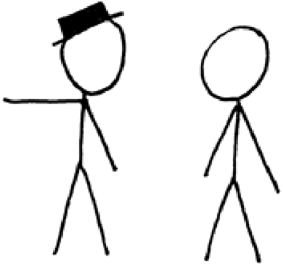
The PCP Theorem
or
How to Catch a Cheat, Efficiently

Chethan Kamath

IST Austria

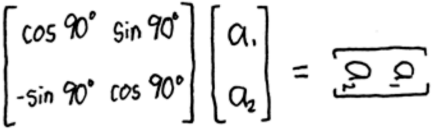
May 29, 2015

Blackhat (the cheat) and Cueball*



*Adaptation of *Miniature 11* by Matoušek. Cast: xkcd.com

Motivation: Modelling Homework

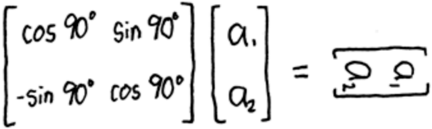


Motivation: Modelling Homework

$$\begin{bmatrix} \cos 90^\circ & \sin 90^\circ \\ -\sin 90^\circ & \cos 90^\circ \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} a_2 & a_1 \end{bmatrix}$$

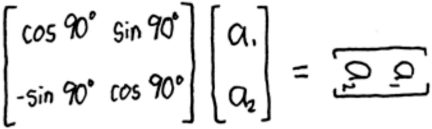
- Cueball: compute **AB** for matrices **A** and **B**

Motivation: Modelling Homework



- Cueball: compute **AB** for matrices **A** and **B**
- If **A** and **B** are $10^4 \times 10^4$
  - Naïve algorithm: $\approx 10^{12}$ steps

Motivation: Modelling Homework

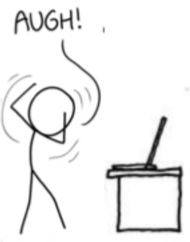


- Cueball: compute $\mathbf{AB}$ for matrices $\mathbf{A}$ and $\mathbf{B}$
- If $\mathbf{A}$ and $\mathbf{B}$ are $10^4 \times 10^4$
  - Naïve algorithm: $\approx 10^{12}$ steps
  - Best known algorithm: $\gg 2 \times 10^{12}$ steps!

Motivation: Modelling Homework

$$\begin{bmatrix}\cos 90^\circ & \sin 90^\circ \\ -\sin 90^\circ & \cos 90^\circ\end{bmatrix}\begin{bmatrix}a_1 \\ a_2\end{bmatrix} = \boxed{a_2 \quad a_1}$$

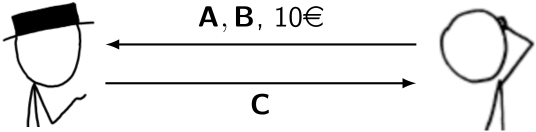
- Cueball: compute $\mathbf{AB}$ for matrices $\mathbf{A}$ and $\mathbf{B}$
- If $\mathbf{A}$ and $\mathbf{B}$ are $10^4 \times 10^4$
  - Naïve algorithm: $\approx 10^{12}$ steps
  - Best known algorithm: $\gg 2 \times 10^{12}$ steps!
  - Takes Cueball $\approx$ 15 minutes on his Mac



Blackhat: I can do it faster!

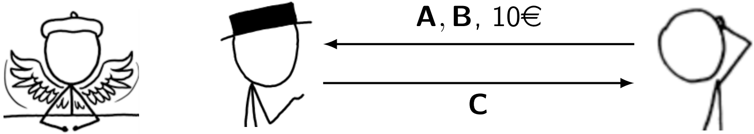
- Blackhat: I can do it in 1 minute for 10€

Blackhat: I can do it faster!



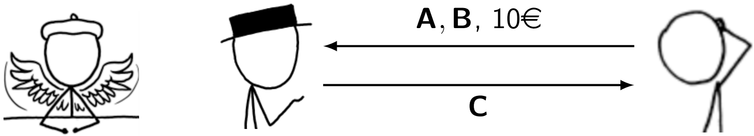
- Blackhat: I can do it in 1 minute for 10€

Blackhat: I can do it faster!



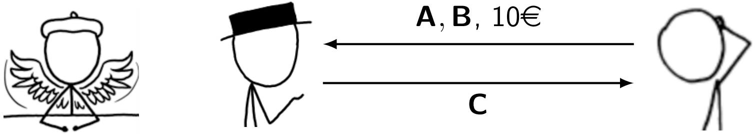
- Blackhat: I can do it in 1 minute for 10€

Blackhat: I can do it faster!



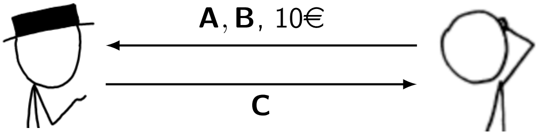
- Blackhat: I can do it in 1 minute for 10€
- Can Cueball verify that **C** is the correct answer?
  - Naïve way: compute **AB** on his Mac and *compare* to **C**
  - Defeats the purpose: it takes 15 minutes

Blackhat: I can do it faster!

