

Uncertainty Principle

Alexander Trembl

June 20, 2024

Abstract

This is a formal proof of the uncertainty principle known from quantum mechanics. It is based upon work on complex vector spaces contained in the QHLProver session[1]. The formalization follows the proof outlined in the book "Quantum computation and quantum information" by Nielsen and Chuang[2].

Contents

1	Setup	2
2	Auxiliary Lemmas	2
3	Main Proof	5

```

theory Uncertainty-Principle
  imports QHLProver.Complex-Matrix
begin

```

1 Setup

```

abbreviation bra-ket ( $\langle\langle\cdot|\cdot\rangle\rangle$ )
  where  $\langle u|v\rangle \equiv \text{inner-prod } u \ v$ 

```

Fix an n-dimensional normalized quantum state ψ .

```

locale quantum-state =
  fixes  $n:: \text{nat}$ 
  and  $\psi:: \text{complex Matrix.vec}$ 
  assumes  $\text{dim}[simp]: \psi \in \text{carrier-vec } n$ 
  and  $\text{normalized}[simp]: \langle\psi|\psi\rangle = 1$ 

```

```

begin

```

Observables on ψ are hermitian matrices of appropriate dimensions.

```

abbreviation observable::  $\text{complex Matrix.mat} \Rightarrow \text{bool}$  where
  observable  $A \equiv A \in \text{carrier-mat } n \ n \wedge \text{hermitian } A$ 

```

The mean value of an observable A is defined as $\langle\psi|A|\psi\rangle$. It is useful to have a scalar matrix of appropriate dimension containing this value. On paper, this is usually implicit.

```

abbreviation mean-mat ::  $\text{complex Matrix.mat} \Rightarrow \text{complex Matrix.mat}$  ( $\langle\langle\cdot\rangle\rangle$ )
  where  $\langle\langle A\rangle\rangle \equiv \langle\psi| A *_v \psi\rangle \cdot_m 1_m \ n$ 

```

The standard deviation of an observable $A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2}$. Since the standard deviation is real (see lemma `std-dev-real`), we can define it as being of type `real` using `norm`. This simultaneously restricts it to positive values. (powers of two are expanded for simplicity)

```

abbreviation std-dev ::  $\text{complex Matrix.mat} \Rightarrow \text{real}$  ( $\Delta$ )
  where  $\Delta \ A \equiv \text{norm } (\text{csqrt } (\langle\psi| (A * A *_v \psi)\rangle - \langle\psi| A *_v \psi\rangle * \langle\psi| A *_v \psi\rangle))$ 

```

```

end

```

```

abbreviation commutator ::  $\text{complex Matrix.mat} \Rightarrow \text{complex Matrix.mat} \Rightarrow \text{complex Matrix.mat}$  ( $\llbracket\cdot, \cdot\rrbracket$ )
  where commutator  $A \ B \equiv (A * B - B * A)$ 

```

```

abbreviation anticommutator ::  $\text{complex Matrix.mat} \Rightarrow \text{complex Matrix.mat} \Rightarrow \text{complex Matrix.mat}$  ( $\{\!\{ \cdot, \cdot \}\!\}$ )
  where anticommutator  $A \ B \equiv (A * B + B * A)$ 

```

2 Auxiliary Lemmas

```

lemma inner-prod-distrib-add-mat:

```

fixes $u\ v :: \text{complex vec}$
assumes
 $u \in \text{carrier-vec } n$
 $v \in \text{carrier-vec } m$
 $A \in \text{carrier-mat } n\ m$
 $B \in \text{carrier-mat } n\ m$
shows $\langle u | (A + B) *_v v \rangle = \langle u | A *_v v \rangle + \langle u | B *_v v \rangle$
apply (*subst add-mult-distrib-mat-vec*)
using *assms* **by** (*auto intro: inner-prod-distrib-right*)

lemma *inner-prod-distrib-minus-mat*:
fixes $u\ v :: \text{complex vec}$
assumes
 $u \in \text{carrier-vec } n$
 $v \in \text{carrier-vec } m$
 $A \in \text{carrier-mat } n\ m$
 $B \in \text{carrier-mat } n\ m$
shows $\langle u | (A - B) *_v v \rangle = \langle u | A *_v v \rangle - \langle u | B *_v v \rangle$
apply (*subst minus-mult-distrib-mat-vec*)
using *assms* **by** (*auto intro: inner-prod-minus-distrib-right*)

