

# Kronecker Algebra

Computer Systems

Johann Blieberger

Verifying Programs

The Kronecker Sum

## Kronecker Product of Finite State Machines (FSMs)

#### Definition

Given an m-by-n matrix A and a p-by-q matrix B, their Kronecker product denoted by  $A \otimes B$  is a mp-by-nq block matrix defined by

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \dots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \dots & a_{m,n}B \end{pmatrix}.$$

#### Example

For example, if

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

and

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix},$$

then

$$A\otimes B=\begin{pmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & a_{1,1}b_{1,3} & a_{1,2}b_{1,1} & a_{1,2}b_{1,2} & a_{1,2}b_{1,3}\\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & a_{1,1}b_{2,3} & a_{1,2}b_{2,1} & a_{1,2}b_{2,2} & a_{1,2}b_{2,3}\\ a_{1,1}b_{3,1} & a_{1,1}b_{3,2} & a_{1,1}b_{3,3} & a_{1,2}b_{3,1} & a_{1,2}b_{3,2} & a_{1,2}b_{3,3}\\ a_{2,1}b_{1,1} & a_{2,1}b_{1,2} & a_{2,1}b_{1,3} & a_{2,2}b_{1,1} & a_{2,2}b_{1,2} & a_{2,2}b_{1,3}\\ a_{2,1}b_{2,1} & a_{2,1}b_{2,2} & a_{2,1}b_{2,3} & a_{2,2}b_{2,1} & a_{2,2}b_{2,2} & a_{2,2}b_{2,3}\\ a_{2,1}b_{3,1} & a_{2,1}b_{3,2} & a_{2,1}b_{3,3} & a_{2,2}b_{3,1} & a_{2,2}b_{3,2} & a_{2,2}b_{3,3} \end{pmatrix}.$$

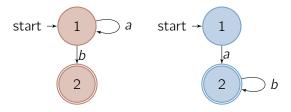


Abbildung: FSMs A (left) and B (right)

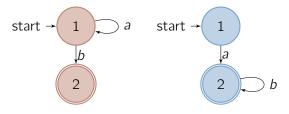


Abbildung: FSMs A (left) and B (right)

#### Example

matrices

$$A = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}, A \otimes B = \begin{pmatrix} \cdot & aa & \cdot & ba \\ \cdot & ab & \cdot & bb \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

#### Initial and Final States

Let  $S_A$  and  $S_B$  be the initial state vectors of the operands,  $F_A$  and  $F_B$  their final state vectors. Then the initial vector of the Kronecker product is given by  $S_A \otimes S_B$  and its final vector is  $F_A \otimes F_B$ .

#### Example

$$S_A = (1,0), S_B = (1,0), F_A = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \text{ and } F_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \text{ Thus } S_{A \otimes B} = (1,0,0,0) \text{ and } S_{A \otimes B} = (1,0,0,0)$$

$$F_{A\otimes B} = \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix}$$

which simply state that the initial state of the Kronecker product FSM  $A \otimes B$  is state 1 and its final state is state 4.

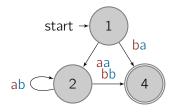


Abbildung: Graphical Representation of  $A \otimes B$ 

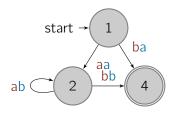


Abbildung: Graphical Representation of  $A \otimes B$ 

#### Surprise

matrix has size four

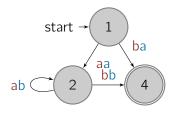


Abbildung: Graphical Representation of  $A \otimes B$ 

#### Surprise

matrix has size four only three states above

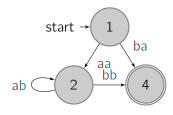
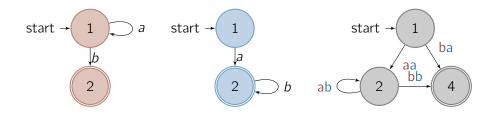


Abbildung: Graphical Representation of  $A \otimes B$ 

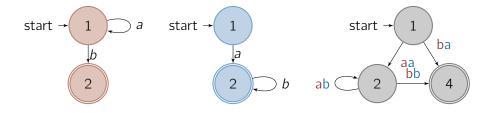
#### Surprise

matrix has size four only three states above State 3 cannot be reached from the initial state 1!



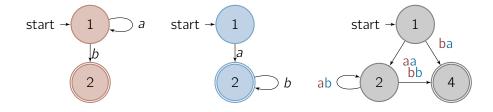
Both FSMs, A and B perform their state transitions in *lockstep*.

