Mathematical tricks frequently used in quantum information

November 29, 2025

This short note collects common mathematical tools and tricks used across quantum information theory. The aim is to provide a compact reference suitable for quick lookup while working on problems, proofs, or calculations in quantum information and quantum computing.

1 Notation and conventions

- Finite-dimensional Hilbert spaces: $\mathcal{H}$, $\dim \mathcal{H} = d$.

- Density operators: $\rho \geq 0$, $\operatorname{tr} \rho = 1$.

- Matrix/vectorization: for matrix A, $\vec{(A)}$ denotes column-stacking.

- Partial trace: $\operatorname{tr}_B(\rho_{AB}) = \rho_A$.

- Pauli matrices: X, Y, Z; computational basis $\{|0\rangle, |1\rangle\}$.

2 Linear algebra basics and "tricks"

2.1 Spectral decomposition and functions of operators

If $A = \sum_i \lambda_i |u_i\rangle \langle u_i|$, then for any (suitably defined) function f,

$$f(A) = \sum_i f(\lambda_i) |u_i\rangle \langle u_i|.$$

Useful for: $A^{1/2}$, $\log A$, $\exp(A)$.

2.2 Polar decomposition

Any operator M can be written $M = U|M|$ where $|M| = \sqrt{M^\dagger M}$ and U is partial isometry. Use to relate singular values to spectra.

2.3 Singular-value and Schmidt decompositions (swap trick)

For a bipartite vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ there exist orthonormal bases so that

$$|\psi\rangle = \sum_i \sqrt{\lambda_i} |a_i\rangle \otimes |b_i\rangle$$

with $\{\lambda_i\}$ the Schmidt coefficients. This is the SVD of the coefficient matrix. The swap trick identity often used in trace calculations is

$$\operatorname{tr}\left[(A \otimes B) |\Phi\rangle \langle \Phi|\right] = \operatorname{tr}(AB^T),$$

where $|\Phi\rangle = \sum_i |i\rangle \otimes |i\rangle$ (unnormalised) and T is transpose in the chosen basis.

2.4 Resolution of the identity

Let $\mathcal{H}$ be a (finite-dimensional, unless stated) Hilbert space, and let $\{|\psi_i\rangle\}$ denote an orthonormal basis. Operators on $\mathcal{H}$ are denoted by capital letters $A, B, \ldots$. The inner product is linear in the second slot: $\langle\phi|\psi\rangle$.

Discrete (orthonormal) basis

If $\{|e_i\rangle\}_{i=1}^{d}$ is an orthonormal basis of $\mathcal{H}$ then

$$\sum_{i=1}^{d} |e_i\rangle\langle e_i| = I. \tag{1}$$

This identity is often inserted between operators or vectors to expand them in the chosen basis.

Proof. For any vector $|\psi\rangle = \sum_i c_i |e_i\rangle$ we have

$$\left(\sum_i |e_i\rangle\langle e_i|\right)|\psi\rangle = \sum_i |e_i\rangle\langle e_i|\psi\rangle = \sum_i c_i |e_i\rangle = |\psi\rangle,$$

hence the operator equals the identity.

Trick (useful insertion). To compute matrix elements of an operator A between states $|\phi\rangle, |\psi\rangle$ one inserts the resolution:

$$\langle\phi|A|\psi\rangle = \sum_i \langle\phi|A|e_i\rangle\langle e_i|\psi\rangle.$$

More generally, insert $I = \sum_i |e_i\rangle\langle e_i|$ wherever convenient to switch between bases or to expand products of operators.

2.5 Cyclicity of the trace

For any two (finite-dimensional) operators A and B one has

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA).$$

More generally, for a product of operators,

$$\mathrm{Tr}(A_1 A_2 \cdots A_n) = \mathrm{Tr}(A_n A_1 A_2 \cdots A_{n-1}),$$

i.e. the trace is invariant under cyclic permutations.

Proof. Choose an orthonormal basis $\{|e_i\rangle\}$. Then

$$\mathrm{Tr}(AB) = \sum_i \langle e_i|AB|e_i\rangle = \sum_{i,j} \langle e_i|A|e_j\rangle\langle e_j|B|e_i\rangle$$

$$= \sum_{i,j} \langle e_j|B|e_i\rangle\langle e_i|A|e_j\rangle = \sum_j \langle e_j|BA|e_j\rangle = \mathrm{Tr}(BA).$$

Tricks and consequences

- **Cyclic reorder to simplify.** If one factor is diagonal in the chosen basis, move it cyclically to simplify the trace.

- **Trace of a commutator vanishes:** $\mathrm{Tr}([A, B]) = 0$, since $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

- **Expectation via trace:** For a density matrix ρ and observable O, $\langle O\rangle = \mathrm{Tr}(\rho O) = \mathrm{Tr}(O\rho)$ and one may cyclically permute to place convenient factors together.

