}\rangle$  he receives from  $A$  indeed satisfies  $\langle r|H^b|\mathcal{R}\rangle = 1$ .

Let us first address validity. If  $A$  follows the protocol, then we indeed have  $H^b|\mathcal{R}\rangle = |r\rangle$ . When  $B$  performs a measurement in the computational basis, he has 0 probability of getting  $|\bar{b}\rangle$  (here  $\bar{x} \equiv x \oplus 1$ ). Thus  $B$  never rejects if the protocol is followed, and the protocol is valid.

Is it hiding? Suppose  $A$  follows the protocol, and  $r$  is indeed uniformly random. Then a nefarious  $B$  is faced with the task of distinguishing

$$\rho_0 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}\mathbf{1}, \quad \rho_1 = H\rho_0H = \mathbf{1}, \quad (466)$$

which is impossible. Therefore the protocol is also hiding.

What about binding? Suppose  $A$  gives  $B$  the state  $|\mathcal{R}\rangle = H^b|r\rangle$ , but then commits  $(b', r')$ . When  $B$  follows the protocol and applies  $H^{b'}$  to  $|\mathcal{R}\rangle$ , he is left with  $H^{b+b'}|r\rangle$ , and he accepts with probability

$$P_{acc} = |\langle r'|H^{b+b'}|r\rangle|^2. \quad (467)$$

We can evaluate the bindingness of this protocol by looking at  $A$ 's ability to get  $B$  to accept a reveal bit of her choosing, averaged over many trials with different committed bits  $b$ . We let  $P_b$  be the probability that  $A$  gets  $B$  to accept the reveal  $(b', r')$ , averaged over  $b$  (with  $b$  drawn from the uniform measure). The protocol is not binding if  $A$  gets her way more than possible by chance, i.e. if

$$P_0 + P_1 > 1. \quad (468)$$

In this protocol, it is easy to check that

$$P_0 = P_1 = \frac{1}{2} (|\langle r'|r\rangle|^2 + |\langle r'|H|r\rangle|^2). \quad (469)$$

If  $r' = \bar{r}$ , then  $P_0 = P_1 = 1/2$ , which does not give  $A$  a successful attack on the protocol. If  $r' = r$ , then  $P_0 = P_1 = 3/4$ , so that  $P_0 + P_1 = 3/2 > 1$ . Thus by choosing  $r' = r$ ,  $A$  can give a successful attack on the protocol, and the scheme is not binding.

### *second attempt*

Now let us try flipping the roles of  $b, r$  in the above protocol:  $A$  sends  $B$  the state  $H^r|b\rangle$ , commits  $(b, r)$ , and  $B$  checks whether or not  $|\langle b|H^r|\mathcal{R}\rangle| = 1$ . This protocol is valid, for the same reason as before.

Is it hiding? Now the two reduced density matrices that  $B$  must distinguish between are (again assuming  $A$  follows the protocol, so that  $r$  is uniformly random)

$$\rho_0 = \frac{1}{2}(|0\rangle\langle 0| + H|0\rangle\langle 0|H), \quad \rho_1 = \frac{1}{2}(|1\rangle\langle 1| + H|1\rangle\langle 1|H). \quad (470)$$

But then

$$\|\rho_0 - \rho_1\|_1 = \frac{1}{\sqrt{2}} \|H\|_1 > 0, \quad (471)$$

and so the protocol is clearly not hiding. Using the result from the above discussion on trace distance,  $B$  can make a guess with failure probability

$$P_{err} = \frac{1}{2} - \frac{1}{4} \|\rho_0 - \rho_1\|_1 = \frac{1}{2}(1 - 1/\sqrt{2}) < 1/2. \quad (472)$$

What about binding? We can adopt the same test as applied above. Here

$$P_0 = P_1 = \frac{1}{2} \left( |\langle 0 | H^{r+r'} | 0 \rangle|^2 + |\langle 0 | H^{r+r'} | 1 \rangle|^2 \right). \quad (473)$$

Regardless of whether  $r = \bar{r}'$  or  $r = r'$ ,  $P_0 = P_1 = 1/2$ , and  $A$  is not able to stack the odds in her favor. Thus this protocol is indeed binding. Therefore we have constructed protocols which are perfectly binding or perfectly hiding, but not both.

### *security from noisy storage*

Suppose that  $B$  stores his qubits in some noisy memory, where the noise is ‘trusted’ and is not assumed to have any agency vis-a-vis affecting the outcome of the BC protocol. Operationally, this means that  $B$  *must* measure his qubit(s) as soon as he receives them from  $A$ .

Recall that the attack on our first protocol came from  $A$ , who could manipulate her reveal bits so as to tilt the odds in her favor. With the present noisy memory constraint, the measurement has to be performed at the commit phase!

One possible protocol is as follows.  $B$  chooses to measure the recieved qubit in the  $z$ -basis after applying  $H^c$ , where  $c$  is the outcome of a random coin controlled by  $B$ . The protocol proceeds with  $A$  revealing  $(b, r)$ . Suppose  $b = 0$ . If  $c = 0$ , then  $B$  knows the value of  $r$  upon measurement, and the protocol is sound. If  $c = 1$ , then the outcome of  $B$ ’s measurement has a  $1/2$  chance of agreeing with  $r$ . The reverse is true if  $b = 1$ , and in both cases, the protocol has a  $3/4 > 1/2$  chance of being accepted, so that the protocol is valid (but not perfectly so). The protocol is hiding for the same reason as before.

The question is whether or not the immediate measurement has removed  $A$ ’s ability to cheat. Consider computing  $P_0$ . Then  $A$  commits  $(0, r')$ . To find  $P_0$ , we compare the actual state that  $B$  performed a measurement on with the state that  $A$  claimed  $B$  performed a measurement on. Taking  $b$  to be distributed uniformly as before,  $B$ ’s acceptance probability (on setting  $r' = r$ ) seems to be

$$P_0 = \frac{5}{8}, \quad (474)$$

which unfortunately is larger than  $1/2$ . Perhaps there is a better protocol that I am missing.

### *hiding amplification*

Consider a BC scheme which is perfectly valid and binding, but only  $\varepsilon$ -hiding (so that  $P_{guess} = 1/2 + \varepsilon$ ). We can amplify hiding as follows. If  $A$  wishes to commit  $b$ , she chooses

$b = 0$	actual	claimed
$c = 0$	$ r\rangle$	$ r'\rangle$
$c = 1$	$H r\rangle$	$H r'\rangle$
$b = 1$	actual	claimed
$c = 0$	$H r\rangle$	$ r'\rangle$
$c = 1$	$ r\rangle$	$H r'\rangle$

two bits  $b_{1,2}$  randomly, subject to the constraint that  $b_1 \oplus b_2 = b$ . She then commits  $b_{1,2}$  under the  $\varepsilon$ -hiding scheme. If  $B$ 's best strategy is to just guess  $b_{1,2}$  separately (and then to compute  $b_{\text{guess}} = b_{1,\text{guess}} \oplus b_{2,\text{guess}}$ ), then the hiding improves. Indeed, we now have

$$P_{\text{guess}} = P_{\text{both right}} + P_{\text{both wrong}} = (1/2 + \varepsilon)^2 + (1/2 - \varepsilon)^2 = \frac{1}{2} + 2\varepsilon^2. \quad (475)$$

So as long as  $\varepsilon < 1/2$ , we can iterate this strategy to get a scheme with arbitrarily good hiding (by the impossibility of BC, evidently such an  $\varepsilon$ -hiding but otherwise perfect BC scheme does not exist).



## Distinguishing states with measurements and some facts about dual norms

---

In this diary entry we prove some simple facts about  $L_p$  norms and their duals, and use them to solve a baby state discrimination problem.



### *distinguishing between two states: setup*

We are given one of two  $d$ -dimensional states  $\sigma_1, \sigma_2$ , and asked to do our best to distinguish between  $\sigma_1$  and  $\sigma_2$  using a two-outcome measurement given by Hermitian matrices  $M_1 = M, M_2 = \mathbf{1} - M$ . The probability of guessing wrong is

$$\begin{aligned} P_{\text{err}} &= p_1 \text{Tr}[\sigma_1 M_2] + p_2 \text{Tr}[\sigma_2 M_1] = \text{Tr}[p_1(\sigma_1 - \sigma_1 M) + p_2 \sigma_2 M] = p_1 + \text{Tr}[M(p_2 \sigma_2 - p_1 \sigma_1)] \\ &\equiv p_1 + \text{Tr}[M \Delta]. \end{aligned} \quad (476)$$

In the following we will see how to choose  $M$  so as to minimize  $P_{\text{err}}$ .

### *dual norms*

Define the dual norm by

$$||X||_p^\vee \equiv \max_{||\Lambda||_p \leq 1} |\text{Tr}[X\Lambda]|. \quad (477)$$

This is easily checked to be a norm; the only slightly non-trivial part is the  $\Delta$  inequality: we have

$$||X + Y||_p^\vee = \max_{||\Lambda||_p \leq 1} |\text{Tr}[X\Lambda] + \text{Tr}[Y\Lambda]|. \quad (478)$$

The RHS is however obviously  $\leq ||X||_p^\vee + ||Y||_p^\vee$ , since unless the same  $\Lambda$  maximizes both traces, one of the traces will be sub-maximal, giving a  $\leq$ .

To relate  $||X||_p^\vee$  to one of the  $L_q$  norms, it is convenient to use Holder's inequality, which says that for all  $p$ ,

$$|\langle X, Y \rangle| \leq ||X||_p ||Y||_{p^\vee}, \quad (479)$$

where  $p^\vee \equiv (1 - 1/p)^{-1}$  (which satisfies  $1/p + 1/p^\vee = 1$ ), and for us the inner product is  $\langle X, Y \rangle = \text{Tr}[XY^\dagger]$ . When  $p = 2$  we have  $p^\vee = 2$  and the above inequality is just CS. When  $p = 1$  we have  $p^\vee = \infty$ , and Holder's inequality is easy to check. Indeed, letting  $\mathbf{x}$  and  $\mathbf{y}$  be the (sorted) eigenvalues of  $X$  and  $Y$  (we will take  $X, Y$  to be Hermitian for notational simplicity), the inner product is

$$|\langle X, Y \rangle| = \mathbf{x}^T \Gamma \mathbf{y}, \quad (480)$$

where  $\Gamma_{ij} = |\langle x_i | y_j \rangle|^2$ , with  $|x_i\rangle, |y_j\rangle$  the corresponding eigenvectors of  $X, Y$ .  $\Gamma$  is a doubly stochastic matrix (at least if we assume no degeneracies; dealing with them is straightforward), and hence  $\Gamma = \sum_\sigma p_\sigma \hat{\sigma}$ , where  $\hat{\sigma}$  is a permutation matrix and  $\sum_\sigma p_\sigma = 1$ . Since  $\mathbf{x}, \mathbf{y}$  are the sorted eigenvalues, the inner product is maximal if  $\Gamma = \mathbf{1}$  (or in general, if  $\Gamma = \hat{\sigma}$ , where  $\sigma$  is the permutation from the sorted basis of  $X$  to the sorted basis of  $Y$ ). Thus

$$|\langle X, Y \rangle| \leq |\mathbf{x} \cdot \mathbf{y}| \leq \max_i |x_i| ||\mathbf{y}||_1 = ||X||_\infty ||Y||_1. \quad (481)$$

Using Holder's inequality, we thus have

$$||X||_p^\vee \leq ||X||_{p^\vee}, \quad (482)$$

where equality holds if there exists some  $\Lambda$  such that  $||\Lambda||_p = 1$  and  $|\text{Tr}[X\Lambda]| = ||X||_{p^\vee}$ . Such a  $\Lambda$  is however easy to find. Let  $\Lambda = \text{diag}(\boldsymbol{\lambda})$  be diagonal in  $X$ 's eigenbasis, with  $||\Lambda||_p = 1$ . Take the ansatz  $\lambda_i = \text{sgn}(x_i) |x_i|^\alpha / \mathcal{N}$ , where  $\mathcal{N}$  ensures  $||\Lambda||_p = 1$ . Then

$$|\text{Tr}[X\Lambda]| = \frac{\sum_i |x_i|^{1+\alpha}}{(\sum_i |x_i|^{p\alpha})^{1/p}}. \quad (483)$$

In order for the RHS to be  $||X||_{p^\vee}$ , we need  $1 + \alpha = p\alpha$ ; thus  $\alpha = 1/(p - 1)$ . Plugging in to the above, we see that the RHS is indeed equal to  $||X||_{p^\vee}$ . Thus

$$||X||_p^\vee = ||X||_{p^\vee}. \quad (484)$$

### *optimal choice of $M$*

We now want to find the PSD operator  $M$  (with  $\|M\|_\infty \leq 1$ ) which minimizes  $P_{err}$ . Letting  $|\Delta_i\rangle$  be the eigenvectors of  $\Delta$ ,

$$\text{Tr}[M\Delta] = \sum_i \Delta_i \langle \Delta_i | M | \Delta_i \rangle. \quad (485)$$

Since  $M$  is PSD,  $\Delta_i \langle \Delta_i | M | \Delta_i \rangle > 0$  for all  $i$ . Therefore to minimize  $\text{Tr}[M\Delta]$ ,  $M$  cannot have any support on the space generated by  $\{|\Delta_i\rangle | \Delta_i > 0\}$ . Using the same stochastic matrix argument as above, we see that the best choice is to make  $M$  simultaneously diagonalizable with  $\Delta$ , by taking  $M = \sum_{\Delta_i < 0} |\Delta_i\rangle \langle \Delta_i|$ . With this choice,

$$P_{err,opt} = p_1 - \sum_{\Delta_i < 0} |\Delta_i|. \quad (486)$$

### *examples*

We now evaluate  $P_{err,opt}$  in a few instructive cases.

- $p_1 = 1, p_2 = 0$ . In this case  $\Delta = -p_1\sigma_1$ , and all eigenvalues are negative (so that  $M = \mathbf{1}$ ). Then  $P_{err,opt} = p_1(1 - \text{Tr}[\sigma_1]) = 0$ , as required.
- $p_1 \geq 1/2$  and  $\sigma_1 = \sigma_2$ . Then  $\Delta = (1 - 2p_1)\sigma_1$ , and again all eigenvalues of  $\Delta$  are non-positive, so that  $M = \mathbf{1}$ . Then

$$P_{err,opt} = 1 - p_1. \quad (487)$$

This makes sense because here we are just guessing the outcome of a biased coin flip.

- $p_1 = 1/2$ , with arbitrary  $\sigma_1, \sigma_2$ . In this case it is helpful to write

$$P_{err,opt} = \frac{1}{2} - \frac{1}{2} \max_{\|\Lambda\|_\infty \leq 1} \text{Tr}[(-\Delta)(\mathbf{1} + \Lambda)], \quad (488)$$

where we have written  $M = (\mathbf{1} + \Lambda)/2$ ; here  $\|M\|_\infty \leq 1$  if  $\|\Lambda\|_\infty \leq 1$ , with the identity matrix ensuring that  $M$  is PSD. Since  $\text{Tr}[\Delta] = \frac{1}{2}\text{Tr}[\sigma_1 - \sigma_2] = 0$ , we have

$$\begin{aligned} P_{err,opt} &= \frac{1}{2} - \frac{1}{2} \max_{\|\Lambda\|_\infty \leq 1} \text{Tr}[(-\Delta)\Lambda] \\ &= \frac{1}{2}(1 - \|\Delta\|_\infty^\vee) = \frac{1}{2}(1 - \|\Delta\|_1) \\ &= \frac{1}{2} - \frac{1}{4}\|\sigma_1 - \sigma_2\|_1. \end{aligned} \quad (489)$$

A sanity check here is that  $\sigma_1 = \sigma_2$  implies  $P_{err,opt} = 1/2$ . Alternatively, if  $\text{Supp}(\sigma_1) \cap \text{Supp}(\sigma_2) = \emptyset$ , then  $\|\sigma_1 - \sigma_2\|_1 = 4$ , and we get  $P_{err,opt} = 0$ , as required.



- $p_1 = 1/2$  and  $\sigma_1 = |\psi_1\rangle\langle\psi_1|, \sigma_2 = |\psi_2\rangle\langle\psi_2|$ . From the above, we need only evaluate  $|||\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2|||_1$ . We do this by orthogonalizing, defining the vector  $|\phi\rangle \equiv (|\psi_2\rangle - |1\rangle c)/\sqrt{1-|c|^2}$ , where  $c \equiv \langle\psi_1|\psi_2\rangle$ . Then

$$\sigma_1 - \sigma_2 = (1 - |c|^2)(|\psi_1\rangle\langle\psi_1| - |\phi\rangle\langle\phi|) - \sqrt{1 - |c|^2}(c|\psi_1\rangle\langle\phi| + h.c.), \quad (490)$$

which has eigenvalues  $\pm\sqrt{1 - |c|^2}$ . Therefore

$$P_{err,opt} = \frac{1}{2}(1 - \sqrt{1 - |c|^2}) = \frac{1}{2}(1 - |\sin \theta|), \quad (491)$$

where  $\theta = \cos^{-1}(|c|)$ . When  $\theta = 0$  the two states are gauge equivalent, and our best strategy is simply to randomly guess. When  $\theta = \pm\pi/2$  the two states are orhtogonal, and so as above we get  $P_{err,opt} = 0$ .



