ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Abstract Storage Devices

Robert König Ueli Maurer Stefano Tessaro

SOFSEM 2009

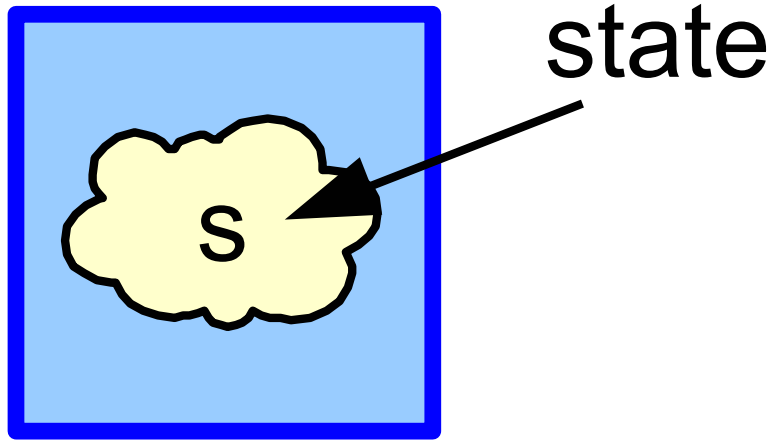
January 27, 2009

Outline

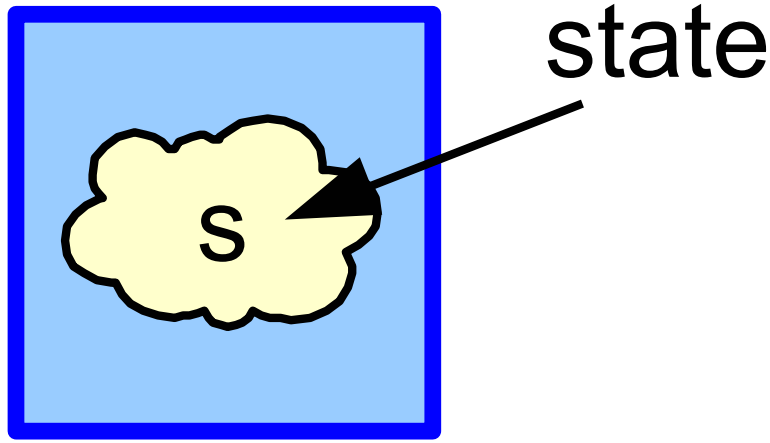
1. Motivation: Storage Devices
2. Abstract Storage Devices (ASD's)
3. Reducibility
4. Factoring ASD's
5. Future Directions

Outline

Storage Devices

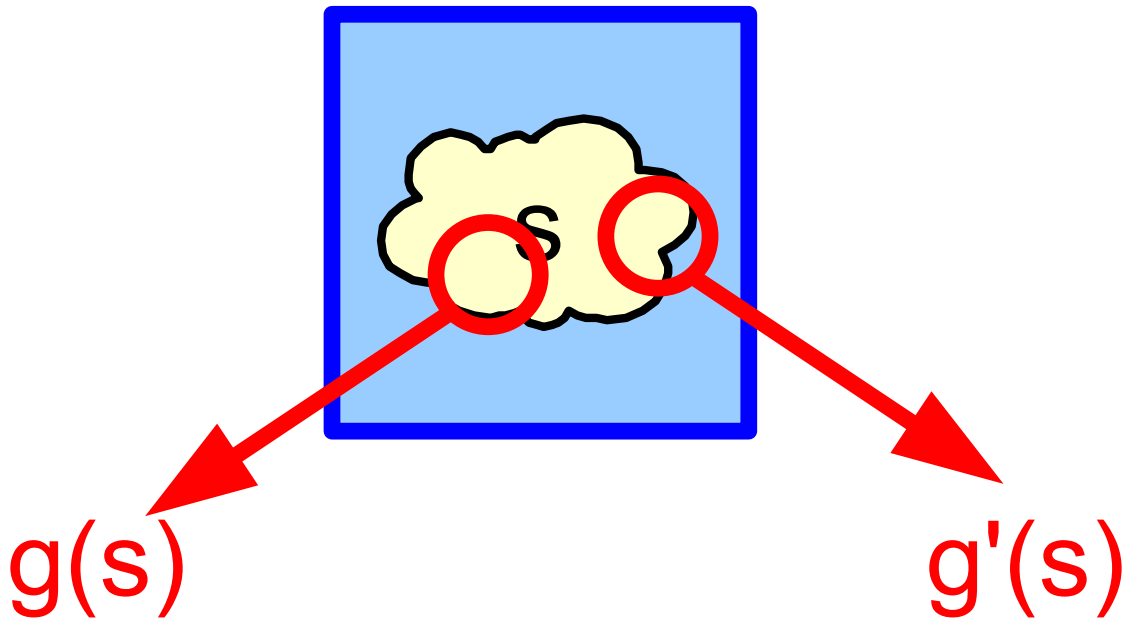


Storage Devices

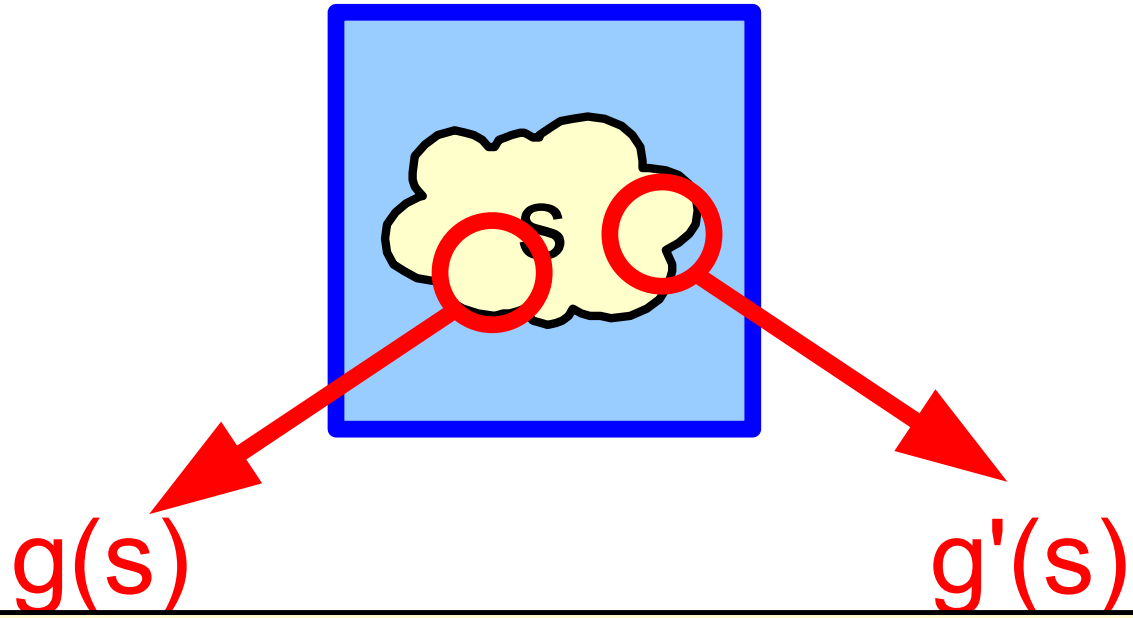


Multiple retrieval operations + partial information

Storage Devices



Storage Devices



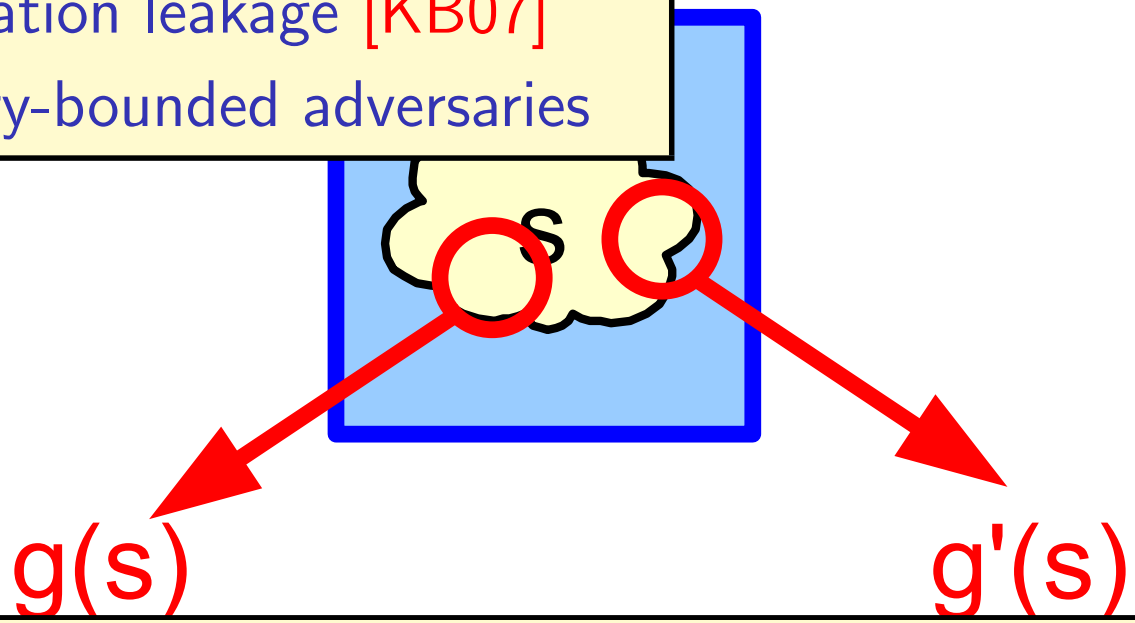
Motivation

- Physical laws (e.g. quantum state)
- Efficiency constraints

Storage Devices

Cryptographic Applications

- Information leakage [KB07]
- Memory-bounded adversaries



Motivation

- Physical laws (e.g. quantum state)
- Efficiency constraints

Outline

Deterministic Storage Device

This work. We consider **deterministic** devices.

