Gems of TCS

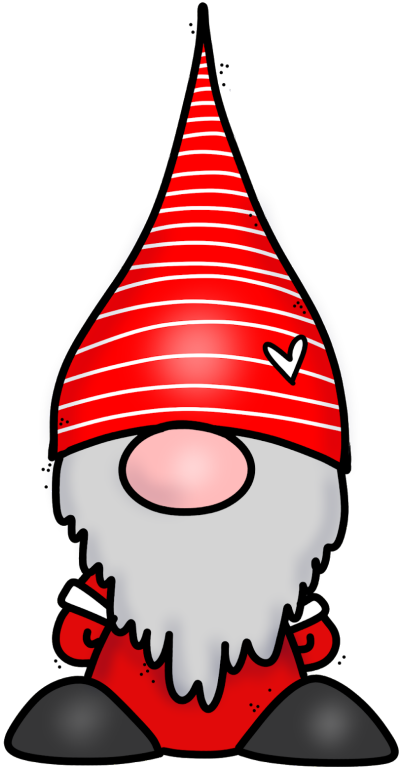
Error Correcting Codes

Sasha Golovnev

April 6, 2021

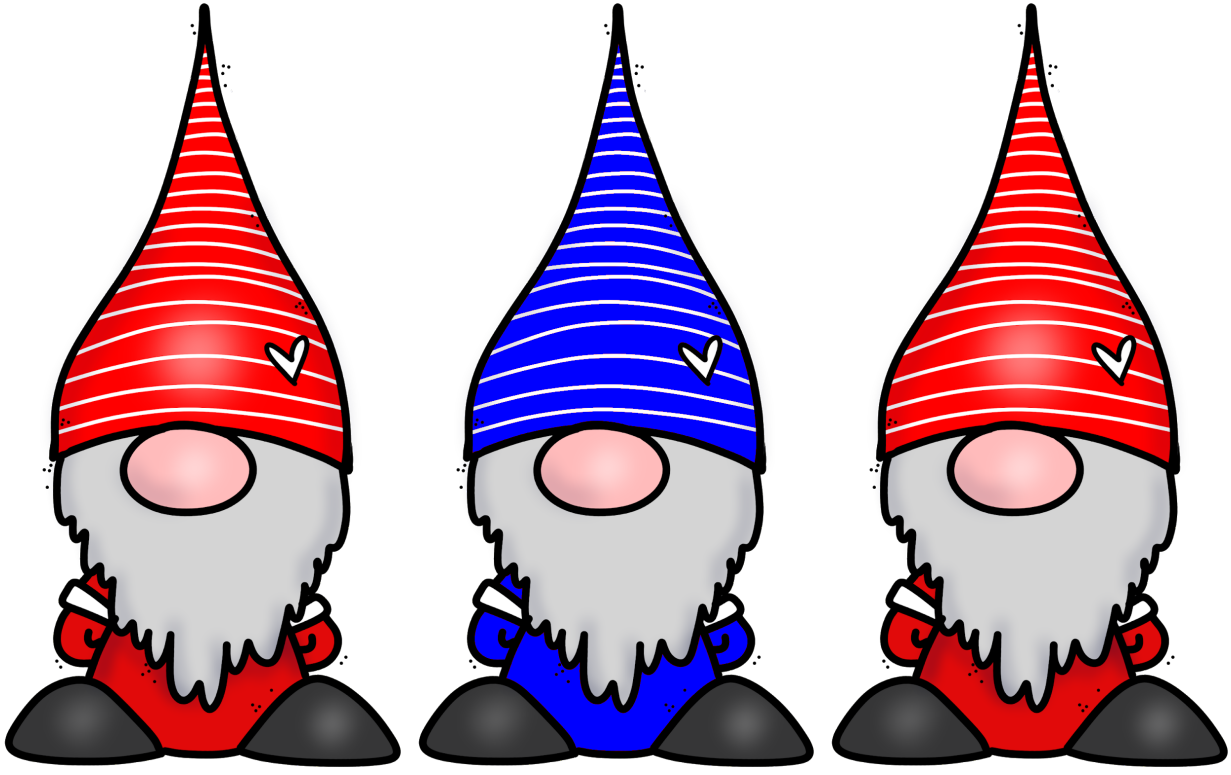
Error Correcting Codes

Area of CS that saves little gnomes' lives



Hat Game

Hat Game



The New York Times

Why Mathematicians Now Care About Their Hat Color

By Sara Robinson

April 10, 2001

It takes a particularly clever puzzle to stump a mind accustomed to performing mental gymnastics.

