

Projective-Measurements

Mnacho

September 13, 2023

Contents

1 Preliminaries	1
1.1 Misc	1
1.2 Unifying notions between Isabelle Marries Dirac and QHL- Prover	3
1.3 Types to sets lemmata transfers	3
2 Linear algebra complements	4
2.1 Additional properties of matrices	4
2.2 Complements on complex matrices	5
2.3 Tensor product complements	8
2.4 Fixed carrier matrices locale	9
2.5 A locale for square matrices	10
2.6 Projectors	13
2.7 Rank 1 projection	15
3 Projective measurements	17
3.1 First definitions	18
3.2 Measurements with observables	20
3.2.1 On the diagonal elements of a matrix	21
3.2.2 Construction of measurement outcomes	23
3.2.3 Projective measurement associated with an observable	24
3.2.4 Properties on the spectrum of a Hermitian matrix	27
3.2.5 Similar properties for eigenvalues rather than spec- trum indices	30
4 The CHSH inequality	31
4.1 Inequality statement	31
4.2 Properties of specific observables	36
4.2.1 Ket 0, Ket 1 and the corresponding projectors	36
4.2.2 The X and Z matrices and two of their combinations	37
4.2.3 No local hidden variable	41

```

theory Linear-Algebra-Complements imports
  Isabelle-Marries-Dirac.Tensor
  Isabelle-Marries-Dirac.More-Tensor
  QHLProver.Gates
  HOL-Types-To-Sets.Group-On-With
  HOL-Probability.Probability

```

```

begin
hide-const(open) S

```

1 Preliminaries

1.1 Misc

```

lemma mult-real-cpx:
  fixes a::complex
  fixes b::complex
  assumes a ∈ Reals
  shows  $a * (\text{Re } b) = \text{Re } (a * b)$  <proof>

```

```

lemma fct-bound:
  fixes f::complex ⇒ real
  assumes  $f(-1) + f 1 = 1$ 
  and  $0 \leq f 1$ 
  and  $0 \leq f (-1)$ 
  shows  $-1 \leq f 1 - f(-1) \wedge f 1 - f(-1) \leq 1$ 
  <proof>

```

```

lemma fct-bound':
  fixes f::complex ⇒ real
  assumes  $f(-1) + f 1 = 1$ 
  and  $0 \leq f 1$ 
  and  $0 \leq f (-1)$ 
  shows  $|f 1 - f(-1)| \leq 1$  <proof>

```

```

lemma pos-sum-1-le:
  assumes finite I
  and  $\forall i \in I. (0::real) \leq f i$ 
  and  $(\sum_{i \in I} f i) = 1$ 
  and  $j \in I$ 
  shows  $f j \leq 1$ 
  <proof>

```

```

lemma last-subset:
  assumes  $A \subseteq \{a, b\}$ 
  and  $a \neq b$ 
  and  $A \neq \{a, b\}$ 

```

and $A \neq \{\}$
and $A \neq \{a\}$
shows $A = \{b\}$ $\langle proof \rangle$

lemma *disjoint-Un*:
assumes *disjoint-family-on* A (*insert* x F)
and $x \notin F$
shows $(A\ x) \cap (\bigcup a \in F. A\ a) = \{\}$
 $\langle proof \rangle$

lemma *sum-but-one*:
assumes $\forall j < (n::nat). j \neq i \longrightarrow f\ j = (0::'a::ring)$
and $i < n$
shows $(\sum j \in \{0 ..< n\}. f\ j * g\ j) = f\ i * g\ i$
 $\langle proof \rangle$

lemma *sum-2-elems*:
assumes $I = \{a, b\}$
and $a \neq b$
shows $(\sum a \in I. f\ a) = f\ a + f\ b$
 $\langle proof \rangle$

lemma *sum-4-elems*:
shows $(\sum i < (4::nat). f\ i) = f\ 0 + f\ 1 + f\ 2 + f\ 3$
 $\langle proof \rangle$

lemma *disj-family-sum*:
shows $finite\ I \implies disjoint_family_on\ A\ I \implies (\bigwedge i. i \in I \implies finite\ (A\ i)) \implies$
 $(\sum i \in (\bigcup n \in I. A\ n). f\ i) = (\sum n \in I. (\sum i \in A\ n. f\ i))$
 $\langle proof \rangle$

lemma *integrable-real-mult-right*:
fixes $c::real$
assumes *integrable* $M\ f$
shows *integrable* M $(\lambda w. c * f\ w)$
 $\langle proof \rangle$

1.2 Unifying notions between Isabelle Marries Dirac and QHLPProver

lemma *mult-conj-cmod-square*:
fixes $z::complex$
shows $z * conjugate\ z = (cmod\ z)^2$
 $\langle proof \rangle$

lemma *vec-norm-sq-cpx-vec-length-sq*:
shows $(vec_norm\ v)^2 = (cpx_vec_length\ v)^2$
 $\langle proof \rangle$

lemma *vec-norm-eq-cpx-vec-length*:
shows $\text{vec-norm } v = \text{cpx-vec-length } v$ $\langle \text{proof} \rangle$

lemma *cpx-vec-length-square*:
shows $\|v\|^2 = (\sum i = 0..<\text{dim-vec } v. (\text{cmod } (\text{Matrix.vec-index } v \ i)))^2$ $\langle \text{proof} \rangle$

lemma *state-qbit-norm-sq*:
assumes $v \in \text{state-qbit } n$
shows $(\text{cpx-vec-length } v)^2 = 1$
 $\langle \text{proof} \rangle$

lemma *dagger-adjoint*:
shows $\text{dagger } M = \text{Complex-Matrix.adjoint } M$ $\langle \text{proof} \rangle$

1.3 Types to sets lemmata transfers

context *ab-group-add-on-with* **begin**

context includes *lifting-syntax* **assumes** $\text{ltd}: \exists (\text{Rep}::'s \Rightarrow 'a) (\text{Abs}::'a \Rightarrow 's)$.
type-definition *Rep* *Abs* *S* **begin**

interpretation *local-typedef-ab-group-add-on-with* $\text{pls } z \ \text{mns } \text{um } S \ \text{TYPE}('s)$ $\langle \text{proof} \rangle$

lemmas *lt-sum-union-disjoint* = *sum.union-disjoint*
 $[\text{var-simplified explicit-ab-group-add},$
 $\text{unoverload-type } 'c,$
 $OF \ \text{type.comm-monoid-add-axioms},$
 $\text{untransferred}]$

lemmas *lt-disj-family-sum* = *disj-family-sum*
 $[\text{var-simplified explicit-ab-group-add},$
 $\text{unoverload-type } 'd,$
 $OF \ \text{type.comm-monoid-add-axioms},$
 $\text{untransferred}]$

lemmas *lt-sum-reindex-cong* = *sum.reindex-cong*
 $[\text{var-simplified explicit-ab-group-add},$
 $\text{unoverload-type } 'd,$
 $OF \ \text{type.comm-monoid-add-axioms},$
 $\text{untransferred}]$

end

lemmas *sum-with-union-disjoint* =
lt-sum-union-disjoint
 $[\text{cancel-type-definition},$
 $OF \ \text{carrier-ne},$
 $\text{simplified pred-fun-def}, \ \text{simplified}]$

lemmas *disj-family-sum-with* =
lt-disj-family-sum

[cancel-type-definition,
OF carrier-ne,
simplified pred-fun-def, simplified]

lemmas *sum-with-reindex-cong* =
lt-sum-reindex-cong
[cancel-type-definition,
OF carrier-ne,
simplified pred-fun-def, simplified]

end

lemma (in *comm-monoid-add-on-with*) *sum-with-cong'*:
shows *finite I* $\implies (\bigwedge i. i \in I \implies A\ i = B\ i) \implies (\bigwedge i. i \in I \implies A\ i \in S) \implies$
 $(\bigwedge i. i \in I \implies B\ i \in S) \implies \text{sum-with pls } z\ A\ I = \text{sum-with pls } z\ B\ I$
<proof>

2 Linear algebra complements

2.1 Additional properties of matrices

lemma *smult-one*:
shows $(1::'a::\text{monoid-mult}) \cdot_m A = A$ <proof>

lemma *times-diag-index*:
fixes $A::'a::\text{comm-ring Matrix.mat}$
assumes $A \in \text{carrier-mat } n\ n$
and $B \in \text{carrier-mat } n\ n$
and *diagonal-mat B*
and $j < n$
and $i < n$
shows $\text{Matrix.vec-index } (\text{Matrix.row } (A*B)\ j)\ i = \text{diag-mat } B\ !\ i * A\ \$\$ (j, i)$
<proof>

lemma *inner-prod-adjoint-comp*:
assumes $(U::'a::\text{conjugatable-field Matrix.mat}) \in \text{carrier-mat } n\ n$
and $(V::'a::\text{conjugatable-field Matrix.mat}) \in \text{carrier-mat } n\ n$
and $i < n$
and $j < n$
shows $\text{Complex-Matrix.inner-prod } (\text{Matrix.col } V\ i)\ (\text{Matrix.col } U\ j) =$
 $((\text{Complex-Matrix.adjoint } V) * U)\ \$\$ (i, j)$
<proof>

lemma *mat-unit-vec-col*:
assumes $(A::'a::\text{conjugatable-field Matrix.mat}) \in \text{carrier-mat } n\ n$
and $i < n$
shows $A * _v (\text{unit-vec } n\ i) = \text{Matrix.col } A\ i$
<proof>

lemma *mat-prod-unit-vec-cong*:
assumes $(A::'a::\text{conjugatable-field Matrix.mat}) \in \text{carrier-mat } n \ n$
and $B \in \text{carrier-mat } n \ n$
and $\bigwedge i. i < n \implies A *_{\nu} (\text{unit-vec } n \ i) = B *_{\nu} (\text{unit-vec } n \ i)$
shows $A = B$
 $\langle \text{proof} \rangle$

lemma *smult-smult-times*:
fixes $a::'a::\text{semigroup-mult}$
shows $a \cdot_m (k \cdot_m A) = (a * k) \cdot_m A$
 $\langle \text{proof} \rangle$

lemma *mat-minus-minus*:
fixes $A :: 'a :: \text{ab-group-add Matrix.mat}$
assumes $A \in \text{carrier-mat } n \ m$
and $B \in \text{carrier-mat } n \ m$
and $C \in \text{carrier-mat } n \ m$
shows $A - (B - C) = A - B + C$
 $\langle \text{proof} \rangle$

2.2 Complements on complex matrices

lemma *hermitian-square*:
assumes *hermitian* M
shows $M \in \text{carrier-mat } (\text{dim-row } M) \ (\text{dim-row } M)$
 $\langle \text{proof} \rangle$

lemma *hermitian-add*:
assumes $A \in \text{carrier-mat } n \ n$
and $B \in \text{carrier-mat } n \ n$
and *hermitian* A
and *hermitian* B
shows *hermitian* $(A + B)$ $\langle \text{proof} \rangle$

lemma *hermitian-minus*:
assumes $A \in \text{carrier-mat } n \ n$
and $B \in \text{carrier-mat } n \ n$
and *hermitian* A
and *hermitian* B
shows *hermitian* $(A - B)$ $\langle \text{proof} \rangle$

lemma *hermitian-smult*:
fixes $a::\text{real}$
fixes $A::\text{complex Matrix.mat}$
assumes $A \in \text{carrier-mat } n \ n$
and *hermitian* A
shows *hermitian* $(a \cdot_m A)$
 $\langle \text{proof} \rangle$

lemma *unitary-eigenvalues-norm-square:*

fixes $U::\text{complex Matrix.mat}$

assumes *unitary* U

and $U \in \text{carrier-mat } n \ n$

and *eigenvalue* $U \ k$

shows *conjugate* $k * k = 1$

$\langle \text{proof} \rangle$

lemma *outer-prod-smult-left:*

fixes $v::\text{complex Matrix.vec}$

shows *outer-prod* $(a \cdot_v v) w = a \cdot_m \text{outer-prod } v \ w$

$\langle \text{proof} \rangle$

lemma *outer-prod-smult-right:*

fixes $v::\text{complex Matrix.vec}$

shows *outer-prod* $v (a \cdot_v w) = (\text{conjugate } a) \cdot_m \text{outer-prod } v \ w$

$\langle \text{proof} \rangle$

lemma *outer-prod-add-left:*

fixes $v::\text{complex Matrix.vec}$

assumes *dim-vec* $v = \text{dim-vec } x$

shows *outer-prod* $(v + x) w = \text{outer-prod } v \ w + (\text{outer-prod } x \ w)$