- 1 At the beginning, both FSMs are in their initial state. *B* has to proceed to state 2, thereby generating output *a*. *A* has two possible successor states:
  - A stays in state 1, producing output a. This corresponds to state transition  $1 \rightarrow 2$  in the product FSM.
  - B A proceeds to its state 2 (output: b). This corresponds to state transition  $1 \rightarrow 4$  in the product FSM.



Both FSMs, A and B perform their state transitions in *lockstep*.

If the previous step was 1A, both FSMs can now produce together an arbitrary number of ab-pairs. This corresponds to the transition  $2 \rightarrow 2$  in the product FSM. When A issues a b, B also has to produce a b. This corresponds to transition  $2 \rightarrow 4$  in the product FSM. Then both FSMs are in their final states. A cannot do a further state transition and both FSMs and the product FSM terminate.



Both FSMs, A and B perform their state transitions in *lockstep*.

If the previous step was 1B, both FSMs are in their final states. Since A cannot proceed, both FSMs and the product FSM terminate.

#### Theorem

Given two FSMs A and B, their Kronecker product FSM generates the same output than A and B do when they execute in lockstep.

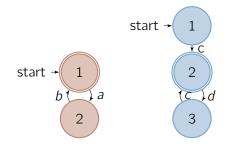


Abbildung: FSMs C (left) and D (right)

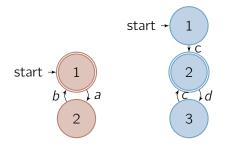


Abbildung: FSMs C (left) and D (right)

C terminates only when it has done an even number of state transitions

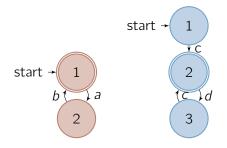


Abbildung: FSMs C (left) and D (right)

- C terminates only when it has done an even number of state transitions
- D can terminate only after it has done an odd number of transitions

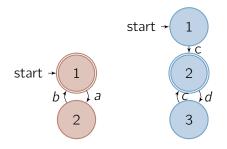


Abbildung: FSMs C (left) and D (right)

 ${\cal C}$  terminates only when it has done an even number of state transitions  ${\cal D}$  can terminate only after it has done an odd number of transitions overall output of  ${\cal C}$  ...  $(ab)^*$ 

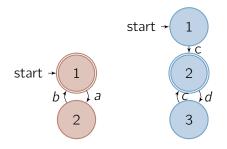


Abbildung: FSMs C (left) and D (right)

C terminates only when it has done an even number of state transitions D can terminate only after it has done an odd number of transitions overall output of C ...  $(ab)^*$  overall output of D ...  $C(dc)^*$ 

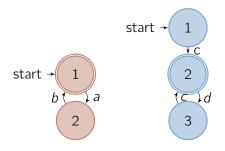


Abbildung: FSMs C (left) and D (right)

C terminates only when it has done an even number of state transitions D can terminate only after it has done an odd number of transitions overall output of C ...  $(ab)^*$  overall output of D ...  $c(dc)^*$  the Kronecker product of C and D ...

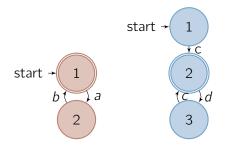


Abbildung: FSMs C (left) and D (right)

C terminates only when it has done an even number of state transitions D can terminate only after it has done an odd number of transitions overall output of C ...  $(ab)^*$  overall output of D ...  $c(dc)^*$  the Kronecker product of C and D ... 0.

$$C = \begin{pmatrix} \cdot & a \\ b & \cdot \end{pmatrix} \text{ and } D = \begin{pmatrix} \cdot & c & \cdot \\ \cdot & \cdot & d \\ \cdot & c & \cdot \end{pmatrix}$$

$$C \otimes D = \begin{pmatrix} \cdot & \cdot & \cdot & ac & \cdot \\ \cdot & \cdot & \cdot & ac & \cdot \\ \cdot & \cdot & \cdot & ac & \cdot \\ \cdot & bc & \cdot & \cdot & \cdot \\ \cdot & bc & \cdot & \cdot & \cdot \end{pmatrix}$$

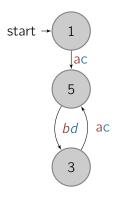


Abbildung: Graphical Representation of  $C \otimes D$ 

the final state 2

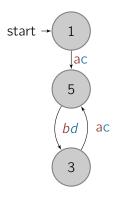


Abbildung: Graphical Representation of  $C \otimes D$ 

the final state 2 cannot be reached from the initial state 1.

