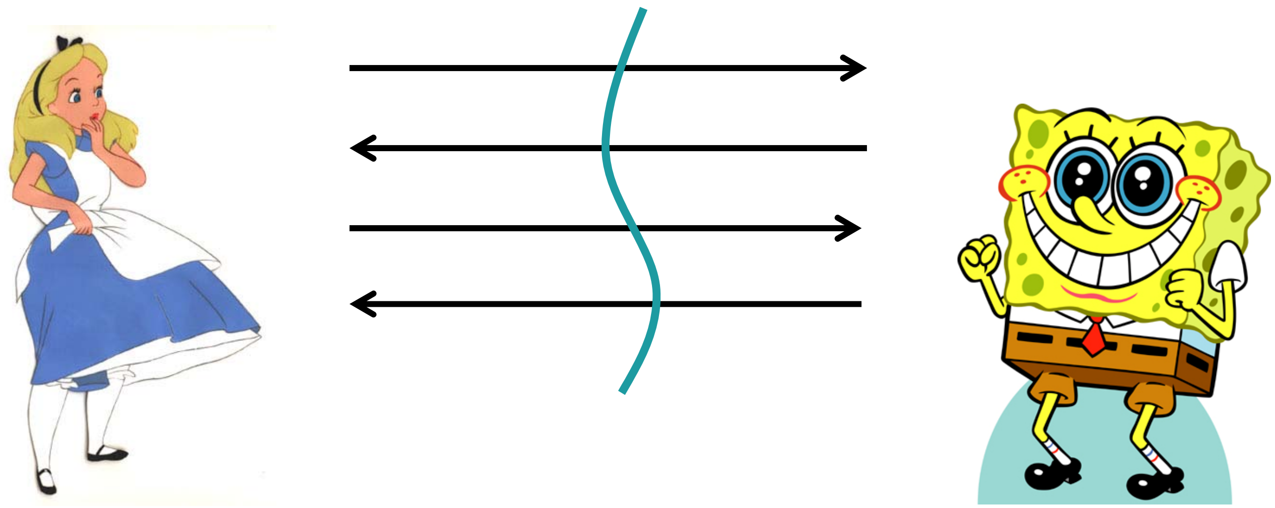
COMMUNICATION COMPLEXITY AND DISTRIBUTED COMPUTING

COMMUNICATION COMPLEXITY

$$f(X, Y) = ?$$



$X \in \{0,1\}^n$ $\qquad$ $Y \in \{0,1\}^n$

EXAMPLE: EQUALITY

- $f(X,Y) = \begin{cases} 1, & \text{if } X = Y \\ 0, & \text{if } X \neq Y \end{cases}$
- Naïve protocol: Alice sends X to Bob
  - $O(n)$ bits
- Can we do better?
  - Deterministically: no

RANDOMIZED PROTOCOL

- With public randomness:
  - Select random $Z \in \{0,1\}^n$
  - Alice sends $\langle X, Z \rangle = \sum_{i=1}^{n} X_i Z_i \bmod 2$
  - Bob accepts iff $\langle Y, Z \rangle = \langle X, Z \rangle$
- If $X = Y$: always accept
- If $X \neq Y$:

  non-zero vector

  $$[\langle X, Z \rangle - \langle Y, Z \rangle] \bmod 2 = \langle X - Y, Z \rangle \bmod 2$$
- Reject with probability $1/2$

RANDOMIZED PROTOCOL

- With private randomness…?

Error correcting code:

$C: \{0,1\}^n \to \{0,1\}^N$ such that

- If $X \neq Y$, then $\Delta(\ C(X), C(Y)\ )/N$ is large
- N should be as small as possible…

distance

rate$= n/N$

- Justesen code: rate = $1/3$, distance = $1/6$

RANDOMIZED PROTOCOL

- Protocol with private randomness:
  1. Alice and Bob compute $C(X), C(Y)$
  2. Alice chooses random $i \in \{1, \dots, N\}$, sends $(i, C(X)_i)$
  3. Bob accepts iff $C(Y)_i = C(X)_i$
- Communication complexity: $O(\log n)$
- Error:
  - $X = Y \quad \Rightarrow \quad$ Bob always accepts
  - $X \neq Y \quad \Rightarrow \quad$ Bob rejects w.p. $1/6$
- Can we reduce communication to $O(1)$?