## Channel fidelities

---

Consider a compression scheme for a dmat  $\rho$ . Let  $\mathcal{N} = \mathcal{E} \circ \mathcal{D}$  be the quantum channel corresponding to decoding and then encoding according to this scheme. There are many different metrics by which one could judge the accuracy of the compression scheme. We will consider three possibilities. The first is the

$$\text{entanglement fidelity :} \quad F_e \equiv F(\phi^\rho, (\mathcal{N} \otimes \mathbf{1})\phi^\rho) \quad (492)$$

where  $\phi^\rho$  purifies  $\rho$  and the  $\otimes \mathbf{1}$  acts on the purifying environment. A high  $F_e$  ensures that the channel not only does a good job at preserving a given state, but also does a good job at preserving any entanglement that happens to exist between that state and an external environment. The second is the

$$\text{average fidelity :} \quad \bar{F} \equiv \min \sum_i p_i F(\varphi_i, \mathcal{N}(\varphi_i)), \quad (493)$$

where the min is over all decompositions of  $\rho$  into pure states  $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$  (with  $\langle\varphi_i|\varphi_j\rangle \neq \delta_{ij}$  in general). It should be reasonable that getting large  $\bar{F}$  is easier than large  $F_e$ , since the former does not require preserving entanglement with an external system. The final is the

$$\text{eigenbasis fidelity :} \quad F_\lambda \equiv \sum_i \lambda_i F(\psi_i, \mathcal{N}(\psi_i)), \quad (494)$$

where  $\rho$  is eigendecomposed as  $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ . This is obviously a less stringent version of average fidelity.

In this diary entry we will see various ways in which these fidelities can be related to one another.

▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼

To compare these metrics, first note the trivial bound  $\bar{F} \leq F_\lambda$ , since the minimum over pure state decompositions will of course always be lower than one particular decomposition (the eigendecomposition).

We claim also that  $F_e \leq \bar{F}$ . First let us check that  $F_e$  is well-defined, viz. is independent of the purification. Indeed, since  $\sqrt{\phi^\rho} = \phi^\rho$ , we have

$$F_e = \text{Tr}[\sqrt{\phi^\rho(\mathcal{N} \otimes \mathbf{1})(\phi^\rho)\phi^\rho}], \quad (495)$$

which is clearly invariant under  $\phi^\rho \mapsto (\mathbf{1} \otimes U^\dagger)\phi^\rho(\mathbf{1} \otimes U)$  for all  $U$  acting on the purifying environment. We are then free to choose the canonical purification, viz.

$$|\phi^\rho\rangle = (\sqrt{\rho} \otimes \mathbf{1})|\Gamma\rangle, \quad (496)$$

where  $|\Gamma\rangle = \sum_i |ii\rangle$  is a bunch of Bell pairs between the system and the purifying environment (dropping an unimportant normalization constant). Writing the Kraus operators for  $\mathcal{N}$  as  $\mathcal{K}_a$ , we have

$$\begin{aligned} F_e &= \text{Tr} \left[ \sqrt{\sum_a (\sqrt{\rho} \otimes \mathbf{1})|\Gamma\rangle \langle \Gamma| (\sqrt{\rho} \mathcal{K}_a \sqrt{\rho} \otimes \mathbf{1})|\Gamma\rangle \langle \Gamma|^2 \langle \Gamma| (\sqrt{\rho} \otimes \mathbf{1})} \right] \\ &= \text{Tr} \left[ \sqrt{(\sqrt{\rho} \otimes \mathbf{1})|\Gamma\rangle \langle \Gamma| (\sqrt{\rho} \otimes \mathbf{1}) \sum_a |\text{Tr}[\mathcal{K}_a \rho]|^2} \right] \\ &= \sqrt{\sum_a |\text{Tr}[\mathcal{K}_a \rho]|^2}. \end{aligned} \quad (497)$$

On the other hand, a similar calculation gives

$$\bar{F} = \min_i \sum_a \sqrt{\sum_a |\text{Tr}[p_i \mathcal{K}_a |\varphi_i\rangle \langle \varphi_i|]|^2}. \quad (498)$$

Let  $p_i |\varphi_i\rangle \langle \varphi_i|$  be the decomposition of  $\rho$  that minimizes  $\bar{F}$ , and define

$$v_{ai} \equiv p_i \langle \varphi_i | \mathcal{K}_a | \varphi_i \rangle. \quad (499)$$

Since  $F_e$  only depends on  $\rho$ , we can use this particular decomposition to write

$$F_e = \sqrt{\sum_a \left| \sum_i v_{ai} \right|^2}, \quad \bar{F} = \sum_i \sqrt{\sum_a |v_{ai}|^2}. \quad (500)$$

We then write the difference  $\bar{F}^2 - F_e^2$  as

$$\bar{F}^2 - F_e^2 = \frac{1}{2} \sum_{i,j} \left( 2\sqrt{|\mathbf{v}_i|^2 |\mathbf{v}_j|^2} - (\mathbf{v}_i \cdot \mathbf{v}_j^* + \mathbf{v}_i^* \cdot \mathbf{v}_j) \right), \quad (501)$$

where  $\mathbf{v}_i$  is the vector in Kraus operator space, whose components are  $[v_i]_a = v_{ai}$ . For all  $i, j$  the RHS of the above is then positive by CS. To be pedantic, write  $\mathbf{v}_i = \mathbf{x}_i + i\mathbf{y}_i$ , where  $\mathbf{x}_i, \mathbf{y}_i$  are real. Then the above reads

$$\bar{F}^2 - F_e^2 = \sum_{i,j} (|\langle \mathbf{x}_i, \mathbf{y}_i | \langle \mathbf{x}_j, \mathbf{y}_j \rangle| - (\mathbf{x}_i, \mathbf{y}_i) \cdot (\mathbf{x}_j, \mathbf{y}_j)) \geq 0, \quad (502)$$

with equality holding only if the  $\mathbf{v}_i$  are identical for all  $i$ . Summarizing,

$$F_e \leq \bar{F} \leq F_\lambda. \quad (503)$$

While the separation between  $F_e$  and  $\bar{F}$  turns out to never be very large, a large separation between  $\bar{F}$  and  $F_\lambda$  is possible. Consider for example the state

$$\rho = \varsigma |0\rangle\langle 0| + (1 - \varsigma) |1\rangle\langle 1|, \quad (504)$$

where we have written  $\rho$  in its eigenbasis. We can also decompose  $\rho$  as

$$\rho = (1 - 2\varsigma) |1\rangle\langle 1| + \varsigma(|+\rangle\langle +| + |-\rangle\langle -|). \quad (505)$$

Consider the phase flip channel  $\mathcal{N}(\rho) = Z\rho Z$ . For a pure state  $|\varphi\rangle$ ,

$$F(\varphi, \mathcal{N}(\varphi)) = |\langle \varphi | \mathcal{N}(\varphi) | \varphi \rangle|. \quad (506)$$

Thus the eigenbasis fidelity in this case is simply

$$F_\lambda = \varsigma |\langle 0 | Z | 0 \rangle| + (1 - \varsigma) |\langle 1 | Z | 1 \rangle| = 1. \quad (507)$$

On the other hand, the channel fidelity on the decomposition (505) is

$$F = (1 - 2\varsigma) |\langle 1 | Z | 1 \rangle| + \varsigma \sum_{s=\pm} |\langle s | Z | s \rangle| = 1 - 2\varsigma. \quad (508)$$

Thus by taking  $\varsigma \rightarrow 1/2$  we can make  $\bar{F}$  (which is thus upper-bounded by  $1 - 2\varsigma$ ) arbitrarily small, while  $F_\lambda$  remains equal to 1 for all  $\varsigma$ .



## More on quantum compression

---

Our goal in this diary entry is to show that asymptotically, a density matrix  $\rho$  cannot be transmitted using a channel that compresses  $\rho$  to a density matrix acting on fewer than  $S(\rho)$  qubits.

▼ ▼

An arbitrary compression protocol is specified as follows.  $n$  copies of  $\rho$  are purified using a reference system R as  $|\phi_\rho\rangle_{RA}^{\otimes n}$ . The protocol then operates as

1. A starts with the A part of  $|\phi_\rho\rangle_{RA}^{\otimes n}$
2. A applies an encoding map  $\mathcal{E}$  to her RDM, creating an output  $Q$ .
3. A sends  $Q$  to B
4. B applies  $\mathcal{D}$  to  $Q$

Our goal is to examine the behavior of the squared channel fidelity

$$f \equiv F(\phi_\rho^{\otimes n}, \mathcal{D}(\mathcal{E}(\phi_\rho^{\otimes n})))^2. \quad (509)$$

*simplifying the fidelity*

Let  $\{E_k\}$  and  $\{D_l\}$  be the Kraus operators for  $\mathcal{E}$  and  $\mathcal{D}$ , respectively.  $f$  can be simplified as follows:

$$\begin{aligned} f &= \left( \text{Tr} \left[ \sqrt{\sqrt{\phi_\rho^{\otimes n}} \mathcal{D}(\mathcal{E}(\phi_\rho^{\otimes n})) \sqrt{\phi_\rho^{\otimes n}}} \right] \right)^2 \\ &= \left( \text{Tr} \left[ \sqrt{|\phi_\rho^{\otimes n}\rangle\langle\phi_\rho^{\otimes n}| \sum_{k,l} (D_l E_k \otimes \mathbf{1}_R) |\phi_\rho^{\otimes n}\rangle\langle\phi_\rho^{\otimes n}| (E_k^\dagger D_l^\dagger \otimes \mathbf{1}_R) |\phi_\rho^{\otimes n}\rangle\langle\phi_\rho^{\otimes n}|} \right] \right)^2 \\ &= \sum_{k,l} |\langle\phi_\rho^{\otimes n}| (D_l E_k \otimes \mathbf{1}_R) |\phi_\rho^{\otimes n}\rangle|^2 \\ &= \sum_{k,l} |\text{Tr}[D_l E_k \rho^{\otimes n}]|^2 \end{aligned} \quad (510)$$

*rank of  $D_l E_k$*

Let  $M \equiv \dim Q$  and  $N \equiv \dim(\rho^{\otimes n})$ . We claim that for all  $l, k$ ,  $\text{rank}(D_l E_k) \leq M$ . This is true simply because  $E_k \in L(\mathbb{C}^N, \mathbb{C}^M)$ , and hence the rank of any matrix times  $E_k$  can be at most  $M$ . More formally, perform SVDs as  $D_l = U_D \Lambda_D V_D$  and  $E_k = U_E \Lambda_E V_E$ . Then  $D_l E_k$  is unitarily equivalent to the matrix  $\Lambda_D V_D U_E \Lambda_E V_E U_D^\dagger$ . Since  $\Lambda_D$  is an  $N \times M$  matrix with only at most  $M$  nonzero entries,  $\text{im}(\Lambda_D V_D U_E \Lambda_E V_E U_D^\dagger)$  can obviously have rank at most  $M$ .

### intermediate bound on $f$

Perform now an SVD on  $D_l E_k$ , writing

$$D_l E_k = U_{kl} \Lambda_{kl} V_{kl}, \quad (511)$$

where  $\Lambda_{kl} \in L(\mathbb{C}^N)$  is a diagonal matrix with only  $m \equiv \text{rank}(D_l E_k) \leq M$  nonzero entries. Define  $\Pi_{kl}$  as the projector onto the subspace spanned by the nontrivial eigenvectors of  $\Lambda_{kl}$ . then

$$\text{Tr}[D_l E_k \rho^{\otimes n}] = \text{Tr}[\Lambda_{kl} V_{kl} \rho^{\otimes n} U_{kl}] = \text{Tr}[\Pi_{kl} \Lambda_{kl} V_{kl} \rho^{\otimes n} U_{kl}] = \text{Tr}[P_{kl} D_l E_k \rho^{\otimes n}], \quad (512)$$

where we have defined the projector

$$P_{kl} \equiv U_{kl} \Pi_{kl} U_{kl}^\dagger. \quad (513)$$

We now use the CS inequality to write

$$\begin{aligned} \text{Tr}[D_l E_k \rho^{\otimes n}] &= \text{Tr}[(D_l E_k \sqrt{\rho^{\otimes n}})(\sqrt{\rho^{\otimes n}} P_{kl})] \\ &\leq \sqrt{\text{Tr}[D_l E_k \rho^{\otimes n} E_k^\dagger D_l^\dagger] \text{Tr}[P_{kl} \rho^{\otimes n}]}. \end{aligned} \quad (514)$$

Inserting this in (510),

$$f \leq \sum_{k,l} \text{Tr}[D_l E_k \rho^{\otimes n} E_k^\dagger D_l^\dagger] \text{Tr}[P_{kl} \rho^{\otimes n}]. \quad (515)$$

### bound on $M$

We can now determine the minimal dimension  $M$  of the compressed density matrix  $\mathcal{E}(\rho)$  such that  $f$  is not required to be exponentially small in  $n$ . We start by writing

$$f \leq \sum_{k,l} \text{Tr}[D_l E_k \rho^{\otimes n} E_k^\dagger D_l^\dagger] \max_{k',l'} \text{Tr}[P_{k'l'} \rho^{\otimes n}]. \quad (516)$$

Using  $\sum_i \mathcal{K}_i^\dagger \mathcal{K}_i = \mathbf{1}$  for any set of Kraus operators  $\{\mathcal{K}_i\}$ ,

$$f \leq \max_{k,l} \text{Tr}[P_{k,l} \rho^{\otimes n}]. \quad (517)$$

Define the compression rate  $R$  via  $M \equiv 2^{nR}$ . We then have

$$f \leq \max_{\text{rank } 2^{nR} \text{ projectors } P} \text{Tr}[P \rho^{\otimes n}]. \quad (518)$$

The maximum on the RHS above will be realized by a  $P$  which is diagonal in  $\rho$ 's eigenbasis.<sup>32</sup> The problem of finding  $P$  is thus equivalent to the problem of finding the  $2^{nR}$ -element set of

---

<sup>32</sup>For the usual reason: if  $U$  is the unitary converting  $\rho^{\otimes n}$ 's eigenbasis to  $P$ 's eigenbasis, then  $\text{Tr}[P \rho^{\otimes n}] = \sum_{i,j} |U_{ij}|^2 p_i \lambda_j$ , where  $p_i \in \{0,1\}$  are the eigenvalues of  $P$  and  $\lambda_j$  are the eigenvalues of  $\rho^{\otimes n}$ . Then the matrix with entries  $|U_{ij}|^2$  is doubly stochastic, and since both the vectors  $\mathbf{\lambda}, \mathbf{p}$  are positive, the maximum is satisfied when  $|U_{ij}|^2$  is a single permutation matrix.

largest weight given the probability distribution  $\lambda^{\otimes n}$ , where  $\lambda$  is the distribution determined by the eigenvalues of  $\rho$ .

When  $n \rightarrow \infty$ , almost all of the weight in  $\lambda^{\otimes n}$  will be occupied by the typical set  $T_\lambda^n$  of  $\lambda^{\otimes n}$ . Since the probability of any given element in  $T_\lambda^n$  is nearly equal to  $2^{-nH(\lambda)} = 2^{-nS(\rho)}$  (up to  $\delta$ s that we won't need to keep track of), the best we can do (again, up to  $\delta$ s) is to let  $P$  project onto as large of a subset of  $T_\lambda^n$  as possible (by the above, the choice of subset is unimportant), and to arbitrarily include additional elements outside of  $T_\lambda^n$  as needed if  $\text{rank}(P) = 2^{nR} > |T_\lambda^n|$ . If  $2^{nR} < |T_\lambda^n|$ , we thus have

$$f \leq 2^{n(R-S(\rho))}, \quad (519)$$

which is the total weight of  $2^{nR}$  elements of  $T_\lambda^n$ . Thus if  $R < S(\rho)$ ,  $f \rightarrow 0$  as  $n \rightarrow \infty$ , implying that compression of  $\rho$  to a size less than  $S(\rho)$  is impossible.



## Data hiding with Werner states

---

A bipartite state  $\rho$  is said to be PPT if it has positive semi-definite partial transpose, i.e. if  $\rho^\Gamma \geq 0$ , where  $\Gamma$  denotes the partial trace over one part of the system (since  $\rho^T$  is PSD if  $\rho$  is, which subsystem we transpose doesn't matter). It is easy to see that all separable states are PPT.

Our goal in this diary entry is to understand a bit more about PPT states, and discuss an application to data hiding with Werner states.



### PPT preserved under local unitaries

While taking the transpose is a basis-dependent operation, the set PPT is invariant under unitaries that split as tensor products over the two subsystems. That is, if  $\rho \in \text{PPT}$  then

$$(U \otimes V)\rho(U \otimes V)^\dagger \in \text{PPT} \quad (520)$$

for all unitaries  $U, V$ . To see this we simply note that

$$[(U \otimes V)\rho(U \otimes V)^\dagger]^\Gamma = (U \otimes V^T)\rho^\Gamma(U \otimes V^T)^\dagger. \quad (521)$$

Now if  $\rho \in \text{PPT}$ , then  $\rho^\Gamma$  is PSD. But then  $W^\dagger \rho^\Gamma W$  is PSD for any matrix  $W$  (unitary or otherwise). Thus taking  $W = U \otimes V^T$ , we see that  $[(U \otimes V)\rho(U \otimes V)^\dagger]^\Gamma$  is PSD, as claimed (if the unitary did not factor as a  $\otimes$  the resulting matrix would not be of the form  $W^\dagger \rho^\Gamma W$ ).

## Werner states

Let  $F$  be the SWAP operator, and define

$$\Pi_{\pm} \equiv \frac{\mathbf{1} \pm F}{2}. \quad (522)$$

$\text{Tr}[\Pi_{\pm}] = d(d \pm 1)/2$  on account of the number of independent symmetric (antisymmetric) states in  $\mathbb{C}^d \otimes \mathbb{C}^d$  being  $d(d+1)/2$  and  $d(d-1)/2$ , respectively (given explicitly by  $\{|i, j\rangle + |j, i\rangle\}/\sqrt{2}$  and  $\{|i, j\rangle - |j, i\rangle\}/\sqrt{2} : i \neq j$ ).