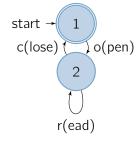


Abbildung: Graphical Representation of File Usage Scenario F

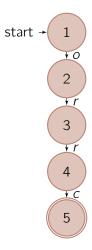


Abbildung: Graphical Representation of File Usage System A

$$A \otimes F = \begin{pmatrix} \cdot & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & r & \cdot & \cdot \\ \cdot & \cdot & r & \cdot & \cdot \\ \cdot & \cdot & \cdot & c \\ \cdot & \cdot & \cdot & \cdot & c \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} \otimes \begin{pmatrix} \cdot & 0 \\ c & r \end{pmatrix} = \begin{pmatrix} \cdot & \cdot & \cdot & 00 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 00 & 0r & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & r0 & r & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & r0 & r & r & r & \cdot & \cdot \\ \cdot & \cdot & \cdot & r & r & r & r & r & \cdot \\ \cdot & \cdot & \cdot & \cdot & r & r & r & r & r \\ \cdot & \cdot & \cdot & \cdot & r & r & r & r & r & r \\ \cdot & \cdot & \cdot & \cdot & r & r & r & r & r & r \\ \cdot & \cdot & \cdot & \cdot & r & r & r & r & r \\ \cdot & \cdot & \cdot & \cdot & r & r & r & r & r \\ \cdot & \cdot & \cdot & r & r & r & r & r & r \\ \cdot & \cdot & \cdot & r & r & r & r & r \\ \cdot & \cdot & \cdot & r & r & r & r & r \\ \cdot & \cdot & r & r & r & r & r & r \\ \cdot & \cdot & r & r & r & r & r & r \\ \cdot & \cdot & r & r & r & r & r & r \\ \cdot & \cdot & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r \\ \cdot & r & r & r & r & r & r & r \\ \cdot & r & r$$

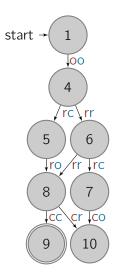


Abbildung: Graphical Representation of  $A \otimes F$ 

pairings rc, ro, ... do not make sense (lockstep!)

pairings *rc*, *ro*, ... do not make sense (lockstep!) we change the definition of the Kronecker product a little bit:

pairings rc, ro, ... do not make sense (lockstep!) we change the definition of the Kronecker product a little bit: We assume that  $rc = ro = \cdots = 0$ 

```
pairings rc, ro, ... do not make sense (lockstep!) we change the definition of the Kronecker product a little bit: We assume that rc = ro = \cdots = 0 and for simplicity set oo = o, rr = r, and cc = c.
```

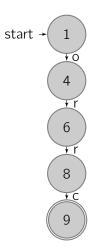


Abbildung: Graphical Representation of "new"  $A \otimes F$ 

Figures are very similar

Figures are very similar In fact only the node IDs differ

Figures are very similar In fact only the node IDs differ

In graph theory, an *isomorphism* of graphs G and H is a bijection f between the node sets of G and H such that any two nodes u and v of G are adjacent in G if and only if f(u) and f(v) are adjacent in H. If an isomorphism exists between two graphs, then the graphs are called *isomorphic*. We write  $G \simeq H$  in such a case.

Figures are very similar In fact only the node IDs differ

In graph theory, an *isomorphism* of graphs G and H is a bijection f between the node sets of G and H such that any two nodes u and v of G are adjacent in G if and only if f(u) and f(v) are adjacent in H. If an isomorphism exists between two graphs, then the graphs are called *isomorphic*. We write  $G \simeq H$  in such a case.

So, clearly the graphs of our example are isomorphic.

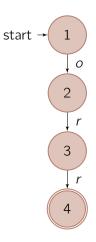


Abbildung: Graphical Representation of File Usage System  ${\it B}$ 

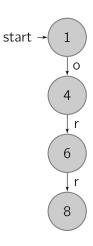


Abbildung: Graphical Representation of  $B \otimes F$ 

Isomorphic?

Isomorphic?

#### Definition

An isomorphism of two control flow graphs (CFGs) G and H is a bijection f between the node sets of G and H such that any two nodes u and v of G are adjacent in G if and only if f(u) and f(v) are adjacent in H. In addition, let r be the root node of G. Then f(r) has to be the root node of H. For all final nodes g of G, g have to be final nodes of g, and for all final nodes g of g, then the CFGs are called g isomorphic which we denote by  $g \in H$ .

Isomorphic?

