

# Quantum Chernoff Bound

## Formal statement

Let  $\rho$  and  $\sigma$  be density operators on a finite-dimensional Hilbert space  $\mathcal{H}$ . We consider the symmetric binary hypothesis-testing problem

$$H_0 : \text{the state is } \rho, \quad H_1 : \text{the state is } \sigma.$$

For  $n$  independent copies, the two possible states are

$$\rho_n = \rho^{\otimes n}, \quad \sigma_n = \sigma^{\otimes n}.$$

A binary quantum test is an operator  $0 \leq T_n \leq I$ . We interpret  $T_n$  as the decision "accept  $H_0$ ," namely decide that the state is  $\rho^{\otimes n}$ . The two errors are

$$\alpha_n(T_n) = \text{Tr}[(I - T_n)\rho^{\otimes n}]$$

and

$$\beta_n(T_n) = \text{Tr}[T_n\sigma^{\otimes n}].$$

In the symmetric Bayesian setting, the prior probabilities are fixed numbers

$$\pi_0 > 0, \quad \pi_1 > 0, \quad \pi_0 + \pi_1 = 1.$$

The average error probability of the test  $T_n$  is

$$P_{e,n}(T_n) = \pi_0 \alpha_n(T_n) + \pi_1 \beta_n(T_n).$$

The optimal symmetric error probability is

$$P_{e,n}^{\text{opt}} = \min_{0 \leq T_n \leq I} \{ \pi_0 \text{Tr}[(I - T_n)\rho^{\otimes n}] + \pi_1 \text{Tr}[T_n\sigma^{\otimes n}] \}.$$

The quantum Chernoff bound says that

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log P_{e,n}^{\text{opt}} = \xi_{\text{QCB}}(\rho, \sigma)$$

where

$$\xi_{\text{QCB}}(\rho, \sigma) = -\log \inf_{0 \leq s \leq 1} \text{Tr}(\rho^s \sigma^{1-s}).$$

The quantity

$$Q(\rho, \sigma) = \inf_{0 \leq s \leq 1} \text{Tr}(\rho^s \sigma^{1-s})$$

is the quantum Chernoff coefficient, and

$$\xi_{\text{QCB}}(\rho, \sigma) = -\log Q(\rho, \sigma)$$

is the quantum Chernoff distance or quantum Chernoff exponent.

The exponent is independent of the fixed nonzero priors  $\pi_0, \pi_1$ . Priors change the finite- $n$  prefactor, but not the asymptotic exponential rate. If logarithms are base two, the exponent is measured in bits per copy. If natural logarithms are used, it is measured in nats per copy.

## Meaning of the theorem

Quantum Stein's lemma and the quantum Chernoff bound answer different hypothesis-testing questions.

Quantum Stein's lemma is asymmetric. It constrains the type-I error and asks how fast the type-II error can decay. Its exponent is the quantum relative entropy

$$D(\rho \parallel \sigma).$$

The quantum Chernoff bound is symmetric. It treats the two hypotheses together through the average Bayesian error

$$P_{e,n} = \pi_0 \alpha_n + \pi_1 \beta_n.$$

Its exponent is not  $D(\rho\|\sigma)$ . It is

$$\xi_{\text{QCB}}(\rho, \sigma) = -\log \inf_{0 \leq s \leq 1} \text{Tr}(\rho^s \sigma^{1-s}).$$

The mental image is this. In Stein testing, one hypothesis is protected: we insist that the probability of rejecting  $\rho$  stays small, and then we punish false acceptance of  $\rho$  under  $\sigma$ . In Chernoff testing, neither hypothesis is protected in that asymmetric way. We ask for the fastest possible exponential decay of the total probability of making either mistake.

The answer is a balanced overlap between  $\rho$  and  $\sigma$ . The parameter  $s \in [0, 1]$  continuously tilts the comparison between the two states. The minimizing value of  $s$  finds the best exponential tradeoff between the two possible errors.

## One-copy Helstrom form

For fixed  $n$ , the optimal Bayesian test is the Helstrom measurement. Define

$$\Delta_n = \pi_0 \rho^{\otimes n} - \pi_1 \sigma^{\otimes n}.$$

The optimal test accepts  $H_0$  on the positive spectral subspace of  $\Delta_n$ . The optimal error probability is

$$P_{e,n}^{\text{opt}} = \frac{1}{2} (1 - \|\pi_0 \rho^{\otimes n} - \pi_1 \sigma^{\otimes n}\|_1).$$

This formula is exact, but it is usually hard to evaluate for large  $n$ . The quantum Chernoff bound gives the asymptotic exponential rate of this exact Helstrom error.

