31/01/23 Network Security

Fig 2.15 - Using extended Euclidean algorithm to find multiplicative inverse → Pg - 37

Example - 2.25

Find the multiplicative inverse of 11 in Z_{26}

$11^{-1} \bmod 26$

Solu :-

$n_1 = 26, \quad n_2 = 11,$

q	n_1	n_2	n	t_1	t_2	t
	26	11	-4	0	1	-2
2						

Ans - -7 or 19

Ex - 2.26

Ex - 2.27

Find the inverse of 12 in Z_{26}

Solu :-

The gcd (26, 12) is 2 ≠ 1. Do not exist

Pg-39 Addition and Multiplication Tables

Pg-65

Multiplicative Ciphers

Example-3.7

Example-3.8

26 7 3 5 01

Pg-66 → Affine ciphers

Example-3.10

Example-3.11

Example-3.12

$7^{-1} \bmod 26$

$7 \times 15 = 105$

$7 \times 15 = 105$; $(7 + 2 \times 7^{-1}) \bmod 26$ $26 \times 4 = 104$ $\frac{1}{}$

$= 1.$

$26 \times 4 = 104.$

01/02/23 Network Security

Matrix

Example - 2.34

Fig - 2.26

$21^{-1} \bmod 26 = 5$

→ 2.4

• Linear Congruence

$ax \equiv b \pmod n$

Example - 2.35

$10x \equiv 2 \pmod{15}$

$\gcd(10, 15) = 5$, since 5 doesnot divide 2,

we have no solu;

Example - 2.36 Ans. → 6 and 15

$14x \equiv 12 \pmod{18}$

$7x \equiv 6 \pmod 9$ $(6 \times 4 \bmod) = 6$

$\Rightarrow x \equiv 6(7^{-1}) \pmod 9 \Rightarrow 6$

$x_i = x_0 + i \times (n/d)$

6×4

$= 6 + 1 \times (18/2)$

$= 15$

$\therefore x_0 = 6$

$x_1 = 15$

Fig-2.27

Example - 2.38

Example - 3.12

Hill cipher is polyalphabetic - Pg-75

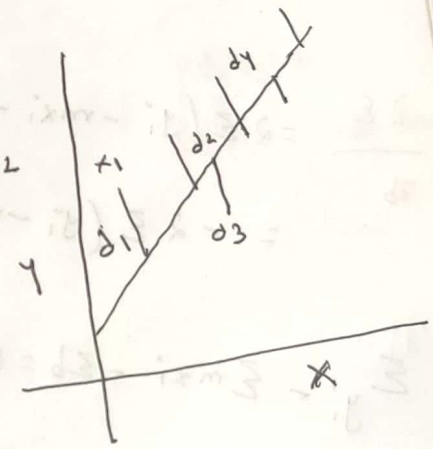
Fig-3.15

06/02/23

ML

- Linear Regression

$E = d_1^2 + d_2^2 + d_3^2 + d_4^2 + \cdots d_n^2$



on the basis of input, we will predict the output

- MAE → Maximum Absolute Error
- MSE

$E = |y_1 - \hat{y}_1| + |y_2 - \hat{y}_2| + \cdots$

$y = mx + b$

$\hat{y}$ → predicted value

↳ M

$$d = y_i - \hat{y}_i$$

$$E = \sum_{i=1}^{n} (y_i - \hat{y}_i)^2$$

$$E \sum_{i=1} (y_i - mx_i - b)^2$$

$$b = \bar{y} - m\bar{x}$$

$$m = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sum_{i=1}^{n} (x_i - \bar{x})^2}$$

$$\frac{\partial \varepsilon}{\partial b} = 2 \varepsilon (y_i - mx_i - b) \times -1$$