#### Definition

An isomorphism of two control flow graphs (CFGs) G and H is a bijection f between the node sets of G and H such that any two nodes u and v of G are adjacent in G if and only if f(u) and f(v) are adjacent in H. In addition, let r be the root node of G. Then f(r) has to be the root node of H. For all final nodes G0 of G1 have to be final nodes of G2 have to be final nodes of G3. If an isomorphism exists between two CFGs, then the CFGs are called *isomorphic* which we denote by  $G \cong H$ 3.

With this definition we still have  $A \otimes F \simeq A$  but  $B \otimes F \not\simeq B$  because there is no final node in this case.

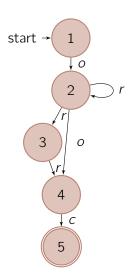


Abbildung: Graphical Representation of File Usage System C

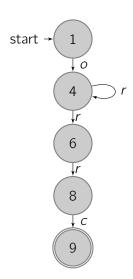


Abbildung: Graphical Representation of  $C \otimes F$ 

Isomorphic?

Isomorphic?

#### General Statement

- Assume we pick a path on program P's side, that complies to the usage scenario U. Then a corresponding path will be present in  $P \otimes U$ .
- 2 Assume we pick a path on program P's side, that does not comply completely to the usage scenario U. Then a "corresponding" path in  $P \otimes U$  will end as soon as the path does not comply to U. This will result in  $P \not\simeq P \otimes U$ .

Isomorphic?

#### General Statement

- Assume we pick a path on program P's side, that complies to the usage scenario U. Then a corresponding path will be present in  $P \otimes U$ .
- Assume we pick a path on program P's side, that does not comply completely to the usage scenario U. Then a "corresponding" path in  $P \otimes U$  will end as soon as the path does not comply to U. This will result in  $P \not\simeq P \otimes U$ .

Thus we can state:

#### Theorem

Given P, a control flow graph (CFG) of a program, and a usage scenario U, program P complies to U if and only if  $P \simeq P \otimes U$ .

programs will use several objects (classes, modules, packages, ...) for implementing their own task.

- programs will use several objects (classes, modules, packages, ...) for implementing their own task.
- checking against each of their usage scenarios could be done one after the other.

- programs will use several objects (classes, modules, packages, ...) for implementing their own task.
- checking against each of their usage scenarios could be done one after the other.
- here: check a program against two and more usage scenarios at the same time.

- programs will use several objects (classes, modules, packages, ...) for implementing their own task.
- checking against each of their usage scenarios could be done one after the other.
- here: check a program against two and more usage scenarios at the same time.
- Kronecker sum.

Assume that  $U \in M_n(\mathcal{U})$  and  $W \in M_m(\mathcal{W})$  and that  $\mathcal{U} \cap \mathcal{W} = \emptyset$ .

Assume that  $U \in M_n(\mathcal{U})$  and  $W \in M_m(\mathcal{W})$  and that  $\mathcal{U} \cap \mathcal{W} = \emptyset$ . Introduce self loops on both sides.

Assume that  $U \in M_n(\mathcal{U})$  and  $W \in M_m(\mathcal{W})$  and that  $\mathcal{U} \cap \mathcal{W} = \emptyset$ . Introduce self loops on both sides.

#### Definition

$$U \oplus W = U \otimes \left(W + \left(\sum_{x \in \mathcal{U}} x\right) I_m\right) + \left(U + \left(\sum_{y \in \mathcal{W}} y\right) I_n\right) \otimes W =$$

$$U \otimes W + U \otimes \left(\left(\sum_{x \in \mathcal{U}} x\right) I_m\right) + U \otimes W + \left(\left(\sum_{y \in \mathcal{W}} y\right) I_n\right) \otimes W.$$

Note that  $U \otimes W = Z_{n \cdot m}$  because the edge labels of U and W are disjoint. Hence we get

$$U \oplus W = U \otimes I_m + I_n \otimes W.$$

#### Theorem

With the definitions above, a program A can be checked against two usage scenarios U and W by calculating

$$A \odot (U \oplus W) = A \odot (U \otimes I_m + I_n \otimes W)$$
.

We can even check a program against more than two usage scenarios at the same time.

We can even check a program against more than two usage scenarios at the same time. In order to be able to write this in a concise way, we introduce

$$\bigoplus_{x \in \mathcal{X}} x$$

similar to the sigma notation for standard sums.

We can even check a program against more than two usage scenarios at the same time. In order to be able to write this in a concise way, we introduce

$$\bigoplus_{x \in \mathcal{X}} x$$

similar to the sigma notation for standard sums.

