

# Simultaneous diagonalization of pairwise commuting Hermitian matrices

Mnacho Echenim

February 6, 2026

## Abstract

A Hermitian matrix is a square complex matrix  $A$  that is equal to its conjugate transpose  $A^\dagger$ . The (finite-dimensional) spectral theorem states that for any such matrix  $A$ , we have the equality  $A = U \cdot B \cdot U^\dagger$ , where  $U$  is a unitary matrix and  $B$  is a diagonal matrix containing only real elements. We formalize the generalization of this result, which states that if  $\{A_1, \dots, A_n\}$  are Hermitian and pairwise commuting matrices, then there exists a unitary matrix  $U$  such that  $A_i = U \cdot B_i \cdot U^\dagger$ , for  $i = 1, \dots, n$ , and each  $B_i$  is diagonal and contains only real elements. Sets of pairwise commuting Hermitian matrices are called *Complete Sets of Commuting Observables* in Quantum Mechanics, where they represent physical quantities that can be simultaneously measured to uniquely distinguish quantum states.

## Contents

<b>1</b>	<b>Some preliminary results</b>	<b>1</b>
1.1	Roots of a polynomial . . . . .	1
1.2	Linear algebra preliminaries . . . . .	2
<b>2</b>	<b>Properties of the spectrum of a matrix</b>	<b>4</b>
2.1	Results on diagonal matrices . . . . .	4
2.2	Unitary equivalence . . . . .	6
2.3	On the spectrum of a matrix . . . . .	10
<b>3</b>	<b>Properties of the inner product</b>	<b>11</b>
3.1	Some analysis complements . . . . .	11
3.2	Inner product results . . . . .	13
<b>4</b>	<b>Matrix decomposition</b>	<b>16</b>
<b>5</b>	<b>Additional results on block decompositions of matrices</b>	<b>18</b>
5.1	Split block results . . . . .	18
5.2	Diagonal block matrices . . . . .	20

<b>6</b>	<b>Block matrix decomposition</b>	<b>24</b>
6.1	Subdiagonal extraction . . . . .	24
6.2	Predicates on diagonal block matrices . . . . .	25
6.3	Counting similar neighbours in a list . . . . .	27
<b>7</b>	<b>Sorted hermitian decomposition</b>	<b>30</b>
<b>8</b>	<b>Commuting Hermitian families</b>	<b>33</b>
8.1	Intermediate properties . . . . .	33
8.2	The main result . . . . .	35

**Acknowledgments** This work was partially supported by Agence Nationale de la Recherche, through *Plan France 2030 (ref. ANR-22-PETQ-0007)*.

**theory** *Spectral-Theory-Complements* **imports** *HOL-Combinatorics.Permutations*  
*Projective-Measurements.Linear-Algebra-Complements*  
*Projective-Measurements.Projective-Measurements*

**begin**

## 1 Some preliminary results

### 1.1 Roots of a polynomial

Results on polynomials, the main one being that the set of roots of a polynomial is uniquely defined.

**lemma** *root-poly-linear*:

**shows**  $\text{poly} (\prod a \leftarrow L. [:- a, 1:]) (c :: 'a :: \text{field}) = 0 \implies c \in \text{set } L$   
*<proof>*

**lemma** *poly-root-set-subseteq*:

**assumes**  $(\prod (a :: 'a :: \text{field}) \leftarrow L. [:- a, 1:]) = (\prod a \leftarrow M. [:- a, 1:])$   
**shows**  $\text{set } L \subseteq \text{set } M$   
*<proof>*

**lemma** *poly-root-set-eq*:

**assumes**  $(\prod (a :: 'a :: \text{field}) \leftarrow L. [:- a, 1:]) = (\prod a \leftarrow M. [:- a, 1:])$   
**shows**  $\text{set } L = \text{set } M$  *<proof>*

### 1.2 Linear algebra preliminaries

**lemma** *minus-zero-vec-eq*:

**fixes**  $v :: 'a :: \{ab\text{-group-add}\}$  *Matrix.vec*  
**assumes**  $\text{dim-vec } v = n$   
**and**  $\text{dim-vec } w = n$

**and**  $v - w = 0_v \ n$   
**shows**  $v = w$   
 $\langle proof \rangle$

**lemma** *right-minus-zero-mat*:  
**fixes**  $A::'a::\{group-add\} \ Matrix.mat$   
**shows**  $A - 0_m \ (dim-row \ A) \ (dim-col \ A) = A$   
 $\langle proof \rangle$

**lemma** *smult-zero*:  
**shows**  $(0::'a::comm-ring) \cdot_m \ A = 0_m \ (dim-row \ A) \ (dim-col \ A) \ \langle proof \rangle$

**lemma** *rank-1-proj-col-carrier*:  
**assumes**  $i < dim-col \ A$   
**shows**  $rank-1-proj \ (Matrix.col \ A \ i) \in carrier-mat \ (dim-row \ A) \ (dim-row \ A)$   
 $\langle proof \rangle$

**lemma** *zero-adjoint*:  
**shows**  $Complex-Matrix.adjoint \ (0_m \ n \ m) = ((0_m \ m \ n)::'a::conjugatable-field \ Matrix.mat)$   
 $\langle proof \rangle$

**lemma** *assoc-mat-mult-vec'*:  
**assumes**  $A \in carrier-mat \ n \ n$   
**and**  $B \in carrier-mat \ n \ n$   
**and**  $C \in carrier-mat \ n \ n$   
**and**  $v \in carrier-vec \ n$   
**shows**  $A * B * C *_v \ v = A *_v \ (B *_v \ (C *_v \ v)) \ \langle proof \rangle$

**lemma** *adjoint-dim'*:  
 $A \in carrier-mat \ n \ m \implies Complex-Matrix.adjoint \ A \in carrier-mat \ m \ n$   
 $\langle proof \rangle$

**definition** *mat-conj where*  
 $mat-conj \ U \ V = U * V * (Complex-Matrix.adjoint \ U)$

**lemma** *mat-conj-adjoint*:  
**shows**  $mat-conj \ (Complex-Matrix.adjoint \ U) \ V = Complex-Matrix.adjoint \ U * V * U \ \langle proof \rangle$

**lemma** *map2-mat-conj-exp*:  
**assumes**  $length \ A = length \ B$   
**shows**  $map2 \ (*) \ (map2 \ (*) \ A \ B) \ (map \ Complex-Matrix.adjoint \ A) = map2 \ mat-conj \ A \ B \ \langle proof \rangle$

**lemma** *mat-conj-unit-commute*:  
**assumes** *unitary*  $U$   
**and**  $U * A = A * U$   
**and**  $A \in carrier-mat \ n \ n$

**and**  $U \in \text{carrier-mat } n \ n$   
**shows**  $\text{mat-conj } U \ A = A$   
 $\langle \text{proof} \rangle$

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

**lemma** *hermitian-mat-conj'*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $U \in \text{carrier-mat } n \ n$   
**and** *hermitian*  $A$   
**shows** *hermitian*  $(\text{mat-conj } (\text{Complex-Matrix.adjoint } U) \ A)$   
 $\langle \text{proof} \rangle$

**lemma** *mat-conj-uminus-eq*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $U \in \text{carrier-mat } n \ n$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $A = \text{mat-conj } U \ B$   
**shows**  $-A = \text{mat-conj } U \ (-B)$   $\langle \text{proof} \rangle$

**lemma** *mat-conj-smult*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $U \in \text{carrier-mat } n \ n$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $A = U * B * (\text{Complex-Matrix.adjoint } U)$   
**shows**  $x \cdot_m A = U * (x \cdot_m B) * (\text{Complex-Matrix.adjoint } U)$   $\langle \text{proof} \rangle$

**lemma** *mult-adjoint-hermitian*:  
**fixes**  $A :: 'a :: \text{conjugatable-field } \text{Matrix.mat}$   
**assumes**  $A \in \text{carrier-mat } n \ m$   
**shows** *hermitian*  $((\text{Complex-Matrix.adjoint } A) * A)$   $\langle \text{proof} \rangle$

**lemma** *hermitian-square-hermitian*:  
**fixes**  $A :: 'a :: \text{conjugatable-field } \text{Matrix.mat}$   
**assumes** *hermitian*  $A$   
**shows** *hermitian*  $(A * A)$   
 $\langle \text{proof} \rangle$

## 2 Properties of the spectrum of a matrix

### 2.1 Results on diagonal matrices

**lemma** *diagonal-mat-uminus*:  
**fixes**  $A :: 'a :: \{\text{ring}\} \ \text{Matrix.mat}$

**assumes** *diagonal-mat*  $A$   
**shows** *diagonal-mat*  $(-A)$   $\langle$ *proof* $\rangle$

**lemma** *diagonal-mat-smult*:  
**fixes**  $A::'a::\{\text{ring}\}$  *Matrix.mat*  
**assumes** *diagonal-mat*  $A$   
**shows** *diagonal-mat*  $(x \cdot_m A)$   $\langle$ *proof* $\rangle$

**lemma** *diagonal-imp-upper-triangular*:  
**assumes** *diagonal-mat*  $A$   
**and**  $A \in \text{carrier-mat } n \ n$   
**shows** *upper-triangular*  $A$   $\langle$ *proof* $\rangle$

**lemma** *set-diag-mat-uminus*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**shows** *set*  $(\text{diag-mat } (-A)) = \{-a \mid a. a \in \text{set } (\text{diag-mat } A)\}$  **(is ?L = ?R)**  
 $\langle$ *proof* $\rangle$

**lemma** *set-diag-mat-smult*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**shows** *set*  $(\text{diag-mat } (x \cdot_m A)) = \{x * a \mid a. a \in \text{set } (\text{diag-mat } A)\}$  **(is ?L = ?R)**  
 $\langle$ *proof* $\rangle$

**lemma** *diag-mat-diagonal-eq*:  
**assumes** *diag-mat*  $A = \text{diag-mat } B$   
**and** *diagonal-mat*  $A$   
**and** *diagonal-mat*  $B$   
**and** *dim-col*  $A = \text{dim-col } B$   
**shows**  $A = B$   
 $\langle$ *proof* $\rangle$

**lemma** *diag-elems-ne*:  
**assumes**  $B \in \text{carrier-mat } n \ n$   
**and**  $0 < n$   
**shows** *diag-elems*  $B \neq \{\}$   
 $\langle$ *proof* $\rangle$

**lemma** *diagonal-mat-mult-vec*:  
**fixes**  $B::'a::\text{conjugatable-field}$  *Matrix.mat*  
**assumes** *diagonal-mat*  $B$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $v \in \text{carrier-vec } n$   
**and**  $i < n$   
**shows** *vec-index*  $(B *_v v) \ i = B \ \$\$ \ (i,i) * (\text{vec-index } v \ i)$   
 $\langle$ *proof* $\rangle$

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

**lemma** *diagonal-mat-mult-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**  $(A*B) \ \$\$ (i,j) = B \ \$\$ (j,j) * A \ \$\$ (i, j)$