$\langle \text{proof} \rangle$

lemma *outer-prod-add-right:*

fixes $v::\text{complex Matrix.vec}$

assumes *dim-vec* $w = \text{dim-vec } x$

shows *outer-prod* $v (w + x) = \text{outer-prod } v \ w + (\text{outer-prod } v \ x)$

$\langle \text{proof} \rangle$

lemma *outer-prod-minus-left:*

fixes $v::\text{complex Matrix.vec}$

assumes *dim-vec* $v = \text{dim-vec } x$

shows *outer-prod* $(v - x) w = \text{outer-prod } v \ w - (\text{outer-prod } x \ w)$

$\langle \text{proof} \rangle$

lemma *outer-prod-minus-right:*

fixes $v::\text{complex Matrix.vec}$

assumes *dim-vec* $w = \text{dim-vec } x$

shows *outer-prod* $v (w - x) = \text{outer-prod } v \ w - (\text{outer-prod } v \ x)$

$\langle \text{proof} \rangle$

lemma *outer-minus-minus:*

fixes $a::\text{complex Matrix.vec}$

assumes *dim-vec* $a = \text{dim-vec } b$

and *dim-vec* $u = \text{dim-vec } v$

shows *outer-prod* $(a - b) (u - v) = \text{outer-prod } a \ u - \text{outer-prod } a \ v -$
 $\text{outer-prod } b \ u + \text{outer-prod } b \ v$

$\langle \text{proof} \rangle$

lemma *outer-trace-inner*:
assumes $A \in \text{carrier-mat } n \ n$
and $\text{dim-vec } u = n$
and $\text{dim-vec } v = n$
shows $\text{Complex-Matrix.trace } (\text{outer-prod } u \ v \ * \ A) = \text{Complex-Matrix.inner-prod } v \ (A \ *_v \ u)$
 $\langle \text{proof} \rangle$

lemma *zero-hermitian*:
shows $\text{hermitian } (0_m \ n \ n) \langle \text{proof} \rangle$

lemma *trace-1*:
shows $\text{Complex-Matrix.trace } ((1_m \ n)::\text{complex Matrix.mat}) = (n::\text{complex}) \langle \text{proof} \rangle$

lemma *trace-add*:
assumes $\text{square-mat } A$
and $\text{square-mat } B$
and $\text{dim-row } A = \text{dim-row } B$
shows $\text{Complex-Matrix.trace } (A + B) = \text{Complex-Matrix.trace } A + \text{Complex-Matrix.trace } B$
 $\langle \text{proof} \rangle$

lemma *bra-vec-carrier*:
shows $\text{bra-vec } v \in \text{carrier-mat } 1 \ (\text{dim-vec } v)$
 $\langle \text{proof} \rangle$

lemma *mat-mult-ket-carrier*:
assumes $A \in \text{carrier-mat } n \ m$
shows $A \ * \ |v\rangle \in \text{carrier-mat } n \ 1 \langle \text{proof} \rangle$

lemma *mat-mult-ket*:
assumes $A \in \text{carrier-mat } n \ m$
and $\text{dim-vec } v = m$
shows $A \ * \ |v\rangle = |A \ *_v \ v\rangle$
 $\langle \text{proof} \rangle$

lemma *unitary-density*:
assumes $\text{density-operator } R$
and $\text{unitary } U$
and $R \in \text{carrier-mat } n \ n$
and $U \in \text{carrier-mat } n \ n$
shows $\text{density-operator } (U \ * \ R \ * \ (\text{Complex-Matrix.adjoint } U)) \langle \text{proof} \rangle$

2.3 Tensor product complements

lemma *tensor-vec-dim[simp]*:
shows $\text{dim-vec } (\text{tensor-vec } u \ v) = \text{dim-vec } u \ * \ (\text{dim-vec } v)$
 $\langle \text{proof} \rangle$

lemma *index-tensor-vec[simp]*:
assumes $0 < \dim\text{-vec } v$
and $i < \dim\text{-vec } u * \dim\text{-vec } v$
shows $\text{vec-index } (\text{tensor-vec } u \ v) \ i =$
 $\text{vec-index } u \ (i \ \text{div} \ (\dim\text{-vec } v)) * \text{vec-index } v \ (i \ \text{mod} \ \dim\text{-vec } v)$
 $\langle \text{proof} \rangle$

lemma *outer-prod-tensor-comm*:
fixes $a::\text{complex Matrix.vec}$
fixes $u::\text{complex Matrix.vec}$
assumes $0 < \dim\text{-vec } a$
and $0 < \dim\text{-vec } b$
shows $\text{outer-prod } (\text{tensor-vec } u \ v) \ (\text{tensor-vec } a \ b) = \text{tensor-mat } (\text{outer-prod } u \ a)$
 $(\text{outer-prod } v \ b)$
 $\langle \text{proof} \rangle$

lemma *tensor-mat-adjoint*:
assumes $m1 \in \text{carrier-mat } r1 \ c1$
and $m2 \in \text{carrier-mat } r2 \ c2$
and $0 < c1$
and $0 < c2$
and $0 < r1$
and $0 < r2$
shows $\text{Complex-Matrix.adjoint } (\text{tensor-mat } m1 \ m2) =$
 $\text{tensor-mat } (\text{Complex-Matrix.adjoint } m1) \ (\text{Complex-Matrix.adjoint } m2)$
 $\langle \text{proof} \rangle$

lemma *index-tensor-mat'*:
assumes $0 < \dim\text{-col } A$
and $0 < \dim\text{-col } B$
and $i < \dim\text{-row } A * \dim\text{-row } B$
and $j < \dim\text{-col } A * \dim\text{-col } B$
shows $(A \otimes B) \ \$(i, j) =$
 $A \ \$(i \ \text{div} \ (\dim\text{-row } B), j \ \text{div} \ (\dim\text{-col } B)) * B \ \$(i \ \text{mod} \ (\dim\text{-row } B), j \ \text{mod} \ (\dim\text{-col } B))$
 $\langle \text{proof} \rangle$

lemma *tensor-mat-carrier*:
shows $\text{tensor-mat } U \ V \in \text{carrier-mat } (\dim\text{-row } U * \dim\text{-row } V) \ (\dim\text{-col } U * \dim\text{-col } V)$ $\langle \text{proof} \rangle$

lemma *tensor-mat-id*:
assumes $0 < d1$
and $0 < d2$
shows $\text{tensor-mat } (1_m \ d1) \ (1_m \ d2) = 1_m \ (d1 * d2)$
 $\langle \text{proof} \rangle$

lemma *tensor-mat-hermitian*:

```

assumes  $A \in \text{carrier-mat } n \ n$ 
and  $B \in \text{carrier-mat } n' \ n'$ 
and  $0 < n$ 
and  $0 < n'$ 
and hermitian  $A$ 
and hermitian  $B$ 
shows hermitian (tensor-mat  $A \ B$ )  $\langle \text{proof} \rangle$ 

```

```

lemma tensor-mat-unitary:
  assumes Complex-Matrix.unitary  $U$ 
  and Complex-Matrix.unitary  $V$ 
and  $0 < \text{dim-row } U$ 
and  $0 < \text{dim-row } V$ 
shows Complex-Matrix.unitary (tensor-mat  $U \ V$ )
 $\langle \text{proof} \rangle$ 

```

2.4 Fixed carrier matrices locale

We define a locale for matrices with a fixed number of rows and columns, and define a finite sum operation on this locale. The `Type_To_Sets` transfer tools then permits to obtain lemmata on the locale for free.

```

locale fixed-carrier-mat =
  fixes fc-mats::'a::field Matrix.mat set
  fixes dimR dimC
  assumes fc-mats-carrier: fc-mats = carrier-mat dimR dimC
begin

```

```

sublocale semigroup-add-on-with fc-mats (+)
 $\langle \text{proof} \rangle$ 

```

```

sublocale ab-semigroup-add-on-with fc-mats (+)
 $\langle \text{proof} \rangle$ 

```

```

sublocale comm-monoid-add-on-with fc-mats (+)  $0_m \ \text{dimR} \ \text{dimC}$ 
 $\langle \text{proof} \rangle$ 

```

```

sublocale ab-group-add-on-with fc-mats (+)  $0_m \ \text{dimR} \ \text{dimC} \ (-) \ \text{uminus}$ 
 $\langle \text{proof} \rangle$ 
end

```

```

lemma (in fixed-carrier-mat) smult-mem:
  assumes  $A \in \text{fc-mats}$ 
  shows  $a \cdot_m A \in \text{fc-mats}$   $\langle \text{proof} \rangle$ 

```

```

definition (in fixed-carrier-mat) sum-mat where
sum-mat  $A \ I = \text{sum-with } (+) \ (0_m \ \text{dimR} \ \text{dimC}) \ A \ I$ 

```

```

lemma (in fixed-carrier-mat) sum-mat-empty[simp]:
  shows sum-mat  $A \ \{\} = 0_m \ \text{dimR} \ \text{dimC}$   $\langle \text{proof} \rangle$ 

```

lemma (in *fixed-carrier-mat*) *sum-mat-carrier*:
shows $(\bigwedge i. i \in I \implies (A\ i) \in \text{fc-mats}) \implies \text{sum-mat } A\ I \in \text{carrier-mat } \text{dim}R$
 $\text{dim}C$
 ⟨proof⟩

lemma (in *fixed-carrier-mat*) *sum-mat-insert*:
assumes $A\ x \in \text{fc-mats}$ $A\ 'I \subseteq \text{fc-mats}$
and A : *finite* I **and** $x: x \notin I$
shows $\text{sum-mat } A\ (\text{insert } x\ I) = A\ x + \text{sum-mat } A\ I$ ⟨proof⟩

2.5 A locale for square matrices

locale *cpx-sq-mat* = *fixed-carrier-mat fc-mats::complex Matrix.mat set for fc-mats*
 +
assumes *dim-eq*: $\text{dim}R = \text{dim}C$
and *npos*: $0 < \text{dim}R$

lemma (in *cpx-sq-mat*) *one-mem*:
shows $1_m\ \text{dim}R \in \text{fc-mats}$ ⟨proof⟩

lemma (in *cpx-sq-mat*) *square-mats*:
assumes $A \in \text{fc-mats}$
shows *square-mat* A ⟨proof⟩

lemma (in *cpx-sq-mat*) *cpx-sq-mat-mult*:
assumes $A \in \text{fc-mats}$
and $B \in \text{fc-mats}$
shows $A * B \in \text{fc-mats}$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *sum-mat-distrib-left*:
shows *finite* $I \implies R \in \text{fc-mats} \implies (\bigwedge i. i \in I \implies (A\ i) \in \text{fc-mats}) \implies$
 $\text{sum-mat } (\lambda i. R * (A\ i))\ I = R * (\text{sum-mat } A\ I)$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *sum-mat-distrib-right*:
shows *finite* $I \implies R \in \text{fc-mats} \implies (\bigwedge i. i \in I \implies (A\ i) \in \text{fc-mats}) \implies$
 $\text{sum-mat } (\lambda i. (A\ i) * R)\ I = (\text{sum-mat } A\ I) * R$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *trace-sum-mat*:
fixes $A::'b \Rightarrow \text{complex Matrix.mat}$
shows *finite* $I \implies (\bigwedge i. i \in I \implies (A\ i) \in \text{fc-mats}) \implies$
 $\text{Complex-Matrix.trace } (\text{sum-mat } A\ I) = (\sum\ i \in I. \text{Complex-Matrix.trace } (A\ i))$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *cpx-sq-mat-smult*:
assumes $A \in \text{fc-mats}$

shows $x \cdot_m A \in \text{fc-mats}$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *mult-add-distrib-right*:
assumes $A \in \text{fc-mats}$ $B \in \text{fc-mats}$ $C \in \text{fc-mats}$
shows $A * (B + C) = A * B + A * C$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *mult-add-distrib-left*:
assumes $A \in \text{fc-mats}$ $B \in \text{fc-mats}$ $C \in \text{fc-mats}$
shows $(B + C) * A = B * A + C * A$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *mult-sum-mat-distrib-left*:
shows $\text{finite } I \implies (\bigwedge i. i \in I \implies (A \ i) \in \text{fc-mats}) \implies B \in \text{fc-mats} \implies$
 $(\text{sum-mat } (\lambda i. B * (A \ i)) \ I) = B * (\text{sum-mat } A \ I)$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *mult-sum-mat-distrib-right*:
shows $\text{finite } I \implies (\bigwedge i. i \in I \implies (A \ i) \in \text{fc-mats}) \implies B \in \text{fc-mats} \implies$
 $(\text{sum-mat } (\lambda i. (A \ i) * B) \ I) = (\text{sum-mat } A \ I) * B$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *trace-sum-mat-mat-distrib*:
assumes $\text{finite } I$
and $\bigwedge i. i \in I \implies B \ i \in \text{fc-mats}$
and $A \in \text{fc-mats}$
and $C \in \text{fc-mats}$
shows $(\sum_{i \in I. \text{Complex-Matrix.trace}(A * (B \ i) * C)) =$
 $\text{Complex-Matrix.trace}(A * (\text{sum-mat } B \ I) * C)$
 ⟨proof⟩