Thus the theorem is not saying that the Chernoff expression is the exact finite-copy error. It says that, exponentially,

$$P_{e,n}^{\text{opt}} \approx \exp[-n \xi_{\text{QCB}}(\rho, \sigma)].$$

More precisely,

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log P_{e,n}^{\text{opt}} = \xi_{\text{QCB}}(\rho, \sigma).$$

## Achievability: why this exponent can be reached

The achievability direction says that there exist tests whose average error probability decays at least as fast as

$$\exp[-n\xi_{\text{QCB}}(\rho, \sigma)].$$

The key inequality is an operator version of the classical Chernoff bound. For positive operators  $A, B$  and  $0 \leq s \leq 1$ , one has

$$\frac{1}{2} \text{Tr}(A + B - |A - B|) \leq \text{Tr}(A^s B^{1-s}).$$

Now set

$$A = \pi_0 \rho^{\otimes n}, \quad B = \pi_1 \sigma^{\otimes n}.$$

The left-hand side is exactly the optimal Bayesian error probability:

$$P_{e,n}^{\text{opt}} = \frac{1}{2} \text{Tr}(A + B - |A - B|).$$

Therefore

$$P_{e,n}^{\text{opt}} \leq \text{Tr} [(\pi_0 \rho^{\otimes n})^s (\pi_1 \sigma^{\otimes n})^{1-s}].$$

Using tensor-product multiplicativity,

$$(\rho^{\otimes n})^s = (\rho^s)^{\otimes n}$$

and

$$(\sigma^{\otimes n})^{1-s} = (\sigma^{1-s})^{\otimes n}.$$

Hence

$$\begin{aligned} P_{e,n}^{\text{opt}} &\leq \pi_0^s \pi_1^{1-s} \text{Tr} [(\rho^s \sigma^{1-s})^{\otimes n}] \\ &= \pi_0^s \pi_1^{1-s} [\text{Tr}(\rho^s \sigma^{1-s})]^n. \end{aligned}$$

This is true for every  $s \in [0,1]$ . Therefore

$$P_{e,n}^{\text{opt}} \leq \max\{\pi_0, \pi_1\} \left[ \inf_{0 \leq s \leq 1} \text{Tr}(\rho^s \sigma^{1-s}) \right]^n,$$

up to a constant factor independent of  $n$ . Taking logarithms, dividing by  $n$ , and sending  $n \rightarrow \infty$ , the prior-dependent constant disappears. We obtain

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log P_{e,n}^{\text{opt}} \geq -\log \inf_{0 \leq s \leq 1} \text{Tr}(\rho^s \sigma^{1-s}).$$

This proves that the Chernoff exponent is achievable.

## Converse: why no larger exponent is possible

The converse direction says that no measurement strategy can make the symmetric Bayesian error decay faster than the Chernoff exponent.

This is the technically deeper half of the theorem. The proof is not just a direct application of the classical Chernoff bound, because  $\rho$  and  $\sigma$  may not commute. There may be no basis in which the two states are simultaneously classical probability distributions.

The key idea of the Nussbaum-Szkoła converse is to associate to  $\rho$  and  $\sigma$  a pair of classical distributions that encode the spectral overlap between the two density operators. Let

$$\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$$

and

$$\sigma = \sum_j \mu_j |f_j\rangle\langle f_j|.$$

Define classical distributions on pairs  $(i,j)$  by

$$P(i, j) = \lambda_i |\langle e_i | f_j \rangle|^2$$

and

$$Q(i, j) = \mu_j |\langle e_i | f_j \rangle|^2.$$

These distributions satisfy

$$\sum_{i,j} P(i, j)^s Q(i, j)^{1-s} = \text{Tr}(\rho^s \sigma^{1-s}).$$

Thus their classical Chernoff coefficient is exactly the quantum Chernoff coefficient. The classical Chernoff converse says that no classical test between  $P^{\otimes n}$  and  $Q^{\otimes n}$  can have an error exponent larger than

$$-\log \inf_{0 \leq s \leq 1} \sum_{i,j} P(i, j)^s Q(i, j)^{1-s}.$$

The hard part is to show that a hypothetical quantum test with a better exponent would imply a classical test for these Nussbaum-Szkoła distributions with a better-than-classical Chernoff exponent, which is impossible. This proves

$$\limsup_{n \rightarrow \infty} -\frac{1}{n} \log P_{e,n}^{\text{opt}} \leq \xi_{\text{QCB}}(\rho, \sigma).$$

Together with achievability, this gives

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log P_{e,n}^{\text{opt}} = \xi_{\text{QCB}}(\rho, \sigma).$$

So the theorem is a complete asymptotic characterization of symmetric binary quantum hypothesis testing.