*<proof>*

**lemma** *diagonal-mat-times-diag*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and** *diagonal-mat A*  
**and** *diagonal-mat B*  
**shows** *diagonal-mat (A\*B)* *<proof>*

**lemma** *diagonal-mat-commute*:  
**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 A*  
**and** *diagonal-mat B*  
**shows**  $A * B = B * A$   
*<proof>*

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

**lemma** *diagonal-mat-sq-index'*:  
**fixes**  $B::'a::\{\text{ring}\}$  *Matrix.mat*  
**assumes** *diagonal-mat B*  
**and**  $B \in \text{carrier-mat } n \ n$

**and**  $i < n$   
**and**  $j < n$   
**shows**  $(B * B) \$(i,j) = B\$(i,j) * B\$(i,j)$   
 <proof>

**lemma** *diagonal-mat-sq-diag*:  
**fixes**  $B::'a::\{ring\} Matrix.mat$   
**assumes** *diagonal-mat*  $B$   
**and**  $B \in carrier\text{-}mat\ n\ n$   
**shows** *diagonal-mat*  $(B * B)$  <proof>

**lemma** *real-diagonal-hermitian*:  
**fixes**  $B::complex\ Matrix.mat$   
**assumes**  $B \in carrier\text{-}mat\ n\ n$   
**and** *diagonal-mat*  $B$   
**and**  $\forall i < dim\text{-}row\ B. B\$(i, i) \in Reals$   
**shows** *hermitian*  $B$  <proof>

## 2.2 Unitary equivalence

**definition** *unitarily-equiv* **where**  
*unitarily-equiv*  $A\ B\ U \equiv (unitary\ U \wedge$   
*similar-mat-wit*  $A\ B\ U\ (Complex\text{-}Matrix.adjoint\ U))$

**lemma** *unitarily-equivD*:  
**assumes** *unitarily-equiv*  $A\ B\ U$   
**shows** *unitary*  $U$   
*similar-mat-wit*  $A\ B\ U\ (Complex\text{-}Matrix.adjoint\ U)$  <proof>

**lemma** *unitarily-equivI*:  
**assumes** *similar-mat-wit*  $A\ B\ U\ (Complex\text{-}Matrix.adjoint\ U)$   
**and** *unitary*  $U$   
**shows** *unitarily-equiv*  $A\ B\ U$  <proof>

**lemma** *unitarily-equivI'*:  
**assumes**  $A = mat\text{-}conj\ U\ B$   
**and** *unitary*  $U$   
**and**  $A \in carrier\text{-}mat\ n\ n$   
**and**  $B \in carrier\text{-}mat\ n\ n$   
**shows** *unitarily-equiv*  $A\ B\ U$  <proof>

**lemma** *unitarily-equiv-carrier*:  
**assumes**  $A \in carrier\text{-}mat\ n\ n$   
**and** *unitarily-equiv*  $A\ B\ U$   
**shows**  $B \in carrier\text{-}mat\ n\ n$   $U \in carrier\text{-}mat\ n\ n$   
 <proof>

**lemma** *unitarily-equiv-carrier'*:  
**assumes** *unitarily-equiv*  $A\ B\ U$

**shows**  $A \in \text{carrier-mat } (\text{dim-row } A) (\text{dim-row } A)$   
 $B \in \text{carrier-mat } (\text{dim-row } A) (\text{dim-row } A)$   
 $U \in \text{carrier-mat } (\text{dim-row } A) (\text{dim-row } A)$   
 ⟨proof⟩

**lemma** *unitarily-equiv-eq*:  
**assumes** *unitarily-equiv*  $A B U$   
**shows**  $A = U * B * (\text{Complex-Matrix.adjoint } U)$  ⟨proof⟩

**lemma** *unitarily-equiv-smult*:  
**assumes**  $A \in \text{carrier-mat } n n$   
**and** *unitarily-equiv*  $A B U$   
**shows** *unitarily-equiv*  $(x \cdot_m A) (x \cdot_m B) U$   
 ⟨proof⟩

**lemma** *unitarily-equiv-uminus*:  
**assumes**  $A \in \text{carrier-mat } n n$   
**and** *unitarily-equiv*  $A B U$   
**shows** *unitarily-equiv*  $(-A) (-B) U$   
 ⟨proof⟩

**lemma** *unitarily-equiv-adjoint*:  
**assumes** *unitarily-equiv*  $A B U$   
**shows** *unitarily-equiv*  $B A (\text{Complex-Matrix.adjoint } U)$   
 ⟨proof⟩

**lemma** *unitary-mult-conjugate*:  
**assumes**  $A \in \text{carrier-mat } n n$   
**and**  $V \in \text{carrier-mat } n n$   
**and**  $U \in \text{carrier-mat } n n$   
**and**  $B \in \text{carrier-mat } n n$   
**and** *unitary*  $V$   
**and** *mat-conj*  $(\text{Complex-Matrix.adjoint } V) A = \text{mat-conj } U B$   
**shows**  $A = V * U * B * \text{Complex-Matrix.adjoint } (V * U)$   
 ⟨proof⟩

**lemma** *unitarily-equiv-conjugate*:  
**assumes**  $A \in \text{carrier-mat } n n$   
**and**  $V \in \text{carrier-mat } n n$   
**and**  $U \in \text{carrier-mat } n n$   
**and**  $B \in \text{carrier-mat } n n$   
**and** *unitarily-equiv*  $(\text{mat-conj } (\text{Complex-Matrix.adjoint } V) A) B U$   
**and** *unitary*  $V$   
**shows** *unitarily-equiv*  $A B (V * U)$   
 ⟨proof⟩

**lemma** *mat-conj-commute*:  
**assumes**  $A \in \text{carrier-mat } n n$   
**and**  $B \in \text{carrier-mat } n n$

**and**  $U \in \text{carrier-mat } n \ n$   
**and** *unitary*  $U$   
**and**  $A*B = B*A$   
**shows**  $(\text{mat-conj } (\text{Complex-Matrix.adjoint } U) \ A) \ * \$   
 $(\text{mat-conj } (\text{Complex-Matrix.adjoint } U) \ B) =$   
 $(\text{mat-conj } (\text{Complex-Matrix.adjoint } U) \ B) \ *$   
 $(\text{mat-conj } (\text{Complex-Matrix.adjoint } U) \ A) \ (\text{is } ?L*?R = ?R* ?L)$   
 $\langle \text{proof} \rangle$

**lemma** *unitarily-equiv-commute*:  
**assumes** *unitarily-equiv*  $A \ B \ U$   
**and**  $A*C = C*A$   
**shows**  $B \ * \ (\text{Complex-Matrix.adjoint } U \ * \ C \ * \ U) =$   
 $\text{Complex-Matrix.adjoint } U \ * \ C \ * \ U \ * \ B$   
 $\langle \text{proof} \rangle$

**definition** *unitary-diag* **where**  
*unitary-diag*  $A \ B \ U \equiv \text{unitarily-equiv } A \ B \ U \ \wedge \ \text{diagonal-mat } B$

**lemma** *unitary-diagI*:  
**assumes** *similar-mat-wit*  $A \ B \ U \ (\text{Complex-Matrix.adjoint } U)$   
**and** *diagonal-mat*  $B$   
**and** *unitary*  $U$   
**shows** *unitary-diag*  $A \ B \ U \ \langle \text{proof} \rangle$

**lemma** *unitary-diagI'*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and** *diagonal-mat*  $B$   
**and** *unitary*  $U$   
**and**  $A = \text{mat-conj } U \ B$   
**shows** *unitary-diag*  $A \ B \ U \ \langle \text{proof} \rangle$

**lemma** *unitary-diagD*:  
**assumes** *unitary-diag*  $A \ B \ U$   
**shows** *similar-mat-wit*  $A \ B \ U \ (\text{Complex-Matrix.adjoint } U)$   
*diagonal-mat*  $B$  *unitary*  $U \ \langle \text{proof} \rangle$

**lemma** *unitary-diag-imp-unitarily-equiv[simp]*:  
**assumes** *unitary-diag*  $A \ B \ U$   
**shows** *unitarily-equiv*  $A \ B \ U \ \langle \text{proof} \rangle$

**lemma** *unitary-diag-diagonal[simp]*:  
**assumes** *unitary-diag*  $A \ B \ U$   
**shows** *diagonal-mat*  $B \ \langle \text{proof} \rangle$

**lemma** *unitary-diag-carrier*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and** *unitary-diag*  $A \ B \ U$

**shows**  $B \in \text{carrier-mat } n \ n$   $U \in \text{carrier-mat } n \ n$   
 ⟨proof⟩

**lemma** *unitary-mult-square-eq*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $U \in \text{carrier-mat } n \ n$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $A = \text{mat-conj } U \ B$   
**and**  $(\text{Complex-Matrix.adjoint } U) * U = 1_m \ n$   
**shows**  $A * A = \text{mat-conj } U \ (B*B)$   
 ⟨proof⟩

**lemma** *hermitian-square-similar-mat-wit*:  
**fixes**  $A::\text{complex Matrix.mat}$   
**assumes** *hermitian*  $A$   
**and**  $A \in \text{carrier-mat } n \ n$   
**and** *unitary-diag*  $A \ B \ U$   
**shows** *similar-mat-wit*  $(A * A) \ (B * B) \ U \ (\text{Complex-Matrix.adjoint } U)$   
 ⟨proof⟩

**lemma** *unitarily-equiv-square*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and** *unitarily-equiv*  $A \ B \ U$   
**shows** *unitarily-equiv*  $(A*A) \ (B*B) \ U$   
 ⟨proof⟩

**lemma** *conjugate-eq-unitarily-equiv*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $V \in \text{carrier-mat } n \ n$   
**and** *unitarily-equiv*  $A \ B \ U$   
**and** *unitary*  $V$   
**and**  $V * B * (\text{Complex-Matrix.adjoint } V) = B$   
**shows** *unitarily-equiv*  $A \ B \ (U*V)$   
 ⟨proof⟩

**definition** *real-diag-decomp* **where**  
*real-diag-decomp*  $A \ B \ U \equiv \text{unitary-diag } A \ B \ U \ \wedge$   
 $(\forall i < \text{dim-row } B. B\$\$(i, i) \in \text{Reals})$

**lemma** *real-diag-decompD[simp]*:  
**assumes** *real-diag-decomp*  $A \ B \ U$   
**shows** *unitary-diag*  $A \ B \ U$   
 $(\forall i < \text{dim-row } B. B\$\$(i, i) \in \text{Reals})$  ⟨proof⟩

**lemma** *hermitian-decomp-decomp'*:  
**fixes**  $A::\text{complex Matrix.mat}$   
**assumes** *hermitian-decomp*  $A \ B \ U$   
**shows** *real-diag-decomp*  $A \ B \ U$

*<proof>*

**lemma** *real-diag-decomp-hermitian:*

**fixes** *A::complex Matrix.mat*  
**assumes** *real-diag-decomp A B U*  
**shows** *hermitian A*

*<proof>*

**lemma** *unitary-conjugate-real-diag-decomp:*

**assumes** *A ∈ carrier-mat n n*  
**and** *Us ∈ carrier-mat n n*  
**and** *unitary Us*  
**and** *real-diag-decomp (mat-conj (Complex-Matrix.adjoint Us) A) B U*  
**shows** *real-diag-decomp A B (Us \* U) <proof>*

