

Tensor Product of Matrices

T.V.H. Prathamesh

February 23, 2021

Abstract

In this work, the Kronecker tensor product of matrices and the proofs of some of its properties are formalized. Properties which have been formalized include associativity of the tensor product and the mixed-product property. This formalization of tensor product of matrices relies on the formalization of matrices by Christian Sternagel and Rene Thiemann under the title ‘Executable Matrix Operations on Matrices of Arbitrary Dimensions’.

Contents

1	Tensor Product of Matrices	1
1.1	Defining the Tensor Product	1
1.2	Associativity and Distributive properties	12

We define Tensor Product of Matrices and prove properties such as associativity and mixed product property(distributivity) of the tensor product.

1 Tensor Product of Matrices

```
theory Matrix-Tensor
imports Matrix.Utility Matrix.Matrix-Legacy
begin
```

1.1 Defining the Tensor Product

We define a multiplicative locale here - mult, where the multiplication satisfies commutativity, associativity and contains a left and right identity

```
locale mult =
  fixes id::'a
  fixes f:: 'a ⇒ 'a ⇒ 'a (infixl * 60)
  assumes comm: f a b = f b a
  assumes assoc: (f (f a b) c) = (f a (f b c))
  assumes left-id: f id x = x
  assumes right-id: f x id = x
```

context *mult*

begin

$\text{times } a \ v$, gives us the product of the vector v with multiplied pointwise with a

primrec *times*:: $'a \Rightarrow 'a \ \text{vec} \Rightarrow 'a \ \text{vec}$

where

$\text{times } n \ [] = []$

$\text{times } n \ (y\#ys) = (f \ n \ y)\#(\text{times } n \ ys)$

lemma *times-scalar-id*: $\text{times } id \ v = v$

$\langle \text{proof} \rangle$

lemma *times-vector-id*: $\text{times } v \ [id] = [v]$

$\langle \text{proof} \rangle$

lemma *preserving-length*: $\text{length } (\text{times } n \ y) = (\text{length } y)$

$\langle \text{proof} \rangle$

vec_vec_Tensor is the tensor product of two vectors. It is illustrated by the following relation

$\text{vec_vec_Tensor}(v_1, v_2, \dots, v_n)(w_1, w_2, \dots, w_m) = (v_1 \cdot w_1, \dots, v_1 \cdot w_m, \dots, v_n \cdot w_1, \dots, v_n \cdot w_m)$

primrec *vec-vec-Tensor*:: $'a \ \text{vec} \Rightarrow 'a \ \text{vec} \Rightarrow 'a \ \text{vec}$

where

$\text{vec-vec-Tensor } [] \ ys = []$

$\text{vec-vec-Tensor } (x\#xs) \ ys = (\text{times } x \ ys)\@(\text{vec-vec-Tensor } xs \ ys)$

lemma *vec-vec-Tensor-left-id*: $\text{vec-vec-Tensor } [id] \ v = v$

$\langle \text{proof} \rangle$

lemma *vec-vec-Tensor-right-id*: $\text{vec-vec-Tensor } v \ [id] = v$

$\langle \text{proof} \rangle$

theorem *vec-vec-Tensor-length* :

$(\text{length}(\text{vec-vec-Tensor } x \ y)) = (\text{length } x) * (\text{length } y)$

$\langle \text{proof} \rangle$

theorem *vec-length*: **assumes** $\text{vec } m \ x$ **and** $\text{vec } n \ y$

shows $\text{vec } (m*n) \ (\text{vec-vec-Tensor } x \ y)$

$\langle \text{proof} \rangle$

vec_mat_Tensor is the tensor product of two vectors. It is illustrated by the following relation

$\text{vec_mat_Tensor } (v_1, v_2, \dots, v_n)(C_1, C_2, \dots, C_m) = (v_1 \cdot C_1, \dots, v_n \cdot C_1, \dots, v_1 \cdot C_m, \dots, v_n \cdot C_m)$

primrec *vec-mat-Tensor*:: 'a vec \Rightarrow 'a mat \Rightarrow 'a mat

where

vec-mat-Tensor xs [] = []

vec-mat-Tensor xs (ys#yss) = (*vec-vec-Tensor* xs ys)#(*vec-mat-Tensor* xs yss)

lemma *vec-mat-Tensor-vector-id*: *vec-mat-Tensor* [id] v = v

<proof>

lemma *vec-mat-Tensor-matrix-id*: *vec-mat-Tensor* v [[id]] = [v]

<proof>

theorem *vec-mat-Tensor-length*:

length(*vec-mat-Tensor* xs ys) = *length* ys

<proof>

theorem *length-matrix*:

assumes mat nr nc (y#ys) **and** *length* v = k

and (*vec-mat-Tensor* v (y#ys) = x#xs)

shows (*vec* (nr*k) x)

<proof>

lemma *matrix-set-list*:

assumes mat nr nc M

and *length* v = k

and x \in set M

shows \exists ys. \exists zs. (ys@x#zs = M)

<proof>

primrec *reduct* :: 'a mat \Rightarrow 'a mat

where

reduct [] = []

| *reduct* (x#xs) = xs

lemma *length-reduct*:

assumes m \neq []

shows *length* (*reduct* m) + 1 = (*length* m)

