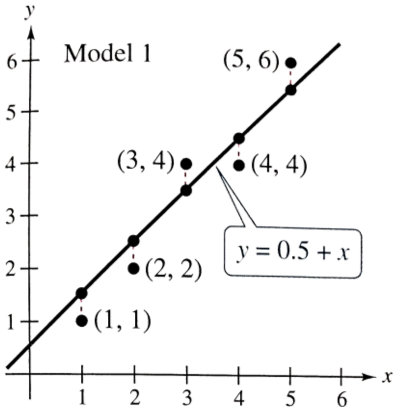
2.6 Applications of Matrix Operations

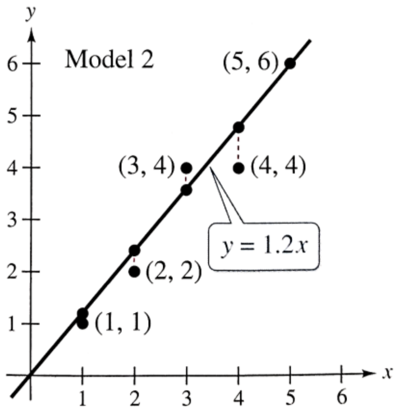
<u>Least Squares Regression Analysis</u>

Consider the points (1,1), (2,2), (3,4), (4,4), (5,6) in the xy-plane. We want to determine a line that best "fits" these points, i.e. that comes as close as possible to passing through them.
Let's try the following two linear function models:

$f(x) = 0.5 + x$ $\qquad\qquad\qquad\qquad$ $f(x) = 1.2x$



Model 1: $f(x) = 0.5 + x$				*Model 2:* $f(x) = 1.2x$			
x_i	y_i	$f(x_i)$	$[y_i - f(x_i)]^2$	x_i	y_i	$f(x_i)$	$[y_i - f(x_i)]^2$
1	1	1.5	$(-0.5)^2$	1	1	1.2	$(-0.2)^2$
2	2	2.5	$(-0.5)^2$	2	2	2.4	$(-0.4)^2$
3	4	3.5	$(+0.5)^2$	3	4	3.6	$(+0.4)^2$
4	4	4.5	$(-0.5)^2$	4	4	4.8	$(-0.8)^2$
5	6	5.5	$(+0.5)^2$	5	6	6.0	$(0.0)^2$
Sum			1.25	Sum			1.00



To measure the accuracy of these models, we calculate the sum of "squared error" $\left(y_i - f(x_i)\right)^2$ between the y-coordinates y_i of the given points and the function values $f(x_i)$ at the corresponding x-coordinates x_i of the points.
We see that model 2: $f(x) = 1.2x$ better fits the points, because it has a sum of squared error that is smaller than model 1: $f(x) = 0.5 + x$. (But, we'll see that $f(x) = 1.2x$ isn't the best fit.)

In general, consider n points $(x_1, y_1), \dots, (x_n, y_n)$ on the xy-plane. We want to find a linear function $f(x) = a_0 + a_1 x$ that best fits these points. Let $e_i = y_i - f(x_i)$ be the error between their y-coordinates y_i and the function values $f(x_i)$ at their x-coordinates, for $i = 1, \dots, n$.
This gives a linear system:

$$y_1 = f(x_1) + e_1 = (a_0 + a_1 x_1) + e_1$$
$$\vdots$$
$$y_n = f(x_n) + e_n = (a_0 + a_1 x_n) + e_n$$

which is expressed in matrix form as $Y = XA + E$, where:

$$Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \qquad X = \begin{pmatrix} 1 & x_1 \\ \vdots & \vdots \\ 1 & x_n \end{pmatrix}, \qquad A = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}, \qquad E = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

The linear function that best fits the given points is the one that minimizes the sum of squared error:

$$E^T E = \sum_{i=1}^{n} (e_i)^2 = \left(y_1 - f(x_1)\right)^2 + \cdots + \left(y_n - f(x_n)\right)^2$$

It turns out that the solution A for the coefficients of the linear function f is given by the formula:

$$A = (X^T X)^{-1} X^T Y$$

Then $f(x) = a_0 + a_1 x$ is called the *least squares regression line* for the given points.

Example. Let's find the least squares regression line $f(x) = a_0 + a_1 x$ for the points (1,1), (2,2), (3,4), (4,4), (5,6).