Deterministic Storage Device

This work. We consider **deterministic** devices.

Motivation

- Natural examples
- Interesting phenomena
- Combinatorial characterization

Deterministic Storage Device

This work. We consider **deterministic** devices.

Motivation

- Natural examples
- Interesting phenomena
- Combinatorial characterization

Observation. Output labeling irrelevant

Abstract Storage Devices (ASD's)

Abstract Storage Device (ASD). Ordered pair $D = (\mathcal{S}, \Pi)$

- $\mathcal{S}$: state space
- Π: partition set, i.e. $\pi \in \Pi$ have form

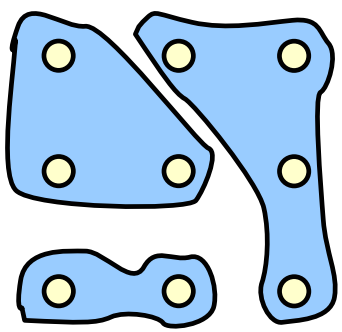
$$\pi = \left\{ \mathcal{B}_1, \ldots, \mathcal{B}_\ell \neq \emptyset \;\middle|\; (\forall i \neq j : \mathcal{B}_i \cap \mathcal{B}_j = \emptyset) \wedge \bigcup_{i=1}^{\ell} \mathcal{B}_i = \mathcal{S} \right\}.$$

Abstract Storage Devices (ASD's)

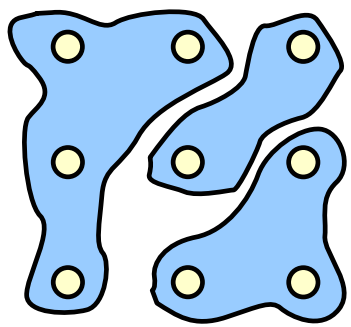
Abstract Storage Device (ASD). Ordered pair $D = (\mathcal{S}, \Pi)$

- $\mathcal{S}$: state space
- Π: partition set, i.e. $\pi \in \Pi$ have form

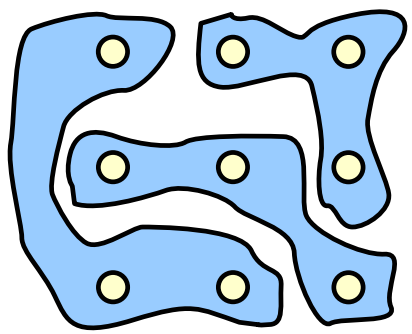
$$\pi = \left\{ \mathcal{B}_1, \ldots, \mathcal{B}_\ell \neq \emptyset \,\middle|\, (\forall i \neq j : \mathcal{B}_i \cap \mathcal{B}_j = \emptyset) \wedge \bigcup_{i=1}^{\ell} \mathcal{B}_i = \mathcal{S} \right\}.$$



