

Module P: Applications of Linear Algebra

Module P Section 1

Definition P.1

In geology, a **phase** is any physically separable material in the system, such as various minerals or liquids.

A **component** is a chemical compound necessary to make up the phases; these are usually oxides such as Calcium Oxide (CaO) or Silicone Dioxide (SiO_2).

In a typical application, a geologist knows how to build each phase from the components, and is interested in determining reactions among the different phases.

Observation P.2

Consider the 3 components

$$\vec{c}_1 = \text{CaO} \quad \vec{c}_2 = \text{MgO} \quad \text{and} \quad \vec{c}_3 = \text{SiO}_2$$

and the 5 phases:

$$\vec{p}_1 = \text{Ca}_3\text{MgSi}_2\text{O}_8$$

$$\vec{p}_2 = \text{CaMgSiO}_4$$

$$\vec{p}_3 = \text{CaSiO}_3$$

$$\vec{p}_4 = \text{CaMgSi}_2\text{O}_6$$

$$\vec{p}_5 = \text{Ca}_2\text{MgSi}_2\text{O}_7$$

Geologists already know (or can easily deduce) that

$$\vec{p}_1 = 3\vec{c}_1 + \vec{c}_2 + 2\vec{c}_3$$

$$\vec{p}_2 = \vec{c}_1 + \vec{c}_2 + \vec{c}_3$$

$$\vec{p}_3 = \vec{c}_1 + 0\vec{c}_2 + \vec{c}_3$$

$$\vec{p}_4 = \vec{c}_1 + \vec{c}_2 + 2\vec{c}_3$$

$$\vec{p}_5 = 2\vec{c}_1 + \vec{c}_2 + 2\vec{c}_3$$

since, for example:

$$\vec{c}_1 + \vec{c}_3 = \text{CaO} + \text{SiO}_2 = \text{CaSiO}_3 = \vec{p}_3$$

Activity P.3 (*~5 min*) To study this vector space, each of the three components $\vec{c}_1, \vec{c}_2, \vec{c}_3$ may be considered as the three components of a Euclidean vector.

$$\vec{p}_1 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}, \vec{p}_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \vec{p}_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \vec{p}_4 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}, \vec{p}_5 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}.$$

Determine if the set of phases is linearly dependent or linearly independent.

Activity P.4 (*~15 min*) Geologists are interested in knowing all the possible chemical reactions among the 5 phases:

$$\vec{p}_1 = \text{Ca}_3\text{MgSi}_2\text{O}_8 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_2 = \text{CaMgSiO}_4 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \vec{p}_3 = \text{CaSiO}_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\vec{p}_4 = \text{CaMgSi}_2\text{O}_6 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_5 = \text{Ca}_2\text{MgSi}_2\text{O}_7 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}.$$

That is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\vec{p}_1 + x_2\vec{p}_2 + x_3\vec{p}_3 + x_4\vec{p}_4 + x_5\vec{p}_5 = 0.$$

Activity P.4 (~ 15 min) Geologists are interested in knowing all the possible chemical reactions among the 5 phases:

$$\vec{p}_1 = \text{Ca}_3\text{MgSi}_2\text{O}_8 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_2 = \text{CaMgSiO}_4 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \vec{p}_3 = \text{CaSiO}_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\vec{p}_4 = \text{CaMgSi}_2\text{O}_6 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_5 = \text{Ca}_2\text{MgSi}_2\text{O}_7 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}.$$

That is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\vec{p}_1 + x_2\vec{p}_2 + x_3\vec{p}_3 + x_4\vec{p}_4 + x_5\vec{p}_5 = \vec{0}.$$

Part 1: Set up a system of equations equivalent to this vector equation.

Activity P.4 (~ 15 min) Geologists are interested in knowing all the possible chemical reactions among the 5 phases:

$$\vec{p}_1 = \text{Ca}_3\text{MgSi}_2\text{O}_8 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_2 = \text{CaMgSiO}_4 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \vec{p}_3 = \text{CaSiO}_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\vec{p}_4 = \text{CaMgSi}_2\text{O}_6 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_5 = \text{Ca}_2\text{MgSi}_2\text{O}_7 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}.$$

That is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\vec{p}_1 + x_2\vec{p}_2 + x_3\vec{p}_3 + x_4\vec{p}_4 + x_5\vec{p}_5 = 0.$$

Part 1: Set up a system of equations equivalent to this vector equation.