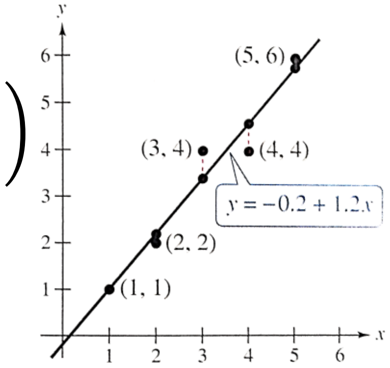
Let $X = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 5 \end{pmatrix}$, $Y = \begin{pmatrix} 1 \\ 2 \\ 4 \\ 4 \\ 6 \end{pmatrix}$, and $A = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$. Then $X^T X = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 15 \\ 15 & 55 \end{pmatrix}$,

$$(X^T X)^{-1} = \frac{1}{50}\begin{pmatrix} 55 & -15 \\ -15 & 5 \end{pmatrix}, \qquad X^T Y = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 4 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 17 \\ 63 \end{pmatrix}$$

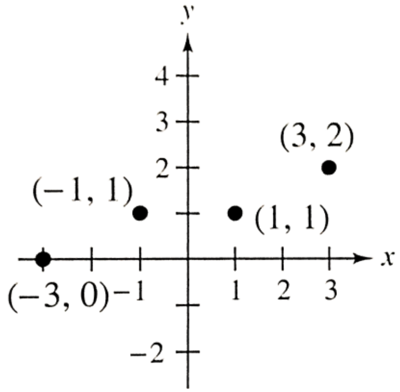
So, we get:

$$A = (X^T X)^{-1} X^T Y = \frac{1}{50}\begin{pmatrix} 55 & -15 \\ -15 & 5 \end{pmatrix}\begin{pmatrix} 17 \\ 63 \end{pmatrix} = \frac{1}{50}\begin{pmatrix} -10 \\ 60 \end{pmatrix} = \begin{pmatrix} -1/5 \\ 6/5 \end{pmatrix}$$

Therefore, the least squares regression line is $f(x) = -\frac{1}{5} + \frac{6}{5}x$.



Exercise. Find the least squares regression line $f(x) = a_0 + a_1 x$ for the following points:



Cryptography

We can use a matrix and its inverse to encrypt and decrypt messages as follows. Assign a blank space and each letter of the alphabet to a number a_i:

$$\_\_ = a_0, \mathrm{A} = a_1, \mathrm{B} = a_2, \mathrm{C} = a_3, \ldots, \mathrm{X} = a_{24}, \mathrm{Y} = a_{25}, \mathrm{Z} = a_{26}$$

Choose a $n \times n$ invertible matrix A. Write a word message and convert each letter to a number according to the assignment above (using the blank space to separate words). Partition the numerical message into $1 \times n$ row matrices. Then:

- Multiply each $1 \times n$ row matrix on the right by A to form encoded $1 \times n$ row matrices (encryption).
- Multiply each encoded $1 \times n$ row matrix on the right by A^{-1} to get the decoded numerical message (decryption).

$$\vec{x}A = \vec{y} \text{ (encryption)} \Leftrightarrow \vec{x} = \vec{y}A^{-1} \text{ (decryption)}$$

In this section, we will use the following letter assignment for simplicity:

$$\_\_ = 0, \mathrm{A} = 1, \mathrm{B} = 2, \mathrm{C} = 3, \ldots, \mathrm{X} = 24, \mathrm{Y} = 25, \mathrm{Z} = 26$$

Example. Use $A = \begin{pmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{pmatrix}$ to encrypt and decrypt the word message:

MEET ME AT HOME

Convert each letter to a number: 13 5 5 20 0 13 5 0 1 20 0 8 15 13 5

Partition the numerical message into 1×3 row matrices:

$$(13 \quad 5 \quad 5)\,(20 \quad 0 \quad 13)\,(5 \quad 0 \quad 1)\,(20 \quad 0 \quad 8)\,(15 \quad 13 \quad 5)$$

Multiply each of these on the right by A:

$$(13 \quad 5 \quad 5)\begin{pmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{pmatrix} = (13 \quad -26 \quad 21)$$

$$(20 \quad 0 \quad 13)\begin{pmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{pmatrix} = (33 \quad -53 \quad -12)$$

$$(5 \quad 0 \quad 1)\begin{pmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{pmatrix} = (6 \quad -11 \quad 6)$$

$$\begin{pmatrix}20 & 0 & 8\end{pmatrix}\begin{pmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{pmatrix} = \begin{pmatrix}28 & -48 & 8\end{pmatrix}$$

$$\begin{pmatrix}15 & 13 & 5\end{pmatrix}\begin{pmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{pmatrix} = \begin{pmatrix}7 & -22 & 49\end{pmatrix}$$