Proving the usual Cauchy-Schwarz inequality using its formulation for complex vector spaces.

lemma *Cauchy-Schwarz*:
assumes $v \in \text{carrier-vec } n\ u \in \text{carrier-vec } n$
shows $\text{norm } (\langle u|v \rangle)^2 \leq \text{Re } (\langle u|u \rangle * \langle v|v \rangle)$
proof –
have $\text{norm } (\langle u|v \rangle)^2 \leq (\langle u|u \rangle * \langle v|v \rangle)$
using *assms*
by (*metis Cauchy-Schwarz-complex-vec complex-norm-square conjugate-complex-def inner-prod-swap*)
moreover **have** $(\langle u|u \rangle * \langle v|v \rangle) \in \mathbb{R}$
by (*simp add: complex-is-Real-iff*)
ultimately show *?thesis* **by** (*simp add: less-eq-complex-def*)
qed

context *quantum-state*
begin

Show that the the standard deviation yields a real value. This justifies our definition in terms of the norm.

lemma *std-dev-real*:
assumes *observable* A
shows $\text{csqrt } (\langle \psi | (A * A *_v \psi) \rangle - \langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle) \in \mathbb{R}$
proof (*subst csqrt-of-real-nonneg*)
— The term under the square root is real ...
have $(\langle \psi | A * A *_v \psi \rangle - \langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle) \in \mathbb{R}$
apply (*intro Reals-diff Reals-mult hermitian-inner-prod-real*)
using *assms* **by** (*auto simp: hermitian-def adjoint-mult*)

then show $Im (\langle \psi | A * A *_v \psi \rangle - \langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle) = 0$
using *complex-is-Real-iff* **by** *simp*
next
have $*:adjoint A = A$ **using** *assms hermitian-def* **by** *blast*
— ... and positive (Cauchy-Schwarz)
have $\langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle \leq \langle \psi | \psi \rangle * \langle \psi | A * A *_v \psi \rangle$
apply (*subst assoc-mult-mat-vec*) **prefer** 4
apply (*subst (2) adjoint-def-alter*) **prefer** 4
apply (*subst (2) adjoint-def-alter*) **prefer** 4
apply (*subst (1 2) **)
apply (*rule Cauchy-Schwarz-complex-vec[OF dim]*)
using *assms* **by** *auto*
then show $0 \leq Re (\langle \psi | A * A *_v \psi \rangle - \langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle)$
by (*simp add: less-eq-complex-def*)
— Thus the result of the complex square root is real
qed *simp*

This is an alternative way of formulating the standard deviation.

lemma *std-dev-alt:*

assumes *observable A*

shows $\Delta A = norm (csqrt (\langle \psi | (A - \langle A \rangle) * (A - \langle A \rangle) *_v \psi \rangle))$

proof —

— Expand the matrix term

have $(A - \langle A \rangle) * (A - \langle A \rangle) = (A + - \langle A \rangle) * (A + - \langle A \rangle)$

using *assms minus-add-uminus-mat* **by** *force*

also have $*: \dots = A * A + A * - \langle A \rangle + - \langle A \rangle * A + - \langle A \rangle * - \langle A \rangle$

apply (*mat-assoc n*)

using *assms* **by** *auto*

also have $\dots = A * A - \langle A \rangle * A - \langle A \rangle * A + \langle A \rangle * \langle A \rangle$

using *uminus-mult-right-mat* *assms* **by** *auto*

also have $\dots = A * A - \langle \psi | A *_v \psi \rangle \cdot_m A - \langle \psi | A *_v \psi \rangle \cdot_m A + \langle A \rangle * \langle A \rangle$

using *assms* **by** *auto*

finally have 1:

$\langle \psi | (A - \langle A \rangle) * (A - \langle A \rangle) *_v \psi \rangle =$

$\langle \psi | (A * A - \langle \psi | A *_v \psi \rangle \cdot_m A - \langle \psi | A *_v \psi \rangle \cdot_m A + \langle A \rangle * \langle A \rangle) *_v \psi \rangle$

by *simp*

— The mean is linear, so it distributes over the matrix term ...

have 2:

$\langle \psi | (A * A - \langle \psi | A *_v \psi \rangle \cdot_m A - \langle \psi | A *_v \psi \rangle \cdot_m A + \langle A \rangle * \langle A \rangle) *_v \psi \rangle =$

$\langle \psi | A * A *_v \psi \rangle - \langle \psi | \langle \psi | A *_v \psi \rangle \cdot_m A *_v \psi \rangle - \langle \psi | \langle \psi | A *_v \psi \rangle \cdot_m A *_v \psi \rangle +$

$\langle \psi | \langle A \rangle * \langle A \rangle *_v \psi \rangle$

apply (*subst inner-prod-distrib-add-mat*) **prefer** 5

apply (*subst inner-prod-distrib-minus-mat*) **prefer** 5

apply (*subst inner-prod-distrib-minus-mat*)

using *assms* **by** *auto*

— ... and a scaling factor can be pulled outside

have 3: $\langle \psi | \langle \psi | A *_v \psi \rangle \cdot_m A *_v \psi \rangle = \langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle$

by (metis assms dim inner-prod-smult-left mult-mat-vec-carrier smult-mat-mult-mat-vec-assoc)

— This also means that this is just the mean squared
have $\langle \psi | \langle A \rangle * \langle A \rangle *_v \psi \rangle = \langle \psi | A *_v \psi \rangle * \langle \psi | \langle A \rangle *_v \psi \rangle$
apply (subst mult-smult-assoc-mat) **prefer** 3
apply (subst smult-mat-mult-mat-vec-assoc) **prefer** 3
apply (subst inner-prod-smult-left)
using assms **by** (auto intro!: mult-mat-vec-carrier)
also have ... = $\langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle$
apply (subst smult-mat-mult-mat-vec-assoc) **prefer** 3
apply (subst inner-prod-smult-left[where n = n])
using assms **by** auto
finally have 4: $\langle \psi | \langle A \rangle * \langle A \rangle *_v \psi \rangle = \langle \psi | A *_v \psi \rangle * \langle \psi | A *_v \psi \rangle$ **by** simp

— With these four equivalences we can rewrite the standard deviation as specified
show ?thesis

by (simp add: 1 2 3 4)

qed

3 Main Proof

Note that when swapping two observables inside an inner product, it is the same as conjugating the result.

lemma cnj-observables:

assumes observable A observable B

shows cnj $\langle \psi | (A * B) *_v \psi \rangle = \langle \psi | (B * A) *_v \psi \rangle$

proof —

have cnj (conjugate $\langle A * B *_v \psi | \psi \rangle$) = $\langle \text{adjoint } (B * A) *_v \psi | \psi \rangle$

using assms **by** (metis (full-types) adjoint-mult complex-cnj-cnj conjugate-complex-def hermitian-def)

then show ?thesis

using assms **by** (metis adjoint-def-alter dim inner-prod-swap mult-carrier-mat mult-mat-vec-carrier)

qed

With the above lemma we can make two observations about the behaviour of the commutator/ anticommutator inside an inner product.