Define the *Werner state*  $W_{\lambda}$  by

$$W_{\lambda} \equiv \lambda \frac{\Pi_{+}}{d(d+1)/2} + (1-\lambda) \frac{\Pi_{-}}{d(d-1)/2}. \quad (523)$$

We would like to know when  $W_{\lambda}$  is PPT. A first requirement is of course that  $W_{\lambda}$  is PSD, which is true provided  $\lambda, 1-\lambda \geq 0$ . Thus wolog we may take  $0 \leq \lambda \leq 1$ . We then need to compute  $W_{\lambda}^{\Gamma}$ . To do this we first note that  $F^{\Gamma} = d|\Phi\rangle\langle\Phi|$ , where  $|\Phi\rangle$  is the state

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle \otimes |i\rangle. \quad (524)$$

Since  $\mathbf{1}^{\Gamma} = \mathbf{1}$ , the partial transpose of  $W_{\lambda}$  is

$$W_{\lambda}^{\Gamma} = \mathbf{1} \left( \frac{\lambda}{d(d+1)} + \frac{1-\lambda}{d(d-1)} \right) + d\Phi \left( \frac{\lambda}{d(d+1)} - \frac{1-\lambda}{d(d-1)} \right), \quad (525)$$

where  $\Phi$  without brackets means  $|\Phi\rangle\langle\Phi|$ . To determine when  $W_{\lambda}$  is PPT, we look to see when  $W_{\lambda}^{\Gamma}$  has negative eigenvalues. From the above expression we see that the eigenvectors of  $W_{\lambda}^{\Gamma}$  are either  $|\Phi\rangle$ , or orthogonal to  $|\Phi\rangle$ . Those orthogonal to  $|\Phi\rangle$  will always have positive eigenvalues since the coefficient of  $\mathbf{1}$  is positive for all  $\lambda \in [0, 1]$ , and hence we can look at  $|\Phi\rangle$  wolog. Some easy algebra shows that  $|\Phi\rangle$  has eigenvalue

$$W_{\lambda}^{\Gamma}|\Phi\rangle = \frac{1}{d}(2\lambda - 1)|\Phi\rangle, \quad (526)$$

which is non-negative if  $\lambda \geq 1/2$ . Thus  $W_{\lambda \in [0, 1/2]}$  is entangled, and  $W_{\lambda \in [1/2, 1]}$  is PPT.

## PPT states and $|\Phi\rangle$

**Proposition 6.** *If  $\rho$  is PPT, then*

$$\text{Tr}[\Phi\rho] \leq \frac{1}{d}. \quad (527)$$

To prove this, we need

**Lemma 3.** For all  $A, B$ ,

$$\text{Tr}[AB] = \text{Tr}[A^{\Gamma}B^{\Gamma}]. \quad (528)$$

*Proof.* This is mostly easily proved by drawing a picture:

$$(529)$$

□

We can now prove the proposition:

*Proof.* We use the lemma to write

$$\text{Tr}[\Phi\rho] = \text{Tr}[\Phi^\Gamma\rho^\Gamma] \leq \|\Phi^\Gamma\|_\infty \|\rho^\Gamma\|_1, \quad (530)$$

where we used  $\text{Tr}[AB] \leq \|A\|_1 \|B\|_\infty$ . Now since  $\rho$  is assumed to be PPT, all of the eigenvalues of  $\rho^\Gamma$  are positive, and hence  $\|\rho^\Gamma\|_1 = \text{Tr}[\rho^\Gamma]$ . But since  $\text{Tr}[\rho^\Gamma] = \text{Tr}[\rho] = 1$ , we then have  $\|\rho^\Gamma\|_1 = 1$ , and so

$$\text{Tr}[\Phi\rho] \leq \|\Phi^\Gamma\|_\infty. \quad (531)$$

But since  $F^\Gamma = d\Phi$ ,

$$\Phi^\Gamma = \frac{1}{d}F, \quad (532)$$

and so

$$\text{Tr}[\Phi\rho] \leq \frac{1}{d}\|F\|_\infty = \frac{1}{d}. \quad (533)$$

□

### Data hiding with $W_0$ and $W_1$

Consider now using LOCC to distinguish between  $W_0$  and  $W_1$ . A measurement set discriminating between these two possibilities consists of two PSD operators  $\{M_0, M_1\}$  such that  $M_0 + M_1 = \mathbf{1}$ . Since the measurements are implemented with LOCC, both  $M_0, M_1$  will be PPT, so that  $M_{0,1}^\Gamma$  are PSD.

Since  $F(A \otimes B)F = B \otimes A$ ,  $F$  commutes with  $U \otimes U$  for all  $U \in \mathcal{U}(d)$ , and consequently  $W_\lambda$  does as well. Since both  $W_0, W_1$  commute with all  $U \otimes U$ , any measurement which discriminates between them will also commute with all  $U \otimes U$ . But the only operators which commute in this way are  $\mathbf{1}$  and  $F$ ; thus

$$M_0 = a\mathbf{1} + bF, \quad M_1 = (1 - a)\mathbf{1} - bF \quad (534)$$

for some real numbers  $a, b$ .

Since the most negative eigenvalue of  $F$  is  $-1$  and the most positive is  $+1$ ,  $M_0$  being PSD requires

$$0 \leq |b| \leq a. \quad (535)$$



But then  $M_1$  being PSD implies

$$|b| \leq 1 - a, \quad (536)$$

and so

$$|b| < \min(a, 1 - a). \quad (537)$$

We can also constrain  $a, b$  by virtue of the measurement protocol being done with LOCC. We have

$$M_0^\Gamma = a\mathbf{1} + bd\Phi. \quad (538)$$

If  $b > 0$ , this is PSD. If  $b < 0$ , then the eigenvector with smallest eigenvalue is  $|\Phi\rangle$ , and positivity then mandates

$$b > -a/d. \quad (539)$$

Finally,

$$M_1^\Gamma = (1 - a)\mathbf{1} - b\Phi. \quad (540)$$

If  $b < 0$  this is PSD, while if  $b > 0$  we require  $b \leq (1 - a)/d$ . Thus the additional constraint of being LOCC means that

$$-\frac{a}{d} \leq b \leq \frac{1 - a}{d}. \quad (541)$$

Imagine we draw a density matrix uniformly at random from  $W_0, W_1$ . Define the bias

$$\delta \equiv \text{Tr}[M_0 W_0] + \text{Tr}[M_1 W_1] - 1, \quad (542)$$

which represents twice the deviation of the probability of correctly distinguishing between  $W_0, W_1$  away from  $1/2$  (i.e. randomly guessing gives  $\delta = 0$  and getting it right every time gives  $\delta = 1$ ). We can calculate the bias using

$$\text{Tr}[M_0 W_0] = \frac{1}{d(d-1)} \text{Tr}[(a-b)\mathbf{1} + (b-a)F] = a - b, \quad (543)$$

since  $\text{Tr}[F] = d$ . Similarly,

$$\text{Tr}[M_1 W_1] = \frac{1}{d(d+1)} \text{Tr}[(1-a-b)(\mathbf{1} + F)] = 1 - a - b. \quad (544)$$

Thus  $\delta = -2b$  with this set of measurements. Since (541) says that  $b$  must be of order  $1/d$ , we have

$$\delta \leq O(1/d). \quad (545)$$

This bound can be saturated by a LOCC protocol which simply measures both subsystems in the computational basis and checks to see if the results agree. If they do agree then the state must for sure be  $\Pi_+$ , while if they do not agree then we cannot be sure. If we simply guess randomly between  $W_0$  and  $W_1$  in the case where they do agree, the measurement bias is

$$\begin{aligned} \delta &= \sum_i \text{Tr}[|ii\rangle\langle ii| W_1] + \frac{1}{2} \sum_{i \neq j} \text{Tr}[|ij\rangle\langle ij| (W_0 + W_1)] - 1 \\ &= \frac{2d}{d(d+1)} + \frac{1}{2} \left( 1 + \frac{d-1}{d+1} \right) - 1 \\ &= \frac{1}{d+1}, \end{aligned} \quad (546)$$

so that  $O(1/d)$  is indeed achievable by an LOCC protocol.

Note however if we relax to non-LOCC measurements, distinguishing between  $W_0$  and  $W_1$  can be done perfectly. This can be done by e.g. taking  $a = -b = 1/2$ , which is consistent with both  $M_{0,1}$  being PSD but not PPT. In this case we have  $M_0 = \Pi_-$  and  $M_1 = \Pi_+$ , which are simply proportional to  $W_0$  and  $W_1$ , respectively — since  $\text{Tr}[W_0 W_1] = 0$ , perfectly distinguishing the two states is thus possible. Indeed, in this case it is easy to show that  $\delta = 1$ .



## Entanglement distillation with CSS codes

---

In this diary entry we discuss classical secrecy distillation and a minimal extension thereof to the quantum setting by using CSS codes.



### Classical secrecy distillation

Consider a situation in which A and B have shared access to a private source that produces random elements of  $\mathbb{Z}_2^n$ , but which is such that the strings received by B are subjected to errors caused by a binary symmetric channel with error probability  $p$ . We are interested in establishing a public protocol by which A and B can ‘distill’ their strings to eliminate the effects of errors, and thereby produce pairs of *identical* secret strings. This can be done as follows.

Let A possess string  $x \in \mathbb{Z}_2^n$  and B possess string  $y \in \mathbb{Z}_2^n$ , with  $y = x + e$  for some error string  $e \in \mathbb{Z}_2^n$  distributed according to the BSC with flip probability  $p$ . The protocol proceeds by A randomly generating a rank- $k$  matrix  $M \in \mathbb{Z}_2^{n \times k}$  for some  $k < n$  (thus  $M$  is random except for the constraint that its rows all be linearly independent). A then sends  $M$  and  $Mx$  to B through a public channel, with B then tasked to use  $M, Mx$  to recover  $x$  from  $y$ . Note that conditioned on  $M, Mx$ , A’s state has  $n - k$  bits of entropy, simply because an eavesdropper knows that  $x$  must be of the form  $Mx + z$  for some  $z \in \ker(M)$ , with  $\ker(M)$  a random subspace of  $\mathbb{Z}_2^n$  with dimension  $n - k$ .

To reconstruct  $x$ , B must find the unique error  $e$  satisfying  $x = y + e$ . Intuitively, this will always be possible provided that the number of constraints on  $e$  imposed by the equation  $My = Mx + Me$  is more than the number of possible choices of  $e$ . To make this precise, note that by accepting an exponentially small chance of error, B can simply perform an exhaustive search over  $\mathcal{T}_{p,\delta}^n$  for strings  $e$  satisfying  $Mx = M(y + e)$ , where  $\mathcal{T}_{p,\delta}^n$  is the typical

subspace associated with the error channel (in what follows all  $\delta$ s will be omitted), whose dimension is  $|\mathcal{T}_p^n| = 2^{nH_2(p)}$  to leading order (note that we are not trying to make an *efficient* secret-sharing protocol!).

By assumption, it is exponentially likely for the error  $e \equiv x + y$  to be contained in  $\mathcal{T}_p^n$ . B will then fail to reconstruct  $x$  with order 1 probability only if there is some  $e' \in \mathcal{T}_p^n$  with  $M(y + e) = M(y + e')$  and  $e' \neq e$ . If this occurs then we must have  $e + e' \in \ker(M)$ . Since  $M$  and thereby  $\ker(M)$  is distributed randomly in  $\mathbb{Z}_2^n$ , the probability that this happens is

$$\Pr[\exists e' \in \mathcal{T}_p^n : e + e' \in \ker(M)] \leq |\ker(M)| \frac{|\mathcal{T}_p^n|}{2^n} = 2^{n(R-H_2(p))}, \quad (547)$$

where the rate  $R \equiv k/n$ . Thus as long as we choose the rate  $R > H_2(p)$ , B can always reconstruct A with perfect fidelity (with only exponentially small probability of error).

Thus after performing this protocol, A and B effectively have shared access to a random  $n$ -bit string. To establish this they have given up knowledge of  $M, Mx$  to an eavesdropper. Since this gives the eavesdropper  $k$  bits of information, A and B effectively share  $n - k = n(1 - R) \rightarrow n(1 - H_2(p))$  private bits. Thus noisy shared access to a random source allows A and B to distill secret bits at a rate asymptotically given by  $1 - H_2(p)$ .

### Minimal quantum generalization

Now we consider the minimal quantum generalization of the above situation, which uses stabilizer codes to achieve entanglement distillation. The strategy is the familiar one (and is the same as in the classical case) — we simply choose a random code and argue that it works with exponentially good probability. We first consider a simple setting in which the errors are classical, so that the corresponding stabilizers are also classical.

In this setting A and B share  $n$  copies of the Bell state  $|\Phi_2\rangle$ , but B's half incurs an error by the channel  $\mathcal{N}_X$ , where

$$\mathcal{N}_\sigma(\rho) = (1 - p)\rho + p\sigma\rho\sigma, \quad (548)$$

meaning that the state shared by A and B is not  $\Phi_2^{\otimes n}$  but rather  $[(1 \otimes \mathcal{N}_X)(\Phi_2)]^{\otimes n}$ . How well can Bell pairs be distilled in this case?

Since the errors here only occur in one basis, our protocol should differ from the above classical one only in changes of notation. Indeed, we proceed by having A generate a random matrix  $A \in \mathbb{Z}_2^{k \times n}$ , again subject to the constraint that the different rows  $M_1, \dots, M_k$  are linearly independent in  $\mathbb{Z}_2^n$ . For each row, A measures

$$Z^{M_i} \equiv \bigotimes_{j=1}^n Z_j^{M_{i,j}} \quad (549)$$

and sends both  $M$  and the measurement result  $(-1)^{m_i^A}$  to B, who then performs his own measurement of  $Z^{M_i}$ , yielding the result  $(-1)^{m_i^N}$ . Prior to measurement, the density matrix is essentially (meaning 'equal up to terms with weight exponentially small in  $n$ ') given by

$$\rho_{pre} \equiv [(1 \otimes \mathcal{N}_X)(\Phi_2)]^{\otimes n} \approx 2^{-n(1+H_2(p))} \sum_{e \in \mathcal{T}_p^n} \sum_{x, y \in \mathbb{Z}_2^n} |x, x + e\rangle \langle y, y + e|. \quad (550)$$

Post-measurement,

$$\rho_{post} \propto \sum_{e \in \mathcal{T}_p^n} \sum_{x, y \in \mathbb{Z}_2^n} \delta(M(x+e), m^B) \delta(M(y+e), m^B) \delta(Mx, m^A) \delta(My, m^A) |x, x+e\rangle \langle y, y+e|. \quad (551)$$

Let  $x^A$  be some fixed element in  $\mathbb{Z}_2^n / \ker(M)$  satisfying  $Mx^A = m^A$ . Then

$$\rho_{post} \propto \sum_{e \in \mathcal{T}_p^n} \sum_{w, z \in \ker(M)} \delta_{m^A + Ae, m^B} |x^A + w, x^A + w + e\rangle \langle x^A + z, x^A + z + e|. \quad (552)$$

Now as argued above, as long as  $H_2(p) < R$ , given  $m^A, m^B$ , it is exponentially likely for there to be only a single  $e$  satisfying the delta function in the above equation. In the language of stabilizer codes, it is exponentially unlikely to find two operators  $X^e, X^{e'}$  such that  $X^{e+e'} \in N(\mathcal{S})$  (the errors  $e, e'$  have the same ‘syndrome’), where (for now)  $\mathcal{S}$  is the algebra generated by the  $Z^{M_i}$ .

Then letting the stabilizer space  $S$  be the affine space  $S \equiv x^A + \ker(M)$ , we have

$$\rho_{post} \approx (\mathbf{1} \otimes X^e) |S\rangle \langle S| (\mathbf{1} \otimes X^e), \quad |S\rangle \equiv \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x, x\rangle \equiv |\Phi^{\otimes n}|_S. \quad (553)$$

Since the RDMs of  $\rho_{post}$  are maximally mixed when restricted to  $S$ , the entanglement entropy  $S(\rho_{post}) = n(1 - R)$ , since  $\dim[\ker(M)] = 2^{n(1-R)}$ . Thus asymptotically (i.e. sending  $R \rightarrow H_2(p)$ ), A and B can distill  $n(1 - H_2(p))$  ebits from this protocol, matching the number of secret bits distillable in the classical case.

### Adding in phase errors

Now we consider what happens when phase flip errors are added in, with the state shared by A and B being  $[(\mathbf{1} \otimes \mathcal{N}_Z \circ \mathcal{N}_X)(\Phi_2)]^{\otimes n}$ . If A and B were to repeat the above protocol unmodified, they would obtain the post-measurement state

$$\rho_{post} \approx \frac{1}{|\ker(M)|} \sum_{x, y \in S} \sum_{f \in \mathcal{T}_p^n} |x, x+e\rangle \langle y, y+e| (-1)^{f \cdot (x-y)}, \quad (554)$$

which by virtue of the signs is very mixed, complicating the distillation procedure. To get around this, we add in an  $X$ -stabilizer check which together with the matrix  $M$  produces a CSS code and allows A, B to recover a pure state.

The protocol initially proceeds as before, with A generating a random rank- $k$  matrix  $M$ , measuring the  $Z^{M_i}$  operators, and sending  $M$  and the measurement result to B. The added step consists of A generating an additional random rank- $k$  matrix  $N \in \mathbb{Z}_2^{k \times n}$  subject to the constraint  $MN^T = 0$ , measuring

$$X^{N_i} \equiv \bigotimes_{j=1}^n X^{N_{i,j}}, \quad (555)$$

and sending both  $N$  and the measurement result to B. Note that

$$Z^{M_i} X^{N_j} = X^{N_j} Z^{M_i} \prod_{l=1}^n (-1)^{M_{il} N_{jl}} = X^{N_j} Z^{M_i} (-1)^{[MN^T]_{ij}}, \quad (556)$$

so that the two measurements commute by virtue of the constraint that  $MN^T = 0$ .