<proof>

lemma *mat-empty-column-length*: **assumes** mat nr nc M **and** M = []

shows nc = 0

<proof>

lemma *vec-uniqueness*:

assumes *vec* m v

and *vec* n v

shows m = n

<proof>

lemma *mat-uniqueness*:
assumes *mat nr1 nc M*
and *mat nr2 nc M* **and** $z = \text{hd } M$ **and** $M \neq []$
shows $(\forall x \in (\text{set } M). (nr1 = nr2))$
 $\langle \text{proof} \rangle$

lemma *mat-empty-row-length*: **assumes** *mat nr nc M* **and** $M = []$
shows *mat 0 nc M*
 $\langle \text{proof} \rangle$

abbreviation *null-matrix*:: 'a list list
where
null-matrix $\equiv [Nil]$

lemma *null-mat:null-matrix* = $[[]]$
 $\langle \text{proof} \rangle$

lemma *zero-matrix*: *mat 0 0 []* $\langle \text{proof} \rangle$

row_length gives the length of the first row of a matrix. For a 'valid' matrix, it is equal to the number of rows

definition *row-length*:: 'a mat \Rightarrow nat
where
row-length $xs \equiv$ if $(xs = [])$ then 0 else $(\text{length } (\text{hd } xs))$

lemma *row-length-Nil*:
row-length $[] = 0$
 $\langle \text{proof} \rangle$

lemma *row-length-Null*:
row-length $[[]] = 0$
 $\langle \text{proof} \rangle$

lemma *row-length-vect-mat*:
row-length $(\text{vec-mat-Tensor } v \ m) = \text{length } v * (\text{row-length } m)$
 $\langle \text{proof} \rangle$

Tensor is the tensor product of matrices

primrec *Tensor*:: 'a mat \Rightarrow 'a mat \Rightarrow 'a mat (**infixl** \otimes 63)
where
Tensor $[] \ xs = []$
Tensor $(x \# \ xs) \ ys = (\text{vec-mat-Tensor } x \ ys) @ (\text{Tensor } xs \ ys)$

lemma *Tensor-null*: $xs \otimes [] = []$
 $\langle \text{proof} \rangle$

Tensor commutes with left and right identity

lemma *Tensor-left-id*: $[[id]] \otimes xs = xs$

<proof>

lemma *Tensor-right-id:* $xs \otimes [[id]] = xs$

<proof>

row_length of tensor product of matrices is the product of their respective row lengths

lemma *row-length-mat:*

$(row_length\ (m1 \otimes m2)) = (row_length\ m1) * (row_length\ m2)$

<proof>

lemma *hd-set:assumes* $x \in set\ (a \# M)$ **shows** $(x = a) \vee (x \in (set\ M))$

<proof>

for every valid matrix can also be written in the following form

theorem *matrix-row-length:*

assumes *mat nr nc M*

shows *mat (row-length M) (length M) M*

<proof>

lemma *reduct-matrix:*

assumes *mat (row-length (a # M)) (length (a # M)) (a # M)*

shows *mat (row-length M) (length M) M*

<proof>

theorem *well-defined-vec-mat-Tensor:*

$(mat\ (row_length\ M)\ (length\ M)\ M) \implies$

$(mat\ ((row_length\ M) * (length\ v))\ (length\ M)\ (vec_mat_Tensor\ v\ M))$

<proof>

The following theorem gives length of tensor product of two matrices

lemma *length-Tensor:* $(length\ (M1 \otimes M2)) = (length\ M1) * (length\ M2)$

<proof>

lemma *append-reduct-matrix:*

$(mat\ (row_length\ (M1 @ M2))\ (length\ (M1 @ M2))\ (M1 @ M2))$

$\implies (mat\ (row_length\ M2)\ (length\ M2)\ M2)$

<proof>

The following theorem proves that tensor product of two valid matrices is a valid matrix

theorem *well-defined-Tensor*:

(*mat* (*row-length* *M1*) (*length* *M1*) *M1*)
∧ (*mat* (*row-length* *M2*) (*length* *M2*) *M2*)
⇒ (*mat* ((*row-length* *M1*)*(*row-length* *M2*)) ((*length* *M1*)*(*length* *M2*)) (*M1*⊗*M2*))
⟨*proof*⟩

theorem *effective-well-defined-Tensor*:

assumes (*mat* (*row-length* *M1*) (*length* *M1*) *M1*)
and (*mat* (*row-length* *M2*) (*length* *M2*) *M2*)
shows *mat*
 ((*row-length* *M1*)*(*row-length* *M2*))
 ((*length* *M1*)*(*length* *M2*))
 (*M1*⊗*M2*)
⟨*proof*⟩

definition *natmod*::*nat* ⇒ *nat* ⇒ *nat* (**infixl** *nmod* 50)

where

natmod *x y* = *nat* ((*int* *x*) *mod* (*int* *y*))

theorem *times-elements*:

∀ *i*.((*i*<(*length* *v*)) → (*times* *a v*)!*i* = *f a* (*v*!*i*))
⟨*proof*⟩

lemma *simpl-times-elements*:

assumes (*i*<(*length* *xs*))
shows ((*i*<(*length* *v*)) → (*times* *a v*)!*i* = *f a* (*v*!*i*))
⟨*proof*⟩

lemma *append-simpl*: *i*<(*length* *xs*) → (*xs*@*ys*)!*i* = (*xs*!*i*)

⟨*proof*⟩

lemma *append-simpl2*: *i* ≥(*length* *xs*) → (*xs*@*ys*)!*i* = (*ys*!(*i* - (*length* *xs*)))

⟨*proof*⟩

lemma *append-simpl3*:

assumes *i* > (*length* *y*)
shows (*i* <((*length* (*z*#*zs*))*(*length* *y*)))
 → (*i* - (*length* *y*)) < (*length* *zs*)*(*length* *y*)

⟨*proof*⟩

lemma *append-simpl4*:

(*i* > (*length* *y*))
 → ((*i* <((*length* (*z*#*zs*))*(*length* *y*))))
 → ((*i* - (*length* *y*)) < (*length* *zs*)*(*length* *y*))
⟨*proof*⟩

lemma *vec-vec-Tensor-simpl*:

$i < (\text{length } y) \longrightarrow (\text{vec-vec-Tensor } (z\#zs) y)!i = (\text{times } z y)!i$
 $\langle \text{proof} \rangle$

lemma *vec-vec-Tensor-simpl2*:

$(i \geq (\text{length } y))$
 $\longrightarrow ((\text{vec-vec-Tensor } (z\#zs) y)!i = (\text{vec-vec-Tensor } zs y)!(i - (\text{length } y)))$
 $\langle \text{proof} \rangle$

lemma *division-product*:

assumes $(b::\text{int}) > 0$
and $a \geq b$
shows $(a \text{ div } b) = ((a - b) \text{ div } b) + 1$
 $\langle \text{proof} \rangle$

lemma *int-nat-div*:

$(\text{int } a) \text{ div } (\text{int } b) = \text{int } ((a::\text{nat}) \text{ div } b)$
 $\langle \text{proof} \rangle$

lemma *int-nat-eq*:

assumes $\text{int } (a::\text{nat}) = \text{int } b$
shows $a = b$
 $\langle \text{proof} \rangle$

lemma *nat-div*:

assumes $(b::\text{nat}) > 0$
and $a > b$
shows $(a \text{ div } b) = ((a - b) \text{ div } b) + 1$
 $\langle \text{proof} \rangle$

lemma *mod-eq*:

$(m::\text{int}) \text{ mod } n = (m + (-1)*n) \text{ mod } n$
 $\langle \text{proof} \rangle$

lemma *nat-mod-eq*: $\text{int } m \text{ mod } \text{int } n = \text{int } (m \text{ mod } n)$

$\langle \text{proof} \rangle$

lemma *nat-mod*:

assumes $(m::\text{nat}) > n$
shows $(m::\text{nat}) \text{ mod } n = (m - n) \text{ mod } n$
 $\langle \text{proof} \rangle$

lemma *logic*:

assumes $A \longrightarrow B$
and $\neg A \longrightarrow B$
shows B
 $\langle \text{proof} \rangle$

theorem *vec-vec-Tensor-elements*:

assumes $(y \neq [])$

shows

$$\begin{aligned} & \forall i. ((i < ((\text{length } x) * (\text{length } y))) \\ & \quad \longrightarrow ((\text{vec-vec-Tensor } x \ y)!i) \\ & \quad \quad = f (x!(i \text{ div } (\text{length } y))) (y!(i \text{ mod } (\text{length } y)))) \end{aligned}$$

$\langle \text{proof} \rangle$

a few more results that will be used later on

lemma *nat-int*: $\text{nat } (\text{int } x + \text{int } y) = x + y$

$\langle \text{proof} \rangle$

lemma *int-nat-equiv*: $(x > 0) \longrightarrow (\text{nat } ((\text{int } x) + -1) + 1) = x$

$\langle \text{proof} \rangle$

lemma *list-int-nat*: $(k > 0) \longrightarrow ((x \# xs)!k = xs!(\text{nat } ((\text{int } k) + -1)))$

$\langle \text{proof} \rangle$

lemma *row-length-eq*:

$$\begin{aligned} & (\text{mat } (\text{row-length } (a \# b \# N)) (\text{length } (a \# b \# N)) (a \# b \# N)) \\ & \quad \longrightarrow \\ & \quad (\text{row-length } (a \# b \# N) = (\text{row-length } (b \# N))) \end{aligned}$$

$\langle \text{proof} \rangle$

The following theorem tells us the relationship between entries of `vec_mat_Ten`-`sor v M` and entries of `v` and `M` respectively

theorem *vec-mat-Tensor-elements*:

$$\begin{aligned} & \forall i. \forall j. \\ & \quad (((i < ((\text{length } v) * (\text{row-length } M))) \\ & \quad \wedge (j < (\text{length } M))) \\ & \quad \wedge (\text{mat } (\text{row-length } M) (\text{length } M) M) \\ & \quad \longrightarrow ((\text{vec-mat-Tensor } v \ M)!j!i) \\ & \quad \quad = f (v!(i \text{ div } (\text{row-length } M))) (M!j!(i \text{ mod } (\text{row-length } M))) \end{aligned}$$

$\langle \text{proof} \rangle$

The following theorem tells us about the relationship between entries of tensor products of two matrices and the entries of matrices

theorem *matrix-Tensor-elements*:

fixes $M1 \ M2$

shows

$$\begin{aligned} & \forall i. \forall j. (((i < ((\text{row-length } M1) * (\text{row-length } M2))) \\ & \quad \wedge (j < (\text{length } M1) * (\text{length } M2))) \\ & \quad \wedge (\text{mat } (\text{row-length } M1) (\text{length } M1) M1) \\ & \quad \wedge (\text{mat } (\text{row-length } M2) (\text{length } M2) M2) \\ & \quad \longrightarrow ((M1 \otimes M2)!j!i) = \\ & \quad \quad f \\ & \quad \quad (M1!(j \text{ div } (\text{length } M2))!(i \text{ div } (\text{row-length } M2))) \end{aligned}$$

$$(M2!(j \text{ mod } \text{length } M2)!(i \text{ mod } (\text{row-length } M2)))$$

<proof>

we restate the theorem in two different forms for convenience of reuse

theorem *effective-matrix-tensor-elements:*

$$\begin{aligned} &(((i < ((\text{row-length } M1) * (\text{row-length } M2)))) \\ &\wedge (j < (\text{length } M1) * (\text{length } M2))) \\ &\wedge (\text{mat } (\text{row-length } M1) (\text{length } M1) M1) \\ &\wedge (\text{mat } (\text{row-length } M2) (\text{length } M2) M2) \\ \implies &((M1 \otimes M2)!j!i) \\ &= f (M1!(j \text{ div } (\text{length } M2))!(i \text{ div } (\text{row-length } M2))) \\ &\quad (M2!(j \text{ mod } \text{length } M2)!(i \text{ mod } (\text{row-length } M2))) \end{aligned}$$

<proof>

theorem *effective-matrix-tensor-elements2:*

$$\begin{aligned} \text{assumes } &i < (\text{row-length } M1) * (\text{row-length } M2) \\ \text{and } &j < (\text{length } M1) * (\text{length } M2) \\ \text{and } &\text{mat } (\text{row-length } M1) (\text{length } M1) M1 \\ \text{and } &\text{mat } (\text{row-length } M2) (\text{length } M2) M2 \\ \text{shows } &(M1 \otimes M2)!j!i = \\ &(M1!(j \text{ div } (\text{length } M2))!(i \text{ div } (\text{row-length } M2))) \\ &\quad * (M2!(j \text{ mod } \text{length } M2)!(i \text{ mod } (\text{row-length } M2))) \end{aligned}$$