Part 2: Find a basis for its solution space.

Activity P.4 (~ 15 min) Geologists are interested in knowing all the possible chemical reactions among the 5 phases:

$$\vec{p}_1 = \text{Ca}_3\text{MgSi}_2\text{O}_8 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_2 = \text{CaMgSiO}_4 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \vec{p}_3 = \text{CaSiO}_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\vec{p}_4 = \text{CaMgSi}_2\text{O}_6 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} \quad \vec{p}_5 = \text{Ca}_2\text{MgSi}_2\text{O}_7 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}.$$

That is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\vec{p}_1 + x_2\vec{p}_2 + x_3\vec{p}_3 + x_4\vec{p}_4 + x_5\vec{p}_5 = 0.$$

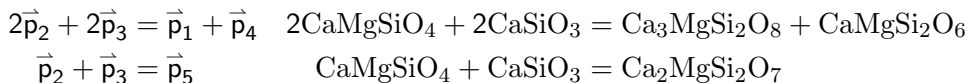
Part 1: Set up a system of equations equivalent to this vector equation.

Part 2: Find a basis for its solution space.

Part 3: Interpret each basis vector as a vector equation and a chemical equation.

Activity P.5 (*~10 min*) We found two basis vectors $\begin{bmatrix} 1 \\ -2 \\ -2 \\ 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ -1 \\ -1 \\ 0 \\ 1 \end{bmatrix}$,

corresponding to the vector and chemical equations

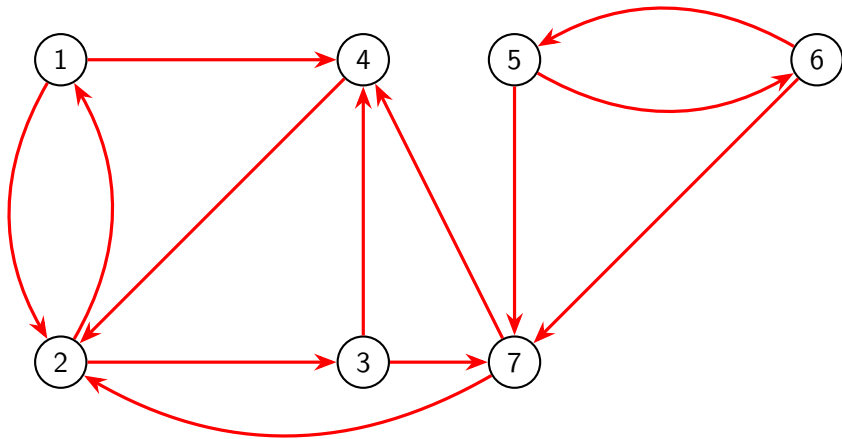


Combine the basis vectors to produce a chemical equation among the five phases that does not involve $\vec{p}_2 = \text{CaMgSiO}_4$.

Module P Section 2

Activity P.6 (~ 10 min)**A \$700,000,000,000 Problem:**

In the picture below, each circle represents a webpage, and each arrow represents a link from one page to another.



Based on how these pages link to each other, write a list of the 7 webpages in order from most important to least important.

Observation P.7

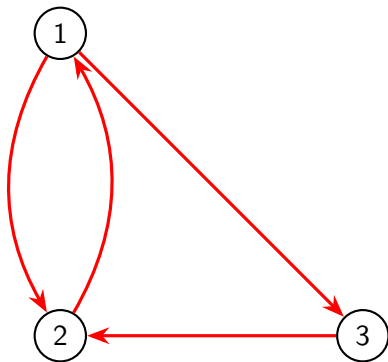
The \$700,000,000,000 Idea:

Links are endorsements.

- 1 A webpage is important if it is linked to (endorsed) by important pages.
- 2 A webpage distributes its importance equally among all the pages it links to (endorses).

Example P.8

Consider this small network with only three pages. Let x_1, x_2, x_3 be the importance of the three pages respectively.

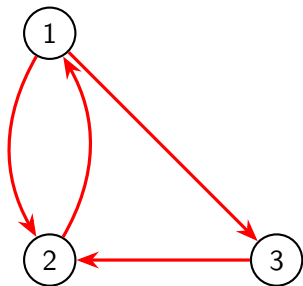


- 1 x_1 splits its endorsement in half between x_2 and x_3
- 2 x_2 sends all of its endorsement to x_1
- 3 x_3 sends all of its endorsement to x_2 .

