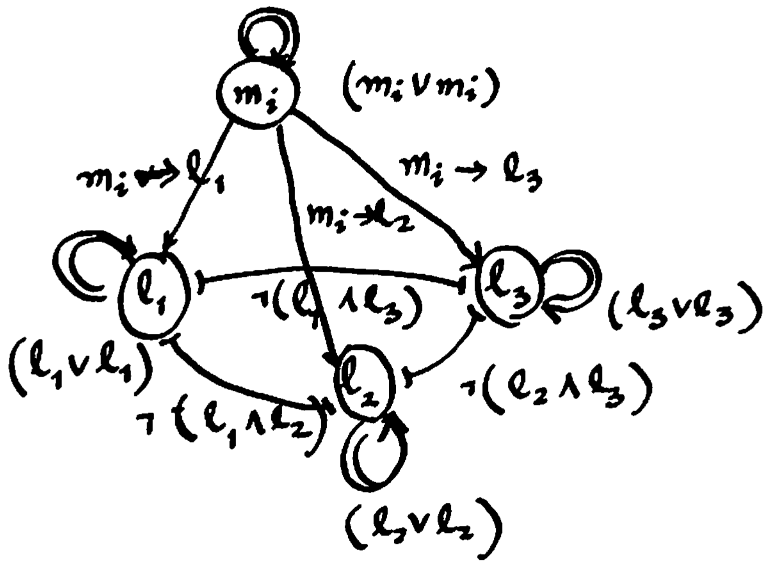
LECTURE #8

Misc. MAX-2-SAT is NP-Complete.

Let clause $c_i = (\ell_1 \vee \ell_2 \vee \ell_3)$



A $m_i \vee m_i$

B $\ell_1 \vee \ell_1 \quad \ell_2 \vee \ell_2 \quad \ell_3 \vee \ell_3$

C $\neg m_i \vee \ell_1 \quad \neg m_i \vee \ell_2 \quad \neg m_i \vee \ell_3$

D $\neg \ell_1 \vee \neg \ell_2 \quad \neg \ell_2 \vee \neg \ell_3 \quad \neg \ell_1 \vee \neg \ell_3$

I Assume c_i = SAT

$\ell_1 = T, \ \ell_2 = F, \ \ell_3 = F \qquad m_i = F$

$$\left.\begin{array}{l} A \to 0 \\ B \to 1 \\ C \to 3 \\ D \to 3 \end{array}\right\} 7$$

$\ell_1 = T \quad \ell_2 = T \quad \ell_3 = F \qquad m_i = T$

$$\left.\begin{array}{l} A \to 1 \\ B \to 2 \\ C \to 2 \\ D \to 2 \end{array}\right\} 7$$

$\ell_1 = T \quad \ell_2 = T \quad \ell_3 = T \qquad m_i = T$

$$\left.\begin{array}{l} A \to 1 \\ B \to 3 \\ C \to 3 \\ D \to 0 \end{array}\right\} 7$$

II Assume $c_i \neq$ SAT

$\ell_1 = F \quad \ell_2 = F \quad \ell_3 = F \qquad m_i = F$

$$\left.\begin{array}{l} A \to 0 \\ B \to 0 \\ C \to 3 \\ D \to 3 \end{array}\right\} 6$$

Given a 3-CNF $\Rightarrow$ Create a 2-CNF

#variables = n #variables = $n+m$

clauses = m # clauses = $10m$

3-CNF = SAT $\Leftrightarrow$ 2-CNF = 7m-2-SAT

MAX-2-SAT for 7m or more clauses.

PRINCIPLE OF OPTIMALITY:

"The subsolution of an optimal solution of the problem are themselves optimal solutions for their subproblems."

Example: Shortest path problem

$G = (V, E)$ $a, b \in V$ $a \to x_1, \ldots, x_n \to b$

is a shortest path from a to b $\Rightarrow$ $x_i \to x_{i+1} \cdots x_{j-1} \to x_j$ is a shortest path from x_i ~~to~~ x_j.

