Week 4

Knapsack Problem (0/1 Knapsack problem).

$[a_1, a_2, \ldots, a_n] \rightarrow$ a vector of distinct +ve integers.
$\rightarrow$ object weights.

$a_{i1}, a_{i2}, \ldots a_{ik} \rightarrow$ a sub collection of these numbers.

$s = a_{i1} + a_{i2} + \cdots + a_{ik} \rightarrow$ easy to compute.

opposite problem

given a +ve integer s,
determine, if possible, a subcollection
$a_{i1}, a_{i2}, \ldots, a_{ik}$ having total weight s.

$\downarrow$

Reformulation (Subset sum problem)

decision version.

Problem Instance: $I = (a_1, a_2, \ldots, a_n, s)$,
where $a_1, a_2, \ldots, a_n$ & s are +ve integers.
The a_i's are called sizes/weights and s is called the target sum.

Question: Is there a 0-1 vector $x = (x_1, x_2, \ldots, x_n)$
such that $x_1 a_1 + x_2 a_2 + \cdots + x_n a_n = s$?

$x = (x_1, x_2, \ldots, x_n) \rightarrow \{0,1\}^n$
$a = (a_1, a_2, \ldots, a_n)$

$\boxed{x \cdot a = s.}$

NP complete problem

<u>Example</u> $[a_1, a_2, a_3, a_4, a_5, a_6] = [3, 4, 6, 8, 10, 12]$, $s = 28$

find all solns.

<u>Soln.</u>

$a = [3, 4, 6, 8, 10, 12]$ or $[3, 4, 6, 8, 10, 12]$

$x = 001011$ or 011110

$a.x = 6 + 10 + 12 = 28$ $\quad$ $a.x = 4 + 6 + 8 + 10 = 28$

Merkle-Hellman Knapsack Cryptosystem

$\mathcal{P} = \{0,1\}^n \rightarrow$ n-bit vectors.

$\mathcal{C} = \mathbb{Z}_{\geq 0} \rightarrow$ non-negative integers.

$\text{Alice} \xrightarrow[\text{message}]{\text{private}} \text{Bob}.$

$SK_{Bob} \rightarrow$ private key $\begin{cases} [a_1, a_2, \dots, a_n] \\ m \\ \omega \end{cases}$

$[b_1, b_2, \dots, b_n] \rightarrow$ public. PK_{Bob}.

Bob's Private key

$[a_1, a_2, \dots, a_n] \rightarrow$ super increasing seq.

integer $m > \sum_{i=1}^{n} a_i$ ~~,~~

$1 < \omega < m$ s.t. $\gcd(\omega, m) = 1$.

Bob's public key

$[b_1, b_2, \dots, b_n]$ where $b_i \rightarrow$ least +ve integer

$$b_i \equiv \omega a_i \pmod m$$

least non-negative integer.

Encryption

$x = (x_1, x_2, \dots, x_n)$

$\mathcal{E}_{PK_{Bob}}(x) =$ ~~$x_1 b_1 + \dots$~~ $x \cdot b = x_1 b_1 + x_2 b_2 + \dots + x_n b_n = s$.

$s' = \omega^{-1} s = \omega^{-1} \sum_{i=1}^{n} x_i b_i = \sum_{i=1}^{n} x_i \omega^{-1} b_i \equiv \sum_{i=1}^{n} a_i x_i \pmod m \equiv \sum_{i=1}^{n} x_i a_i$

Decryption.

$\mathcal{D}_{SK_{Bob}}(s) =$ ~~$\omega^{-1} s$~~ $(x_1, x_2, \dots, x_n)$

Compute $s' = \omega^{-1} s \pmod m$ &

Solve the knapsack problem $(a_1, a_2, \dots, a_n, s')$ where $(a_1, \dots, a_n)$ is superincreasing

0/1 Knapsack problem

$s' = 63$.

$[a_1, a_2, a_3, a_4, a_5, a_6] = [1, 2, 4, 9, 20, 48]$.

0 1 1 1 0 1

$s' = 6-4 = 2$

$s' = 15-9 = 6$

$s' = 63-48 = 15$

$[x_1, x_2, x_3, x_4, x_5, x_6]$

0 1 1 1 0 1 → the plaintext.

