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*⟫ ≡ $\langle\psi|\ A *_v \psi\rangle \cdot_m 1_m\ n$

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* :: *complex Matrix.mat* ⇒ *real* (‹Δ›)
where $\Delta\ A \equiv$ *norm* (*csqrt* $(\langle\psi|\ (A * A *_v \psi)\rangle - \langle\psi|\ A *_v \psi\rangle * \langle\psi|\ A *_v \psi\rangle))$

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 $\langle u|\ (A + B) *_v\ v\rangle = \langle u|\ A *_v\ v\rangle + \langle u|\ B *_v\ v\rangle$
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* :: *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 $\langle u|\ (A - B) *_v\ v\rangle = \langle u|\ A *_v\ v\rangle - \langle u|\ B *_v\ v\rangle$
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 $v \in$ *carrier-vec n* $u \in$ *carrier-vec n*
shows *norm* $(\langle u|v\rangle)$^*2* $\leq$ *Re* $(\langle u|u\rangle * \langle v|v\rangle)$
proof−
have *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 *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 (⟨ψ|A ∗ A ∗v ψ⟩ − ⟨ψ|A ∗v ψ⟩ ∗ ⟨ψ|A ∗v ψ⟩) = 0
    using complex-is-Real-iff by simp
next
  have ∗:adjoint A = A using assms hermitian-def by blast
  — ... and positive (Cauchy-Schwarz)
  have ⟨ψ|A ∗v ψ⟩ ∗ ⟨ψ|A ∗v ψ⟩ ≤ ⟨ψ|ψ⟩ ∗ ⟨ψ|A ∗ A ∗v ψ⟩
    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 ≤ Re (⟨ψ|A ∗ A ∗v ψ⟩ − ⟨ψ|A ∗v ψ⟩ ∗ ⟨ψ|A ∗v ψ⟩)
    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 Δ A = norm (csqrt (⟨ψ| (A − ⟪A⟫) ∗ (A − ⟪A⟫) ∗v ψ⟩))
proof−
  — Expand the matrix term
  have (A − ⟪A⟫) ∗ (A − ⟪A⟫) = (A + − ⟪A⟫) ∗ (A + − ⟪A⟫)
    using assms minus-add-uminus-mat by force
  also have ∗: ... = A ∗ A + A ∗ − ⟪A⟫ + − ⟪A⟫ ∗ A + − ⟪A⟫ ∗ − ⟪A⟫
    apply (mat-assoc n)
    using assms by auto
  also have ... = A ∗ A − ⟪A⟫ ∗ A − ⟪A⟫ ∗ A + ⟪A⟫ ∗ ⟪A⟫
    using uminus-mult-right-mat assms by auto
  also have ... = A ∗ A − ⟨ψ| A ∗v ψ⟩ ·m A − ⟨ψ| A ∗v ψ⟩ ·m A + ⟪A⟫ ∗ ⟪A⟫
    using assms by auto
  finally have 1:
     ⟨ψ| (A − ⟪A⟫) ∗ (A − ⟪A⟫) ∗v ψ⟩ =
      ⟨ψ| (A ∗ A − ⟨ψ| A ∗v ψ⟩ ·m A − ⟨ψ| A ∗v ψ⟩ ·m A + ⟪A⟫ ∗ ⟪A⟫) ∗v ψ⟩
    by simp