## 2.3 On the spectrum of a matrix

**lemma** *similar-spectrum-eq:*

**fixes** *A::complex Matrix.mat*  
**assumes** *A ∈ carrier-mat n n*  
**and** *similar-mat A B*  
**and** *upper-triangular B*  
**shows** *spectrum A = set (diag-mat B)*

*<proof>*

**lemma** *unitary-diag-spectrum-eq:*

**fixes** *A::complex Matrix.mat*  
**assumes** *A ∈ carrier-mat n n*  
**and** *unitary-diag A B U*  
**shows** *spectrum A = set (diag-mat B)*

*<proof>*

**lemma** *unitary-diag-spectrum-eq':*

**fixes** *A::complex Matrix.mat*  
**assumes** *A ∈ carrier-mat n n*  
**and** *unitary-diag A B U*  
**shows** *spectrum A = diag-elems B*

*<proof>*

**lemma** *hermitian-real-diag-decomp:*

**fixes** *A::complex Matrix.mat*  
**assumes** *A ∈ carrier-mat n n*  
**and** *0 < n*  
**and** *hermitian A*

**obtains** *B U where real-diag-decomp A B U*

*<proof>*

**lemma** *spectrum-smult:*

**fixes** *A::complex Matrix.mat*

**assumes** *hermitian A*  
**and**  $A \in \text{carrier-mat } n \ n$   
**and**  $0 < n$   
**shows**  $\text{spectrum } (x \cdot_m A) = \{x * a \mid a. a \in \text{spectrum } A\}$   
 $\langle \text{proof} \rangle$

**lemma** *spectrum-uminus*:  
**fixes**  $A::\text{complex Matrix.mat}$   
**assumes** *hermitian A*  
**and**  $A \in \text{carrier-mat } n \ n$   
**and**  $0 < n$   
**shows**  $\text{spectrum } (-A) = \{-a \mid a. a \in \text{spectrum } A\}$   
 $\langle \text{proof} \rangle$

### 3 Properties of the inner product

#### 3.1 Some analysis complements

**lemma** *add-conj-le*:  
**shows**  $z + \text{cnj } z \leq 2 * \text{cmod } z$   
 $\langle \text{proof} \rangle$

**lemma** *abs-real*:  
**fixes**  $x::\text{complex}$   
**assumes**  $x \in \text{Reals}$   
**shows**  $\text{abs } x \in \text{Reals}$   $\langle \text{proof} \rangle$

**lemma** *csqrt-cmod-square*:  
**shows**  $\text{csqrt } ((\text{cmod } z)^2) = \text{cmod } z$   
 $\langle \text{proof} \rangle$

**lemma** *cpx-real-le*:  
**fixes**  $z::\text{complex}$   
**assumes**  $0 \leq z$   
**and**  $0 \leq u$   
**and**  $z^2 \leq u^2$   
**shows**  $z \leq u$   
 $\langle \text{proof} \rangle$

**lemma** *mult-conj-real*:  
**fixes**  $v::\text{complex}$   
**shows**  $v * (\text{conjugate } v) \in \text{Reals}$   
 $\langle \text{proof} \rangle$

**lemma** *real-sum-real*:  
**assumes**  $\bigwedge i. i < n \implies ((f \ i)::\text{complex}) \in \text{Reals}$   
**shows**  $(\sum i \in \{0 ..< n\}. f \ i) \in \text{Reals}$   
 $\langle \text{proof} \rangle$

**lemma** *real-mult-re*:  
**assumes**  $a \in \text{Reals}$  **and**  $b \in \text{Reals}$   
**shows**  $\text{Re } (a * b) = \text{Re } a * \text{Re } b$   $\langle \text{proof} \rangle$

**lemma** *complex-positive-Im*:  
**fixes**  $b::\text{complex}$   
**assumes**  $0 \leq b$   
**shows**  $\text{Im } b = 0$   
 $\langle \text{proof} \rangle$

**lemma** *cmod-pos*:  
**fixes**  $z::\text{complex}$   
**assumes**  $0 \leq z$   
**shows**  $\text{cmod } z = z$   
 $\langle \text{proof} \rangle$

**lemma** *cpx-pos-square-pos*:  
**fixes**  $z::\text{complex}$   
**assumes**  $0 \leq z$   
**shows**  $0 \leq z^2$   
 $\langle \text{proof} \rangle$

**lemma** *cmod-mult-pos*:  
**fixes**  $b::\text{complex}$   
**fixes**  $z::\text{complex}$   
**assumes**  $0 \leq b$   
**shows**  $\text{cmod } (b * z) = \text{Re } b * \text{cmod } z$   $\langle \text{proof} \rangle$

**lemma** *cmod-conjugate-square-eq*:  
**fixes**  $z::\text{complex}$   
**shows**  $\text{cmod } (z * (\text{conjugate } z)) = z * (\text{conjugate } z)$   
 $\langle \text{proof} \rangle$

**lemma** *pos-sum-gt-comp*:  
**assumes** *finite*  $I$   
**and**  $\bigwedge i. i \in I \implies (0::\text{real}) \leq f i$   
**and**  $j \in I$   
**and**  $c < f j$   
**shows**  $c < \text{sum } f I$   
 $\langle \text{proof} \rangle$

**lemma** *pos-sum-le-comp*:  
**assumes** *finite*  $I$   
**and**  $\bigwedge i. i \in I \implies (0::\text{real}) \leq f i$   
**and**  $\text{sum } f I \leq c$

**shows**  $\forall i \in I. f i \leq c$   
 $\langle proof \rangle$

**lemma** *square-pos-mult-le*:  
**assumes** *finite I*  
**and**  $\bigwedge i. i \in I \implies ((0::real) \leq f i \wedge f i \leq 1)$   
**shows**  $sum (\lambda x. f x * f x) I \leq sum f I$   $\langle proof \rangle$

**lemma** *square-pos-mult-lt*:  
**assumes** *finite I*  
**and**  $\bigwedge i. i \in I \implies ((0::real) \leq f i \wedge f i \leq 1)$   
**and**  $j \in I$   
**and**  $f j < 1$   
**and**  $0 < f j$   
**shows**  $sum (\lambda x. f x * f x) I < sum f I$   $\langle proof \rangle$

### 3.2 Inner product results

In particular we prove the triangle inequality, i.e. that for vectors  $u$  and  $v$  we have  $\|u + v\| \leq \|u\| + \|v\|$ .

**lemma** *inner-prod-vec-norm-pow2*:  
**shows**  $(vec\text{-}norm\ v)^2 = v \cdot c\ v$   $\langle proof \rangle$

**lemma** *inner-prod-mult-mat-vec-left*:  
**assumes**  $v \in carrier\text{-}vec\ n$   
**and**  $w \in carrier\text{-}vec\ n'$   
**and**  $A \in carrier\text{-}mat\ m\ n$   
**and**  $B \in carrier\text{-}mat\ m\ n'$   
**shows**  $inner\text{-}prod\ (A *_{v}\ v)\ (B *_{v}\ w) =$   
 $inner\text{-}prod\ (((Complex\text{-}Matrix.\text{adjoint}\ B) * A) *_{v}\ v)\ w$   
 $\langle proof \rangle$

**lemma** *rank-1-proj-trace-inner*:  
**fixes**  $A :: 'a::conjugatable\text{-}field\ Matrix.\text{mat}$  **and**  $v :: 'a\ Matrix.\text{vec}$   
**assumes**  $A: A \in carrier\text{-}mat\ n\ n$   
**and**  $v: v \in carrier\text{-}vec\ n$   
**shows**  $Complex\text{-}Matrix.\text{trace}\ (A * (\text{rank}\text{-}1\text{-}proj\ v)) = Complex\text{-}Matrix.\text{inner}\text{-}prod$   
 $v\ (A *_{v}\ v)$   
 $\langle proof \rangle$

**lemma** *unitary-inner-prod*:  
**assumes**  $v \in carrier\text{-}vec\ n$   
**and**  $w \in carrier\text{-}vec\ n$   
**and**  $U \in carrier\text{-}mat\ n\ n$   
**and**  $Complex\text{-}Matrix.\text{unitary}\ U$   
**shows**  $inner\text{-}prod\ (U *_{v}\ v)\ (U *_{v}\ w) = inner\text{-}prod\ v\ w$

*<proof>*

**lemma** *unitary-vec-norm:*

**assumes**  $v \in \text{carrier-vec } n$

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

**and** *Complex-Matrix.unitary*  $U$

**shows**  $\text{vec-norm } (U *_v v) = \text{vec-norm } v$  *<proof>*

**lemma** *unitary-col-norm-square:*

**assumes** *unitary*  $U$

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

**and**  $i < n$

**shows**  $\|\text{Matrix.col } U \ i\|^2 = 1$

*<proof>*

**lemma** *unitary-col-norm:*

**assumes** *unitary*  $U$

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

**and**  $i < n$

**shows**  $\|\text{Matrix.col } U \ i\| = 1$  *<proof>*

**lemma** *inner-mult-diag-expand:*

**fixes**  $B::\text{complex Matrix.mat}$

**assumes** *diagonal-mat*  $B$

**and**  $B \in \text{carrier-mat } n \ n$

**and**  $v \in \text{carrier-vec } n$

**shows**  $\text{inner-prod } (B *_v v) \ v =$

$(\sum i \in \{0 \ .. < n\}. (\text{conjugate } (B \ \$\$ (i,i))) * (\text{vec-index } v \ i * (\text{conjugate } (\text{vec-index } v \ i))))$

*<proof>*

**lemma** *inner-mult-diag-expand':*

**fixes**  $B::\text{complex Matrix.mat}$

**assumes** *diagonal-mat*  $B$

**and**  $B \in \text{carrier-mat } n \ n$

**and**  $v \in \text{carrier-vec } n$

**shows**  $\text{inner-prod } v \ (B *_v v) =$

$(\sum i \in \{0 \ .. < n\}. B \ \$\$ (i,i) * (\text{vec-index } v \ i * (\text{conjugate } (\text{vec-index } v \ i))))$

*<proof>*

**lemma** *self-inner-prod-real:*

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

**shows** *Complex-Matrix.inner-prod*  $v \ v \in \text{Reals}$

*<proof>*

**lemma** *inner-mult-diag-real:*

**fixes**  $B::\text{complex Matrix.mat}$

**assumes** *diagonal-mat*  $B$

**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $\forall i < n. B\$(i, i) \in \text{Reals}$   
**and**  $v \in \text{carrier-vec } n$   
**shows**  $\text{inner-prod } (B *_v v) v \in \text{Reals}$   
 $\langle \text{proof} \rangle$

**lemma** *inner-mult-diag-real*:  
**fixes**  $B::\text{complex Matrix.mat}$   
**assumes** *diagonal-mat*  $B$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $\forall i < n. B\$(i, i) \in \text{Reals}$   
**and**  $v \in \text{carrier-vec } n$   
**shows**  $\text{inner-prod } v (B *_v v) \in \text{Reals}$   
 $\langle \text{proof} \rangle$

