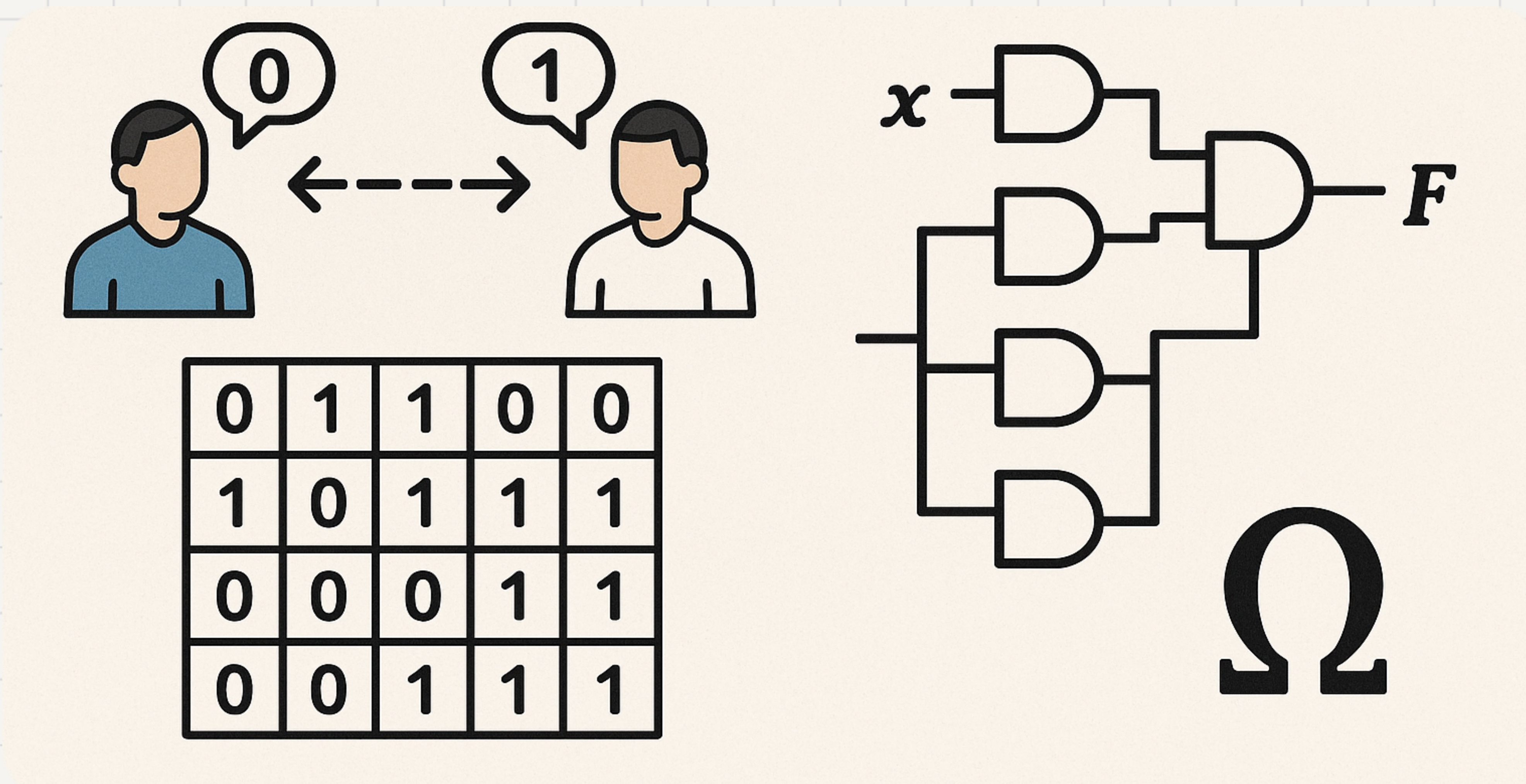
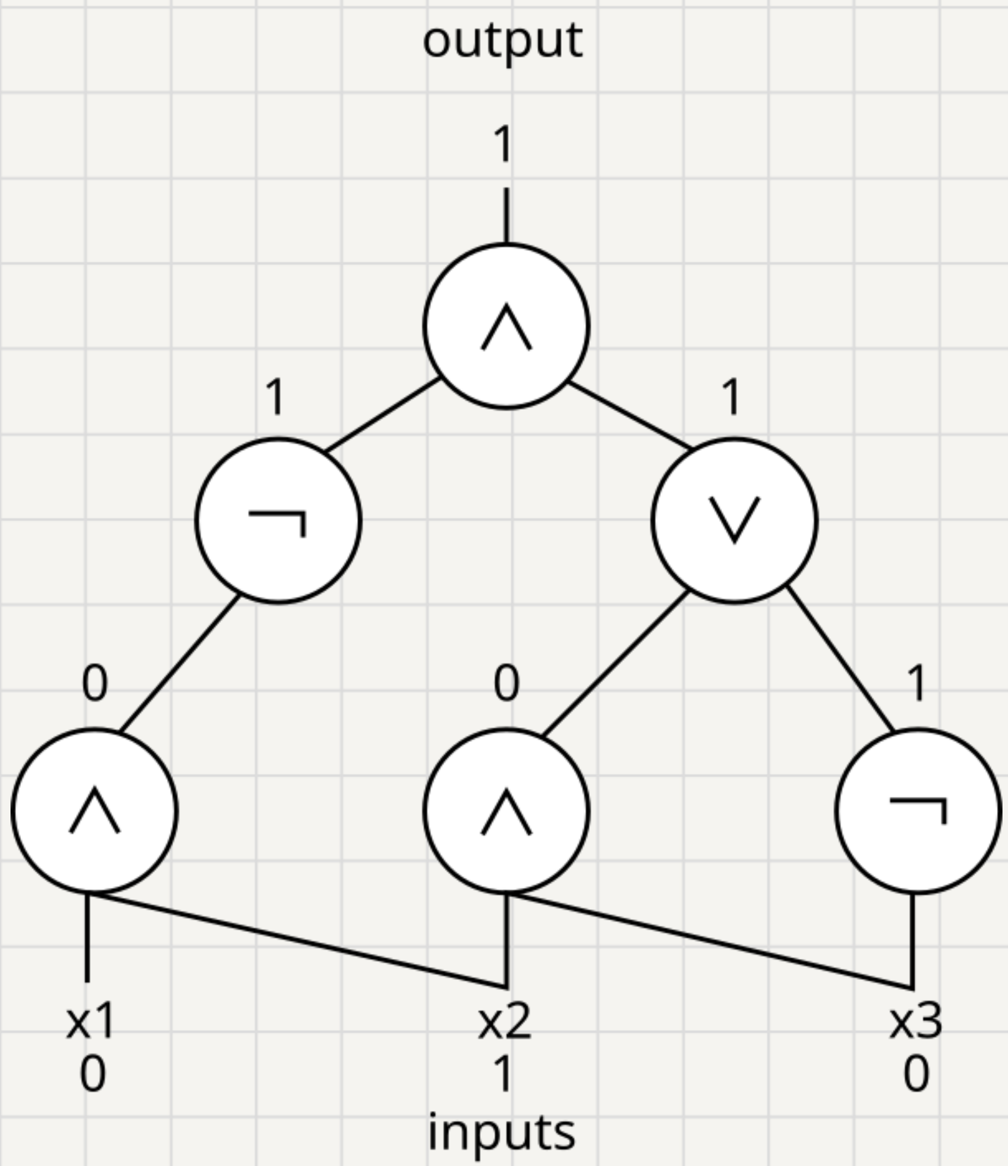
Complexity Theory



