Fuchs-van de Graaf Inequalities

Formal statement

Let ρ and σ be density operators on a finite-dimensional Hilbert space. Define the trace distance by

$$D(\rho,\sigma)=\frac{1}{2}\|\rho-\sigma\|_1,$$

where

$$\|X\|_1=\operatorname{Tr}\sqrt{X^\dagger X}.$$

Define the root fidelity by

$$F(\rho,\sigma)=\|\sqrt{\rho}\sqrt{\sigma}\|_1=\operatorname{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}.$$

With these conventions, the Fuchs-van de Graaf inequalities are

$$1-F(\rho,\sigma)\le D(\rho,\sigma)\le\sqrt{1-F(\rho,\sigma)^2}.$$

Equivalently, the fidelity is bounded in terms of trace distance by

$$1-D(\rho,\sigma)\le F(\rho,\sigma)\le\sqrt{1-D(\rho,\sigma)^2}.$$

Some books use the squared-fidelity convention

$$F_{\mathrm{sq}}(\rho,\sigma)=F(\rho,\sigma)^2.$$

With that convention, the same inequalities are written as

$$1-\sqrt{F_{\mathrm{sq}}(\rho,\sigma)}\le D(\rho,\sigma)\le\sqrt{1-F_{\mathrm{sq}}(\rho,\sigma)}.$$

The theorem was introduced in quantum information through the work of Fuchs and van de Graaf on cryptographic distinguishability measures. It is now a standard tool because trace distance has a direct operational meaning as distinguishability, while fidelity has a direct geometric meaning as maximum purification overlap.

Meaning before the proof

Trace distance and fidelity answer two different questions.

Trace distance asks how well two states can be distinguished by the best possible measurement. If ρ and σ are given with equal prior probabilities, then the Helstrom theorem gives

$$P_{\text{succ}}^{\text{opt}} = \frac{1}{2}\left(1 + D(\rho, \sigma)\right).$$

Thus D(ρ,σ)=0 means that no measurement can distinguish the states, while D(ρ,σ)=1 means that the states can be perfectly distinguished.

Fidelity asks how close the states are geometrically. For pure states,

$$\rho = |\psi\rangle\langle\psi|, \qquad \sigma = |\phi\rangle\langle\phi|,$$

we have

$$F(\rho, \sigma) = |\langle\psi|\phi\rangle|.$$

For mixed states, Uhlmann's theorem says that F(ρ,σ) is the largest possible absolute inner product between purifications of ρ and σ. Thus fidelity is a geometric overlap after optimally choosing the hidden reference systems.

The Fuchs-van de Graaf inequalities say that these two notions cannot disagree too much. If two states have high fidelity, then they must be hard to distinguish. If they have small trace distance, then their fidelity must be large. The theorem is a conversion tool between geometric closeness and operational indistinguishability.

Classical prototype

The quantum inequalities are best understood by first looking at ordinary probability distributions. Let $p=(p_i)$ and $q=(q_i)$ be probability distributions. Define the total variation distance

$$\mathrm{TV}(p,q) = \frac{1}{2}\sum_i |p_i - q_i|,$$

and the classical fidelity, also called the Bhattacharyya coefficient,

$$B(p,q) = \sum_i \sqrt{p_i q_i}.$$

Then

$$1 - B(p,q) \le \mathrm{TV}(p,q) \le \sqrt{1 - B(p,q)^2}.$$

We prove this because it contains the whole idea.

For the lower bound, use the identity

$$\mathrm{TV}(p,q) = 1 - \sum_i \min\{p_i, q_i\}.$$

For each i,

$$\min\{p_i, q_i\} \le \sqrt{p_i q_i}.$$

Therefore

$$\sum_i \min\{p_i, q_i\} \le \sum_i \sqrt{p_i q_i} = B(p,q),$$

and hence

$$1 - B(p,q) \le 1 - \sum_i \min\{p_i, q_i\} = \mathrm{TV}(p,q).$$

For the upper bound, write

$$|p_i - q_i| = |\sqrt{p_i} - \sqrt{q_i}|(\sqrt{p_i} + \sqrt{q_i}).$$

By the Cauchy-Schwarz inequality,

$$\begin{aligned}\mathrm{TV}(p,q) &= \frac{1}{2}\sum_i |\sqrt{p_i}-\sqrt{q_i}|(\sqrt{p_i}+\sqrt{q_i}) \\ &\le \frac{1}{2}\sqrt{\sum_i(\sqrt{p_i}-\sqrt{q_i})^2}\sqrt{\sum_i(\sqrt{p_i}+\sqrt{q_i})^2}.\end{aligned}$$