This corresponds to the **page rank system**

$$\begin{aligned}x_2 &= x_1 \\ \frac{1}{2}x_1 + x_3 &= x_2 \\ \frac{1}{2}x_1 &= x_3\end{aligned}$$

Observation P.9



$$x_2 = x_1$$

$$\frac{1}{2}x_1 + x_3 = x_2$$

$$\frac{1}{2}x_1 = x_3$$

$$\begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

By writing this linear system in terms of matrix multiplication, we obtain the **page**

rank matrix $A = \begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & 0 \end{bmatrix}$ and page rank vector $\vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$.

Thus, computing the importance of pages on a network is equivalent to solving the matrix equation $A\vec{x} = \vec{1}\vec{x}$.

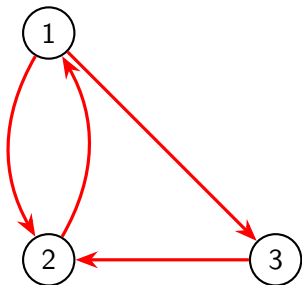
Activity P.10 (~ 5 min) Thus, our \$700,000,000,000 problem is what kind of problem?

$$\begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 1 \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

- a An antiderivative problem
- b A bijection problem
- c A cofactoring problem
- d A determinant problem
- e An eigenvector problem

Activity P.11 (~ 10 min) Find a page rank vector \vec{x} satisfying $A\vec{x} = 1\vec{x}$ for the following network's page rank matrix A .

That is, find the eigenspace associated with $\lambda = 1$ for the matrix A , and choose a vector from that eigenspace.



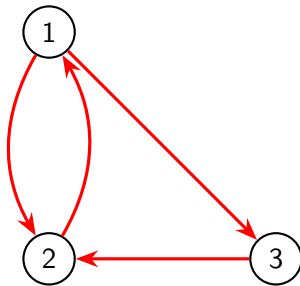
$$A = \begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & 0 \end{bmatrix}$$

Observation P.12

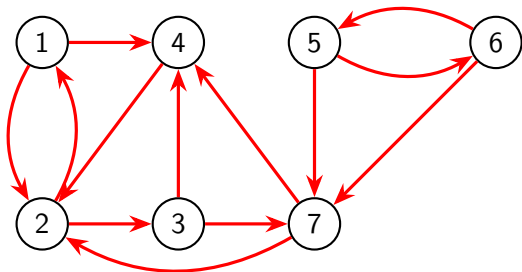
Row-reducing $A - I = \begin{bmatrix} -1 & 1 & 0 \\ \frac{1}{2} & -1 & 1 \\ \frac{1}{2} & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{bmatrix}$ yields the basic

eigenvector $\begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}$.

Therefore, we may conclude that pages 1 and 2 are equally important, and both pages are twice as important as page 3.



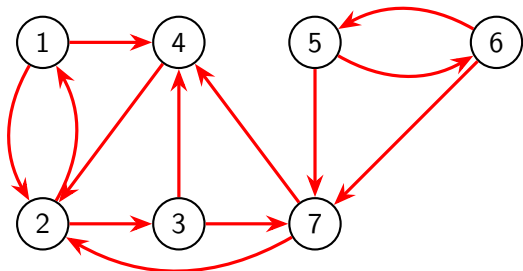
Activity P.13 (~ 5 min) Compute the 7×7 page rank matrix for the following network.



For example, since website 1 distributes its endorsement equally between 2 and 4,

the first column is $\begin{bmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$.

Activity P.14 (*~10 min*) Find a page rank vector for the given page rank matrix.

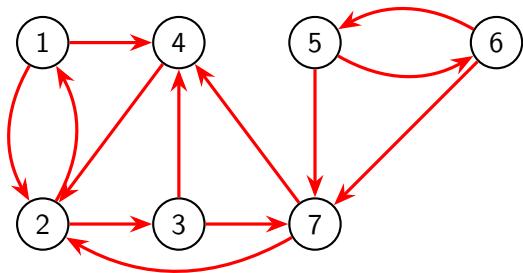


$$A = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 1 & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$$

Which webpage is most important?

Observation P.15

Since a page rank vector for the network is given by \vec{x} , it's reasonable to consider page 2 as the most important page.