  — The mean is linear, so it distributes over the matrix term ...
  have 2:
    ⟨ψ| (A ∗ A − ⟨ψ| A ∗v ψ⟩ ·m A − ⟨ψ| A ∗v ψ⟩ ·m A + ⟪A⟫ ∗ ⟪A⟫) ∗v ψ⟩ =
      ⟨ψ|A ∗ A ∗v ψ⟩ − ⟨ψ|⟨ψ|A ∗v ψ⟩ ·m A ∗v ψ⟩ − ⟨ψ|⟨ψ|A ∗v ψ⟩ ·m A ∗v ψ⟩ +
⟨ψ|⟪A⟫ ∗ ⟪A⟫ ∗v ψ⟩
    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: ⟨ψ|⟨ψ|A ∗v ψ⟩ ·m A ∗v ψ⟩ = ⟨ψ|A ∗v ψ⟩ ∗ ⟨ψ|A ∗v ψ⟩
```

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 $\langle\psi|\langle\!\langle A\rangle\!\rangle * \langle\!\langle A\rangle\!\rangle *_v \psi\rangle = \langle\psi|A *_v \psi\rangle * \langle\psi|\langle\!\langle A\rangle\!\rangle *_v \psi\rangle$
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*: $\langle\psi|\langle\!\langle A\rangle\!\rangle * \langle\!\langle A\rangle\!\rangle *_v \psi\rangle = \langle\psi|A *_v \psi\rangle * \langle\psi|A *_v \psi\rangle$ **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* $\langle A * B *_v \psi|\psi\rangle$) = $\langle$*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 $\langle\psi|\ [\![A, B]\!] *_v \psi\rangle = 2 * \mathrm{i} * Im(\langle\psi|\ A * B *_v \psi\rangle)$
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-minus-mat*)
also have ... $= \langle\psi|\ A * B *_v \psi\rangle -$ *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 $\langle\psi|\ \{\!|A,\ B|\!\}\ *_v\ \psi\rangle = \mathit{2} * \mathit{Re}(\langle\psi|\ A * B *_v\ \psi\rangle)$
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 ... $= \langle\psi|\ A * B *_v\ \psi\rangle + \mathit{cnj}\ \langle\psi|\ A * B *_v\ \psi\rangle$
    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 $(\mathit{norm}\ \langle\psi|\ [\![A,\ B]\!]\ *_v\ \psi\rangle)\hat{}\mathit{2} \le\ \mathit{4} * \mathit{Re}\ (\langle\psi|\ A * A *_v\ \psi\rangle * \langle\psi|\ B * B *_v\ \psi\rangle)$
proof −
  — The inner product of our quantum state under A and B can be expressed in terms of its real and imaginary part
  let $?x = \mathit{Re}(\langle\psi|\ A * B *_v\ \psi\rangle)$
  let $?y = \mathit{Im}(\langle\psi|\ A * B *_v\ \psi\rangle)$

  — These parts can be expressed using the commutator/anticommutator as shown above
  have *im*: $(\mathit{norm}\ \langle\psi|\ [\![A,\ B]\!]\ *_v\ \psi\rangle)\hat{}\mathit{2} = \mathit{4} * ?y\hat{}\mathit{2}$
    apply (*subst commutator-im*[*OF assms*])
    using *cmod-power2* **by** *simp*

  have *re*: $(\mathit{norm}\ \langle\psi|\ \{\!|A,\ B|\!\}\ *_v\ \psi\rangle)\hat{}\mathit{2} = \mathit{4} * ?x\hat{}\mathit{2}$
    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** $(\mathit{norm}\ \langle\psi|\ [\![A,\ B]\!]\ *_v\ \psi\rangle)\hat{}\mathit{2} + (\mathit{norm}\ \langle\psi|\ \{\!|A,\ B|\!\}\ *_v\ \psi\rangle)\hat{}\mathit{2} = \mathit{4} * (?x\hat{}\mathit{2} + ?y\hat{}\mathit{2})$
    by *simp*
  also have ... $= \mathit{4} * \mathit{norm}(\langle\psi|\ A * B *_v\ \psi\rangle)\hat{}\mathit{2}$
    using *cmod-power2* **by** *simp*
  also have ... $= \mathit{4} * \mathit{norm}(\langle A *_v\ \psi|\ B *_v\ \psi\rangle)\hat{}\mathit{2}$
    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 $A \in$ *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 −
— 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 $[\![A - \langle\!\langle A\rangle\!\rangle, B - \langle\!\langle B\rangle\!\rangle]\!] = A * B - \langle\!\langle A\rangle\!\rangle * B - A * \langle\!\langle B\rangle\!\rangle - \langle\!\langle A\rangle\!\rangle * (- \langle\!\langle B\rangle\!\rangle) - (B * A + (- (\langle\!\langle B\rangle\!\rangle * A)) + (- (B * \langle\!\langle A\rangle\!\rangle)) - \langle\!\langle B\rangle\!\rangle * (- \langle\!\langle A\rangle\!\rangle))$
apply (*mat-assoc n*)
using *assms* **by** *auto*
— Remove the last subtraction in the parentheses and unnecessary minus signs
also have ... $= A * B - \langle\!\langle A\rangle\!\rangle * B - A * \langle\!\langle B\rangle\!\rangle - (- (\langle\!\langle A\rangle\!\rangle * \langle\!\langle B\rangle\!\rangle)) - (B * A + (- (\langle\!\langle B\rangle\!\rangle * A)) + (- (B * \langle\!\langle A\rangle\!\rangle)) - (- (\langle\!\langle B\rangle\!\rangle * \langle\!\langle A\rangle\!\rangle)))$
using *assms* **by** *auto*
also have ... $= A * B - \langle\!\langle A\rangle\!\rangle * B - A * \langle\!\langle B\rangle\!\rangle + - (- (\langle\!\langle A\rangle\!\rangle * \langle\!\langle B\rangle\!\rangle)) - (B * A + (- (\langle\!\langle B\rangle\!\rangle * A)) + (- (B * \langle\!\langle A\rangle\!\rangle)) + (- (- (\langle\!\langle B\rangle\!\rangle * \langle\!\langle A\rangle\!\rangle))))$
apply (*mat-assoc n*)
using *assms* **by** *auto*
also have ... $= A * B - \langle\!\langle A\rangle\!\rangle * B - A * \langle\!\langle B\rangle\!\rangle + \langle\!\langle A\rangle\!\rangle * \langle\!\langle B\rangle\!\rangle - (B * A + (- (\langle\!\langle B\rangle\!\rangle * A)) + (- (B * \langle\!\langle A\rangle\!\rangle)) + \langle\!\langle B\rangle\!\rangle * \langle\!\langle A\rangle\!\rangle)$
by *simp*
— Remove parentheses
also have ... $= A * B - \langle\!\langle A\rangle\!\rangle * B - A * \langle\!\langle B\rangle\!\rangle + \langle\!\langle A\rangle\!\rangle * \langle\!\langle B\rangle\!\rangle - B * A + (- (- (\langle\!\langle B\rangle\!\rangle * A))) + (- (- (B * \langle\!\langle A\rangle\!\rangle))) - \langle\!\langle B\rangle\!\rangle * \langle\!\langle A\rangle\!\rangle$
apply (*mat-assoc n*)
using *assms* **by** *auto*
also have ... $=A * B - \langle\!\langle A\rangle\!\rangle * B - A * \langle\!\langle B\rangle\!\rangle + \langle\!\langle A\rangle\!\rangle * \langle\!\langle B\rangle\!\rangle - B * A + \langle\!\langle B\rangle\!\rangle * A + B * \langle\!\langle A\rangle\!\rangle - \langle\!\langle B\rangle\!\rangle * \langle\!\langle A\rangle\!\rangle$
using *uminus-uminus-mat* **by** *simp*
— Commutative mean
also have ...$= A * B - \langle\!\langle A\rangle\!\rangle * B - A * \langle\!\langle B\rangle\!\rangle + \langle\!\langle A\rangle\!\rangle * \langle\!\langle B\rangle\!\rangle - B * A + A * \langle\!\langle B\rangle\!\rangle + \langle\!\langle A\rangle\!\rangle * B - \langle\!\langle A\rangle\!\rangle * \langle\!\langle B\rangle\!\rangle$
using *assms* **by** *auto*
— Reorder terms