So it's no ordinary puzzle that's spreading through networks of

Hat Game

- Red and Blue hats are placed randomly (and independently) oh gnomes' heads

Hat Game

- Red and Blue hats are placed randomly (and independently) oh gnomes' heads
- Each gnome sees all hats except for their own one

Hat Game

- Red and Blue hats are placed randomly (and independently) oh gnomes' heads
- Each gnome sees all hats except for their own one
- No communication!

Hat Game

- Red and Blue hats are placed randomly (and independently) oh gnomes' heads
- Each gnome sees all hats except for their own one
- No communication!
- Strategy session before the start

Hat Game

- Red and Blue hats are placed randomly (and independently) oh gnomes' heads
- Each gnome sees all hats except for their own one
- No communication!
- Strategy session before the start
- Simultaneously guess color of their own hat or pass

Winning Conditions

- Win: no player guessed incorrectly AND at least one guessed correctly

Winning Conditions

- Win: no player guessed incorrectly AND at least one guessed correctly

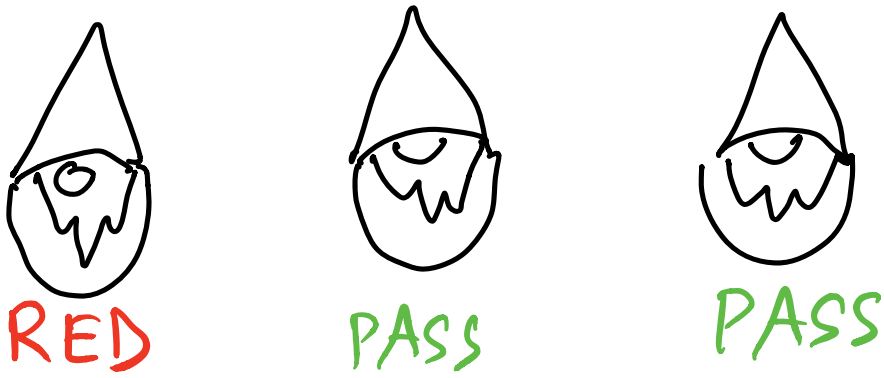
All gnomes are released

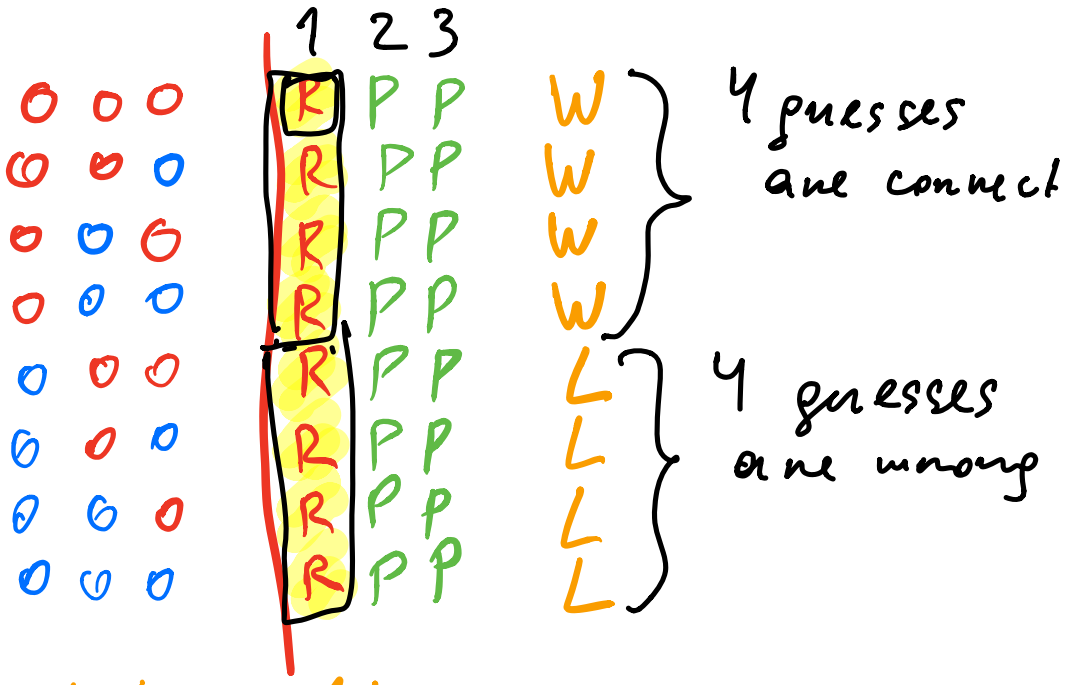
- Lose: at least one guessed incorrectly OR all passed