Altogether, these form the encrypted message:

$$\begin{pmatrix}13 & -26 & 21\end{pmatrix}\begin{pmatrix}33 & -53 & -12\end{pmatrix}\begin{pmatrix}6 & -11 & 6\end{pmatrix}\begin{pmatrix}28 & -48 & 8\end{pmatrix}\begin{pmatrix}7 & -22 & 49\end{pmatrix}$$

Note: We can remove the matrix partitions to express this as:

$$13\ \ -26\ \ 21\ \ 33\ \ -53\ \ -12\ \ 6\ \ -11\ \ 6\ \ 28\ \ -48\ \ 8\ \ 7\ \ -22\ \ 49$$

To decrypt this message, we need the inverse of A:

$$(A|I_3) = \left(\begin{array}{ccc|ccc}1 & -2 & 2 & 1 & 0 & 0\\ -1 & 1 & 3 & 0 & 1 & 0\\ 1 & -1 & -4 & 0 & 0 & 1\end{array}\right) \begin{array}{c} R_1 + R_2 \to R_2 \\ -R_1 + R_3 \to R_3\end{array} \left(\begin{array}{ccc|ccc}1 & -2 & 2 & 1 & 0 & 0\\ 0 & -1 & 5 & 1 & 1 & 0\\ 0 & 1 & -6 & -1 & 0 & 1\end{array}\right) \begin{array}{c} 2R_3 + R_1 \to R_1 \\ R_3 + R_2 \to R_2\end{array}$$

$$\left(\begin{array}{ccc|ccc}1 & 0 & -10 & -1 & 0 & 2\\ 0 & 0 & -1 & 0 & 1 & 1\\ 0 & 1 & -6 & -1 & 0 & 1\end{array}\right) - R_2 \to R_2 \left(\begin{array}{ccc|ccc}1 & 0 & -10 & -1 & 0 & 2\\ 0 & 0 & 1 & 0 & -1 & -1\\ 0 & 1 & -6 & -1 & 0 & 1\end{array}\right) R_2 \leftrightarrow R_3$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -10 & -1 & 0 & 2 \\ 0 & 1 & -6 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & -1 \end{array}\right) \begin{array}{c} 10R_3 + R_1 \to R_1 \\ 6R_3 + R_2 \to R_2 \end{array} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & -10 & -8 \\ 0 & 1 & 0 & -1 & -6 & -5 \\ 0 & 0 & 1 & 0 & -1 & -1 \end{array}\right) = (I_3|A^{-1})$$

Then we multiply each encoded 1×3 matrix on the right by A^{-1}:

$$\begin{pmatrix} 13 & -26 & 21 \end{pmatrix} \begin{pmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 13 & 5 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 33 & -53 & -12 \end{pmatrix} \begin{pmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 20 & 0 & 13 \end{pmatrix}$$

$$\begin{pmatrix} 6 & -11 & 6 \end{pmatrix} \begin{pmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 28 & -48 & 8 \end{pmatrix} \begin{pmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 20 & 0 & 8 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -22 & 49 \end{pmatrix} \begin{pmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 15 & 13 & 5 \end{pmatrix}$$

This gives back the original message:

$$(13 \quad 5 \quad 5)\,(20 \quad 0 \quad 13)\,(5 \quad 0 \quad 1)\,(20 \quad 0 \quad 8)\,(15 \quad 13 \quad 5)$$

$$13 \;\; 5 \;\; 5 \;\; 20 \;\; 0 \;\; 13 \;\; 5 \;\; 0 \;\; 1 \;\; 20 \;\; 0 \;\; 8 \;\; 15 \;\; 13 \;\; 5$$

$$\text{MEET ME AT HOME}$$

Exercise. Decode the message 22 39 20 40 78 135 20 40 using the encoding matrix:

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

Practice Problems:

Use A^{-1} to decode the message.

3. $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$

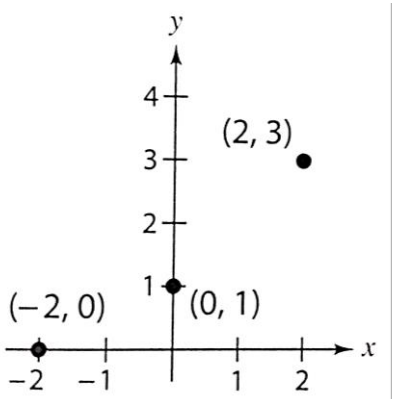
11 21 64 112 25 50 29 53 23 46 40 75 55 92

5. $A = \begin{pmatrix} 1 & 2 & 2 \\ 3 & 7 & 9 \\ -1 & -4 & -7 \end{pmatrix}$

13 19 10 -1 -33 -77 3 -2 -14 4 1 -9 -5 -25 -47 4 1 -9

Find the least squares regression line for the given points.

15.



17.