## Classical commuting case

Suppose  $\rho$  and  $\sigma$  commute. Then they are diagonal in the same basis:

$$\rho = \sum_x P(x)|x\rangle\langle x|, \quad \sigma = \sum_x Q(x)|x\rangle\langle x|.$$

Then

$$\text{Tr}(\rho^s \sigma^{1-s}) = \sum_x P(x)^s Q(x)^{1-s}.$$

Therefore

$$\xi_{\text{QCB}}(\rho, \sigma) = -\log \inf_{0 \leq s \leq 1} \sum_x P(x)^s Q(x)^{1-s}.$$

This is exactly the classical Chernoff information. In this case, the optimal measurement is simply the common eigenbasis measurement, and the quantum theorem reduces to the classical theorem.

This commuting case is important because it explains the formula. The expression

$$\sum_x P(x)^s Q(x)^{1-s}$$

is a tilted overlap between the two distributions. The quantum expression

$$\text{Tr}(\rho^s \sigma^{1-s})$$

is the noncommutative analogue of that tilted overlap.

### Example: identical states

If

$$\rho = \sigma,$$

then

$$\text{Tr}(\rho^s \sigma^{1-s}) = \text{Tr} \rho = 1.$$

Thus

$$\xi_{\text{QCB}}(\rho, \rho) = -\log 1 = 0.$$

This is correct. If the two hypotheses produce exactly the same quantum state, then no measurement on any number of copies can distinguish them. The optimal error probability does not decay exponentially. It stays at the smaller prior probability if one always guesses the more likely hypothesis.

### Example: orthogonal states

Suppose

$$\rho\sigma = 0,$$

meaning their supports are orthogonal. Then for  $0 < s < 1$ ,

$$\text{Tr}(\rho^s \sigma^{1-s}) = 0.$$

Therefore

$$\xi_{\text{QCB}}(\rho, \sigma) = +\infty.$$

This means the error probability can become zero after finitely many copies. In fact, it is already zero with one copy if the supports are orthogonal. A projective measurement onto the support of  $\rho$  versus the support of  $\sigma$  distinguishes the states perfectly.

### Example: two nonorthogonal pure states

Let

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

For  $0 < s < 1$ , pure-state projectors satisfy

$$\rho^s = \rho, \quad \sigma^{1-s} = \sigma.$$

Hence

$$\text{Tr}(\rho^s \sigma^{1-s}) = \text{Tr}(|\psi\rangle\langle\psi|\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|^2.$$

Therefore

$$\xi_{\text{QCB}}(\rho, \sigma) = -\log |\langle\psi|\phi\rangle|^2.$$

For example, take

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

Then

$$|\langle 0|+\rangle|^2 = \frac{1}{2},$$

so with base-two logarithms,

$$\xi_{\text{QCB}} = 1.$$

Thus the optimal symmetric error probability decays like

$$P_{e,n}^{\text{opt}} \asymp 2^{-n}$$

up to subexponential factors.

This example is also a good way to distinguish the Chernoff bound from Stein's lemma. For the same pair  $|0\rangle$  and  $|+\rangle$ , the Stein exponent  $D(|0\rangle\langle 0| \parallel |+\rangle\langle +|)$  is infinite because the support condition fails. But the symmetric Chernoff exponent is finite because both errors are treated together.

## Example: pure state versus maximally mixed qubit

Let

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

For  $0 < s \leq 1$ ,

$$\rho^s = \rho,$$

and

$$\sigma^{1-s} = \left(\frac{I}{2}\right)^{1-s} = 2^{s-1}I.$$

Therefore

$$\text{Tr}(\rho^s \sigma^{1-s}) = 2^{s-1}.$$

The minimum over  $0 \leq s \leq 1$  is  $1/2$ , attained at  $s=0$  by continuity. Hence

$$\xi_{\text{QCB}} = \log_2 2 = 1$$

bit per copy.