$$= -2 \varepsilon (y_i - mx_i - b)$$

$$\varepsilon y_i - \varepsilon mx_i - \varepsilon b = 0$$

$$\frac{\sum y_i}{n} - \frac{\sum m x_i}{n} - \frac{\sum b}{n} = 0$$

$$\bar{y} - m\bar{x} = b$$

$$\frac{\partial E}{\partial m} = 2(y_i - mx_i - b) \times (-x_i)$$

$$= \sum 2(y_i - mx_i - \bar{y} + m\bar{x})(-x_i + \bar{x})$$

$$E = \sum (y_i - mx_i - \bar{y} + m\bar{x})^2$$

$$\sum (y_i - mx_i - \bar{y} + m\bar{x})(\bar{x} - x_i) = 0$$

$$\sum (y_i - \sum m x_i - \sum \bar{y} + \sum m\bar{x})\bar{x} - x_i) = 0$$

$$\sum (y_i - m x_i^2 - \bar{y} + m\bar{x})(x_i - \bar{x}) = 0$$

$$\sum [(y_i - \bar{y}) - m(x_i - \bar{x})(x_i - \bar{x})]$$

$$\sum (y_i - \bar{y})(x_i - \bar{x}) - m(x_i - \bar{x})^2 = 0$$

$$\sum (y_i - \bar{y})(x_i - \bar{x}) = m \sum (x_i - \bar{x})^2$$

$$m = \frac{\sum y_i - \bar{y})(x_i - \bar{x})}{\sum (x_i - \bar{x})^2}$$

MAE

MSE

RMSE

R2 Score

Adjusted R2 Score

R2 Score $= 1 - \frac{SSR}{SSM}$

$$= 1 - \frac{\sum_{i=1}^{n} (y_i - \hat{y}_{i,R})^2}{\sum_{i=1}^{n} (y_i - \hat{y}_{i,m})^2}$$

6/02/23

Network Security

- Finite Field (Pg-106)

Figure -4.7

GF(p^n) Fields

Example -4.14

Example -4.15

irr(Pg) → list of irreducible polynomials.

Example -4.17

Example -4.18

Example -4.19

Example -4.24

Multiplication Using Computer

Table -4.9

Example -4.22

Example -4.23

Z = 15

C.W 7/01/23

R

Adj

Simple

C.W
7/01/23

Machine Learning

R Squared R^2

Adjusted R^2 Score $= 1 - \left[\frac{(1 - R_2)(n-1)}{n-1-k} \right]$

n → no. of rows

k → no. of colo.

Simple linear Regression -

$$b = \bar{y} - m\bar{x}$$

$$m = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sum_{i=1}^{n} (x_i - \bar{x})^2}$$

Linear Regression

SLR — MLR — Polynomial

$$E = \sum_{i=1}^{n} (y_i - \hat{y}_i)^2$$

$$y = \beta_0 + \beta_1 x \qquad y = mx + b$$

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3$$

$$y = \beta_0 + \sum_{i=1}^{n} \beta_i x_i \qquad (y = mx + b)$$

$$\begin{bmatrix} \hat{y}_1 \\ \hat{y}_2 \\ \hat{y}_3 \\ \hat{y}_n \end{bmatrix} = \begin{bmatrix} \beta_0 & \beta_1 x_{11} & \beta_2 x_{12} + \beta_3 x_{13} & \cdots & \beta_m x_{1m} \\ \beta_0 & \beta_1 x_{21} & \beta_2 x_{22} + \beta_3 x_{23} & \cdots & \beta_m x_{2m} \\ \beta_0 & & & & \\ \vdots & & & & \\ \beta_0 & \beta_1 x_{n1} & \cdots & & \beta_m x_{nm} \end{bmatrix}$$

$x_1 \mid x_2 \; x_3 \; \cdots \; x_m$

$$\begin{bmatrix} \hat{y}_1 \\ \hat{y}_2 \\ \hat{y}_3 \\ \hat{y}_n \end{bmatrix} = \begin{bmatrix} 1 & x_{11} & x_{12} & \cdots & x_{1m} \\ 1 & x_{21} & x_{22} & \cdots & x_{2m} \\ 1 & 1 & & & \\ 1 & 1 & & & \\ 1 & x_{n1} & x_{n1} & \cdots & x_{nm} \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{bmatrix}$$

$$\hat{Y}_{n\times 1} = X_{n\times(m+1)} \; \beta_{(m+1)\times 1}$$

$$E = \sum_{i=1}^{n} (y_i - \hat{y}_i)^2 = e^T e$$

$$e = \begin{bmatrix} y_1 - \hat{y}_1 \\ y_2 - \hat{y}_2 \\ \vdots \\ y_n - \hat{y}_n \end{bmatrix}$$

$\therefore e^T$

e^T

$\therefore e^T.e = [(y_1 - \hat{y}_1).(y_2 - \hat{y}_2) \longrightarrow (y_n - \hat{y}_n)]$