**lemma** *inner-prod-mult-mat-vec-right*:  
**assumes**  $v \in \text{carrier-vec } n$   
**and**  $w \in \text{carrier-vec } n'$   
**and**  $A \in \text{carrier-mat } m \ n$   
**and**  $B \in \text{carrier-mat } m \ n'$   
**shows**  $\text{inner-prod } (A *_v v) (B *_v w) =$   
 $\text{inner-prod } v (((\text{Complex-Matrix.adjoint } A) * B) *_v w)$   
 $\langle \text{proof} \rangle$

**lemma** *Cauchy-Schwarz-complex-vec-norm*:  
**assumes**  $\text{dim-vec } x = \text{dim-vec } y$   
**shows**  $\text{cmod } (\text{inner-prod } x y) \leq \text{vec-norm } x * \text{vec-norm } y$   
 $\langle \text{proof} \rangle$

**lemma** *vec-norm-triangle-sq*:  
**fixes**  $u::\text{complex Matrix.vec}$   
**assumes**  $\text{dim-vec } u = \text{dim-vec } v$   
**shows**  $(\text{vec-norm } (u + v))^2 \leq (\text{vec-norm } u + \text{vec-norm } v)^2$   
 $\langle \text{proof} \rangle$

**lemma** *vec-norm-triangle*:  
**fixes**  $u::\text{complex Matrix.vec}$   
**assumes**  $\text{dim-vec } u = \text{dim-vec } v$   
**shows**  $\text{vec-norm } (u + v) \leq \text{vec-norm } u + \text{vec-norm } v$   
 $\langle \text{proof} \rangle$

## 4 Matrix decomposition

**lemma** (*in cpx-sq-mat*) *sum-decomp-cols*:  
**fixes**  $A::\text{complex Matrix.mat}$   
**assumes** *hermitian*  $A$   
**and**  $A \in \text{fc-mats}$   
**and** *unitary-diag*  $A \ B \ U$   
**shows**  $\text{sum-mat } (\lambda i. (\text{diag-mat } B \ ! \ i) \cdot_m \text{rank-1-proj } (\text{Matrix.col } U \ i))$

$\{.. < \dim R\} = A$   
 ⟨proof⟩

**lemma** *unitary-col-inner-prod*:

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

and  $0 < n$

and *Complex-Matrix.unitary*  $A$

and  $j < n$

and  $k < n$

shows *Complex-Matrix.inner-prod* (*Matrix.col*  $A \ j$ ) (*Matrix.col*  $A \ k$ ) =  
 ( $1_m \ n$ )  $\$\$(j,k)$

⟨proof⟩

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

assumes *finite*  $I$

and  $j \in I$

and  $A \ j * A \ j = A \ j$

and  $\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}$

and  $\bigwedge i. i \in I \implies i \neq j \implies A \ i * (A \ j) = (0_m \ \dim R \ \dim R)$

shows (*sum-mat*  $A \ I$ ) \* ( $A \ j$ ) = ( $A \ j$ ) ⟨proof⟩

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

assumes *finite*  $I$

and  $j \in I$

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

and  $\bigwedge i. i \in I \implies A \ i \in \text{fc-mats}$

and  $\bigwedge i. i \in I \implies i \neq j \implies A \ i * B = (0_m \ \dim R \ \dim R)$

shows (*sum-mat*  $A \ I$ ) \*  $B = A \ j * B$  ⟨proof⟩

**lemma** *unitarily-equiv-rank-1-proj-col-carrier*:

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

and *unitarily-equiv*  $A \ B \ U$

and  $i < n$

shows *rank-1-proj* (*Matrix.col*  $U \ i$ )  $\in \text{carrier-mat } n \ n$

⟨proof⟩

**lemma** *decomp-eigenvector*:

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

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

and  $0 < n$

and *hermitian*  $A$

and *unitary-diag*  $A \ B \ U$

and  $j < n$

shows *Complex-Matrix.trace* ( $A * (\text{rank-1-proj} (\text{Matrix.col } U \ j))) = B \ \$(j,j)$

⟨proof⟩

**lemma** *positive-unitary-diag-pos*:

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

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

**and** *Complex-Matrix.positive*  $A$   
**and** *unitary-diag*  $A B U$   
**and**  $j < n$   
**shows**  $0 \leq B \text{ } \$(j, j)$   
 $\langle \text{proof} \rangle$

**lemma** *unitary-diag-trace-mult-sum*:  
**fixes**  $A::\text{complex Matrix.mat}$   
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $C \in \text{carrier-mat } n \ n$   
**and** *hermitian*  $A$   
**and** *unitary-diag*  $A B U$   
**and**  $0 < n$   
**shows**  $\text{Complex-Matrix.trace } (C * A) =$   
 $(\sum i = 0 ..< n. B \text{ } \$(i, i) * \text{Complex-Matrix.trace } (C * \text{rank-1-proj } (\text{Matrix.col } U \ i)))$   
 $\langle \text{proof} \rangle$

**lemma** *unitarily-equiv-trace*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and** *unitarily-equiv*  $A B U$   
**shows**  $\text{Complex-Matrix.trace } A = \text{Complex-Matrix.trace } B$   
 $\langle \text{proof} \rangle$

**lemma** *unitarily-equiv-trace'*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and** *unitarily-equiv*  $A B U$   
**shows**  $\text{Complex-Matrix.trace } A = (\sum i = 0 ..< \text{dim-row } A. B \text{ } \$(i, i))$   
 $\langle \text{proof} \rangle$

**lemma** *positive-decomp-cmod-le*:  
**fixes**  $A::\text{complex Matrix.mat}$   
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $C \in \text{carrier-mat } n \ n$   
**and**  $0 < n$   
**and** *Complex-Matrix.positive*  $A$   
**and** *unitary-diag*  $A B U$   
**and**  $\bigwedge i. i < n \implies \text{cmod } (\text{Complex-Matrix.trace } (C * \text{rank-1-proj } (\text{Matrix.col } U \ i))) \leq M$   
**shows**  $\text{cmod } (\text{Complex-Matrix.trace } (C * A)) \leq \text{Re } (\text{Complex-Matrix.trace } A) * M$   
 $\langle \text{proof} \rangle$   
**end**

**theory** *Commuting-Hermitian* **imports** *Spectral-Theory-Complements* *Commuting-Hermitian-Misc*  
*Projective-Measurements.Linear-Algebra-Complements*  
*Projective-Measurements.Projective-Measurements* **begin**

## 5 Additional results on block decompositions of matrices

### 5.1 Split block results

**lemma** *split-block-diag-carrier*:  
 assumes  $D \in \text{carrier-mat } n \ n$   
 and  $a \leq n$   
 and *split-block*  $D \ a \ a = (D1, D2, D3, D4)$   
**shows**  $D1 \in \text{carrier-mat } a \ a \ D4 \in \text{carrier-mat } (n-a) \ (n-a)$   
 *<proof>*

**lemma** *split-block-diagonal*:  
 assumes *diagonal-mat*  $D$   
 and  $D \in \text{carrier-mat } n \ n$   
 and  $a \leq n$   
 and *split-block*  $D \ a \ a = (D1, D2, D3, D4)$   
**shows** *diagonal-mat*  $D1 \wedge \text{diagonal-mat } D4$  *<proof>*

**lemma** *split-block-times-diag-index*:  
 fixes  $B::'a::\text{comm-ring } \text{Matrix.mat}$   
 assumes *diagonal-mat*  $D$   
 and  $D \in \text{carrier-mat } n \ n$   
 and  $B \in \text{carrier-mat } n \ n$   
 and  $a \leq n$   
 and *split-block*  $B \ a \ a = (B1, B2, B3, B4)$   
 and *split-block*  $D \ a \ a = (D1, D2, D3, D4)$   
 and  $i < \text{dim-row } (D4 * B4)$   
 and  $j < \text{dim-col } (D4 * B4)$   
**shows**  $(B4 * D4) \ \$\$ \ (i, j) = (B*D) \ \$\$ \ (i+a, j+a)$   
  $(D4 * B4) \ \$\$ \ (i, j) = (D*B) \ \$\$ \ (i+a, j+a)$   
 *<proof>*

**lemma** *split-block-commute-subblock*:  
 fixes  $B::'a::\text{comm-ring } \text{Matrix.mat}$   
 assumes *diagonal-mat*  $D$   
 and  $D \in \text{carrier-mat } n \ n$   
 and  $B \in \text{carrier-mat } n \ n$   
 and  $a \leq n$   
 and *split-block*  $B \ a \ a = (B1, B2, B3, B4)$   
 and *split-block*  $D \ a \ a = (D1, D2, D3, D4)$   
 and  $B * D = D * B$   
**shows**  $B4 * D4 = D4 * B4$   
 *<proof>*

**lemma** *commute-diag-mat-zero-comp*:  
 fixes  $D::'a::\{\text{field}\} \ \text{Matrix.mat}$   
 assumes *diagonal-mat*  $D$   
 and  $D \in \text{carrier-mat } n \ n$

**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $B * D = D * B$   
**and**  $i < n$   
**and**  $j < n$   
**and**  $D_{(i,i)} \neq D_{(j,j)}$   
**shows**  $B_{(i,j)} = 0$   
 $\langle \text{proof} \rangle$

**lemma** *commute-diag-mat-split-block*:  
**fixes**  $D :: 'a :: \{\text{field}\} \text{Matrix.mat}$   
**assumes** *diagonal-mat*  $D$   
**and**  $D \in \text{carrier-mat } n \ n$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $B * D = D * B$   
**and**  $k \leq n$   
**and**  $\forall i \ j. (i < k \wedge k \leq j \wedge j < n) \longrightarrow D_{(i,i)} \neq D_{(j,j)}$   
**and**  $(B_1, B_2, B_3, B_4) = \text{split-block } B \ k \ k$   
**shows**  $B_2 = 0_m \ k \ (n-k)$   $B_3 = 0_m \ (n-k) \ k$   
 $\langle \text{proof} \rangle$

**lemma** *split-block-hermitian-1*:  
**assumes** *hermitian*  $A$   
**and**  $n \leq \text{dim-row } A$   
**and**  $(A_1, A_2, A_3, A_4) = \text{split-block } A \ n \ n$   
**shows** *hermitian*  $A_1$   $\langle \text{proof} \rangle$

**lemma** *split-block-hermitian-4*:  
**assumes** *hermitian*  $A$   
**and**  $n \leq \text{dim-row } A$   
**and**  $(A_1, A_2, A_3, A_4) = \text{split-block } A \ n \ n$   
**shows** *hermitian*  $A_4$   $\langle \text{proof} \rangle$

**lemma** *diag-block-split-block*:  
**assumes**  $B \in \text{carrier-mat } n \ n$   
**and**  $k < n$   
**and**  $(B_1, B_2, B_3, B_4) = \text{split-block } B \ k \ k$   
**and**  $B_2 = 0_m \ k \ (n-k)$   
**and**  $B_3 = 0_m \ (n-k) \ k$   
**shows**  $B = \text{diag-block-mat } [B_1, B_4]$   
 $\langle \text{proof} \rangle$