definition (in *cpx-sq-mat*) *zero-col* **where**
 $\text{zero-col } U = (\lambda i. \text{if } i < \text{dimR} \text{ then } \text{Matrix.col } U \ i \ \text{else } 0_v \ \text{dimR})$

lemma (in *cpx-sq-mat*) *zero-col-dim*:
assumes $U \in \text{fc-mats}$
shows $\text{dim-vec}(\text{zero-col } U \ i) = \text{dimR}$ ⟨proof⟩

lemma (in *cpx-sq-mat*) *zero-col-col*:
assumes $i < \text{dimR}$
shows $\text{zero-col } U \ i = \text{Matrix.col } U \ i$ ⟨proof⟩

lemma (in *cpx-sq-mat*) *sum-mat-index*:
shows $\text{finite } I \implies (\bigwedge i. i \in I \implies (A \ i) \in \text{fc-mats}) \implies i < \text{dimR} \implies j < \text{dimC}$
 \implies
 $(\text{sum-mat } (\lambda k. (A \ k)) \ I) \ \text{\$ \$ } (i,j) = (\sum_{k \in I. (A \ k) \ \text{\$ \$ } (i,j))$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *sum-mat-cong*:
shows $\text{finite } I \implies (\bigwedge i. i \in I \implies A \ i = B \ i) \implies (\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}) \implies$
 $(\bigwedge i. i \in I \implies B \ i \in \text{fc-mats}) \implies \text{sum-mat } A \ I = \text{sum-mat } B \ I$
 <proof>

lemma (in *cpx-sq-mat*) *smult-sum-mat*:
shows $\text{finite } I \implies (\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}) \implies a \cdot_m \text{sum-mat } A \ I =$
 $\text{sum-mat } (\lambda i. a \cdot_m (A \ i)) \ I$
 <proof>

lemma (in *cpx-sq-mat*) *zero-sum-mat*:
shows $\text{finite } I \implies \text{sum-mat } (\lambda i. ((0_m \ \text{dim}R \ \text{dim}R)::\text{complex Matrix.mat})) \ I =$
 $((0_m \ \text{dim}R \ \text{dim}R)::\text{complex Matrix.mat})$
 <proof>

lemma (in *cpx-sq-mat*) *sum-mat-adjoint*:
shows $\text{finite } I \implies (\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}) \implies$
 $\text{Complex-Matrix.adjoint } (\text{sum-mat } A \ I) = \text{sum-mat } (\lambda i. \text{Complex-Matrix.adjoint } (A \ i)) \ I$
 <proof>

lemma (in *cpx-sq-mat*) *sum-mat-hermitian*:
assumes *finite I*
and $\forall i \in I. \text{hermitian } (A \ i)$
and $\forall i \in I. A \ i \in \text{fc-mats}$
shows $\text{hermitian } (\text{sum-mat } A \ I)$
 <proof>

lemma (in *cpx-sq-mat*) *sum-mat-positive*:
shows $\text{finite } I \implies (\bigwedge i. i \in I \implies \text{Complex-Matrix.positive } (A \ i)) \implies$
 $(\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}) \implies \text{Complex-Matrix.positive } (\text{sum-mat } A \ I)$
 <proof>

lemma (in *cpx-sq-mat*) *sum-mat-left-ortho-zero*:
shows $\text{finite } I \implies$
 $(\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}) \implies (B \in \text{fc-mats}) \implies$
 $(\bigwedge i. i \in I \implies A \ i * B = (0_m \ \text{dim}R \ \text{dim}R)) \implies$
 $(\text{sum-mat } A \ I) * B = 0_m \ \text{dim}R \ \text{dim}R$
 <proof>

lemma (in *cpx-sq-mat*) *sum-mat-right-ortho-zero*:
shows $\text{finite } I \implies$
 $(\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}) \implies (B \in \text{fc-mats}) \implies$
 $(\bigwedge i. i \in I \implies B * A \ i = (0_m \ \text{dim}R \ \text{dim}R)) \implies$
 $B * (\text{sum-mat } A \ I) = 0_m \ \text{dim}R \ \text{dim}R$
 <proof>

lemma (in *cpx-sq-mat*) *sum-mat-ortho-square*:

shows $finite\ I \implies (\bigwedge i. i \in I \implies ((A\ i)::complex\ Matrix.mat) * (A\ i) = A\ i)$
 \implies
 $(\bigwedge i. i \in I \implies A\ i \in fc\ mats) \implies$
 $(\bigwedge i\ j. i \in I \implies j \in I \implies i \neq j \implies A\ i * (A\ j) = (0_m\ dimR\ dimR)) \implies$
 $(sum\ mat\ A\ I) * (sum\ mat\ A\ I) = (sum\ mat\ A\ I)$
 $\langle proof \rangle$

lemma *diagonal-unit-vec*:

assumes $B \in carrier\ mat\ n\ n$
and *diagonal-mat* $(B::complex\ Matrix.mat)$
shows $B *_v (unit\ vec\ n\ i) = B \$\$ (i,i) \cdot_v (unit\ vec\ n\ i)$
 $\langle proof \rangle$

lemma *mat-vec-mult-assoc*:

assumes $A \in carrier\ mat\ n\ p$
and $B \in carrier\ mat\ p\ q$
and *dim-vec* $v = q$
shows $A *_v (B *_v v) = (A * B) *_v v$ $\langle proof \rangle$

lemma (**in** *cpx-sq-mat*) *similar-eigenvectors*:

assumes $A \in fc\ mats$
and $B \in fc\ mats$
and $P \in fc\ mats$
and *similar-mat-wit* $A\ B\ P$ (*Complex-Matrix.adjoint* P)
and *diagonal-mat* B
and $i < n$
shows $A *_v (P *_v (unit\ vec\ dimR\ i)) = B \$\$ (i,i) \cdot_v (P *_v (unit\ vec\ dimR\ i))$
 $\langle proof \rangle$

2.6 Projectors

definition *projector* **where**

projector $M \iff (hermitian\ M \wedge M * M = M)$

lemma *projector-hermitian*:

assumes *projector* M
shows *hermitian* M $\langle proof \rangle$

lemma *zero-projector[simp]*:

shows *projector* $(0_m\ n\ n)$ $\langle proof \rangle$

lemma *projector-square-eq*:

assumes *projector* M
shows $M * M = M$ $\langle proof \rangle$

lemma *projector-positive*:

assumes *projector* M
shows *Complex-Matrix.positive* M
 $\langle proof \rangle$

lemma *projector-collapse-trace*:
assumes *projector* ($P::\text{complex Matrix.mat}$)
and $P \in \text{carrier-mat } n \ n$
and $R \in \text{carrier-mat } n \ n$
shows $\text{Complex-Matrix.trace } (P * R * P) = \text{Complex-Matrix.trace } (R * P)$
 $\langle \text{proof} \rangle$

lemma *positive-proj-trace*:
assumes *projector* ($P::\text{complex Matrix.mat}$)
and $\text{Complex-Matrix.positive } R$
and $P \in \text{carrier-mat } n \ n$
and $R \in \text{carrier-mat } n \ n$
shows $\text{Complex-Matrix.trace } (R * P) \geq 0$
 $\langle \text{proof} \rangle$

lemma *trace-proj-pos-real*:
assumes *projector* ($P::\text{complex Matrix.mat}$)
and $\text{Complex-Matrix.positive } R$
and $P \in \text{carrier-mat } n \ n$
and $R \in \text{carrier-mat } n \ n$
shows $\text{Re } (\text{Complex-Matrix.trace } (R * P)) = \text{Complex-Matrix.trace } (R * P)$
 $\langle \text{proof} \rangle$

lemma (**in** *cpx-sq-mat*) *trace-sum-mat-proj-pos-real*:
fixes $f::'a \Rightarrow \text{real}$
assumes *finite* I
and $\forall i \in I. \text{projector } (P \ i)$
and $\text{Complex-Matrix.positive } R$
and $\forall i \in I. P \ i \in \text{fc-mats}$
and $R \in \text{fc-mats}$
shows $\text{Complex-Matrix.trace } (R * (\text{sum-mat } (\lambda i. f \ i \cdot_m (P \ i)) \ I)) =$
 $\text{Re } (\text{Complex-Matrix.trace } (R * (\text{sum-mat } (\lambda i. f \ i \cdot_m (P \ i)) \ I)))$
 $\langle \text{proof} \rangle$

2.7 Rank 1 projection

definition *rank-1-proj* **where**
 $\text{rank-1-proj } v = \text{outer-prod } v \ v$

lemma *rank-1-proj-square-mat*:
shows $\text{square-mat } (\text{rank-1-proj } v) \langle \text{proof} \rangle$

lemma *rank-1-proj-dim[simp]*:
shows $\text{dim-row } (\text{rank-1-proj } v) = \text{dim-vec } v \langle \text{proof} \rangle$

lemma *rank-1-proj-carrier[simp]*:
shows $\text{rank-1-proj } v \in \text{carrier-mat } (\text{dim-vec } v) \ (\text{dim-vec } v) \langle \text{proof} \rangle$

lemma *rank-1-proj-coord*:

assumes $i < \dim\text{-vec } v$

and $j < \dim\text{-vec } v$

shows $(\text{rank-1-proj } v) \text{ \#\# } (i, j) = \text{Matrix.vec-index } v \ i * (\text{cnj } (\text{Matrix.vec-index } v \ j))$ $\langle \text{proof} \rangle$

lemma *rank-1-proj-adjoint*:

shows $\text{Complex-Matrix.adjoint } (\text{rank-1-proj } (v::\text{complex Matrix.vec})) = \text{rank-1-proj } v$
 $\langle \text{proof} \rangle$

lemma *rank-1-proj-hermitian*:

shows $\text{hermitian } (\text{rank-1-proj } (v::\text{complex Matrix.vec}))$ $\langle \text{proof} \rangle$

lemma *rank-1-proj-trace*:

assumes $\|v\| = 1$

shows $\text{Complex-Matrix.trace } (\text{rank-1-proj } v) = 1$
 $\langle \text{proof} \rangle$

lemma *rank-1-proj-mat-col*:

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

and $i < n$

and $j < n$

and $k < n$

shows $(\text{rank-1-proj } (\text{Matrix.col } A \ i)) \text{ \#\# } (j, k) = A \text{ \#\# } (j, i) * \text{conjugate } (A \text{ \#\# } (k, i))$
 $\langle \text{proof} \rangle$

lemma (**in** *cpx-sq-mat*) *weighted-sum-rank-1-proj-unitary-index*:

assumes $A \in \text{fc-mats}$

and $B \in \text{fc-mats}$

and *diagonal-mat* B

and *Complex-Matrix.unitary* A

and $j < \dim R$

and $k < \dim R$

shows $(\text{sum-mat } (\lambda i. (\text{diag-mat } B)!i \cdot_m \text{rank-1-proj } (\text{Matrix.col } A \ i)) \{.. < \dim R\}) \text{ \#\# } (j, k) =$
 $(A * B * (\text{Complex-Matrix.adjoint } A)) \text{ \#\# } (j, k)$
 $\langle \text{proof} \rangle$

lemma (**in** *cpx-sq-mat*) *weighted-sum-rank-1-proj-unitary*:

assumes $A \in \text{fc-mats}$

and $B \in \text{fc-mats}$

and *diagonal-mat* B

and *Complex-Matrix.unitary* A

shows $(\text{sum-mat } (\lambda i. (\text{diag-mat } B)!i \cdot_m \text{rank-1-proj } (\text{Matrix.col } A \ i)) \{.. < \dim R\}) =$
 $(A * B * (\text{Complex-Matrix.adjoint } A))$
 $\langle \text{proof} \rangle$

lemma *rank-1-proj-projector*:
assumes $\|v\| = 1$
shows *projector* (*rank-1-proj* v)
 \langle *proof* \rangle

lemma *rank-1-proj-positive*:
assumes $\|v\| = 1$
shows *Complex-Matrix.positive* (*rank-1-proj* v)
 \langle *proof* \rangle

lemma *rank-1-proj-density*:
assumes $\|v\| = 1$
shows *density-operator* (*rank-1-proj* v) \langle *proof* \rangle