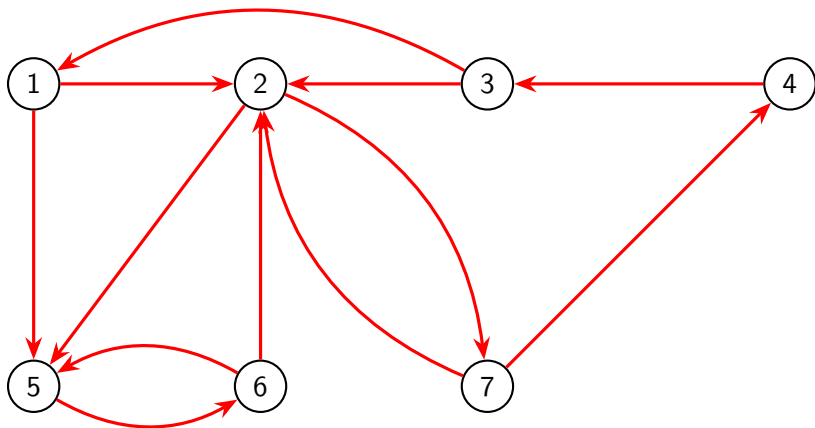


$$\vec{x} = \begin{bmatrix} 2 \\ 4 \\ 2 \\ 2.5 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Based upon this page rank vector, here is a complete ranking of all seven pages from most important to least important:

2, 4, 1, 3, 7, 5, 6

Activity P.16 (~ 10 min) Given the following diagram, use a page rank vector to rank the pages 1 through 7 in order from most important to least important.



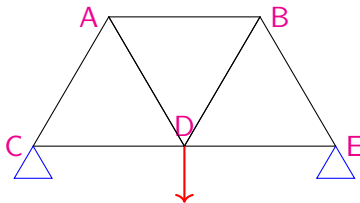
Module P Section 3

Example P.17

In engineering, a **truss** is a structure designed from several beams of material called **struts**, assembled to behave as a single object.



Activity P.18 (~ 5 min) Consider the representation of a simple truss pictured below. All of the seven struts are of equal length, affixed to two anchor points applying a normal force to nodes C and E , and with a $10000N$ load applied to the node given by D .

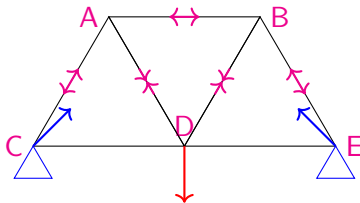


Which of the following must hold for the truss to be stable?

- a) All of the struts will experience compression.
- b) All of the struts will experience tension.
- c) Some of the struts will be compressed, but others will be tensioned.

Observation P.19

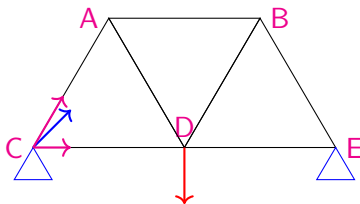
Since the forces must balance at each node for the truss to be stable, some of the struts will be compressed, while others will be tensioned.



By finding vector equations that must hold at each node, we may determine many of the forces at play.

Remark P.20

For example, at the bottom left node there are 3 forces acting.

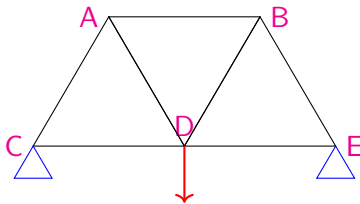


Let \vec{F}_{CA} be the force on C given by the compression/tension of the strut CA , let \vec{F}_{CD} be defined similarly, and let \vec{N}_C be the normal force of the anchor point on C .

For the truss to be stable, we must have

$$\vec{F}_{CA} + \vec{F}_{CD} + \vec{N}_C = \vec{0}.$$

Activity P.21 (~ 10 min) Using the conventions of the previous slide, and where \vec{L} represents the load vector on node D , find four more vector equations that must be satisfied for each of the other four nodes of the truss.



