Lecture 13: relations and matrices

Jon Sterling
With contributions from Marcelo Fiore.

January 19, 2024

These lecture notes were prepared by Jon Sterling using Marcelo Fiore's lectures as source material. Any mistakes were introduced by Jon Sterling.

1 Basic definitions

jms-00J6

Definition 1.1 (Relation). A ***(binary) relation*** R from a set A to a set B, written $R \colon A \nrightarrow B$ or $R \in \mathrm{Rel}(A, B)$ is defined to be a subset $R \subseteq A \times B$. We shall typically write $a \ R \ b$ for $(a, b) \in R$. More generally, a ***relation between multiple sets*** $(A_i)_{i \in I}$ is defined to be a subset of the cartesian product $\prod_{i \in I} A_i$.

jms-00I7

Lemma 1.2 (Relational extensionality). Let A and B be two sets, and let $R, S \colon A \nrightarrow B$ be two relations from A to B. Then we have $R = S$ if and only if $\forall a \in A. \, \forall b \in B. \, a \ R \ b \iff a \ S \ b$.

jms-00IM

Proof. We recall that relation from A to B is nothing more than a subset of $A \times B$. By the axiom of extensionality, two subsets of $A \times B$ are equal if and only if they contain precisely the same elements. □

2 Uses of relations in computer science

jms-00I8

Example 2.1 (Relations in program specification). In the simplest terms, a specification of a program is a relation that describes the possible input/output pairs that can occur. For example, the specification that a given program compute the square root is captured by the relation $\mathsf{sq} \colon \mathbb{R}_{\geq 0} \nrightarrow \mathbb{R}$ given by pairs (x, y) such that $x = y^2$.

jms-00I9

Example 2.2 (Relations in operational semantics). Let E represent the set of states in a machine; then the behavior of this machine is usually described by a pair of relations $S \colon E \nrightarrow E$ and $V \colon E \nrightarrow \{\star\}$, such that $e \ S \ e'$ when it is possible for the machine to transition from state e to e' and such that $e \ V \ \star$ when the machine can halt in state e.

jms-00IA

Example 2.3 (Relations in program typing). Let E be the set of expression in a given programming language, and let T be the set of types in that programming

jms-00IB

language. Then the property of a given program having a certain type forms a relation $E \nrightarrow T$.

Example 2.4 (Relations for program equivalence). Let e, e' be two programs of type τ. We say that e and e' are ***observationally equivalent*** when for any other program $h\colon \tau \to ()$, then $h(e)$ terminates if and only if $h(e')$ terminates. If E_τ is the set of programs of type τ, observational equivalence therefore forms a relation $E_\tau \nrightarrow E_\tau$. jms-00IC

Example 2.5 (Networks as relations). A ***network*** is given by a set of nodes N and a relation $C\colon N \nrightarrow N$ expressing with two nodes are connected. jms-00ID

Example 2.6 (Relations in databases). We now come to an example of a relation between multiple sets: we could define a relation $R \subseteq \text{Movies} \times \text{Directors} \times \text{Years} \times \text{People}$ consisting of tuples (m, d, y, p) where m is a movie directed by d in year y with p as a cast member. jms-00IE

3 Formal examples of relations jms-00IF

Example 3.1 (The empty relation). For any two sets A and B, we may form the ***empty relation*** $\varnothing\colon A \nrightarrow B$ that relates *no* elements. In other words, $\varnothing$ is the empty subset of $A \times B$. jms-00IG

Example 3.2 (The full relation). For any two sets A and B, we may form the ***full relation*** $(A \times B)\colon A \nrightarrow B$, also called the ***total relation***, so that $a\ (A \times B)\ b$ for all $a \in A$ and $b \in B$. In other words, $(A \times B)$ is the *total* subset of $A \times B$. jms-00IH

Example 3.3 (The identity relation). For any set A, we can form the ***identity relation*** $\mathsf{id}_A\colon A \nrightarrow A$, also called the ***equality relation***, which relates each element of A to itself. In other words, we have $a\ \mathsf{id}_A\ a'$ if and only if $a = a'$. jms-00II

We have already seen the square root relation from positive reals to reals, which corresponds to a *total* but *many-valued* function. We can define an analogous relationship in Example 3.4 below from positive integers (naturals) to integers, which will correspond to a *partial* and many-valued function.