π_1



π_2



π_3

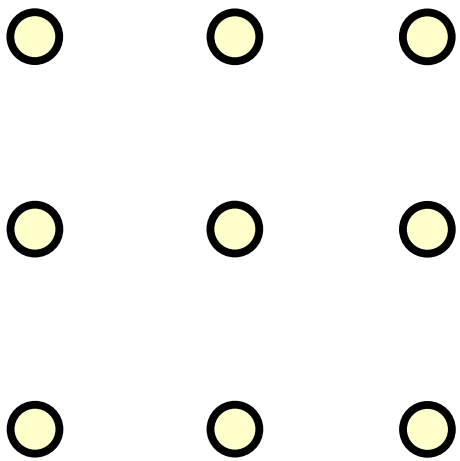
ASD's – Write and Read

Write operation

Retrieval operation

ASD's – Write and Read

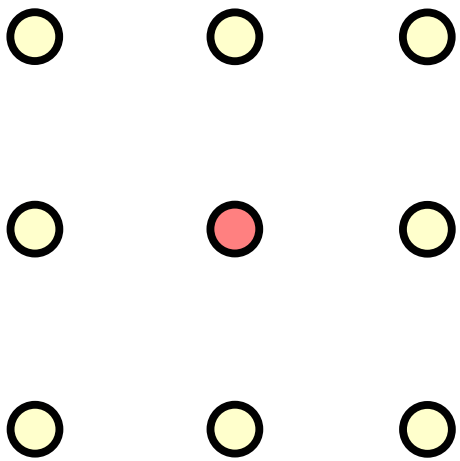
Write operation



Retrieval operation

ASD's – Write and Read

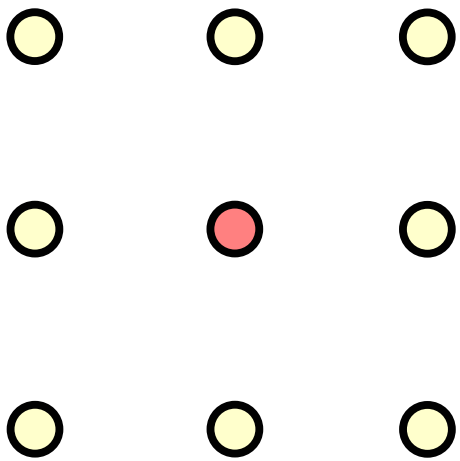
Write operation



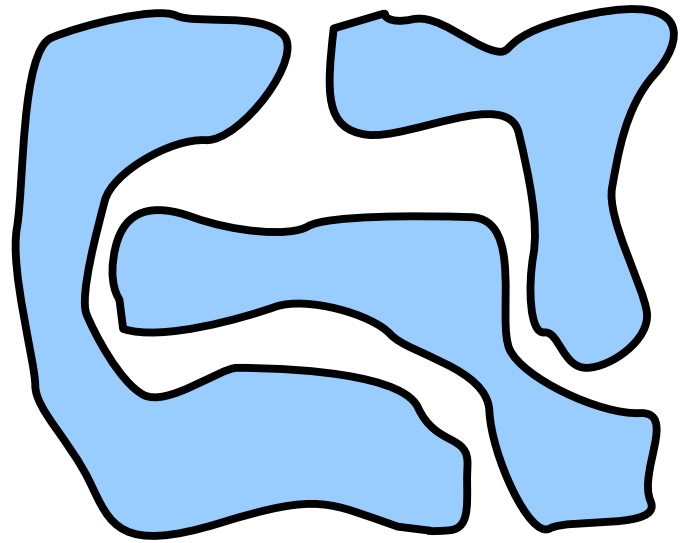
Retrieval operation

ASD's – Write and Read

Write operation

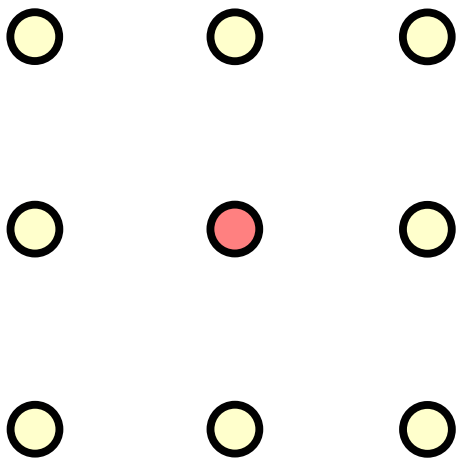


Retrieval operation

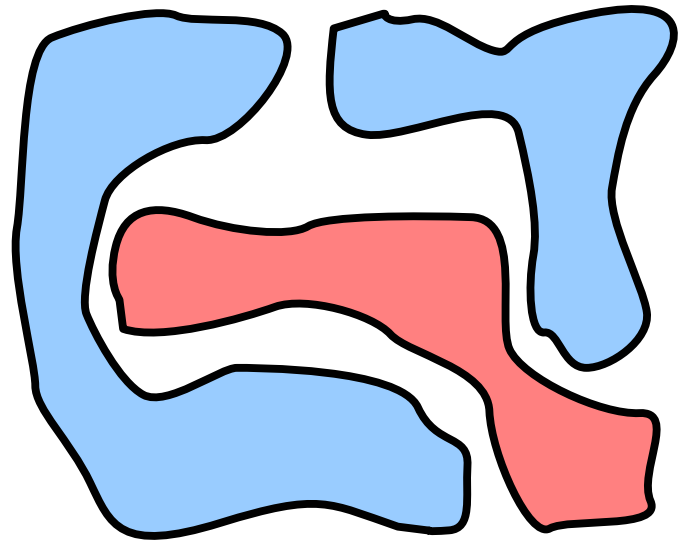


ASD's – Write and Read

Write operation

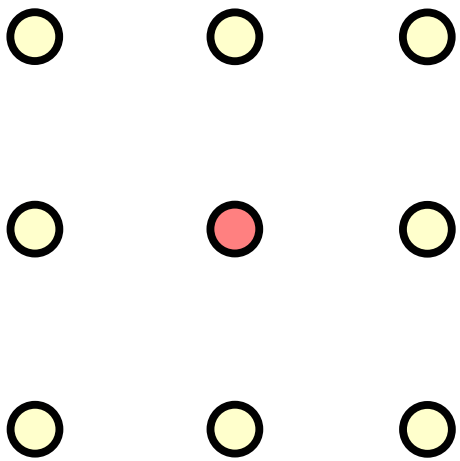


Retrieval operation

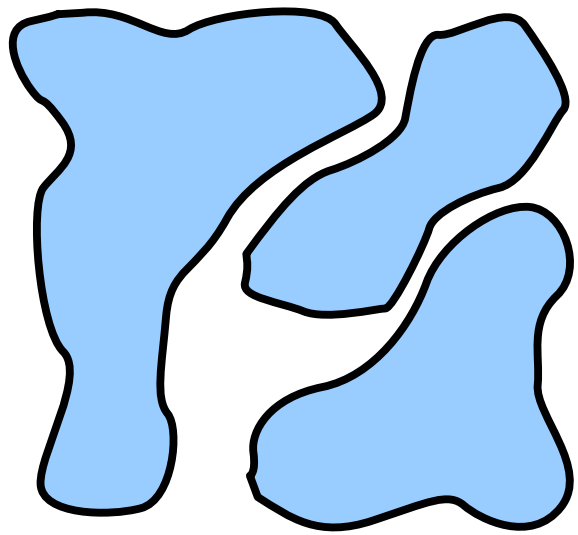


ASD's – Write and Read

Write operation

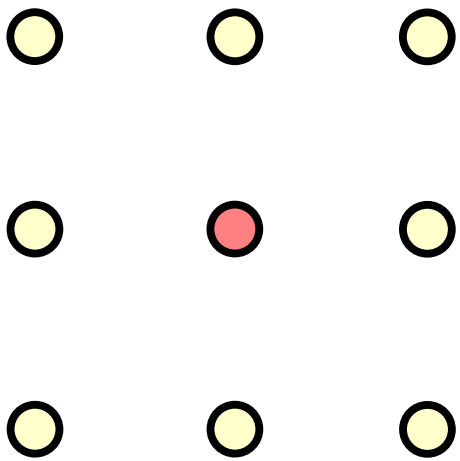


Retrieval operation