$A : ?$

$B : ?$

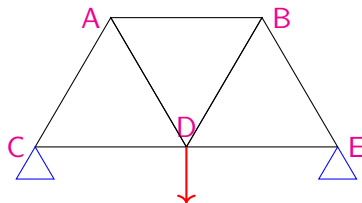
$$C : \vec{F}_{CA} + \vec{F}_{CD} + \vec{N}_C = \vec{0}$$

$D : ?$

$E : ?$

Remark P.22

The five vector equations may be written as follows.



$$A : \vec{F}_{AC} + \vec{F}_{AD} + \vec{F}_{AB} = \vec{0}$$

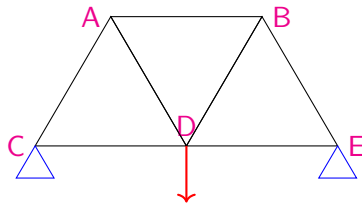
$$B : \vec{F}_{BA} + \vec{F}_{BD} + \vec{F}_{BE} = \vec{0}$$

$$C : \vec{F}_{CA} + \vec{F}_{CD} + \vec{N}_C = \vec{0}$$

$$D : \vec{F}_{DC} + \vec{F}_{DA} + \vec{F}_{DB} + \vec{F}_{DE} + \vec{L} = \vec{0}$$

$$E : \vec{F}_{EB} + \vec{F}_{ED} + \vec{N}_E = \vec{0}$$

Observation P.23

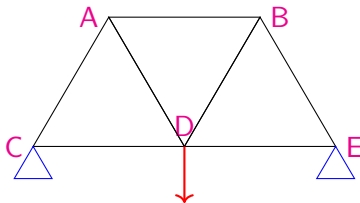


Each vector has a vertical and horizontal component, so it may be treated as a vector in \mathbb{R}^2 . Note that \vec{F}_{CA} must have the same magnitude (but opposite direction) as \vec{F}_{AC} .

$$\vec{F}_{CA} = x \begin{bmatrix} \cos(60^\circ) \\ \sin(60^\circ) \end{bmatrix} = x \begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix}$$

$$\vec{F}_{AC} = x \begin{bmatrix} \cos(-120^\circ) \\ \sin(-120^\circ) \end{bmatrix} = x \begin{bmatrix} -1/2 \\ -\sqrt{3}/2 \end{bmatrix}$$

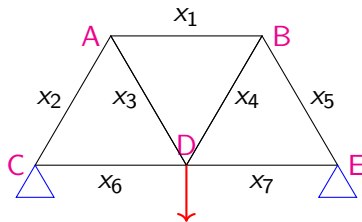
Activity P.24 (~ 5 min) To write a linear system that models the truss under consideration with constant load 10000 newtons, how many scalar variables will be required?



- a) 7: 5 from the nodes, 2 from the anchors
- b) 9: 7 from the struts, 2 from the anchors
- c) 11: 7 from the struts, 4 from the anchors
- d) 12: 7 from the struts, 4 from the anchors, 1 from the load
- e) 13: 5 from the nodes, 7 from the struts, 1 from the load

Observation P.25

Since the angles for each strut are known, one variable may be used to represent each.



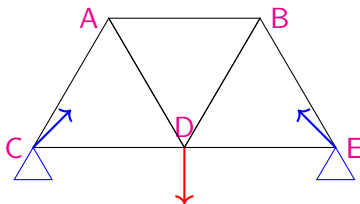
For example:

$$\vec{F}_{AB} = -\vec{F}_{BA} = x_1 \begin{bmatrix} \cos(0) \\ \sin(0) \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\vec{F}_{BE} = -\vec{F}_{EB} = x_5 \begin{bmatrix} \cos(-60^\circ) \\ \sin(-60^\circ) \end{bmatrix} = x_5 \begin{bmatrix} 1/2 \\ -\sqrt{3}/2 \end{bmatrix}$$

Observation P.26

Since the angle of the normal forces for each anchor point are unknown, two variables may be used to represent each.



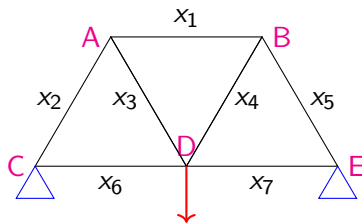
$$\vec{N}_C = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \quad \vec{N}_D = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$$

The load vector is constant.

$$\vec{L} = \begin{bmatrix} 0 \\ -10000 \end{bmatrix}$$

Remark P.27

Each of the five vector equations found previously represent two linear equations: one for the horizontal component and one for the vertical.