lemma commutator-im:

assumes observable A observable B

shows $\langle \psi | \llbracket A, B \rrbracket *_v \psi \rangle = 2 * i * \text{Im}(\langle \psi | A * B *_v \psi \rangle)$

proof —

have $\langle \psi | \llbracket A, B \rrbracket *_v \psi \rangle = \langle \psi | A * B *_v \psi \rangle - \langle \psi | B * A *_v \psi \rangle$

using assms **by** (auto intro!: inner-prod-distrib-minus-mat)

also have ... = $\langle \psi | A * B *_v \psi \rangle - \text{cnj } \langle \psi | A * B *_v \psi \rangle$

by (subst cnj-observables[OF assms], simp)

finally show ?thesis

using complex-diff-cnj **by** simp

qed

lemma anticommutator-re:
assumes *observable A observable B*
shows $\langle \psi | \{A, B\} *_v \psi \rangle = 2 * \text{Re}(\langle \psi | A * B *_v \psi \rangle)$
proof –
have $\langle \psi | \{A, B\} *_v \psi \rangle = \langle \psi | A * B *_v \psi \rangle + \langle \psi | B * A *_v \psi \rangle$
using *assms by (auto intro!: inner-prod-distrib-add-mat)*
also have ... = $\langle \psi | A * B *_v \psi \rangle + \text{cnj} \langle \psi | A * B *_v \psi \rangle$
by (*subst cnj-observables[OF assms], simp*)
finally show *?thesis*
using *complex-add-cnj by simp*
qed

This intermediate step already looks similar to the uncertainty principle. The LHS will play the role of the lower bound in the uncertainty principle. The RHS will turn into the standard deviation of our observables under a certain substitution.

lemma commutator-ineq:
assumes *observable A observable B*
shows $(\text{norm} \langle \psi | [A, B] *_v \psi \rangle)^2 \leq 4 * \text{Re}(\langle \psi | A * A *_v \psi \rangle * \langle \psi | B * B *_v \psi \rangle)$
proof –
– The inner product of our quantum state under A and B can be expressed in terms of its real and imaginary part
let *?x = Re(⟨ψ | A * B *_v ψ⟩)*
let *?y = Im(⟨ψ | A * B *_v ψ⟩)*

– These parts can be expressed using the commutator/anticommutator as shown above

have *im:* $(\text{norm} \langle \psi | [A, B] *_v \psi \rangle)^2 = 4 * ?y^2$
apply (*subst commutator-im[OF assms]*)
using *cmod-power2 by simp*

have *re:* $(\text{norm} \langle \psi | \{A, B\} *_v \psi \rangle)^2 = 4 * ?x^2$
apply (*subst anticommutator-re[OF assms]*)
using *cmod-power2 by simp*

– Meaning, the sum of the commutator terms gives us $2\langle \psi | AB | \psi \rangle$. Squared we get ...

from *im re have* $(\text{norm} \langle \psi | [A, B] *_v \psi \rangle)^2 + (\text{norm} \langle \psi | \{A, B\} *_v \psi \rangle)^2 = 4 * (?x^2 + ?y^2)$

by *simp*
also have ... = $4 * \text{norm}(\langle \psi | A * B *_v \psi \rangle)^2$
using *cmod-power2 by simp*
also have ... = $4 * \text{norm}(\langle A *_v \psi | B *_v \psi \rangle)^2$
apply (*subst assoc-mult-mat-vec*) **prefer** 4
apply (*subst adjoint-def-alter*)
using *assms hermitian-def by (auto, force)*
– Now we use the Cauchy-Schwarz inequality

also have ... $\leq 4 * Re (\langle A *_v \psi | A *_v \psi \rangle * \langle B *_v \psi | B *_v \psi \rangle)$
by (*smt (verit) assms Cauchy-Schwarz dim mult-mat-vec-carrier*)
 — Rewrite this term
also have ... $= 4 * Re (\langle \psi | A * A *_v \psi \rangle * \langle \psi | B * B *_v \psi \rangle)$
apply (*subst (1 2) assoc-mult-mat-vec*) **prefer** 7
apply (*subst (3 4) adjoint-def-alter*)
using *assms* **by** (*auto simp: hermitian-def*)
 — Dropping a positive term on the LHS does not affect the inequality
finally show *?thesis*
using *norm-ge-zero* **by** (*smt (verit, ccfv-threshold) zero-le-power2*)
qed

