Day 9
Follow up of Avis's lectures

- Error correcting code 誤り訂正符号
  - Red-blue hatters puzzles 帽子色当てクイズ
    - Peter Winkler: Mathematical Puzzles
  - Information and Nim game 情報と石取りゲーム
  - Make impossible looking thing possible
- Secure transmission 安全な通信
  - Mailing a precious ring 指輪郵送パズル
  - Diffie-Helman protocol デフィー・ヘルマン法
  - Euclid's mutual division algorithm ユークリッドの互除法

Red-blue hatters (1)

- 15 boys ware blue or red hat. None can see his own hat, and want to guess it.
- They are in a line, and see front boys.
  - From the last, each person call a color .
  - Others can hear the call.
- Game 1: If k boys are right, get k dollars
- Game 2: Get 100 dollars if and only if everyone is right.
- Problem: Which do you prefer?
  - You can discuss your strategy.

What we learned

Small information helps much!

小さいサイズの情報が大きな効果を持つ！

We can often control large information by using small information.

How to utilize this idea???

Error correcting code (1)

- We send an information consists of n bits, but one bit might be flipped
- We add one bits, and send n+1 bits so that we can detect the error automatically.
- How to do it ? → Parity bit!
  - If odd number of 1 (or 0), parity bit is 1 (0).

This is just detection, not necessarily recover the error.

Nim game (三山崩し)

- A game between Alice and Bob
- Given (a,b,c) of nonnegative integers
  - Piles of stones
- Each player must reduce one of a, b, or c
- The player who makes (0,0,0) wins.
  - (4,3,1) Alice takes two stones from 4
  - (2,3,1) Bob takes one stone from 2
  - (1,3,1) Alice takes three stones from 3
  - (1,0,1) Bob resigns.
- Given (a,b,c), find which is the winner.

Analysis

- If (a,b,0) , Alice wins unless a=b.
- If (a,b,1),　勝ちパターンは？
  - Alice Wins
    - (1,1,1) , (2, 1,1) , (2,2,1) → move to (a,a,0)
  - (3,2,1) → No way
    - (3,3,1), (4,2,1),(4,3,1) → move to (3,2,1)
    - (4,4,1) → move to (4,4,0)
  - (5,4,1) → No way
  - Losing pattern (n, n-1, 1) ？ But (4,3,1)??

Vector mod-2 summation
二進ベクトルとしての和

Mod-2 summation (Sum in GF(2))
0+0=0, 1+0=0+1=1, 1+1=0

Vector (bit-wise) 2-adic summation
01001011 ★ 11011011 = 10010000

Theorem:
In Nim, Alice wins unless
a ★ b ★c = 0

Prof. Avis‘s version

- Prof. Avis’s version is slightly different
- The one taking the last stone “loses”
  - My version “wins”.
- Homework: consider Avis’s version
  - How the strategy changes?

Red-blue hatters (2)

- A team of 15 boys ware red or blue hats
  - The color of hats are randomly given,
  - Each sees 14 hats, except his own hat.
- Each guesses his hat color, and answer it similutaneously. But he may “pass”.
  - If anyone gives a wrong answer, they lose.
  - If all say “pass”, they lose.
- What is your team strategy?
  - Target: more than 90% winning probability

Solution

- We use vector mod-2 sum.
- 15 boys has ID: from 0001 to 1111.
- Strategy:
  - Each boy compute the vector mod-2 sum of red-hat boys, if the sum equals his ID, he tells
    " My hat is blue!"
  - If the sum equals 0000, tell "My hat is red".
  - Otherwise, pass.
- Winning probability: 15/16.

Error correcting code (2)

- We send an information consists of 11 bits, but one bit might be flipped
- We add four bits, and send 15 bits so that we can recover error automatically.
- How to do it ?
- Humming code: Use the idea of blue-red hat problem.

Hamming code

- A bit sequence (a(1), a(2),..,a(n)) is Hamming code if the vector 2-adic sum of 1-position indices is 0
  - (1,0,0,1,1,0,0) is a Hamming code
    - Since 1 ★4★5= 001★100★101=000
  - (0,1,0,0,1,0,1) is a Hamming code
- How to make a Hamming code?
  - (1,0,1,0) → (x,y,1,z,0,1,0) → (1,0,1,1,0,1,0)
- 2^k- k -1 bit data → 2^k -1 bit Hamming code

The dot-town (3)

- In a village, every residence has either red or blue dot in his (or her) forhead ,but if he figures out his color, he must leave the village immediately.
- Everyday, the residents gather.
- One day, a stranger comes, and anything related to the number of dots.
  - E.g. “The number of red people is not 100”
- Then prove that the village becomes empty eventually.

Secure mail quiz

- Bob want to send engage ring to Alice. But they live far away, and he need to mail it. Unfortunately, in their country “Kopernica”, mail is always stolen unless it is in a box locked by a padlock.
- Each of Bob and Alice has many padlocks, but has no key for padlocks of each other.
- How Bob safely send the ring (or a pair of his padlock and key) to Alice??

Deffie-Helman system

- Whitfield Deffie was captured the idea of the secure key exchange
  - He want to turn the Alice-Bob puzzle to the secure network protocol
- Martin Helman joined him, and find a way by using elementary number theory.
  - Deffie was a kind of hippy researcher and Helman was a professor of Stanford