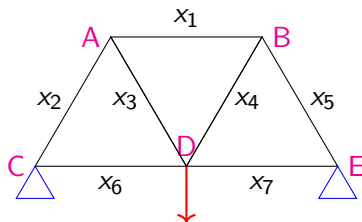
$$C : \vec{F}_{CA} + \vec{F}_{CD} + \vec{N}_C = \vec{0}$$

$$\Leftrightarrow x_2 \begin{bmatrix} \cos(60^\circ) \\ \sin(60^\circ) \end{bmatrix} + x_6 \begin{bmatrix} \cos(0^\circ) \\ \sin(0^\circ) \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Using the approximation $\sqrt{3}/2 \approx 0.866$, we have

$$\Leftrightarrow x_2 \begin{bmatrix} 0.5 \\ 0.866 \end{bmatrix} + x_6 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Activity P.28 (~ 10 min) Expand the vector equation given below using sine and cosine of appropriate angles, then compute each component (approximating $\sqrt{3}/2 \approx 0.866$).



$$D : \vec{F}_{DA} + \vec{F}_{DB} + \vec{F}_{DC} + \vec{F}_{DE} = -\vec{L}$$

$$\Leftrightarrow x_3 \begin{bmatrix} \cos(?) \\ \sin(?) \end{bmatrix} + x_4 \begin{bmatrix} \cos(?) \\ \sin(?) \end{bmatrix} + x_6 \begin{bmatrix} \cos(?) \\ \sin(?) \end{bmatrix} + x_7 \begin{bmatrix} \cos(?) \\ \sin(?) \end{bmatrix} = \begin{bmatrix} ? \\ ? \end{bmatrix}$$

$$\Leftrightarrow x_3 \begin{bmatrix} ? \\ ? \end{bmatrix} + x_4 \begin{bmatrix} ? \\ ? \end{bmatrix} + x_6 \begin{bmatrix} ? \\ ? \end{bmatrix} + x_7 \begin{bmatrix} ? \\ ? \end{bmatrix} = \begin{bmatrix} ? \\ ? \end{bmatrix}$$

Observation P.29

The full augmented matrix given by the ten equations in this linear system is given below, where the elevent columns correspond to $x_1, \dots, x_7, y_1, y_2, z_1, z_2$, and the ten rows correspond to the horizontal and vertical components of the forces acting at A, \dots, E .

$$\left[\begin{array}{cccccccccccc|c} 1 & -0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -0.866 & -0.866 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -0.866 & -0.866 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0.866 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -0.5 & 0.5 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.866 & 0.866 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10000 \\ 0 & 0 & 0 & 0 & -0.5 & 0 & -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.866 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right]$$

Observation P.30

This matrix row-reduces to the following.

$$\sim \left[\begin{array}{cccccccccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -5773.7 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -5773.7 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5773.7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5773.7 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -5773.7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 2886.8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 2886.8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 5000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 5000 \end{array} \right]$$

Observation P.31

Clontz &
Lewis

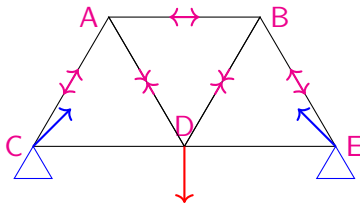
Module P

Section 1

Section 2

Section 3

Section 4



Thus we know the truss must satisfy the following conditions.

$$x_1 = x_2 = x_5 = -5882.4$$

$$x_3 = x_4 = 5882.4$$

$$x_6 = x_7 = 2886.8 + z_1$$

$$y_1 = -z_1$$

$$y_2 = z_2 = 5000$$

In particular, the negative x_1, x_2, x_5 represent tension (forces pointing into the nodes), and the positive x_3, x_4 represent compression (forces pointing out of the nodes). The vertical normal forces $y_2 + z_2$ counteract the 10000 load.

Module P Section 4

Definition P.32

Cryptography is the practice and study of encoding messages so that only the intended receiver can decode them.

For example, the ROT13 cipher both encodes and decodes messages by shifting each letter thirteen places in the alphabet, cycling from *Z* back to *A*. This may be accomplished by converting each letter to a number

$$A \equiv 1, B \equiv 2, \dots, Y \equiv 25, Z \equiv 0$$

and adding 13 (modulo 26):

$$\text{HELLO} \equiv \begin{bmatrix} 8 \\ 5 \\ 12 \\ 12 \\ 15 \end{bmatrix} \xleftrightarrow{\text{ROT}_{13}} \begin{bmatrix} 21 \\ 18 \\ 25 \\ 25 \\ 2 \end{bmatrix} \equiv \text{URYVB}$$

Module P

Section 1

Section 2

Section 3

Section 4

Activity P.33 (*~10 min*) Suppose your instructor saw another student passing a note that said

MFUT DIFBU PO UIF UFTU

How could the instructor decode this message, taking advantage of the fact that THE is one of the most commonly used words in the English language?