Now

$$\sum_i(\sqrt{p_i}-\sqrt{q_i})^2 = 2-2B(p,q),$$

and

$$\sum_i(\sqrt{p_i}+\sqrt{q_i})^2 = 2+2B(p,q).$$

Therefore

$$\mathrm{TV}(p,q) \le \frac{1}{2}\sqrt{(2-2B)(2+2B)} = \sqrt{1-B^2}.$$

Thus the classical inequalities are proven.

From classical distributions to quantum states

To pass from classical probability distributions to quantum states, we use two operational characterizations.

The first is the trace-distance measurement formula:

$$D(\rho,\sigma) = \max_{\{M_y\}} \mathrm{TV}(p_y,q_y),$$

where

$$p_y = \mathrm{Tr}(M_y\rho), \qquad q_y = \mathrm{Tr}(M_y\sigma),$$

and the maximum is over all POVMs M(y)\. This is the measurement interpretation behind the Helstrom theorem.

The second is the fidelity measurement formula:

$$F(\rho, \sigma) = \min_{\{M_y\}} \sum_y \sqrt{p_y q_y}.$$

This formula says that if we measure both states using the same POVM, the resulting classical distributions always have Bhattacharyya coefficient at least the quantum fidelity; moreover, there exists an optimal measurement whose classical Bhattacharyya coefficient equals the quantum fidelity. This is closely related to the Fuchs-Caves characterization of fidelity.

We now combine these two formulas with the classical inequalities.

For the lower bound, choose a measurement M(y)\ that minimizes the classical Bhattacharyya coefficient, so that

$$\sum_y \sqrt{p_y q_y} = F(\rho, \sigma).$$

For this measurement, the classical inequality gives

$$\mathrm{TV}(p, q) \geq 1 - F(\rho, \sigma).$$

Since trace distance is the maximum total variation distance over all measurements,

$$D(\rho, \sigma) \geq \mathrm{TV}(p, q) \geq 1 - F(\rho, \sigma).$$

Thus

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma).$$

For the upper bound, choose a measurement that maximizes the total variation distance, so that

$$\mathrm{TV}(p, q) = D(\rho, \sigma).$$

For this measurement, the classical inequality gives

$$D(\rho,\sigma) \leq \sqrt{1 - B(p,q)^2},$$

where

$$B(p,q) = \sum_y \sqrt{p_y q_y}.$$

Since the quantum fidelity is the minimum possible classical Bhattacharyya coefficient,

$$B(p,q) \geq F(\rho,\sigma).$$

Therefore

$$\sqrt{1 - B(p,q)^2} \leq \sqrt{1 - F(\rho,\sigma)^2}.$$

Hence

$$D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}.$$

Combining both sides gives

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}.$$

This proves the Fuchs-van de Graaf inequalities.

Why the proof is conceptually important

The proof says that the quantum theorem is not a mysterious algebraic accident. It is the classical relationship between total variation distance and Bhattacharyya coefficient, lifted to quantum theory through optimal measurements.

Trace distance appears because we maximize classical distinguishability over measurements. Fidelity appears because we minimize classical overlap over measurements. The inequalities are true classically for every measurement outcome distribution, and the quantum theorem follows by choosing the right measurements at the right steps.

This is exactly why the theorem is useful. It lets us translate between two languages. Trace distance is the language of operational distinguishability. Fidelity is the language of overlap, purification, and geometry.

Example: identical states

If

$$\rho = \sigma,$$

then

$$D(\rho, \sigma) = 0$$

and

$$F(\rho, \sigma) = 1.$$

The inequalities become

$$1 - 1 \leq 0 \leq \sqrt{1 - 1^2},$$

or

$$0 \leq 0 \leq 0.$$

Both bounds are tight. Operationally, identical states cannot be distinguished at all. Geometrically, they have perfect fidelity.

