Magic or Mathematics ?!?

Prerona Chatterjee

NISER Bhubaneswar

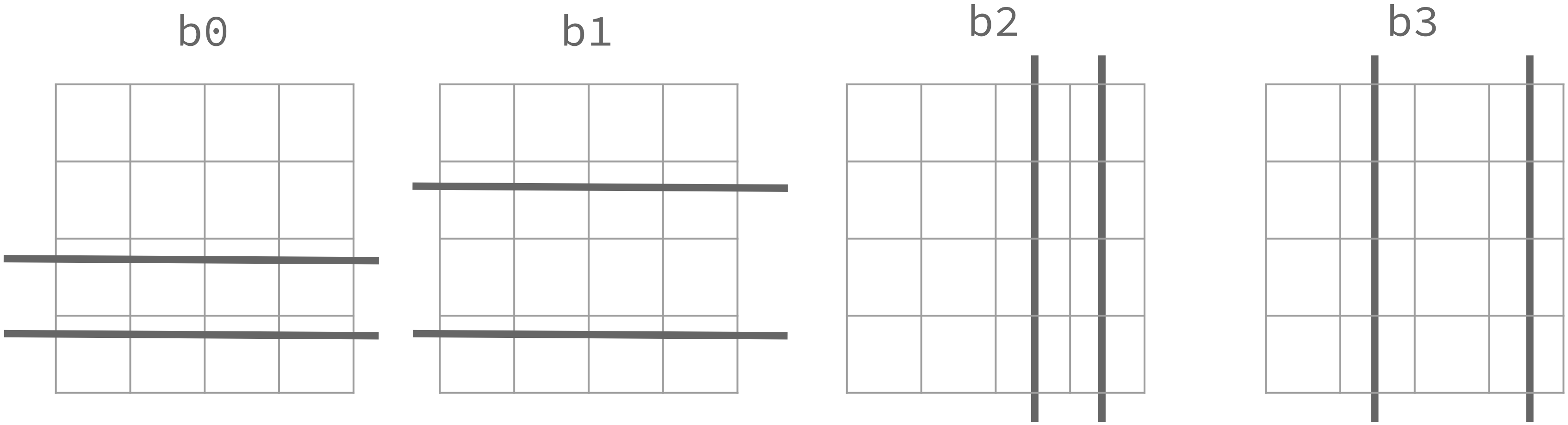
The Power of Two !!

Fill arbitrarily
with red/black.

The Power of Two!!

$B \equiv b0\ b1\ b2\ b3 \in \{0,1\}^4$

0 : #black is even
1 : #black is odd



Given: Grid corresponding to
a0 a1 a2 a3

Given: Grid corresponding to
a0 a1 a2 a3

Want: Grid corresponding to
c0 c1 c2 c3

Given: Grid corresponding to
a0 a1 a2 a3

Want: Grid corresponding to
c0 c1 c2 c3

Step 1: Find b0 b1 b2 b3
such that

$$\begin{array}{r} \text{a0 a1 a2 a3} \\ \oplus\ \text{b0 b1 b2 b3} \\ \hline \text{c0 c1 c2 c3} \\ \hline \end{array}$$

XOR (Addition Mod 2)

Given: Grid corresponding to
a0 a1 a2 a3

Want: Grid corresponding to
c0 c1 c2 c3

Step 1: Find b0 b1 b2 b3
such that

$$\begin{array}{rl} & a0\ a1\ a2\ a3 \\ \oplus & b0\ b1\ b2\ b3 \\ \hline & c0\ c1\ c2\ c3 \\ \hline \end{array}$$

$0 \oplus 0 = 0 = 1 \oplus 1$

$0 \oplus 1 = 1 = 1 \oplus 0$

Given: Grid corresponding to
a0 a1 a2 a3

Want: Grid corresponding to
c0 c1 c2 c3

Step 1: Find b0 b1 b2 b3
such that

$$\begin{array}{rcccc} & a0 & a1 & a2 & a3 \\ \oplus & b0 & b1 & b2 & b3 \\ \hline & c0 & c1 & c2 & c3 \\ \hline \end{array}$$

XOR (Addition Mod 2)

$0 \oplus 0 = 0 = 1 \oplus 1$

$0 \oplus 1 = 1 = 1 \oplus 0$

$$\begin{array}{rcccc} & a0 & a1 & a2 & a3 \\ \oplus & b0 & b1 & b2 & b3 \\ \hline & a0 \oplus b0 & a1 \oplus b1 & a2 \oplus b2 & a3 \oplus b3 \end{array}$$

XOR (Addition Mod 2)

Given: Grid corresponding to
a0 a1 a2 a3

Want: Grid corresponding to
c0 c1 c2 c3

Step 1: Find b0 b1 b2 b3
such that

$$\begin{array}{r}
\text{a0 a1 a2 a3} \\
\oplus \;\; \text{b0 b1 b2 b3} \\
\hline
\text{c0 c1 c2 c3} \\
\hline
\end{array}$$

$$0 \oplus 0 = 0 = 1 \oplus 1$$

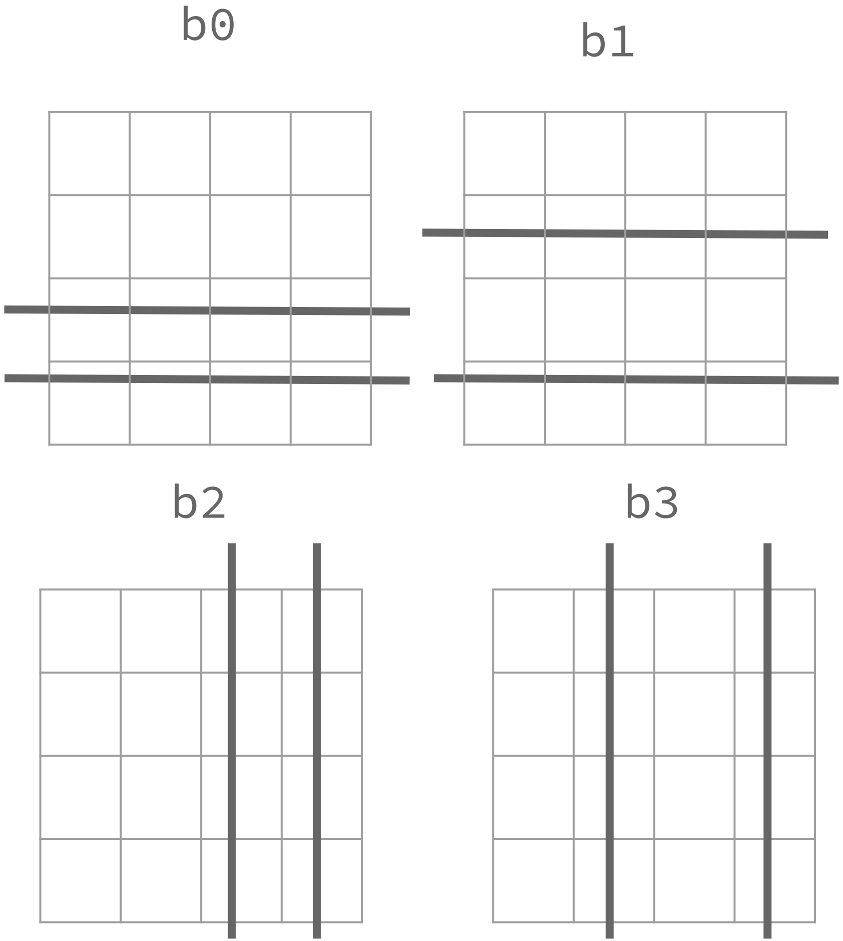
$$0 \oplus 1 = 1 = 1 \oplus 0$$

$$\begin{array}{ccccc}
 & \text{a0} & \text{a1} & \text{a2} & \text{a3} \\
\oplus & \text{b0} & \text{b1} & \text{b2} & \text{b3} \\
\hline
 & \text{a0}\oplus\text{b0} & \text{a1}\oplus\text{b1} & \text{a2}\oplus\text{b2} & \text{a3}\oplus\text{b3}
\end{array}$$