This is part of the substitution we need in the final proof. This lemma shows that the commutator simplifies nicely under that substitution.

lemma *commutator-sub-mean[simp]*:

assumes $A \in \text{carrier-mat } n \ n \ B \in \text{carrier-mat } n \ n$

shows $\llbracket A - \langle A \rangle, B - \langle B \rangle \rrbracket = \llbracket A, B \rrbracket$

proof —

— Simply expand everything. The unary minus signs are deliberate, because we want to have addition in the parentheses. Otherwise *mat-assoc* cannot remove the parentheses.

have $\llbracket A - \langle A \rangle, B - \langle B \rangle \rrbracket = A * B - \langle A \rangle * B - A * \langle B \rangle - \langle A \rangle * (- \langle B \rangle) - (B * A + (- (\langle B \rangle * A)) + (- (B * \langle A \rangle))) - \langle B \rangle * (- \langle A \rangle)$

apply (*mat-assoc n*)

using *assms* **by** *auto*

— Remove the last subtraction in the parentheses and unnecessary minus signs

also have ... $= A * B - \langle A \rangle * B - A * \langle B \rangle - (- (\langle A \rangle * \langle B \rangle)) - (B * A + (- (\langle B \rangle * A)) + (- (B * \langle A \rangle))) - (- (\langle B \rangle * \langle A \rangle))$

using *assms* **by** *auto*

also have ... $= A * B - \langle A \rangle * B - A * \langle B \rangle + - (- (\langle A \rangle * \langle B \rangle)) - (B * A + (- (\langle B \rangle * A)) + (- (B * \langle A \rangle))) + (- (- (\langle B \rangle * \langle A \rangle)))$

apply (*mat-assoc n*)

using *assms* **by** *auto*

also have ... $= A * B - \langle A \rangle * B - A * \langle B \rangle + \langle A \rangle * \langle B \rangle - (B * A + (- (\langle B \rangle * A)) + (- (B * \langle A \rangle))) + \langle B \rangle * \langle A \rangle$

by *simp*

— Remove parentheses

also have ... $= A * B - \langle A \rangle * B - A * \langle B \rangle + \langle A \rangle * \langle B \rangle - B * A + (- (- (\langle B \rangle * A)) + (- (- (B * \langle A \rangle)))) - \langle B \rangle * \langle A \rangle$

apply (*mat-assoc n*)

using *assms* **by** *auto*

also have ... $= A * B - \langle A \rangle * B - A * \langle B \rangle + \langle A \rangle * \langle B \rangle - B * A + \langle B \rangle * A + B * \langle A \rangle - \langle B \rangle * \langle A \rangle$

using *uminus-uminus-mat* **by** *simp*

— Commutative mean

also have ... $= A * B - \langle A \rangle * B - A * \langle B \rangle + \langle A \rangle * \langle B \rangle - B * A + A * \langle B \rangle + \langle A \rangle * B - \langle A \rangle * \langle B \rangle$

using *assms* **by** *auto*

— Reorder terms

also have ... = $A * B - B * A + \langle\langle A \rangle\rangle * B - \langle\langle A \rangle\rangle * B + A * \langle\langle B \rangle\rangle - A * \langle\langle B \rangle\rangle$
 + $\langle\langle A \rangle\rangle * \langle\langle B \rangle\rangle - \langle\langle A \rangle\rangle * \langle\langle B \rangle\rangle$
apply (*mat-assoc n*)
using *assms by auto*
 — Everything but the first two terms are eliminated, resulting in the commutator
finally show *?thesis using assms minus-r-inv-mat by auto*
qed

theorem *uncertainty-principle:*

assumes *observable C observable D*

shows $\Delta C * \Delta D \geq \text{norm } \langle\psi | \llbracket C, D \rrbracket *_{\nu} \psi \rangle / 2$

proof —

— Perform the substitution

let $?A = C - \langle\langle C \rangle\rangle$

let $?B = D - \langle\langle D \rangle\rangle$

— These matrices are valid observables

from *assms have observables-A-B: observable ?A observable ?B*

using *hermitian-inner-prod-real assms Reals-cnj-iff*

by (*auto simp: hermitian-def adjoint-minus adjoint-one adjoint-scale*)