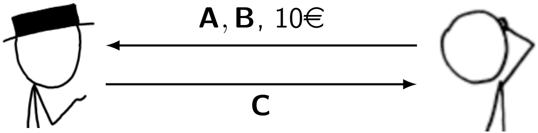


- Blackhat: I can do it in 1 minute for 10€
- Can Cueball verify that $\mathbf{C}$ is the correct answer?
  - Naïve way: compute $\mathbf{AB}$ on his Mac and *compare* to $\mathbf{C}$
  - Defeats the purpose: it takes 15 minutes
- Can Cueball verify efficiently (say < 1 minute)?

Solution: Randomness†



Solution: Randomness†

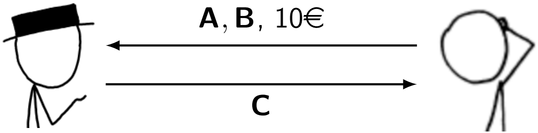


pick random $\mathbf{r}$

$$\mathbf{A}(\mathbf{B}\mathbf{r}) \stackrel{?}{=} \mathbf{C}\mathbf{r}$$

† Freivalds' algorithm

Solution: Randomness[†]



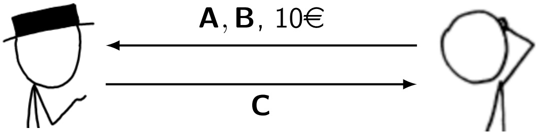
pick random $\mathbf{r}$

$$\mathbf{A}(\mathbf{B}\mathbf{r}) \stackrel{?}{=} \mathbf{C}\mathbf{r}$$

- Takes < 1 second on his Mac!

[†] Freivalds' algorithm

Solution: Randomness[†]



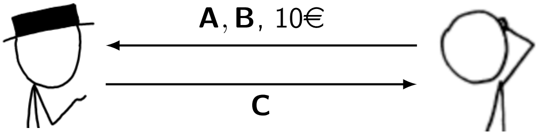
pick random $\color{blue}{\mathbf{r}}$

$\mathbf{A}(\mathbf{B}\mathbf{r}) \stackrel{?}{=} \mathbf{C}\mathbf{r}$

- Takes $<$ 1 second on his Mac!
- Fact: If $\mathbf{C} \neq \mathbf{AB}$ then $\mathbf{A}(\mathbf{Br}) \neq \mathbf{Cr}$ with probability $\geq 1/2$

[†] Freivalds' algorithm

Solution: Randomness[†]



pick random $\mathbf{r}$

$$\mathbf{A}(\mathbf{B}\mathbf{r}) \stackrel{?}{=} \mathbf{C}\mathbf{r}$$

- Takes < 1 second on his Mac!
- Fact: If $\mathbf{C} \neq \mathbf{AB}$ then $\mathbf{A}(\mathbf{B}\mathbf{r}) \neq \mathbf{C}\mathbf{r}$ with probability $\geq 1/2$
- Repeat with $\mathbf{r}_1, \ldots, \mathbf{r}_q$ for more confidence

[†]Freivalds' algorithm

Generalisation: PCP Theorem[‡]

- Substitute matrix multiplication $\rightarrow$ any effectively solvable computational problem

[‡] Arora and Safra, 1998

Generalisation: PCP Theorem[‡]

- Substitute matrix multiplication $\rightarrow$ any effectively solvable computational problem

- **P**robablistically **c**heckable **p**roofs (PCP)
- PCP Theorem: *solution to any effectively solvable problem, can be verified randomly in a relatively short time*
  - $\mathsf{NP} = \mathsf{PCP}[\log, 1]$

[‡] Arora and Safra, 1998

Generalisation: PCP Theorem[‡]

- Substitute matrix multiplication $\rightarrow$ any effectively solvable computational problem

- **P**robablistically **c**heckable **p**roofs (PCP)
- PCP Theorem: *solution to any effectively solvable problem, can be verified randomly in a relatively short time*
  - $\mathrm{NP} = \mathrm{PCP}[\log, 1]$

- Intuition: verify random parts of the solution

[‡] Arora and Safra, 1998

Moral of the Story

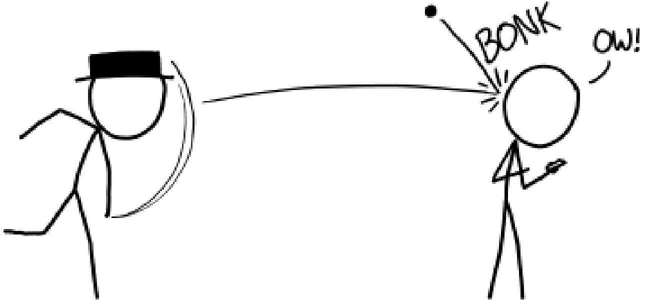
- Randomness is a powerful resource
  - Verify computation

Moral of the Story

- Randomness is a powerful resource
  - Verify computation
  - Cryptography

Moral of the Story

- Randomness is a powerful resource
  - Verify computation
  - Cryptography
- Don't trust people wearing hats!



Thank you!