Ans: a0⊕c0 a1⊕c1 a2⊕c2 a3⊕c3

```
Step 2: Find position to switch
    such that grid now
    corresponds to c0 c1 c2 c3
```

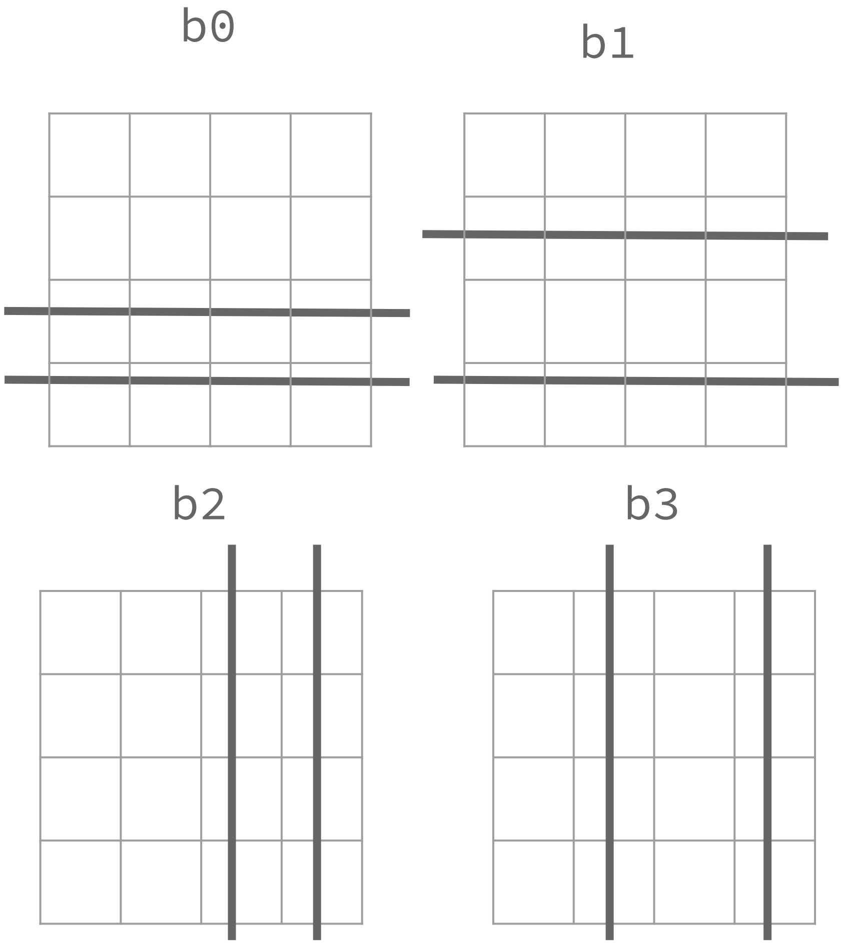
Step 2: Find position to switch
    such that grid now
    corresponds to c0 c1 c2 c3



Step 2: Find position to switch such that grid now corresponds to c0 c1 c2 c3

1 : One of the marked grid points must be switched.

0 : None of the marked grid points must be switched.

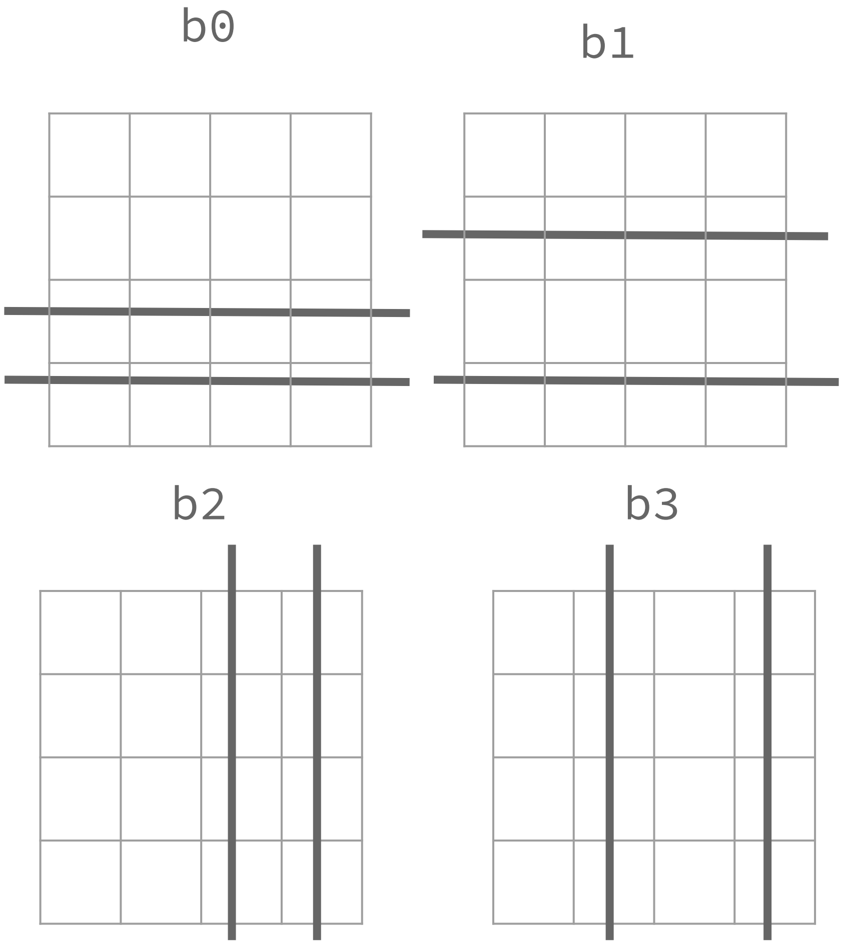


Step 2: Find position to switch such that grid now corresponds to c0 c1 c2 c3

1 : One of the marked grid points must be switched.

0 : None of the marked grid points must be switched.

0000	0001	0010	0011
0100	0101	0110	0111
1000	1001	1010	1011
1100	1101	1110	1111



Coding Theory

Corruption of Data

- Weak Signal
- Cables affected
- Damaged SD Card

Coding Theory

Corruption of Data

- Weak Signal
- Cables affected
- Damaged SD Card

Corruption can happen...

Either because the channel
is affected

Or damage occurs over time.

Coding Theory

Reinforcing the Data to handle corruption

Message

Corruption of Data

- Weak Signal
- Cables affected
- Damaged SD Card

Corruption can happen...

Either because the channel is affected

Or damage occurs over time.

Coding Theory

Corruption of Data

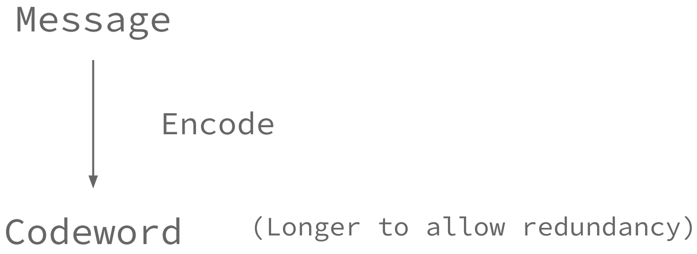
- Weak Signal
- Cables affected
- Damaged SD Card

Corruption can happen...