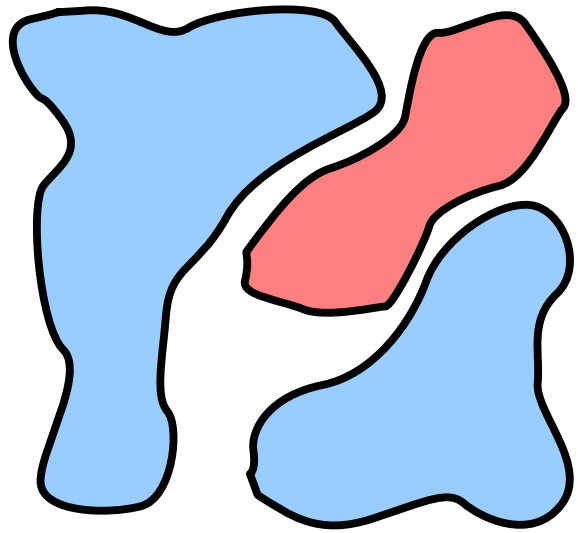


ASD's – Write and Read

Write operation

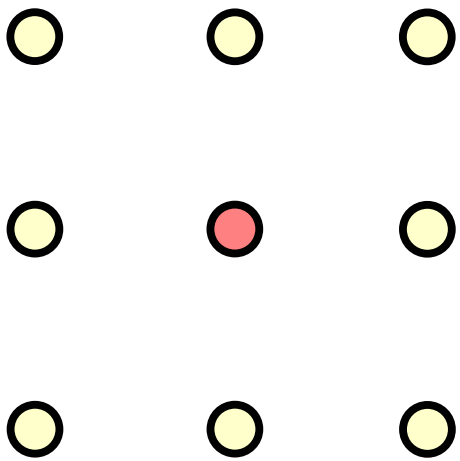


Retrieval operation

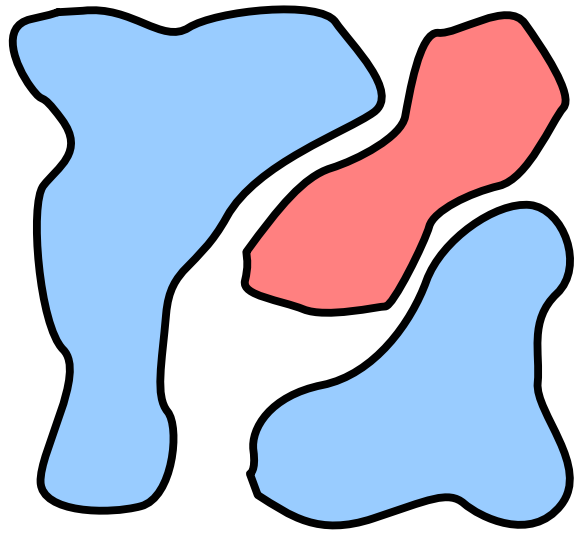


ASD's – Write and Read

Write operation

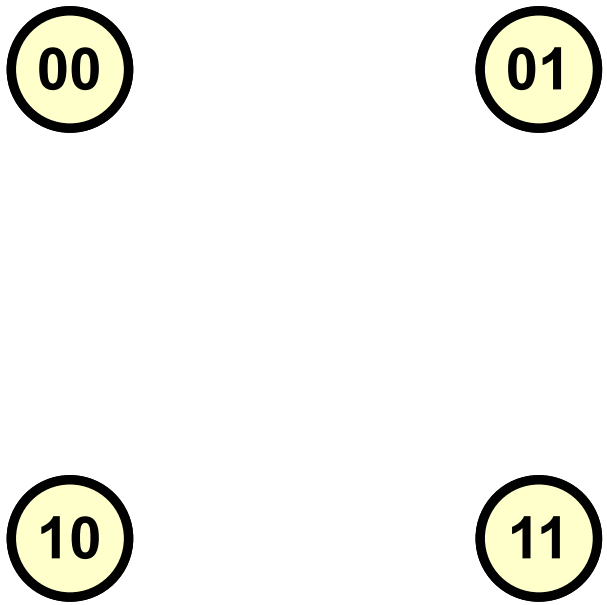


Retrieval operation

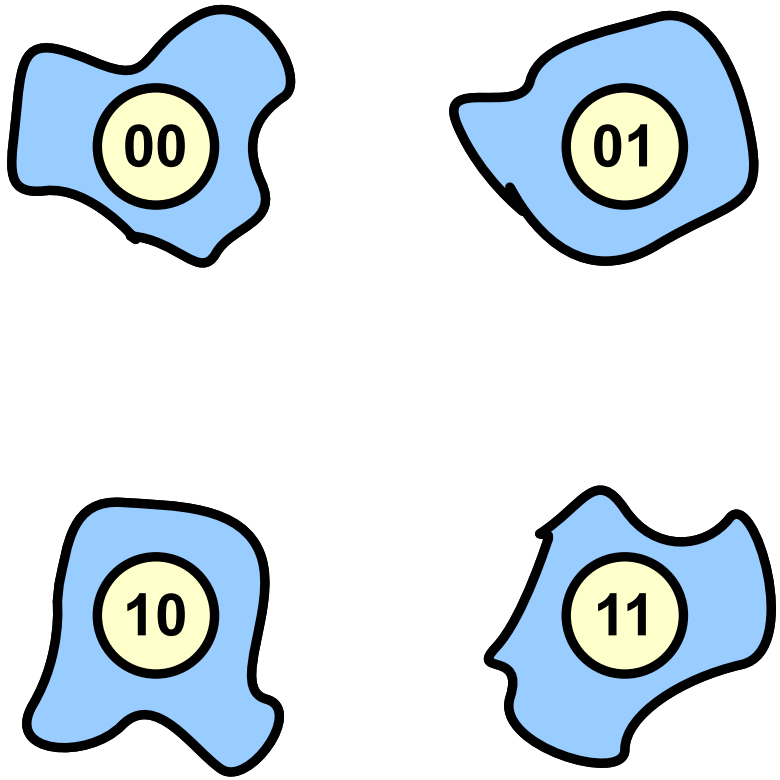


In this talk: $\forall s \neq s' : \exists \pi : s \not\equiv_\pi s'$

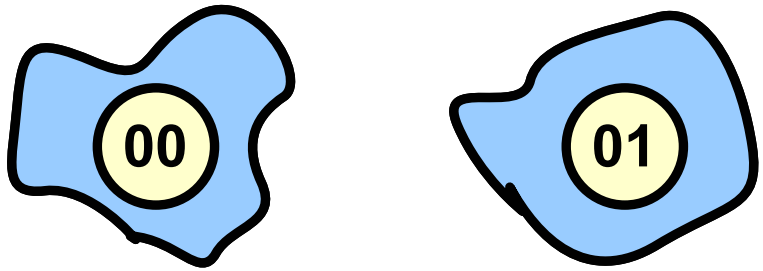
ASD's – Examples

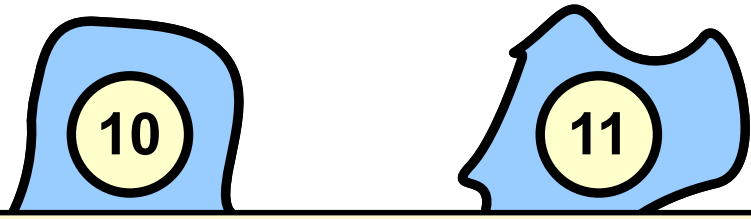


ASD's – Examples



ASD's – Examples

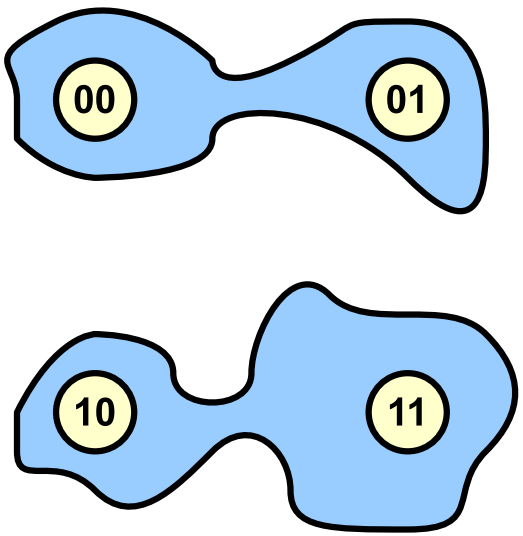


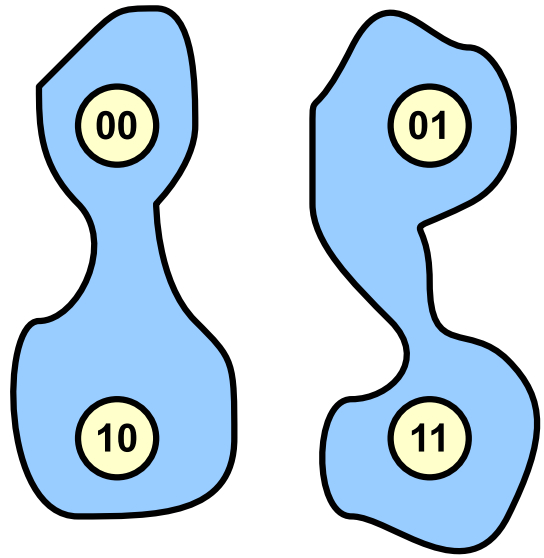


Perfect Device C_s:

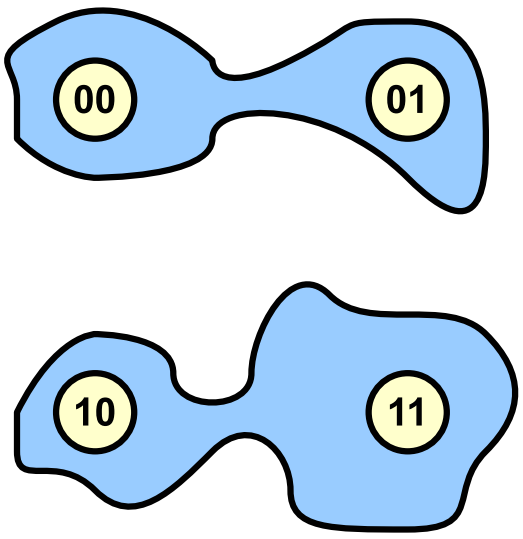
- $\mathcal{S} := \{0, \ldots, s-1\}$
- $\Pi := \{\mathrm{id}\}$, with $\mathrm{id} := \{\{0\}, \ldots, \{s-1\}\}$