lemma (**in** *cpx-sq-mat*) *sum-rank-1-proj-unitary-index*:
assumes $A \in$ *fc-mats*
and *Complex-Matrix.unitary* A
and $j < \dim R$
and $k < \dim R$
shows (*sum-mat* ($\lambda i.$ *rank-1-proj* (*Matrix.col* A i)) $\{.. < \dim R\}$) $\$\$$ (j, k) = (1_m $\dim R$) $\$\$$ (j, k)
 \langle *proof* \rangle

lemma (**in** *cpx-sq-mat*) *rank-1-proj-sum-density*:
assumes *finite* I
and $\forall i \in I. \|u\ i\| = 1$
and $\forall i \in I. \dim\text{-vec}$ (u i) = $\dim R$
and $\forall i \in I. 0 \leq p\ i$
and ($\sum i \in I. p\ i$) = 1
shows *density-operator* (*sum-mat* ($\lambda i. p\ i \cdot_m$ (*rank-1-proj* ($u\ i$))) I) \langle *proof* \rangle

lemma (**in** *cpx-sq-mat*) *sum-rank-1-proj-unitary*:
assumes $A \in$ *fc-mats*
and *Complex-Matrix.unitary* A
shows (*sum-mat* ($\lambda i.$ *rank-1-proj* (*Matrix.col* A i)) $\{.. < \dim R\}$) = (1_m $\dim R$)
 \langle *proof* \rangle

lemma (**in** *cpx-sq-mat*) *rank-1-proj-unitary*:
assumes $A \in$ *fc-mats*
and *Complex-Matrix.unitary* A
and $j < \dim R$
and $k < \dim R$
shows *rank-1-proj* (*Matrix.col* A j) * (*rank-1-proj* (*Matrix.col* A k)) =
(1_m $\dim R$) $\$\$$ (j, k) \cdot_m (*outer-prod* (*Matrix.col* A j) (*Matrix.col* A k))
 \langle *proof* \rangle

```

lemma (in cpx-sq-mat) rank-1-proj-unitary-ne:
  assumes  $A \in \text{fc-mats}$ 
and Complex-Matrix.unitary  $A$ 
and  $j < \text{dim}R$ 
and  $k < \text{dim}R$ 
and  $j \neq k$ 
shows  $\text{rank-1-proj } (\text{Matrix.col } A \ j) * (\text{rank-1-proj } (\text{Matrix.col } A \ k)) = (0_m \ \text{dim}R \ \text{dim}R)$ 
  <proof>

```

```

lemma (in cpx-sq-mat) rank-1-proj-unitary-eq:
  assumes  $A \in \text{fc-mats}$ 
and Complex-Matrix.unitary  $A$ 
and  $j < \text{dim}R$ 
shows  $\text{rank-1-proj } (\text{Matrix.col } A \ j) * (\text{rank-1-proj } (\text{Matrix.col } A \ j)) = \text{rank-1-proj } (\text{Matrix.col } A \ j)$ 
  <proof>

```

end

```

theory Projective-Measurements imports
  Linear-Algebra-Complements

```

begin

3 Projective measurements

In this part we define projective measurements, also referred to as von Neumann measurements. The latter are characterized by a set of orthogonal projectors, which are used to compute the probabilities of measure outcomes and to represent the state of the system after the measurement.

The state of the system (a density operator in this case) after a measurement is represented by the `density_collapse` function.

3.1 First definitions

We begin by defining a type synonym for couples of measurement values (reals) and the associated projectors (complex matrices).

```

type-synonym measure-outcome = real  $\times$  complex Matrix.mat

```

The corresponding values and projectors are retrieved thanks to `meas_outcome_val` and `meas_outcome_prj`.

```

definition meas-outcome-val::measure-outcome  $\Rightarrow$  real where

```

$meas\text{-}outcome\text{-}val\ Mi = fst\ Mi$

definition $meas\text{-}outcome\text{-}prj::measure\text{-}outcome \Rightarrow complex\ Matrix.mat$ **where**
 $meas\text{-}outcome\text{-}prj\ Mi = snd\ Mi$

We define a predicate for projective measurements. A projective measurement is characterized by the number p of possible measure outcomes, and a function M mapping outcome i to the corresponding `measure_outcome`.

definition (in $cpx\text{-}sq\text{-}mat$) $proj\text{-}measurement::nat \Rightarrow (nat \Rightarrow measure\text{-}outcome) \Rightarrow bool$ **where**

$proj\text{-}measurement\ n\ M \longleftrightarrow$
 $(inj\text{-}on\ (\lambda i. meas\text{-}outcome\text{-}val\ (M\ i))\ \{..<\ n\}) \wedge$
 $(\forall j < n. meas\text{-}outcome\text{-}prj\ (M\ j) \in fc\text{-}mats \wedge$
 $projector\ (meas\text{-}outcome\text{-}prj\ (M\ j))) \wedge$
 $(\forall i < n. \forall j < n. i \neq j \longrightarrow$
 $meas\text{-}outcome\text{-}prj\ (M\ i) * meas\text{-}outcome\text{-}prj\ (M\ j) = 0_m\ dimR\ dimR) \wedge$
 $sum\text{-}mat\ (\lambda j. meas\text{-}outcome\text{-}prj\ (M\ j))\ \{..<\ n\} = 1_m\ dimR$

lemma (in $cpx\text{-}sq\text{-}mat$) $proj\text{-}measurement\text{-}inj$:
assumes $proj\text{-}measurement\ p\ M$
shows $inj\text{-}on\ (\lambda i. meas\text{-}outcome\text{-}val\ (M\ i))\ \{..<\ p\} \langle proof \rangle$

lemma (in $cpx\text{-}sq\text{-}mat$) $proj\text{-}measurement\text{-}carrier$:
assumes $proj\text{-}measurement\ p\ M$
and $i < p$
shows $meas\text{-}outcome\text{-}prj\ (M\ i) \in fc\text{-}mats \langle proof \rangle$

lemma (in $cpx\text{-}sq\text{-}mat$) $proj\text{-}measurement\text{-}ortho$:
assumes $proj\text{-}measurement\ p\ M$
and $i < p$
and $j < p$
and $i \neq j$
shows $meas\text{-}outcome\text{-}prj\ (M\ i) * meas\text{-}outcome\text{-}prj\ (M\ j) = 0_m\ dimR\ dimR$
 $\langle proof \rangle$

lemma (in $cpx\text{-}sq\text{-}mat$) $proj\text{-}measurement\text{-}id$:
assumes $proj\text{-}measurement\ p\ M$
shows $sum\text{-}mat\ (\lambda j. meas\text{-}outcome\text{-}prj\ (M\ j))\ \{..<\ p\} = 1_m\ dimR \langle proof \rangle$

lemma (in $cpx\text{-}sq\text{-}mat$) $proj\text{-}measurement\text{-}square$:
assumes $proj\text{-}measurement\ p\ M$
and $i < p$
shows $meas\text{-}outcome\text{-}prj\ (M\ i) \in fc\text{-}mats \langle proof \rangle$

lemma (in $cpx\text{-}sq\text{-}mat$) $proj\text{-}measurement\text{-}proj$:
assumes $proj\text{-}measurement\ p\ M$
and $i < p$
shows $projector\ (meas\text{-}outcome\text{-}prj\ (M\ i)) \langle proof \rangle$

We define the probability of obtaining a measurement outcome: this is a positive number and the sum over all the measurement outcomes is 1.

definition (in *cpx-sq-mat*) *meas-outcome-prob* :: *complex Matrix.mat* \Rightarrow
*(nat \Rightarrow real \times complex Matrix.mat) \Rightarrow nat \Rightarrow complex **where**
meas-outcome-prob *R M i* = *Complex-Matrix.trace* (*R** (*meas-outcome-prj* (*M i*)))*

lemma (in *cpx-sq-mat*) *meas-outcome-prob-real*:

assumes *R* \in *fc-mats*

and *density-operator* *R*

and *proj-measurement* *n M*

and *i* < *n*

shows *meas-outcome-prob* *R M i* \in \mathbb{R}

<proof>

lemma (in *cpx-sq-mat*) *meas-outcome-prob-pos*:

assumes *R* \in *fc-mats*

and *density-operator* *R*

and *proj-measurement* *n M*

and *i* < *n*

shows $0 \leq$ *meas-outcome-prob* *R M i* *<proof>*

lemma (in *cpx-sq-mat*) *meas-outcome-prob-sum*:

assumes *density-operator* *R*

and *R* \in *fc-mats*

and *proj-measurement* *n M*

shows ($\sum j \in \{..< n\}$. *meas-outcome-prob* *R M j*) = 1

<proof>

We introduce the maximally mixed density operator. Intuitively, this density operator corresponds to a uniform distribution of the states of an orthonormal basis. This operator will be used to define the density operator after a measurement for the measure outcome probabilities equal to zero.

definition *max-mix-density* :: *nat* \Rightarrow *complex Matrix.mat* **where**

max-mix-density *n* = ((1::real)/ *n*) \cdot_m (1_{*m*} *n*)

lemma *max-mix-density-carrier*:

shows *max-mix-density* *n* \in *carrier-mat* *n n* *<proof>*

lemma *max-mix-is-density*:

assumes $0 < n$

shows *density-operator* (*max-mix-density* *n*) *<proof>*

lemma (in *cpx-sq-mat*) *max-mix-density-square*:

shows *max-mix-density* *dimR* \in *fc-mats* *<proof>*

Given a measurement outcome, `density_collapse` represents the resulting density operator. In practice only the measure outcomes with nonzero probabilities are of interest; we (arbitrarily) collapse the density operator

for zero-probability outcomes to the maximally mixed density operator.

definition *density-collapse* :: *complex Matrix.mat* \Rightarrow *complex Matrix.mat* \Rightarrow *complex Matrix.mat* **where**
density-collapse $R P =$ (if ((*Complex-Matrix.trace* ($R * P$)) = 0) then (*max-mix-density* (*dim-row* R))
 else ((1::real) / ((*Complex-Matrix.trace* ($R * P$)))) \cdot_m ($P * R * P$))

lemma *density-collapse-carrier*:
assumes $0 < \text{dim-row } R$
and $P \in \text{carrier-mat } n \ n$
and $R \in \text{carrier-mat } n \ n$
shows (*density-collapse* $R P$) $\in \text{carrier-mat } n \ n$
 $\langle \text{proof} \rangle$

lemma *density-collapse-operator*:
assumes *projector* P
and *density-operator* R
and $0 < \text{dim-row } R$
and $P \in \text{carrier-mat } n \ n$
and $R \in \text{carrier-mat } n \ n$
shows *density-operator* (*density-collapse* $R P$)
 $\langle \text{proof} \rangle$

3.2 Measurements with observables

It is standard in quantum mechanics to represent projective measurements with so-called *observables*. These are Hermitian matrices which encode projective measurements as follows: the eigenvalues of an observable represent the possible projective measurement outcomes, and the associated projectors are the projectors onto the corresponding eigenspaces. The results in this part are based on the spectral theorem, which states that any Hermitian matrix admits an orthonormal basis consisting of eigenvectors of the matrix.