Either because the channel is affected

Or damage occurs over time.

Reinforcing the Data to handle corruption



Message

Encode

Codeword (Longer to allow redundancy)

Coding Theory

Corruption of Data

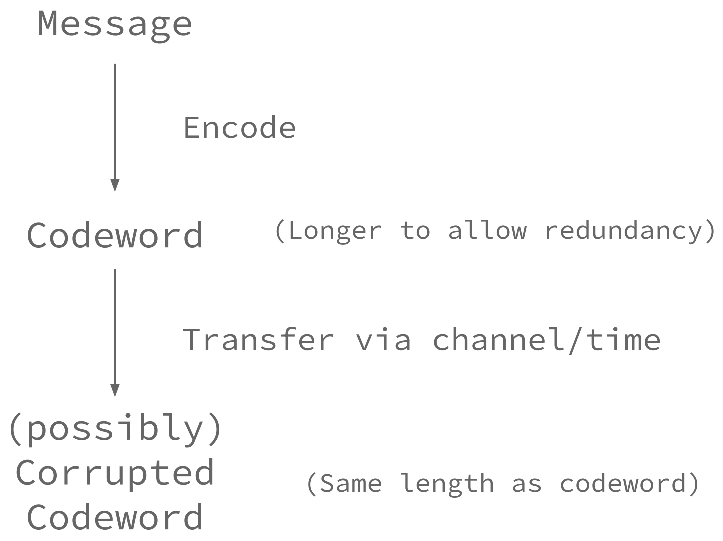
- Weak Signal
- Cables affected
- Damaged SD Card

Corruption can happen...

Either because the channel is affected

Or damage occurs over time.

Reinforcing the Data to handle corruption



Message

Encode

Codeword

(Longer to allow redundancy)

Transfer via channel/time

(possibly) Corrupted Codeword

(Same length as codeword)

Coding Theory

Corruption of Data

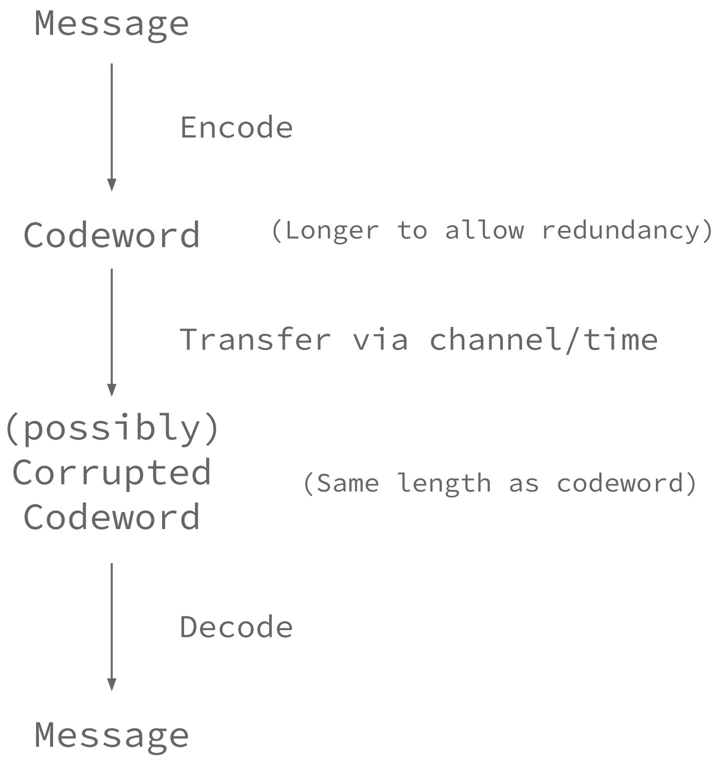
- Weak Signal
- Cables affected
- Damaged SD Card

Corruption can happen...

Either because the channel is affected

Or damage occurs over time.

Reinforcing the Data to handle corruption



Message

Encode

Codeword (Longer to allow redundancy)

Transfer via channel/time

(possibly) Corrupted Codeword (Same length as codeword)

Decode

Message

Coding Theory

Corruption of Data

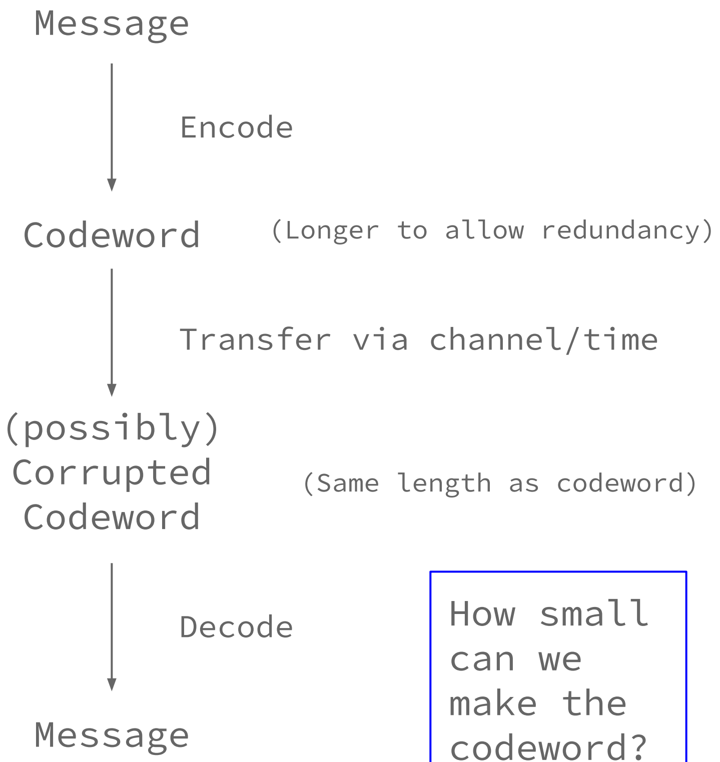
- Weak Signal
- Cables affected
- Damaged SD Card

Corruption can happen...

Either because the channel is affected

Or damage occurs over time.

Reinforcing the Data to handle corruption



Message

Encode

Codeword

(Longer to allow redundancy)

Transfer via channel/time

(possibly) Corrupted Codeword

(Same length as codeword)