Circuits & Communication

Circuit complexity



To solve a problem L, we need a family $\{C_n\}_{n\in\mathbb{N}}$ for each input length.

The class P/Poly consists of all problems solved by poly-size circuits.

Is this model equivalent to poly-time Turing machines?

P/Poly and advice

Interestingly P/Poly is **not equal** to P!

In fact, in contains **undecidable** problems...

Note that P/Poly is **not uniform**: Each C_n could be completely different!

Put differently: P/Poly = poly-time TM with **polynomial-size advice**

For every input size $n \in \mathbb{N}$ we can store advice string $a_n \in \{0,1\}^{p(n)}$

If the problem is encoded in unary, we can just write the answer!

Randomised circuits

Unlike P vs BPP, for circuits randomness doesn't matter!

We can use the advice to **derandomise** the circuit.

Suppose we have $\Pr_r[C_n(x;r) = 1_L(x)] \geq 2/3$.

Idea: provide a good random string as advice.

Problem: for every x, there might be different good string.

Solution: Use Chernoff to reduce the soundness to $\epsilon = 1/2^{n+2}$,

For every $x \in \{0,1\}^n$, $\quad \Pr_r[C_n(x;r) \neq 1_L(x)] \leq \epsilon$

Hence, $\Pr_r[\exists x\ C_n(x;r) \neq 1_L(x)] \leq 2^n \Pr_r[C_n(x;r) \neq 1_L(x)] \leq 1/4$

That is, w.p. 3/4 there exists r s.t. for every $x \in \{0,1\}^n$, $C_n(x;r) = 1_L(x)$

Communication complexity

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

Goal: compute $f(x, y)$ using a minimal amount of communication.