Indeed, for  $n$  copies, the test

$$T_n = |0^n\rangle\langle 0^n|$$

accepts  $\rho^{\otimes n}$  perfectly and accepts  $\sigma^{\otimes n} = I/2^n$  with probability  $2^{-n}$ . With equal priors, the average error is

$$P_{e,n} = \frac{1}{2} \cdot 2^{-n},$$

which has exponent one bit per copy.

### **Example: a commuting binary mixed-state pair**

Let

$$\rho = \begin{pmatrix} 0.8 & 0 \\ 0 & 0.2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 0.3 & 0 \\ 0 & 0.7 \end{pmatrix}.$$

These states commute, so the quantum Chernoff coefficient is classical:

$$Q_s = 0.8^s 0.3^{1-s} + 0.2^s 0.7^{1-s}.$$

Numerically, the minimum occurs near

$$s \approx 0.489,$$

where

$$Q_s \approx 0.864.$$

Thus

$$\xi_{\text{QCB}} = -\log_2(0.864) \approx 0.211$$

bits per copy.

This exponent is smaller than either distribution's one-sided relative entropy in general, because symmetric testing must balance the two possible errors rather than protecting one hypothesis and optimizing the other.

## Relation to Rényi overlaps

The expression

$$\text{Tr}(\rho^s \sigma^{1-s})$$

is closely related to Petz-type quantum Rényi divergences. For  $0 < s < 1$ , it is a noncommutative analogue of the classical tilted overlap

$$\sum_x P(x)^s Q(x)^{1-s}.$$

The Chernoff distance chooses the tilt that makes this overlap as small as possible:

$$\xi_{\text{QCB}} = -\log \min_s Q_s.$$

So the Chernoff exponent is not the overlap at a fixed value of  $s$ . It is the best tilted overlap across all  $s \in [0, 1]$ . The special value  $s = 1/2$  gives

$$\text{Tr}(\sqrt{\rho}\sqrt{\sigma}),$$

which is sometimes useful, but it is not generally the minimizing value and should not be confused with the full Chernoff coefficient.

## Relation to fidelity

The quantum Chernoff coefficient and fidelity are related but different. Fidelity is

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

The Chernoff coefficient is

$$Q(\rho, \sigma) = \inf_{0 \leq s \leq 1} \text{Tr}(\rho^s \sigma^{1-s}).$$

For pure states, they are directly related:

$$Q(\rho, \sigma) = F(\rho, \sigma)^2.$$

For general mixed noncommuting states, they are not the same. Fidelity measures geometric closeness, while the Chernoff coefficient gives the optimal symmetric asymptotic discrimination exponent. The two quantities are both measures of state overlap, but they arise from different operational problems.

## Collective measurements

The theorem optimizes over all quantum tests  $0 \leq T_n \leq I$  on the full tensor-product space  $\mathcal{H}^{\otimes n}$ . Therefore the optimal test may be collective across the  $n$  copies.

In commuting cases, measuring each copy in the common eigenbasis reduces the problem to classical hypothesis testing, and no genuinely collective quantum measurement is needed. For pure-state pairs, relatively simple strategies can achieve the exponent. But for general noncommuting mixed states, the theorem allows collective measurements, and the proof of the optimal exponent is genuinely quantum.

This is one reason the theorem is important. It is not only a statement about a particular measurement. It is a statement about the best possible measurement permitted by quantum mechanics in the many-copy limit.

## Comparison with Stein and Hoeffding exponents

Quantum Stein's lemma says that, under a fixed type-I constraint,

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \beta_{n,\varepsilon} = D(\rho \parallel \sigma).$$

The quantum Chernoff bound says that, when both errors are combined into a symmetric Bayesian error,

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log P_{e,n}^{\text{opt}} = \xi_{\text{QCB}}(\rho, \sigma).$$

Between these two regimes lies Hoeffding-type hypothesis testing, where one fixes an exponential decay rate for one error and optimizes the exponent of the other. These results form a hierarchy of asymptotic hypothesis-testing theorems. Stein corresponds to asymmetric constrained testing. Chernoff corresponds to symmetric Bayesian testing. Hoeffding describes the tradeoff curve between the two.

## How to use the theorem

To apply the quantum Chernoff bound, compute

$$Q_s = \text{Tr}(\rho^s \sigma^{1-s})$$

for  $0 \leq s \leq 1$ . Then minimize over  $s$ :

$$Q = \inf_{0 \leq s \leq 1} Q_s.$$

The optimal symmetric error exponent is

$$\xi_{\text{QCB}} = -\log Q.$$

For large  $n$ , the optimal error probability behaves exponentially as

$$P_{e,n}^{\text{opt}} \approx e^{-n\xi_{\text{QCB}}}$$

if natural logarithms are used, or

$$P_{e,n}^{\text{opt}} \approx 2^{-n\xi_{\text{QCB}}}$$

if base-two logarithms are used.