3.2.1 On the diagonal elements of a matrix

We begin by introducing definitions that will be used on the diagonalized version of a Hermitian matrix.

definition *diag-elems* **where**
diag-elems $B = \{B_{(i,i)} \mid i. i < \text{dim-row } B\}$

Relationship between *diag_elems* and the list *diag_mat*

lemma *diag-elems-set-diag-mat*:
shows *diag-elems* $B = \text{set } (\text{diag-mat } B)$ $\langle \text{proof} \rangle$

lemma *diag-elems-finite[simp]*:
shows *finite* (*diag-elems* B) $\langle \text{proof} \rangle$

lemma *diag-elems-mem*[simp]:
assumes $i < \text{dim-row } B$
shows $B \$(i,i) \in \text{diag-elems } B$ $\langle \text{proof} \rangle$

When x is a diagonal element of B , `diag_elem_indices` returns the set of diagonal indices of B with value x .

definition *diag-elem-indices* **where**
 $\text{diag-elem-indices } x \ B = \{i \mid i. i < \text{dim-row } B \wedge B \$(i,i) = x\}$

lemma *diag-elem-indices-elem*:
assumes $a \in \text{diag-elem-indices } x \ B$
shows $a < \text{dim-row } B \wedge B \$(a,a) = x$ $\langle \text{proof} \rangle$

lemma *diag-elem-indices-itself*:
assumes $i < \text{dim-row } B$
shows $i \in \text{diag-elem-indices } (B \$(i,i)) \ B$ $\langle \text{proof} \rangle$

lemma *diag-elem-indices-finite*:
shows *finite* $(\text{diag-elem-indices } x \ B)$ $\langle \text{proof} \rangle$

We can therefore partition the diagonal indices of a matrix B depending on the value of the diagonal elements. If B admits p elements on its diagonal, then we define bijections between its set of diagonal elements and the initial segment $[0..p - 1]$.

definition *dist-el-card* **where**
 $\text{dist-el-card } B = \text{card } (\text{diag-elems } B)$

definition *diag-idx-to-el* **where**
 $\text{diag-idx-to-el } B = (\text{SOME } h. \text{bij-betw } h \ \{.. < \text{dist-el-card } B\} \ (\text{diag-elems } B))$

definition *diag-el-to-idx* **where**
 $\text{diag-el-to-idx } B = \text{inv-into } \{.. < \text{dist-el-card } B\} \ (\text{diag-idx-to-el } B)$

lemma *diag-idx-to-el-bij*:
shows *bij-betw* $(\text{diag-idx-to-el } B) \ \{.. < \text{dist-el-card } B\} \ (\text{diag-elems } B)$
 $\langle \text{proof} \rangle$

lemma *diag-el-to-idx-bij*:
shows *bij-betw* $(\text{diag-el-to-idx } B) \ (\text{diag-elems } B) \ \{.. < \text{dist-el-card } B\}$
 $\langle \text{proof} \rangle$

lemma *diag-idx-to-el-less-inj*:
assumes $i < \text{dist-el-card } B$
and $j < \text{dist-el-card } B$
and $\text{diag-idx-to-el } B \ i = \text{diag-idx-to-el } B \ j$
shows $i = j$
 $\langle \text{proof} \rangle$

lemma *diag-idx-to-el-less-surj*:
assumes $x \in \text{diag-elems } B$
shows $\exists k \in \{.. < \text{dist-el-card } B\}. x = \text{diag-idx-to-el } B \ k$
 $\langle \text{proof} \rangle$

lemma *diag-idx-to-el-img*:
assumes $k < \text{dist-el-card } B$
shows $\text{diag-idx-to-el } B \ k \in \text{diag-elems } B$
 $\langle \text{proof} \rangle$

lemma *diag-elems-real*:
fixes $B :: \text{complex Matrix.mat}$
assumes $\forall i < \text{dim-row } B. B\$\$(i,i) \in \text{Reals}$
shows $\text{diag-elems } B \subseteq \text{Reals}$
 $\langle \text{proof} \rangle$

lemma *diag-elems-Re*:
fixes $B :: \text{complex Matrix.mat}$
assumes $\forall i < (\text{dim-row } B). B\$\$(i,i) \in \text{Reals}$
shows $\{\text{Re } x \mid x. x \in \text{diag-elems } B\} = \text{diag-elems } B$
 $\langle \text{proof} \rangle$

lemma *diag-idx-to-el-real*:
fixes $B :: \text{complex Matrix.mat}$
assumes $\forall i < \text{dim-row } B. B\$\$(i,i) \in \text{Reals}$
and $i < \text{dist-el-card } B$
shows $\text{Re } (\text{diag-idx-to-el } B \ i) = \text{diag-idx-to-el } B \ i$
 $\langle \text{proof} \rangle$

lemma *diag-elem-indices-empty*:
assumes $B \in \text{carrier-mat } \text{dimR } \text{dimC}$
and $i < (\text{dist-el-card } B)$
and $j < (\text{dist-el-card } B)$
and $i \neq j$
shows $\text{diag-elem-indices } (\text{diag-idx-to-el } B \ i) \ B \cap$
 $(\text{diag-elem-indices } (\text{diag-idx-to-el } B \ j) \ B) = \{\}$
 $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *diag-elem-indices-disjoint*:
assumes $B \in \text{carrier-mat } \text{dimR } \text{dimC}$
shows *disjoint-family-on* $(\lambda n. \text{diag-elem-indices } (\text{diag-idx-to-el } B \ n) \ B)$
 $\{.. < \text{dist-el-card } B\} \langle \text{proof} \rangle$

lemma *diag-elem-indices-union*:
assumes $B \in \text{carrier-mat } \text{dimR } \text{dimC}$
shows $(\bigcup i \in \{.. < \text{dist-el-card } B\}. \text{diag-elem-indices } (\text{diag-idx-to-el } B \ i) \ B) =$
 $\{.. < \text{dimR}\}$
 $\langle \text{proof} \rangle$

3.2.2 Construction of measurement outcomes

The construction of a projective measurement for a hermitian matrix A is based on the Schur decomposition $A = U * B * U^\dagger$, where B is diagonal and U is unitary. The columns of U are normalized and pairwise orthogonal; they are used to construct the projectors associated with a measurement value

definition (in *cpx-sq-mat*) *project-vecs* **where**
project-vecs ($f :: \text{nat} \Rightarrow \text{complex Matrix.vec}$) $N = \text{sum-mat } (\lambda i. \text{rank-1-proj } (f i)) N$

lemma (in *cpx-sq-mat*) *project-vecs-dim*:
assumes $\forall i \in N. \text{dim-vec } (f i) = \text{dimR}$
shows *project-vecs* $f N \in \text{fc-mats}$
<proof>

definition (in *cpx-sq-mat*) *mk-meas-outcome* **where**
mk-meas-outcome $B U = (\lambda i. (\text{Re } (\text{diag-idx-to-el } B i),$
project-vecs $(\lambda i. \text{zero-col } U i) (\text{diag-elem-indices } (\text{diag-idx-to-el } B i) B)))$

lemma (in *cpx-sq-mat*) *mk-meas-outcome-carrier*:
assumes *Complex-Matrix.unitary* U
and $U \in \text{fc-mats}$
and $B \in \text{fc-mats}$
shows *meas-outcome-prj* $((\text{mk-meas-outcome } B U) j) \in \text{fc-mats}$
<proof>

lemma (in *cpx-sq-mat*) *mk-meas-outcome-sum-id*:
assumes *Complex-Matrix.unitary* U
and $U \in \text{fc-mats}$
and $B \in \text{fc-mats}$
shows *sum-mat* $(\lambda j. \text{meas-outcome-prj } ((\text{mk-meas-outcome } B U) j))$
 $\{.. <(\text{dist-el-card } B)\} = 1_m \text{dimR}$
<proof>

lemma (in *cpx-sq-mat*) *make-meas-outcome-prj-ortho*:
assumes *Complex-Matrix.unitary* U
and $U \in \text{fc-mats}$
and $B \in \text{fc-mats}$
and $i < \text{dist-el-card } B$
and $j < \text{dist-el-card } B$
and $i \neq j$
shows *meas-outcome-prj* $((\text{mk-meas-outcome } B U) i) *$
meas-outcome-prj $((\text{mk-meas-outcome } B U) j) = 0_m \text{dimR dimR}$
<proof>

lemma (in *cpx-sq-mat*) *make-meas-outcome-projectors*:
assumes *Complex-Matrix.unitary* U
and $U \in \text{fc-mats}$

and $B \in \text{fc-mats}$
and $j < \text{dist-el-card } B$
shows $\text{projector } (\text{meas-outcome-prj } ((\text{mk-meas-outcome } B \ U) \ j)) \langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) $\text{mk-meas-outcome-fst-inj}$:
assumes $\forall i < (\text{dim-row } B). B\$(i,i) \in \text{Reals}$
shows $\text{inj-on } (\lambda i. \text{meas-outcome-val } ((\text{mk-meas-outcome } B \ U) \ i)) \{.. < \text{dist-el-card } B\}$
 $\langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) $\text{mk-meas-outcome-fst-bij}$:
assumes $\forall i < (\text{dim-row } B). B\$(i,i) \in \text{Reals}$
shows $\text{bij-betw } (\lambda i. \text{meas-outcome-val } ((\text{mk-meas-outcome } B \ U) \ i)) \{.. < \text{dist-el-card } B\}$
 $\{\text{Re } x \mid x. x \in \text{diag-elems } B\}$
 $\langle \text{proof} \rangle$

3.2.3 Projective measurement associated with an observable

definition eigvals where
 $\text{eigvals } M = (\text{SOME } as. \text{char-poly } M = (\prod a \leftarrow as. [:- a, 1:]) \wedge \text{length } as = \text{dim-row } M)$

lemma $\text{eigvals-poly-length}$:
assumes $(M :: \text{complex Matrix.mat}) \in \text{carrier-mat } n \ n$
shows $\text{char-poly } M = (\prod a \leftarrow (\text{eigvals } M). [:- a, 1:]) \wedge \text{length } (\text{eigvals } M) = \text{dim-row } M$
 $\langle \text{proof} \rangle$

We define the spectrum of a matrix A : this is its set of eigenvalues; its elements are roots of the characteristic polynomial of A .

definition spectrum where
 $\text{spectrum } M = \text{set } (\text{eigvals } M)$

lemma spectrum-finite :
shows $\text{finite } (\text{spectrum } M) \langle \text{proof} \rangle$

lemma $\text{spectrum-char-poly-root}$:
fixes $A :: \text{complex Matrix.mat}$
assumes $A \in \text{carrier-mat } n \ n$
and $k \in \text{spectrum } A$
shows $\text{poly } (\text{char-poly } A) \ k = 0 \langle \text{proof} \rangle$

lemma $\text{spectrum-eigenvalues}$:
fixes $A :: \text{complex Matrix.mat}$
assumes $A \in \text{carrier-mat } n \ n$
and $k \in \text{spectrum } A$
shows $\text{eigenvalue } A \ k \langle \text{proof} \rangle$

The main result that is used to construct a projective measurement for

a Hermitian matrix is that it is always possible to decompose it as $A = U * B * U^\dagger$, where B is diagonal and only contains real elements, and U is unitary.

definition *hermitian-decomp* **where**

hermitian-decomp $A B U \equiv \text{similar-mat-wit } A B U \text{ (Complex-Matrix.adjoint } U)$
 $\wedge \text{diagonal-mat } B \wedge$
 $\text{diag-mat } B = (\text{eigvals } A) \wedge \text{unitary } U \wedge (\forall i < \text{dim-row } B. B\$(i, i) \in \text{Reals})$

lemma *hermitian-decomp-sim*:

assumes *hermitian-decomp* $A B U$

shows *similar-mat-wit* $A B U \text{ (Complex-Matrix.adjoint } U)$ $\langle \text{proof} \rangle$

lemma *hermitian-decomp-diag-mat*:

assumes *hermitian-decomp* $A B U$

shows *diagonal-mat* $B \langle \text{proof} \rangle$

lemma *hermitian-decomp-eigenvalues*:

assumes *hermitian-decomp* $A B U$

shows *diag-mat* $B = (\text{eigvals } A) \langle \text{proof} \rangle$

lemma *hermitian-decomp-unitary*:

assumes *hermitian-decomp* $A B U$

shows *unitary* $U \langle \text{proof} \rangle$

lemma *hermitian-decomp-real-eigvals*:

assumes *hermitian-decomp* $A B U$

shows $\forall i < \text{dim-row } B. B\$(i, i) \in \text{Reals} \langle \text{proof} \rangle$

lemma *hermitian-decomp-dim-carrier*:

assumes *hermitian-decomp* $A B U$

shows $B \in \text{carrier-mat } (\text{dim-row } A) (\text{dim-col } A) \langle \text{proof} \rangle$

lemma *similar-mat-wit-dim-row*:

assumes *similar-mat-wit* $A B Q R$

shows $\text{dim-row } B = \text{dim-row } A \langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *hermitian-schur-decomp*:

assumes *hermitian* A

and $A \in \text{fc-mats}$

obtains $B U$ **where** *hermitian-decomp* $A B U$
 $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *hermitian-spectrum-real*:

assumes $A \in \text{fc-mats}$

and *hermitian* A

and $a \in \text{spectrum } A$

shows $a \in \text{Reals}$
 $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *spectrum-ne*:
assumes $A \in \text{fc-mats}$
and *hermitian* A
shows $\text{spectrum } A \neq \{\}$
 $\langle \text{proof} \rangle$

lemma *unitary-hermitian-eigenvalues*:
fixes $U :: \text{complex Matrix.mat}$
assumes *unitary* U
and *hermitian* U
and $U \in \text{carrier-mat } n \ n$
and $0 < n$
and $k \in \text{spectrum } U$
shows $k \in \{-1, 1\}$
 $\langle \text{proof} \rangle$

lemma *unitary-hermitian-Re-spectrum*:
fixes $U :: \text{complex Matrix.mat}$
assumes *unitary* U
and *hermitian* U
and $U \in \text{carrier-mat } n \ n$
and $0 < n$
shows $\{\text{Re } x \mid x \in \text{spectrum } U\} \subseteq \{-1, 1\}$
 $\langle \text{proof} \rangle$