All gnomes are executed

Max. push freezing released

First Attempt.

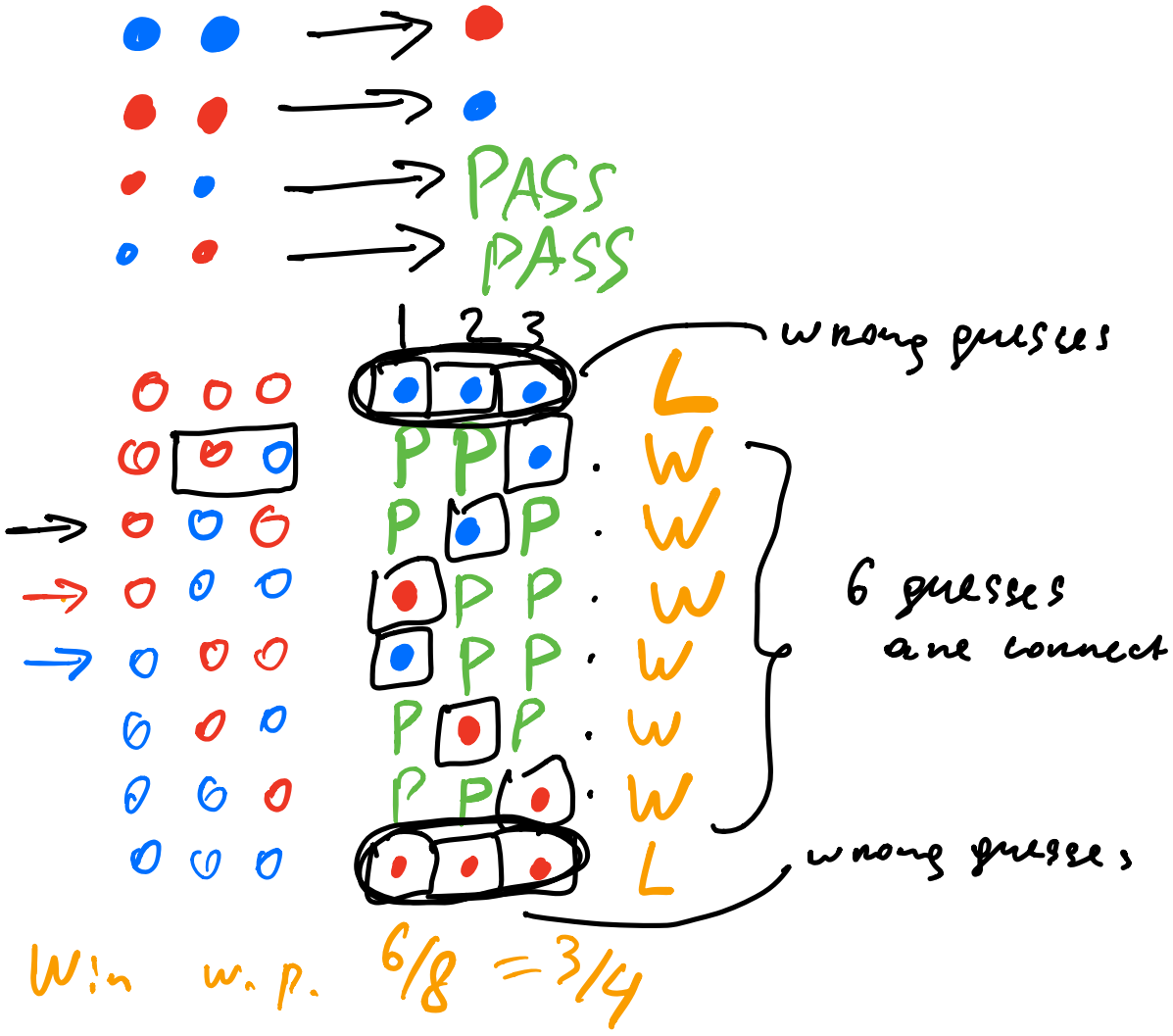




w.p. $4/8 = 1/2$

Better (Optimal) Strategy

Each guess:



Win w.p. $6/8 = 3/4$

6 connect guesses

6 wrong guesses

I'll guess BLUE

This guess is correct ● ● ●

This guess is wrong ● ● ●