$\times \begin{bmatrix} y_1 - \hat{y}_1 \\ y_2 - \hat{y}_2 \\ \vdots \\ y_n - \hat{y}_n \end{bmatrix}$

$= E$

$e^T.e = (Y - \hat{Y})^T (Y - \hat{Y})$

$(AB)^T = B^T.A^T$

$= (Y^T - \hat{Y}^T)(Y - \hat{Y})$

$= [Y^T - (XB)^T][Y - XB]$

$= Y^T Y - Y^T XB - Y(XB)^T Y + (XB)^T XB$

Now,

$Y^T XB = Y(XB)^T Y$ $\quad Y = A, \quad XB = B$

$A^T B = B^T A$ — ①

$(A^T B)^T = B^T A$

$CC^T = C$

$= Y^T Y - 2Y^T XB + (XB)^T XB$

$$E = Y^T Y - 2Y^T XB + B^T X^T XB$$

Scanned with CamScanner

$$\frac{dE}{dB} = -2Y^T X + \frac{d}{dB}\left(B^T X^T X B\right)$$

$$= -2Y^T X + 2X^T X B^T = 0$$

$$2X^T X B^T = 2Y^T X$$

$$B^T = \frac{Y^T X}{X^T X}$$

$$\Rightarrow B^T = Y^T X \left(X^T X\right)^{-1}$$

$$\Rightarrow B = \left[Y^T X \left(X^T X\right)^{-1}\right]^T$$

$$\therefore B = \left[\left(X^T X\right)^{-1}\right]^T X^T Y$$

$$J = A^T X A$$

$$\frac{dy}{dA} = 2XA$$

Scanned with CamScanner

#101123

Network Security

Table 4.10 –

Example – 4.25 (Practice)

- DES → Data Encription standard.
- AES →

$2^4 - 2 \Rightarrow 2^4 - 2$
$= 14$

Example - 4.25

$g^0 = 0001$

$g^1 = 0010$

$g^2 = 0100$

$g^3 = 1000$

$g^4 = 0010$

$g^5 = g_{4} + 1$

$g^{10} = g(g^3 + g)$

$= g^2 + g + 1$

$= 0100 + 0010 + 1$

1000
0100
1100

$(g^{10} =$

$g_{11} = g(g^{10}) = g(g^2 + g + 1) = g^3 + g^2 + 1$

$= (1110)$

$g_{12} = 1111$

$g_{14} = 1001$

0100
0001
0101
$+1$

Example - 4.2

$(\frac{5}{5}) \% 7 = (5*5) \bmod 7 = 1$

$(5*5) \bmod 7 = 4$

Data Encryption Standard (DES)