The projective measurement associated with matrix M is obtained from its Schur decomposition, by considering the number of distinct elements on the resulting diagonal matrix and constructing the projectors associated with each of them.

type-synonym *proj-meas-rep* = $\text{nat} \times (\text{nat} \Rightarrow \text{measure-outcome})$

definition *proj-meas-size*::*proj-meas-rep* \Rightarrow *nat* **where**
proj-meas-size $P = \text{fst } P$

definition *proj-meas-outcomes*::*proj-meas-rep* \Rightarrow (*nat* \Rightarrow *measure-outcome*) **where**
proj-meas-outcomes $P = \text{snd } P$

definition (in *cpx-sq-mat*) *make-pm*::*complex Matrix.mat* \Rightarrow *proj-meas-rep* **where**
make-pm $A = (\text{let } (B, U, -) = \text{unitary-schur-decomposition } A \text{ (eigvals } A) \text{ in}$
 $(\text{dist-el-card } B, \text{mk-meas-outcome } B \ U))$

lemma (in *cpx-sq-mat*) *make-pm-decomp*:
shows *make-pm* $A = (\text{proj-meas-size } (\text{make-pm } A), \text{proj-meas-outcomes } (\text{make-pm } A))$
 $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *make-pm-proj-measurement*:
assumes $A \in \text{fc-mats}$
and *hermitian* A

and $\text{make-pm } A = (n, M)$
shows $\text{proj-measurement } n \ M$
 $\langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) $\text{make-pm-proj-measurement}'$:
assumes $A \in \text{fc-mats}$
and $\text{hermitian } A$
shows $\text{proj-measurement } (\text{proj-meas-size } (\text{make-pm } A)) (\text{proj-meas-outcomes } (\text{make-pm } A))$
 $\langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) $\text{make-pm-projectors}$:
assumes $A \in \text{fc-mats}$
and $\text{hermitian } A$
and $i < \text{proj-meas-size } (\text{make-pm } A)$
shows $\text{projector } (\text{meas-outcome-prj } (\text{proj-meas-outcomes } (\text{make-pm } A) \ i))$
 $\langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) make-pm-square :
assumes $A \in \text{fc-mats}$
and $\text{hermitian } A$
and $i < \text{proj-meas-size } (\text{make-pm } A)$
shows $\text{meas-outcome-prj } (\text{proj-meas-outcomes } (\text{make-pm } A) \ i) \in \text{fc-mats}$
 $\langle \text{proof} \rangle$

3.2.4 Properties on the spectrum of a Hermitian matrix

lemma (**in** cpx-sq-mat) $\text{hermitian-schur-decomp}'$:
assumes $\text{hermitian } A$
and $A \in \text{fc-mats}$
obtains $B \ U$ **where** $\text{hermitian-decomp } A \ B \ U \wedge$
 $\text{make-pm } A = (\text{dist-el-card } B, \text{mk-meas-outcome } B \ U)$
 $\langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) $\text{spectrum-meas-outcome-val-eq}$:
assumes $\text{hermitian } A$
and $A \in \text{fc-mats}$
and $\text{make-pm } A = (p, M)$
shows $\text{spectrum } A = (\lambda i. \text{meas-outcome-val } (M \ i)) \ \{.. < p\}$
 $\langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) $\text{spectrum-meas-outcome-val-eq}'$:
assumes $\text{hermitian } A$
and $A \in \text{fc-mats}$
and $\text{make-pm } A = (p, M)$
shows $\{\text{Re } x \mid x. x \in \text{spectrum } A\} = (\lambda i. \text{meas-outcome-val } (M \ i)) \ \{.. < p\}$
 $\langle \text{proof} \rangle$

lemma (**in** cpx-sq-mat) $\text{make-pm-eigenvalues}$:

assumes $A \in \text{fc-mats}$
and *hermitian* A
and $i < \text{proj-meas-size } (\text{make-pm } A)$
shows $\text{meas-outcome-val } (\text{proj-meas-outcomes } (\text{make-pm } A) i) \in \text{spectrum } A$
 ⟨*proof*⟩

lemma (*in cpx-sq-mat*) *make-pm-spectrum*:
assumes $A \in \text{fc-mats}$
and *hermitian* A
and $\text{make-pm } A = (p, M)$
shows $(\lambda i. \text{meas-outcome-val } (\text{proj-meas-outcomes } (\text{make-pm } A) i)) \text{ ‘ } \{.. < p\} = \text{spectrum } A$
 ⟨*proof*⟩

lemma (*in cpx-sq-mat*) *spectrum-size*:
assumes *hermitian* A
and $A \in \text{fc-mats}$
and $\text{make-pm } A = (p, M)$
shows $p = \text{card } (\text{spectrum } A)$
 ⟨*proof*⟩

lemma (*in cpx-sq-mat*) *spectrum-size'*:
assumes *hermitian* A
and $A \in \text{fc-mats}$
shows $\text{proj-meas-size } (\text{make-pm } A) = \text{card } (\text{spectrum } A)$ ⟨*proof*⟩

lemma (*in cpx-sq-mat*) *make-pm-projectors'*:
assumes *hermitian* A
and $A \in \text{fc-mats}$
and $a < \text{card } (\text{spectrum } A)$
shows $\text{projector } (\text{meas-outcome-prj } (\text{proj-meas-outcomes } (\text{make-pm } A) a))$
 ⟨*proof*⟩

lemma (*in cpx-sq-mat*) *meas-outcome-prj-carrier*:
assumes *hermitian* A
and $A \in \text{fc-mats}$
and $a < \text{card } (\text{spectrum } A)$
shows $\text{meas-outcome-prj } (\text{proj-meas-outcomes } (\text{make-pm } A) a) \in \text{fc-mats}$
 ⟨*proof*⟩

lemma (*in cpx-sq-mat*) *meas-outcome-prj-trace-real*:
assumes *hermitian* A
and *density-operator* R
and $R \in \text{fc-mats}$
and $A \in \text{fc-mats}$
and $a < \text{card } (\text{spectrum } A)$
shows $\text{Re } (\text{Complex-Matrix.trace } (R * \text{meas-outcome-prj } (\text{proj-meas-outcomes } (\text{make-pm } A) a))) =$
 $\text{Complex-Matrix.trace } (R * \text{meas-outcome-prj } (\text{proj-meas-outcomes } (\text{make-pm } A)$

a))
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *sum-over-spectrum*:
 assumes $A \in \text{fc-mats}$
 and *hermitian* A
 and *make-pm* $A = (p, M)$
 shows $(\sum y \in \text{spectrum } A. f y) = (\sum i < p. f (\text{meas-outcome-val } (M i)))$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *sum-over-spectrum'*:
 assumes $A \in \text{fc-mats}$
 and *hermitian* A
 and *make-pm* $A = (p, M)$
 shows $(\sum y \in \{\text{Re } x \mid x \in \text{spectrum } A\}. f y) = (\sum i < p. f (\text{meas-outcome-val } (M i)))$
 ⟨proof⟩

When a matrix A is decomposed into a projective measurement $\{(\lambda_a, \pi_a)\}$, it can be recovered by the formula $A = \sum \lambda_a \pi_a$.

lemma (in *cpx-sq-mat*) *make-pm-sum*:
 assumes $A \in \text{fc-mats}$
 and *hermitian* A
 and *make-pm* $A = (p, M)$
 shows $\text{sum-mat } (\lambda i. (\text{meas-outcome-val } (M i)) \cdot_m \text{meas-outcome-prj } (M i)) \{.. < p\} = A$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *trace-hermitian-pos-real*:
 fixes $f::'a \Rightarrow \text{real}$
 assumes *hermitian* A
 and *Complex-Matrix.positive* R
 and $A \in \text{fc-mats}$
 and $R \in \text{fc-mats}$
 shows *Complex-Matrix.trace* $(R * A) = \text{Re } (\text{Complex-Matrix.trace } (R * A))$
 ⟨proof⟩

lemma (in *cpx-sq-mat*) *hermitian-Re-spectrum*:
 assumes *hermitian* A
 and $A \in \text{fc-mats}$
 and $\{\text{Re } x \mid x \in \text{spectrum } A\} = \{a, b\}$
 shows $\text{spectrum } A = \{\text{complex-of-real } a, \text{complex-of-real } b\}$
 ⟨proof⟩

3.2.5 Similar properties for eigenvalues rather than spectrum indices

In this part we go the other way round: given an eigenvalue of A , `spectrum_to_pm_idx` permits to retrieve its index in the associated projective measurement

definition (in *cpx-sq-mat*) *spectrum-to-pm-idx*
where *spectrum-to-pm-idx* A $x = (\text{let } (B, U, -) = \text{unitary-schur-decomposition } A$
(eigvals $A)$ *in*
 $\text{diag-el-to-idx } B$ $x)$

lemma (in *cpx-sq-mat*) *spectrum-to-pm-idx-bij*:
assumes *hermitian* A
and $A \in \text{fc-mats}$
shows *bij-betw* (*spectrum-to-pm-idx* A) (*spectrum* A) $\{.. < \text{card } (\text{spectrum } A)\}$
 $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *spectrum-to-pm-idx-lt-card*:
assumes $A \in \text{fc-mats}$
and *hermitian* A
and $a \in \text{spectrum } A$
shows *spectrum-to-pm-idx* A $a < \text{card } (\text{spectrum } A)$ $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *spectrum-to-pm-idx-inj*:
assumes *hermitian* A
and $A \in \text{fc-mats}$
shows *inj-on* (*spectrum-to-pm-idx* A) (*spectrum* A) $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *spectrum-meas-outcome-val-inv*:
assumes $A \in \text{fc-mats}$
and *hermitian* A
and *make-pm* $A = (p, M)$
and $i < p$
shows *spectrum-to-pm-idx* A (*meas-outcome-val* (M i)) = i
 $\langle \text{proof} \rangle$

lemma (in *cpx-sq-mat*) *meas-outcome-val-spectrum-inv*:
assumes $A \in \text{fc-mats}$
and *hermitian* A
and $x \in \text{spectrum } A$
and *make-pm* $A = (p, M)$
shows *meas-outcome-val* (M (*spectrum-to-pm-idx* A x)) = x
 $\langle \text{proof} \rangle$

definition (in *cpx-sq-mat*) *eigen-projector* **where**
eigen-projector A $a =$
 $\text{meas-outcome-prj } ((\text{proj-meas-outcomes } (\text{make-pm } A)) (\text{spectrum-to-pm-idx } A$ $a))$

lemma (in *cpx-sq-mat*) *eigen-projector-carrier*:
assumes $A \in \text{fc-mats}$

and $a \in \text{spectrum } A$
and *hermitian* A
shows *eigen-projector* A $a \in \text{fc-mats}$ *<proof>*

We obtain the following result, which is similar to `make_pm_sum` but with a sum on the elements of the spectrum of Hermitian matrix A , which is a more standard statement of the spectral decomposition theorem.

lemma (*in cpx-sq-mat*) *make-pm-sum'*:
assumes $A \in \text{fc-mats}$
and *hermitian* A
shows *sum-mat* $(\lambda a. a \cdot_m (\text{eigen-projector } A a)) (\text{spectrum } A) = A$
<proof>

end

theory *CHSH-Inequality* **imports**
Projective-Measurements

begin

4 The CHSH inequality

The local hidden variable assumption for quantum mechanics was developed to make the case that quantum theory was incomplete. In this part we formalize the CHSH inequality, which provides an upper-bound of a quantity involving expectations in a probability space, and exploit this inequality to show that the local hidden variable assumption does not hold.