In every strategy,

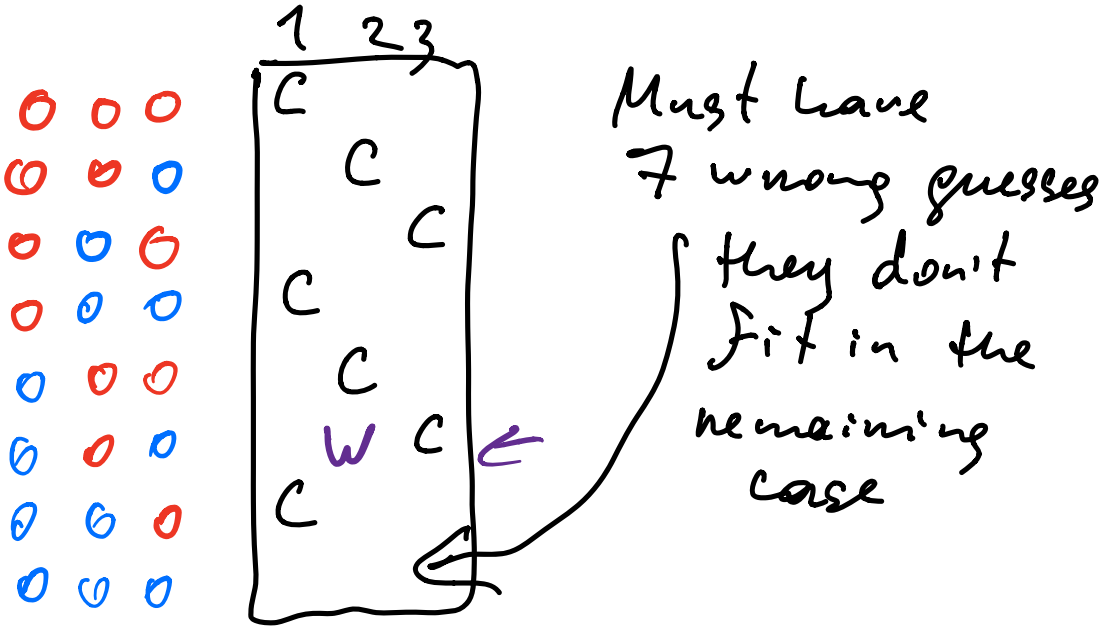
correct = # wrong

In naive str, we evenly spread 4 correct and 4 wrong guesses

In opt str, spread out 6 correct guesses, group 6 wrong guesses

Optimality

Assume WIN in 7 cases



Contradiction => 6 is maximum

Generalizations

● ● → 0/1.