Let Alice / Bob's measurements of  $Z^{M_i}$  and  $X^{N_i}$  be given by the eigenvalues  $(-1)^{m_i^{A/B}}$  and  $(-1)^{n_i^{A/B}}$ , respectively. After the measurements, the density matrix is approximately proportional to

$$\rho_{post} \propto \sum_{e,f \in \mathcal{T}_p^n} (\Pi_{n^A} \Pi_{m^A} \otimes \Pi_{n^B} \Pi_{m^B} X^e Z^f) \Phi_2^{\otimes n}, \quad (557)$$

where  $\Phi_2^{\otimes n}$  denotes the matrix  $\mathcal{O}(|\Phi_2\rangle\langle\Phi_2|)^{\otimes n} \mathcal{O}^\dagger$ . Since the measurements commute, we may write this as

$$\rho_{post} \propto \sum_{e,f \in \mathcal{T}_p^n} (\mathbf{1} \otimes (\Pi_{n^B} Z^f \Pi_{n^A}) (\Pi_{m^B} X^e \Pi_{m^A})) \Phi_2^{\otimes n}. \quad (558)$$

As shown above, as long as the dimension of the projectors are small enough (i.e. as long as  $H_2(p) < R$ ), it is exponentially likely for there to be one and only one choice of  $e, f$  for which the terms  $\Pi_{n^B} Z^f \Pi_{n^A}$ ,  $\Pi_{m^B} X^e \Pi_{m^A}$  are non-vanishing. Thus as before, the measurements have the effect of collapsing the sums over  $e, f$  to a single term, thereby yielding the pure state

$$\rho_{post} \approx (\mathbf{1} \otimes X^e Z^f) |S_{MN}\rangle \langle S_{MN}| (\mathbf{1} \otimes X^e Z^f), \quad (559)$$

where  $|S_{MN}\rangle$  is defined analogously to  $|S\rangle$  above, with  $S_{MN}$  the affine space  $(\mathcal{S}_M \cap \mathcal{S}_N)|\psi\rangle$ , where  $|\psi\rangle$  satisfies  $Z^{M_i}|\psi\rangle = (-1)^{m_i^A}|\psi\rangle$ ,  $X^{N_i}|\psi\rangle = (-1)^{n_i^A}|\psi\rangle$ , and where  $\mathcal{S}_{M/N}$  are the operators which commute with the checks  $Z_i^M, X_i^N$ . Since we are taking the intersection  $\mathcal{S}_M \cap \mathcal{S}_N$ , the number of distilled Bell pairs is consequently reduced from the case with only bit-flip errors. Specifically, since  $M, N$  commute with one another they impose  $2k$  constraints on the stabilized subspace, which consequently has dimension  $|S_{MN}| = 2^{n-2k} = 2^{n(1-2R)}$ . Thus the number of distilled Bell pairs is asymptotically  $1 - 2H_2(p)$ .

## Coherent information

We now compute the coherent information  $I_c \equiv S(B) - S(E)$  in the two quantum cases above (where  $E$  denotes the purifying environment and we are computing with the density matrices  $(\mathbf{1} \otimes \mathcal{N}_X)(\Phi_2^{\otimes n})$  or  $(\mathbf{1} \otimes \mathcal{N}_Z \circ \mathcal{N}_X)(\Phi_2^{\otimes n})$ ). In the case where we only have bit flip errors, the RDMs are

$$\rho_B \propto \sum_{e \in \mathcal{T}_p^n} \text{Tr}_{AE}[|e\rangle\langle e| \otimes (\mathbf{1}_A \otimes X^e) \Phi_2^{\otimes n} (\mathbf{1}_A \otimes X^e)] = \sum_{e \in \mathcal{T}_p^n} X^e \mathbf{1}_B X^e \propto \mathbf{1}_B \quad (560)$$

and

$$\rho_E \propto \mathbf{1}_E \quad (561)$$

for similar reasons. Thus for just bit flips, we have (using log base 2 in the definition of  $S$ )

$$I_c = n(1 - H_2(p)), \quad (562)$$

which agrees with the distillable entanglement.

For the case of both bit and phase flips,  $\rho_B$  is again just proportional to  $\mathbf{1}_B$ ; this is just because if we trace out  $A$  before applying the channel we see that the state is maximally

mixed on  $B$ , and hence is invariant under the subsequent channel  $\mathcal{N}_Z \circ \mathcal{N}_X$ . The same applies to  $\rho_E$ , which is proportional to  $\mathbf{1}_E$  and now has dimension  $|\mathcal{T}_p^n|^2$ . Thus the coherent information in this case is

$$I_c = n(1 - 2H_2(p)), \quad (563)$$

matching the number of distillable Bell pairs derived above.



## Quantum Pinsker

---

In today's diary entry we will derive the quantum Pinsker inequality and discuss a simple application thereof.



### Derivation

We first derive the quantum Pinsker inequality:

**Proposition 7.** *For any two density matrices  $\rho, \sigma$ ,*

$$D(\rho||\sigma) \geq \frac{1}{2 \ln 2} \|\rho - \sigma\|_1^2, \quad (564)$$

where  $D(\rho||\sigma) \equiv \text{Tr}[\rho \ln \rho - \rho \ln \sigma]$  is the quantum relative entropy.

*Proof.* The proof strategy is to reduce the calculation to one involving classical probability distributions, and to then use the classical Pinsker inequality. To this end we introduce the random variables

$$r_{\pm} \equiv \text{Tr}[\Pi_{\pm} \rho], \quad s_{\pm} \equiv \text{Tr}[\Pi_{\pm} \sigma], \quad (565)$$

where

$$\Pi_{\pm} \equiv \sum_{\lambda \in \mathcal{E}_{\pm}(\rho - \sigma)} |\lambda\rangle\langle\lambda|, \quad (566)$$

with  $\mathcal{E}_{\pm}(\mathcal{O})$  denoting the set of positive / negative eigenvalues of  $\mathcal{O}$ , respectively. Then

$$\begin{aligned} \|\rho - \sigma\|_1 &= \sum_{\lambda \in \mathcal{E}_+(\rho - \sigma)} \lambda + \left| \sum_{\lambda \in \mathcal{E}_-(\rho - \sigma)} \lambda \right| \\ &= |\text{Tr}[\Pi_+(\rho - \sigma)]| + |\text{Tr}[\Pi_-(\rho - \sigma)]| \\ &= |r_+ - s_+| + |r_- - s_-| \\ &= 2|r_+ - s_+| \\ &= \|r - s\|_1. \end{aligned} \quad (567)$$

Now we use the classical Pinsker inequality, which when applied to two Bernoulli random variables with probabilities  $p, p + \varepsilon$  reads

$$D\left(\left(\begin{smallmatrix} p + \varepsilon \\ 1 - p - \varepsilon \end{smallmatrix}\right) \middle\| \left(\begin{smallmatrix} p \\ 1 - p \end{smallmatrix}\right)\right) \leq \frac{2}{\ln 2} \varepsilon^2. \quad (568)$$

In our case, taking  $p \rightarrow s_+$  and  $\varepsilon \rightarrow r_+ - s_+ = r_- - s_-$ , we have

$$D(r||s) \geq \frac{2}{\ln 2} |r_+ - s_+|^2 = \frac{1}{2 \ln 2} \|r - s\|_1. \quad (569)$$

Putting these together, we have

$$\|\rho - \sigma\|_1 \leq D(r||s), \quad (570)$$

and all that remains is to relate  $D(r||s)$  to  $D(\rho||\sigma)$ . This is however easy, since  $D(r||s)$  is always less than  $D(\rho||\sigma)$ . Formally, this follows from the monotonicity of the relative entropy under quantum channels  $D(\rho||\sigma) \geq D(\mathcal{N}(\rho)||\mathcal{N}(\sigma))$ , where in the present case the channel  $\mathcal{N}$  is defined as

$$\mathcal{N}(\mathcal{O}) = \sum_{\alpha=\pm} \text{Tr}[\Pi_\alpha \mathcal{O}] |\alpha\rangle\langle\alpha|. \quad (571)$$

Thus putting in this inequality we get (564) as desired. □

## Applications

One application is that if  $S(\rho) \leq \varepsilon$ , then  $\rho$  is  $\varepsilon$ -close (in the 1-norm) to a pure state. This is a rather trivial application of (564): let  $\rho = \sum_\lambda \lambda |\lambda\rangle\langle\lambda|$ , and let  $\lambda_m$  be the largest eigenvalue of  $\rho$ . Then

$$\begin{aligned} \frac{1}{2 \ln 2} \|\rho - |\lambda_m\rangle\langle\lambda_m|\|_1 &\leq D(|\lambda_m\rangle\langle\lambda_m||\rho) = -S(|\lambda_m\rangle\langle\lambda_m|) - \langle\lambda_m| \ln(\rho) |\lambda_m\rangle = -\ln(\lambda_m) \\ &< S(\rho), \end{aligned} \quad (572)$$

where in the last inequality we used

$$S(\rho) = \sum_\lambda \lambda \ln(1/\lambda) \leq \sum_\lambda \lambda \ln(1/\lambda_m) = -\ln \lambda_m. \quad (573)$$

This then gives

$$\frac{1}{2 \ln 2} \|\rho - |\lambda_m\rangle\langle\lambda_m|\|_1 \leq \varepsilon, \quad (574)$$

so that  $\rho$  is close in trace distance to  $|\lambda_m\rangle\langle\lambda_m|$ .

A similar statement is that a bipartite state  $\rho_{AB}$  is  $\varepsilon$ -close to a product state (again in trace distance) if  $I(A : B)_\rho \leq \varepsilon$ . This follows from

$$\begin{aligned} I(A : B) &= S(A) + S(B) - S(AB) \\ &= -\text{Tr}[\rho_{AB} \ln(\rho_A \otimes \mathbf{1}_B) + \rho_{AB} \ln(\mathbf{1}_A \otimes \rho_B) - \rho_{AB} \ln \rho_{AB}] \\ &= D(\rho_{AB} || \rho_A \otimes \rho_B). \end{aligned} \quad (575)$$

Thus  $I(A : B)_\rho \leq \varepsilon$  means that  $\rho_{AB}$  is close to  $\rho_A \otimes \rho_B$ :

$$\varepsilon \geq D(\rho_{AB} || \rho_A \otimes \rho_B) \geq \frac{1}{2 \ln 2} \|\rho_{AB} - \rho_A \otimes \rho_B\|_1^2. \quad (576)$$



## One-axis twisting

---

Today I attended a very nice talk by Norm Yao on spin squeezing. In his talk he briefly introduced the “one axis twisting” model as a simple model for understanding spin squeezing. In this diary entry we will try to derive the formulae he quoted on his slides for the squeezing rate. I have made no attempt to dig through the literature and hence won’t provide citations to the original sources. Any mistakes in the following discussion are due to me not understanding the talk fully.



Simplifying a bit, the goal of quantum metrology is to use (an appropriate type of) quantum entanglement to perform a measurement of an external field which is more precise than what could be achieved with classical methods. The most common setting is where one aims to measure the strength of a magnetic field; if this field is represented by the Hamiltonian  $\sum_i Z_i$  then the GHZ state provides an optimal state for performing the sensing, basically due to the fact that the GHZ state involves a coherent superposition of states with macroscopically different values of the quantum number we want to sense (viz.  $S^z$ ).

One challenge with this is that the GHZ state is hard to prepare. To this end we might look for states which are good for sensing (i.e. involve superpositions of states with relatively large differences in magnetic moments), but which are still easy to prepare. For us, a state of  $N$  qubits will count as being easy to prepare if it is obtained by quenching a product state by a simple Hamiltonian and evolving for time  $\text{poly}(N)$  with some reasonably small polynomial.

The OG example of such a state is apparently the one constructed by quenching a state with maximal spin along the  $\mathbf{a}$  direction by the Hamiltonian  $\frac{1}{N}(\mathbf{S}_T \cdot \mathbf{b})^2$ , where  $\mathbf{b} \cdot \mathbf{a} = 0$  ( $\mathbf{S}_T$  is the total spin operator of the  $N$  qubits). For concreteness, we will consider performing a quench on the state  $|+\rangle^{\otimes N}$  with the Hamiltonian

$$H = \frac{1}{N} \sum_{i,j} Z_i Z_j = \frac{1}{N} Z_T^2, \quad (577)$$



where  $Z_T = \sum_i Z_i$  is the “total  $S^z$  spin” (in quotes because we are not including factors of  $1/2$ ).

Thinking back to when we learned about squeezed states in optics, it is perhaps reasonable that  $|\psi(t)\rangle = e^{-itH}|+\rangle^{\otimes N}$  is a squeezed state of some form (recall that photonic squeezed states are created using squeezing operators like  $e^{\zeta a^2 - \zeta^* a^{\dagger 2}}$  or by including interactions like this into a Hamiltonian; the resemblance between the nonlinearities here and the  $Z_T^2$  Hamiltonian should be apparent). That  $|\psi(t)\rangle$  is indeed squeezed can be ‘proven’ with a simple physical argument. At  $t = 0$ , the total spin  $\mathbf{S}$  is prepared in a ‘cloud’ spread out near the point  $\hat{\mathbf{x}}$  on the Bloch sphere (with radius  $\sim L/2$ ). Evolution with  $H$  makes the cloud of spin precess around the  $\hat{\mathbf{z}}$  direction *with a rate that depends on the  $z$ -component of the spin*. Thus the part of the cloud lying at positive  $z$  will precess one way around  $\hat{\mathbf{z}}$ , while the part at negative  $z$  will precess the opposite way. The precession is faster for larger  $|z|$ , and the result is a dynamics which ‘shears’ the cloud, distending it by wrapping it around the sphere. Pictorially, this shearing process then leads to a squeezing of the cloud, and getting a squeezed spin state for long enough times is then quite reasonable (this was the logic given in Norm’s talk).

Now we make this intuition more precise. We will aim to compute a figure of merit introduced in the talk, which adapted to the present notation is

$$\xi^2(t) \equiv N \frac{\min_{\phi} \text{var}(Z_T(t) \cos \phi + Y_T(t) \sin \phi)}{\langle X_T(t) \rangle^2}. \quad (578)$$

Here the minimum over  $\phi$  acts to select out the “most squeezed” direction of the spin in the plane normal to the initial magnetization vector  $\parallel \hat{\mathbf{x}}$ . On one of Norm’s slides he claimed that the minimum value  $\xi_s^2$  of  $\xi^2(t)$  is  $\xi_s^2 \sim N^{-2/3}$ , and that this minimum is reached at a time  $t \sim N^{1/3}$ . These results are what we will aim to reproduce below.

To calculate the variance appearing in  $\xi^2$ , we start off with the useful relation

$$S_T^s(t) = e^{itZ_T^2/N} S_T^s e^{-itZ_T^2/N} = S_T^s e^{\frac{it}{N}[(Z_T+2s)^2 - Z_T^2]} = S_T^s e^{s \frac{4it}{N} Z_T + \frac{4it}{N}} = e^{s \frac{4it}{N} Z_T - \frac{4it}{N}} S_T^s \quad (579)$$

together with  $Z_T(t) = Z_T$ . Thus defining  $\lambda \equiv 4t/N$ , we have

$$\begin{aligned} \langle X_T(t) \rangle &= \sum_s \langle e^{is\lambda Z_T - i\lambda} S_T^s \rangle \\ &= N \sum_s \langle + | S^s | + \rangle (\langle + | \cos(\lambda Z) | + \rangle)^{N-1} \\ &= N \cos(\lambda)^{N-1} \end{aligned} \quad (580)$$

where the second line follows from an explicit expansion of  $S_T^s$ . On the other hand we obviously have

$$\langle Y_T(t) \rangle = \langle Z_T(t) \rangle = 0. \quad (581)$$

Now for the two point functions. We start with

$$\begin{aligned}
 \langle S_T^s(t) S_T^{-s}(t) \rangle &= \frac{1}{4} \sum_{j,k} \langle + | (X + sJ)_j (X - sJ)_k | + \rangle \\
 &= \frac{1}{4} \sum_{j,k} \langle + | 2\delta_{j,k} + (1 - \delta_{j,k}) X_j X_k | + \rangle \\
 &= \frac{N(N+1)}{4}.
 \end{aligned} \tag{582}$$

The other combination is

$$\begin{aligned}
 \langle S_T^s(t)^2 \rangle &= \langle S_T^s e^{2i\lambda Z_T} S_T^s \rangle \\
 &= \cos(2\lambda)^{N-2} N(N-1) \langle + | S^s e^{2i\lambda Z} | + \rangle \langle + | e^{2i\lambda Z} S^s | + \rangle \\
 &= \frac{N(N-1)}{4} \cos(2\lambda)^{N-2}.
 \end{aligned} \tag{583}$$

The  $ZZ$  correlators are of course  $\langle Z_T(t)^2 \rangle = N$  since the initial state has  $\sqrt{N}$  fluctuations in both  $Z_T$  and  $Y_T$ , and  $Z_T$  commutes with the Hamiltonian. The last correlator we will need is

$$\begin{aligned}
 \langle Z_T(t) S_T^s(t) \rangle &= \langle Z_T e^{i\lambda s Z_T - i\lambda S_T^s} \rangle \\
 &= \sum_{j,k} \left( \delta_{j,k} \cos(\lambda)^{N-1} \frac{s}{2} + (1 - \delta_{j,k}) \frac{\cos(\lambda)^{N-2}}{2} \langle + | Z e^{i\lambda s Z} | + \rangle \right) \\
 &= \frac{s}{2} (N \cos(\lambda)^{N-1} + iN(N-1) \cos(\lambda)^{N-2} \sin(\lambda)).
 \end{aligned} \tag{584}$$

Define the operator  $W_\phi \equiv \cos(\phi) Z_T + \sin(\phi) Y_T$ . Since  $\langle W_\phi(t) \rangle = 0$  for all  $t$ ,  $\text{var}(W_\phi(t))^2 = \langle W_\phi(t)^2 \rangle$ , which we compute via

$$\begin{aligned}
 \langle W_\phi(t)^2 \rangle &= \cos(\phi)^2 \langle Z_T(t)^2 \rangle + \sin(\phi)^2 \langle Y_T(t)^2 \rangle + \cos(\phi) \sin(\phi) \langle \{Z_T(t), Y_T(t)\} \rangle \\
 &= \cos(\phi)^2 N + \sin(\phi)^2 \sum_s \langle S_T^s(t) S_T^{-s}(t) - S_T^s(t) S_T^s(t) \rangle + 2\text{Im} \langle Z_T(t) (S_T^+(t) - S_T^-(t)) \rangle \\
 &= \cos(\phi)^2 N + \sin(\phi)^2 \left( N^2 \frac{1 - \cos(2\lambda)^{N-2}}{2} + N \frac{1 + \cos(2\lambda)^{N-2}}{2} \right) \\
 &\quad + 2 \sin(\phi) \cos(\phi) N(N-1) \cos(\lambda)^{N-2} \sin(\lambda).
 \end{aligned} \tag{585}$$

Note that the RHS is equal to  $N$  at  $t = 0$ , as required by the isotropic (in the  $yz$  plane)  $\sqrt{N}$  fluctuations present in the initial state.