Example: orthogonal states

Let

$$\rho = |0\rangle\langle 0|, \qquad \sigma = |1\rangle\langle 1|.$$

Then

$$D(\rho, \sigma) = 1,$$

because the two states can be perfectly distinguished by measuring in the computational basis. Also,

$$F(\rho, \sigma) = |\langle 0|1\rangle| = 0.$$

The inequalities become

$$1 - 0 \leq 1 \leq \sqrt{1 - 0^2},$$

or

$$1 \leq 1 \leq 1.$$

Again both bounds are tight. Orthogonality is the extreme case where geometric non-overlap and operational distinguishability coincide perfectly.

Example: two nonorthogonal pure states

Let

$$\rho = |\psi\rangle\langle\psi|, \qquad \sigma = |\phi\rangle\langle\phi|.$$

For pure states,

$$F(\rho, \sigma) = |\langle\psi|\phi\rangle|.$$

A direct calculation gives

$$D(\rho, \sigma) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}.$$

Therefore the upper Fuchs-van de Graaf bound is saturated:

$$D(\rho,\sigma) = \sqrt{1 - F(\rho,\sigma)^2}.$$

For example, take

$$|\psi\rangle = |0\rangle, \qquad |\phi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Then

$$F = \frac{1}{\sqrt{2}}, \qquad D = \sqrt{1 - \frac{1}{2}} = \frac{1}{\sqrt{2}}.$$

The lower bound says

$$1 - \frac{1}{\sqrt{2}} \leq \frac{1}{\sqrt{2}},$$

which is true but not tight. The upper bound is exact.

Operationally, this says that the distinguishability of two pure states is completely determined by their Hilbert-space angle.

Example: a pure state and the maximally mixed qubit

Let

$$\rho = |0\rangle\langle 0|, \qquad \sigma = \frac{I}{2}.$$

The trace distance is

$$D(\rho,\sigma) = \frac{1}{2}\left\| |0\rangle\langle 0| - \frac{I}{2} \right\|_1.$$

In the computational basis,

$$|0\rangle\langle 0| - \frac{I}{2} = \begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix}.$$

The trace norm is 1, so

$$D(\rho, \sigma) = \frac{1}{2}.$$

The fidelity is

$$F(\rho, \sigma) = \sqrt{\langle 0|\frac{I}{2}|0\rangle} = \frac{1}{\sqrt{2}}.$$

The inequalities say

$$1 - \frac{1}{\sqrt{2}} \leq \frac{1}{2} \leq \sqrt{1 - \frac{1}{2}}.$$

Numerically,

$$0.2929 \leq 0.5 \leq 0.7071.$$

This example shows that the inequalities are often not tight. They are conversion bounds, not exact formulas in general.

Example: commuting mixed states

Suppose

$$\rho = \begin{pmatrix} 0.9 & 0 \\ 0 & 0.1 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}.$$

These states commute, so the problem reduces to the classical distributions

$$p = (0.9, 0.1), \qquad q = (0.5, 0.5).$$

The trace distance is

$$D(\rho,\sigma)=\frac{1}{2}(|0.9-0.5|+|0.1-0.5|)=0.4.$$

The fidelity is

$$F(\rho,\sigma)=\sqrt{0.9\cdot 0.5}+\sqrt{0.1\cdot 0.5}\approx 0.8944.$$

The inequalities become

$$1-0.8944\le 0.4\le\sqrt{1-0.8944^2}.$$

That is

$$0.1056\le 0.4\le 0.4472.$$

The states are fairly close in fidelity, but still moderately distinguishable because the classical probabilities differ appreciably.

How to use the theorem in estimates

The inequalities are most useful when one distance is easy to bound and the other is operationally needed.

If a proof gives a trace-distance bound

$$D(\rho,\sigma)\le\varepsilon,$$

then the theorem gives

$$F(\rho,\sigma)\ge 1-\varepsilon.$$

So operational indistinguishability implies high geometric overlap.

If a proof gives a fidelity bound

$$F(\rho,\sigma)\ge 1-\varepsilon,$$

then

$$D(\rho,\sigma) \le \sqrt{1-(1-\varepsilon)^2} = \sqrt{2\varepsilon-\varepsilon^2}.$$

For small ε, this is approximately

$$D(\rho,\sigma) \lesssim \sqrt{2\varepsilon}.$$

This square-root loss is common in quantum information estimates. A very high fidelity guarantee converts into a trace-distance guarantee, but the parameter becomes square-root weaker.