Input $\in \{0,1\}^3$

Two strings from $\{0,1\}^3$ are **close** if they're same string or differ in one position

010	011	close
011	011	close
011	000	are **not** close

Pick a set of BAD inputs $B \subseteq \{0,1\}^3$

Property of B

Every string from $\{0,1\}^3$ is close to **exactly one** string from B

Ex. $B = \{000, 111\}$

- String 000 is close 000
- Every string w one 1 is close to 000
- Every string w two 1s is close to 111
- String 111 is close to 111

Given B, a strategy for 3 gnomes s.t. they lose only if the input $\in B$

She knows, input is either 0 0 1 or 1 0 1

If none of the inputs is BAD ($\in B$)

PASS

If one of them is BAD ($\in B$), then she makes the opposite guess

Sees 0 0

Guesses 1 0 0

Proof that we lose only in BAD cases ($\in B$)

Win if input $\notin B$.

$B = \{000, 111\}$

input & B

011 is close 111

*11 → 011 WIN

0*1 → PASS

01* → PASS

We win in $8 - |B|$

Prop. we win $\frac{8 - |B|}{8}$

For three genomes, $|B| = 2$

we win $\frac{6}{8} = \frac{3}{4}$

For any # of gnomes n,
if we have set B s.t.
every string $\{0,1\}^n$
is close to exactly one
string from B
then we have strategy
that wins on all inputs & B

When do such sets B exist?

Every string from B

s is close to s
s_1 s_2 s_3 ... s_n are close to s
$n+1$ close strings

Total # of strings $2^n = |B| \cdot (n+1)$

$$|B| = \frac{2^n}{n+1}$$

2^n multiple of $(n+1)$

$n+1 = 2^k \iff n = 2^k - 1$

$3 = 2^2 - 1$ $\quad$ $7 = 2^3 - 1$

In fact, set B exists for each such n

Solution for 7 Gnomes

Set B for 7 gnomes

You can check every $0,1^7$ is close to exactly one of these 16 strings

0000000	0001111	0010110	0011001
0100101	0101010	0110011	0111100
1000011	1001100	1010101	1011010
1100110	1101001	1110000	1111111

1010010

Each of 128 strings from $0,1^7$

IF there are 7 gnomes, then they will lose only in 16 cases.

Win $128-16$ cases

They win w.p. $\frac{128-16}{128} = \frac{112}{128} = \frac{7}{8}$

$n = 2^k - 1$ gnomes lose in

$|B| = \frac{2^n}{n+1}$

win $2^n - \frac{2^n}{n+1}$

win w.p.

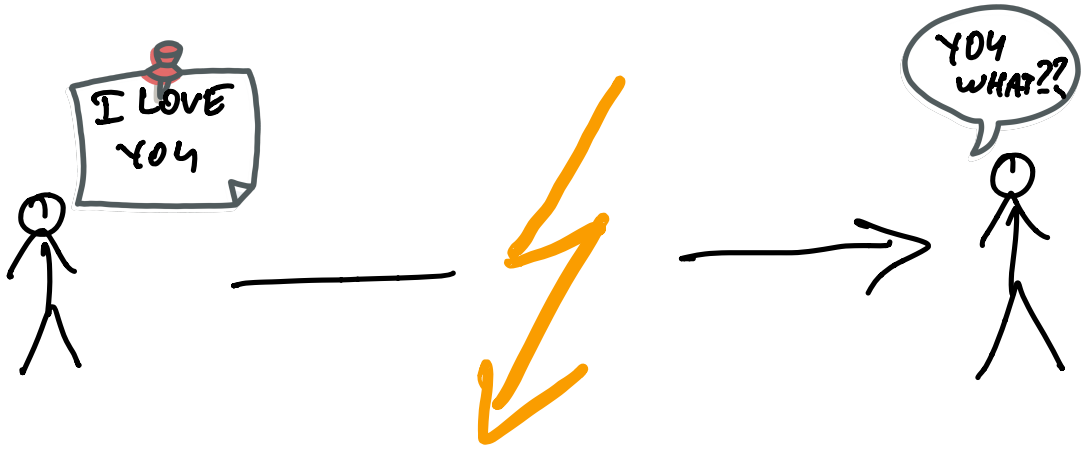
$$\frac{2^n - \frac{2^n}{n+1}}{2^n} = \frac{n}{n+1} = 1 - \frac{1}{n+1}$$