To simplify the above expression, we bring all of the trig functions involving  $\phi$  into a common form. One of the intermediate steps along the way involves writing  $\cos(2\phi)\alpha + \sin(2\phi)\beta = \sqrt{\alpha^2 + \beta^2} \cos(2\phi - 2\theta)$ , where  $\theta = \arctan(\beta/\alpha)$ . Some unilluminating algebra along these lines leads to

$$\langle W_\phi(t)^2 \rangle = \frac{1}{4} (N^2(1 - \cos(2\lambda)^{N-2}) + N(3 + \cos(2\lambda)^{N-2})) + \sqrt{\Xi^2 + \Upsilon^2} \cos(2\phi - 2\theta), \tag{586}$$

where we have defined

$$\begin{aligned}\theta &\equiv \arctan(\Xi/\Upsilon) \\ \Xi &\equiv N(N-1)\cos(\lambda)^{N-2}\sin(\lambda) \\ \Upsilon &\equiv N(N-1)\frac{\cos(2\lambda)^{N-2}-1}{4}.\end{aligned}\tag{587}$$

The most squeezed direction is clearly the direction defined by  $\phi = \theta - \pi/2$  (while  $\phi = \theta$  is accordingly the least squeezed). We now need to evaluate the squeezing factor  $\xi^2$  in the case where  $\phi = \theta - \pi/2$ , and find the time  $t$  at which  $\xi^2$  is maximized.

By either plotting  $\xi^2(\lambda)$  or by recognizing that we have a  $\langle X_T(t) \rangle^2 = N^2 \cos(\lambda)^{2N-2}$  in the denominator, one sees that the maximum of  $\xi^2$  is attained at small  $\lambda \ll 1$ . Simply performing a series expansion of  $\xi^2$  in small  $\lambda$  doesn't work however, as doing so yields a squeezing time  $t_s \equiv \operatorname{argmin}_t(\xi^2)$  which scales as  $t_s = \Theta(N^0)$  and a gives a squeezing parameter  $\xi_s^2 \equiv \xi^2(t = t_s)$  of  $\xi_s^2 = \Theta(N^{-1/2})$  — which is has the same scaling with  $N$  as  $\xi^2(0)$ !

Playing around with the plots of  $\xi^2(t)$  more carefully (by rescaling  $t$  by  $N$ ) shows that  $t_s$  is not small (and in fact grows with  $N$ ), but that  $t_s/N$  always is. Thus we can find the minimum by expanding in  $\lambda \ll 1$  while at the same time taking  $\lambda N \gg 1$ . Doing so yields

$$\langle W_\phi(t)^2 \rangle \sim N \left( \frac{A}{(N\lambda)^2} + B\lambda^2(N\lambda)^2 \right),\tag{588}$$

where (don't quote me on this)  $A = 1, B = 384$  (really?). Thus

$$\xi_s^2 \sim \frac{A}{(N\lambda)^2} + B\lambda^2(N\lambda)^2,\tag{589}$$

which is minimized when  $\lambda = (2B/A)^{-1/6} N^{-2/3}$ ; writing this in terms of  $t$  gives

$$t_s = \gamma N^{1/3}, \quad \gamma \equiv \frac{A^{1/6}}{4(2B)^{1/6}},\tag{590}$$

which correctly gives the  $N^{1/3}$  scaling quoted on Norm's slide. By plugging this back in, we see that

$$\xi_s = \gamma' N^{-2/3}, \quad \gamma' \equiv \frac{A}{\gamma^2} + B\gamma^4,\tag{591}$$

which also correctly gives the claimed  $N^{-2/3}$  scaling (and hence does better than the  $N^{-1/2}$  that we get in the unsqueezed  $t = 0$  state).



## Dual unitary 2-qubit gates

Today I saw someone claim that  $U(a, b) = e^{i[a(XX+YY)+bZZ]}$  is a 2-qubit dual unitary gate. This can't be true for all  $a, b$  since  $U(0, 0) = \mathbf{1}$  is obviously not dual unitary. In today's entry we will therefore work out the constraints needed on  $a, b$  to ensure dual-unitarity.

☛ ☛

As a first hint, note that SWAP is obviously dual unitary. By symmetry (or SW duality), SWAP must be proportional to  $\sum_{\mu} \sigma^{\mu} \otimes \sigma^{\mu}$ ; indeed we have  $\text{SWAP} = (11 + XX + YY + ZZ)/2$ . Since the 11 part just gives a phase when exponentiated, we have

$$U(\alpha/2, \alpha/2) = \exp(i\alpha \text{SWAP}) = \cos \alpha + i(\sin \alpha) \text{SWAP}, \quad (592)$$

which is dual-unitary iff  $\cos \alpha = 0$ , viz. iff  $\alpha \in \pi(\mathbb{Z} + 1/2)$ .

Since we are only dealing with  $4 \times 4$  matrices, we can generalize beyond this specific case by simply writing things out explicitly. Consider a 2-qubit gate  $U_{ab}^{cd}$  given by

$$U = \begin{pmatrix} a & b & e & f \\ c & d & g & h \\ i & j & m & n \\ k & l & o & p \end{pmatrix}. \quad (593)$$

Taking the “spacetime” dual of this amounts to rotating the matrix elements as  $U_{ab}^{cd} \rightarrow U_{ca}^{db}$ , thus the dual is

$$\hat{U} = \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix}. \quad (594)$$

By computing  $\hat{U}^\dagger \hat{U}$ , it is easy to check that  $U(a, b)$  is dual-unitary for any  $b$  when  $a \in \pi(\mathbb{Z} + 1/2)$ , but is never dual-unitary if  $a \notin \pi(\mathbb{Z} + 1/2)$ .

In fact it is not hard to go further and convince oneself that the 1-parameter family  $U(\pi/2, b)$  almost exhausts all of the 2-qubit dual unitary gates. The reason for the “almost” is that replacing  $U \rightarrow (V_1 \otimes V_2)U(V_3 \otimes V_4)$  — where the  $V_i$  are arbitrary single-qubit unitaries — obviously maps dual unitaries to dual unitaries. Since  $U(\pi/2, b)$  can be written in terms of a SWAP gate and a power of a CZ gate after dropping overall phases and single-qubit unitaries (as  $\text{CZ} = \frac{1}{2}(11 + 1Z + Z1 - ZZ)$ ), 2-qubit dual unitaries can thus be parametrized as

$$U = (V_1 \otimes V_2)(\text{SWAP} (CZ)^\lambda)(V_3 \otimes V_4), \quad (595)$$

where  $\lambda$  is arbitrary.



## The toric code as a homological product

---

Today's entry stemmed from an exercise assigned by Alexander Kubica during one of his lectures at the 2023 Boulder summer school, which was to show that the toric code can be written as the homological product of two repetition codes.<sup>33</sup> In this diary entry we will try to understand some general features of homological products, and will then demonstrate this fact.

▼ ▼

### General aspects of the product construction

To get warmed up, let us educate ourselves about the parity-check formalism for quantum codes. For a general code with  $n_{stab}$  stabilizers and  $n_{phys}$  qubits, we are given a  $n_{stab} \times 2n_{phys}$  check matrix in the form  $H = (A_X | A_Z)$ , where

$$\langle a | A_\mu | i \rangle = \begin{cases} 1 & \text{if stabilizer } a \text{ has a } \sigma^\mu \text{ on site } i \\ 0 & \text{else} \end{cases} \quad (596)$$

with  $\mu \in \{X, Z\}$ . The matrix element  $\langle a | A_X A_Z^T | b \rangle$  tells us the parity of the number of  $X$ s of stabilizer  $a$  that overlap with the  $Z$ s of stabilier  $b$ ; thus the stabilizers mutually commute only if

$$A_X A_Z^T + A_Z A_X^T = 0, \quad (597)$$

where addition above and below will always tacitly be performed mod 2.

For CSS codes, a given stabilizer can always be chosen to contain either only  $X$ s or only  $Z$ s, and in this case we may thus write  $A_X = (H_X; 0_{n_{s,z} \times n})$  and  $A_Z = (0_{n_{s,x} \times n}; H_Z)$ , where  $n_{s,\mu}$  is the number of  $\mu$  stabilizers and  $(A; B)$  is our ideosyncratic notation for `np.vstack(A, B)`. One then finds

$$A_X A_Z^T + A_Z A_X^T = \begin{pmatrix} 0 & H_X H_Z^T \\ H_Z H_X^T & 0 \end{pmatrix}, \quad (598)$$

meaning that the stabilizers commute only if (duh)  $H_X H_Z^T = 0$ . The homological way of writing this is using the exact sequence<sup>34</sup>

$$C_Z \xrightarrow{H_Z^T} C_{phys} \xrightarrow{H_X} C_X, \quad (599)$$

where exactness of course means  $H_X H_Z^T = 0$ . Here  $C_{phys}$  is the space of physical qubits, while the code spaces  $C_{X,Z}$  determine the  $X, Z$  stabilizers of the quantum code. Note that

---

<sup>33</sup>In the lecture he used  $\oplus$  in a strange way, to mean the equivalent of `np.hstack`. Here we will use the more standard notation  $(A | B)$ .

<sup>34</sup>Of course we could also flip  $X$  and  $Z$  around, since  $H_X H_Z^T = 0$  is equivalent to  $H_Z H_X^T = 0$ .

$H_X H_Z^T = 0$  can be rewritten as  $(C_Z)^\perp \subseteq C_X$ , with equality only when there are no logical dof, since the number of logical qubits is  $k = \dim[C_X/(C_Z)^\perp]$ .<sup>35</sup>

We now come to homological products, which were designed as a way of creating quantum LDPC codes with the same distance scaling as the TC, but with constant rate. Consider two classical PC codes with check matrices  $H_i$  of dimensions  $r_i \times n_i$ ,  $i = 1, 2$  (here we are using rather questionable notation where  $r_i$  is equal to  $n_i - k_i$ , with  $k_i$  the dimension of the code space, only when  $H_i$  is non-degenerate [which here means that  $\ker(H_i^T) = 0$ , viz. there are no nontrivial linear relations between the  $H_i$  parity checks]). From these we construct a CSS code with check matrices<sup>36</sup>

$$H_X = (H_1 \otimes \mathbf{1}_{n_2} \mid \mathbf{1}_{r_1} \otimes H_2^T), \quad H_Z = (\mathbf{1}_{n_1} \otimes H_2 \mid H_1^T \otimes \mathbf{1}_{r_2}) \quad (600)$$

where  $(A|B)$  means `np.hstack(A, B)`.  $H_X, H_Z$  form a CSS code for all choices of  $H_i$  for the simple reason that

$$H_X H_Z^T = 2H_1 \otimes H_2^T \cong 0. \quad (601)$$

Letting  $H_i : A_i \rightarrow B_i$ , the exact sequence associated with this CSS code is

$$A_1 \otimes B_2 \xrightarrow{H_Z^T} (A_1 \otimes A_2; B_1 \otimes B_2) \xrightarrow{H_X} B_1 \otimes A_2. \quad (602)$$

We can understand why this construction is called a homological product by organizing things in a geometric way. First note that the number of physical qubits, viz. the number of rows of  $H_X$  (or  $H_Z$ ) is

$$n = n_1 n_2 + r_1 r_2. \quad (603)$$

Thus we have physical qubits for both each pair of physical bits and each pair of checks in the original classical codes. The number of  $X$  and  $Z$  checks are

$$\#(X\text{-checks}) = r_1 n_2, \quad \#(Z\text{-checks}) = r_2 n_1. \quad (604)$$

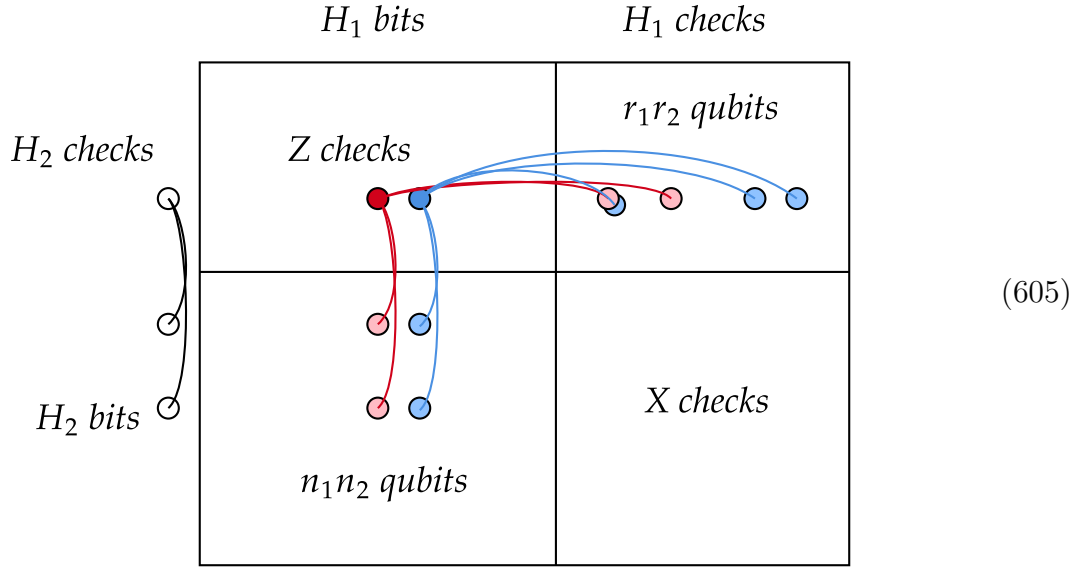
From (600), we see that each  $X$  check is labeled by a check from code 1 and a bit from code 2, with the opposite being true for the  $Z$  checks. We will thus find it convenient to draw

---

<sup>35</sup>To remind oneself of how this works, think about the TC. Here  $H_X$  takes the boundary of points on the lattice square lattice, while  $H_Z^T$  maps a collection of plaquettes to its boundary; obviously then  $(C_Z)^\perp \subset C_X$ .  $X$  and  $Z$  are exchanged by going to the dual lattice.

<sup>36</sup>Note that in the literature (as in Kubica's lecture) sometimes the transposes are placed in different places, but the convention here seems to be the best choice as it makes most clear the rate of the product code in terms of the parameters of the two classical codes  $H_i$  (although it means that the sequences associated with the  $H_i$  go in "opposite" directions; see below).

things in the following way:



where we imagine the whole square being filled with a  $n_2r_2 \times n_1r_1$  matrix of qubits, the diagonal blocks of which are ancillaes used for measuring the  $n_2r_1$  and  $n_1r_2$   $Z$  and  $X$  checks, and the off-diagonal blocks of which are the  $n_1n_2$  and  $r_1r_2$  physical qubits used to store logical information.

In the figure we have drawn an example of an  $H_2$  check on the left in white and two examples of  $Z$  checks in red and blue. These two  $Z$  checks are on the same row of the lattice, and hence share the same  $H_2$  check; they are however on different columns and thus involve different qubits in the upper right block. By staring at this figure for long enough one sees why the  $Z$  and  $X$  checks automatically commute.

We now claim the following proposition about the parameters of the resulting quantum code, which is my interpretation of a simplified version of the result in Tillich + Zemor 2013:

**Proposition 8.** *If the  $H_i$  are chosen to be non-degenerate,<sup>37</sup> then the product construction gives a  $[[n, k, d]]$  quantum code with*

$$\begin{aligned} n &= n_1n_2 + r_1r_2 \\ k &= k_1k_2 \\ d &= \min(d_1, d_2), \end{aligned} \tag{606}$$

where the distance  $d_i$  of the classical code  $H_i$  is defined by the “lightest” (in Hamming weight) nonzero codeword in  $\ker(H_i)$ .

*Proof.* The value of  $n$  is obvious, as this is simply equal to the number of columns of  $H_{X,Z}$ . For the code dimension, recall that  $k = n - \text{rk}(H_X) - \text{rk}(H_Z)$ . Since we have assumed  $\ker(H_{1,2}^T) = 0$ ,  $\mathbf{1}_{r_1} \otimes H_2^T$  and  $H_1^T \otimes \mathbf{1}_{r_2}$  are full-rank, and thus so too are both  $H_X$  and  $H_Z$

<sup>37</sup>Meaning that  $\ker(H_i^T) = 0$ .

(just consider e.g. vectors of the form  $(0|s)$  for  $H_X$ ). Since  $H_X$  ( $H_Z$ ) has  $r_1 n_2$  ( $r_2 n_1$ ) rows, the code dimension is thus

$$k = n - r_1 n_2 - r_2 n_1 = k_1 k_2 \quad (607)$$

as claimed.

Now for the distance. The fact that  $d = \min(d_1, d_2)$  essentially follows from the fact that the logical operators of the quantum code are inherited from those of  $H_{1,2}$ . This can be seen by looking at the figure above: each logical operator for  $H_2$  gives us a set of  $X$  logical operators supported on single columns of the system, while each logical for  $H_1$  gives us a  $Z$  logical supported on single rows.