Pg - 153

Figure - 6.2

Table - 6.1

7/02/23

NLP

Language Modeling → N grams Modeling

Probabilistic Language Models —

- Raw Bigram Counts

out of 9222 sentences

8/02/23

ML

Topic → Gradient decent

8/02/23

Fig - 6.2

Initial Permu

1 2 3

5 - -

- The - bit

the 8 - b

- The bits

into th

the bits

(8 - i) +

- The

in oc

output

go

8/02/23

Network Security

Fig - 6.2

DES —

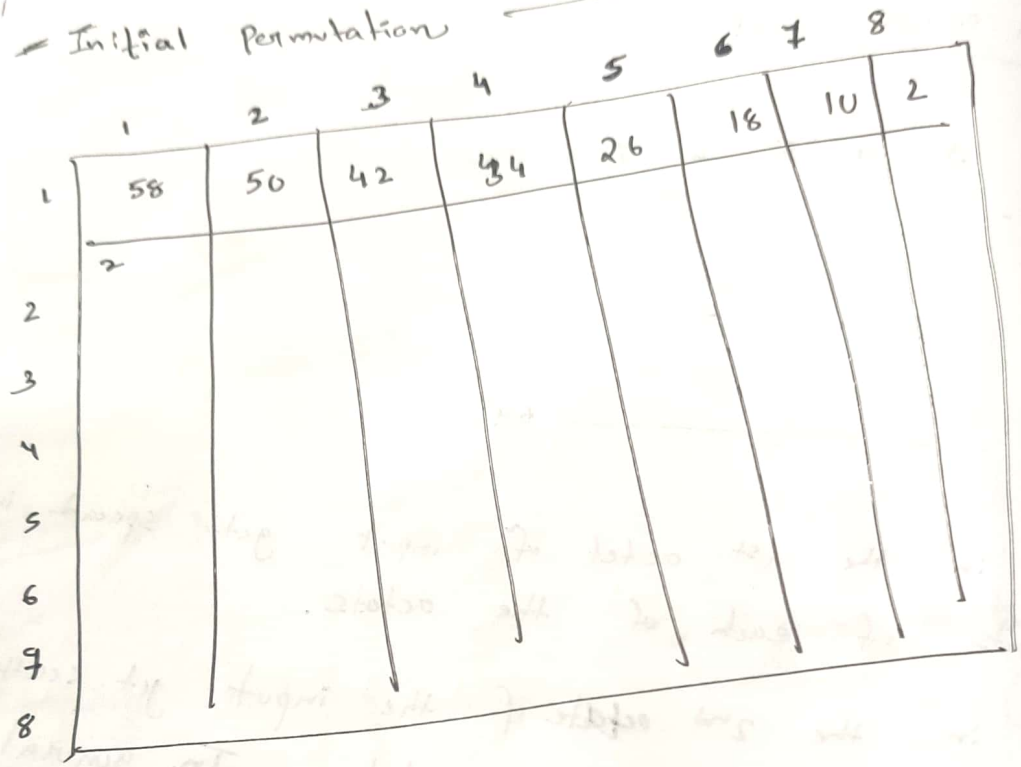
Initial Permutation - IP

1 2 3 4 5 6 7 8

- The 1-bit in the 1st octet of input get spread into the 8-bits of each of the octate.
- The bits in the 2nd octate of the input get scattered into the 7th-bits of the octate. In general, the bits of the ith octate get spread into the $(8-i)+1^{th}$ octate.
- The pattern of the spreading of the 8th bit, in octate i of the input among the output octate is that, even number bits go into octate 1 to 4

, and the add number bits go into octate 5 to 8.

- Initial Permutation



Final permutation

40 08 48 16 56 24 64 32

33 01 41 09 49 17 57 25

Example -6.1

Example -6.2

Example -6.3

• Avalanche

8/02/23

- The

- Na

- Mu

Example -6.1

Example -6.2

Example -6.3

S-box → confusion

P-box → Permutation box

confusion → S-box

diffusion → Transposition.

Avalanche effect

8/02/23

NLP

N-Gram Language Processing

- The Shannon Visualization Method

- Naive Bayes

- Multinomial Naive Bayes Model.

$$P(c) = \frac{P(c|d)}{P(d)}$$

- Naive Bayes classifier

a-2

to-3

(a)

$P(a) = \frac{2}{5}$

$P(c) = \frac{c}{m}$

G.W
13/02/23

NLP

Naive Bayers classifier

$$C_{MAP} = \underset{c \in C}{\operatorname{argmax}} \; P(c|d)$$

MAP is "maximum a posteriori" = most likely class

$$= \underset{c \in C}{\operatorname{argmax}} \; \frac{P(d|c)\,P(c)}{P(d)}$$

Bayes rule

$$= \underset{c \in C}{\operatorname{argmax}} \; P(d|c)\,P(c)$$

Dropping the denominator

$$P(x|y,z) = P(x|z)$$

→ conditional independence Theorem

$$P(x|c) = P(x_1, x_2, x_3 \dots | c)$$

$$= P(x_1|c), P(x_2|c)\,P(x_3|c) \dots P(x_n|c)$$

$$P(x_1, x_2|c) = \frac{P(x_1, x_2, c)}{P(c)} = \frac{P(x_1|x_2,c)\,P(x_2|c)\,P(c)}{P(c)}$$

$$= P(x_1|c)\;P(x_2|c)$$

$\hat{y} \leftarrow \underset{c}{\operatorname{argmax}} \begin{cases} P(w_1|c=0) \cdot P(w_2|c=0) \cdots P(w_n|c=0) P(c=0) \\ P(w_1|c=1) \cdot P(w_2|c=1) \cdots P(w_n|c=1) \end{cases}$

13/02/23

Network Security

AES (Advanced Encryption Standard)