$A^{(k)}[i,j]$ = Length of the shortest path from i to j using only ~~nodes~~ intermediate nodes with labels $\leq k$.

$$A^{(0)}[i,j] = w[i,j]$$

$$A^{(k)}[i,j] = \min\left(A^{(k-1)}[i,j],\ A^{(k-1)}[i,k] + A^{(k-1)}[k,j]\right)$$

Space = $O(n^2)$ Time = $O(n^3)$.

↓

Memoization.

Knapsack Problem: 0-1 knapsack: Item $i = \langle v_i, w_i \rangle$ (value, weight)

maximize $\sum_{i=1}^{n} v_i x_i$ s.t. $\sum_{i=1}^{n} w_i x_i \leq W$ $x_i \in \{0,1\}$

$m[i,w]$ = Max Value using items $\in$ $[1..i]$ with weights $\leq w$.

Recurrence

$$m[i,w] = m[i-1,w] \quad \text{if } w_i > w$$

$$m[i,w] = \max\left(m[i-1,w],\ m[i-1,w-w_i]+v_i\right) \text{ if } w_i \le W$$

$$M[n,W] = \text{Soln}.$$

Space $= O(nW)$ Time $= O(nW)$. $W = O(2^{\langle W \rangle})$

= Exp. in the #bits needed to succinctly represent the input

Superincreasing Sequences.

$a_1, a_2, \ldots, a_n$ s.t $\sum_{i=1}^{j-1} a_i \le a_j$.

Assume that $w_1, w_2, \ldots, w_n$ & $v_1, v_2, \ldots, v_n$ are both super increasing

& $W \le w_1 + w_2 + \cdots + w_n$ [otherwise, there is nothing to solve].

The 0-1 Knapsack problem is in P.

Consider the recurrence:

$$m[i,w] = m[i-1,w] \quad \text{if } w_i > w$$

$$m[i,w] = m[i-1,w-w_i] + v_i \quad \text{if } w_i \le w.$$

Note $m[i-1,w] \le v_1 + \cdots v_{i-1} \le v_i$

Also note that $w - w_i \le w_1 + \cdots + w_{i-1} \le w_i$

$$w_i \ge \frac{w}{2}$$

$$w - w_i \le w/2$$

$\therefore$ # steps is $\le \log W$.

Space $= O(n\cancel{\log}W)$ Time $= O(n \log W)$

Consider a knapsack problem in which

$\beta_1, \beta_2, \cdots, \beta_n$ = superincreasing

$v_i = \omega_i = \beta_i$

Check if $\sum x_i v_i \geq W$ subject to

$\sum x_i \omega_i \leq W \quad x_i \in \{0,1\}$

$\Rightarrow$ Given a W check if $\exists_{x_i \in \{0,1\}} \sum x_i \beta_i = W$

This problem is in P.

Let's create a "hard" but related instance of the problem.

$\pi \in S_n$ is a permutation. (Random).

$m > \sum_{i=1}^{n} \beta_i$

$\omega \in \mathbb{Z}_m^*$

$\alpha_1, \alpha_2, \cdots, \alpha_n$ ← New sequence.

$\alpha_i = \omega \cdot \beta_{\pi(i)} \bmod m.$

Let $x \in \{0,1\}^n$ a message and its encryption is

$$\sum \alpha_i x_i = S.$$

Solving for x_i is hard $\Rightarrow$ (A "Hard" Instance of an NPC problem → Knapsack)

$$W = \omega^{-1} S = \sum_{i=1}^{n} \beta_{\pi(i)} x_i \bmod m. = \sum_{i=1}^{n} \beta_{\pi(i)} x_i$$

Since $\sum \beta_{\pi(i)} x_i < \sum \beta_i < m.$

So with the knowledge of ω and β_i's, W provides an easy instance of an NPC problem, and S (hence W) can be decrypted.