Decode

Message

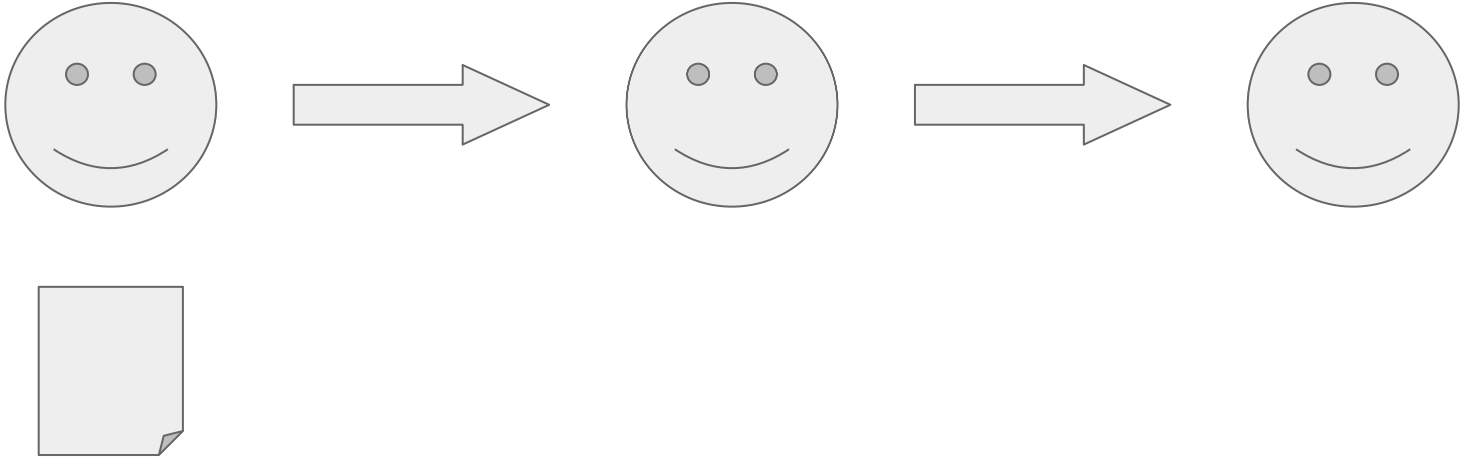
How small can we make the codeword?

Sending Secret Messages!!

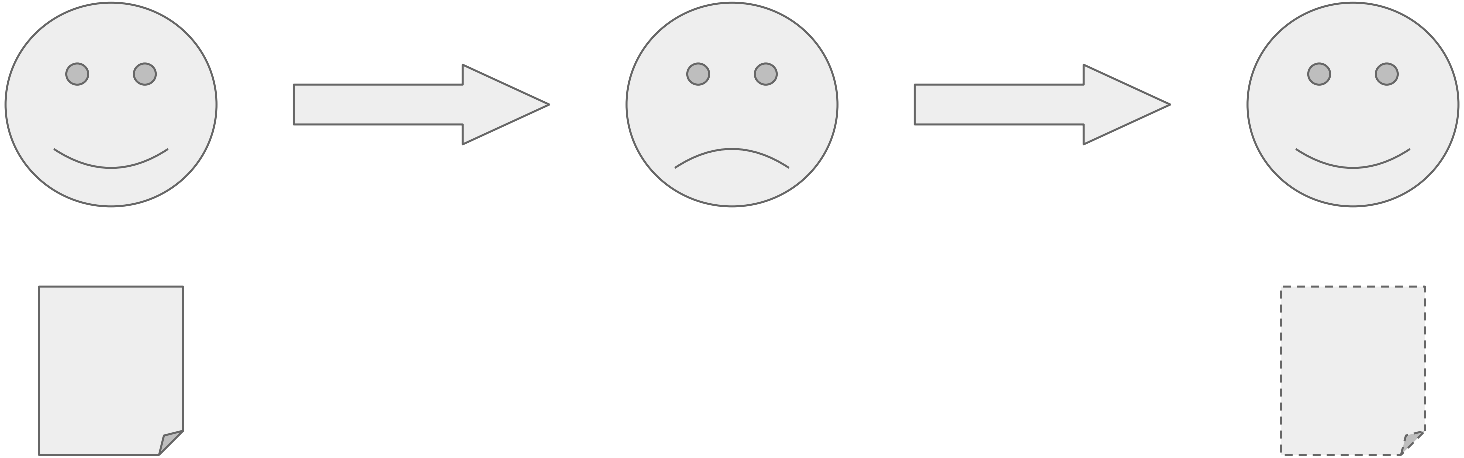
Sending secret messages

Sending secret messages

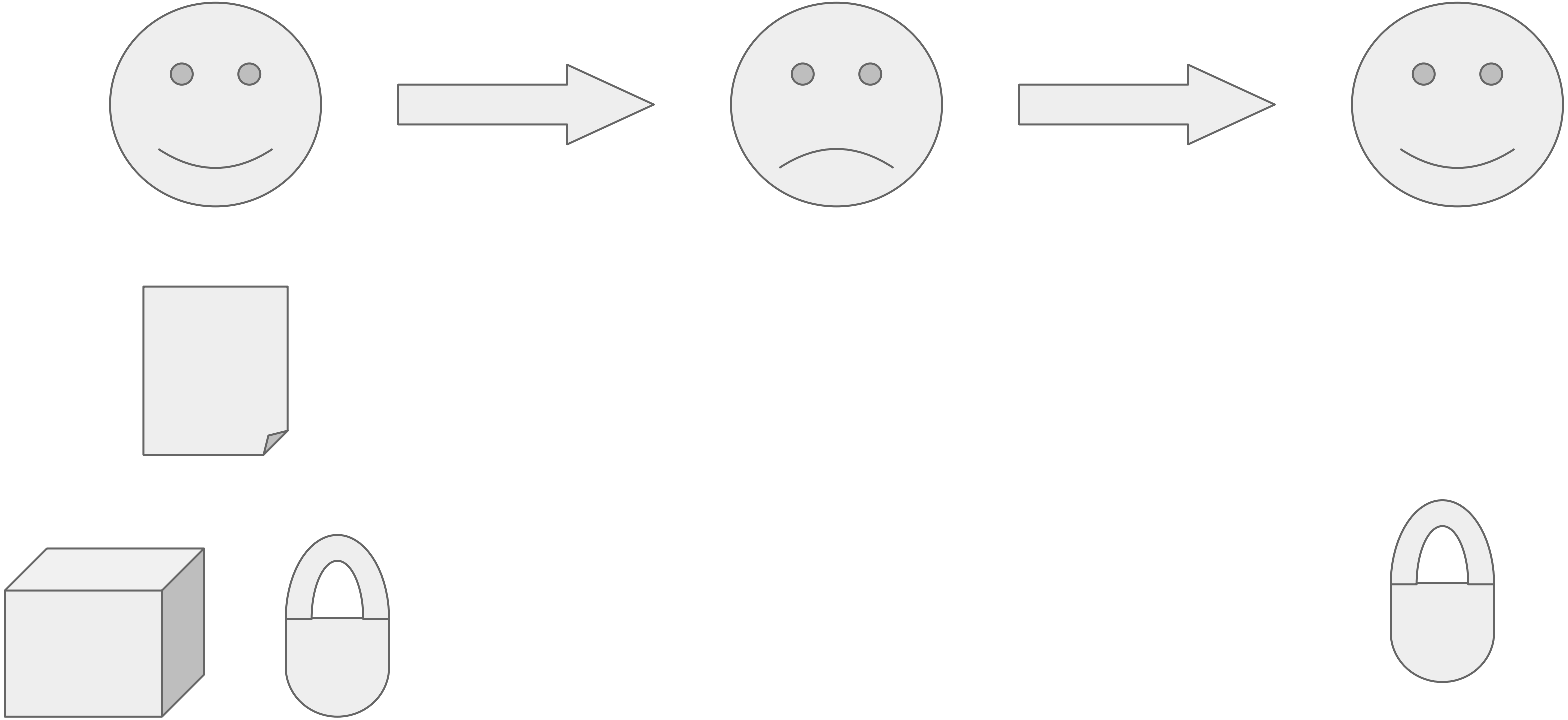
Sending secret messages



Sending secret messages



Sending secret messages



Sending secret messages

- A puts the note in the box and locks it. Gives it to B.

Sending secret messages

- A puts the note in the box and locks it. Gives it to B.
- B gives it to C.

Sending secret messages

- A puts the note in the box and locks it. Gives it to B.
- B gives it to C.
- C adds their lock as well. Gives it to B.