Fig - 7.1

↓

Fig - 7.2

↓

Fig - 7.3

N_n = round → 10, 12, 14

Mehedi → 08 → 03
↓ ↓ ↓ → 04
02 04 07

Figure -

0C 08
04
07
04

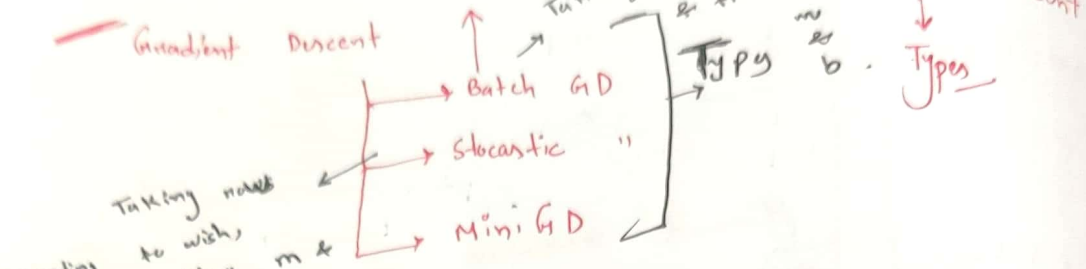
C.W

14/02/23

ML

Linear Regression

Gradient Descent



$$b_{new} = b_{old} - \eta \frac{\partial}{\partial b}$$

$$E = \frac{\sum_{i=0}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sum (x_i - \bar{x})^2}$$

η = Learning rate.

$$m_{new} = m_{old} - \eta \frac{\partial}{\partial m}$$

- Main motive ⇒ Finding valve of m and b.
  ⇒ Reduce error.

Stocastic → Taking a new randomly & approaching to solu. → updating the valves.

→ Finding m & b

↙ ⇒ Useful for big / large data set.

non convex model ⇒ more used in DL

→ it can also switch.

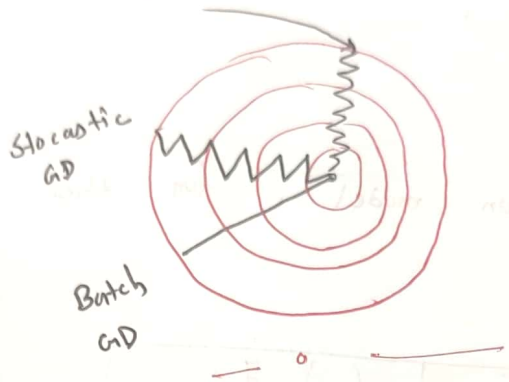
Mini → takes some pts (not all) as i/p

→ it is a batch blw batch & Stocastic GD.

→ we take learning schedule.

→ initially LR will be high, then we will decrease the LR at the end, to get a proper solution.

Mini Batch GD.



Polynomial Regression

x_1	x_2	y

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_1^2 + \beta_3 x_2 + \beta_4 x_2^2 + \beta_5 x_3 + \beta_6 x_3^2$$

- Linear Regression = $y = \beta_0 + \beta_1 x$ or $y = mx + b$
- Multiple " = $\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n$

Regression, for ML → as Internal-1 syllabus → Unit-1 and Unit-2 for UT

- Polynomial Regression = - take degree carefully,
  - take degree, that does not overfit the data
  - if taken more, it will over train the data.

Eqn → $y = \beta_0 + \beta_1 x_1 + \beta_2 x_1^2 + \beta_3 x_1^3 + \cdots$

- underfitting
- overfitting → It will pass through all points.

$$\sum y_i = n\beta_0 + \beta_1 \left(\sum x_i\right) + \beta_2 \sum x_i^2$$

$$\sum y_i x = \beta_0 \sum x_i + \beta_1 \sum x_i^2 + \beta_2 \sum x_i^3 + \cdots$$