If  $\rho$  and  $\sigma$  commute, diagonalize them together and reduce the computation to the classical Chernoff formula. If one or both states are pure, the expression often simplifies dramatically. If the states are general mixed noncommuting states, one usually computes  $Q_s$  numerically by diagonalizing  $\rho$  and  $\sigma$  and minimizing the scalar function of  $s$ .

## Common mistakes

A common mistake is to confuse the quantum Chernoff exponent with quantum relative entropy. Relative entropy appears in asymmetric Stein testing. The Chernoff distance appears in symmetric Bayesian testing.

A second mistake is to forget the minimization over  $s$ . The exponent is not generally

$$-\log \text{Tr}(\sqrt{\rho}\sqrt{\sigma}).$$

That expression corresponds to  $s=1/2$ , which is not always optimal.

A third mistake is to think that the Chernoff bound is an exact finite-copy formula. It is an asymptotic exponent. The exact finite-copy optimal error is given by the Helstrom trace-norm formula applied to  $\rho^{\otimes n}$  and  $\sigma^{\otimes n}$ .

A fourth mistake is to think that the prior probabilities determine the exponent. Fixed nonzero priors affect finite-copy constants, but they vanish after taking

$$-\frac{1}{n} \log(\cdot)$$

and sending  $n \rightarrow \infty$ .

A fifth mistake is to assume product measurements are always optimal. The theorem optimizes over all collective measurements on  $n$  copies. In genuinely noncommuting mixed-state problems, collective measurements may be needed to achieve the optimal exponent.

## Final mental image

The quantum Chernoff bound says that if we must distinguish

$$\rho^{\otimes n} \quad \text{from} \quad \sigma^{\otimes n}$$

and both mistakes are counted in the Bayesian average error, then the best possible error probability decays exponentially at rate

$$\xi_{\text{QCB}}(\rho, \sigma) = -\log \inf_{0 \leq s \leq 1} \text{Tr}(\rho^s \sigma^{1-s}).$$

The quantity inside the logarithm is a tilted quantum overlap. The minimization over  $s$  finds the most discriminating tilt. The logarithm converts this overlap into an exponential distinguishability rate.

In one sentence:

the quantum Chernoff distance is the optimal symmetric many-copy distinguish:

That is why the theorem is the symmetric counterpart of quantum Stein's lemma and one of the central asymptotic laws of quantum hypothesis testing.

## References

Audenaert, K. M. R., J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acín, and F. Verstraete. "Discriminating States: The Quantum Chernoff Bound." *Physical Review Letters* 98, no. 16 (2007): 160501. DOI: 10.1103/PhysRevLett.98.160501.

Nussbaum, Michael, and Arleta Szkoła. "The Chernoff Lower Bound for Symmetric Quantum Hypothesis Testing." *The Annals of Statistics* 37, no. 2 (2009): 1040-1057. DOI: 10.1214/08-AOS593.

Audenaert, K. M. R., Michael Nussbaum, Arleta Szkoła, and Frank Verstraete. "Asymptotic Error Rates in Quantum Hypothesis Testing." *Communications in Mathematical Physics* 279 (2008): 251-283. DOI: 10.1007/s00220-008-0417-5.

Chernoff, Herman. "A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the Sum of Observations." *The Annals of Mathematical Statistics* 23, no. 4 (1952): 493-507.

Helstrom, Carl W. *Quantum Detection and Estimation Theory*. Academic Press, 1976.

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

Hayashi, Masahito. *Quantum Information Theory: Mathematical Foundation*. Springer, 2017.

---

# Document information

## Quantum Chernoff Bound

---

<b>Project</b>	[QIT 002] State Distinguishability and Measurement Theorems
<b>Document</b>	Primary document
<b>Author</b>	mujirin
<b>Verifier</b>	Not verified
<b>Downloaded</b>	July 04, 2026 22:30 KST
<b>Status</b>	Working
<b>Document link</b>	<a href="https://www.theorytrace.com/projects/state-distinguishability-and-measurement-theorems/documents/untitled-document-6ff18b/">https://www.theorytrace.com/projects/state-distinguishability-and-measurement-theorems/documents/untitled-document-6ff18b/</a>