More formally, let  $c_i$  be the minimum-weight codeword(s) in  $\ker(H_i)$ , and consider the vectors  $v_X = (c_1 \otimes e_1|0)$  and  $v_Z = (e_1 \otimes c_2|0)$ , where  $e_1 = (1, 0, \dots, 0)$ . Clearly  $v_\mu \in \ker(H_\mu)$  and  $v_\mu \notin \text{im}(H_\mu^T)$ ; thus the weight of the lightest nontrivial logical operators in the product code is upper bounded by the weights of the logicals of the classical code, showing that  $d \leq \min(d_1, d_2)$  (note to self: is it weird that these logicals just act on the  $n_1 n_2$  block of physical qubits?). At the time of writing I am however unsure of the best way to derive the matching lower bound. □

Note that if the  $H_i$  are sparse, then so are  $H_{X,Z}$ , and that unlike the usual CSS construction (where e.g.  $C_X = C_1$  and  $C_Z = C_2$ ), we do not require that  $(C_2)^\perp \subseteq C_1$ . Also note that with this technology, an  $[n, \Theta(n), \sqrt{n}]$  quantum code is just as easy to construct as a  $(n, \Theta(n), \Theta(n))$  classical code. The former is itself (apparently) easy to construct asymptotically by using drawing the code's tanner graph randomly from an ensemble of biregular graphs, and so the product procedure thus gives an efficient construction of quantum codes with constant rate and  $d = \Theta(\sqrt{n})$ .

### *The toric code as a homological product*

Now for the toric code on  $T^2$ , which we want to show can be constructed as a homological product of two repetition codes. That this is true should be unsurprising since the torus is itself the product of two circles.<sup>38</sup> This construction is facilitated by making a nice choice of parity check matrix for the repetition code. Since an  $n$ -bit repetition code only stores one logical bit, a full-rank parity check matrix would be a  $(n-1) \times n$  matrix. It is however more convenient to choose the degenerate  $n \times n$  check matrix

$$H_{rep} = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots \\ 0 & 1 & 1 & 0 & \dots \\ & & \vdots & & \\ 1 & 0 & 0 & \dots & 1 \end{pmatrix} \quad (608)$$

---

<sup>38</sup>Of course we are familiar with  $T^2 = S^1 \times S^1$  as manifolds. As discrete graphs, we define the *graph product*  $G_1 \times G_2$  of two graphs  $G_1, G_2$  as the graph with nodes  $(x, y), x \in G_1, y \in G_2$ , and with an edge drawn between  $(x, y)$  and  $(x', y')$  if either  $x = x', (y, y') \in G_2$  or  $y = y', (x, x') \in G_1$  (but not both; this is kind of like how the product of two Lie algebras is generated not by  $\mathfrak{g}_1 \otimes \mathfrak{g}_2$  but by  $\mathfrak{g}_1 \otimes \mathbf{1} + \mathbf{1} \otimes \mathfrak{g}_2$ ).



so that  $[H_{rep}]_{ij} = \delta_{i,j} + \delta_{i+1,j}$ . We then claim that the toric code check matrices (for a square lattice  $T^2$ ) can be written as

$$H_X = (\mathbf{1} \otimes H_{rep} | H_{rep}^T \otimes \mathbf{1}), \quad H_Z = (H_{rep} \otimes \mathbf{1} | \mathbf{1} \otimes H_{rep}^T). \quad (609)$$

The decoding of this statement is as follows. For reasons to be explained momentarily, let us use notation where  $H_\mu = (H_\mu^V | H_\mu^H)$ . Since the  $H_\mu^{V/H}$  are  $n^2 \times n^2$  matrices, we will index their entries by tuples  $(x, y) \in \mathbb{Z}_n^2$ . We claim that the nonzero entries of the bra  $\langle x, y | H_\mu^{V/H}$  give the locations of the vertical / horizontal links which contain the support of the TC  $\mu$  stabilizer located at the vertex  $(x, y)$ . To check the veracity of this, consider first  $H_X^{V/H}$ . We have

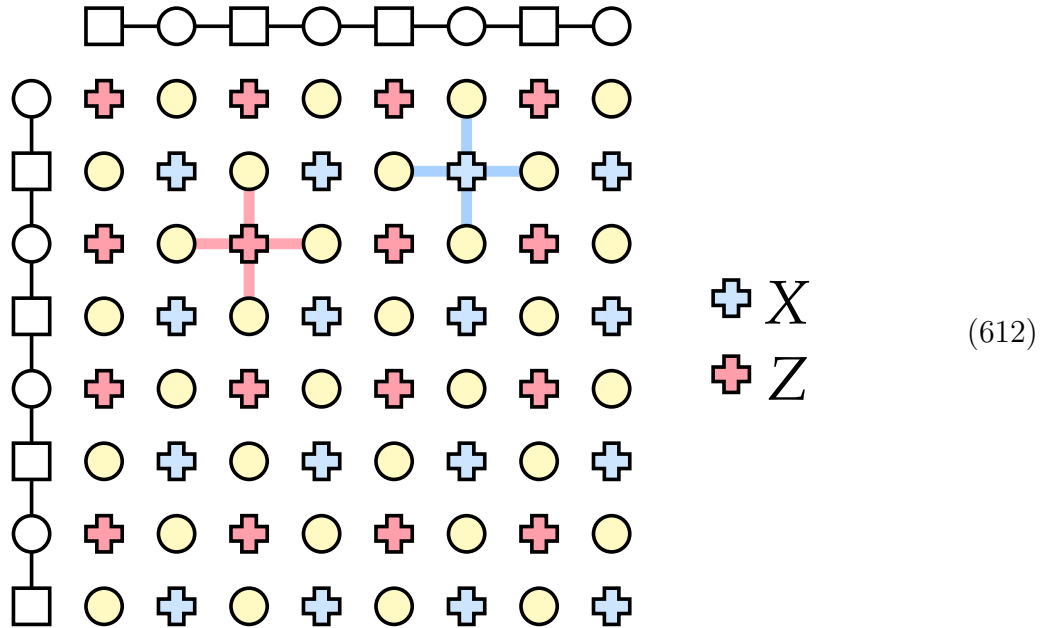
$$[H_X^V]_{xy;x'y'} = \delta_{x,x'}(\delta_{y,y'} + \delta_{y-1,y'}), \quad [H_X^H]_{xy;x'y'} = (\delta_{x,x'} + \delta_{x+1,x'})\delta_{y,y'}. \quad (610)$$

The nonzero entries of these matrices match what we expect from the star stabilizers if we identify the link  $\langle (x-1, y), (x, y) \rangle$  as the horizontal link associated with the vertex  $(x, y)$ , and  $\langle (x, y+1), (x, y) \rangle$  as the vertical link associated with  $(x, y)$ . We can also check that the same convention produces what we expect from  $H_Z$ , with the transposes arranging the links around a plaquette rather than around a vertex:

$$[H_Z^V]_{xy;x'y'} = (\delta_{x,x'} + \delta_{x-1,x'})\delta_{y,y'}, \quad [H_Z^H]_{xy;x'y'} = \delta_{x,x'}(\delta_{y,y'} + \delta_{y+1,y'}). \quad (611)$$

Therefore the product of two repetition codes indeed gives us the TC!

While the above logic of course suffices, it is also good to draw a picture. To better reflect the local geometry that arises in the product, we choose to draw the tanner graphs of each of the repetition code as length  $2n$  chains, where the even sites are checks, the odd sites are bits, and each check is connected to each of its nearest neighbor bits. To get a nice looking lattice we will also stagger the first repetition code by one lattice spacing relative to the second repetition code. Following the general procedure outlined above then gives:



where yellow dots are physical qubits, red crosses mark the locations of  $Z$  stabilizers (which connect to each of their four nearest neighboring qubits), and blue crosses mark the locations of  $X$  stabilizers (ditto). The usual square lattice one usually thinks about in the context of the toric code has vertices on the  $X$  stabilizer locations (or, just as well, on the  $Z$  stabilizer locations).



## Nice CSS codes

In this diary entry we review some simple facts about a class of CSS codes that I first encountered when working through Aharonov and Ben-Or's original fault tolerance paper.



### CSS reminder

A CSS code correcting  $t$  errors takes as input two classical codes  $C_2 \subset C_1$ , with  $C_1, C_2^\perp$  both able to correct at least  $t$  errors. The construction outputs a code  $\text{CSS}(C_1, C_2)$  with  $|C_1| - |C_2|$  linearly independent codewords

$$|\bar{a}\rangle \propto \sum_{w \in C_2} |w + a\rangle, \quad (613)$$

where  $a \in C_1/C_2$ . Letting  $H_i, G_i$  be the parity check and generator matrices of  $C_i$ ,<sup>39</sup> and using notation where  $A^{|w\rangle} = \bigotimes_{i=1}^{|w|} A^{w_i}$  for any vector  $|w\rangle$  and matrix  $A$ , the stabilizers are

$$S_{Z,\mu} = Z^{\langle \mu | H_1}, \quad S_{X,\alpha} = X^{G_2 | \alpha}, \quad (614)$$

with  $S_{Z,\mu} |\bar{a}\rangle = |\bar{a}\rangle$  by virtue of  $C_2 \subset C_1$ , which guarantees that  $|w + a\rangle \in C_1$  for each  $w, a$ . There are thus  $n - |C_1|$   $Z$  stabilizers and  $|C_2|$   $X$  stabilizers.

<sup>39</sup>Here we are working in the convention where  $\langle \mu | H$  determines the support of the  $\mu$ th stabilizer, and  $G|m\rangle$  is the  $m$ th codeword; thus  $HG = 0$  and in the canonical form one has  $H = (h|\mathbf{1}_{n-k})$ ,  $G = (\mathbf{1}_k; h)$  for an  $(n-k) \times (n-k)$  matrix  $h$  (here  $(A|B) \equiv \text{np.vstack}(A, B)$  while  $(A; B) \equiv \text{np.hstack}(A, B)$ ).

## ‘Nice’ CSS codes

In their fault tolerance paper, Aharonov and Ben-Or found a class of error correcting codes for which computation and error correction are particularly simple. In particular, in these codes, all Clifford operations are realized transversally. We will refer to such codes as *nice* CSS codes. The examples Aharonov and Ben-Or gave are constructed as  $\text{CSS}(C, C^\perp)$ , where  $C$  is a punctured doubly even self-dual codes (PDESDCs), namely a code such that

- $C$  is obtained from a code  $C'$  by removing one bit (in particular, the generator matrix  $G'$  of  $C'$  is obtained from the generator  $G$  of  $C$  by adding a single row to  $G$ ; we of course require that this row contain some non-zero entries) ,
- All codewords of  $C'$  have weight divisible by 4,
- $C'$  is self-dual, viz.  $C' = C'^\perp$ .

Note that  $|C| = |C'|$ : if this were not true then there would be two codewords of  $C'$  agreeing on their first  $n$  characters, and so the string  $0^n 1$  would be in  $C'$ , which would force the last bit of strings in  $C'$  to not participate in any parity check.

In the following we will let  $H, G$  be the parity check and generator matrices of  $C$ , and  $H', G'$  those of  $C'$ .

**Proposition 9.** *For  $C$  a punctured doubly even self-dual code,  $C^\perp \subset C$ , and  $|C/C^\perp| = 1$ . Thus  $\text{CSS}(C, C^\perp)$  is a well-defined CSS code with one logical qubit.*

*Proof.* First we show  $C^\perp \subset C$ . Suppose  $G^T w = 0$ , so that  $w \in C^\perp$ . Then since  $G'^T = (G|v)$  for some  $k$ -length vector  $v$ , we have  $G'^T(v0) = 0$ , and so  $v0 \in C'^\perp = C'$ . But if  $v0 \in C'$  we must have  $v \in C$ , and so  $C^\perp \subset C$ .

Now we show  $|C^\perp/C| = 1$ . First, for any  $[n, k]$  code,  $|C| + |C^\perp| = n$ : not because  $C \cup C^\perp$  generates the entire space, but because  $|C| = \dim \ker(H) = k$  and  $|C^\perp| = \dim \ker(G^T) = n - k$ . Since  $C'$  is self-dual, this gives  $|C'| = |C| = (n + 1)/2$ , and consequently  $|C^\perp| = n - |C| = (n - 1)/2$ , yielding  $|C| - |C^\perp| = 1$  as promised.  $\square$

Note that if  $C$  is to be a PDESDC we must evidently take  $n$  to be odd.

The above result means that if  $C$  is a PDESDC,  $\text{CSS}(C, C^\perp)$  defines a single logical qubit. Explicitly,

**Proposition 10.** *If  $C$  is a PDESDC, we may take the logical states in  $\text{CSS}(C, C^\perp)$  as*

$$|\bar{a}\rangle \propto \sum_{w \in C^\perp} |w + a1^n\rangle, \quad (615)$$

where  $a \in \{0, 1\}$ .

*Proof.* We only need to show that the string  $1^n$  is in  $C$  but not  $C^\perp$ . First, since all codewords in  $C'$  have even weight, we have  $G^T 1^{n+1} = 0$ , so that  $1^{n+1} \in C'^\perp = C'$ ; hence  $1^n \in C$ . Aharonov and Ben-Or say that  $1^n \notin C^\perp$  because  $n$  is odd, which I don't see immediately. Instead, we argue by contradiction: if  $1^n \in C^\perp$ , then  $G^T 1^n = 0$ , so that all codewords in  $C$  would need to have even weight. But since all codewords in  $C'$  have even weight, this would only be possible if all codewords of  $C'$  were obtained from those of  $C$  by appending a single 0, which is a contradiction.  $\square$

**Proposition 11.** *If  $w \in C^\perp$ ,  $\text{wt}(w) = 4$ . If  $w \in C \setminus C^\perp$ ,  $\text{wt}(w) = 3$ .*

*Proof.* First note that  $w \in C^\perp$  iff  $w0 \in C'^\perp = C'$ . Thus if  $w \in C^\perp$ , we have  $\text{wt}(w) = \text{wt}(w0) = 4$ . For the second part, suppose  $w \in C \setminus C^\perp$ . Then  $w0 \notin C'$ . However we must have  $w1 \in C'$ , and so  $\text{wt}(w) = \text{wt}(w1) - 1 = 3$ .  $\square$

Since we showed above that  $1^n \in C \setminus C^\perp$ , this shows that PDESDCs can exist only if  $n = 3 \pmod{4}$ .

## Transversal Clifford gates

The main merit of nice CSS codes is that Clifford gates are implemented transversally, which simplifies proofs of fault tolerance. In what follows we will let  $\tilde{\mathcal{O}}$  denote the transversal application of an operator, viz. the tensor product of  $n$  copies of an operator  $\mathcal{O}$  (with  $\mathcal{O}$  for us always acting either on single qubits or pairs of qubits).

### Paulis

The fact that the logical states are as given in (615) immediately implies that the logical  $Z$  and  $X$  are indeed given by  $\tilde{Z}, \tilde{X}$  (of course this is redundant given that  $S, H, \text{CNOT}$  generate the Clifford group but still worth noting). For  $\tilde{X}$  this follows from  $\tilde{X}|w\rangle = |w + 1^n\rangle$ ; for  $\tilde{Z}$  it follows from the fact that  $\text{wt}(w) \in 4\mathbb{Z}$  for all  $w \in C^\perp$ .

### $S$

When we apply  $S = \text{diag}(1, i)$  transversally,

$$\tilde{S}|\bar{a}\rangle \propto \sum_{u \in C^\perp} i^{(u+a1^n) \cdot 1^n} = i^{-a} |\bar{a}\rangle, \quad (616)$$

where we used  $i^{u \cdot 1^n} = 1$  for  $u \in C^\perp$  (using yet again that  $\text{wt}(u) \in 4\mathbb{Z}$  for  $u \in C^\perp$ ) and  $i^{a1^n \cdot 1^n} = i^{an} = i^{-a}$  since  $n = 3 \pmod{4}$ . Therefore  $\tilde{S}$  applies a logical  $S^\dagger$ , which is of course just as good as applying  $S$  itself.

### Hadamard

Letting  $\mathbb{Z}_2 = \{0, 1\}$ ,

$$\begin{aligned} \tilde{H}|\bar{a}\rangle &\propto \sum_{w \in C^\perp} \sum_{u \in \mathbb{Z}_2^n} (-1)^{u \cdot (w+a1^n)} |u\rangle \\ &\propto \sum_{u \in C} (-1)^{au \cdot 1^n} |u\rangle \\ &\propto \sum_{b \in \mathbb{Z}_2} \sum_{u \in C^\perp} (-1)^{ab1^n \cdot 1^n + au \cdot 1^n} \\ &= \sum_{b \in \mathbb{Z}_2} (-1)^{ab} |\bar{b}\rangle, \end{aligned} \quad (617)$$

where we used  $u \cdot 1^n = 0$  for any  $u \in C^\perp$  (on account of  $\text{wt}(u) \in 4\mathbb{Z}$  for all  $u \in C^\perp$ ),  $(-1)^{ab1^n \cdot 1^n} = (-1)^{abn} = (-1)^{ab}$  on account of  $n = 3 \pmod{4}$ , and the fact that  $C = C^\perp + \mathbb{Z}_2 1^n$ .