Example 3.4 (The integer square root relation). The square root operation corresponds to a relation $R_2\colon \mathbb{N} \nrightarrow \mathbb{Z}$ such that $m\ R_2\ n$ if and only if $m = n^2$. jms-00IJ

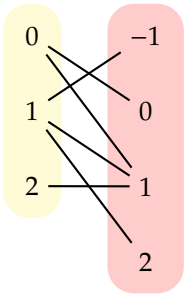
4 Visualising relations jms-00J5

Notation 4.1 (Internal diagrams of relations). A useful way to visualise a relation between two sets is by means of ***internal diagrams***: each set is depicted as a blob containing its elements, and lines are drawn from the elements of one blob to the elements of the second blob when they are related. jms-00IK

In particular, let $R\colon \mathbb{N} \nrightarrow \mathbb{Z}$ be the following relation:

$$R = \{(0,0), (1,-1), (0,1), (1,2), (1,1), (2,1)\}$$

We can depict R by the following internal diagram:



Exercise 4.2 (An internal diagram). Draw the internal diagram corresponding to the following relation: jms-00IL

$$S : \mathbb{Z} \nrightarrow \mathbb{Z}$$
$$S = \{(1,0),(1,2),(2,1),(2,3)\}$$

5 Relational composition jms-00IQ

Definition 5.1 (Relational composites). Given relations $R : A \nrightarrow B$ and $S : B \nrightarrow C$, we can define the ***relational composite*** $S \circ R : A \nrightarrow C$ in a way that generalises composition of functions. In particular, we define $S \circ R$ to be the following subset of $A \times C$: jms-00IN

$$S \circ R : A \nrightarrow C$$
$$S \circ R = \{(a,c) \in A \times C \mid \exists b \in B.\, a\ R\ b \wedge b\ S\ c\}$$

Example 5.2 (Negation invariance of the square root relation). Recall the square root relation $\mathsf{sq} : \mathbb{R}_{\geq 0} \nrightarrow \mathbb{R}$ from Example 2.1, and let $\mathsf{neg} : \mathbb{R} \nrightarrow \mathbb{R}$ be the relation $\{(x,y) \in \mathbb{R}^2 \mid x = -y\}$. Then the relational composite $\mathsf{neg} \circ \mathsf{sq} : \mathbb{R}_{\geq 0} \nrightarrow \mathbb{R}$ is equal to sq. jms-00IO

Proof. By relational extensionality, it suffices to check that for any $x \in \mathbb{R}_{\geq 0}$ and $y \in \mathbb{R}$, we have $x\ (\mathsf{neg} \circ \mathsf{sq})\ y$ if and only if $x\ \mathsf{sq}\ y$. We compute:

$$\begin{aligned} x\ (\mathsf{neg} \circ \mathsf{sq})\ y &\iff \exists z \in \mathbb{R}.\, x\ \mathsf{sq}\ z \wedge z\ \mathsf{neg}\ y \\ &\iff \exists z \in \mathbb{R}.\, x = z^2 \wedge z = -y \\ &\iff x = (-y)^2 \\ &\iff x = y^2 \\ &\iff x\ \mathsf{sq}\ y \end{aligned}$$

□

Lemma 5.3 (Associativity and unit laws of relational composition). Relational composition is associative and has the identity relation as a neutral element. jms-00IP

Proof. To prove associativity, we fix relations $R : A \nrightarrow B$, $S : B \nrightarrow C$, and $T : C \nrightarrow D$ to prove $(T \circ S) \circ R = T \circ (S \circ R)$. To get started, we compute the intermediate composites:

$$b\ (T \circ S)\ d \iff \exists c \in C.\, b\ S\ c \wedge c\ T\ d$$
$$a\ (S \circ R)\ c \iff \exists b \in B.\, a\ R\ b \wedge b\ S\ c$$

