Discrete Mathematics,

Lecture 14.

Additive Structure of Matrices

Let M, N be two $(m \times n)$-matrices.

The matrix sum

$$M + N \in \mathrm{Mat}(m,n)$$
$$(M+N)_{i,j} = M_{i,j} + N_{i,j}$$

The <u>zero matrix</u>

$$\mathbb{0} \in \mathrm{Mat}(m,n)$$
$$\mathbb{0}_{i,j} = 0$$

<u>Lemma.</u> For all $M \in \mathrm{Mat}(m,n)$, we have $M + \mathbb{0} = M$, $\mathbb{0} + M = M$

For M, N we have $M + N = N + M$

For L, M, N we have $L + (M+N) = (L+M) + N$

Proof. To show $M + \mathbb{0} = M$, we check for all $i \in [m], j \in [n]$

$$(M + \mathbb{0})_{i,j} = M_{i,j} + \mathbb{0}_{i,j} = M_{i,j} + 0 = M_{i,j} \qquad \blacksquare$$

Thm: $M, N \in \mathrm{Mat}_{\mathbb{B}}(m,n)$

$$\underline{\mathrm{rel}}_{\mathbb{B}}(M+N) = \underline{\mathrm{rel}}_{\mathbb{B}} M \cup \underline{\mathrm{rel}}_{\mathbb{B}} N$$

Moreover, $\underline{\mathrm{rel}}_{\mathbb{B}}\, \mathbb{0} = \emptyset$.

Proof. $i\,(\mathrm{rel}_{\mathbb{B}}(M+N))\,j \iff (M+N)_{i,j} = 1$ (true)

$\iff M_{i,j} + N_{i,j} = 1$

$\iff M_{i,j} \vee N_{i,j} = \mathrm{true}$

$\iff i\ \underline{\mathrm{rel}} M\ j \ \vee\ i\ \underline{\mathrm{rel}} N\ j$.

$\iff i\ (\underline{\mathrm{rel}} M \cup \underline{\mathrm{rel}} N)\ j$. ∎

Directed graphs

Definition 130 *A* directed graph (A, R) *consists of a set* A *and a relation* R *on* A *(i.e. a relation from* A *to* A*).*

$R : A \nrightarrow A$

$R \in \mathrm{Rel}(A)$

Corollary 132 *For every set A, the structure*

$$\big(\ \mathrm{Rel}(A)\ ,\ \mathrm{id}_A\ ,\circ\ \big)$$

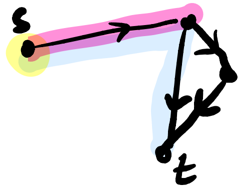
is a monoid.

Definition 133 *For $R \in \mathrm{Rel}(A)$ and $n \in \mathbb{N}$, we let*

$$R^{\circ n} = \underbrace{R \circ \cdots \circ R}_{n \text{ times}} \in \mathrm{Rel}(A)$$

be defined as id_A for $n = 0$, and as $R \circ R^{\circ m}$ for $n = m + 1$.

Paths



Proposition 135 *Let* (A, R) *be a directed graph. For all* $n \in \mathbb{N}$ *and* $s, t \in A$, $s \; R^{\circ n} \; t$ *iff there exists a path of length* n *in* R *with source* s *and target* t.

PROOF: By induction on n, we prove $P(n)$

$$P(n) = \forall s, t \in A.\ s \; R^{\circ n} \; t \iff s \overset{n}{\rightsquigarrow} t$$

1) Want $P(0)$.

$$P(0) \equiv \forall s, t \in A.\ \underline{s \; R^{\circ 0} \; t} \iff \underbrace{s \overset{0}{\rightsquigarrow} t}_{s = t} \quad !$$

$$\frac{s \; \mathrm{id}_A \; t}{s = t}$$

∎

By induction on n, we prove $P(n)$

$$P(n) = \forall s,t \in A.\ s\, R^{\circ n}\, t \iff s \leadsto^{n} t$$

2) Inductive step. Assume $P(n)$ to prove $P(n+1)$ holds.

Fix $s,t \in A$, we must show $s\, R^{\circ(n+1)}\, t \iff s \leadsto^{n+1} t$

$$s\, R^{\circ(n+1)}\, t$$
$$\equiv$$
$$s\,(R \circ R^{\circ n})\,t$$
$$\equiv$$
$$\exists u \in A.\ s R u \wedge \underbrace{u\, R^{\circ n}\, t}_{\equiv\ \exists u \leadsto^{n} t}$$

Summing up:

We must show $\left(\begin{array}{l}\exists n \\ s R u \wedge u \leadsto^{n} t\end{array}\right) \iff s \leadsto^{n+1} t$

$$s \leadsto^{1} u \leadsto^{n} t \mapsto s \leadsto^{n+1} t.$$

$\blacksquare$

Definition 136 *For* $R \in \mathrm{Rel}(A)$, *let*

$$R^{\circ *} = \bigcup \{ R^{\circ n} \in \mathrm{Rel}(A) \mid n \in \mathbb{N} \} = \bigcup_{n \in \mathbb{N}} R^{\circ n} \quad .$$

Corollary 137 *Let* (A, R) *be a directed graph. For all* $s, t \in A$, $s\ R^{\circ *}\ t$ *iff there exists a path with source* s *and target* t *in* R*.*

Thm Let $A = [n]$. Then we have $R^{\circ *} = \bigcup_{k \leq n} R^{\circ k}$.