SET DISJOINTNESS

- Input: $X, Y \subseteq \{1, \ldots, n\}$
- Output: $X \cap Y = \emptyset$?
- **Theorem** [Kalyanasundaran, Schnitger '92, Razborov '92]:
  - Randomized CC = $\Omega(n)$
  - Easy to see for deterministic protocols

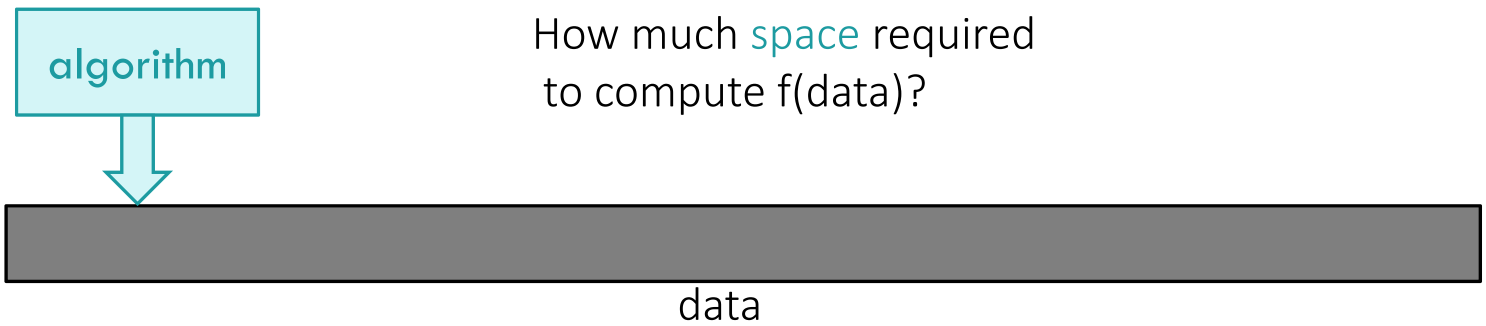
WHAT IS IT GOOD FOR?

Lower bounds in:

- Circuit complexity
- Streaming algorithms
- Data structures
- Distributed computing
- …

STREAMING LOWER BOUNDS

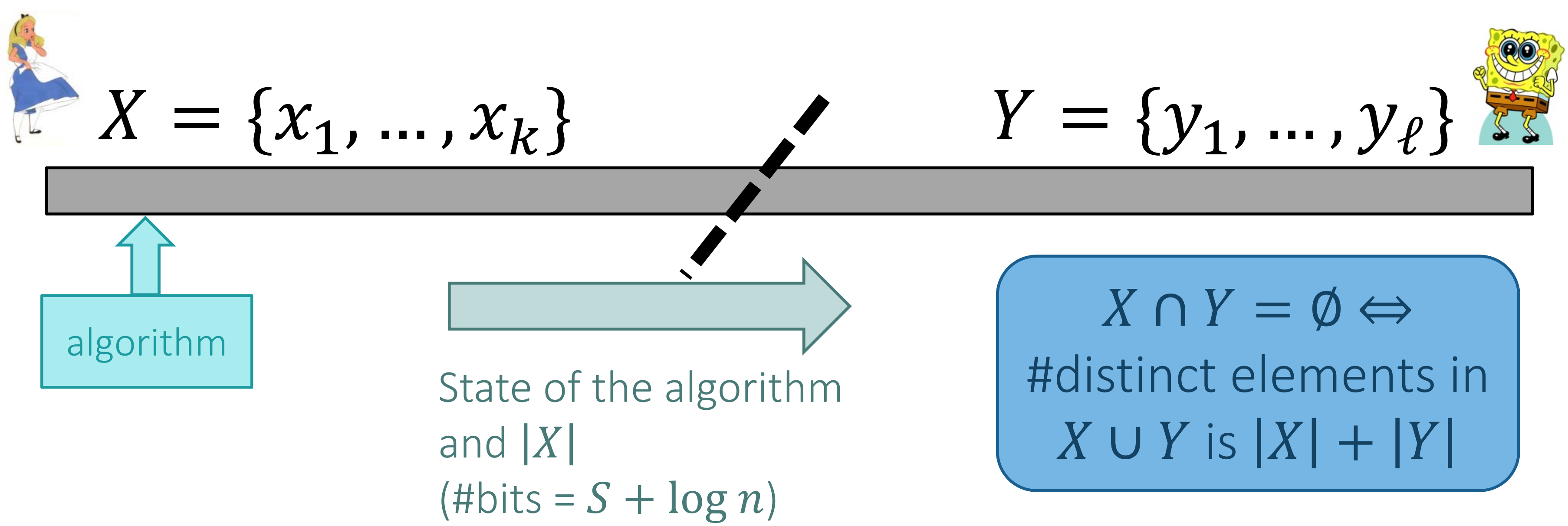
- Streaming algorithm:



- Example: Distinct Elements
  - How many distinct items in the data?
  - $n =$ universe size
  - Obviously $O(n)$ sufficient
  - Claim: $\Omega(n)$ required
- Reduction from Disjointness [Alon, Matias, Szegedy ’99]

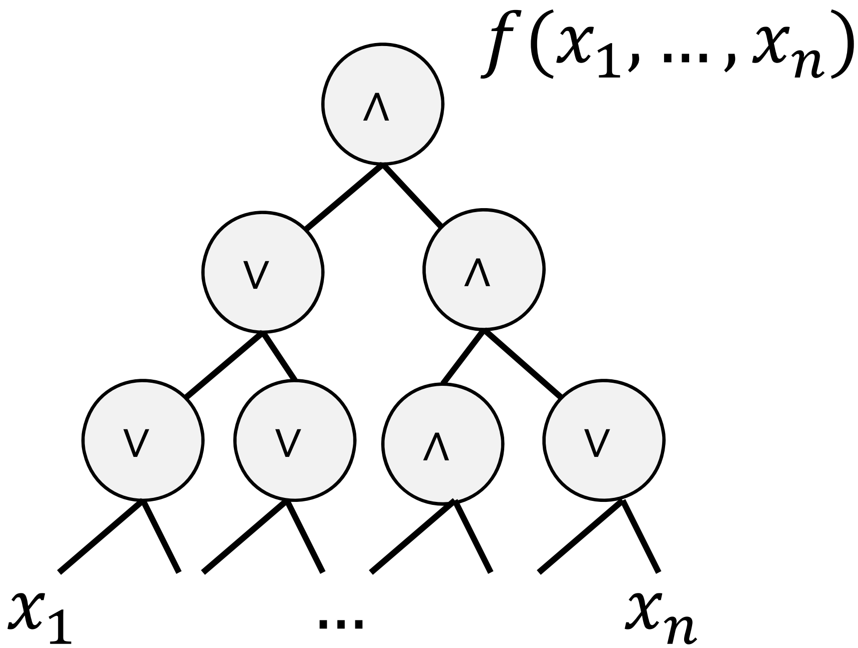
REDUCTION FROM DISJOINTNESS:

- Fix streaming algorithm for Distinct Elements with space S
- Construct protocol for Disjointness with n elements:



APPLICATION 2: KW GAMES

- Monotone circuit depth lower bounds:



- How deep does the circuit need to be to compute f?

APPLICATION 2: KW GAMES

- Karchmer-Wigderson'93,Karchmer-Raz-Wigderson'94:

find i such that $X_i \neq Y_i$

$X : f(X) = 0$

$Y : f(Y) = 1$

APPLICATION 2: KW GAMES

- Claim: if KW_f has deterministic CC $\geq d$, then f requires circuit depth $\geq d$.
- Circuit with depth d $\Rightarrow$ protocol with length d :