## 5.2 Diagonal block matrices

**abbreviation** *four-block-diag* **where**  
*four-block-diag*  $B_1 \ B_2 \equiv$   
 $(\text{four-block-mat } B_1 \ (0_m \ (\text{dim-row } B_1) \ (\text{dim-col } B_2)))$   
 $(0_m \ (\text{dim-row } B_2) \ (\text{dim-col } B_1)) \ B_2$

**lemma** *four-block-diag-cong-comp*:

**assumes**  $\dim\text{-row } A1 = \dim\text{-row } B1$   
**and**  $\dim\text{-col } A1 = \dim\text{-col } B1$   
**and**  $\text{four-block-diag } A1 \ A2 = \text{four-block-diag } B1 \ B2$   
**shows**  $A1 = B1$   
 $\langle \text{proof} \rangle$

**lemma** *four-block-diag-cong-comp'*:  
**assumes**  $\dim\text{-row } A1 = \dim\text{-row } B1$   
**and**  $\dim\text{-col } A1 = \dim\text{-col } B1$   
**and**  $\text{four-block-diag } A1 \ A2 = \text{four-block-diag } B1 \ B2$   
**shows**  $A2 = B2$   
 $\langle \text{proof} \rangle$

**lemma** *four-block-mat-real-diag*:  
**assumes**  $\forall i < \dim\text{-row } B1. B1\$(i,i) \in \text{Reals}$   
**and**  $\forall i < \dim\text{-row } B2. B2\$(i,i) \in \text{Reals}$   
**and**  $\dim\text{-row } B1 = \dim\text{-col } B1$   
**and**  $\dim\text{-row } B2 = \dim\text{-col } B2$   
**and**  $i < \dim\text{-row } (\text{four-block-diag } B1 \ B2)$   
**shows**  $(\text{four-block-diag } B1 \ B2)\$(i,i) \in \text{Reals}$   
 $\langle \text{proof} \rangle$

**lemma** *four-block-diagonal*:  
**assumes**  $\dim\text{-row } B1 = \dim\text{-col } B1$   
**and**  $\dim\text{-row } B2 = \dim\text{-col } B2$   
**and** *diagonal-mat*  $B1$   
**and** *diagonal-mat*  $B2$   
**shows** *diagonal-mat*  $(\text{four-block-diag } B1 \ B2) \langle \text{proof} \rangle$

**lemma** *four-block-diag-zero*:  
**assumes**  $B \in \text{carrier-mat } 0 \ 0$   
**shows**  $\text{four-block-diag } A \ B = A$   
 $\langle \text{proof} \rangle$

**lemma** *four-block-diag-zero'*:  
**assumes**  $B \in \text{carrier-mat } 0 \ 0$   
**shows**  $\text{four-block-diag } B \ A = A$   
 $\langle \text{proof} \rangle$

**lemma** *mult-four-block-diag*:  
**assumes**  $A1 \in \text{carrier-mat } nr1 \ n1 \ D1 \in \text{carrier-mat } nr2 \ n2$   
**and**  $A2 \in \text{carrier-mat } n1 \ nc1 \ D2 \in \text{carrier-mat } n2 \ nc2$   
**shows**  $\text{four-block-diag } A1 \ D1 \ *$   
 $\text{four-block-diag } A2 \ D2$   
 $= \text{four-block-diag } (A1 \ * \ A2) \ (D1 \ * \ D2)$   
 $\langle \text{proof} \rangle$

**lemma** *four-block-diag-adjoint*:  
**shows**  $(\text{Complex-Matrix.adjoint } (\text{four-block-diag } A1 \ A2)) =$

(*four-block-diag* (*Complex-Matrix.adjoint* *A1*)  
(*Complex-Matrix.adjoint* *A2*))  
⟨*proof*⟩

**lemma** *four-block-diag-unitary*:

**assumes** *unitary* *U1*

**and** *unitary* *U2*

**shows** *unitary*

(*four-block-diag* *U1* *U2*)

(**is** *unitary* ?*fU*)

⟨*proof*⟩

**lemma** *four-block-diag-similar*:

**assumes** *unitarily-equiv* *A1* *B1* *U1*

**and** *unitarily-equiv* *A2* *B2* *U2*

**and** *dim-row* *A1* = *dim-col* *A1*

**and** *dim-row* *A2* = *dim-col* *A2*

**shows** *similar-mat-wit*

(*four-block-diag* *A1* *A2*)

(*four-block-diag* *B1* *B2*)

(*four-block-diag* *U1* *U2*)

(*Complex-Matrix.adjoint* (*four-block-diag* *U1* *U2*))

⟨*proof*⟩

**lemma** *four-block-unitarily-equiv*:

**assumes** *unitarily-equiv* *A1* *B1* *U1*

**and** *unitarily-equiv* *A2* *B2* *U2*

**and** *dim-row* *A1* = *dim-col* *A1*

**and** *dim-row* *A2* = *dim-col* *A2*

**shows** *unitarily-equiv*

(*four-block-diag* *A1* *A2*)

(*four-block-diag* *B1* *B2*)

(*four-block-diag* *U1* *U2*)

(**is** *unitarily-equiv* ?*fA* ?*fB* ?*fU*)

⟨*proof*⟩

**lemma** *four-block-unitary-diag*:

**assumes** *unitary-diag* *A1* *B1* *U1*

**and** *unitary-diag* *A2* *B2* *U2*

**and** *dim-row* *A1* = *dim-col* *A1*

**and** *dim-row* *A2* = *dim-col* *A2*

**shows** *unitary-diag*

(*four-block-diag* *A1* *A2*)

(*four-block-diag* *B1* *B2*)

(*four-block-diag* *U1* *U2*)

(**is** *unitary-diag* ?*fA* ?*fB* ?*fU*)

⟨*proof*⟩

**lemma** *four-block-real-diag-decomp*:

**assumes** *real-diag-decomp*  $A1\ B1\ U1$   
**and** *real-diag-decomp*  $A2\ B2\ U2$   
**and**  $\dim\text{-row}\ A1 = \dim\text{-col}\ A1$   
**and**  $\dim\text{-row}\ A2 = \dim\text{-col}\ A2$   
**shows** *real-diag-decomp*  
*(four-block-diag*  $A1\ A2)$   
*(four-block-diag*  $B1\ B2)$   
*(four-block-diag*  $U1\ U2)$   
**(is** *real-diag-decomp*  $?fA\ ?fB\ ?fU)$   
*<proof>*

**lemma** *diag-block-mat-mult*:  
**assumes**  $\text{length}\ A1 = \text{length}\ B1$   
**and**  $\forall i < \text{length}\ A1. \dim\text{-col}\ (A!!i) = \dim\text{-row}\ (B!!i)$   
**shows** *diag-block-mat*  $A1 * (\text{diag-block-mat}\ B1) =$   
*(diag-block-mat*  $(\text{map2}\ (*)\ A1\ B1))$  *<proof>*

**lemma** *real-diag-decomp-block*:  
**fixes**  $A1::\text{Complex-Matrix.mat}\ \text{list}$   
**assumes**  $A1 \neq []$   
**and**  $\text{list-all}\ (\lambda A. 0 < \dim\text{-row}\ A \wedge \text{hermitian}\ A)\ A1$   
**shows**  $\exists B1\ U1. \text{length}\ U1 = \text{length}\ A1 \wedge$   
 $(\forall i < \text{length}\ A1.$   
 $U1!!i \in \text{carrier-mat}\ (\dim\text{-row}\ (A!!i))\ (\dim\text{-col}\ (A!!i)) \wedge \text{unitary}\ (U1!!i) \wedge$   
 $B1!!i \in \text{carrier-mat}\ (\dim\text{-row}\ (A!!i))\ (\dim\text{-col}\ (A!!i))) \wedge$   
 $\text{real-diag-decomp}\ (\text{diag-block-mat}\ A1)\ (\text{diag-block-mat}\ B1)\ (\text{diag-block-mat}\ U1)$   
*<proof>*

**lemma** *diag-block-mat-adjoint*:  
**shows** *Complex-Matrix.adjoint*  $(\text{diag-block-mat}\ A1) =$   
*diag-block-mat*  $(\text{map}\ \text{Complex-Matrix.adjoint}\ A1)$   
*<proof>*

**lemma** *diag-block-mat-mat-conj*:  
**assumes**  $\text{length}\ A1 = \text{length}\ B1$   
**and**  $\forall i < \text{length}\ A1. \dim\text{-col}\ (A!!i) = \dim\text{-row}\ (B!!i)$   
**and**  $\forall i < \text{length}\ A1. \dim\text{-row}\ (B!!i) = \dim\text{-col}\ (B!!i)$   
**shows** *mat-conj*  $(\text{diag-block-mat}\ A1)\ (\text{diag-block-mat}\ B1) =$   
*diag-block-mat*  $(\text{map2}\ \text{mat-conj}\ A1\ B1)$   
*<proof>*

**lemma** *diag-block-mat-commute*:  
**assumes**  $\text{length}\ A1 = \text{length}\ B1$   
**and**  $\forall i < \text{length}\ A1. A1!!i * (B1!!i) = B1!!i * (A1!!i)$   
**and**  $\forall i < \text{length}\ A1. \dim\text{-col}\ (A1!!i) = \dim\text{-row}\ (B1!!i)$   
**and**  $\forall i < \text{length}\ A1. \dim\text{-col}\ (B1!!i) = \dim\text{-row}\ (A1!!i)$   
**shows** *diag-block-mat*  $A1 * (\text{diag-block-mat}\ B1) =$   
*diag-block-mat*  $B1 * (\text{diag-block-mat}\ A1)$   
*<proof>*

**lemma** *diag-block-mat-length-1*:  
**assumes**  $\text{length } A1 = 1$   
**shows**  $\text{diag-block-mat } A1 = A1!0$   
 $\langle \text{proof} \rangle$

**lemma** *diag-block-mat-cong-hd*:  
**assumes**  $0 < \text{length } A1$   
**and**  $\text{length } A1 = \text{length } B1$   
**and**  $\text{dim-row } (\text{hd } A1) = \text{dim-row } (\text{hd } B1)$   
**and**  $\text{dim-col } (\text{hd } A1) = \text{dim-col } (\text{hd } B1)$   
**and**  $\text{diag-block-mat } A1 = \text{diag-block-mat } B1$   
**shows**  $\text{hd } A1 = \text{hd } B1$   
 $\langle \text{proof} \rangle$

**lemma** *diag-block-mat-cong-tl*:  
**assumes**  $0 < \text{length } A1$   
**and**  $\text{length } A1 = \text{length } B1$   
**and**  $\text{dim-row } (\text{hd } A1) = \text{dim-row } (\text{hd } B1)$   
**and**  $\text{dim-col } (\text{hd } A1) = \text{dim-col } (\text{hd } B1)$   
**and**  $\text{diag-block-mat } A1 = \text{diag-block-mat } B1$   
**shows**  $\text{diag-block-mat } (\text{tl } A1) = \text{diag-block-mat } (\text{tl } B1)$   
 $\langle \text{proof} \rangle$