Using the above, we can compute the full composites:

$$\begin{aligned} a\ ((T \circ S) \circ R)\ d &\iff \exists b \in B.\, a\ R\ b \wedge b\ (T \circ S)\ d \\ &\iff \exists b \in B.\, a\ R\ b \wedge \exists c \in C.\, c\ S\ c \wedge c\ T\ d \\ &\iff \exists b \in B.\, \exists c \in C.\, a\ R\ b \wedge b\ S\ c \wedge c\ T\ d \\ &\iff \exists c \in C.\, (\exists b \in B.\, a\ R\ b \wedge b\ S\ c) \wedge c\ T\ d \\ &\iff \exists c \in C.\, a\ (S \circ R)\ c \wedge c\ T\ d \\ &\iff a\ (T \circ (S \circ R))\ d \end{aligned}$$

For the right and left neutrality, we must prove that $R \circ \mathsf{id}_A = R = \mathsf{id}_B \circ R$ for all $r : A \nrightarrow B$. We prove only the first law, as the other proof is analogous:

$$\begin{aligned} a\ (R \circ \mathsf{id}_A)\ b &\iff \exists a' \in A.\, a\ \mathsf{id}_A\ a' \wedge a'\ R\ b \\ &\iff \exists a' \in A.\, a = a' \wedge a'\ R\ b \\ &\iff a\ R\ b \end{aligned}$$

□

6 Relations and matrices

jms-00IR

Relations between finite sets can be desribed in a more computationally friendly way by their tabulation as *matrices*. In particular, we shall see in § 6.4 that an $(m \times n)$-matrix over the boolean semiring is precisely the same thing as a relation from $[m]$ to $[n]$, where $[l] = \{i \mid 0 \leq i < l\}$ is the set of natural numbers strictly smaller than l. Then we will see that relational composition is, under this correspondence, the same as *matrix multiplication*.

Definition 6.1 (Matrix over a semiring). For natural numbers m and n, an $(m \times n)$-***matrix*** over a semiring $(S, 0, \oplus, 1, \odot)$ is given by entries $M_{i,j} \in S$ for all $i \in [m]$ and $j \in [n]$. We will write $\mathrm{Mat}_S(m, m)$ for the set of $(m \times n)$-***matrices***.

jms-00IS

Notation 6.2 (Matrices as tables). $(m \times n)$-matrices can be depicted in tables or grids with rows in the first dimension and columns in the second dimension. For example, let $M \in \mathrm{Mat}_{\mathbb{B}}(3, 2)$ be the matrix over the booleans defined by the following equation:

jms-00J4

$$M_{i,j} = \begin{cases} \mathsf{true} & \text{if } \mathsf{parity}(i) = \mathsf{parity}(j) \\ \mathsf{false} & \text{otherwise} \end{cases}$$

Then M is depicted by the following table with three rows and two columns:

$$M = \begin{bmatrix} \mathsf{true} & \mathsf{false} \\ \mathsf{false} & \mathsf{true} \\ \mathsf{true} & \mathsf{false} \end{bmatrix}$$

Definition 6.3 (The identity matrix). For any $m \in \mathbb{N}$, we define the ***identity*** $(m \times m)$***-matrix*** over a given semiring S as follows: jms-00IT

$$I^m_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

The identity matrix is sometimes called the ***diagonal matrix***, for reasons that become apparent when visualising it according to Notation 6.2:

$$I^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

6.4 Correspondence between matrices and finite relations jms-00J1

Definition 6.4.1 (The matrix associated to a finite relation). Let $R \colon [m] \nrightarrow [n]$ be a relation; for any semiring S, we may form the $(n \times n)$***-matrix over*** S ***associated to*** R as follows: jms-00IY

$$\left(\underline{\mathrm{mat}}_S\, R\right)_{i\in[m],j\in[n]} = \begin{cases} 1 & \text{if } i \mathrel{R} j \\ 0 & \text{otherwise} \end{cases}$$

We have defined a function $\underline{\mathrm{mat}}_S \colon \mathrm{Rel}([m],[n]) \to \mathrm{Mat}_S(m,n)$.