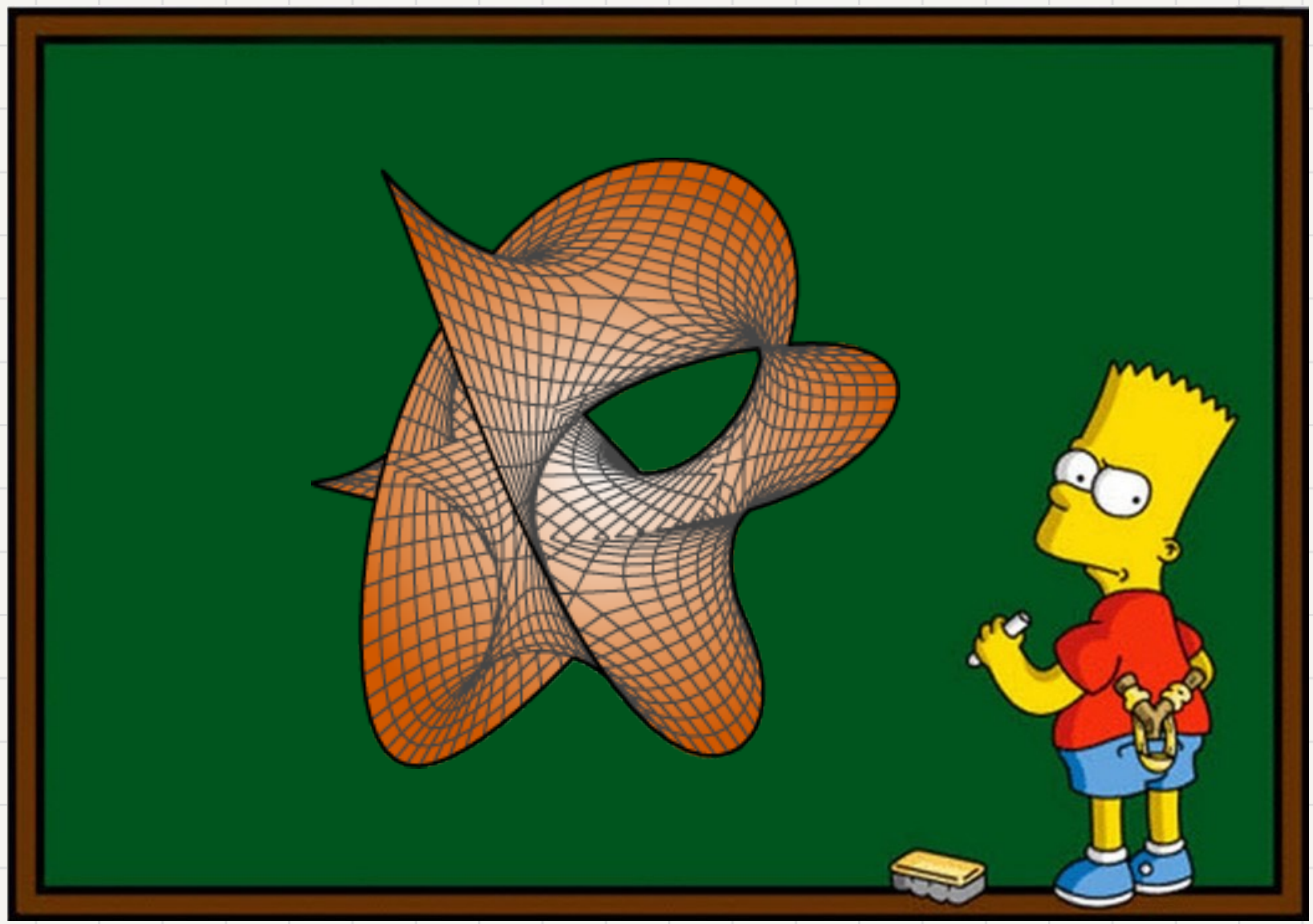
Test your intuition

$$f(x, y) = \text{gcd}(x, y)$$

$$f(x, y) = \text{parity}(x \circ y)$$

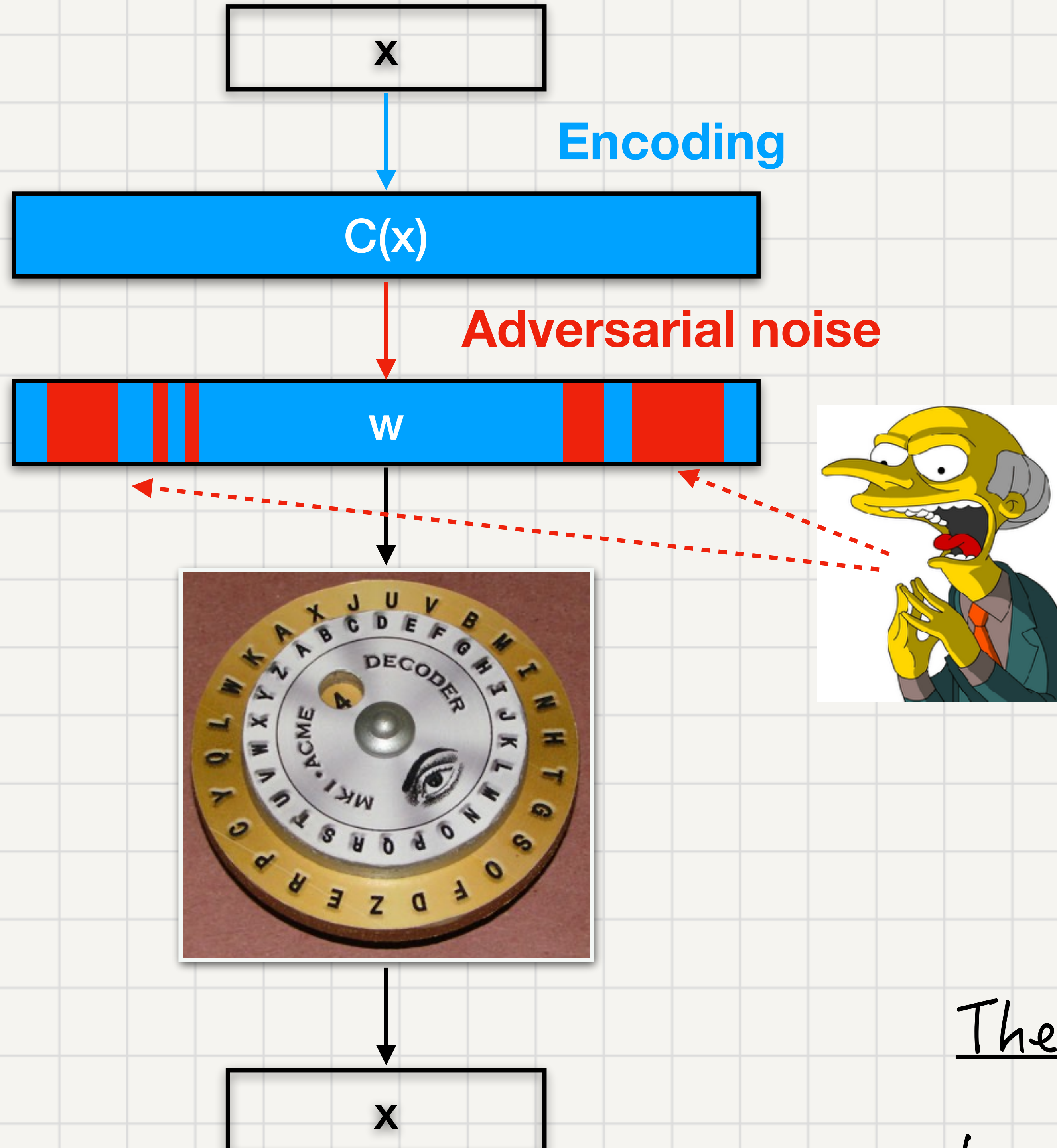
$$f(x, y) = \text{equal}(x, y)$$

Detour: error-correcting codes in a nutshell

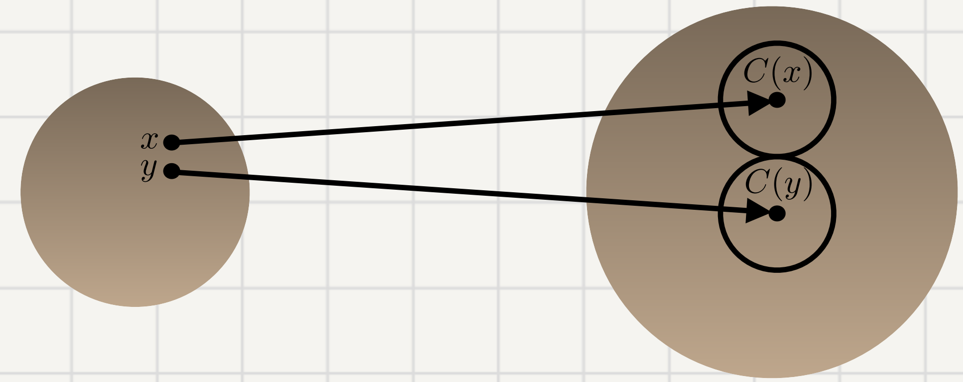


Error-correcting codes