Conversely, if

$$D(\rho,\sigma) \le \delta,$$

then the Helstrom theorem says that for equal priors,

$$P_{\text{succ}}^{\text{opt}} \le \frac{1}{2}(1+\delta).$$

So no measurement can distinguish the states with advantage more than δ/2 above random guessing.

Operational interpretation in cryptography and error correction

In cryptography, trace distance is often the security metric because it directly controls distinguishing advantage. If an adversary's real state and ideal state are close in trace distance, then no measurement can reliably tell whether the adversary is in the real or ideal experiment.

Fidelity is often easier to work with geometrically because it behaves naturally with purifications and Uhlmann's theorem. The Fuchs-van de Graaf inequalities allow one to prove security or correctness in the fidelity language and then translate the result into trace-distance language.

In quantum error correction, one may prove that the recovered state has high fidelity with the original state. The inequalities then imply that the recovered state is also close in trace distance, meaning that all subsequent measurements have nearly the same outcome statistics.

Thus the theorem is a bridge between two kinds of guarantees. Fidelity says the states are geometrically close. Trace distance says the states are operationally hard to distinguish.

Common mistakes

A common mistake is to mix fidelity conventions. If fidelity means

$$F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1,$$

then the upper bound is

$$D(\rho,\sigma) \le \sqrt{1 - F(\rho,\sigma)^2}.$$

If fidelity means the squared quantity

$$F_{\mathrm{sq}}(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2,$$

then the upper bound is

$$D(\rho,\sigma) \le \sqrt{1 - F_{\mathrm{sq}}(\rho,\sigma)}.$$

A second mistake is to think that the inequalities give an exact conversion. They do not. They give upper and lower bounds. Exact equality holds in important special cases, such as identical states, orthogonal states, and the upper bound for pairs of pure states, but not in general.

A third mistake is to forget the factor 1/2 in trace distance. The trace distance between states is

$$D(\rho,\sigma) = \frac{1}{2}\|\rho - \sigma\|_1,$$

not \|ρ-σ\|₁. Without the factor 1/2, the range would be [0,2] instead of [0,1].

A fourth mistake is to interpret high fidelity as meaning that every matrix entry is close. Fidelity is basis-independent and geometric. Trace distance is also basis-independent but operational. Neither is a statement about entrywise closeness in a particular basis.

Final mental image

The Fuchs-van de Graaf inequalities say that the two most important notions of closeness between quantum states are quantitatively linked:

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}.$$

Trace distance is the distance seen by the best measurement. Fidelity is the best overlap seen by purifications. One is operational; the other is geometric. The theorem says that if two states are close in one sense, they are necessarily close in the other sense, with explicit conversion formulas.

In one sentence:

> geometric overlap controls operational distinguishability, and operational indisti

This is why the theorem appears everywhere in quantum information theory, from state discrimination and cryptography to error correction, channel approximation, and continuity bounds.

References

Fuchs, Christopher A., and Jeroen van de Graaf. "Cryptographic Distinguishability Measures for Quantum-Mechanical States." IEEE Transactions on Information Theory 45, no. 4 (1999): 1216-1227. DOI: 10.1109/18.761271. Also available as arXiv:quant-ph/9712042.

Fuchs, Christopher A., and Carlton M. Caves. "Mathematical Techniques for Quantum Communication Theory." Open Systems & Information Dynamics 3 (1995): 345-356.

Nielsen, Michael A., and Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 10th anniversary edition, 2010.

Watrous, John. The Theory of Quantum Information. Cambridge University Press, 2018.

Wilde, Mark M. Quantum Information Theory. Cambridge University Press, 2nd edition, 2017.

Document information

Fuchs-van de Graaf Inequalities

Project	[QIT 002] State Distinguishability and Measurement Theorems
Document	Primary document
Author	mujirin
Verifier	Not verified
Downloaded	July 03, 2026 20:23 KST
Status	Working
Document link	https://theorytrace.com/projects/state-distinguishability-and-measurement-theorems/documents/untitled-document-9793ca/