Sending secret messages

- A puts the note in the box and locks it. Gives it to B.
- B gives it to C.
- C adds their lock as well. Gives it to B.
- B gives it to A.

Sending secret messages

- A puts the note in the box and locks it. Gives it to B.
- B gives it to C.
- C adds their lock as well. Gives it to B.
- B gives it to A.
- A removes their lock using their key. Gives it to B.

Sending secret messages

- A puts the note in the box and locks it. Gives it to B.
- B gives it to C.
- C adds their lock as well. Gives it to B.
- B gives it to A.
- A removes their lock using their key. Gives it to B.
- B gives it to C.

Sending secret messages

- A puts the note in the box and locks it. Gives it to B.
- B gives it to C.
- C adds their lock as well. Gives it to B.
- B gives it to A.
- A removes their lock using their key. Gives it to B.
- B gives it to C.
- C unlocks their lock using their key to reveal note.

Sending secret messages

- A puts the note in the box and locks it. Gives it to B.
- B gives it to C.
- C adds their lock as well. Gives it to B.
- B gives it to A.
- A removes their lock using their key. Gives it to B.
- B gives it to C.
- C unlocks their lock using their key to reveal note.

This protocol is secure assuming B does not have any equipment to break the lock.

Cryptography

When one is setting up any kind of password:

- UPI Pin
- GMail Password
- Netbanking Password

Cryptography

When one is setting up any kind of password:

- UPI Pin
- GMail Password
- Netbanking Password

Or when two parties are communicating for the first time and want to set up a “secure” line..

Cryptography

When one is setting up any kind of password:

- UPI Pin
- GMail Password
- Netbanking Password

Or when two parties are communicating for the first time and want to set up a “secure” line..

They use the “Diffie Helman Key Exchange Protocol”.

Cryptography

When one is setting up any kind of password:

- UPI Pin
- GMail Password
- Netbanking Password

Or when two parties are communicating for the first time and want to set up a “secure” line..

They use the “Diffie Helman Key Exchange Protocol”.

Diffie-helman key exchange

F : Easy to compute but hard to invert function

In real-life: F ≡ Multiplying 2 large Prime Numbers

Cryptography

When one is setting up any kind of password:

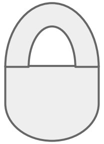
- UPI Pin
- GMail Password
- Netbanking Password

Or when two parties are communicating for the first time and want to set up a “secure” line..

They use the “Diffie Helman Key Exchange Protocol”.

Q: How to communicate via a messenger you don’t trust?

Diffie-helman key exchange



F : Easy to compute but hard to invert function

In real-life: F ≡ Multiplying 2 large Prime Numbers

Cryptography

When one is setting up any kind of password:

- UPI Pin
- GMail Password
- Netbanking Password

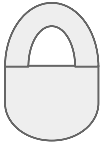
Or when two parties are communicating for the first time and want to set up a “secure” line..

They use the “Diffie Helman Key Exchange Protocol”.

Q: How to communicate via a messenger you don’t trust?

Ans: Encryption and Decryption !!

Diffie-Helman Key Exchange



F : Easy to compute but hard to invert function

In real-life: F ≡ Multiplying 2 large Prime Numbers

Cryptography

When one is setting up any kind of password:

- UPI Pin
- GMail Password
- Netbanking Password

Or when two parties are communicating for the first time and want to set up a “secure” line..

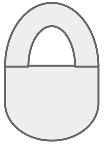
They use the “Diffie Helman Key Exchange Protocol”.

Q: How to communicate via a messenger you don’t trust?

Ans: Encryption and Decryption !!

Alter the message to make it look meaningless in such a way that if you have the “key” you can “decrypt”

Diffie-Helman Key Exchange



F : Easy to compute but hard to invert function

In real-life: F ≡ Multiplying 2 large Prime Numbers

BACKUP GAMES

Using Probabilities

Interactive Proofs

How does one make sure that those claiming to be experts are actually so?

Keep asking questions till you are (almost) sure... :)

Using Probabilities

Interactive Proofs

How does one make sure that those claiming to be experts are actually so?

Keep asking questions till you are (almost) sure... :)

Secure Computation

How does one solve a problem as a team when no one trusts anyone?

Ensuring Privacy: Don’t reveal anything more than necessary.

Using Probabilities

Interactive Proofs

How does one make sure that those claiming to be experts are actually so?

Keep asking questions till you are (almost) sure... :)

Secure Computation

How does one solve a problem as a team when no one trusts anyone?

Ensuring Privacy: Don’t reveal anything more than necessary.

These can’t be done always.
The question is for what problems can these be done?

Understanding ChatGPT

Large Language Models

ChatGPT etc. is NOT magic!

It is JUST statistics!!

Large Language Models

ChatGPT etc. is NOT magic!

It is JUST statistics!!

It is JUST a “next word predictor”!

Large Language Models

ChatGPT etc. is NOT magic!

It is JUST statistics!!

It is JUST a “next word predictor”!

So you CAN NOT blindly trust what it outputs.

You MUST verify always!

Large Language Models

ChatGPT etc. is NOT magic!

It is JUST statistics!!

It is JUST a “next word predictor”!

So you CAN NOT blindly trust what it outputs.

You MUST verify always!

Based on the “training data”,

Large Language Models

ChatGPT etc. is NOT magic!

It is JUST statistics!!

It is JUST a “next word predictor”!

So you CAN NOT blindly trust what it outputs.

You MUST verify always!

Based on the “training data”,

Assign probabilities to “What the next word should be?” given the previous (few) words.

Large Language Models

ChatGPT etc. is NOT magic!

It is JUST statistics!!

It is JUST a “next word predictor”!

So you CAN NOT blindly trust what it outputs.

You MUST verify always!

Based on the “training data”,

Assign probabilities to “What the next word should be?” given the previous (few) words.

Simplest: Output the word with highest probability.

Large Language Models

ChatGPT etc. is NOT magic!

It is JUST statistics!!

It is JUST a “next word predictor”!

So you CAN NOT blindly trust what it outputs.

You MUST verify always!

Based on the “training data”,

Assign probabilities to “What the next word should be?” given the previous (few) words.

Simplest: Output the word with highest probability.

Improved:

- Output words depending on their probabilities (along with a other factors).
- Update factors using feedback.

Theoretical Computer Science

- A Problem that needs to be solved.

- A Problem that needs to be solved.
- A Mathematical Model that describes the abilities/restrictions of the solver.

- A Problem that needs to be solved.
- A Mathematical Model that describes the abilities/restrictions of the solver.

Study the amount of resources needed by the model to solve the problem.

Higher Studies in Math/CS theory

Exams and Institutes

Undergraduate Level

- JEE (IISc, IITs & NITs)
- CMI
- ISI
- IAT (IISERs)
- NEST (NISER and CEBS)

Graduate Level (PhD/Int. PhD)

- NET
- GATE
- JEST
- TIFR-GS
- NBHM

TIFR, IISc, CMI, ISI, HRI, NISER, ISI, IISERs, IITs.