4.1 Inequality statement

lemma *chsh-real*:
fixes $A0::\text{real}$
assumes $|A0 * B1| \leq 1$
and $|A0 * B0| \leq 1$
and $|A1 * B0| \leq 1$
and $|A1 * B1| \leq 1$
shows $|A0 * B1 - A0 * B0 + A1 * B0 + A1 * B1| \leq 2$
<proof>

lemma (*in prob-space*) *chsh-expect*:
fixes $A0::'a \Rightarrow \text{real}$
assumes $AE w \text{ in } M. |A0 w| \leq 1$
and $AE w \text{ in } M. |A1 w| \leq 1$

and $AE\ w\ in\ M. |B0\ w| \leq 1$
and $AE\ w\ in\ M. |B1\ w| \leq 1$
and $integrable\ M\ (\lambda w. A0\ w * B1\ w)$
and $integrable\ M\ (\lambda w. A1\ w * B1\ w)$
and $integrable\ M\ (\lambda w. A1\ w * B0\ w)$
and $integrable\ M\ (\lambda w. A0\ w * B0\ w)$
shows $|expectation\ (\lambda w. A1\ w * B0\ w) + expectation\ (\lambda w. A0\ w * B1\ w) +$
 $expectation\ (\lambda w. A1\ w * B1\ w) - expectation\ (\lambda w. A0\ w * B0\ w)| \leq 2$
 $\langle proof \rangle$

The local hidden variable assumption states that separated quantum measurements are independent. It is standard for this assumption to be stated in a context where the hidden variable admits a density; it is stated here in a more general contest involving expectations, with no assumption on the existence of a density.

definition $pos-rv:: 'a\ measure \Rightarrow ('a \Rightarrow real) \Rightarrow bool\ where$
 $pos-rv\ M\ Xr \equiv Xr \in borel-measurable\ M \wedge (AE\ w\ in\ M. (0::real) \leq Xr\ w)$

definition $prv-sum:: 'a\ measure \Rightarrow complex\ Matrix.mat \Rightarrow (complex \Rightarrow 'a \Rightarrow real)$
 $\Rightarrow bool\ where$
 $prv-sum\ M\ A\ Xr \equiv (AE\ w\ in\ M. (\sum_{a \in spectrum\ A} Xr\ a\ w) = 1)$

definition $(in\ cpx-sq-mat)\ lhv\ where$
 $lhv\ M\ A\ B\ R\ XA\ XB \equiv$
 $prob-space\ M \wedge$
 $(\forall a \in spectrum\ A. pos-rv\ M\ (XA\ a)) \wedge$
 $(prv-sum\ M\ A\ XA) \wedge$
 $(\forall b \in spectrum\ B. pos-rv\ M\ (XB\ b)) \wedge$
 $(prv-sum\ M\ B\ XB) \wedge$
 $(\forall a \in spectrum\ A . \forall b \in spectrum\ B.$
 $(integrable\ M\ (\lambda w. XA\ a\ w * XB\ b\ w)) \wedge$
 $integral^L\ M\ (\lambda w. XA\ a\ w * XB\ b\ w) =$
 $Re\ (Complex-Matrix.trace(eigen-projector\ A\ a * (eigen-projector\ B\ b) * R))$

lemma $(in\ cpx-sq-mat)\ lhv-posl:$
assumes $lhv\ M\ A\ B\ R\ XA\ XB$
shows $AE\ w\ in\ M. (\forall a \in spectrum\ A. 0 \leq XA\ a\ w)$
 $\langle proof \rangle$

lemma $(in\ cpx-sq-mat)\ lhv-lt1-l:$
assumes $lhv\ M\ A\ B\ R\ XA\ XB$
shows $AE\ w\ in\ M. (\forall a \in spectrum\ A. XA\ a\ w \leq 1)$
 $\langle proof \rangle$

lemma $(in\ cpx-sq-mat)\ lhv-posr:$
assumes $lhv\ M\ A\ B\ R\ XA\ XB$
shows $AE\ w\ in\ M. (\forall b \in spectrum\ B. 0 \leq XB\ b\ w)$

<proof>

lemma (in *cpx-sq-mat*) *lhv-lt1-r*:

assumes *lhv M A B R XA XB*

shows *AE w in M. ($\forall a \in \text{spectrum } B. XB a w \leq 1$)*

<proof>

lemma (in *cpx-sq-mat*) *lhv-AE-propl*:

assumes *lhv M A B R XA XB*

shows *AE w in M. ($\forall a \in \text{spectrum } A. 0 \leq XA a w \wedge XA a w \leq 1$) \wedge ($\sum_{a \in \text{spectrum } A} XA a w = 1$)*

<proof>

lemma (in *cpx-sq-mat*) *lhv-AE-propr*:

assumes *lhv M A B R XA XB*

shows *AE w in M. ($\forall a \in \text{spectrum } B. 0 \leq XB a w \wedge XB a w \leq 1$) \wedge ($\sum_{a \in \text{spectrum } B} XB a w = 1$)*

<proof>

lemma (in *cpx-sq-mat*) *lhv-integral-eq*:

fixes *c::real*

assumes *lhv M A B R XA XB*

and *a ∈ spectrum A*

and *b ∈ spectrum B*

shows *integral^L M ($\lambda w. XA a w * XB b w$) =*

*Re (Complex-Matrix.trace(eigen-projector A a * (eigen-projector B b) * R))*

<proof>

lemma (in *cpx-sq-mat*) *lhv-integrable*:

fixes *c::real*

assumes *lhv M A B R XA XB*

and *a ∈ spectrum A*

and *b ∈ spectrum B*

shows *integrable M ($\lambda w. XA a w * XB b w$)* *<proof>*

lemma (in *cpx-sq-mat*) *lhv-scal-integrable*:

fixes *c::real*

assumes *lhv M A B R XA XB*

and *a ∈ spectrum A*

and *b ∈ spectrum B*

shows *integrable M ($\lambda w. c * XA a w * d * XB b w$)*

<proof>

lemma (in *cpx-sq-mat*) *lhv-lsum-scal-integrable*:

assumes *lhv M A B R XA XB*

and *a ∈ spectrum A*

shows *integrable M ($\lambda x. \sum_{b \in \text{spectrum } B} b * XA a x * (f b) * XB b x$)*

<proof>

lemma (in *cpx-sq-mat*) *lhv-sum-integrable*:

assumes $lhv\ M\ A\ B\ R\ XA\ XB$

shows *integrable* M ($\lambda w.$ $(\sum a \in spectrum\ A. (\sum b \in spectrum\ B. f\ a * XA\ a\ w * g\ b * XB\ b\ w))$)

<proof>

lemma (in *cpx-sq-mat*) *spectrum-abs-1-weighted-suml*:

assumes $lhv\ M\ A\ B\ R\ Va\ Vb$

and $\{Re\ x\ |x. x \in spectrum\ A\} \neq \{\}$

and $\{Re\ x\ |x. x \in spectrum\ A\} \subseteq \{-1, 1\}$

and *hermitian* A

and $A \in fc\ mats$

shows $AE\ w\ in\ M.$ $|\sum_{a \in spectrum\ A} Re\ a * Va\ a\ w| \leq 1$

<proof>

lemma (in *cpx-sq-mat*) *spectrum-abs-1-weighted-sumr*:

assumes $lhv\ M\ B\ A\ R\ Vb\ Va$

and $\{Re\ x\ |x. x \in spectrum\ A\} \neq \{\}$

and $\{Re\ x\ |x. x \in spectrum\ A\} \subseteq \{-1, 1\}$

and *hermitian* A

and $A \in fc\ mats$

shows $AE\ w\ in\ M.$ $|\sum_{a \in spectrum\ A} Re\ a * Va\ a\ w| \leq 1$

<proof>

definition *qt-expect where*

qt-expect $A\ Va = (\lambda w. (\sum_{a \in spectrum\ A} Re\ a * Va\ a\ w))$

lemma (in *cpx-sq-mat*) *spectr-sum-integrable*:

assumes $lhv\ M\ A\ B\ R\ Va\ Vb$

shows *integrable* M ($\lambda w.$ *qt-expect* $A\ Va\ w * qt-expect\ B\ Vb\ w$)

<proof>

lemma (in *cpx-sq-mat*) *lhv-sum-integral'*:

assumes $lhv\ M\ A\ B\ R\ XA\ XB$

shows $integral^L\ M$ ($\lambda w.$ $(\sum a \in spectrum\ A. f\ a * XA\ a\ w) * (\sum b \in spectrum\ B. g\ b * XB\ b\ w)) =$

$(\sum a \in spectrum\ A. f\ a * (\sum b \in spectrum\ B. g\ b * integral^L\ M\ (\lambda w. XA\ a\ w * XB\ b\ w)))$

<proof>

lemma (in *cpx-sq-mat*) *sum-qt-expect-trace*:

assumes $lhv\ M\ A\ B\ R\ XA\ XB$

shows $(\sum a \in spectrum\ A. f\ a * (\sum b \in spectrum\ B. g\ b * integral^L\ M\ (\lambda w. XA\ a\ w * XB\ b\ w))) =$

$(\sum a \in spectrum\ A. f\ a * (\sum b \in spectrum\ B. g\ b *$

$Re\ (Complex-Matrix.trace(eigen-projector\ A\ a * (eigen-projector\ B\ b) * R)))$)

<proof>

lemma (in *cpx-sq-mat*) *sum-eigen-projector-trace-dist*:

assumes *hermitian B*
and $A \in \text{fc-mats}$
and $B \in \text{fc-mats}$
and $R \in \text{fc-mats}$
shows $(\sum b \in \text{spectrum } B. (b * \text{Complex-Matrix.trace}(A * (\text{eigen-projector } B \ b) * R))) = \text{Complex-Matrix.trace}(A * B * R)$
 ⟨*proof*⟩

lemma (in *cpx-sq-mat*) *sum-eigen-projector-trace-right*:
assumes *hermitian A*
and $A \in \text{fc-mats}$
and $B \in \text{fc-mats}$
shows $(\sum a \in \text{spectrum } A. \text{Complex-Matrix.trace}(a * \text{eigen-projector } A \ a * B)) = \text{Complex-Matrix.trace}(A * B)$
 ⟨*proof*⟩

lemma (in *cpx-sq-mat*) *sum-eigen-projector-trace*:
assumes *hermitian A*
and *hermitian B*
and $A \in \text{fc-mats}$
and $B \in \text{fc-mats}$
and $R \in \text{fc-mats}$
shows $(\sum a \in \text{spectrum } A. a * (\sum b \in \text{spectrum } B. (b * \text{Complex-Matrix.trace}(\text{eigen-projector } A \ a * (\text{eigen-projector } B \ b) * R)))) = \text{Complex-Matrix.trace}(A * B * R)$
 ⟨*proof*⟩

We obtain the main result of this part, which relates the quantum expectation value of a joint measurement with an expectation.

lemma (in *cpx-sq-mat*) *sum-qt-expect*:
assumes *lhv M A B R XA XB*
and $A \in \text{fc-mats}$
and $B \in \text{fc-mats}$
and $R \in \text{fc-mats}$
and *hermitian A*
and *hermitian B*
shows $\text{integral}^L M (\lambda w. (\text{qt-expect } A \ XA \ w) * (\text{qt-expect } B \ XB \ w)) = \text{Re}(\text{Complex-Matrix.trace}(A * B * R))$
 ⟨*proof*⟩

4.2 Properties of specific observables

In this part we consider a specific density operator and specific observables corresponding to joint bipartite measurements. We will compute the quantum expectation value of this system and prove that it violates the CHSH inequality, thus proving that the local hidden variable assumption cannot

hold.

4.2.1 Ket 0, Ket 1 and the corresponding projectors

definition *ket-0::complex Matrix.vec* **where**
ket-0 = unit-vec 2 0

lemma *ket-0-dim*:
shows *dim-vec ket-0 = 2* \langle *proof* \rangle

lemma *ket-0-norm*:
shows $\|ket-0\| = 1$ \langle *proof* \rangle

lemma *ket-0-mat*:
shows *ket-vec ket-0 = Matrix.mat-of-cols-list 2 [[1, 0]]*
 \langle *proof* \rangle

definition *ket-1::complex Matrix.vec* **where**
ket-1 = unit-vec 2 1

lemma *ket-1-dim*:
shows *dim-vec ket-1 = 2* \langle *proof* \rangle

lemma *ket-1-norm*:
shows $\|ket-1\| = 1$ \langle *proof* \rangle

definition *ket-01*
where *ket-01 = tensor-vec ket-0 ket-1*

lemma *ket-01-dim*:
shows *dim-vec ket-01 = 4* \langle *proof* \rangle

definition *ket-10*
where *ket-10 = tensor-vec ket-1 ket-0*

lemma *ket-10-dim*:
shows *dim-vec ket-10 = 4* \langle *proof* \rangle

We define `ket_psim`, one of the Bell states (or EPR pair).

definition *ket-psim* **where**
ket-psim = 1/(sqrt 2) ·_v (ket-01 - ket-10)

lemma *ket-psim-dim*:
shows *dim-vec ket-psim = 4* \langle *proof* \rangle

lemma *ket-psim-norm*:
shows $\|ket-psim\| = 1$
 \langle *proof* \rangle

`rho_psim` represents the density operator associated with the quantum state `ket_psim`.

definition *rho-psim where*
rho-psim = rank-1-proj ket-psim

lemma *rho-psim-carrier:*
shows rho-psim ∈ carrier-mat 4 4 <proof>

lemma *rho-psim-dim-row:*
shows dim-row rho-psim = 4 <proof>

lemma *rho-psim-density:*
shows density-operator rho-psim <proof>

4.2.2 The X and Z matrices and two of their combinations

In this part we prove properties of two standard matrices in quantum theory, X and Z , as well as two of their combinations: $\frac{X+Z}{\sqrt{2}}$ and $\frac{Z-X}{\sqrt{2}}$. Note that all of these matrices are observables, they will be used to violate the CHSH inequality.