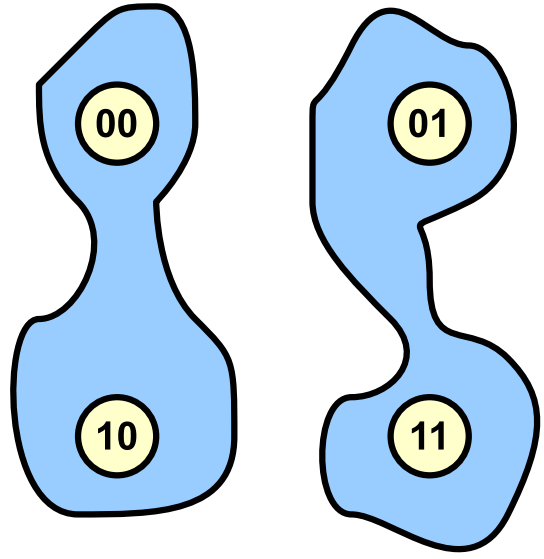
ASD's – Examples





ASD's – Examples

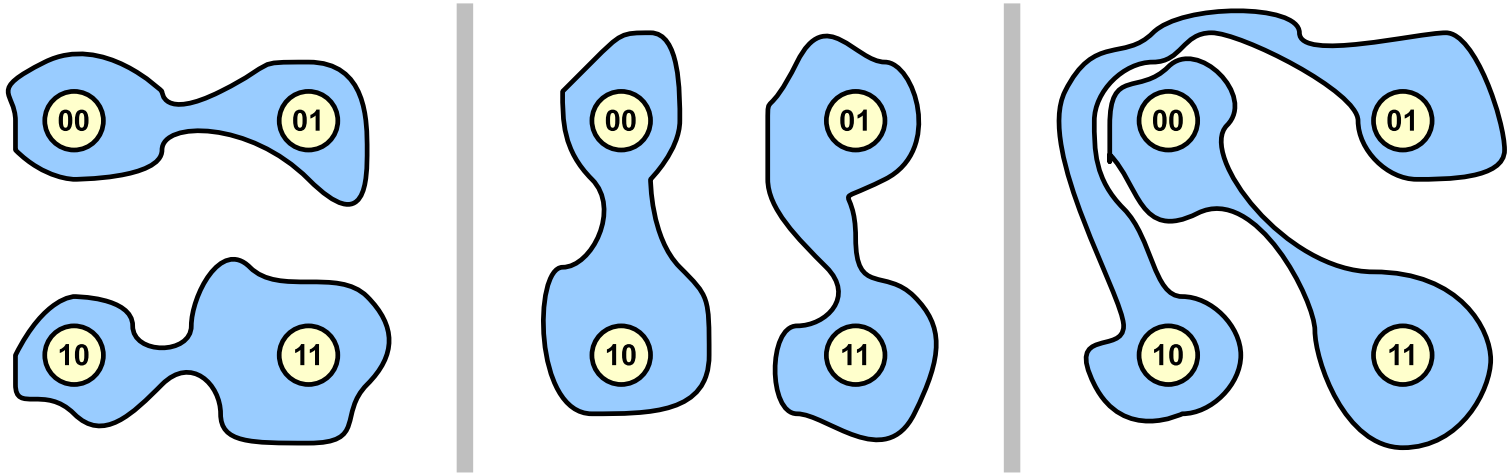




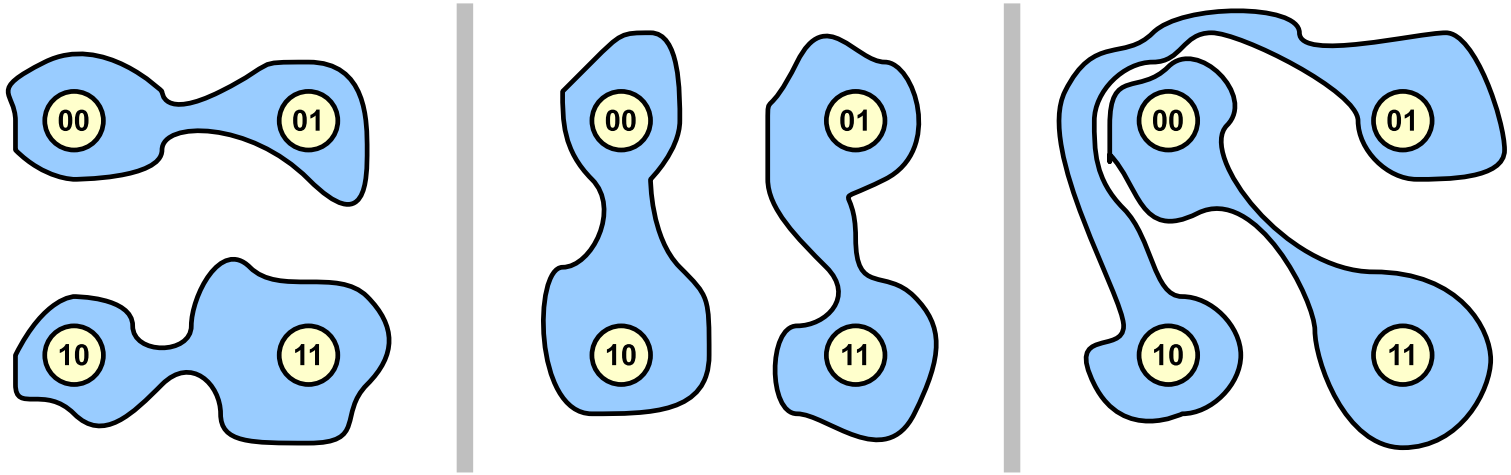
Projective Device P_n:

- $\mathcal{S} := \{0,1\}^n$
- $\Pi := \{\pi_1, \ldots, \pi_n\}$, with $\pi_i := \{\{x : x_i = 0\}, \{x : x_i = 1\}\}$

ASD's – Examples



ASD's – Examples



Linear Device L_n:

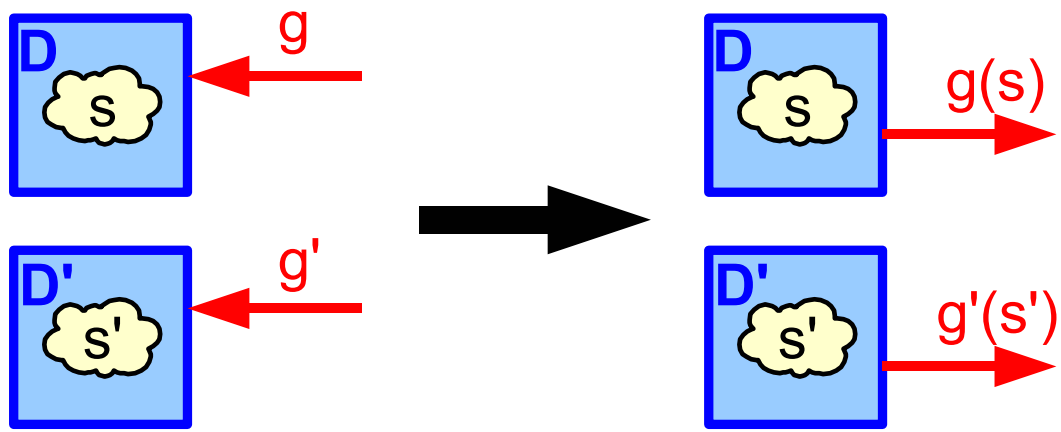
- $\mathcal{S} := \{0,1\}^n$, $\Pi := \{\pi_a : a \in \{0,1\}^n\}$
- $\pi_a := \{\{x : \langle a, x\rangle = 0\}, \{x : \langle a, x\rangle = 1\}\}$

Composing ASD's – Direct Products

Direct product $D \times D'$

- $\mathcal{S}(D \times D') := \mathcal{S}(D) \times \mathcal{S}(D')$;
- $\Pi(D \times D') := \{\pi \times \pi' \mid \pi \in \Pi(D), \pi' \in \Pi(D')\}$, where

$$\pi \times \pi' := \{\mathcal{B} \times \mathcal{B}' \mid \mathcal{B} \in \pi, \mathcal{B}' \in \pi'\}$$

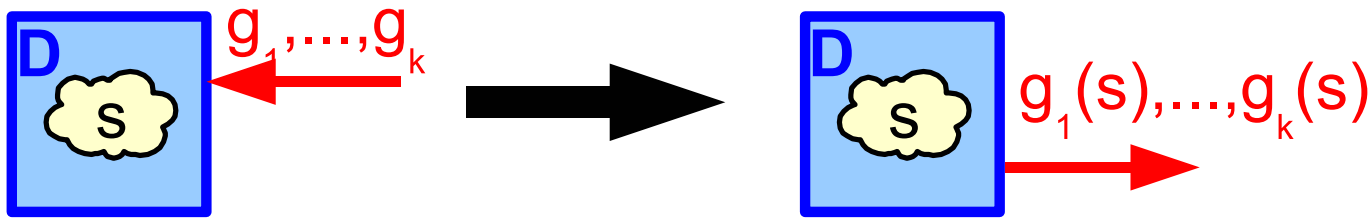


Composing ASD's – Sequence Device

k-Sequence Device $D^{(k)}$

- $\mathcal{S}(D^{(k)}) := \mathcal{S}(D)$;
- $\Pi(D^{(k)}) := \{\pi_1 \wedge \cdots \wedge \pi_k \mid \pi_1, \ldots, \pi_k \in \Pi(D)\}$, where

$$\pi \wedge \pi' := \{\mathcal{B} \cap \mathcal{B}' \mid \mathcal{B} \in \pi, \mathcal{B}' \in \pi'\}.$$



Outline

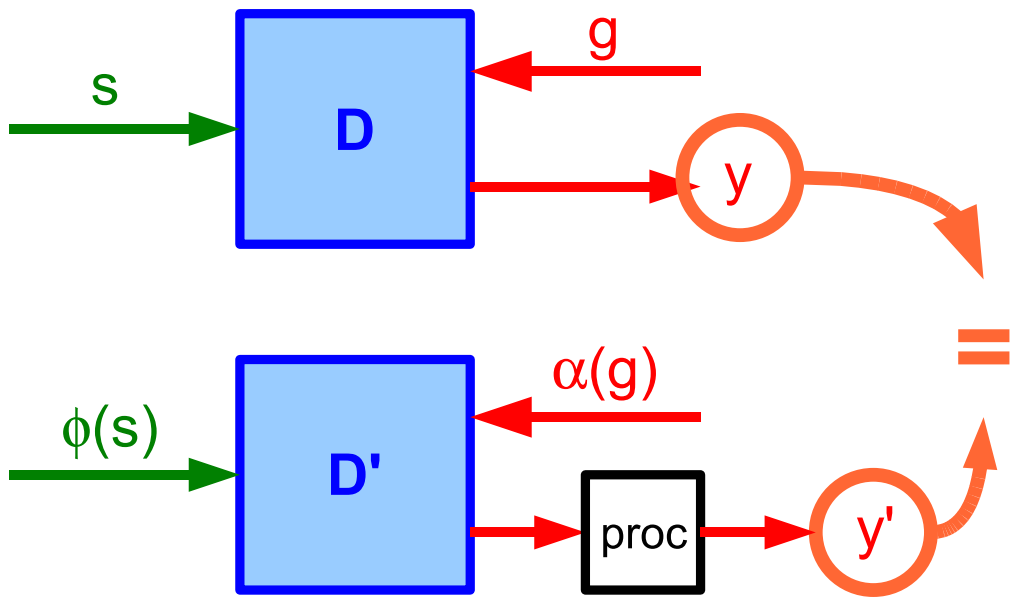
ASD Reducibility

Question. Is ASD D' stronger than D? Can we implement D using D'?

ASD Reducibility

Question. Is ASD D' stronger than D? Can we implement D using D'?