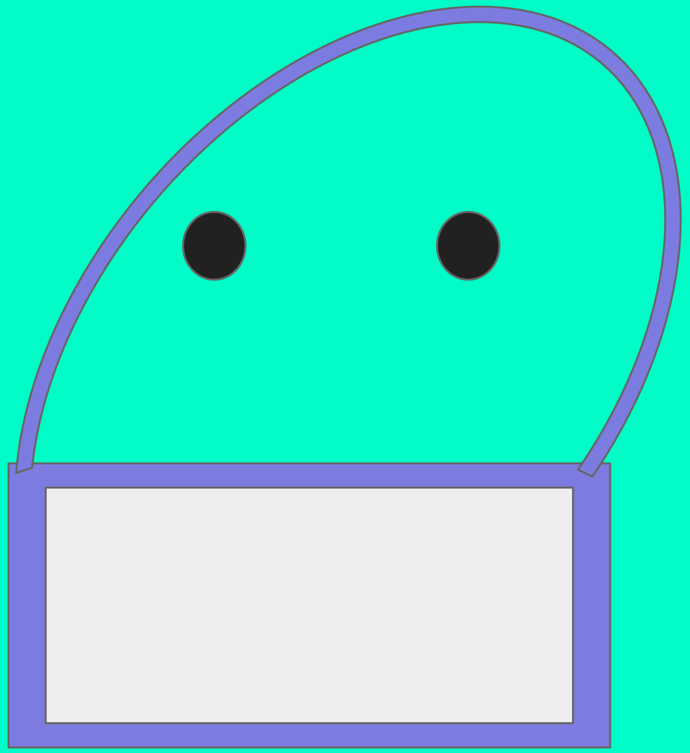
Master's Level

- JAM (for MSc in IISc, IITs & NITs)
- GATE (for MTech in IITs and NITs)

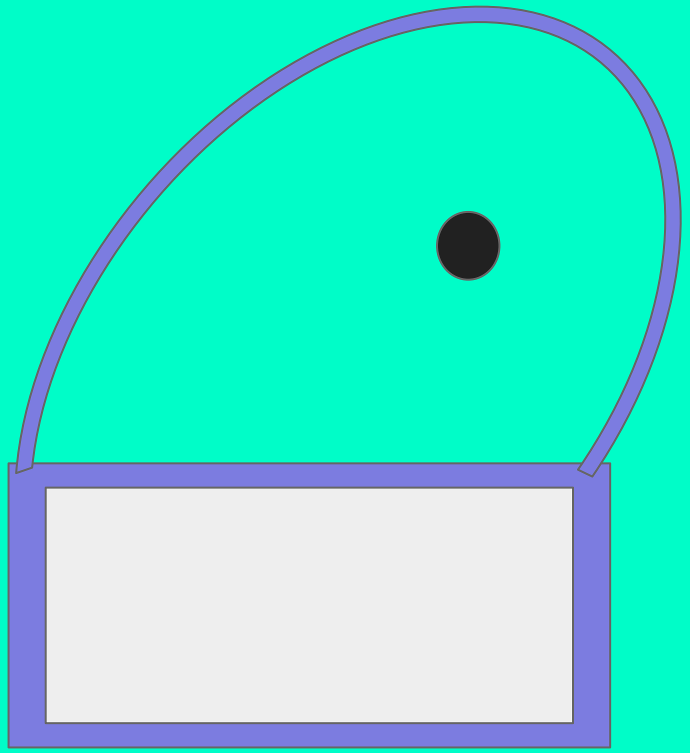
- CMI
- ISI

Just One More Puzzle...

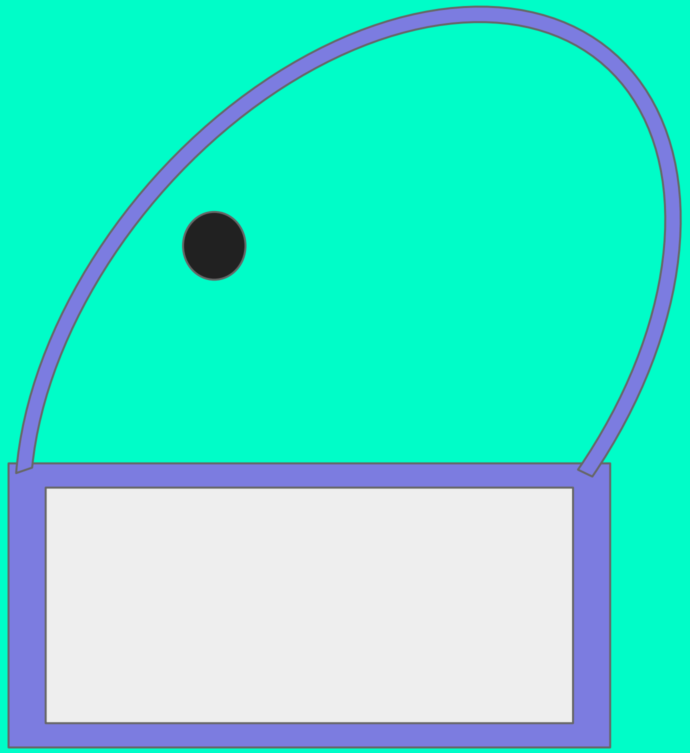
The Picture Hanging Puzzle



The Picture Hanging Puzzle

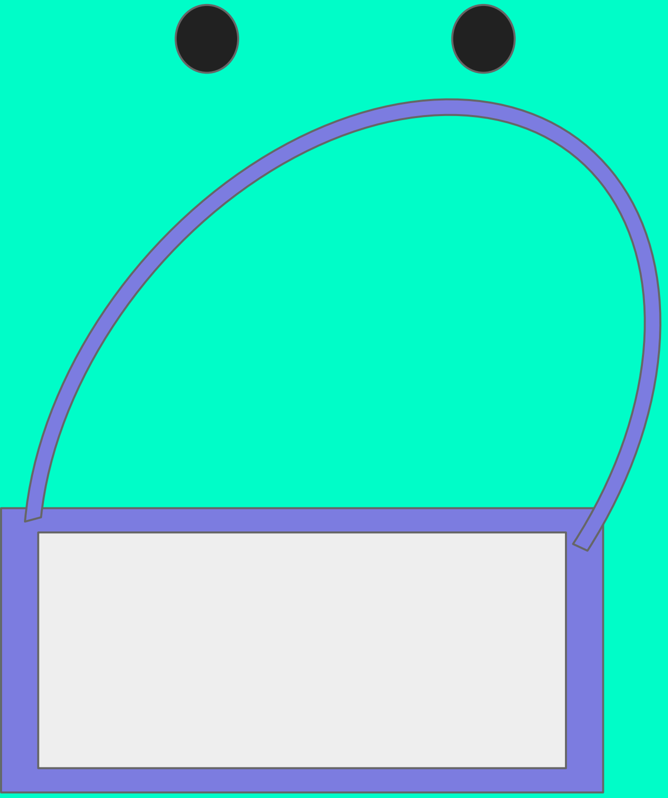


The Picture Hanging Puzzle



The Picture Hanging Puzzle

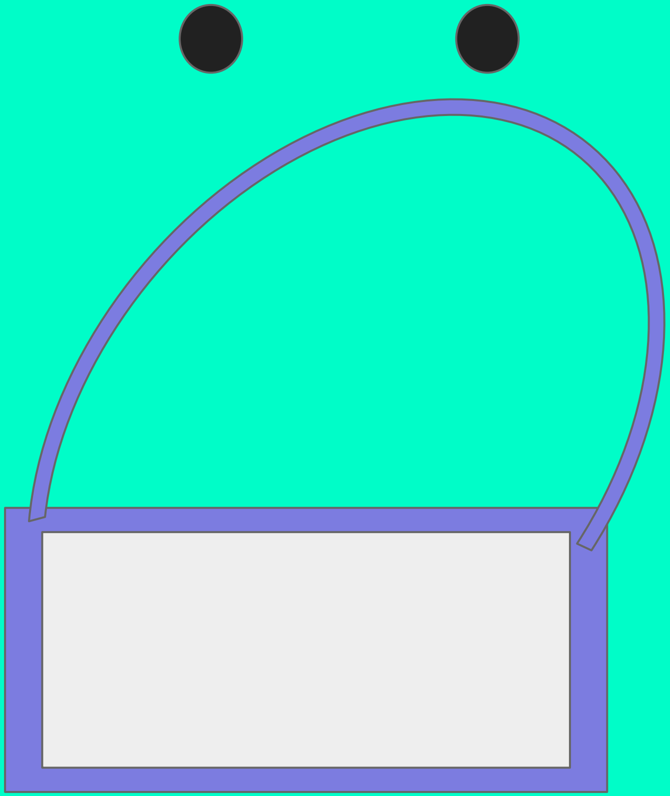
Hang the picture such that:



The Picture Hanging Puzzle

Hang the picture such that:

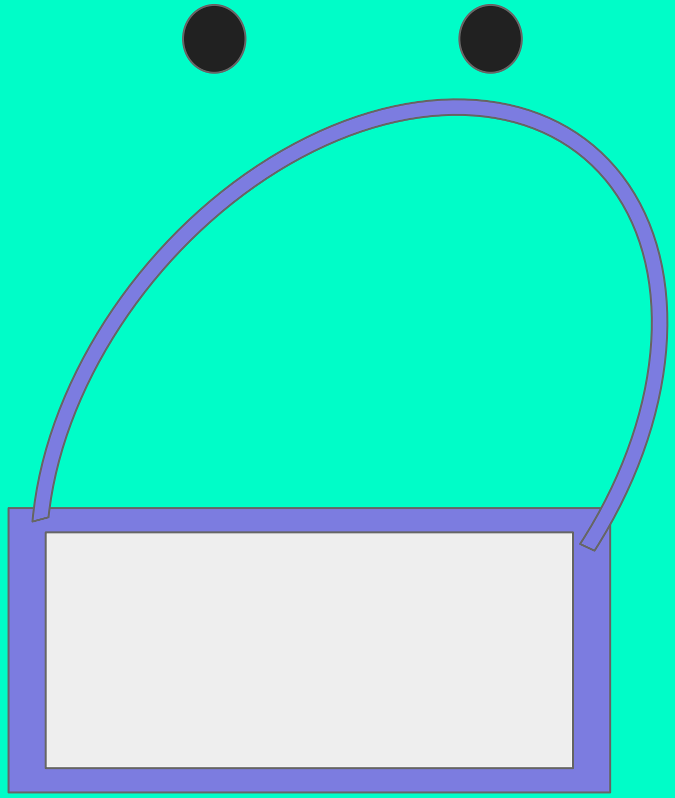
- If both the pegs are there, then the picture will stay.



The Picture Hanging Puzzle

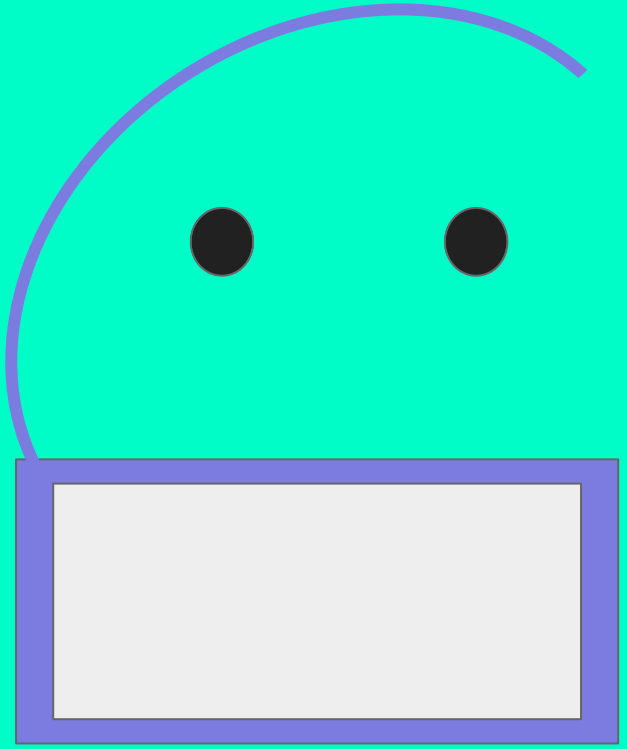
Hang the picture such that:

- If both the pegs are there, then the picture will stay.
- If either one of pegs are taken off, the picture will fall.