```
  also have ...= A ∗ B − B ∗ A + ⟪A⟫ ∗ B − ⟪A⟫ ∗ B + A ∗ ⟪B⟫ − A ∗ ⟪B⟫
+ ⟪A⟫ ∗ ⟪B⟫ − ⟪A⟫ ∗ ⟪B⟫
    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 Δ C ∗ Δ D ≥ norm ⟨ψ|⟦C,D⟧ ∗v ψ⟩ / 2
proof −
  — Perform the substitution
  let ?A = C − ⟪C⟫
  let ?B = D − ⟪D⟫

  — 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 (norm ⟨ψ| ⟦?A, ?B⟧ ∗v ψ⟩)^2 ≤ 4 ∗ Re (((⟨ψ| ?A ∗ ?A ∗v ψ⟩) ∗ (⟨ψ| ?B ∗
?B ∗v ψ⟩))
    using commutator-ineq[OF observables-A-B] by auto
  — Simplify the commutator
  then have (norm ⟨ψ| ⟦C, D⟧ ∗v ψ⟩)^2 ≤ 4 ∗ Re (((⟨ψ| ?A ∗ ?A ∗v ψ⟩) ∗ (⟨ψ|
?B ∗ ?B ∗v ψ⟩))
    using assms by simp
  — Apply sqrt to both sides
  then have sqrt ((norm (⟨ψ| ⟦C, D⟧ ∗v ψ⟩))^2) ≤ sqrt (4 ∗ Re (((⟨ψ| ?A ∗ ?A
∗v ψ⟩) ∗ (⟨ψ| ?B ∗ ?B ∗v ψ⟩)))
    using real-sqrt-le-mono by blast
  — Simplify
  then have norm (⟨ψ| ⟦C, D⟧ ∗v ψ⟩) ≤ 2 ∗ sqrt (Re (((⟨ψ| ?A ∗ ?A ∗v ψ⟩) ∗ (⟨ψ|
?B ∗ ?B ∗v ψ⟩)))
    by (auto cong: real-sqrt-mult)
  — Because these inner products are positive and real, norm = Re
  then have norm (⟨ψ| ⟦C, D⟧ ∗v ψ⟩) ≤ 2 ∗ sqrt ( |Re (((⟨ψ| ?A ∗ ?A ∗v ψ⟩) ∗
(⟨ψ| ?B ∗ ?B ∗v ψ⟩))|)
    by (smt (verit, ccfv-SIG) real-sqrt-le-iff)
  then have norm (⟨ψ| ⟦C, D⟧ ∗v ψ⟩) ≤ 2 ∗ sqrt (norm (((⟨ψ| ?A ∗ ?A ∗v ψ⟩) ∗
(⟨ψ| ?B ∗ ?B ∗v ψ⟩)))
    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 norm (⟨ψ| ⟦C, D⟧ ∗v ψ⟩) ≤ 2 ∗ norm (csqrt (⟨ψ| ?A ∗ ?A ∗v ψ⟩)) ∗
norm (csqrt (⟨ψ| ?B ∗ ?B ∗v ψ⟩))
    by (simp add: norm-mult real-sqrt-mult)
```

then show $\Delta\ C * \Delta\ D \geq$ *norm* $\langle\psi|[\![C,\ D]\!] *_v\ \psi\rangle\ /\ 2$
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.