**lemma** *diag-block-mat-cong-comp*:  
**assumes**  $\text{length } A1 = \text{length } B1$   
**and**  $\forall i < \text{length } A1. \text{dim-row } (A1 ! i) = \text{dim-row } (B1 ! i)$   
**and**  $\forall i < \text{length } A1. \text{dim-col } (A1 ! i) = \text{dim-col } (B1 ! i)$   
**and**  $\text{diag-block-mat } A1 = \text{diag-block-mat } B1$   
**and**  $j < \text{length } A1$   
**shows**  $A1!j = B1!j$   $\langle \text{proof} \rangle$

**lemma** *diag-block-mat-commute-comp*:  
**assumes**  $\text{length } A1 = \text{length } B1$   
**and**  $\forall i < \text{length } A1. \text{dim-row } (A1 ! i) = \text{dim-col } (A1 ! i)$   
**and**  $\forall i < \text{length } A1. \text{dim-row } (A1 ! i) = \text{dim-row } (B1 ! i)$   
**and**  $\forall i < \text{length } A1. \text{dim-col } (A1 ! i) = \text{dim-col } (B1 ! i)$   
**and**  $\text{diag-block-mat } A1 * (\text{diag-block-mat } B1) =$   
 $\text{diag-block-mat } B1 * (\text{diag-block-mat } A1)$   
**and**  $i < \text{length } A1$   
**shows**  $A1!i * B1!i = B1!i * A1!i$   
 $\langle \text{proof} \rangle$

**lemma** *diag-block-mat-dim-row-cong*:  
**assumes**  $\text{length } U1 = \text{length } B1$   
**and**  $\forall i < \text{length } B1. \text{dim-row } (B1!i) = \text{dim-row } (U1!i)$   
**shows**  $\text{dim-row } (\text{diag-block-mat } U1) = \text{dim-row } (\text{diag-block-mat } B1)$   
 $\langle \text{proof} \rangle$

**lemma** *diag-block-mat-dim-col-cong*:  
**assumes**  $\text{length } Ul = \text{length } Bl$   
**and**  $\forall i < \text{length } Bl. \text{dim-col } (B!!i) = \text{dim-col } (U!!i)$   
**shows**  $\text{dim-col } (\text{diag-block-mat } Ul) = \text{dim-col } (\text{diag-block-mat } Bl)$   
 $\langle \text{proof} \rangle$

**lemma** *diag-block-mat-dim-row-col-eq*:  
**assumes**  $\forall i < \text{length } Al. \text{dim-row } (A!!i) = \text{dim-col } (A!!i)$   
**shows**  $\text{dim-row } (\text{diag-block-mat } Al) = \text{dim-col } (\text{diag-block-mat } Al)$   
 $\langle \text{proof} \rangle$

## 6 Block matrix decomposition

### 6.1 Subdiagonal extraction

`extract_subdiags` returns a list of diagonal sub-blocks, the sizes of which are specified by the list of integers provided as parameters.

**fun** *extract-subdiags* **where**  
 $\text{extract-subdiags } B \ [] = []$   
 $| \text{extract-subdiags } B (x\#xs) =$   
 $(\text{let } (B1, B2, B3, B4) = (\text{split-block } B \ x \ x) \text{ in}$   
 $B1 \ \# (\text{extract-subdiags } B4 \ xs))$

**lemma** *extract-subdiags-not-emp*:  
**fixes**  $x::\text{nat}$  **and**  $l::\text{nat list}$   
**assumes**  $(B1, B2, B3, B4) = (\text{split-block } B \ x \ x)$   
**shows**  $\text{hd } (\text{extract-subdiags } B (x\#l)) = B1$   
 $\text{tl } (\text{extract-subdiags } B (x\#l)) = \text{extract-subdiags } B4 \ l$   
 $\langle \text{proof} \rangle$

**lemma** *extract-subdiags-neq-Nil*:  
**shows**  $\text{extract-subdiags } B (a\#l) \neq []$   
 $\langle \text{proof} \rangle$

**lemma** *extract-subdiags-length*:  
**shows**  $\text{length } (\text{extract-subdiags } B \ l) = \text{length } l$   
 $\langle \text{proof} \rangle$

**lemma** *extract-subdiags-carrier*:  
**assumes**  $i < \text{length } l$   
**shows**  $(\text{extract-subdiags } B \ l)!!i \in \text{carrier-mat } (l!!i) (l!!i)$   $\langle \text{proof} \rangle$

**lemma** *extract-subdiags-diagonal*:  
**assumes** *diagonal-mat*  $B$   
**and**  $B \in \text{carrier-mat } n \ n$   
**and**  $l \neq []$   
**and** *sum-list*  $l \leq n$   
**and**  $i < \text{length } l$

**shows** *diagonal-mat* ((*extract-subdiags* *B* *l*)!i) ⟨*proof*⟩

**lemma** *extract-subdiags-diag-elem*:

**fixes** *B*::*complex Matrix.mat*

**assumes** *B* ∈ *carrier-mat* *n n*

**and**  $0 < n$

**and**  $l \neq []$

**and**  $i < \text{length } l$

**and**  $j < l!i$

**and** *sum-list*  $l \leq n$

**and**  $\forall j < \text{length } l. 0 < l!j$

**shows** *extract-subdiags* *B* *l*!i \$\$ (j,j) =  
*diag-mat* *B*!(*n-sum* *i l* + j) ⟨*proof*⟩

**lemma** *hermitian-extract-subdiags*:

**assumes** *hermitian* *A*

**and** *sum-list*  $l \leq \text{dim-row } A$

**and** *list-all* ( $\lambda a. 0 < a$ ) *l*

**shows** *list-all* ( $\lambda B. 0 < \text{dim-row } B \wedge \text{hermitian } B$ ) (*extract-subdiags* *A* *l*)  
 ⟨*proof*⟩

## 6.2 Predicates on diagonal block matrices

The predicate **diag\_compat** ensures that the provided matrix, when decomposed according to the list of integers provided as an input, is indeed a diagonal block matrix.

**fun** *diag-compat* **where**

*diag-compat* *B* [] = (*dim-row* *B* = 0 ∧ *dim-col* *B* = 0)

| *diag-compat* *B* (*x*#*xs*) =

( $x \leq \text{dim-row } B \wedge$

(*let*  $n = \text{dim-row } B$ ; (*B*1, *B*2, *B*3, *B*4) = (*split-block* *B* *x* *x*) in

$B2 = (0_m \ x \ (n - x)) \wedge B3 = (0_m \ (n - x) \ x) \wedge \text{diag-compat } B4 \ xs$ )

When this is the case, the decomposition of a matrix leaves it unchanged.

**lemma** *diag-compat-extract-subdiag*:

**assumes** *B* ∈ *carrier-mat* *n n*

**and** *diag-compat* *B* *l*

**shows** *B* = *diag-block-mat* (*extract-subdiags* *B* *l*) ⟨*proof*⟩

Predicate **diag\_diff** holds when the decomposition of the considered matrix based on the list of integers provided as a parameter, is such that the diagonal elements of separate components are pairwise distinct.

**fun** *diag-diff* **where**

*diag-diff* *D* [] = (*dim-row* *D* = 0 ∧ *dim-col* *D* = 0)

| *diag-diff* *D* (*x*#*xs*) =

( $x \leq \text{dim-row } D \wedge$

(*let* (*D*1, *D*2, *D*3, *D*4) = (*split-block* *D* *x* *x*) in

$(\forall i \ j. i < \text{dim-row } D1 \wedge j < \text{dim-row } D4 \longrightarrow D1\$(i,i) \neq D4 \$(j,j)) \wedge$

*diag-diff D4 xs)*)

**lemma** *diag-diff-hd-diff*:  
**assumes** *diag-diff D (a#xs)*  
**and** *D ∈ carrier-mat n n*  
**and** *i < a*  
**and** *a ≤ j*  
**and** *j < n*  
**shows** *D\$(i,i) ≠ D \$(j,j)*  
*<proof>*

**lemma** *diag-compat-diagonal*:  
**assumes** *B ∈ carrier-mat (dim-row B) (dim-row B)*  
**and** *diagonal-mat B*  
**and** *dim-row B = sum-list l*  
**shows** *diag-compat B l <proof>*

The following lemma provides a sufficient condition for the `diag_compat` predicate to hold.

**lemma** *commute-diag-compat*:  
**fixes** *D::'a::{field} Matrix.mat*  
**assumes** *diagonal-mat D*  
**and** *D ∈ carrier-mat n n*  
**and** *B ∈ carrier-mat n n*  
**and** *B \* D = D \* B*  
**and** *diag-diff D l*  
**shows** *diag-compat B l <proof>*

### 6.3 Counting similar neighbours in a list

The function `eq_comps` takes a list as an input and counts the number of adjacent elements that are identical.

**fun** *eq\_comps* :: *'a list ⇒ nat list* **where**  
*eq\_comps [] = []*  
*| eq\_comps [x] = [1]*  
*| eq\_comps (x#y#l) = (let tmp = (eq\_comps (y#l)) in*  
*if x = y then Suc (hd tmp) # (tl tmp)*  
*else 1 # tmp)*

**lemma** *eq\_comps-not-empty*:  
**assumes** *l ≠ []*  
**shows** *eq\_comps l ≠ [] <proof>*

**lemma** *eq\_comps-empty-if*:  
**assumes** *eq\_comps l = []*  
**shows** *l = []*  
*<proof>*

**lemma** *eq-comps-hd-eq-tl*:  
**assumes**  $x = y$   
**shows**  $tl (eq-comps (x\#y\#l)) = tl (eq-comps (y\#l))$   $\langle proof \rangle$

**lemma** *eq-comps-hd-neq-tl*:  
**assumes**  $x \neq y$   
**shows**  $tl (eq-comps (x\#y\#l)) = eq-comps (y\#l)$   $\langle proof \rangle$

**lemma** *eq-comps-drop*:  
**assumes**  $x\#xs = eq-comps l$   
**shows**  $xs = eq-comps (drop x l)$   $\langle proof \rangle$

**lemma** *eq-comps-neq-0*:  
**assumes**  $a\#m = eq-comps l$   
**shows**  $a \neq 0$   $\langle proof \rangle$

**lemma** *eq-comps-gt-0*:  
**assumes**  $l \neq []$   
**shows**  $list-all (\lambda a. 0 < a) (eq-comps l)$   
 $\langle proof \rangle$

**lemma** *eq-comps-elem-le-length*:  
**assumes**  $a\#m = eq-comps l$   
**shows**  $a \leq length l$   $\langle proof \rangle$

**lemma** *eq-comps-length*:  
**shows**  $length (eq-comps l) \leq length l$   
 $\langle proof \rangle$

**lemma** *eq-comps-eq*:  
**assumes**  $a\#m = eq-comps l$   
**and**  $i < a$   
**shows**  $nth l i = hd l$   $\langle proof \rangle$