Observation P.34

Frequency analysis is a common tool used in breaking **substitution ciphers** that simply substitute letters for other letters. In the message

MFUT DIFBU PO UIF UFTU

the common word THE is encoded as UIF, and the most common letters in the English language E,T match the most common letters used in this message: F,U.

This suggests the following partial decryption:

-ET- -HE-T -- THE TE-T

By considering the context, or the fact that all letters were shifted the same amount, or perhaps by an analysis of other messages sent using the same code, the completed message may be revealed:

LETS CHEAT ON THE TEST

Remark P.35

To defeat naive frequency analysis attacks, one method that may be used is to create a rule that converts groups of letters into new groups of letters, rather than converting single letters individually.

So to send the message

LETS CHEAT ON THE TEST

one might first break it into three-letter pieces.

LET SCH EAT ONT HET EST

Remark P.36

Each piece then may be converted to a Euclidean vector in \mathbb{R}^3 , which may be linearly transformed by multiplying by a matrix A with $\det(A) = 1 = \det(A^{-1})$.

$$\text{For } A = \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix} :$$

$$\text{LET} \equiv \begin{bmatrix} 12 \\ 5 \\ 20 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \\ 20 \end{bmatrix} = \begin{bmatrix} -34 \\ -9 \\ 28 \end{bmatrix}$$

Remark P.37

The resulting vector may be converted back into English letters by adding multiples of 26 to each component to obtain numbers between 0 and 25.

$$\begin{bmatrix} -34 \\ -9 \\ 28 \end{bmatrix} \equiv \begin{bmatrix} -34 + 52 \\ -9 + 26 \\ 28 - 26 \end{bmatrix} = \begin{bmatrix} 18 \\ 17 \\ 2 \end{bmatrix} \equiv \text{RPB}$$

Observation P.38

This process may be done all at once by converting the entire message into a matrix:

$$\begin{aligned} \text{LET SCH } \dots &\equiv \begin{bmatrix} 12 & 19 \\ 5 & 3 & \dots \\ 20 & 8 \end{bmatrix} \\ \rightarrow \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 12 & 19 \\ 5 & 3 & \dots \\ 20 & 8 \end{bmatrix} &= \begin{bmatrix} -34 & 27 \\ -9 & -29 & \dots \\ 28 & -3 \end{bmatrix} \\ &\equiv \begin{bmatrix} 18 & 1 \\ 17 & 23 & \dots \\ 2 & 23 \end{bmatrix} \equiv \text{RQB AVV } \dots \end{aligned}$$

Activity P.39 (~ 10 min) Complete the following encoding of the entire message

given below, using the encoding matrix $A = \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix}$.

$$\text{LET SCH EAT ONT HET EST} \equiv \begin{bmatrix} 12 & 19 & \\ 5 & 3 & \dots \\ 20 & 8 & \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 12 & 19 & \\ 5 & 3 & \dots \\ 20 & 8 & \end{bmatrix} = \begin{bmatrix} -34 & 27 & \\ -9 & -29 & \dots \\ 28 & -3 & \end{bmatrix}$$

$$\equiv \begin{bmatrix} 18 & 1 & \\ 17 & 23 & \dots \\ 2 & 23 & \end{bmatrix} \equiv \text{RQB AWW ESI ILY FYF UII}$$

Activity P.40 (~ 10 min) Reverse this process by using the decoding matrix,

$$A^{-1} = \begin{bmatrix} 6 & 4 & 9 \\ 4 & 3 & 6 \\ 3 & 2 & 5 \end{bmatrix}.$$

$$\text{RQB AWW ESI ILY FYF UUI} \equiv \begin{bmatrix} 18 & 1 & \\ 17 & 23 & \dots \\ 2 & 23 & \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 6 & 4 & 9 \\ 4 & 3 & 6 \\ 3 & 2 & 5 \end{bmatrix} \begin{bmatrix} 18 & 1 & \\ 17 & 23 & \dots \\ 2 & 23 & \end{bmatrix} = \begin{bmatrix} 194 & 305 & \\ 135 & 211 & \dots \\ 98 & 164 & \end{bmatrix}$$

$$\equiv \begin{bmatrix} 12 & 19 & \\ 5 & 3 & \dots \\ 20 & 8 & \end{bmatrix} \equiv \text{LET SCH EAT ONT HET EST}$$