$$\sum y_i x^2 = \beta_0 \sum x_i^2 + \beta_1 \sum x_i^3 + \cdots$$

$$\sum y_i x^3 = \beta_0 \sum x_i^3 + \beta_1 \sum x_i^4 + \cdots$$

Find the Quadratic Regression model for the following data —

x	3	4	5	6	7
y	2.5	3.2	3.8	6.5	11.5

$$y = \beta_0 + \beta_1 x + \beta_2 x^2$$

$$y = 12.4285 - 5.512x + 0.76442x^2$$

14/02/23 Network Security AES

03 × 6E

03 = 0000 0011 = x + 1

6E = 0110 1110 = $x^6 + x^5 + x^3 + x^2 + x^1$

Now,

$(x+1)(x^6 + x^5 + x^3 + x^2 + x^1)$

$= x^7 + x^6 + x^4 + x^3 + x^2 + x^6 + x^5 + x^3 + x^2 + x^1$

$= x^7 + x^4 + x^5 + x^1$

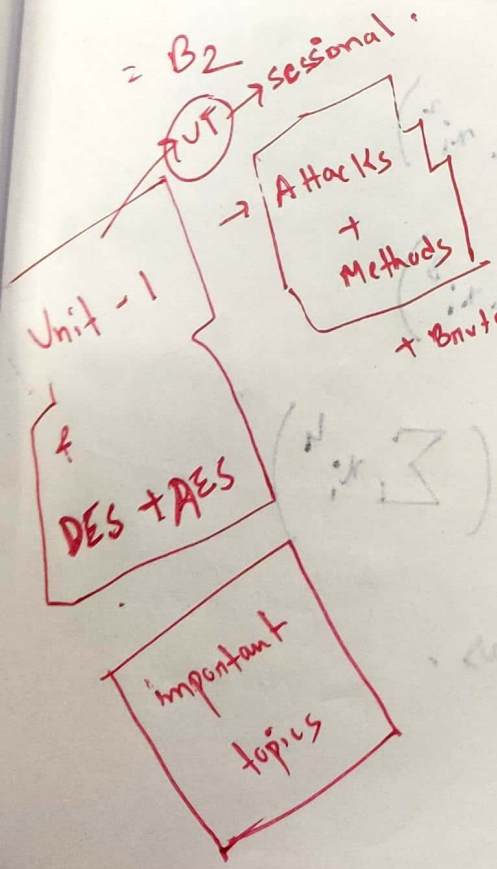
$= x^7 + x^5 + x^4 + x^1$

10110010 ⇒ B2

=

= B2

00010101
10110010
01000110
00100110



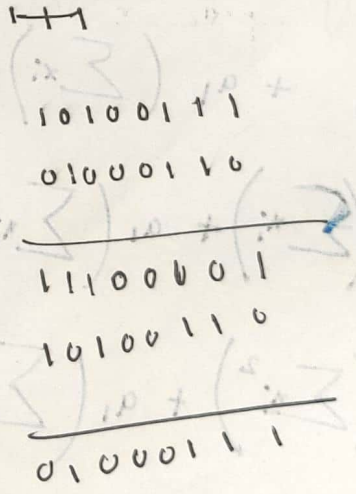
+ Brute force all attacks

+ cypher text attacks

Textbook

+ Extended ⇒ 47

=



Solve

Quadratic Polynomial Regression

Data set –

x	3	4	5	6	7
y	2.5	3.2	3.8	6.5	11.5

Solu:–

Let the quadratic polynomial regression model be

$$y = a_0 + a_1 x + a_2 x^2$$

where

x = independent variable

y = dependent variable

We can calculate y, if a_0, a_1 & a_2 are known.

- The values of a_0, a_1 and a_2 are calculated using the following system of equations

$$\sum y_i = n a_0 + a_1 \left(\sum x_i\right) + a_2 \left(\sum x_i^2\right)$$

$$\sum y_i x_i = a_0 \left(\sum x_i\right) + a_1 \left(\sum x_i^2\right) + a_2 \sum x_i^3$$

$$\sum y_i x_i^2 = a_0 \left(\sum x_i^2\right) + a_1 \left(\sum x_i^3\right) + a_2 \left(\sum x_i^4\right)$$

n = no. of data points given to us.

$\therefore n = 5$ (in this case)

x	y	x^2	x^3	x^4	yx	yx^2
3	2.5	9	27	81	7.5	22.5
4	3.2	16	64	256	12.8	51.2
5	3.8	25	125	625	19	95
6	6.5	36	216	1296	39	234
7	11.5	49	343	2401	80.5	563.5
Σ	25	27.5	135	775	4659	158.8	966.2

Using the given data we have —

$$27.5 = 5a_0 + 25a_1 + 135a_2$$

$$158.8 = 25a_0 + 135a_1 + 775a_2$$

$$966.2 = 135a_0 + 775a_1 + 4659a_2$$

After solving these equations we have

$$a_0 = 12.42857142$$

$$a_1 = -5.5128571$$

$$a_2 = 0.7642857$$