2.6 Normal operators

An operator N on $\mathcal{H}$ is *normal* if

$$[N, N^\dagger] = 0 \quad \Longleftrightarrow \quad NN^\dagger = N^\dagger N. \tag{2}$$

2.7 Properties (finite-dimensional)

1. **Spectral theorem:** A normal operator is unitarily diagonalizable: there exists a unitary U such that

$$N = U \left(\sum_i \lambda_i \, |e_i\rangle \, \langle e_i| \right) U^\dagger,$$

where $\{|e_i\rangle\}$ is an orthonormal basis of eigenvectors and $\lambda_i \in \mathbb{C}$ are eigenvalues.

2. **Orthogonality of eigenvectors:** Eigenvectors corresponding to distinct eigenvalues are orthogonal.

3. **Functions of N:** For analytic functions f one has $f(N) = U \left(\sum_i f(\lambda_i) \, |e_i\rangle \, \langle e_i| \right) U^\dagger$.

2.8 Useful tricks involving normal operators

- **Diagonal basis simplification.** If N is normal, compute expressions by moving to its eigenbasis using the resolution of the identity: insert $I = \sum_i |e_i\rangle \, \langle e_i|$ and replace N by its eigenvalues on those projectors.

- **Norms:** For a normal N, the operator norm equals the spectral radius: $\|N\| = \max_i |\lambda_i|$; similarly, $N^\dagger N$ and $NN^\dagger$ share eigenvalues $|\lambda_i|^2$.

- **Commutation and polynomials:** If N is normal and p is a polynomial, then $p(N)$ commutes with $N^\dagger$.

3 Worked examples

3.1 Using resolution to compute matrix elements

Let A be an operator and $\{|i\rangle\}$ an orthonormal basis. Then

$$(A)_{mn} = \langle m|A|n\rangle = \sum_k \langle m|A|k\rangle\langle k|n\rangle = \langle m|A|n\rangle,$$

(tautological here) but if $A = BC$ one gets

$$(BC)_{mn} = \sum_k B_{mk} C_{kn}.$$

3.2 Trace trick: cyclic reduction

Suppose we want $\mathrm{Tr}(ABC)$ and C is diagonal in basis $\{|i\rangle\}$ with diagonal entries c_i. Then

$$\mathrm{Tr}(ABC) = \mathrm{Tr}(CAB) = \sum_i c_i \langle i|AB|i\rangle,$$

which may be simpler to evaluate.

3.3 Normal operator: polar decomposition

Given any operator M one can write $M = U|M|$ (polar decomposition) with $|M| = \sqrt{M^\dagger M}$. If M is normal then $|M| = \sqrt{M^\dagger M} = \sqrt{M M^\dagger}$ and U commutes with $|M|$; moreover M is unitarily diagonalizable.

Compact reference sheet

- Resolution insertion: $I = \sum_i |e_i\rangle \langle e_i|$ or $I = \int |x\rangle \langle x| \, dx$.

- Cyclicity: $\text{Tr}(AB) = \text{Tr}(BA)$ and $\text{Tr}([A, B]) = 0$.

- Normal: $NN^\dagger = N^\dagger N \Rightarrow$ unitary diagonalization.

These three facts are used constantly when manipulating expressions in quantum mechanics and linear algebra. When in doubt: insert a resolution to expand in a convenient basis, use cyclicity to reorder factors under a trace, and try to diagonalize normal operators to reduce operator problems to scalar algebra.

3.4 Calculating partial trace

Work in product basis: if $\rho_{AB} = \sum_{ijkl} c_{ijkl} |i\rangle_A \langle j| \otimes |k\rangle_B \langle l|$ then $\text{tr}_B \, \rho_{AB} = \sum_{ik} (\sum_l c_{ilkl}) |i\rangle \langle k|$.

4 Quantum states and operations

4.1 Kraus decomposition & Choi isomorphism

A completely-positive trace-preserving (CPTP) map $\mathcal{E}$ admits Kraus operators $\{K_i\}$ with $\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger$ and $\sum_i K_i^\dagger K_i = I$.

5 Techniques for proving channel/entanglement results

5.1 Twirling and symmetric subspaces

Average over a group G to project onto invariant subspaces: twirling maps simplify density operators into forms with fewer parameters. For example,

$$\int_G (U_g \otimes U_g) \, \rho \, (U_g \otimes U_g)^\dagger \, d\mu(g)$$

projects onto the symmetric/antisymmetric sectors.

5.2 Typical subspace and concentration

For many iid copies, most weight of $\rho^{\otimes n}$ lives in the typical subspace with projector Π_{typ}; used heavily in coding theorems.

5.3 Decoupling and one-shot bounds

Decoupling approaches prove achievability results by showing a subsystem becomes approximately product with another; uses random unitaries and norm estimates.