Proof. A has no more than n elements! ∎

The $(n \times n)$-matrix $M = \mathrm{mat}(R)$ of a finite directed graph $\big([n], R\big)$ for n a positive integer is called its *adjacency matrix*.

The adjacency matrix $M^* = \mathrm{mat}(R^{\circ *})$ can be computed by matrix multiplication and addition as M_n where

$$\begin{cases} M_0 & = & I_n \\ M_{k+1} & = & I_n + \big(M \cdot M_k\big) \end{cases}$$

This gives an algorithm for establishing or refuting the existence of paths in finite directed graphs.

$M_0 = I^n$

$M_1 = I^n + M \cdot M_0 = I^n + M \cdot I^n = I^n + M$

$M_2 = I^n + M \cdot M_1 = I^n + M \cdot (I^n + M) = I^n + M \cdot I^n + \overbrace{M \cdot M}^{M^2}$

$= I^n + M + M^2$

In general $M_n = \sum_{k \le n} M^k$.

(Let $M = \underline{\text{mat}}\, R$)

Thm. $\underline{\text{mat}}\,(R^{\circ *}) = M_n$.

Proof. $\underline{\text{mat}}\,(R^{\circ *}) = \underline{\text{mat}}\left(\bigcup_{k \le n} R^{\circ k}\right)$

$= \sum_{k \le n} \underline{\text{mat}}\,(R^{\circ k})$

$= \sum_{k \le n} (\underline{\text{mat}}\, R)^k = M_n$. $\blacksquare$

Preorders

Definition 138 *A* preorder $(P, \sqsubseteq)$ *consists of a set* P *and a relation* $\sqsubseteq$ *on* P *(i.e.* $\sqsubseteq \in \mathcal{P}(P \times P)$*) satisfying the following two axioms.*

- *Reflexivity.*

$$\forall x \in P.\ x \sqsubseteq x$$

- *Transitivity.*

$$\forall x, y, z \in P.\ (x \sqsubseteq y \wedge y \sqsubseteq z) \implies x \sqsubseteq z$$

Examples:

- $(\mathbb{R}, \leq)$ and $(\mathbb{R}, \geq)$.
- $(\mathcal{P}(A), \subseteq)$ and $(\mathcal{P}(A), \supseteq)$. X space, $(\mathcal{O}(X), \subseteq)$
- $(\mathbb{Z}, |)$.

Def. Total $\Leftrightarrow$ $\forall x, y \in A.\ x \leq y \vee y \leq x$

Def. A partial order is a preorder satisfying antisymmetry: $\forall x, y \in A.\ (x \leq y \wedge y \leq x) \Rightarrow x = y$.

Theorem 140 *For* $R \subseteq A \times A$, *let*

$$\mathcal{F}_R = \{ Q \subseteq A \times A \mid R \subseteq Q \wedge Q \text{ is a preorder} \} \quad .$$

Then, (i) $R^{\circ *} \in \mathcal{F}_R$ *and* (ii) $R^{\circ *} \subseteq \bigcap \mathcal{F}_R$. *Hence,* $R^{\circ *} = \bigcap \mathcal{F}_R$.

PROOF: We need to prove $\bigcap \mathcal{F}_R \subseteq R^{\circ *} \wedge R^{\circ *} \subseteq \bigcap \mathcal{F}_R$

To show $\bigcap \mathcal{F}_R \subseteq R^{\circ *}$, we will use the fact that $R^{\circ *} \in \mathcal{F}_R$

$\underbrace{a \ \bigcap \mathcal{F}_R \ b}$ $\Rightarrow a \ R^{\circ *} \ b$

($\forall Q$ preorder containing R, $a \, Q \, b$)

But $R^{\circ *} \in \mathcal{F}_R$, so $a \ R^{\circ *} b$ ☺

To show $R^{\circ *} \in \mathcal{F}_R$, we need

1) $R \subseteq R^{\circ *}$: b/c $R^{\circ *}$ contains paths of length 1

2) $R^{\circ *}$ is reflexive $\wedge$ transitive | Reflexive: b/c $R^{\circ *}$ contains 0-paths

Transitive: $s \overset{m}{\leadsto} t$, $t \overset{n}{\leadsto} u$, $s \overset{m+n}{\leadsto} u$

We have shown that $\bigcap \rightsquigarrow_R \subseteq R^{\circ *}$.

Need: $R^{\circ *} \subseteq \bigcap \rightsquigarrow_R$.

$$a \, R^{\circ *} \, b \Rightarrow \underline{a \bigcap \rightsquigarrow_R b}$$

$$\forall Q \supseteq R,\ Q \text{ preorder.}\ a \, Q \, b$$

Spse $a \, R^{\circ *} \, b$, and fix $Q \supseteq R$ refl. $\wedge$ trans. to show $a \, Q \, b$

$$\Downarrow$$

$$a \overset{n}{\rightsquigarrow} b.$$

1) Base case $(n=0)$. That means $a=b$. Need to show $a \, Q \, \overset{a}{\overset{\|}{b}}$

Use reflexivity of Q.

2) Inductive step.

$a \overset{1}{\rightsquigarrow} c \overset{n}{\rightsquigarrow} b$

By inductive hypothesis we have $c \, Q \, b$.

By assumption we have $a \, Q \, c$.

By transitivity of Q, we $a \, Q \, b$. $\boxtimes$