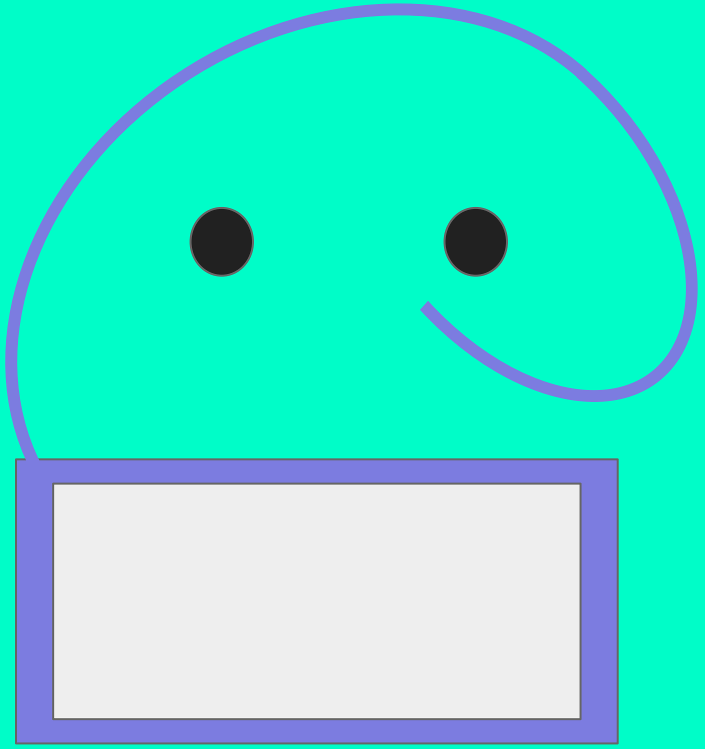
The Picture Hanging Puzzle

Solution: **A**



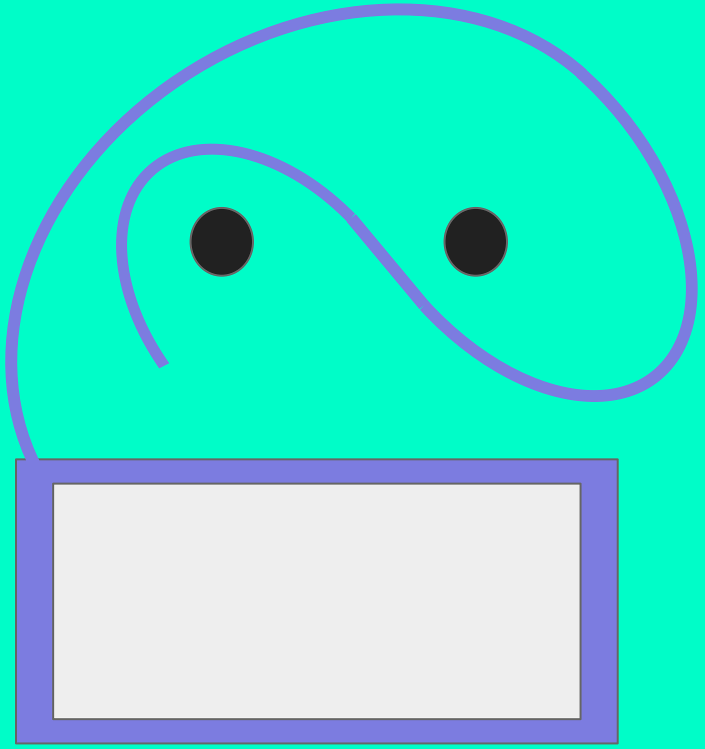
The Picture Hanging Puzzle

Solution: **AB**



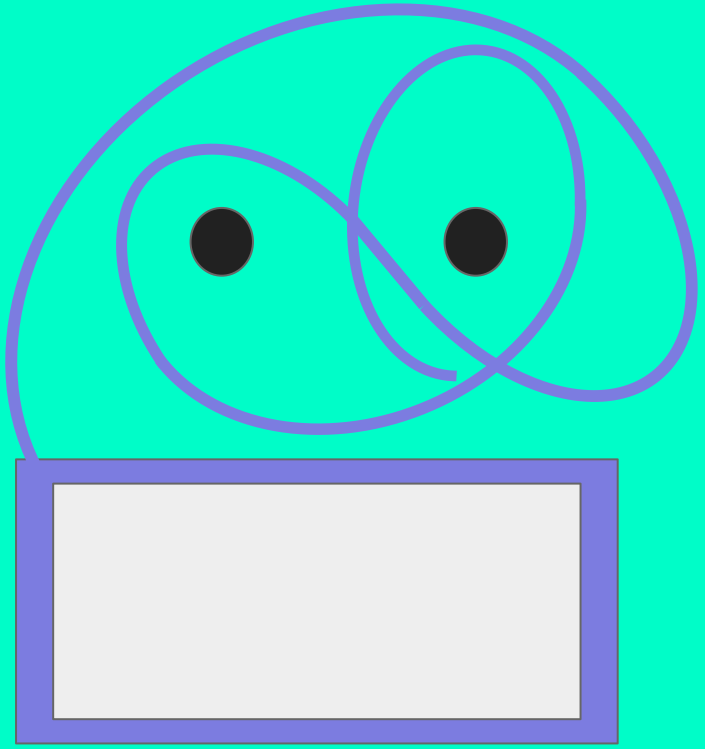
The Picture Hanging Puzzle

Solution: ABA^{-1}



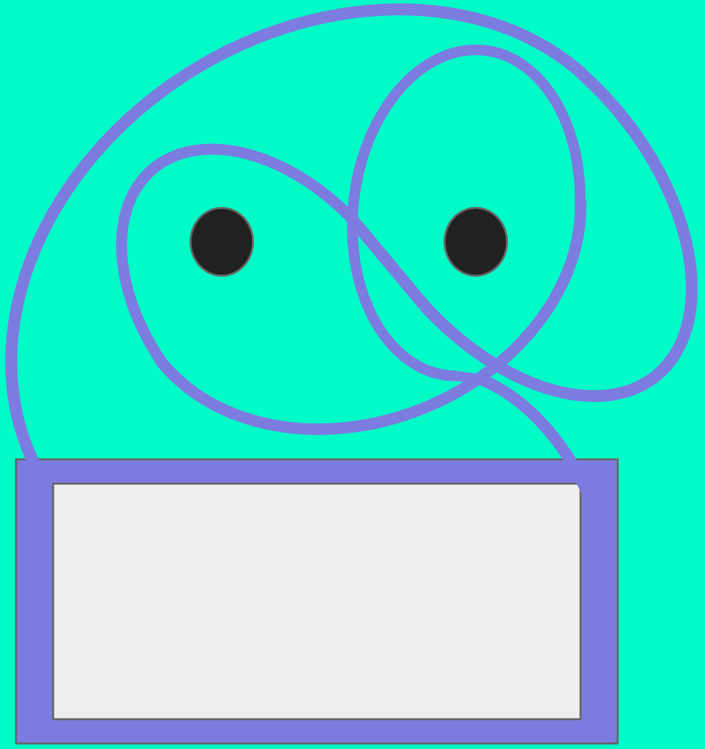
The Picture Hanging Puzzle

Solution: **$ABA^{-1}B^{-1}$**



The Picture Hanging Puzzle

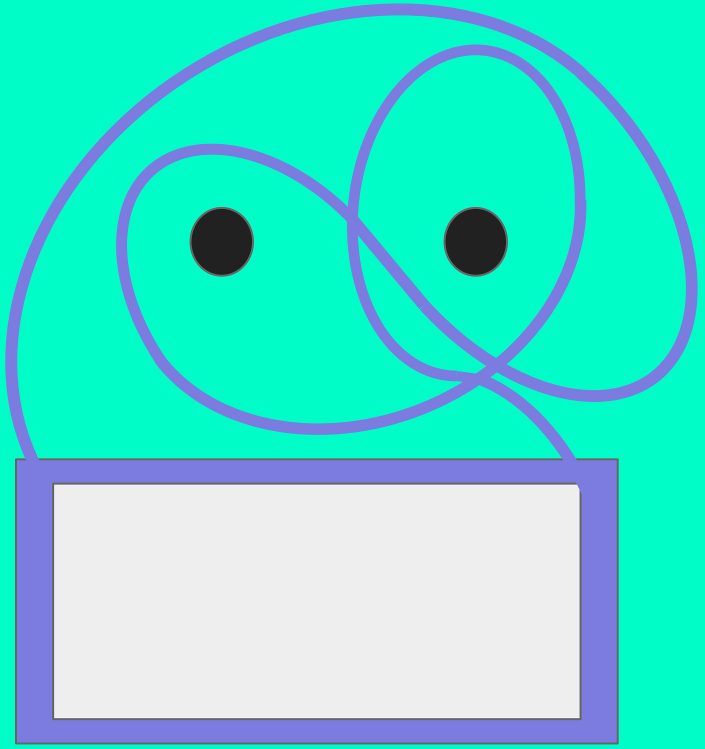
Solution: $\mathbf{ABA^{-1}B^{-1}}$



The Picture Hanging Puzzle

Solution: $ABA^{-1}B^{-1}$

COMMUTATORS



Commutators

- Central concept in Galois Theory.

Commutators

- Central concept in Galois Theory.
- Solving a Rubik’s Cube.

Commutators

- Central concept in Galois Theory.
- Solving a Rubik’s Cube.
- Proving that Quintic equations have no closed form solutions.

Commutators

- Central concept in Galois Theory.
- Solving a Rubik’s Cube.
- Proving that Quintic equations have no closed form solutions.
- Proving that a regular heptagon can not be constructed using only a compass and a ruler.

Commutators

- Central concept in Galois Theory.
- Solving a Rubik’s Cube.
- Proving that Quintic equations have no closed form solutions.
- Proving that a regular heptagon can not be constructed using only a compass and a ruler.
- Proving the algebraic formulas are equivalent to width-3 algebraic branching programs.

Commutators

- Central concept in Galois Theory.
- Solving a Rubik’s Cube.
- Proving that Quintic equations have no closed form solutions.
- Proving that a regular heptagon can not be constructed using only a compass and a ruler.
- Proving the algebraic formulas are equivalent to width-3 algebraic branching programs.

Check out: Chai and Why?(Dec 20, 2020) by Ramprasad Saptharishi

“Commutators! Hanging pictures and solving Rubik’s Cube”

THANK YOU !

prerona.ch @ gmail.com https://preronac.bitbucket.io/