1 Introduction

This document contains detailed notes related to the slides.

2 Polynomials

This is the general form of a polynomial of degree k.

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_kx^k$$

Or, more generally...

$$f(x) = \sum_{k=0}^{n} a_kx^k$$

3 Curve Fitting

A polynomial of degree n may be uniquely defined given $n+1$ points on the line. An infinite number of lines will intersect only n points. These lines may be found by solving the simultaneous equations for the points provided.
These are the points used in the slides.

3.1 Linear Polynomial

A first degree polynomial is represented by the equation

$$f(x) = ax + b$$

Given our secret 42 and a random $a = 4$ we can represent a straight line

$$f(x) = 4x + 42 \tag{1}$$

Suppose we have a single point on this line, say $P = (-17, -26)$, we want to want to find an equation that describes all possible lines that include this point. Given point P, we solve for b:

$$\begin{aligned} -26 &= -17a + b \\ b &= -26 + 17a \end{aligned} \tag{2}$$

Now we may substitute b from equation 2 into equation 1.

$$f_a(x) = ax - 26 + 17a$$
$$f_a(x) = a(x + 17) - 26 \tag{3}$$

Equation 3 describes all lines passing through point $P = (-17, -26)$.

3.2 Quadratic Polynomial

A second degree, or quadratic, polynomial is represented as

$$f(x) = ax^2 + bx + c \tag{4}$$

Given a secret $S = 42$, we can choose random values for a and b. Suppose we choose $a = 7$ and $b = 3$. We may then write

$$f(x) = 7x^2 + 3x + 42 \tag{5}$$

Three points must be given to describe a quadratic equation. Given only two points, we want to find all quadratic curves that pass through the two given points.

Suppose we have points $P_1 = (2, 76)$ and $P_2 = (5, 232)$ discovered by choosing two x values randomly and solving equation 5 for $f(x)$. We may find the equation describing all curves passing through P_1 and P_2 by solving the system of equations as we did in the case of the linear polynomial.

Substitutine P_1 and P_2 into equation 4 we can write

$$f(2) = 4a + 2b + c$$
$$76 = 4a + 2b + c$$
$$c = -4a - 2b + 76 \tag{6}$$

and

$$f(5) = 25a + 5b + c$$
$$232 = 25a + 5b + c$$
$$c = -25a - 5b + 232 \tag{7}$$

Since we know equations 6 and 7 are equal, we can solve for b in terms of a as follows:

$$\begin{aligned}
-4a - 2b + 76 &= -25a - 5b + 232 \\
5b - 2b &= 232 - 76 + 4a - 25a \\
3b &= -21a + 156 \\
b &= -7a + 52 \qquad (8)
\end{aligned}$$

We can now substitute equation 8 into equation 6 to write:

$$\begin{aligned}
c &= -4a - 2(-7a + 52) + 76 \\
&= -4a + 14a - 104 + 76 \\
c &= 10a - 28 \qquad (9)
\end{aligned}$$

Now that we have solved for both b and c in terms of a, we may rewrite equation 4 as follows:

$$\begin{aligned}
f_a(x) &= ax^2 + (-7a + 52)x + 10a - 28 \\
&= ax^2 + -7ax + 52x + 10a - 28 \\
f_a(x) &= a(x^2 - 7x + 10) + 52x - 28 \qquad (10)
\end{aligned}$$

Equation 10 is the set of quadratic curves that pass through points $P_1 = (2, 76)$ and $P_2 = (5, 232)$.

3.3 Cubic Polynomial

A third degree, or cubic, polynomial is represented as:

$$f(x) = ax^3 + bx^2 + cx + d \qquad (11)$$

As before, our secret $S = 42$. We then select random values for a, b, and c. Suppose we have $a = 1$, $b = 3$, and $c = 13$. We may write:

$$f(x) = x^3 + 3x^2 + 13x + 42 \qquad (12)$$

Four points are required to identify a specific cubic equation. Suppose we have three points $P_1 = (-6, -144)$, $P_2 = (1, 59)$, $P_3 = (4, 206)$. We can find the set of cubic polynomials that contains each of P_1, P_2, and P_3 by solving the system of equations as before. We can write:

$$\begin{aligned}
f(-6) &= a(-6)^3 + b(-6)^2 + c(-6) + d \\
-144 &= -216a + 36b - 6c + d \\
d &= 216a - 36b + 6c - 144 \qquad (13)
\end{aligned}$$

$$\begin{aligned} f(1) &= a + b + c + d \\ 59 &= a + b + c + d \\ d &= -a - b - c + 59 \end{aligned} \tag{14}$$

$$\begin{aligned} f(4) &= 4^3 a + 4^2 b + 4c + d \\ 206 &= 64a + 16b + 4c + d \\ d &= -64a - 16b - 4c + 206 \end{aligned} \tag{15}$$

We may now represent c in terms of a and b by simplifying the equality of equations 13 and 14:

$$\begin{aligned} 216a - 36b + 6c - 144 &= -a - b - c + 59 \\ 7c &= -217a + 35b + 203 \\ c &= -31a + 5b + 29 \end{aligned} \tag{16}$$

And now repeat for equations 14 and 15:

$$\begin{aligned} -a - b - c + 59 &= -64a - 16b - 4c + 206 \\ 3c &= -63a - 15b + 147 \\ c &= -21a - 5b + 49 \end{aligned} \tag{17}$$