<proof>

the following lemmas are useful in proving associativity of tensor products

lemma *div-left-ineq:*

$$\begin{aligned} \text{assumes } &(x::\text{nat}) < y * z \\ \text{shows } &(x \text{ div } z) < y \end{aligned}$$

<proof>

lemma *div-right-ineq:*

$$\begin{aligned} \text{assumes } &(x::\text{nat}) < y * z \\ \text{shows } &(x \text{ div } y) < z \end{aligned}$$

<proof>

In the following theorem, we obtain columns of `vec_mat_Tensor` of a vector `v` and a matrix `M` in terms of the vector `v` and columns of the matrix `M`

lemma *col-vec-mat-Tensor-prelim:*

$$\begin{aligned} &\forall j. (j < (\text{length } M)) \\ &\quad \longrightarrow \\ &\quad \text{col } (\text{vec-mat-Tensor } v M) j = \text{vec-vec-Tensor } v (\text{col } M j) \end{aligned}$$

<proof>

lemma *col-vec-mat-Tensor:fixes j M v*

$$\begin{aligned} \text{assumes } &j < (\text{length } M) \\ \text{shows } &\text{col } (\text{vec-mat-Tensor } v M) j = \text{vec-vec-Tensor } v (\text{col } M j) \end{aligned}$$

<proof>

lemma *col-formula:*

fixes $M1$ and $M2$

shows $\forall j.((j < (\text{length } M1) * (\text{length } M2))$
 $\wedge (\text{mat } (\text{row-length } M1) (\text{length } M1) M1)$
 $\wedge (\text{mat } (\text{row-length } M2) (\text{length } M2) M2)$
 $\longrightarrow \text{col } (M1 \otimes M2) j$
 $= \text{vec-vec-Tensor}$
 $(\text{col } M1 (j \text{ div } \text{length } M2))$
 $(\text{col } M2 (j \text{ mod } \text{length } M2)))$

$\langle \text{proof} \rangle$

lemma *row-Cons*: $\text{row } (v \# M) i = (v!i) \# (\text{row } M i)$

$\langle \text{proof} \rangle$

lemma *row-append*: $\text{row } (A @ B) i = (\text{row } A i) @ (\text{row } B i)$

$\langle \text{proof} \rangle$

lemma *row-empty*: $\text{row } [] i = []$

$\langle \text{proof} \rangle$

lemma *vec-vec-Tensor-right-empty*: $\text{vec-vec-Tensor } x [] = []$

$\langle \text{proof} \rangle$

lemma *vec-mat-Tensor* $v ([] \# []) = [[]]$

$\langle \text{proof} \rangle$

lemma $i < 0 \longrightarrow [[]!i] = []$

$\langle \text{proof} \rangle$

lemma *row-vec-mat-Tensor-prelim*:

$\forall i.$

$((i < (\text{length } v) * (\text{row-length } M)) \wedge (\text{mat } nr (\text{length } M) M)$
 $\longrightarrow \text{row } (\text{vec-mat-Tensor } v M) i$
 $= \text{times } (v!(i \text{ div } \text{row-length } M)) (\text{row } M (i \text{ mod } \text{row-length } M)))$

$\langle \text{proof} \rangle$

The following lemma gives us a formula for the row of a tensor of two matrices

lemma *row-formula*:

fixes $M1$ and $M2$

shows $\forall i.((i < (\text{row-length } M1) * (\text{row-length } M2))$
 $\wedge (\text{mat } (\text{row-length } M1) (\text{length } M1) M1)$
 $\wedge (\text{mat } (\text{row-length } M2) (\text{length } M2) M2)$
 $\longrightarrow \text{row } (M1 \otimes M2) i$
 $= \text{vec-vec-Tensor}$
 $(\text{row } M1 (i \text{ div } \text{row-length } M2))$
 $(\text{row } M2 (i \text{ mod } \text{row-length } M2)))$

$\langle \text{proof} \rangle$

lemma *effective-row-formula*:

fixes $M1$ and $M2$
assumes $i < (\text{row-length } M1) * (\text{row-length } M2)$
and $(\text{mat } (\text{row-length } M1) (\text{length } M1) M1)$
and $(\text{mat } (\text{row-length } M2) (\text{length } M2) M2)$
shows $\text{row } (M1 \otimes M2) i$
 $= \text{vec-vec-Tensor}$
 $(\text{row } M1 (i \text{ div } \text{row-length } M2))$
 $(\text{row } M2 (i \text{ mod } \text{row-length } M2))$
 $\langle \text{proof} \rangle$

lemma *alt-effective-matrix-tensor-elements*:
 $((i < ((\text{row-length } M2) * (\text{row-length } M3)))$
 $\wedge (j < (\text{length } M2) * (\text{length } M3)))$
 $\wedge (\text{mat } (\text{row-length } M2) (\text{length } M2) M2)$
 $\wedge (\text{mat } (\text{row-length } M3) (\text{length } M3) M3)$
 $\implies ((M2 \otimes M3)!j!i = f (M2!(j \text{ div } (\text{length } M3))!(i \text{ div } (\text{row-length } M3)))$
 $(M3!(j \text{ mod } \text{length } M3))!(i \text{ mod } (\text{row-length } M3))))$
 $\langle \text{proof} \rangle$

lemma *trans-impl*: $(\forall i j. (P i j \longrightarrow Q i j)) \wedge (\forall i j. (Q i j \longrightarrow R i j))$
 $\implies (\forall i j. (P i j \longrightarrow R i j))$
 $\langle \text{proof} \rangle$

lemma $((x::\text{nat}) \text{ div } y) \text{ div } z = (x \text{ div } (y*z))$
 $\langle \text{proof} \rangle$

lemma $(\neg((a::\text{nat}) < b)) \implies (a \geq b)$
 $\langle \text{proof} \rangle$

lemma *not-null*: $xs \neq [] \implies \exists y ys. xs = y\#ys$
 $\langle \text{proof} \rangle$

lemma $(y::\text{nat}) \neq 0 \implies (x \text{ mod } y) < y$
 $\langle \text{proof} \rangle$

lemma *mod-prop1*: $((a::\text{nat}) \text{ mod } (b*c)) \text{ mod } c = (a \text{ mod } c)$
 $\langle \text{proof} \rangle$

lemma *mod-div-relation*: $((a::\text{nat}) \text{ mod } (b*c)) \text{ div } c = (a \text{ div } c) \text{ mod } b$
 $\langle \text{proof} \rangle$