#### Theorem

With the definitions above, a program A can be checked against usage scenarios  $U_i$  where i = 1, ..., k by calculating

$$A \odot \left(\bigoplus_{i=1}^k U_i\right)$$
.

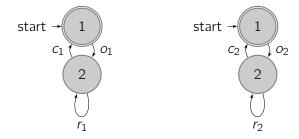
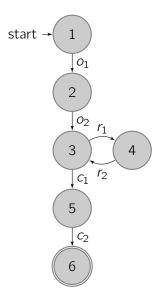


Abbildung: Graphical Representation of File Usage Scenarios  ${\it U}$  and  ${\it W}$ 



$$U = \begin{pmatrix} \cdot & o_1 \\ c_1 & r_1 \end{pmatrix},$$

$$W = \begin{pmatrix} \cdot & o_2 \\ c_2 & r_2 \end{pmatrix},$$

and

$$A = \begin{pmatrix} \cdot & o_1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & o_2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & r_1 & c_1 & \cdot \\ \cdot & \cdot & r_2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & c_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}.$$

$$U \oplus W = U \otimes I_{2} + I_{2} \otimes W =$$

$$\begin{pmatrix} \cdot & o_{1} \\ c_{1} & r_{1} \end{pmatrix} \otimes \begin{pmatrix} 1 & \cdot \\ \cdot & 1 \end{pmatrix} + \begin{pmatrix} 1 & \cdot \\ \cdot & 1 \end{pmatrix} \otimes \begin{pmatrix} \cdot & o_{2} \\ c_{2} & r_{2} \end{pmatrix} =$$

$$\begin{pmatrix} \cdot & \cdot & o_{1} & \cdot \\ \cdot & \cdot & \cdot & o_{1} \\ c_{1} & \cdot & r_{1} & \cdot \\ \cdot & c_{1} & \cdot & r_{1} \end{pmatrix} + \begin{pmatrix} \cdot & o_{2} & \cdot & \cdot \\ c_{2} & r_{2} & \cdot & \cdot \\ \cdot & \cdot & \cdot & o_{2} \\ \cdot & \cdot & c_{2} & r_{2} \end{pmatrix} =$$

$$\begin{pmatrix} \cdot & o_{2} & o_{1} & \cdot \\ c_{2} & r_{2} & \cdot & o_{1} \\ c_{1} & \cdot & r_{1} & o_{2} \\ \cdot & \cdot & c_{1} & c_{2} & r_{1} + r_{2} \end{pmatrix}.$$

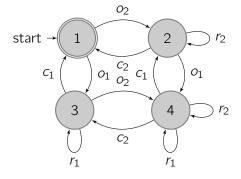
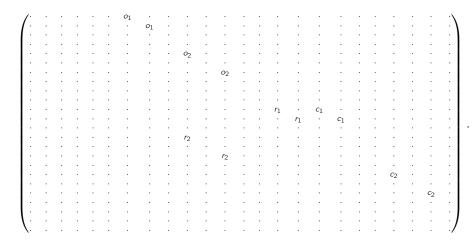


Abbildung: Graphical Representation of  $U \oplus W$ 

$$A \odot (U \oplus W) =$$



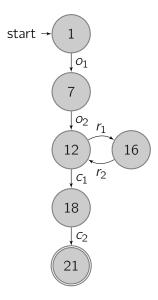


Abbildung: Graphical Representation of  $A \odot (U \oplus W)$ 

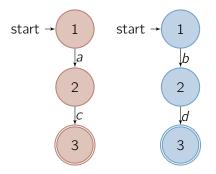


Abbildung: Our introductory example from a previous section

# Matrices

$$A = \begin{pmatrix} \cdot & a & \cdot \\ \cdot & \cdot & c \\ \cdot & \cdot & \cdot \end{pmatrix}$$

and

$$B = \begin{pmatrix} \cdot & b & \cdot \\ \cdot & \cdot & d \\ \cdot & \cdot & \cdot \end{pmatrix}$$

# Kronecker Product 2

# Kronecker Sum $A \otimes I_{3} + I_{3} \otimes B = \begin{pmatrix} \cdot & b & \cdot & a & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & d & \cdot & a & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & b & \cdot & c & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & b & \cdot & c & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & c & \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & c \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & c \\ \cdot & c \\ \cdot & c$

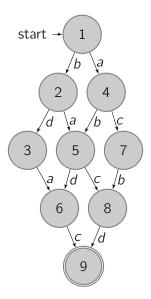


Abbildung: Resulting Interleavings Graph

For more on Kronecker Algebra and its many applications see https://kronalg.blieberger.at.