Repeating once again to solve for b by simplifying the equality represented by the equations 16 and 17:

$$\begin{aligned} -31a + 5b + 29 &= -21a - 5b + 49 \\ 10b &= 10a + 20 \\ b &= a + 2 \end{aligned} \tag{18}$$

At this point, we may substitute equations 18, 16, and 14 into the general cubic polynomial formula 11. Terms with b and c must be replaced as needed in equations 16 and 14 so that we have an equation in terms of a and x only. The algebra is simple but long so here is the result without further ceremony:

$$f_a(x) = a(x^3 + x^2 - 26x + 24) + 2x^2 + 39x + 18 \tag{19}$$

4 Shamir Secret Sharing

4.1 Mathematical Definition

Divide secret S into n parts $S_1, \ldots, S_n$ such that

- Knowledge of any k or more S_i makes secret S computable.
- Knowledge of any $k-1$ or less S_i leaves secret S completely undetermined.

This is called a (k, n) threshold scheme.

The essential idea is that k points are required to define a polynomial of degree $k-1$.

For our purposes we can define a polynomial as follows:

$$
\begin{aligned}
f(x) &= a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \\
f(x0 &= \sum_{i=0}^{k-1} a_i x^i
\end{aligned}
$$

Suppose we want to use a (k, n) threshold scheme to share our secret S, an element in a finite field $\mathbb{F}$ of size P where $0 < k \leq n < P; S < P$ and P is a prime number.

- Choose at random $k-1$ positive integers $a_1, \ldots a_{k-1}$ with $0 < a_i < P; a_i \in \mathbb{N}$ and let $a_0 = S; S < P$.
- Build the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \mod P$
- Construct any n points, *for instance*, set $i = 1, \ldots, n$ to retrieve $(i, f(i))$.

Every participant is given a point, a point, e.g. in integer input to the polynomial and the corresponding integer output.

Given any subset k of these pairs, we can find the coefficients of the polynomial. The secret is the constant term a_0.

4.2 Examples

4.2.1 The Probem

In this example we will omit the requirement that $\mod P$ is applied to the polynomial.

Suppose Eve has managed to obtain a share, say $P = (16, 106)$ which is ak point on the curve defined by 1. Eve knows $f(x) = ax + b$.

She can solve for b in terms of a.

$$\begin{aligned} f(x) &= ax + b \\ P \rightarrow f(16) = 106 &= a(16) + b \\ b &= -16a + 106 \end{aligned} \tag{20}$$

Recall the requirement that $a, b \in \mathbb{N}$.

Eve may then substitute values for unknown a in equation 20.

$$\begin{aligned} a = 0 &\rightarrow b = -16(0) + 106 = 106 \\ a = 1 &\rightarrow b = -16(1) + 106 = 90 \\ a = 2 &\rightarrow b = -16(2) + 106 = 74 \\ a = 3 &\rightarrow b = -16(3) + 106 = 58 \\ a = 4 &\rightarrow b = -16(4) + 106 = 42 \\ a = 5 &\rightarrow b = -16(5) + 106 = 26 \\ a = 6 &\rightarrow b = -16(6) + 106 = 10 \\ a = 7 &\rightarrow b = -16(7) + 106 = -6 \end{aligned}$$

Since the requirement is that $a, b \in \mathbb{N}$, a cannot be negative. Therefore, Eve can conclude

$$\begin{aligned} a &\in [0, 1, 2, 3, 4, 5, 6] \\ b &\in [106, 90, 74, 58, 42, 26, 10] \end{aligned}$$

4.2.2 The Solution

The solution is to require that S is an element in a finite field $\mathbb{F}$ of size P where $S < P$ and P is prime.

Since $S = 42$, choosing $P = 43$ satisfies the requirement that $S < P$ and P is prime.

$$\begin{aligned} f(x) &= 4x + 42 \mod 43 \\ f(16) &= 4(16) + 42 \mod 43 \\ &= 106 \mod 43 \\ f(16) &= 20 \end{aligned}$$

Recall from the definition of a modulus that

$$a \mod P = a - Pm | 0 \leq a - pm \leq P$$

In other words, m is a multiplier.

Eve knows $P = (16, 20)$, $f(x) = ax + b \mod P$, and modulus $P = 43$.

So she can substitute and write

$$\begin{aligned} f(x) &= ax + b \mod P \\ &= ax + b - pm \\ 20 &= 16a + b - 43m \\ b &= -16a + 20 + 43m \end{aligned} \tag{21}$$

As before, Eve can then substitute values for a into equation 21.

$$\begin{aligned} a = 0 &\to b = -16(0) + 20 + 43m = 20 + 43m \\ a = 1 &\to b = -16(1) + 20 + 43m = 4 + 43m \\ a = 2 &\to b = -16(2) + 20 + 43m = -12 + 43m \\ a = 3 &\to b = -16(3) + 20 + 43m = -28 + 43m \\ a = 4 &\to b = -16(4) + 20 + 43m = -44 + 43m \\ a = 5 &\to b = -16(5) + 20 + 43m = -60 + 43m \\ a = 6 &\to b = -16(6) + 20 + 43m = -76 + 43m \\ a = 7 &\to b = -16(7) + 20 + 43m = -92 + 43m \end{aligned} \tag{22}$$

This time since m is unknown, Eve can gain no information about the secret. But since we know $a = 4$ is the correct value, we can see that equation 22 is the correct result. In other words, $m = 2$.

The secret S is equally likely to be any element of the finite field $\mathbb{F}$. No information may be learned about S unless $S_1 \ldots S_k$ are known.