PUBLIC KEY CRYPTO SYSTEM.

PublicKey = $\langle \alpha_1, \cdots, \alpha_n \rangle$

Private Key = $\{ w, m, \langle \beta_{\pi(1)}, \cdots, \beta_{\pi(n)} \rangle \}$

To send a secret message,

Plaintext = $\langle x_1, \cdots, x_n \rangle \in \{0,1\}^n$.

Anyone can send $s = \sum \alpha_i x_i$

But it can only be decrypted by the Private key in polytime.

$$W = w^{-1} s = \sum \beta_i y_i \qquad (\beta_i = \text{super increasing})$$

If

$$\underset{=(y_1, \cdots, y_{n-1}, y_n)}{\text{Solve}(W,n)} = \begin{cases} (\text{solve}(W, n-1), 0) & \text{if } \beta_n > W \\ \text{or} \\ (\text{Solve}(W-\beta_n, n-1), 1) & \text{if } \beta_n \le W \end{cases}$$

$$(x_1, \cdots, x_n) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)} \cdots y_{\pi^{-1}(n)})$$

MERKLE - HELLMAN KNAPSACK CRYPTO SYSTEM: (1978)

NP-Completeness $\begin{cases} \text{Cook} & 1971 \\ \text{Levin} & 1973 \\ \text{Karp} & 1972 \end{cases}$ (21 NP complete proofs).

Merkle - Hellman was broken in 1982 by Shamir using Lattice algorithm (Shortest Vector Problem).

LLL = Lenstra - Lenstra - Lovasz
for fixed dimension integer programming.
(If dim = D = constant, then ILP $\in$ P).

Lattice

A lattice is a set of points in $\mathbb{R}^n$ with a periodic structure.

Given n-linearly independent vectors

$$\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n \in \mathbb{R}^n \quad \left\{ \text{Basis of the Lattice.} \right.$$

The lattice generated by them is the set of vectors

$$\mathcal{L}(\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n) = \left\{ \sum_{i=1}^{n} x_i \vec{b}_i : x_i \in \mathbb{Z} \right\}$$

Basis Matrix

$$B = [\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n] = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix} \in \mathbb{R}^{n \times n}$$

$$\mathcal{L}(B) = \underbrace{\{ Bx : x \in \mathbb{Z}^n \}}$$

λ_i = i^{th} successive minima of $\mathcal{L}$ $\quad 1 \le i \le n$

$\lambda_i(\mathcal{L})$ = Radius of the smallest ball centerd about the origin of $\mathbb{R}^n$ such that it contains i linearly independent lattice vector.

$\lambda_1(\mathcal{L})$ = Shortest Vector Length:

SHORTEST VECTOR PROBLEM: (SVP)

Given a basis for a lattice $\mathcal{L}$,
Find $v \in \mathcal{L}$ such that $\|v\| = \lambda_1 \mathcal{L}$

$\vec{v}$ = shortest non-zero vector in $\mathcal{L}$.

Knapsack Cryptography Attack.

$\langle \alpha_1, \dots, \alpha_n \rangle$ & s.

Choose $B = \lceil \sqrt{n 2^n} \rceil$

$$\mathbb{B} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ \vdots & \vdots & \ddots & \\ & & & 1 \\ -B\alpha_1 & -B\alpha_2 & -B\alpha_n & Bs \end{pmatrix}$$

Suppose $(x_1, \dots, x_n) \in \{0,1\}^n$ is a soln.

Let $z = (x_1, \dots, x_n, 1)^T$

$$\therefore \mathbb{B}z = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ 0 \end{pmatrix} \qquad \|\mathbb{B}z\| \le \sqrt{n}$$

It can be shown that $\mathbb{B}z$ is the SVP for this lattice. (So is $-\mathbb{B}z$).