Exercise

$[a_1, a_2, a_3, a_4, a_5, a_6] = [3, 5, 9, 18, 36, 100]$

$m = 201$

$w = 77$.

a) Bob's public key?

b) $x = 111000$ → ciphertext?

c) decryption process? when Bob receives the ciphertext of part (b).

Example

Suppose that Bob uses the Markle-Hellman knapsack cryptosystem with superincreasing sequence

$[a_1, a_2, a_3, a_4, a_5, a_6] = [1, 2, 4, 9, 20, 48]$, $m = 101$ $\left(> \sum_{i=1}^{6} a_i \right)$.

& $w = 38$ $(\gcd(w, m) = 1)$.

(a) What is Bob's public key?

(b) If Alice uses Bob's public key to encrypt the plaintext 011101, determine the resulting ciphertext.

(c) Perform the decryption process that would need to be done when Bob receives the ciphertext of part (b).

Sol^n.

Bob's public key

a) $\cancel{b(1, 2)}$ $\quad b_i \equiv a_i w \pmod m = 38 a_i \pmod{101}$

$\therefore b_1 = 38$

$b_2 = 76$

$b_3 = 152 = 51$

$b_4 = 342 = 39$

$b_5 = 760 = 53$

$b_6 = 51 \times 12 = 612 = 6$

$[b_1, b_2, b_3, b_4, b_5, b_6]$

$\equiv w [a_1, a_2, a_3, a_4, a_5, a_6] \pmod{101}$

$\equiv [38, 76, 51, 39, 53, 6]$

$\begin{array}{r} 612 \\ 606 \\ \hline 6 \end{array}$ $\quad \begin{array}{r} 172 \\ 101 \\ \hline 71 \\ 8 \\ \hline 568 \\ 505 \\ \hline 63 \end{array}$

$x = [0\ 1\ 1\ 1\ 0\ 1]$

b) $s = b \cdot x = 76 + 51 + 39 + 6 = 172$

$w^{-1} \bmod 101$
$= 38^{-1} \bmod 101 = 8$.

c) $s' \equiv w^{-1} s \pmod m = 8 \times 172 \pmod{101} = 63$

$[a_1, a_2, \cdots, a_n] \to$ superincreasing if

$a_i > a_1 + a_2 + \cdots + a_{i-1}$ for $i = 2, 3, \cdots, n$.

<u>proposition</u> A knapsack problem with superincreasing weights can have <u>at most one sol^n</u>.

<u>Algon.</u> <u>for solving a superincreasing instance of the Knapsack problem.</u>

for $i := n$ downto 1 do

 if $(s \geq a_i)$ then

  $s = s - a_i$

  $x_i = 1$

 else

  $x_i = 0$

 end if

end do

 if $s = 0$ then

  $x = (x_1, x_2, \cdots, x_n)$ is the sol^n.

 else

  No sol^n.

 end if

Example:

~~(a) check that~~

$$[a_1, a_2, a_3, a_4, a_5, a_6] = [1, 2, 4, 9, 20, 48]$$

$\rightarrow$ superincreasing

find all solⁿ with $s = 27$.

$a = [1, 2, 4, 9, 20, 48]$

$x = [x_1, x_2, x_3, x_4, x_5, x_6]$

$\quad\;\; 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0$

$s = 3 - 1 = 1$ $\quad s = 7 - 4 = 3$ $\quad s = 27 - 20 = 7$

$$\sum_{k=0}^{k} 2^k < 2^{k+1}$$

$$= 2^{k+1} - 1$$

111010 $\rightarrow$ a solⁿ as $a \cdot x = 1 + 2 + 4 + 20 = 27$.

Exercise

a) Suppose that $[a_1, a_2, a_3, \ldots, a_n] = [1, 2, 4, \ldots, 2^n]$.
Show that this is superincreasing.

b) Show that any superincreasing seq. $[a_1, a_2, \ldots, a_n]$ must satisfy $a_i \geq 2^{i-1}$ for each i.

thus ~~smallest superincreasing~~ seq.