— Start with commutator-ineq

have $(\text{norm } \langle\psi | \llbracket ?A, ?B \rrbracket *_{\nu} \psi \rangle)^2 \leq 4 * \text{Re } (\langle\psi | ?A * ?A *_{\nu} \psi \rangle) * (\langle\psi | ?B * ?B *_{\nu} \psi \rangle)$

using *commutator-ineq[OF observables-A-B] by auto*

— Simplify the commutator

then have $(\text{norm } \langle\psi | \llbracket C, D \rrbracket *_{\nu} \psi \rangle)^2 \leq 4 * \text{Re } (\langle\psi | ?A * ?A *_{\nu} \psi \rangle) * (\langle\psi | ?B * ?B *_{\nu} \psi \rangle)$

using *assms by simp*

— Apply sqrt to both sides

then have $\text{sqrt } ((\text{norm } (\langle\psi | \llbracket C, D \rrbracket *_{\nu} \psi \rangle))^2) \leq \text{sqrt } (4 * \text{Re } (\langle\psi | ?A * ?A *_{\nu} \psi \rangle) * (\langle\psi | ?B * ?B *_{\nu} \psi \rangle))$

using *real-sqrt-le-mono by blast*

— Simplify

then have $\text{norm } (\langle\psi | \llbracket C, D \rrbracket *_{\nu} \psi \rangle) \leq 2 * \text{sqrt } (\text{Re } (\langle\psi | ?A * ?A *_{\nu} \psi \rangle) * (\langle\psi | ?B * ?B *_{\nu} \psi \rangle))$

by (*auto cong: real-sqrt-mult*)

— Because these inner products are positive and real, norm = Re

then have $\text{norm } (\langle\psi | \llbracket C, D \rrbracket *_{\nu} \psi \rangle) \leq 2 * \text{sqrt } (|\text{Re } (\langle\psi | ?A * ?A *_{\nu} \psi \rangle) * (\langle\psi | ?B * ?B *_{\nu} \psi \rangle)|)$

by (*smt (verit, ccfv-SIG) real-sqrt-le-iff*)

then have $\text{norm } (\langle\psi | \llbracket C, D \rrbracket *_{\nu} \psi \rangle) \leq 2 * \text{sqrt } (\text{norm } (\langle\psi | ?A * ?A *_{\nu} \psi \rangle) * (\langle\psi | ?B * ?B *_{\nu} \psi \rangle))$

by (*auto simp: in-Reals-norm Reals-cnj-iff cnj-observables observables-A-B*)

— Rewrite term to recover the standard deviation (As formulated in std-dev-alt)

then have $\text{norm } (\langle\psi | \llbracket C, D \rrbracket *_{\nu} \psi \rangle) \leq 2 * \text{norm } (\text{csqrt } (\langle\psi | ?A * ?A *_{\nu} \psi \rangle)) * \text{norm } (\text{csqrt } (\langle\psi | ?B * ?B *_{\nu} \psi \rangle))$

by (*simp add: norm-mult real-sqrt-mult*)

```
    then show  $\Delta C * \Delta D \geq \text{norm } \langle \psi | [[C, D]] *_{\nu} \psi \rangle / 2$ 
      using assms by (auto cong: std-dev-alt)
qed
end
end
```

References

- [1] J. Liu, B. Zhan, S. Wang, S. Ying, T. Liu, Y. Li, M. Ying, and N. Zhan. Quantum hoare logic. *Archive of Formal Proofs*, March 2019. <https://isa-afp.org/entries/QHLProver.html>, Formal proof development.
- [2] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.