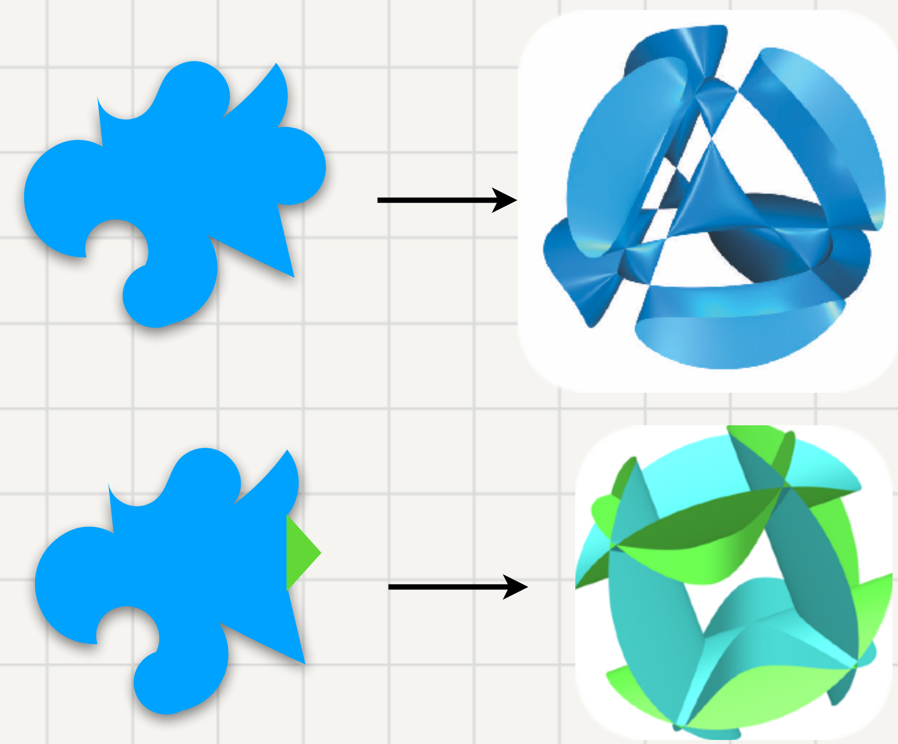
What?



How? $C : \Sigma^k \to \Sigma^n$



C(x) is δ-far from C(y), for all x≠y



Theorem There exists a code C with length $n = O(k)$ and distance $\delta = \Omega(n)$

Communication complexity

$x \in \{0,1\}^n$ $y \in \{0,1\}^n$

Goal: compute $equal(x, y)$ using a minimal amount of communication.

Protocol: Let a C be a code with length $n = O(k)$ and distance $\delta = \Omega(n)$

Alice computes $C(x)$ Bob computes $C(y)$

Alice and bob choose a random $S \subset \{1,\ldots,n\}$ of size $O(1/\delta)$

They accept iff $x|_S = y|_S$ (communication $O(\log n)$)

Note that if $x \neq y$, then $\Pr_i[C(x)_i \neq C(y)_i] \geq \delta$

Questions?