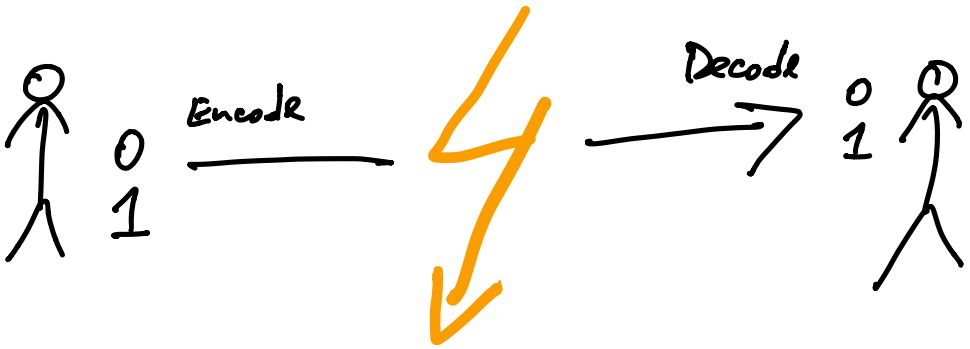
E.g. $n=3$ $\frac{3}{4}$

$n=7$ $7/8$

$n=1023$ $1023/1024$

Hamming Code





$0 \rightarrow 00$

$1 \rightarrow 11$

$00 \rightarrow 0$

$11 \rightarrow 1$

$01 \rightarrow ?$

$10 \rightarrow ?$

$0 \rightarrow 000$

$1 \rightarrow 111$

$000 \rightarrow 0$

$001 \rightarrow 0$

$010 \rightarrow 0$

$011 \rightarrow 1$

$100 \rightarrow 0$

$101 \rightarrow 1$

$110 \rightarrow 1$

$111 \rightarrow$

She decodes because every string from $\{0,1\}^3$ is close to only one encoded message

$B = \{000, 111\}$

B property: every string from $\{0,1\}^3$ is close to exactly one string from B

0000000	0001111	0010110	0011001
0100101	0101010	0110011	0111100
1000011	1001100	1010101	1011010
1100110	1101001	1110000	1111111

I want to encode one of 16 options (4 bits)

I just send one of these

Every string from $\{0,1\}^7$ is close to only one of the 16 strings

---

Error correcting code

Hamming code exists for every $n = 2^k - 1$

Ulam's Problem

I chose a number from $\{1, \ldots, 16\}$

You can ask any YES/NO questions, guess my number.

How many questions do you need?

Binary search 4. $(\log_2 n)$

Ulam's game: $\{1, \ldots, 16\}$

I'll lie ≤ 1 time

Naive strategy

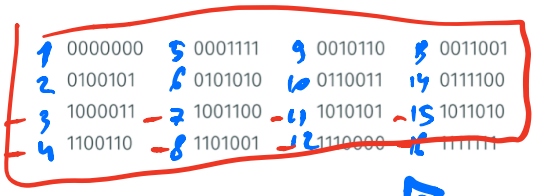
≤ 8?	Y
≤ 8?	N
≤ 8?	Y

≤ 8	Y
≤ 8	Y
≤ 4	Y
≤ 4	Y
≤ 2	Y
≤ 2	Y
≤ 1	Y
≤ 1	N
≤ 1	Y

9 questions

7 questions (using Hamming Code).

16 numbers



1. What is the first bit of your number mapped

2. 2nd bit?

⋮

7. 7th bit?

Is 1st bit 1

↓

Is your number ∈ {3, 4, 7, 8, 11, 12, 15, 16}?