$\forall$ s, g:



This work: zero-error reductions

ASD Reducibility – Definition

Reduction $D \longrightarrow D'$. Ordered pair (ϕ, α) with

$$\phi : \mathcal{S}(D) \longrightarrow \mathcal{S}(D') \text{ and } \alpha : \Pi(D) \longrightarrow \Pi(D')$$

such that

$$\forall \pi \in \Pi(D) : \alpha(\pi) \circ \phi \text{ refines } \pi$$

ASD Reducibility – Definition

$$s \equiv_{\alpha(\pi)\circ\phi} s' \iff \phi(s) \equiv_{\alpha(\pi)} \phi(s')$$

R

$$\phi : \mathcal{S}(D) \to \mathcal{S}(D') \text{ and } \alpha : \Pi(D) \to \Pi(D')$$

such that

$$\forall \pi \in \Pi(D) : \alpha(\pi) \circ \phi \text{ refines } \pi$$

ASD Reducibility – Definition

$$s \equiv_{\alpha(\pi)\circ\phi} s' \iff \phi(s) \equiv_{\alpha(\pi)} \phi(s')$$

R

$$\phi : \mathcal{S}(D) \to \mathcal{S}(D') \text{ and } \alpha : \Pi(D) \to \Pi(D')$$

such that

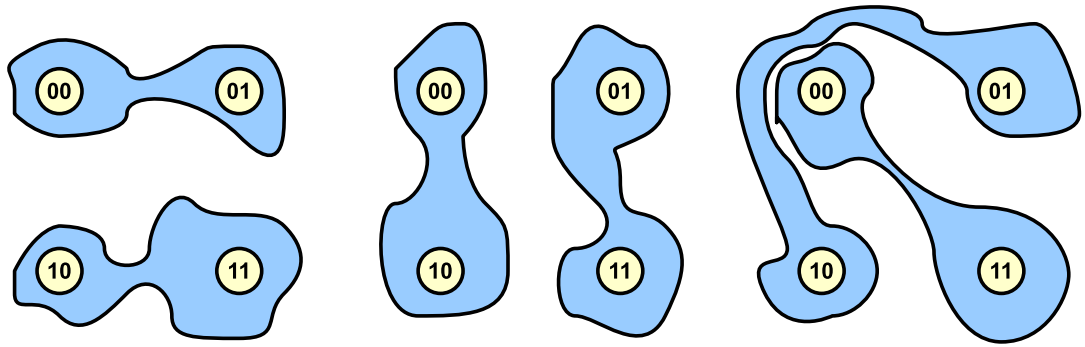
$$\forall \pi \in \Pi(D) : \alpha(\pi) \circ \phi \text{ refines } \pi$$

Notation.

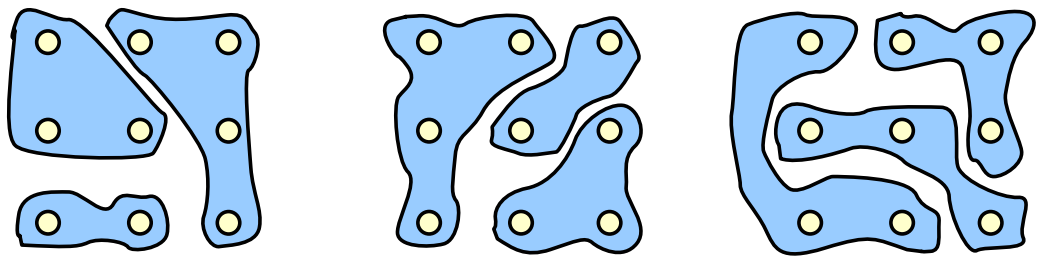
$$D \leq D' :\iff \exists(\phi, \alpha) \text{ reduction } D \to D'$$
$$D \equiv D' :\iff D \leq D' \wedge D' \leq D.$$