Definition 6.4.2 (The relation associated to a matrix). Let M be an $(n \times n)$***-matrix*** over a semiring S. We define the ***relation associated to*** M below: jms-00IZ

$$\underline{\mathrm{rel}}_S\, M \colon [m] \nrightarrow [n]$$
$$i \mathrel{\left(\underline{\mathrm{rel}}_S\, M\right)} j \iff M_{i,j} = 1$$

We have defined a function $\underline{\mathrm{rel}}_S \colon \mathrm{Mat}_S(m,n) \to \mathrm{Rel}([m],[n])$.

Lemma 6.4.3 (A retraction from matrices to finite relations). The associated matrix function $\underline{\mathrm{mat}}_S \colon \mathrm{Rel}([m],[n]) \to \mathrm{Mat}_S(m,n)$ is a section of the associated relation function $\underline{\mathrm{rel}}_S \colon \mathrm{Mat}_S(m,n) \to \mathrm{Rel}([m],[n])$ for any semiring S. jms-00J0

Proof. We must check that $\underline{\mathrm{rel}}_S \circ \underline{\mathrm{mat}}_S = \mathrm{id}_{\mathrm{Rel}([m],[n])}$. Fixing a relation $R \colon [m] \nrightarrow [n]$, we compute:

$$\begin{aligned} i \mathrel{\left(\underline{\mathrm{rel}}_S \left(\underline{\mathrm{mat}}_S\, R\right)\right)} j &\iff \left(\underline{\mathrm{mat}}_S\, R\right)_{i,j} = 1 \\ &\iff i \mathrel{R} j \end{aligned}$$

□

The other composite $\underline{\mathrm{mat}}_S \circ \underline{\mathrm{rel}}_S : \mathrm{Mat}_S(m,n) \to \mathrm{Mat}_S(m,n)$ is not in general the identity function, but is (necessarily) an *idempotent* on the set of matrices over S. We will see that this idempotent, in some sense, measures the degree to which the base semiring S is not boolean.

Lemma 6.4.4 (Finite relations as matrices over the booleans). The idempotent $\underline{\mathrm{mat}}_{\mathbb{B}} \circ \underline{\mathrm{rel}}_{\mathbb{B}} : \mathrm{Mat}_{\mathbb{B}}(m,n) \to \mathrm{Mat}_{\mathbb{B}}(m,n)$ is in fact the identity function on matrices over the boolean semiring $\mathbb{B}$. jms-00IX

Proof. We fix a matrix $M \in \mathrm{Mat}_{\mathbb{B}}(m,n)$ and compute:

$$\begin{aligned}\left(\underline{\mathrm{mat}}_{\mathbb{B}}\left(\underline{\mathrm{rel}}_{\mathbb{B}}\, M\right)\right)_{i,j} &= \begin{cases} 1 & \text{if } i \left(\underline{\mathrm{rel}}_{\mathbb{B}}\, M\right) j \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} 1 & \text{if } M_{i,j} = 1 \\ 0 & \text{otherwise} \end{cases}\end{aligned}$$

Because $\mathbb{B}$ is the boolean semiring, any scalar $s \in S$ is either 0 or 1. Therefore, we conclude:

$$\left(\underline{\mathrm{mat}}_{\mathbb{B}}\left(\underline{\mathrm{rel}}_{\mathbb{B}}\, M\right)\right)_{i,j} = M_{i,j}$$

□

Thus we conclude that an $(m \times n)$-matrix over the booleans is the same thing as a relation from $[m]$ to $[n]$.