lemma *Z-carrier: shows* $Z \in \text{carrier-mat } 2 \ 2$ *<proof>*

lemma *Z-hermitian:*
shows hermitian Z <proof>

lemma *unitary-Z:*
shows Complex-Matrix.unitary Z
<proof>

lemma *X-carrier: shows* $X \in \text{carrier-mat } 2 \ 2$ *<proof>*

lemma *X-hermitian:*
shows hermitian X <proof>

lemma *unitary-X:*
shows Complex-Matrix.unitary X
<proof>

definition *XpZ*
where $XpZ = -1/\text{sqrt}(2) \cdot_m (X + Z)$

lemma *XpZ-carrier:*
shows XpZ ∈ carrier-mat 2 2 <proof>

lemma *XpZ-hermitian:*
shows hermitian XpZ
<proof>

lemma *XpZ-inv*:
 $XpZ * XpZ = 1_m \ 2$ *<proof>*

lemma *unitary-XpZ*:
shows *Complex-Matrix.unitary XpZ*
<proof>

definition *ZmX*
where $ZmX = 1/\text{sqrt}(2) \cdot_m (Z - X)$

lemma *ZmX-carrier*:
shows $ZmX \in \text{carrier-mat } 2 \ 2$ *<proof>*

lemma *ZmX-hermitian*:
shows *hermitian ZmX*
<proof>

lemma *ZmX-inv*:
 $ZmX * ZmX = 1_m \ 2$ *<proof>*

lemma *unitary-ZmX*:
shows *Complex-Matrix.unitary ZmX*
<proof>

definition *Z-XpZ*
where $Z-XpZ = \text{tensor-mat } Z \ XpZ$

lemma *Z-XpZ-carrier*:
shows $Z-XpZ \in \text{carrier-mat } 4 \ 4$ *<proof>*

definition *X-XpZ*
where $X-XpZ = \text{tensor-mat } X \ XpZ$

lemma *X-XpZ-carrier*:
shows $X-XpZ \in \text{carrier-mat } 4 \ 4$ *<proof>*

definition *Z-ZmX*
where $Z-ZmX = \text{tensor-mat } Z \ ZmX$

lemma *Z-ZmX-carrier*:
shows $Z-ZmX \in \text{carrier-mat } 4 \ 4$ *<proof>*

definition *X-ZmX*
where $X-ZmX = \text{tensor-mat } X \ ZmX$

lemma *X-ZmX-carrier*:
shows $X-ZmX \in \text{carrier-mat } 4 \ 4$ *<proof>*

lemma *X-ZmX-rho-psim[simp]*:

shows *Complex-Matrix.trace* ($\text{rho-psim} * X\text{-ZmX}$) = $1 / (\text{sqrt } 2)$
<proof>

lemma *Z-ZmX-rho-psim[simp]*:

shows *Complex-Matrix.trace* ($\text{rho-psim} * Z\text{-ZmX}$) = $-1 / (\text{sqrt } 2)$
<proof>

lemma *X-XpZ-rho-psim[simp]*:

shows *Complex-Matrix.trace* ($\text{rho-psim} * X\text{-XpZ}$) = $1 / (\text{sqrt } 2)$
<proof>

lemma *Z-XpZ-rho-psim[simp]*:

shows *Complex-Matrix.trace* ($\text{rho-psim} * Z\text{-XpZ}$) = $1 / (\text{sqrt } 2)$
<proof>

definition *Z-I where*

$Z\text{-I} = \text{tensor-mat } Z (1_m \ 2)$

lemma *Z-I-carrier:*

shows $Z\text{-I} \in \text{carrier-mat } 4 \ 4$ *<proof>*

lemma *Z-I-hermitian:*

shows *hermitian* $Z\text{-I}$ *<proof>*

lemma *Z-I-unitary:*

shows *unitary* $Z\text{-I}$ *<proof>*

lemma *Z-I-spectrum:*

shows $\{\text{Re } x \mid x \in \text{spectrum } Z\text{-I}\} \subseteq \{-1, 1\}$ *<proof>*

definition *X-I where*

$X\text{-I} = \text{tensor-mat } X (1_m \ 2)$

lemma *X-I-carrier:*

shows $X\text{-I} \in \text{carrier-mat } 4 \ 4$ *<proof>*

lemma *X-I-hermitian:*

shows *hermitian* $X\text{-I}$ *<proof>*

lemma *X-I-unitary:*

shows *unitary* $X\text{-I}$ *<proof>*

lemma *X-I-spectrum:*

shows $\{\text{Re } x \mid x \in \text{spectrum } X\text{-I}\} \subseteq \{-1, 1\}$ *<proof>*

definition *I-XpZ where*

$I\text{-XpZ} = \text{tensor-mat } (1_m \ 2) \ XpZ$

lemma *I-XpZ-carrier:*

shows $I-XpZ \in \text{carrier-mat } 4 \ 4$ $\langle \text{proof} \rangle$

lemma $I-XpZ$ -hermitian:
shows hermitian $I-XpZ$ $\langle \text{proof} \rangle$

lemma $I-XpZ$ -unitary:
shows unitary $I-XpZ$ $\langle \text{proof} \rangle$

lemma $I-XpZ$ -spectrum:
shows $\{ \text{Re } x \mid x. x \in \text{spectrum } I-XpZ \} \subseteq \{-1, 1\}$ $\langle \text{proof} \rangle$

definition $I-ZmX$ where
 $I-ZmX = \text{tensor-mat } (1_m \ 2) \ ZmX$

lemma $I-ZmX$ -carrier:
shows $I-ZmX \in \text{carrier-mat } 4 \ 4$ $\langle \text{proof} \rangle$

lemma $I-ZmX$ -hermitian:
shows hermitian $I-ZmX$ $\langle \text{proof} \rangle$

lemma $I-ZmX$ -unitary:
shows unitary $I-ZmX$ $\langle \text{proof} \rangle$

lemma $I-ZmX$ -spectrum:
shows $\{ \text{Re } x \mid x. x \in \text{spectrum } I-ZmX \} \subseteq \{-1, 1\}$ $\langle \text{proof} \rangle$

lemma $X-I-ZmX$ -eq:
shows $X-I * I-ZmX = X-ZmX$ $\langle \text{proof} \rangle$

lemma $X-I-XpZ$ -eq:
shows $X-I * I-XpZ = X-XpZ$ $\langle \text{proof} \rangle$

lemma $Z-I-XpZ$ -eq:
shows $Z-I * I-XpZ = Z-XpZ$ $\langle \text{proof} \rangle$

lemma $Z-I-ZmX$ -eq:
shows $Z-I * I-ZmX = Z-ZmX$ $\langle \text{proof} \rangle$

4.2.3 No local hidden variable

We show that the local hidden variable hypothesis cannot hold by exhibiting a quantum expectation value that is greater than the upper-bound given by the CHSH inequality.

locale $\text{bin-cpx} = \text{cpx-sq-mat} +$
assumes $\text{dim}4: \text{dim}R = 4$

lemma (in bin-cpx) $X-I-XpZ$ -trace:
assumes $\text{lhv } M \ X-I \ I-XpZ \ R \ \forall x \ \forall p$
and $R \in \text{fc-mats}$

shows $LINT\ w|M. (qt-expect\ X-I\ Vx\ w) * (qt-expect\ I-XpZ\ Vp\ w) =$
 $Re\ (Complex-Matrix.trace\ (R * X-XpZ))$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *X-I-XpZ-chsh*:
assumes $lhv\ M\ X-I\ I-XpZ\ rho-psim\ Vx\ Vp$
shows $LINT\ w|M. (qt-expect\ X-I\ Vx\ w) * (qt-expect\ I-XpZ\ Vp\ w) =$
 $1/sqrt\ 2$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *Z-I-XpZ-trace*:
assumes $lhv\ M\ Z-I\ I-XpZ\ R\ Vz\ Vp$
and $R \in fc-mats$
shows $LINT\ w|M. (qt-expect\ Z-I\ Vz\ w) * (qt-expect\ I-XpZ\ Vp\ w) =$
 $Re\ (Complex-Matrix.trace\ (R * Z-XpZ))$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *Z-I-XpZ-chsh*:
assumes $lhv\ M\ Z-I\ I-XpZ\ rho-psim\ Vz\ Vp$
shows $LINT\ w|M. (qt-expect\ Z-I\ Vz\ w) * (qt-expect\ I-XpZ\ Vp\ w) =$
 $1/sqrt\ 2$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *X-I-ZmX-trace*:
assumes $lhv\ M\ X-I\ I-ZmX\ R\ Vx\ Vp$
and $R \in fc-mats$
shows $LINT\ w|M. (qt-expect\ X-I\ Vx\ w) * (qt-expect\ I-ZmX\ Vp\ w) =$
 $Re\ (Complex-Matrix.trace\ (R * X-ZmX))$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *X-I-ZmX-chsh*:
assumes $lhv\ M\ X-I\ I-ZmX\ rho-psim\ Vx\ Vp$
shows $LINT\ w|M. (qt-expect\ X-I\ Vx\ w) * (qt-expect\ I-ZmX\ Vp\ w) =$
 $1/sqrt\ 2$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *Z-I-ZmX-trace*:
assumes $lhv\ M\ Z-I\ I-ZmX\ R\ Vz\ Vp$
and $R \in fc-mats$
shows $LINT\ w|M. (qt-expect\ Z-I\ Vz\ w) * (qt-expect\ I-ZmX\ Vp\ w) =$
 $Re\ (Complex-Matrix.trace\ (R * Z-ZmX))$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *Z-I-ZmX-chsh*:
assumes $lhv\ M\ Z-I\ I-ZmX\ rho-psim\ Vz\ Vp$
shows $LINT\ w|M. (qt-expect\ Z-I\ Vz\ w) * (qt-expect\ I-ZmX\ Vp\ w) =$
 $-1/sqrt\ 2$
 $\langle proof \rangle$

lemma (in *bin-cpx*) *chsh-upper-bound*:
assumes *prob-space M*
and *lhv M X-I I-XpZ rho-psim Vx Vp*
and *lhv M Z-I I-XpZ rho-psim Vz Vp*
and *lhv M X-I I-ZmX rho-psim Vx Vm*
and *lhv M Z-I I-ZmX rho-psim Vz Vm*
shows $|(\text{LINT } w|M. \text{qt-expect } X\text{-I } Vx \ w * \text{qt-expect } I\text{-ZmX } Vm \ w) +$
 $(\text{LINT } w|M. \text{qt-expect } Z\text{-I } Vz \ w * \text{qt-expect } I\text{-XpZ } Vp \ w) +$
 $(\text{LINT } w|M. \text{qt-expect } X\text{-I } Vx \ w * \text{qt-expect } I\text{-XpZ } Vp \ w) -$
 $(\text{LINT } w|M. \text{qt-expect } Z\text{-I } Vz \ w * \text{qt-expect } I\text{-ZmX } Vm \ w)|$
 ≤ 2
 $\langle \text{proof} \rangle$

lemma (in *bin-cpx*) *quantum-value*:
assumes *lhv M X-I I-XpZ rho-psim Vx Vp*
and *lhv M Z-I I-XpZ rho-psim Vz Vp*
and *lhv M X-I I-ZmX rho-psim Vx Vm*
and *lhv M Z-I I-ZmX rho-psim Vz Vm*
shows $|(\text{LINT } w|M. \text{qt-expect } X\text{-I } Vx \ w * \text{qt-expect } I\text{-ZmX } Vm \ w) +$
 $(\text{LINT } w|M. \text{qt-expect } Z\text{-I } Vz \ w * \text{qt-expect } I\text{-XpZ } Vp \ w) +$
 $(\text{LINT } w|M. \text{qt-expect } X\text{-I } Vx \ w * \text{qt-expect } I\text{-XpZ } Vp \ w) -$
 $(\text{LINT } w|M. \text{qt-expect } Z\text{-I } Vz \ w * \text{qt-expect } I\text{-ZmX } Vm \ w)|$
 $= 2 * \text{sqrt } 2$
 $\langle \text{proof} \rangle$

lemma (in *bin-cpx*) *no-lhv*:
assumes *lhv M X-I I-XpZ rho-psim Vx Vp*
and *lhv M Z-I I-XpZ rho-psim Vz Vp*
and *lhv M X-I I-ZmX rho-psim Vx Vm*
and *lhv M Z-I I-ZmX rho-psim Vz Vm*
shows *False*
 $\langle \text{proof} \rangle$

end