**lemma** *eq-comps-singleton*:  
**assumes**  $[a] = eq-comps l$   
**shows**  $a = length l$   $\langle proof \rangle$

**lemma** *eq-comps-leq*:  
**assumes**  $a\#b\#m = eq-comps l$   
**and** *sorted*  $l$   
**shows**  $hd l < hd (drop a l)$   $\langle proof \rangle$

**lemma** *eq-comps-compare*:  
**assumes** *sorted*  $l$   
**and**  $a\#m = eq-comps l$   
**and**  $i < a$   
**and**  $a \leq j$   
**and**  $j < length l$

**shows**  $\text{nth } l \ i < \text{nth } l \ j$   $\langle \text{proof} \rangle$

**lemma** *eq-comps-singleton-elems*:

**assumes**  $\text{eq-comps } l = [a]$

**shows**  $\forall i < \text{length } l. \text{!}i = \text{!}0$   $\langle \text{proof} \rangle$

**lemma** *eq-comp-Re*:

**assumes**  $\forall z \in \text{set } l. z \in \text{Reals}$

**and**  $m = \text{eq-comps } l$

**shows**  $m = \text{eq-comps } (\text{map } \text{Re } l)$   $\langle \text{proof} \rangle$

**lemma** *eq-comps-sum-list*:

**shows**  $\text{sum-list } (\text{eq-comps } l) = \text{length } l$   
 $\langle \text{proof} \rangle$

**lemma** *eq-comps-elem-lt*:

**assumes**  $1 < \text{length } (\text{eq-comps } l)$

**shows**  $\text{hd } (\text{eq-comps } l) < \text{length } l$   
 $\langle \text{proof} \rangle$

**lemma** *eq-comp-sum-diag-mat*:

**shows**  $\text{sum-list } (\text{eq-comps } (\text{diag-mat } A)) = \text{dim-row } A$   
 $\langle \text{proof} \rangle$

**lemma** *nsum-Suc-elem*:

**assumes**  $1 < \text{length } (\text{eq-comps } l)$

**shows**  $\text{!}(n\text{-sum } (\text{Suc } i) (\text{eq-comps } l)) =$   
 $(\text{drop } (\text{hd } (\text{eq-comps } l)) \ l) \ \text{!}(n\text{-sum } i \ (\text{tl } (\text{eq-comps } l)))$   $\langle \text{proof} \rangle$

**lemma** *eq-comps-elems-eq*:

**assumes**  $l \neq []$

**and**  $i < \text{length } (\text{eq-comps } l)$

**and**  $j < (\text{eq-comps } l) \ \text{!}i$

**shows**  $\text{!}(n\text{-sum } i \ (\text{eq-comps } l)) = \text{!}(n\text{-sum } i \ (\text{eq-comps } l) + j)$   $\langle \text{proof} \rangle$

When the diagonal block matrices are extracted using `eq_comp`, each extracted matrix is a multiple of the identity.

**lemma** *extract-subdiags-eq-comp*:

**fixes**  $A::\text{complex Matrix.mat}$

**assumes** *diagonal-mat*  $A$

**and**  $A \in \text{carrier-mat } n \ n$

**and**  $0 < n$

**and**  $i < \text{length } (\text{eq-comps } (\text{diag-mat } A))$

**shows**  $\exists k. (\text{extract-subdiags } A \ (\text{eq-comps } (\text{diag-mat } A))) \ \text{!}i =$   
 $k \cdot_m (1_m \ ((\text{eq-comps } (\text{diag-mat } A)) \ \text{!}i))$   
 $\langle \text{proof} \rangle$

**lemma** *extract-subdiags-comp-commute*:

**fixes**  $A::\text{complex Matrix.mat}$

```

assumes diagonal-mat A
and  $A \in \text{carrier-mat } n \ n$ 
and  $0 < n$ 
and  $i < \text{length } (\text{eq-comps } (\text{diag-mat } A))$ 
and  $B \in \text{carrier-mat } ((\text{eq-comps } (\text{diag-mat } A))!i) \ ((\text{eq-comps } (\text{diag-mat } A))!i)$ 
shows  $(\text{extract-subdiags } A \ (\text{eq-comps } (\text{diag-mat } A))!i) * B =$ 
 $B * (\text{extract-subdiags } A \ (\text{eq-comps } (\text{diag-mat } A))!i)$ 
<proof>

```

In particular, extracting the diagonal sub-blocks of a diagonal matrix leaves it unchanged.

```

lemma diagonal-extract-eq:
assumes  $B \in \text{carrier-mat } n \ n$ 
and diagonal-mat B
shows  $B = \text{diag-block-mat } (\text{extract-subdiags } B \ (\text{eq-comps } (\text{diag-mat } B)))$ 
<proof>

```

```

fun lst-diff where
  lst-diff  $l \ [] = (l = [])$ 
| lst-diff  $l \ (x\#\!xs) = (x \leq \text{length } l \wedge$ 
   $(\forall i \ j. \ i < x \wedge x \leq j \wedge j < \text{length } l \longrightarrow \text{nth } l \ i < \text{nth } l \ j) \wedge$ 
  lst-diff  $(\text{drop } x \ l) \ xs)$ 

```

```

lemma sorted-lst-diff:
assumes sorted l
and  $m = \text{eq-comps } l$ 
shows lst-diff  $l \ m$  <proof>

```

```

lemma lst-diff-imp-diag-diff:
fixes  $D::'a::\text{preorder } \text{Matrix.mat}$ 
assumes  $D \in \text{carrier-mat } n \ n$ 
and lst-diff  $(\text{diag-mat } D) \ m$ 
shows diag-diff  $D \ m$  <proof>

```

```

lemma sorted-diag-diff:
fixes  $D::'a::\text{linorder } \text{Matrix.mat}$ 
assumes  $D \in \text{carrier-mat } n \ n$ 
and sorted  $(\text{diag-mat } D)$ 
shows diag-diff  $D \ (\text{eq-comps } (\text{diag-mat } D))$ 
<proof>

```

```

lemma Re-sorted-lst-diff:
fixes  $l::\text{complex list}$ 
assumes  $\forall z \in \text{set } l. \ z \in \text{Reals}$ 
and sorted  $(\text{map } \text{Re } l)$ 
and  $m = \text{eq-comps } l$ 
shows lst-diff  $l \ m$  <proof>

```

The following lemma states a sufficient condition for the `diag_diff` predi-

cate to hold.

**lemma** *cpx-sorted-diag-diff*:  
**fixes**  $D :: \text{complex Matrix.mat}$   
**assumes**  $D \in \text{carrier-mat } n \ n$   
**and**  $\forall i < n. D \$(i,i) \in \text{Reals}$   
**and** *sorted* (*map Re* (*diag-mat*  $D$ ))  
**shows** *diag-diff*  $D$  (*eq-comps* (*diag-mat*  $D$ ))  
*<proof>*

## 7 Sorted hermitian decomposition

We prove that any Hermitian matrix  $A$  can be decomposed into a product  $U^\dagger \cdot B \cdot U$ , where  $U$  is a unitary matrix and  $B$  is a diagonal matrix containing only real components which are ordered along the diagonal.

**definition** *per-col where*  
*per-col*  $A \ f = \text{Matrix.mat } (\text{dim-row } A) \ (\text{dim-col } A) \ (\lambda \ (i,j). A \$(i, (f \ j)))$

**lemma** *per-col-carrier*:  
**assumes**  $A \in \text{carrier-mat } n \ m$   
**shows** *per-col*  $A \ f \in \text{carrier-mat } n \ m$  *<proof>*

**lemma** *per-col-col*:  
**assumes**  $A \in \text{carrier-mat } n \ m$   
**and**  $j < m$   
**shows** *Matrix.col* (*per-col*  $A \ f$ )  $j = \text{Matrix.col } A \ (f \ j)$   
*<proof>*

**lemma** *per-col-adjoint-row*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $i < n$   
**and**  $f \ i < n$   
**shows** *Matrix.row* (*Complex-Matrix.adjoint* (*per-col*  $A \ f$ ))  $i =$   
*Matrix.row* (*Complex-Matrix.adjoint*  $A$ ) ( $f \ i$ )  
*<proof>*

**lemma** *per-col-mult-adjoint*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $i < n$   
**and**  $j < n$   
**and**  $f \ i < n$   
**and**  $f \ j < n$   
**shows**  $((\text{Complex-Matrix.adjoint } (\text{per-col } A \ f)) * (\text{per-col } A \ f)) \$(i,j) =$   
 $((\text{Complex-Matrix.adjoint } A) * A) \$(f \ i, f \ j)$   
*<proof>*

**lemma** *idty-index*:  
**assumes** *bij-betw*  $f \ \{.. < n\} \ \{.. < n\}$

**and**  $i < n$   
**and**  $j < n$   
**shows**  $(1_m \ n) \$(i,j) = (1_m \ n) \$(f \ i, f \ j)$   
 <proof>

**lemma** *per-col-unitary*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and** *unitary*  $A$   
**and** *bij-betw*  $f \ \{.. < n\} \ \{.. < n\}$   
**shows** *unitary*  $(\text{per-col } A \ f)$  <proof>

**definition** *per-diag where*  
 $\text{per-diag } A \ f = \text{Matrix.mat } (\text{dim-row } A) (\text{dim-col } A) (\lambda \ (i,j). A \ \$(f \ i, (f \ j)))$

**lemma** *per-diag-carrier*:  
**shows**  $\text{per-diag } A \ f \in \text{carrier-mat } (\text{dim-row } A) (\text{dim-col } A)$   
 <proof>

**lemma** *per-diag-diagonal*:  
**assumes**  $D \in \text{carrier-mat } n \ n$   
**and** *diagonal-mat*  $D$   
**and** *bij-betw*  $f \ \{.. < n\} \ \{.. < n\}$   
**shows** *diagonal-mat*  $(\text{per-diag } D \ f)$  <proof>

**lemma** *per-diag-diag-mat*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $i < n$   
**and**  $f \ i < n$   
**shows**  $\text{diag-mat } (\text{per-diag } A \ f) ! i = \text{diag-mat } A ! (f \ i)$   
 <proof>

**lemma** *per-diag-diag-mat-Re*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $i < n$   
**and**  $f \ i < n$   
**shows**  $\text{map Re } (\text{diag-mat } (\text{per-diag } A \ f) ! i) = \text{map Re } (\text{diag-mat } A) ! (f \ i)$   
 <proof>

**lemma** *per-diag-real*:  
**fixes**  $B :: \text{complex Matrix.mat}$   
**assumes**  $B \in \text{carrier-mat } n \ n$   
**and**  $\forall i < n. B \ \$(i,i) \in \text{Reals}$   
**and** *bij-betw*  $f \ \{.. < n\} \ \{.. < n\}$   
**shows**  $\forall j < n. (\text{per-diag } B \ f) \ \$(j,j) \in \text{Reals}$   
 <proof>

**lemma** *per-col-mult-unitary*:  
**fixes**  $A :: \text{complex Matrix.mat}$   
**assumes**  $A \in \text{carrier-mat } n \ n$