ASD Reducibility – Example

L_2

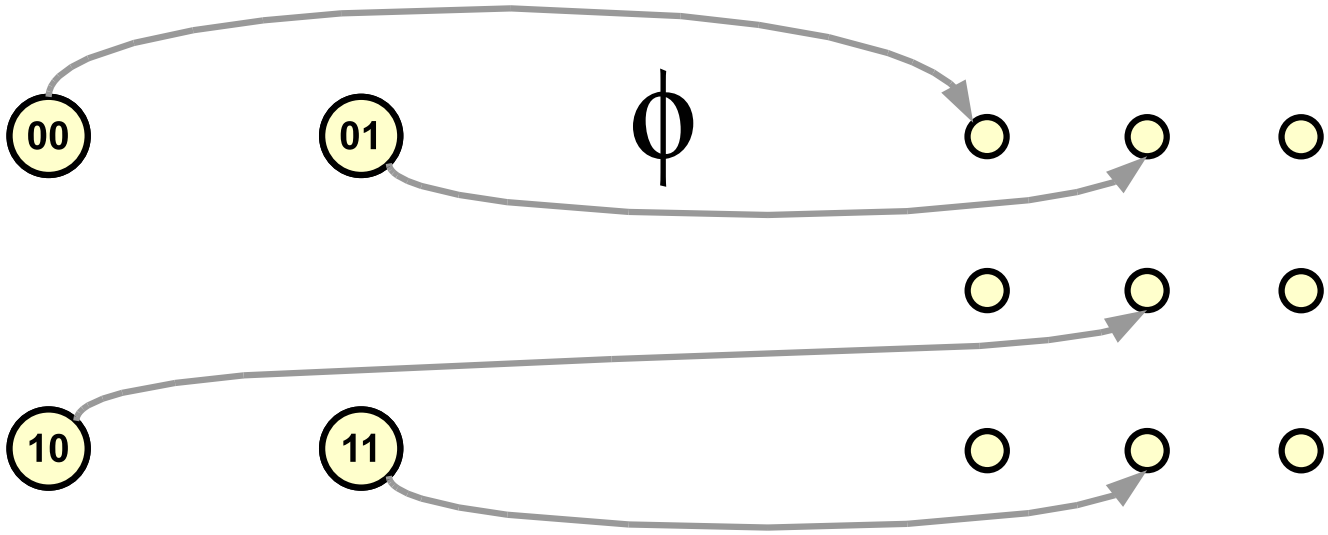


D

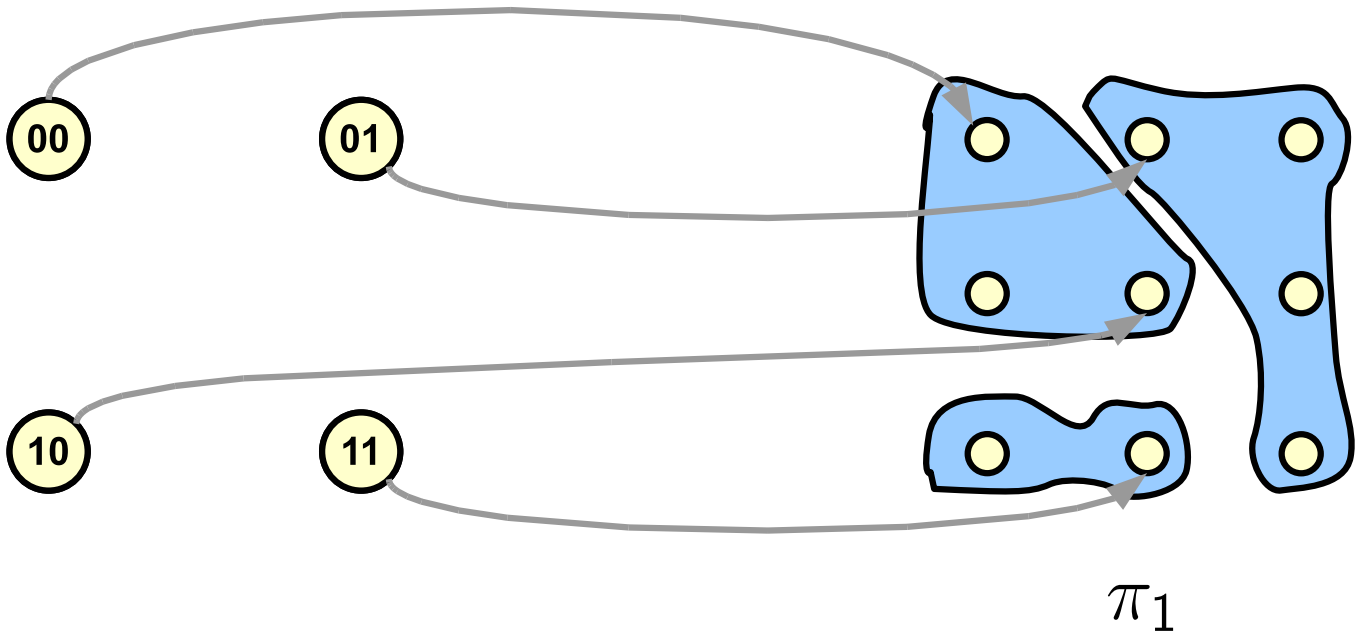


ASD Reducibility – Example

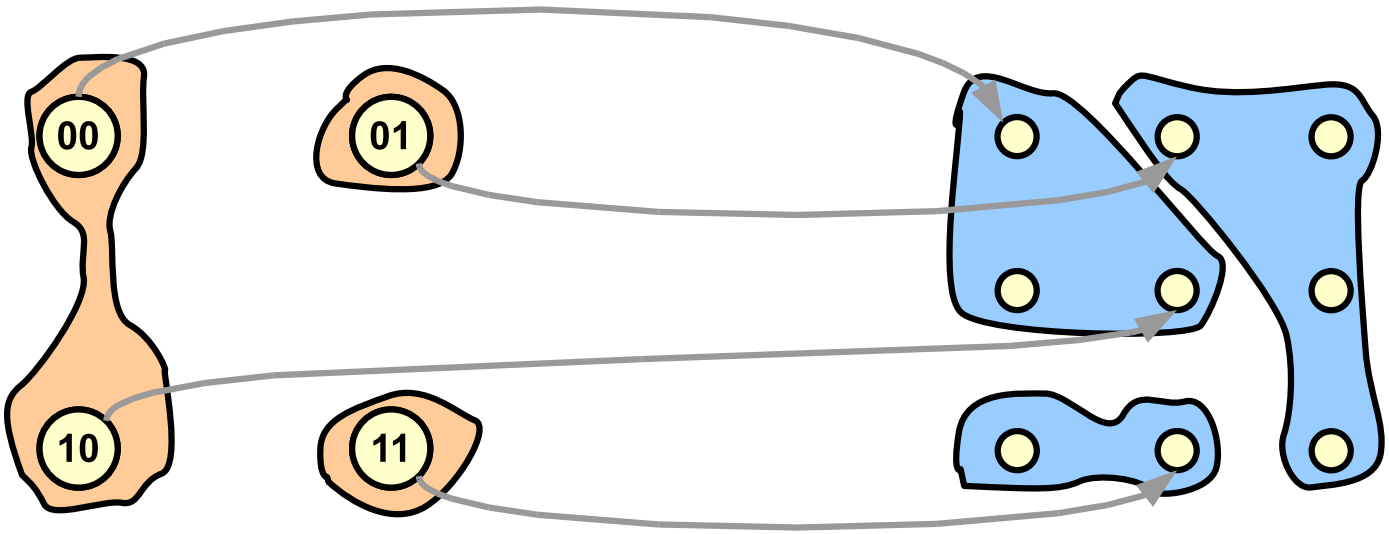
ASD Reducibility – Example



ASD Reducibility – Example

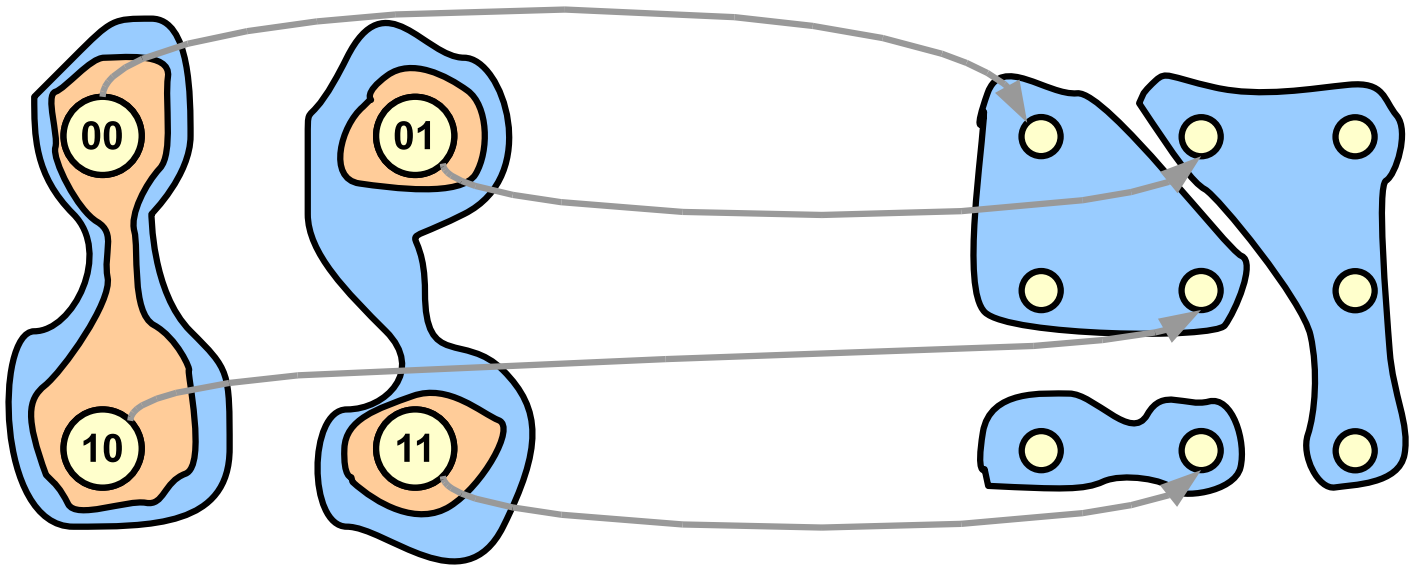


ASD Reducibility – Example



$\pi_1 \circ \phi$ π_1

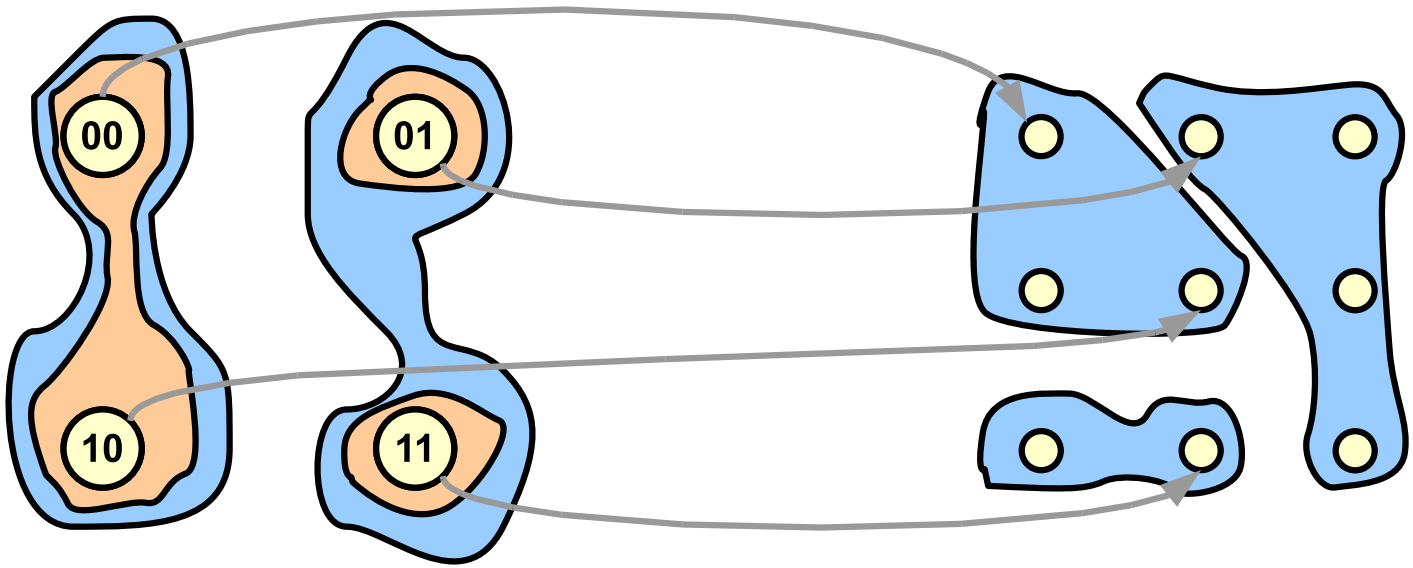
ASD Reducibility – Example



$\pi_1 \circ \phi$ π_1

$\longrightarrow$ refines π_{01}

ASD Reducibility – Example

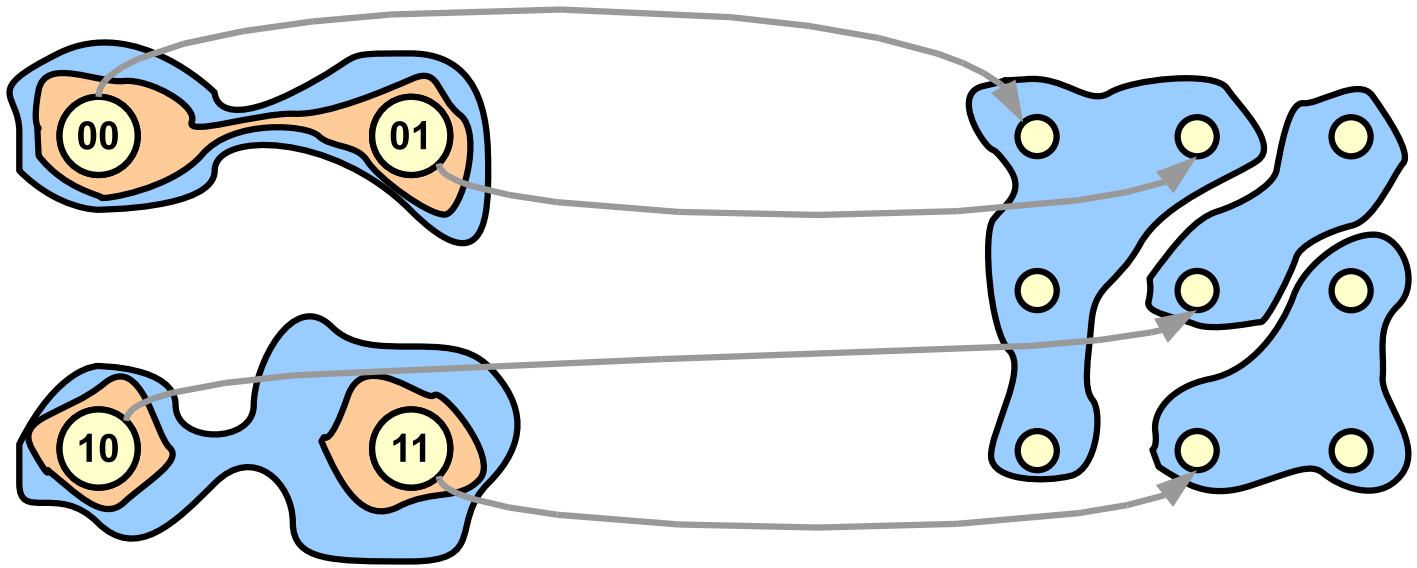


$\pi_1 \circ \phi$ π_1

$\longrightarrow$ refines π_{01}

$\longrightarrow \alpha(\pi_{01}) := \pi_1$

ASD Reducibility – Example

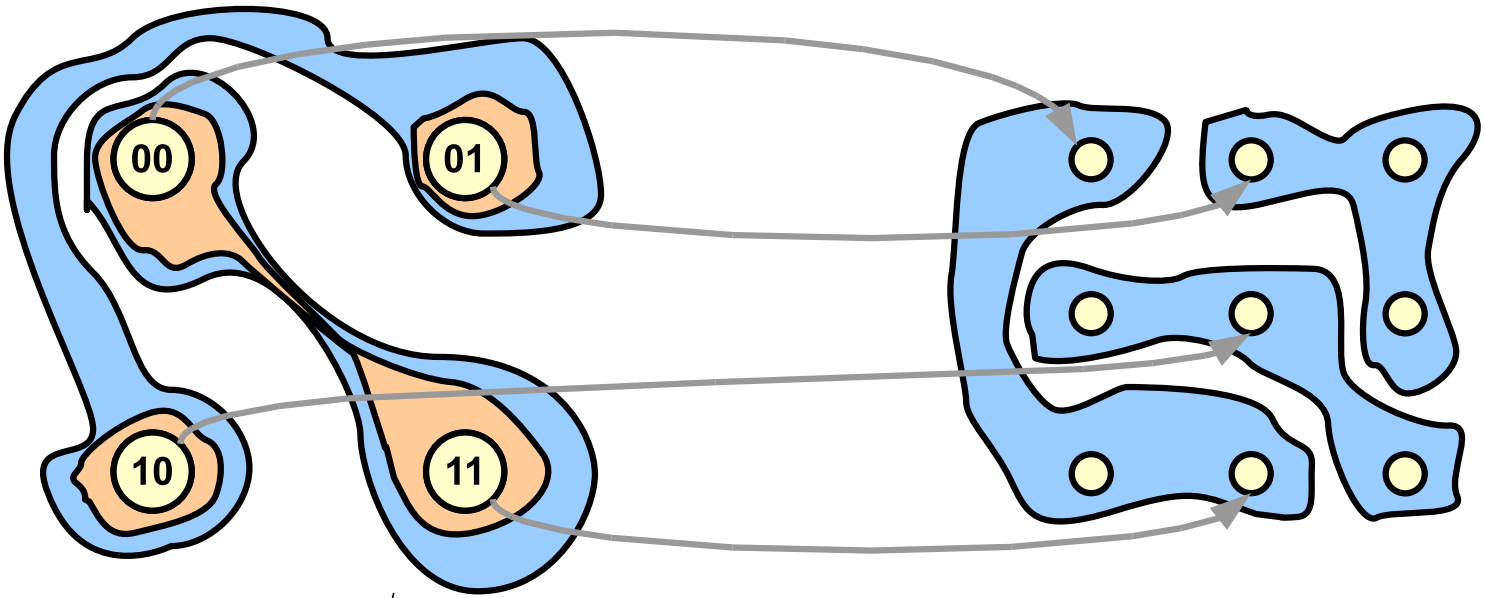