Consider any lattice vector that is not a multiple of z

$$\mathbb{B}z' = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \\ \theta \end{pmatrix} \qquad B \mid \theta : \theta \text{ is divisible by } B.$$

$$\|\mathbb{B}z'\| > B > 2^{n/2} \|x\| \ge 2^{n/2} \lambda_1(\mathcal{L}).$$

Assume that there is a heuristic that solves the SVP with a competive factor $2^{n/2}$

$\Rightarrow$ Produces a nonzero vector $\vec{v}'$

$$\|\vec{v}'\| < 2^{n/2}\lambda_1(\mathcal{L})$$

This heuristic can break Merkle-Hellman Cryptosystem.

Lenstra - Lenstra - Lovasz. (LLL 1982)

Provides a $\left(\frac{2}{\sqrt{3}}\right)^n$ approximation ratio

$$\to \left(\frac{4}{3}\right)^{n/2} = (1.333)^{n/2}.$$

GRAM-SCHMIDT:

Input: $(b_1, \ldots, b_n)$: Basis $\in \mathbb{R}^n$

Output: $(b_1^*, \ldots, b_n^*)$: Basis $\in \mathbb{R}^n$ such that b_i^*'s are mutually orthogonal.

begin

$b_1^* = b_1$

for $i = 2$ to n loop

$$b_i^* := b_i - \sum_{j=1}^{i-1} \left(\frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}\right) b_j^*$$

end

end

WEAK-BASIS REDUCTION.

Input: $(b_1, \cdots, b_n)$ = Basis of Λ.
$(b_1^*, \cdots, b_n^*)$ = GRAM-SCHMIDT $(b_1, \cdots, b_n)$
Output: $(\bar{b}_1, \ldots, \bar{b}_n)$ = A weakly reduced basis of Λ.

begin
  for $i := n$ downto 2 loop
    for $j := i-1$ down to 1 loop
$$b_i := b_i - \left[\frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \right] \cdot b_j$$
    end
  end
end.

L^3-BASIS-REDUCTION.

Input: $(b_1, \ldots, b_n)$: Basis of n-dim. lattice Λ.
Output: $(b_1', \cdots, b_n')$ = ~~WEAK-BASIS-REDUCTION $(b_1, \ldots, b_n)$~~
A reduced basis of Λ.

begin
  loop
    $(b_1^*, \ldots, b_n^*) := \text{G-S}(b_1, \cdots, b_n)$
    $(b_1, \ldots, b_n) := \text{WBR}(b_1, \ldots, b_n)$
    if $\exists_{i \in \{1..n-1\}} \; \|b_{i+1}^*\| < \frac{1}{2}\|b_i^*\|$ then
      $(b_i, b_{i+1}) := (b_{i+1}, b_i)$
    else
      exit loop.
    end.
  end.

Let b_1' be the shortest among the reduced basis of Λ
$$\|b_1'\| \leq 2^{n-1/2} \lambda_1(\mathcal{L})$$

Note Let $\vec{v} = SV(\Lambda)$ $\quad \Lambda \leftarrow (b_1, \ldots, b_n)$

$$v = x_1 b_1 + x_2 b_2 + \cdots + x_n b_n$$

By defn $\|v\| \le \min(\|b_1\|, \cdots, \|b_n\|)$

$$x_i = \frac{\det(b_1, \ldots, b_{i-1}, v, b_{i+1}, \ldots, b_n)}{\det(b_1, \ldots, b_{i-1}, b_i, b_{i+1}, \ldots, b_n)}$$

$$|x_i| \le \frac{\|b_1\| \, \|b_2\| \cdots \|b_n\|}{\det(b_1, b_2 \cdots b_n)} = \delta$$

$\cancel{-2\lceil\delta\rceil \le x_i \le 2\lceil\delta\rceil}$ $\quad -\lceil\delta\rceil < x_i < \lceil\delta\rceil$

Search a space of size $(2\lceil\delta\rceil + 1)^n$ for all possible values of x_i.