*CNOT*

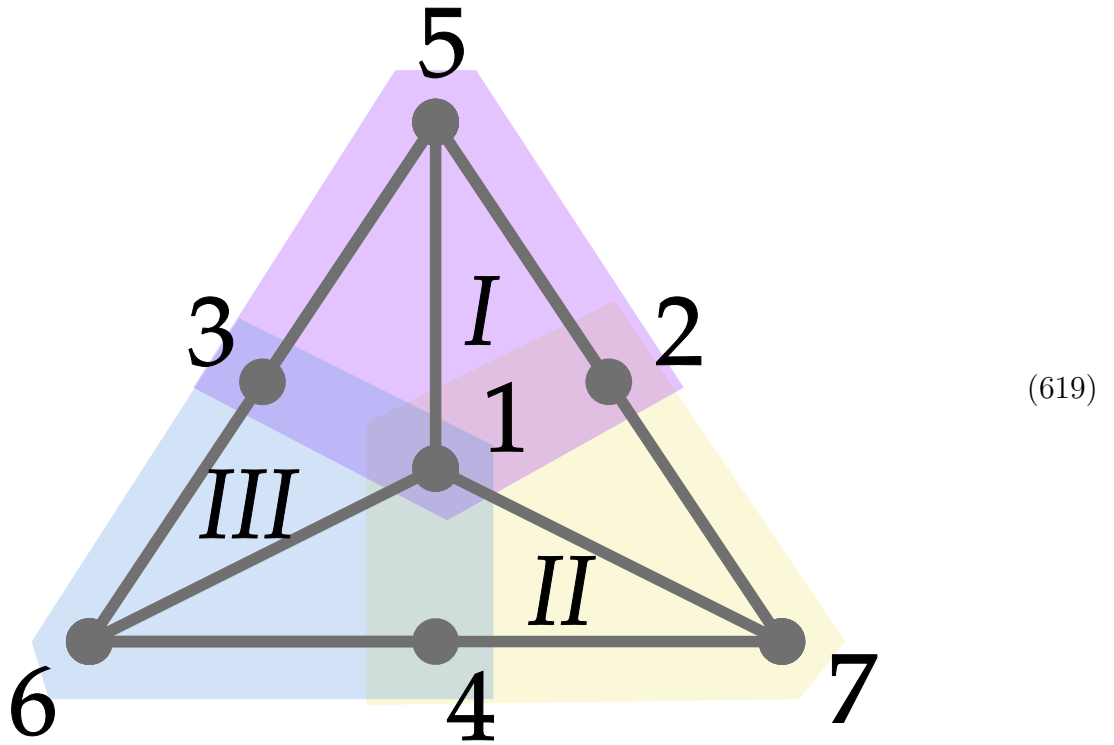
CNOT is easy:

$$\begin{aligned}\widetilde{\text{CNOT}}|\bar{a}, \bar{b}\rangle &\propto \sum_{u,v \in C^\perp} |u + a1^n, u + v + (a+b)1^n\rangle \\ &= |\bar{a}, \overline{a+b}\rangle,\end{aligned}\tag{618}$$

since  $C^\perp$  is linear.

## Example: the Steane code

The Steane code is a simple nice quantum code, equal to  $\text{CSS}(C, C^\perp)$  for  $C$  the Hamming code on 7 bits and  $C^\perp$  the associated Hadamard code. We discuss this example explicitly for the sole purpose of fixing conventions for the Hamming code  $C_{\text{Ham}}$  which can be referred to later. The following labeling of bits gives us Hamming parity check and generator matrices in canonical form:



where the colored segments correspond to the regions on which each stabilizer acts. The parity check and generator matrices are then

$$H_{\text{Ham}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & & 1 & 1 & 1 \\ 1 & 1 & & 1 & 1 \end{pmatrix}\tag{620}$$

and

$$G_{\text{Ham}} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ 1 & 1 & 1 & & \\ 1 & & 1 & 1 & \\ 1 & 1 & & & 1 \end{pmatrix} \quad (621)$$

Note that  $|1^m\rangle \in C_{\text{Ham}}$  on account of all parity checks having (doubly) even weight. One also readily checks that the rows of  $H$  are all orthogonal, so that  $C_{\text{Ham}}^\perp \subset C_{\text{Ham}}$ .

The generator and parity check matrices  $G', H'$  of the code  $C'$  from which the Steane code is obtained by puncturing can be found by adding a row onto  $G$  and a row and column onto  $H$  such that  $G' = H'^T$  (since the unpunctured code is self-dual). From this one sees that in canonical form,

$$G' = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ 1 & 1 & 1 & & \\ 1 & & 1 & 1 & \\ 1 & 1 & & & 1 \\ & 1 & 1 & 1 & \end{pmatrix} \quad (622)$$

and  $H' = G'^T$ . Geometrically, this corresponds to adding another bit “outside” of the tetrahedron, which is connected via a new parity check to the bits marked 2,3,4. Note that all of the parity checks and codewords of  $C'$  have weight 4.

One option for the  $X$  and  $Z$  logicals is of course just to take products of  $X$  and  $Z$  over all 7 sites. Using the stabilizers, we can equivalently take products over any 3 qubits that lie in a straight line; one readily verifies the cute fact that any two such lines always intersect in an odd number of locations.



## Absolutely stable ergodicity breaking cannot be achieved with unital dynamics

---

This diary entry is devoted to showing in a somewhat unnecessary amount of detail that no nontrivial “phases of matter”—here defined as dynamical systems which retain memory of their initial conditions for long times, even in the presence of arbitrary weak perturbations—can exist in systems whose dynamics is driven by a unital quantum channel.



Let  $\text{Dyn}$  be a quantum channel generating a general discrete-time dynamics acting on the set of density matrices for a system with Hilbert space  $\mathcal{H}$ . We will assume that  $\mathcal{H}$  tensor factorizes as a collection of  $L$  qubits. The tensor factorization will turn out to be important, but the assumption that each degree of freedom is a qubit is immaterial.

We will assume that  $\text{Dyn}$  is statistically time-translation invariant, meaning that the action of  $\text{Dyn}$  is either the same at all time steps, or that its action at each time step is determined by sampling from a time-independent probability distribution. We will let  $\text{Dyn}^t(\rho)$  denote the result of evolving the density matrix  $\rho$  under  $\text{Dyn}$  for  $t$  time steps.<sup>40</sup>

We are interested in studying systems with long memories, meaning that there exist density matrices which are nearly invariant under  $\mathcal{H}$ . This is trivially possible when  $\text{Dyn}$  is reducible, i.e. when there exist states which are not connected by  $\text{Dyn}^t$  even when  $t \rightarrow \infty$ . In the more interesting case when the action of  $\text{Dyn}$  is irreducible but possesses states which mix exponentially slowly,  $\text{Dyn}$  will be said to exhibit ergodicity breaking. We formalize these statements in the following definition:

**Definition 3.** The dynamics  $\text{Dyn}$  is said to be *reducible* if there exists a projector  $\Pi_R$  onto a subspace  $R \subset \mathcal{H}$  with  $|R| < \frac{1}{2}|\mathcal{H}|$ , such that  $\text{Tr}[\text{Dyn}^t(\Pi_R)\Pi_R] = \text{Tr}[\Pi_R]$  is independent of  $t$ . Reducible dynamics retains memory of its initial conditions for infinitely long times.

Let  $\rho_R \equiv \Pi_R/|R|$  be the uniform distribution on  $R$ .  $\text{Dyn}$  is said to exhibit *ergodicity breaking* if<sup>41</sup>

$$\lim_{t \rightarrow \infty} \rho_R = \frac{1}{|\mathcal{H}|} \quad (623)$$

is maximally mixed, and if  $\rho_R$  is  $\varepsilon$ -indistinguishable from  $\text{Dyn}^t(\rho_R)$  for times exponentially long in system size:

$$\min\{t : T(\text{Dyn}^t(\rho_R), \rho_R) > \varepsilon\} = e^{\Omega(L)}, \quad (624)$$

where  $T(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$  is the trace distance, and  $\varepsilon < 1/2$  is a fixed  $O(1)$  constant (a binary POVM attempting to distinguish between  $\text{Dyn}^t(\rho_R)$  and  $\rho_R$  succeeds with probability  $1/2 + \varepsilon/2$ ; we choose  $\varepsilon < 1/2$  since the value of  $T(\text{Dyn}^\infty(\rho_R), \rho_R) = 1 - |R|/|\mathcal{H}|$  can be as small as  $1/2$ ).

The strongest possible robustness requirement we can place on ergodicity breaking is that it be present even when  $\text{Dyn}$  is weakly perturbed by a general local quantum channel. To this end, we make the following definition:

---

<sup>40</sup>In this discussion we are assuming that the evolution is Markovian; taking  $\text{Dyn}$  to be non-Markovian but unital (as would e.g. be the case of subsystem evolution) does not change the conclusions about stability below.

<sup>41</sup>One could contemplate a more general version of this definition by replacing  $\text{Tr}[\text{Dyn}^t(\Pi_R)\Pi_R]$  with  $\text{Tr}[\text{Dyn}^t(\Pi)P(t)]$ , where  $P(t)$  is a fixed constant-dimension 1-parameter family of projectors, with  $P(0) = \Pi$ ,  $\dim[P(t)] = \dim[P(0)] \forall t$ . This would correspond to a situation in which an initial state moves ergodically throughout Hilbert space in a non-diffusive way, remaining localized for exponentially long  $t$ . Constructing examples of this could be interesting but would take us rather far afield, and would probably not modify the conclusions about stability given below.

**Definition 4.** Let  $\text{Dyn}_p$  be the dynamics defined by

$$\text{Dyn}_p \equiv \mathcal{N}_p \circ \text{Dyn}, \quad (625)$$

where  $\mathcal{N}_p = \bigotimes_i \mathcal{N}_{i,p}$  is a channel with  $\|\mathcal{N}_{i,p} - \mathbf{1}\|_\diamond \leq p$  for all  $i$ , where each  $\mathcal{N}_i$  acts on an  $O(1)$  number of qubits, and where the support of the  $\mathcal{N}_i$  are disjoint.<sup>42</sup> If  $\text{Dyn}_p$  exhibits ergodicity breaking for all  $p$  less than some  $O(1)$  threshold  $p_*$ ,<sup>43</sup> we say that  $\text{Dyn}$  exhibits *absolutely stable ergodicity breaking*.

The following theorem essentially shows that absolute stability can be achieved only if  $\text{Dyn}$  is allowed to dissipate waste heat to a cold external environment, or if one is allowed to perform measurements and feedback. In particular, if  $\text{Dyn}$  corresponds to unitary evolution under some type of constrained dynamics, then inserting Haar-random single-site gates with probability  $p$  into the dynamics rapidly destroys HSF, for all  $p$  of order 1.

**Theorem 4.** *If each step of  $\text{Dyn}$  is described by a unital channel,  $\text{Dyn}$  cannot exhibit absolutely stable ergodicity breaking. Moreover, there always exist small perturbations of  $\text{Dyn}$  which erase all memory of initial conditions in time  $O(\log(L))$ .*

*Proof.* Suppose by contradiction that  $\text{Dyn}$  is a unital channel exhibiting absolutely stable ergodicity breaking. Let  $\mathcal{D}_p$  be the single-qubit channel which applies depolarizing noise of strength  $p$ . Then<sup>44</sup>

$$\text{Dyn}_p = \mathcal{D}_p^{\otimes L} \circ \text{Dyn} \quad (626)$$

must also exhibit ergodicity breaking for some sufficiently small  $p = O(1)$ . This turns out to be impossible, as follows from the fact that quantum computation in an environment subject to depolarizing noise is impossible without access to fresh qubits (see e.g. the early paper of Aharonov and Ben-Or on reliable computation).

The proof works by noting that each application of  $\text{Dyn}_p$  on a state  $\rho$  increases the entropy of  $\rho$  by a significant amount. First, we recall that if  $\mathcal{N}$  is a unital channel, then the entropy change  $d_{\mathcal{N}} S(\rho) \equiv S(\mathcal{N}(\rho)) - S(\rho) \geq 0$ . This follows from the contractivity of the relative entropy  $S(\mathcal{N}(\rho) \|\mathcal{N}(\sigma)) \leq S(\rho \|\sigma)$ ; when  $\mathcal{N}$  is unital we may set  $\sigma = \mathbf{1}$  and use  $S(\rho \|\mathbf{1}) = -S(\rho)$  to obtain  $S(\mathcal{N}(\rho)) \geq S(\rho)$ . Thus  $d_{\text{Dyn}_p} S(\rho) \geq d_{\mathcal{D}_p^{\otimes L}} S(\rho)$ , and we only need to lower bound  $d_{\mathcal{D}_p^{\otimes L}} S(\rho)$ .

It is clear that a single qubit approaches the maximally mixed state exponentially quickly. Although the details are not needed, if  $\rho = \frac{1}{2}(\mathbf{1} + w^a \sigma^a)$ , a short calculation gives (taking logarithms in base 2)

$$S(\mathcal{D}_p^t(\rho)) = H_2 \left( \frac{1 + |w|(1 - 4p/3)^t}{2} \right) \geq 1 - \frac{|w|^2}{2} (1 - 4p/3)^{2t}, \quad (627)$$

since  $\mathcal{D}_p(\rho)$  replaces  $\rho$  by the maximally mixed state with probability  $4p/3$ . When we have  $L$  qubits, each of which on averages loses its memory in  $O(1)$  time, we expect that fluctuations

<sup>42</sup>Allowing for overlapping support or exponentially-decaying correlations between the  $\mathcal{N}_{i,p}$  is not expected to change anything.

<sup>43</sup>Allowing  $p_* = \Theta(1/\text{poly}(L))$  would not change the conclusions about stability.

<sup>44</sup>Of course  $\|\mathcal{D}_p - \mathbf{1}\|_\diamond$  may not be exactly  $p$  (I haven't calculated its value) but it is clearly proportional to  $p$ , and that is what matters.



in the noise will allow a small  $O(1)$  fraction of the qubits to survive for times  $O(\log(L))$ , thus limiting the memory to times only logarithmic in system size. This is indeed the case as can be demonstrated by following the approach in Aharonov and Ben-Or's paper, which for an arbitrary initial density matrix  $\rho$  can be shown to yield

$$S(\text{Dyn}_p^t(\rho)) \geq L(1 - e^{-\alpha_p t}) + e^{-\alpha_p t} S(\rho), \quad (628)$$

where  $\alpha_p = |\ln(1 - 4p/3)|$ .

We finish the proof by showing the (rather obvious) fact that the above implies that the time in (624) is  $O(\log(L))$ . For notational convenience, let  $\tilde{\mathbf{1}} \equiv \mathbf{1}/|\mathcal{H}|$  denote the maximally mixed state. Then  $S(\text{Dyn}_p^t(\rho) || \tilde{\mathbf{1}}) = L - S(\text{Dyn}_p^t(\rho))$  implies

$$S(\text{Dyn}_p^t(\rho) || \tilde{\mathbf{1}}) \leq e^{-\alpha_p t} (L - S(\rho)). \quad (629)$$

We then use the quantum Pinsker's inequality  $S(\rho || \sigma) \geq \frac{1}{2} \|\rho - \sigma\|_1^2$  to conclude

$$T(\text{Dyn}_p^t(\rho), \tilde{\mathbf{1}}) \leq \sqrt{\frac{L - S(\rho)}{2}} e^{-\alpha_p t/2}. \quad (630)$$

Then using the triangle inequality,

$$\begin{aligned} T(\text{Dyn}_p^t(\rho), \rho_R) &\geq T(\rho_R, \tilde{\mathbf{1}}) - T(\text{Dyn}_p^t(\rho), \tilde{\mathbf{1}}) \\ &\geq 1 - \frac{|R|}{|\mathcal{H}|} - \sqrt{\frac{L - S(\rho)}{2}} e^{-\alpha_p t/2}. \end{aligned} \quad (631)$$

Setting the LHS equal to  $\varepsilon$ , we see that (624) is definitely satisfied by a time  $t_{\text{th}}$ , where

$$t_{\text{th}} = \frac{1}{\alpha_p} \ln \frac{L - S(\rho)}{2(1 - \varepsilon - |R|/|\mathcal{H}|^2)} = O(\log(L)), \quad (632)$$

meaning that memory is lost in a time  $O(\log(L))$ , as claimed.  $\square$

Some remarks:

- This result applies even if  $\text{Dyn}$  is allowed to be arbitrarily nonlocal.
- While we have phrased the perturbation to  $\text{Dyn}$  as occurring within open-system dynamics, this is not essential. Suppose instead that the perturbed dynamics is obtained from  $\text{Dyn}$  by adding Haar-random single-qubit gates on each site with probability  $p$ .<sup>45</sup> If the resulting dynamics breaks ergodicity then it must do so after doing the Haar average, which can be shown to be essentially equivalent to the above depolarizing noise model.

<sup>45</sup>This is of course equivalent to adding random unitaries which are “ $p$ -close” to  $\mathbf{1}$  on every site with probability 1. For example, consider acting with the gate  $e^{i\theta X}$ , where  $\theta$  is sampled according to an arbitrary distribution  $p(\theta)$  (which we might imagine being sharply peaked around  $\theta = 0$ ). Letting  $\langle \theta \rangle_p = 0$  wolog, the average action of the gates is  $\mathbb{E}_\theta e^{i\theta X} \rho e^{-i\theta X} = (1 - \bar{p})\rho + \bar{p}X\rho X$ ,  $\bar{p} \equiv \int d\theta \sin^2(\theta)$ , which is equivalent to applying  $X$  with probability  $\bar{p}$ .

- One is bounded by the same  $\log(L)$  timescale even in the case of an erasure channel with probability  $p$  where one knows the locations of the erasures.



## Global constraints on subsystem entanglement

---

In this diary entry we will prove some rather trivial results about entanglement in systems evolving from product states under constrained dynamics. We will consider constraints coming from either a  $U(1)$  conserved charge, or from a strongly-fragmenting dynamical constraint. Throughout we will consider only dynamics acting on a 1d system of size  $L$ .



### Global $U(1)$ charge

First consider a qubit chain with a conserved  $U(1)$  charge. We begin by showing a result that is painfully obvious but which will be worked out regardless for fun:

**Proposition 12.** *Let  $\rho_Q$  be a random density matrix with charge  $Q$ . Define  $n \equiv Q/L$  and take  $L \rightarrow \infty$ , with  $n$  fixed. Then for any subsystem of size  $A \gg 1$ , with  $A/L \rightarrow 0$ , the entanglement of  $\rho_{Q,A} \equiv \text{Tr}_{A^c}[\rho_Q]$  is almost surely (up to subleading terms scaling as  $o(A)$ )*

$$S(\rho_{Q,A}) = |A|H_2(n) \quad (633)$$

with  $H_2$  the binary Shannon entropy.

In particular, when  $n \neq 1/2$ ,  $A$  is almost surely less than maximally entangled with its complement.