6.5 Multiplication of matrices

jms-00IW

Side remark 6.5.1 (Matrix multiplication in geometry). Although we do not explore it in this course [1], the viewpoint of matrix multiplication as relational composition generalises to a correct explanation of the role of matrices in geometry as presentations of linear maps between vector spaces in terms of an (uncanonical) choice of basis. jms-00IU

Definition 6.5.2 (Product of matrices). Let M be an $(l \times m)$-matrix and let N be a $(m \times n)$-matrix. The ***product*** of M and N, written $M \cdot N$, is the following $(l \times n)$-matrix: jms-00IV

$$(N \cdot M)_{i \in [l], j \in [n]} = \bigoplus_{k \in [m]} M_{i,k} \cdot N_{k,j}$$

Lemma 6.5.3 (Associativity and unit laws of matrix products). The product of matrices is associative and has the identity matrix as neutral element. jms-00J3

Proof. For associativity, fix matrices $L \in \mathrm{Mat}_S(k,l)$, $M \in \mathrm{Mat}_S(l,m)$ and $N \in \mathrm{Mat}_S(m,n)$ to check that $(N \cdot M) \cdot L = N \cdot (M \cdot L)$. Below we use the associativity

of multiplication, commutativity of addition, and distributivity of multiplication over addition in the semiring S:

$$\begin{aligned}((N \cdot M) \cdot L)_{a,b} &= \bigoplus_{c \in [l]} L_{a,c} \cdot (N \cdot M)_{c,b} \\ &= \bigoplus_{c \in [l]} L_{a,c} \cdot \bigoplus_{d \in [m]} M_{c,d} \cdot N_{d,b} \\ &= \bigoplus_{c \in [l]} \bigoplus_{d \in [m]} L_{a,c} \cdot M_{c,d} \cdot N_{d,b} \\ &= \bigoplus_{d \in [m]} \left(\bigoplus_{c \in [l]} L_{a,c} \cdot M_{c,d} \right) \cdot N_{d,b} \\ &= \bigoplus_{d \in [m]} (M \cdot L)_{a,d} \cdot N_{d,b} \\ &= N \cdot (M \cdot L)\end{aligned}$$

For one unit law, we fix $M \in \mathrm{Mat}_S(m, n)$ and recall the definition of the identity matrix to check that $M \cdot I^m = M$.

$$(M \cdot I^m)_{i,j} = \bigoplus_{k \in [m]} I^m_{i,k} \cdot M_{k,j}$$

Unfolding the definition of $I^m_{i,j}$ as given in Definition 6.3, we see that the iterated sum above expands to $m - 1$ copies of $0 \cdot M_{k,j}$ for various $k \neq i$ and one copy of $1 \cdot M_{i,j}$. Thus, we conclude that $M \cdot I^m_{i,j} = M_{i,j}$ using the absorption and unit laws for multiplication as well as the unit laws for addition in S.

The other unit law follows in an analogous way. □

Lemma 6.5.4 (Matrix product is relational composition). Under the correspondence between boolean matrices and finite relations (§ 6.4, Lemma 6.4.4), matrix products of boolean matrices correspond to relational composites. In particular, given $M \in \mathrm{Mat}_{\mathbb{B}}(l, m)$ and $N \in \mathrm{Mat}_{\mathbb{B}}(m, n)$, we have: jms-00J2

$$\underline{\mathrm{rel}}_{\mathbb{B}}\,(N \cdot M) = \underline{\mathrm{rel}}_{\mathbb{B}}\,N \circ \underline{\mathrm{rel}}_{\mathbb{B}}\,M$$

Proof. We use the fact that the additive operation of the boolean semiring is disjunction and the multiplicative operation is conjunction:

$$\begin{aligned}(N \cdot M)_{i,j} &= \bigoplus_{k \in [m]} M_{i,k} \cdot N_{k,j} \\ &= \bigvee_{k \in [m]} M_{i,k} \wedge N_{k,j} \\ &= \exists k \in [m].\, M_{i,k} \wedge N_{k,j}\end{aligned}$$

□

References

[1] Marcelo Fiore and Jon Sterling. *Course: Discrete Mathematics (2023–24)*. URL: https://www.jonmsterling.com/jms-0081.xml.