The following lemma proves that the tensor product of matrices is associative

lemma *associativity*:
fixes $M1$ $M2$ $M3$
shows
 $(\text{mat } (\text{row-length } M1) (\text{length } M1) M1)$
 $\wedge (\text{mat } (\text{row-length } M2) (\text{length } M2) M2)$

$\wedge (\text{mat } (\text{row-length } M3) (\text{length } M3) M3)$
 \implies
 $M1 \otimes (M2 \otimes M3) = (M1 \otimes M2) \otimes M3$ (**is** ?x \implies ?l = ?r)
 <proof>

end

lemma $\wedge (a::\text{nat}) b.(\text{times } a \ b) =(\text{times } b \ a)$
 <proof>

1.2 Associativity and Distributive properties

locale *plus-mult* =
 mult +
fixes *zer*::'a
fixes *g*::'a \Rightarrow 'a \Rightarrow 'a (**infixl** + 60)
fixes *inver*::'a \Rightarrow 'a
assumes *plus-comm*: $g \ a \ b = g \ b \ a$
assumes *plus-assoc*: $(g \ (g \ a \ b) \ c) = (g \ a \ (g \ b \ c))$
assumes *plus-left-id*: $g \ \text{zer} \ x = x$
assumes *plus-right-id*: $g \ x \ \text{zer} = x$
assumes *plus-left-distributivity*: $f \ a \ (g \ b \ c) = g \ (f \ a \ b) \ (f \ a \ c)$
assumes *plus-right-distributivity*: $f \ (g \ a \ b) \ c = g \ (f \ a \ c) \ (f \ b \ c)$
assumes *plus-left-inverse*: $(g \ x \ (\text{inver } x)) = \text{zer}$
assumes *plus-right-inverse*: $(g \ (\text{inver } x) \ x) = \text{zer}$

context *plus-mult*
begin

lemma **fixes** *M1 M2 M3*
shows $(\text{mat } (\text{row-length } M1) (\text{length } M1) M1)$
 $\wedge (\text{mat } (\text{row-length } M2) (\text{length } M2) M2)$
 $\wedge (\text{mat } (\text{row-length } M3) (\text{length } M3) M3)$
 $\implies (M1 \otimes (M2 \otimes M3)) = ((M1 \otimes M2) \otimes M3)$
 <proof>

matrix_mult refers to multiplication of matrices in the locale plus_mult

abbreviation *matrix-mult*::'a mat \Rightarrow 'a mat \Rightarrow 'a mat (**infixl** \circ 65)
where
matrix-mult *M1 M2* \equiv $(\text{mat-multI } \text{zer } g \ f \ (\text{row-length } M1) \ M1 \ M2)$

definition *scalar-product* :: 'a vec \Rightarrow 'a vec \Rightarrow 'a **where**
scalar-product *v w* = $\text{scalar-prodI } \text{zer } g \ f \ v \ w$

lemma *ma* :
assumes *wf1*: $\text{mat } nr \ n \ m1$
and *wf2*: $\text{mat } n \ nc \ m2$
and *i*: $i < nr$

and $j: j < nc$
shows $mat\text{-}multI\ zer\ g\ f\ nr\ m1\ m2\ !\ j\ !\ i$
 $=\ scalar\text{-}prodI\ zer\ g\ f\ (row\ m1\ i)\ (col\ m2\ j)$
 $\langle proof \rangle$

lemma *matrix-index*:
assumes $wf1: mat\ (row\text{-}length\ m1)\ n\ m1$
and $wf2: mat\ n\ nc\ m2$
and $i: i < (row\text{-}length\ m1)$
and $j: j < nc$
shows $matrix\text{-}mult\ m1\ m2\ !\ j\ !\ i$
 $=\ scalar\text{-}product\ (row\ m1\ i)\ (col\ m2\ j)$
 $\langle proof \rangle$

lemma *unique-row-col*:
assumes $mat\ nr1\ nc1\ M$ **and** $mat\ nr2\ nc2\ M$ **and** $M \neq []$
shows $nr1 = nr2$ **and** $nc1 = nc2$
 $\langle proof \rangle$

lemma *matrix-mult-index*:
assumes $m1 \neq []$
and $wf1: mat\ nr\ n\ m1$
and $wf2: mat\ n\ nc\ m2$
and $i: i < nr$
and $j: j < nc$
shows $matrix\text{-}mult\ m1\ m2\ !\ j\ !\ i = scalar\text{-}product\ (row\ m1\ i)\ (col\ m2\ j)$
 $\langle proof \rangle$

the following definition checks if the given four matrices are such that the compositions in the mixed-product property which will be proved, hold true. It further checks that the matrices are non empty and valid

definition *matrix-match*:: $'a\ mat \Rightarrow 'a\ mat \Rightarrow 'a\ mat \Rightarrow 'a\ mat \Rightarrow bool$
where

$matrix\text{-}match\ A1\ A2\ B1\ B2 \equiv$
 $(mat\ (row\text{-}length\ A1)\ (length\ A1)\ A1)$
 $\wedge (mat\ (row\text{-}length\ A2)\ (length\ A2)\ A2)$
 $\wedge (mat\ (row\text{-}length\ B1)\ (length\ B1)\ B1)$
 $\wedge (mat\ (row\text{-}length\ B2)\ (length\ B2)\ B2)$
 $\wedge (length\ A1 = row\text{-}length\ A2)$
 $\wedge (length\ B1 = row\text{-}length\ B2)$
 $\wedge (A1 \neq []) \wedge (A2 \neq []) \wedge (B1 \neq []) \wedge (B2 \neq [])$

lemma *non-empty-mat-mult*:
assumes $wf1: mat\ nr\ n\ A$
and $wf2: mat\ n\ nc\ B$
and $A \neq []$ **and** $B \neq []$
shows $A \circ B \neq []$