**and** *unitary*  $A$   
**and**  $D \in \text{carrier-mat } n \ n$   
**and** *diagonal-mat*  $D$   
**and**  $0 < n$   
**and** *bij-betw*  $f \ \{..< n\} \ \{..< n\}$   
**shows**  $A * D * (\text{Complex-Matrix.adjoint } A) =$   
 $(\text{per-col } A \ f) * (\text{per-diag } D \ f) * (\text{Complex-Matrix.adjoint } (\text{per-col } A \ f))$   
**(is**  $?L = ?R)$   
 $\langle \text{proof} \rangle$

**lemma** *sort-permutation*:  
**assumes**  $m = \text{sort } l$   
**obtains**  $f$  **where** *bij-betw*  $f \ \{..< \text{length } l\} \ \{..< \text{length } l\} \wedge$   
 $(\forall i < \text{length } l. \ l ! \ f \ i = m ! \ i)$   
 $\langle \text{proof} \rangle$

**lemma** *per-diag-sorted-Re*:  
**fixes**  $B :: \text{complex Matrix.mat}$   
**assumes**  $B \in \text{carrier-mat } n \ n$   
**obtains**  $f$  **where** *bij-betw*  $f \ \{..< n\} \ \{..< n\} \wedge$   
 $\text{map } \text{Re} \ (\text{diag-mat } (\text{per-diag } B \ f)) = \text{sort} \ (\text{map } \text{Re} \ (\text{diag-mat } B))$   
 $\langle \text{proof} \rangle$

**lemma** *bij-unitary-diag*:  
**fixes**  $A :: \text{complex Matrix.mat}$   
**assumes** *unitary-diag*  $A \ B \ U$   
**and**  $A \in \text{carrier-mat } n \ n$   
**and** *bij-betw*  $f \ \{..< n\} \ \{..< n\}$   
**and**  $0 < n$   
**shows** *unitary-diag*  $A \ (\text{per-diag } B \ f) \ (\text{per-col } U \ f)$   
 $\langle \text{proof} \rangle$

**lemma** *hermitian-real-diag-sorted*:  
**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $0 < n$   
**and** *hermitian*  $A$   
**obtains**  $Bs \ Us$  **where** *real-diag-decomp*  $A \ Bs \ Us \wedge \text{sorted} \ (\text{map } \text{Re} \ (\text{diag-mat } Bs))$   
 $\langle \text{proof} \rangle$

## 8 Commuting Hermitian families

This part is devoted to the proof that a finite family of commuting Hermitian matrices is simultaneously diagonalizable.

### 8.1 Intermediate properties

**lemma** *real-diag-decomp-mult-dbm-unit*:

**assumes**  $A \in \text{carrier-mat } n \ n$   
**and**  $\text{real-diag-decomp } A \ B \ U$   
**and**  $B = \text{diag-block-mat } Bl$   
**and**  $\text{length } Ul = \text{length } Bl$   
**and**  $\forall i < \text{length } Bl. \text{dim-col } (Bl!i) = \text{dim-row } (Bl!i)$   
**and**  $\forall i < \text{length } Bl. \text{dim-row } (Bl!i) = \text{dim-row } (Ul!i)$   
**and**  $\forall i < \text{length } Bl. \text{dim-col } (Bl!i) = \text{dim-col } (Ul!i)$   
**and**  $\text{unitary } (\text{diag-block-mat } Ul)$   
**and**  $\forall i < \text{length } Ul. Ul!i * Bl!i = Bl!i * Ul!i$   
**shows**  $\text{real-diag-decomp } A \ B \ (U * (\text{diag-block-mat } Ul))$   
 $\langle \text{proof} \rangle$

**lemma** *real-diag-decomp-block-set*:

**assumes**  $Als \neq \{\}$   
**and**  $0 < n$   
**and**  $\forall Al \in Als. \text{length } Al = n$   
**and**  $\forall i < n. \forall Al \in Als. \text{dim-row } (Al!i) = \text{dim-col } (Al!i)$   
**and**  $\forall i < n. \exists U. \forall Al \in Als. \exists B. \text{real-diag-decomp } (Al!i) \ B \ U$   
**shows**  $\exists Ul. (\text{length } Ul = n \wedge (\forall i < n. \forall Al \in Als. (\text{dim-row } (Ul!i) = \text{dim-row } (Al!i) \wedge \text{dim-col } (Ul!i) = \text{dim-col } (Al!i))) \wedge (\forall Al \in Als. \exists Bl. (\text{length } Bl = n \wedge \text{real-diag-decomp } (\text{diag-block-mat } Al) (\text{diag-block-mat } Bl) (\text{diag-block-mat } Ul))))$   
 $\langle \text{proof} \rangle$

**lemma** *real-diag-decomp-eq-comps-props*:

**assumes**  $Ap \in \text{carrier-mat } n \ n$   
**and**  $0 < n$   
**and**  $\text{real-diag-decomp } Ap \ Bs \ Us \wedge \text{sorted } (\text{map } Re \ (\text{diag-mat } Bs))$   
**shows**  $Bs \in \text{carrier-mat } n \ n \ \text{diagonal-mat } Bs \ \text{unitary } Us$   
 $Us \in \text{carrier-mat } n \ n \ \text{diag-diff } Bs \ (\text{eq-comps } (\text{diag-mat } Bs))$   
 $\text{eq-comps } (\text{diag-mat } Bs) \neq [] \ \text{diag-mat } Bs \neq []$   
 $\langle \text{proof} \rangle$

**lemma** *commuting-conj-mat-set-props*:

**fixes**  $As::'a::\text{conjugatable-field } Matrix.\text{mat } \text{set}$   
**and**  $U::'a \ Matrix.\text{mat}$   
**assumes**  $\text{finite } As$   
**and**  $\text{card } As \leq i$   
**and**  $\forall A \in As. \text{hermitian } A \wedge A \in \text{carrier-mat } n \ n$   
**and**  $\forall A \in As. \forall B \in As. A*B = B*A$   
**and**  $\text{unitary } U$   
**and**  $U \in \text{carrier-mat } n \ n$   
**and**  $CjA = (\lambda A2. \text{mat-conj } (\text{Complex-Matrix.adjoint } U) \ A2)'As$   
**shows**  $\text{finite } CjA \ \text{card } CjA \leq i$   
 $\forall A \in CjA. A \in \text{carrier-mat } n \ n \wedge \text{hermitian } A$   
 $\forall C1 \in CjA. \forall C2 \in CjA. C1*C2 = C2*C1$   
 $\langle \text{proof} \rangle$

**lemma** *commute-extract-diag-block-eq*:

**fixes**  $A_p::\text{complex Matrix.mat}$   
**assumes**  $A_p \in \text{carrier-mat } n \ n$   
**and**  $0 < n$   
**and**  $\text{real-diag-decomp } A_p \ B_s \ U_s \wedge \text{sorted } (\text{map } \text{Re } (\text{diag-mat } B_s))$   
**and**  $\text{finite } A_{fp}$   
**and**  $\text{card } A_{fp} \leq i$   
**and**  $\forall A \in A_{fp}. \text{hermitian } A \wedge A \in \text{carrier-mat } n \ n$   
**and**  $\forall A \in A_{fp}. \forall B \in A_{fp}. A * B = B * A$   
**and**  $\forall A \in A_{fp}. A_p * A = A * A_p$   
**and**  $C_j A = (\lambda A_2. \text{mat-conj } (\text{Complex-Matrix.adjoint } U_s) \ A_2) 'A_{fp}$   
**and**  $\text{eqcl} = \text{eq-comps } (\text{diag-mat } B_s)$   
**shows**  $\forall C \in C_j A. C = \text{diag-block-mat } (\text{extract-subdiags } C \ \text{eqcl})$   
 $\langle \text{proof} \rangle$

**lemma**  $\text{extract-dbm-eq-component-commute}$ :  
**assumes**  $\forall C \in C_s. C = \text{diag-block-mat } (\text{extract-subdiags } C \ l)$   
**and**  $\forall C_1 \in C_s. \forall C_2 \in C_s. C_1 * C_2 = C_2 * C_1$   
**and**  $\text{ExC} = (\lambda A. \text{extract-subdiags } A \ l) 'C_s$   
**and**  $j < \text{length } l$   
**and**  $\text{Exi} = (\lambda A. (A!j)) ' \text{ExC}$   
**and**  $A_l \in \text{Exi}$   
**and**  $B_l \in \text{Exi}$   
**shows**  $A_l * B_l = B_l * A_l$   
 $\langle \text{proof} \rangle$

**lemma**  $\text{extract-comm-real-diag-decomp}$ :  
**fixes**  $C_j A::\text{complex Matrix.mat set}$   
**assumes**  $\bigwedge (A_f::\text{complex Matrix.mat set}) \ n \ . \ \text{finite } A_f \implies$   
 $\text{card } A_f \leq i \implies$   
 $A_f \neq \{\}$   
 $(\bigwedge A. A \in A_f \implies A \in \text{carrier-mat } n \ n) \implies$   
 $0 < n \implies (\bigwedge A. A \in A_f \implies \text{hermitian } A) \implies$   
 $(\bigwedge A \ B. A \in A_f \implies B \in A_f \implies A * B = B * A) \implies$   
 $\exists U. \forall A \in A_f. \exists B. \text{real-diag-decomp } A \ B \ U$   
**and**  $\text{finite } C_j A$   
**and**  $C_j A \neq \{\}$   
**and**  $\text{card } C_j A \leq i$   
**and**  $\forall C \in C_j A. C = \text{diag-block-mat } (\text{extract-subdiags } C \ \text{eqcl})$   
**and**  $\forall C_1 \in C_j A. \forall C_2 \in C_j A. C_1 * C_2 = C_2 * C_1$   
**and**  $\text{Exc} = (\lambda A. \text{extract-subdiags } A \ \text{eqcl}) 'C_j A$   
**and**  $\forall E \in \text{Exc}. \text{list-all } (\lambda B. 0 < \text{dim-row } B \wedge \text{hermitian } B) \ E$   
**and**  $\forall i < \text{length } \text{eqcl}. 0 < \text{eqcl}!i$   
**shows**  $\forall i < \text{length } \text{eqcl}. \exists U. \forall A_l \in \text{Exc}. \exists B. \text{real-diag-decomp } (A_l ! i) \ B \ U$   
 $\langle \text{proof} \rangle$

## 8.2 The main result

**theorem**  $\text{commuting-hermitian-family-diag}$ :  
**fixes**  $A_f::\text{complex Matrix.mat set}$

```

assumes finite Af
and  $Af \neq \{\}$ 
and  $\bigwedge A. A \in Af \implies A \in \text{carrier-mat } n \ n$ 
and  $0 < n$ 
and  $\bigwedge A. A \in Af \implies \text{hermitian } A$ 
and  $\bigwedge A \ B. A \in Af \implies B \in Af \implies A * B = B * A$ 
shows  $\exists U. \forall A \in Af. \exists B. \text{real-diag-decomp } A \ B \ U$  <proof>

end

```