Uncertainty Principle

Alexander Treml

March 17, 2025

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

theory *Uncertainty-Principle*
imports *QHLProver.Complex-Matrix*
begin

1 Setup

abbreviation *bra-ket* (‹⟨-|-⟩›)
where $\langle u|v\rangle \equiv$ *inner-prod u v*

Fix an n-dimensional normalized quantum state ψ.

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

begin

Observables on ψ are hermitian matrices of appropriate dimensions.

abbreviation *observable*:: *complex Matrix.mat* ⇒ *bool* **where**
observable A ≡ *A* ∈ *carrier-mat n n* ∧ *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* :: *complex Matrix.mat* ⇒ *complex Matrix.mat* (‹⟪-⟫›)
where ⟪*A*⟫ ≡ ⟨ψ| *A* $*_v$ ψ⟩ $\cdot_m$ 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* :: *complex Matrix.mat* ⇒ *real* (‹Δ›)
where Δ *A* ≡ *norm* (*csqrt* (⟨ψ| (*A* ∗ *A* $*_v$ ψ)⟩ − ⟨ψ| *A* $*_v$ ψ⟩ ∗ ⟨ψ| *A* $*_v$ ψ⟩))

end

abbreviation *commutator* :: *complex Matrix.mat* ⇒ *complex Matrix.mat* ⇒ *complex Matrix.mat* (‹⟦-,-⟧›)
where *commutator A B* ≡ (*A* ∗ *B* − *B* ∗ *A*)

abbreviation *anticommutator* :: *complex Matrix.mat* ⇒ *complex Matrix.mat* ⇒ *complex Matrix.mat* (‹⦃-,-⦄›)
where *anticommutator A B* ≡ (*A* ∗ *B* + *B* ∗ *A*)

2 Auxiliary Lemmas

lemma *inner-prod-distrib-add-mat*:

fixes $u\ v$ :: *complex vec*
assumes
$u \in$ *carrier-vec* n
$v \in$ *carrier-vec* m
$A \in$ *carrier-mat* $n\ m$
$B \in$ *carrier-mat* $n\ m$
shows $\langle u|\ (A + B) *_v\ v\rangle = \langle u|\ A *_v\ v\rangle + \langle u|\ B *_v\ v\rangle$
$\langle proof \rangle$

lemma *inner-prod-distrib-minus-mat*:
fixes $u\ v$ :: *complex vec*
assumes
$u \in$ *carrier-vec* n
$v \in$ *carrier-vec* m
$A \in$ *carrier-mat* $n\ m$
$B \in$ *carrier-mat* $n\ m$
shows $\langle u|\ (A - B) *_v\ v\rangle = \langle u|\ A *_v\ v\rangle - \langle u|\ B *_v\ v\rangle$
$\langle proof \rangle$

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

lemma *Cauchy-Schwarz*:
assumes $v \in$ *carrier-vec* n $u \in$ *carrier-vec* n
shows *norm* $(\langle u|v\rangle)\hat{}2 \leq$ *Re* $(\langle u|u\rangle * \langle v|v\rangle)$
$\langle proof \rangle$

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 *csqrt* $(\langle \psi|\ (A * A *_v\ \psi)\rangle - \langle \psi|\ A *_v\ \psi\rangle * \langle \psi|\ A *_v\ \psi\rangle) \in \mathbb{R}$
$\langle proof \rangle$

This is an alternative way of formulating the standard deviation.

lemma *std-dev-alt*:
assumes *observable* A
shows $\Delta\ A =$ *norm* (*csqrt* $(\langle \psi|\ (A - \langle\!\langle A \rangle\!\rangle) * (A - \langle\!\langle A \rangle\!\rangle) *_v\ \psi\rangle))$
$\langle proof \rangle$

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*⟩

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 $\langle\psi|\ [\![A,\ B]\!] *_v\ \psi\rangle = 2 * \mathrm{i} * Im(\langle\psi|\ A * B *_v\ \psi\rangle)$
⟨*proof*⟩

lemma *anticommutator-re*:
assumes *observable A observable B*
shows $\langle\psi|\ \{\!|A,\ B|\!\} *_v\ \psi\rangle = 2 * Re(\langle\psi|\ A * B *_v\ \psi\rangle)$
⟨*proof*⟩

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 $(norm\ \langle\psi|\ [\![A,\ B]\!] *_v\ \psi\rangle)\hat{}2 \leq\ 4 * Re\ (\langle\psi|\ A * A *_v\ \psi\rangle * \langle\psi|\ B * B *_v\ \psi\rangle)$
⟨*proof*⟩

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 $A \in$ *carrier-mat n n* $B \in$ *carrier-mat n n*
shows $[\![A - \langle\!\langle A\rangle\!\rangle,\ B - \langle\!\langle B\rangle\!\rangle]\!] = [\![A,B]\!]$
⟨*proof*⟩

theorem *uncertainty-principle*:
assumes *observable C observable D*
shows $\Delta\ C * \Delta\ D \geq\ norm\ \langle\psi|[\![C,D]\!] *_v\ \psi\rangle\ /\ 2$
⟨*proof*⟩

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.