*Proof.* Consider first the entanglement of the maximally mixed state with charge sector  $Q$ , which we write as

$$\tilde{\mathbf{1}}_Q \equiv \frac{1}{\binom{L}{Q}} \Pi_Q \quad (634)$$

where  $\Pi_Q$  projects onto the charge  $Q$  sector. The reduced density matrix on  $A$  is, overloading notation by writing  $A$  instead of  $|A|$ :

$$\text{Tr}_{A^c}(\tilde{\mathbf{1}}_Q) = \sum_{q=0}^A \frac{\binom{L-A}{Q-q}}{\binom{L}{Q}} \Pi_{q,A}, \quad (635)$$

where  $\Pi_{q,A}$  projects onto the Hilbert space of  $A$  having charge  $q$ . The entropy of this state is

$$S(\text{Tr}_{A^c}(\tilde{\mathbf{1}}_Q)) = - \sum_{q=0}^A \binom{A}{q} \frac{\binom{L-A}{Q-q}}{\binom{L}{Q}} \ln \frac{\binom{L-A}{Q-q}}{\binom{L}{Q}}. \quad (636)$$

We evaluate this by way of

$$\binom{x}{y} \approx \sqrt{\frac{x}{2\pi y(x-y)}} e^{xH_2(y/x)}. \quad (637)$$

We then use

$$H_2(x + \varepsilon) = H_2(x) + \varepsilon \ln \frac{1-x}{x} - \frac{\varepsilon^2}{2} \frac{1}{x(1-x)} \quad (638)$$

to write, in the aforementioned  $L \rightarrow \infty$  limit,

$$(L-A)H_2\left(\frac{Q-q}{L-A}\right) - LH_2(n) = -A \left( H_2(n) + (q/A - n) \ln \frac{1-n}{n} \right). \quad (639)$$

This gives

$$\begin{aligned} - \binom{A}{q} \frac{\binom{L-A}{Q-q}}{\binom{L}{Q}} \ln \frac{\binom{L-A}{Q-q}}{\binom{L}{Q}} &= A \sqrt{\frac{A}{2\pi q(A-q)}} \left( H_2(n) + (q/A - n) \ln \frac{1-n}{n} \right) \\ &\times e^{A(H_2(q/A) - H_2(n) - (q/A - n) \ln(1-n)/n)} + O(\log(A)). \end{aligned} \quad (640)$$

Doing the integral over  $q$  and dropping all subleading terms then gives the extremely reasonable result

$$S(\text{Tr}_{A^c}(\tilde{\mathbf{1}}_Q)) = \frac{AH_2(n)}{\sqrt{2\pi An(1-n)}} \int_{\mathbb{R}} dp e^{-\frac{p^2}{2An(1-n)}} = AH_2(n). \quad (641)$$

We finish the proof using Page's theorem, which we fomulate as the statement

$$\mathbb{E}_{\rho_Q}[\|\rho_{Q,A} - \text{Tr}_{A^c}(\tilde{\mathbf{1}}_Q)\|_1] \leq 2^{A-L/2}. \quad (642)$$

Markov's inequality then says that with probability  $1 - \Theta(\exp(-L))$ ,  $\rho_{Q,A}$  will be exponentially close in trace distance to  $\text{Tr}_{A^c}(\tilde{\mathbf{1}}_Q)$ , and hence (by Fannes' inequality, if you must) the entanglement entropy of  $\rho_{Q,A}$  will almost surely be exponentially close to  $AH_2(n)$ .  $\square$

### $tJ_z$ dynamics

$tJ_z$  dynamics is the simplest example (perhaps too simple) of exponentially fragmented dynamics with a strong Hilbert space bottleneck. We define the dynamics with an onsite Hilbert space of dimension  $N+1$ ,  $\mathcal{H}_{\text{onsite}} = \text{span}(|0\rangle, \dots, |N\rangle)$ , with the pattern formed by all of the non-zero basis states being conserved by the dynamics (the zero state  $|0\rangle$  is a “free space” and may move around freely). One of the many conserved quantities of this dynamics is a  $U(1)$  charge measuring the number of zeros that appear in a given string:

$$Q \equiv \sum_i |0\rangle\langle 0|_i. \quad (643)$$

As above we will let  $n = Q/L$  denote the average value of this charge.

*OBC: boundary subsystem*

Consider an open chain of length  $L$  partitioned into a left half  $A$  and a right half  $A^c$ . While in the  $U(1)$  case we could have maximally entangled subsystems at charge density  $n = 1/2$ , for  $tJ_z$  this is not possible: if  $\rho$  is a random state in a fixed Krylov sector, then  $\rho_A$  is less than maximally entangled with probability 1:

**Proposition 13.** *Let  $\rho_{\mathbf{s}}$  be a random density matrix in  $\mathcal{K}_{\mathbf{s}}$ , the Krylov sector of states with irreducible string  $\mathbf{s}$ , and define  $Q = |\mathbf{s}|$ ,  $n = Q/L$ . Then the entanglement of  $\rho_{\mathbf{s},A} \equiv \text{Tr}_{A^c}[\rho_{\mathbf{s}}]$  is almost surely (up to  $o(A)$  terms)*

$$S(\rho_{\mathbf{s},A}) = AH_2(n). \quad (644)$$

In particular, the maximum entropy that can be obtained is  $A \ln(2) = \ln |\mathcal{K}_{\max}|$ , less than the Page value of  $A \ln(3)$ .

*Proof.* The proof is exactly the same as in the case for a  $U(1)$  conserved charge, as in this particular setup the spin degrees of freedom contribute no entropy: given the value of the total  $U(1)$  charge in  $A$ , the spin pattern in  $A$  is uniquely fixed. Thus the entropy comes entirely from the  $U(1)$  charge, whose expected density is  $n$ , around which the probability distribution defined by the RDM on  $A$  concentrates.  $\square$

Note that in order to maximize the entanglement entropy in this case, we need to choose a sector at half filling for the  $U(1)$  charge. While such sectors are the ones of largest dimension, they are *not* typical: if we instead pick a *random* (computational basis) product state in which to initialize the dynamics, we will instead almost surely have  $n = 1/(N+1)$  giving a value of  $S(\rho_{\mathbf{s},A})$  even further from the Page value.

*PBC*

Things change when periodic boundary conditions are applied.

**Proposition 14.** *Let  $\mathbf{s}$  be randomly chosen from the set of irreducible strings of length  $|\mathbf{s}| = Q$ , and let  $\rho_{\mathbf{s}}$  be a random density matrix in  $\mathcal{K}_{\mathbf{s}}$ . Then the entanglement of  $\rho_{\mathbf{s},A}$  is almost surely (up to  $o(A)$  terms)*

$$S(\rho_{\mathbf{s},A}) = A(H_2(n) + (1-n)\ln(N)) \quad (645)$$

with  $n = Q/L$  as before.

The physical interpretation of this result is very simple: the first term comes from the entropy of the  $U(1)$  charge, and the second term comes from the entropy produced by moving  $\mathbf{s}$  so that different substrings occupy  $A$ .  $S(\rho_{\mathbf{s},A})$  is maximized when  $n = 1/(N+1)$ , the expected value of  $n$  in a random state, for which it equals the Page value.

*Proof.* We again consider the maximally mixed state  $\tilde{\mathbf{1}}_{\mathbf{s}}$  over the sector  $\mathcal{K}_{\mathbf{s}}$ . With PBC, the dimension of this sector is  $\binom{L}{Q}N_{\sigma}$ , where  $N_{\sigma} = |\Sigma_{\mathbf{s}}|$  is the number of cyclic permutations  $\sigma \in \Sigma_{\mathbf{s}}$  of  $\mathbf{s}$  such that  $\mathbf{s} \neq \sigma(\mathbf{s})$ . We may decompose  $\tilde{\mathbf{1}}_{\mathbf{s}}$  as

$$\tilde{\mathbf{1}}_{\mathbf{s}} = \frac{1}{N_{\sigma,\mathbf{s}}\binom{L}{Q}} \sum_{\sigma \in \Sigma_{\mathbf{s}}} \sum_{q=0}^A \Pi_{\sigma(\mathbf{s})_{1:A-q},A} \otimes \Pi_{\sigma(\mathbf{s})_{A-q:L-A}}, \quad (646)$$

where  $\sigma(\mathbf{s})_{1:A-q}$  is the string defined by the first  $A-q$  characters of  $\sigma(\mathbf{s})$ , and  $\sigma(\mathbf{s})_{A-q:}$  is the remainder of  $\mathbf{s}$ . The RDM on  $A$  can then be rewritten as

$$\rho_{\mathbf{s},A} = \sum_{q=0}^A \sum_{\mathbf{s}_A \in \text{dist}_{A-q}(\mathbf{s})} \sum_{\sigma \in \Sigma_{\mathbf{s}} : \sigma(\mathbf{s})_{1:A-q} = \mathbf{s}_A} \frac{1}{N_{\sigma} \binom{L}{Q}} \binom{L-A}{Q-q} \Pi_{\mathbf{s}_A,A}, \quad (647)$$

where  $\text{dist}_{A-q}(\mathbf{s})$  is the set of distinct substrings of  $\mathbf{s}$  of length  $A-q$ . If  $\mathbf{s}$  is chosen at random, each of these substrings will occur with equal probabilities, and so we will assume that  $\mathbf{s}$  is chosen so that the empirical distribution on  $\mathbf{s}_A$  is exactly uniform (and the entropy is maximized in this case). Note that in order for this to be the case, we require that  $L > 2^A$ .

To simplify notation, define  $N_{\sigma|\mathbf{s}_A} \equiv |\{\sigma \in \Sigma_{\mathbf{s}} : \sigma(\mathbf{s})_{1:A-q} = \mathbf{s}_A\}|$ . Then with the above assumption on  $\mathbf{s}$ ,

$$\rho_{\mathbf{s},A} = \sum_{q=0}^A \sum_{\mathbf{s}_A \in \text{dist}_{A-q}(\mathbf{s})} \frac{N_{\sigma|\mathbf{s}_A}}{N_{\sigma} \binom{L}{Q}} \binom{L-A}{Q-q} \Pi_{\mathbf{s}_A}. \quad (648)$$

Now again by the above assumption,  $|\text{dist}_{A-q}(\mathbf{s})| = N^{A-q}$ , and  $N_{\sigma|\mathbf{s}_A}/N_{\sigma} = N^{-(A-q)}$  (since the latter measures the fraction of cyclic translates of  $\mathbf{s}$  that begin with  $\mathbf{s}_A$ , and all  $\mathbf{s}_A$  occur with equal probability by assumption). Therefore the entanglement entropy is then

$$\begin{aligned} S(\rho_{\mathbf{s},A}) &= - \sum_{q=0}^A \frac{\binom{A}{q} \binom{L-A}{Q-q}}{\binom{L}{Q}} \left( \ln \frac{\binom{L-A}{Q-q}}{\binom{L}{Q}} + \ln N^{-(A-q)} \right) \\ &= AH_2(n) + A \ln N \sum_{q=0}^A (1 - q/A) \frac{\binom{A}{q} \binom{L-A}{Q-q}}{\binom{L}{Q}}, \end{aligned} \quad (649)$$

where we used our earlier result for the case of a single  $U(1)$  charge. The same techniques as used above can then be used to show that the remaining sum evaluates to  $1 - n$  in the appropriate limit, giving the desired result.  $\square$

For this result to work, we needed  $L > N^A$ , and it is straightforward to show that if  $L = o(M^A)$  for any  $M < N$ , then  $S(\rho_{\mathbf{s},A})$  must be less than the Page value. Thus maximally mixing a subsystem with  $tJ_z$  dynamics is possible with periodic boundary conditions, but doing so requires exponential space resources.

### *OBC: bulk subsystem*

As long as the subsystem we consider is located deep in the bulk, this case is not fundamentally different from the PBC setup. The only difference lies in the spatial resources required to achieve a maximal contribution from the spin part of the entropy: to get a uniform distribution on the  $\mathbf{s}_A$ ,  $L$  must be large enough that all of the  $\sim N^A$  distinct choices of  $\mathbf{s}_A$  are within a  $\sim \sqrt{L}$  distance of  $A$ , since each  $A$ -sized substring in  $\mathbf{s}$  can only diffuse over a distance of  $\sim \sqrt{L}$ . Therefore Page values can only be achieved when  $L = \Omega(N^{2A})$ , which necessitates exponentially more spatial resources than in the case with periodic boundary conditions.

### Exponentially modulated symmetry

Finally we consider a spin-1 model whose dynamics conserves

$$Q = \sum_i 2^i S_i^z. \quad (650)$$

This dynamics mandates that subsystems quenched from product states always be at sub-Page entanglement for *all* boundary conditions, even when  $L = \infty$ .

This can be seen by considering the operator

$$Q_A = \sum_{i \in A} 2^{i-i_{l,A}} n_i, \quad (651)$$

where  $i_{l,A}$  is the site at the leftmost end of  $A$ ; with this definition  $Q_A$  can take on any integer between 0 and  $Q_{A,\max} = 2^{|A|+1} - 2$ . Suppose at  $t = 0$  the system is initialized in a product state with a particular initial value  $Q_A(0)$  of  $Q_A$ . Then after evolving the full system  $A \cup A^c$  under constraint-preserving dynamics, the value  $Q_A(t)$  of  $Q_A$  at time  $t$  must be expressible as

$$Q_A(t) = Q_A(0) + a + b2^{|A|}, \quad (652)$$

where  $a, b \in \{-1, 0, 1\}$  express the distinct ways that particles can be transferred between  $A$  and  $A^c$ .

Now it turns out that at large  $l$ , the size of the largest symmetry sector on a system of size  $l$  scales as  $\phi^l + \dots$ , where the  $\dots$  are subleading. Thus

$$\text{rank}(\rho_A(t)) \leq 9\phi^{|A|}, \quad (653)$$

where the factor of 9 comes from the number of ways of choosing  $a, b$ . The entanglement entropy of  $\rho_A$  is accordingly upper bounded as

$$S(\rho_A(t)) \leq |A| \ln(\phi) + \text{const}, \quad (654)$$

which since  $\ln(\phi) < \ln(3)$  means that the coefficient of the volume law can never be made to match the scaling of a random state. It is remarkable that just the imposition of a global symmetry—albeit a rather unconventional one—can produce behavior so at odds with ETH-like expectations.



### Entangled pair representation for $\mathbb{Z}_N^2$ SPTs

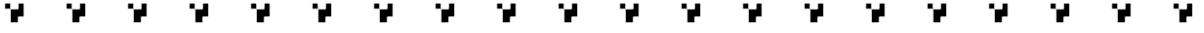
---

In today's entry we will do a short calculation of the unitary which transforms the standard fixed-point wavefunction for the  $\mathbb{Z}_N \times \mathbb{Z}_N$  SPT labeled by the cohomology class  $\omega \in \mathbb{Z}_N$  from

the “standard” representation into the entangled pairs representation. Here the standard representation is the one in which the symmetry operator at each pair of sites is

$$R_g = Z^{g_1} \otimes Z^{g_2}. \quad (655)$$

To make our lives easier we will assume  $\gcd(\omega, N) = 1$ .



In the entangled pairs representation, the representation of the symmetry is  $(V_g^{(\omega)})^* \otimes V_g^{(\omega)}$ , where for  $\mathbb{Z}_N$  the basis we will choose for the projective representation is

$$V_g^{(\omega)} = X^{g_1} Z^{\omega g_2}. \quad (656)$$

We want to then find the unitary  $U_\omega$  which satisfies

$$U_\omega R_g U_\omega^\dagger = X^{g_1} Z^{-\omega g_2} \otimes X^{g_1} Z^{\omega g_2}. \quad (657)$$

We will find it useful to define the matrix

$$F_\alpha \equiv \sum_{a,b \in \mathbb{Z}_N} \zeta_N^{-ab\alpha} |a\rangle \langle b|, \quad (658)$$

which is unitary if  $\alpha \in \mathbb{Z}_N^\times$ . This matrix satisfies

$$F_\alpha Z = X^{1/\alpha} F_\alpha, \quad F_\alpha X = Z^{-\alpha} F_\alpha. \quad (659)$$

We will write  $U_\omega$  in terms of the  $F_\alpha$  and the  $\mathbb{Z}_N$  version of the CZ gate, defined in the obvious way as

$$CZ_N = \sum_{h_1, h_2} \zeta^{-h_1 h_2} |h_1, h_2\rangle \langle h_1, h_2|. \quad (660)$$

**Proposition 15.** *The unitary in question is*

$$U_\omega = (\mathbf{1} \otimes F_\omega) \circ (CZ_N)^\omega \circ (F_1 \otimes F_1). \quad (661)$$

*Proof.* This is of course just simple algebra. After the first step,

$$F_1^{\otimes 2} R_g = (X^{g_1} \otimes X^{g_2}) F_1^{\otimes 2}. \quad (662)$$

Now one readily checks that

$$(CZ_N)^\omega (X^{g_1} \otimes X^{g_2}) = \zeta^{\omega g_1 g_2} (Z^{-\omega g_2} X^{g_1} \otimes Z^{-\omega g_1} X^{g_2}) (CZ_N)^\omega = (X^{g_1} Z^{-\omega g_2} \otimes Z^{-\omega g_1} X^{g_2}) (CZ_N)^\omega. \quad (663)$$

Finally, hitting this with  $\mathbf{1} \otimes F_{-\omega}$ , we have

$$F_{-\omega} Z^{-\omega g_1} X^{g_2} = X^{g_1} Z^{\omega g_2}. \quad (664)$$

Putting the three steps together gives the desired action of  $U_\omega$ .  $\square$



## References

---

- [1] S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM (JACM)*, 51(4):595–605, 2004.
- [2] W. Arveson. *An invitation to  $C^*$ -algebras*, volume 39. Springer Science & Business Media, 2012.
- [3] S. Ghosh, A. Deshpande, D. Hangleiter, A. V. Gorshkov, and B. Fefferman. Sharp complexity phase transitions generated by entanglement. *arXiv preprint arXiv:2212.10582*, 2022.
- [4] M. Heyl. Dynamical quantum phase transitions: a review. *Reports on Progress in Physics*, 81(5):054001, 2018.
- [5] X. Ma and W. Rhodes. Multimode squeeze operators and squeezed states. *Physical Review A*, 41(9):4625, 1990.
- [6] D. N. Page. Average entropy of a subsystem. *Physical review letters*, 71(9):1291, 1993.