<proof>

lemma *tensor-compose-distribution1:*

assumes *wf1:mat (row-length A1) (length A1) A1*
 and *wf2:mat (row-length A2) (length A2) A2*
 and *wf3:mat (row-length B1) (length B1) B1*
 and *wf4:mat (row-length B2) (length B2) B2*
 and *matchAA:length A1 = row-length A2*
 and *matchBB:length B1 = row-length B2*
 and *non-Nil:(A1 ≠ []) ∧ (A2 ≠ []) ∧ (B1 ≠ []) ∧ (B2 ≠ [])*
shows *mat ((row-length A1)*(row-length B1))*
 ((length A2)(length B2))*
 ((A1◦A2)⊗(B1◦B2))

<proof>

lemma *effective-tensor-compose-distribution1:*

matrix-match A1 A2 B1 B2 ⇒ mat ((row-length A1)(row-length B1))*
 ((length A2)(length B2))*
 ((A1◦A2)⊗(B1◦B2))

<proof>

lemma *tensor-compose-distribution2:*

assumes *wf1:mat (row-length A1) (length A1) A1*
 and *wf2:mat (row-length A2) (length A2) A2*
 and *wf3:mat (row-length B1) (length B1) B1*
 and *wf4:mat (row-length B2) (length B2) B2*
 and *matchAA:length A1 = row-length A2*
 and *matchBB:length B1 = row-length B2*
 and *non-Nil:(A1 ≠ []) ∧ (A2 ≠ []) ∧ (B1 ≠ []) ∧ (B2 ≠ [])*
shows *mat ((row-length A1)*(row-length B1))*
 ((length A2)(length B2))*
 ((A1 ⊗ B1) ◦ (A2 ⊗ B2))

<proof>

theorem *tensor-non-empty: assumes A ≠ [] and B ≠ []*

shows *A ⊗ B ≠ []*

<proof>

theorem *non-empty-distribution:*

assumes *mat nr1 n1 A1*
 and *mat n1 nc1 A2*
 and *mat nr2 n2 B1*
 and *mat n2 nc2 B2*
 and *A1 ≠ [] and B1 ≠ [] and A2 ≠ [] and B2 ≠ []*
shows *((A1◦A2)⊗(B1◦B2)) ≠ []*

<proof>

lemma *effective-tensor-compose-distribution2:matrix-match A1 A2 B1 B2 ⇒*

$mat ((row-length A1)*(row-length B1))$
 $((length A2)*(length B2))$
 $((A1 \otimes B1) \circ (A2 \otimes B2))$
 ⟨proof⟩

theorem *effective-matrix-Tensor-elements:*

fixes $M1 M2 i j$

assumes $i < ((row-length M1)*(row-length M2))$

and $j < (length M1)*(length M2)$

and $mat (row-length M1) (length M1) M1$

and $mat (row-length M2) (length M2) M2$

shows

$((M1 \otimes M2)!j!i) = f (M1!(j \text{ div } (length M2))!(i \text{ div } (row-length M2)))$
 $(M2!(j \text{ mod } length M2))!(i \text{ mod } (row-length M2)))$

⟨proof⟩

theorem *effective-matrix-Tensor-elements2:*

fixes $M1 M2$

assumes $mat (row-length M1) (length M1) M1$

and $mat (row-length M2) (length M2) M2$

shows

$(\forall i < ((row-length M1)*(row-length M2)).$

$\forall j < ((length M1)*(length M2))$

$.((M1 \otimes M2)!j!i) = f (M1!(j \text{ div } (length M2))!(i \text{ div } (row-length M2)))$
 $(M2!(j \text{ mod } length M2))!(i \text{ mod } (row-length M2)))$)

⟨proof⟩

definition *matrix-compose-cond::'a mat ⇒ 'a mat ⇒ 'a mat ⇒ 'a mat ⇒ nat ⇒ nat ⇒ bool*

where

matrix-compose-cond $A1 A2 B1 B2 i j \equiv$

$(mat (row-length A1) (length A1) A1)$

$\wedge (mat (row-length A2) (length A2) A2)$

$\wedge (mat (row-length B1) (length B1) B1)$

$\wedge (mat (row-length B2) (length B2) B2)$

$\wedge (length A1 = row-length A2)$

$\wedge (length B1 = row-length B2)$

$\wedge (A1 \neq []) \wedge (A2 \neq []) \wedge (B1 \neq []) \wedge (B2 \neq [])$

$\wedge (i < (row-length A1)*(row-length B1)) \wedge (j < (length A2)*(length B2))$

theorem *elements-matrix-distribution-1:*

assumes $wf1: mat (row-length A1) (length A1) A1$

and $wf2: mat (row-length A2) (length A2) A2$

and $wf3: mat (row-length B1) (length B1) B1$

and $wf4: mat (row-length B2) (length B2) B2$

and $matchAA: length A1 = row-length A2$

and *matchBB*: $\text{length } B1 = \text{row-length } B2$
and *non-Nil*: $(A1 \neq []) \wedge (A2 \neq []) \wedge (B1 \neq []) \wedge (B2 \neq [])$
and $i < (\text{row-length } A1) * (\text{row-length } B1)$ **and** $j < (\text{length } A2) * (\text{length } B2)$
shows
 $((\text{matrix-mult } A1 \ A2) \otimes (\text{matrix-mult } B1 \ B2))!j!i$
 $= f (\text{scalar-product } (\text{row } A1 \ (i \ \text{div} \ (\text{row-length } B1)))$
 $\quad (\text{col } A2 \ (j \ \text{div} \ (\text{length } B2))))$
 $\quad (\text{scalar-product } (\text{row } B1 \ (i \ \text{mod} \ (\text{row-length } B1)))$
 $\quad (\text{col } B2 \ (j \ \text{mod} \ (\text{length } B2))))$
 $\langle \text{proof} \rangle$

lemma *effective-elements-matrix-distribution1*:
matrix-compose-cond $A1 \ A2 \ B1 \ B2 \ i \ j \implies$
 $((\text{matrix-mult } A1 \ A2) \otimes (\text{matrix-mult } B1 \ B2))!j!i$
 $= f (\text{scalar-product } (\text{row } A1 \ (i \ \text{div} \ (\text{row-length } B1))) (\text{col } A2 \ (j \ \text{div} \ (\text{length } B2))))$
 $\quad (\text{scalar-product } (\text{row } B1 \ (i \ \text{mod} \ (\text{row-length } B1))) (\text{col } B2 \ (j \ \text{mod} \ (\text{length } B2))))$
 $\langle \text{proof} \rangle$

lemma *matrix-match-condn-1*:
matrix-match $A1 \ A2 \ B1 \ B2$
 $\wedge (i < (\text{row-length } A1) * (\text{row-length } B1))$
 $\wedge (j < (\text{length } A2) * (\text{length } B2))$
 $\implies ((\text{matrix-mult } A1 \ A2) \otimes (\text{matrix-mult } B1 \ B2))!j!i$
 $= f$
 $\quad (\text{scalar-product}$
 $\quad \quad (\text{row } A1 \ (i \ \text{div} \ (\text{row-length } B1)))$
 $\quad \quad (\text{col } A2 \ (j \ \text{div} \ (\text{length } B2))))$
 $\quad (\text{scalar-product}$
 $\quad \quad (\text{row } B1 \ (i \ \text{mod} \ (\text{row-length } B1)))$
 $\quad \quad (\text{col } B2 \ (j \ \text{mod} \ (\text{length } B2))))$
 $\langle \text{proof} \rangle$

lemma *effective-matrix-match-condn-1*:
assumes *matrix-match* $A1 \ A2 \ B1 \ B2$
shows $\forall i \ j. ((i < (\text{row-length } A1) * (\text{row-length } B1))$
 $\quad \wedge (j < (\text{length } A2) * (\text{length } B2))$
 $\quad \longrightarrow ((A1 \circ A2) \otimes (B1 \circ B2))!j!i$
 $\quad = f$
 $\quad \quad (\text{scalar-product}$
 $\quad \quad \quad (\text{row } A1 \ (i \ \text{div} \ (\text{row-length } B1)))$
 $\quad \quad \quad (\text{col } A2 \ (j \ \text{div} \ (\text{length } B2))))$
 $\quad \quad (\text{scalar-product}$
 $\quad \quad \quad (\text{row } B1 \ (i \ \text{mod} \ (\text{row-length } B1)))$
 $\quad \quad \quad (\text{col } B2 \ (j \ \text{mod} \ (\text{length } B2))))$
 $\langle \text{proof} \rangle$

theorem *elements-matrix-distribution2*:
fixes $A1 \ A2 \ B1 \ B2 \ i \ j$

assumes $wf1:mat$ (row-length $A1$) (length $A1$) $A1$
and $wf2:mat$ (row-length $A2$) (length $A2$) $A2$
and $wf3:mat$ (row-length $B1$) (length $B1$) $B1$
and $wf4:mat$ (row-length $B2$) (length $B2$) $B2$
and $matchAA: length A1 = row-length A2$
and $matchBB: length B1 = row-length B2$
and $non-Nil: (A1 \neq []) \wedge (A2 \neq []) \wedge (B1 \neq []) \wedge (B2 \neq [])$
and $i: i < (row-length A1) * (row-length B1)$ **and** $j: j < (length A2) * (length B2)$

shows

$((A1 \otimes B1) \circ (A2 \otimes B2))!j!i$
 $=$ *scalar-product*
 (*vec-vec-Tensor*
 (*row A1 (i div row-length B1)*
 (*row B1 (i mod row-length B1)*)))
 (*vec-vec-Tensor*
 (*col A2 (j div length B2)*
 (*col B2 (j mod length B2)*)))

$\langle proof \rangle$

lemma *matrix-match-condn-2:*

$matrix-match A1 A2 B1 B2$
 $\wedge ((i < (row-length A1) * (row-length B1))$
 $\wedge (j < (length A2) * (length B2)))$
 $\implies ((A1 \otimes B1) \circ (A2 \otimes B2))!j!i$
 $=$ *scalar-product*
 (*vec-vec-Tensor*
 (*row A1 (i div row-length B1)*
 (*row B1 (i mod row-length B1)*)))
 (*vec-vec-Tensor*
 (*col A2 (j div length B2)*
 (*col B2 (j mod length B2)*)))

$\langle proof \rangle$

lemma *effective-matrix-match-condn-2:*

assumes ($matrix-match A1 A2 B1 B2$)
shows $\forall i j. ((i < (row-length A1) * (row-length B1))$
 $\wedge (j < (length A2) * (length B2)))$
 $\longrightarrow ((A1 \otimes B1) \circ (A2 \otimes B2))!j!i$
 $=$ *scalar-product*
 (*vec-vec-Tensor*
 (*row A1 (i div row-length B1)*
 (*row B1 (i mod row-length B1)*)))
 (*vec-vec-Tensor*
 (*col A2 (j div length B2)*
 (*col B2 (j mod length B2)*)))

$\langle proof \rangle$

lemma *zip-Nil*: $\text{zip } [] [] = []$

<proof>

lemma *zer-left-mult*: $f \text{ zer } x = \text{zer}$

<proof>

lemma *zip-Cons*: $(\text{length } v = \text{length } w) \implies \text{zip } (a\#v) (b\#w) = (a,b)\#(\text{zip } v w)$

<proof>

lemma *scalar-product-times*:

$$\begin{aligned} \forall w1 w2. (\text{length } w1 = \text{length } w2) \wedge (\text{length } w1 = n) \longrightarrow \\ (f (x*y) (\text{scalar-product } w1 w2)) \\ = (\text{scalar-product} \\ (\text{times } x w1) \\ (\text{times } y w2)) \end{aligned}$$

<proof>

lemma *effective-scalar-product-times*:

assumes $(\text{length } w1 = \text{length } w2)$

shows $(f (x*y) (\text{scalar-product } w1 w2))$
 $= (\text{scalar-product } (\text{times } x w1) (\text{times } y w2))$

<proof>

lemma *zip-append*: $(\text{length } zs = \text{length } ws) \wedge (\text{length } xs = \text{length } ys)$

$$\implies (\text{zip } (xs@zs) (ys@ws)) = (\text{zip } xs ys)@(\text{zip } zs ws)$$

<proof>

lemma *scalar-product-append*:

$$\begin{aligned} \forall xs ys zs ws. (\text{length } zs = \text{length } ws) \\ \wedge (\text{length } xs = \text{length } ys) \\ \wedge (\text{length } xs = n) \longrightarrow \\ (\text{scalar-product } (xs@zs) (ys@ws)) \\ = (\text{scalar-product } xs ys) \\ + (\text{scalar-product } zs ws) \end{aligned}$$

<proof>

lemma *effective-scalar-product-append*:

assumes $\text{length } zs = \text{length } ws$ **and** $(\text{length } xs = \text{length } ys)$

shows $(\text{scalar-product } (xs@zs) (ys@ws)) = (\text{scalar-product } xs ys) + (\text{scalar-product } zs ws)$

<proof>

lemma *scalar-product-distributivity*:

$$\begin{aligned} \forall v1 v2 w1 w2. ((\text{length } v1 = \text{length } v2) \wedge (\text{length } v1 = n) \wedge (\text{length } w1 = \text{length } w2)) \\ \longrightarrow (\text{scalar-product } v1 v2) * (\text{scalar-product } w1 w2) \end{aligned}$$

= scalar-product (vec-vec-Tensor v1 w1) (vec-vec-Tensor v2 w2))
 ⟨proof⟩

lemma effective-scalar-product-distributivity:

assumes length v1 = length v2 **and** length w1 = length w2

shows (scalar-product v1 v2)*(scalar-product w1 w2)

= scalar-product (vec-vec-Tensor v1 w1) (vec-vec-Tensor v2 w2)

⟨proof⟩

lemma row-length-constant:**assumes** mat nr nc A **and** j < length A

shows length (A!j) = (row-length A)

⟨proof⟩

theorem row-col-match:

fixes A1 A2 B1 B2 i j

assumes wf1:mat (row-length A1) (length A1) A1

and wf2:mat (row-length A2) (length A2) A2

and wf3:mat (row-length B1) (length B1) B1

and wf4:mat (row-length B2) (length B2) B2

and matchAA:length A1 = row-length A2

and matchBB:length B1 = row-length B2

and non-Nil:(A1 ≠ []) ∧ (A2 ≠ []) ∧ (B1 ≠ []) ∧ (B2 ≠ [])

and i:i < (row-length A1)*(row-length B1) **and** j:j < (length A2)*(length B2)

shows length (row A1 (i div (row-length B1)))

= length (col A2 (j div (length B2)))

and length (row B1 (i mod (row-length B1)))

= length (col B2 (j mod (length B2)))

⟨proof⟩

lemma effective-row-col-match: **assumes** matrix-match A1 A2 B1 B2

shows ∀ i j. ((i < (row-length A1)*(row-length B1)) ∧ (j < (length A2)*(length B2)))

→ length (row A1 (i div (row-length B1))) = length (col A2 (j div (length B2)))

∀ i j. ((i < (row-length A1)*(row-length B1)) ∧ (j < (length A2)*(length B2)))

→ length (row B1 (i mod (row-length B1))) = length (col B2 (j mod (length B2)))

⟨proof⟩

theorem prelim-element-match:

matrix-match A1 A2 B1 B2 ⇒ (∀ i j. ((i < (row-length A1)*(row-length B1))
 ∧ (j < (length A2)*(length B2))))

→

((A1 ∘ A2) ⊗ (B1 ∘ B2))!j!i

$= ((A1 \otimes B1) \circ (A2 \otimes B2)) ! j ! i$

$\langle proof \rangle$

theorem *element-match:*

matrix-match $A1\ A2\ B1\ B2 \implies (\forall i < ((row\text{-}length\ A1) * (row\text{-}length\ B1)).$
 $\quad \quad \quad \forall j < ((length\ A2) * (length\ B2)).$
 $((A1 \circ A2) \otimes (B1 \circ B2)) ! j ! i$
 $\quad \quad \quad = ((A1 \otimes B1) \circ (A2 \otimes B2)) ! j ! i)$

$\langle proof \rangle$

lemma *application: fixes* $m1\ m2$

shows $\forall m1\ m2. (mat\ nr\ nc\ m1)$
 $\quad \wedge (mat\ nr\ nc\ m2)$
 $\quad \wedge (\forall j < nc. \forall i < nr. m1 ! j ! i = m2 ! j ! i)$
 $\quad \longrightarrow (m1 = m2)$

$\langle proof \rangle$

theorem *tensor-compose-condn:*

assumes $wf1: mat\ nr\ nc\ ((A1 \circ A2) \otimes (B1 \circ B2))$
and $wf2: mat\ nr\ nc\ ((A1 \otimes B1) \circ (A2 \otimes B2))$
and $wf3: \forall j < nc. \forall i < nr. (((A1 \circ A2) \otimes (B1 \circ B2)) ! j ! i$
 $\quad \quad \quad = ((A1 \otimes B1) \circ (A2 \otimes B2)) ! j ! i)$
shows $((A1 \circ A2) \otimes (B1 \circ B2))$
 $\quad \quad \quad = ((A1 \otimes B1) \circ (A2 \otimes B2))$

$\langle proof \rangle$

The following theorem gives us the distributivity relation of tensor product with matrix multiplication

theorem *distributivity:*

assumes *matrix-match* $A1\ A2\ B1\ B2$
shows $((A1 \circ A2) \otimes (B1 \circ B2)) = ((A1 \otimes B1) \circ (A2 \otimes B2))$

$\langle proof \rangle$

end

end