$\pi_2 \circ \phi$ π_2

$\longrightarrow$ refines π_{10}

$\longrightarrow \alpha(\pi_{10}) := \pi_2$

ASD Reducibility – Example



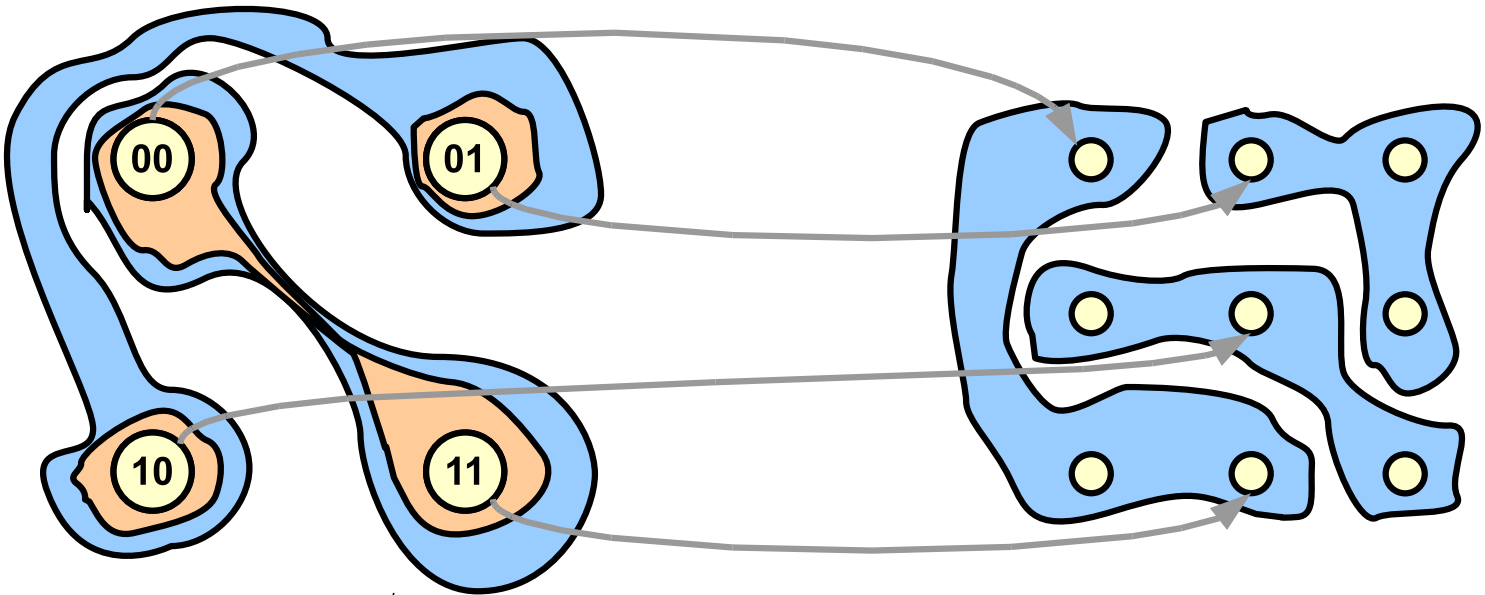
$\pi_3 \circ \phi$ π_3

$\longrightarrow$ refines π_{11}

$\longrightarrow \alpha(\pi_{11}) := \pi_3$

ASD Reducibility – Example

(ϕ, α) is valid reduction $\Rightarrow L_2 \leq D$



$\pi_3 \circ \phi$ $\qquad\qquad$ π_3

$\longrightarrow$ refines π_{11}

$\longrightarrow \alpha(\pi_{11}) := \pi_3$

ASD Reducibility – Complexity

Question. Complexity of deciding reducibility?

ASD Reducibility – Complexity

Question. Complexity of deciding reducibility?

Theorem. ASD Reducibility is $\mathcal{NP}$-complete.

Question. Complexity of deciding reducibility?

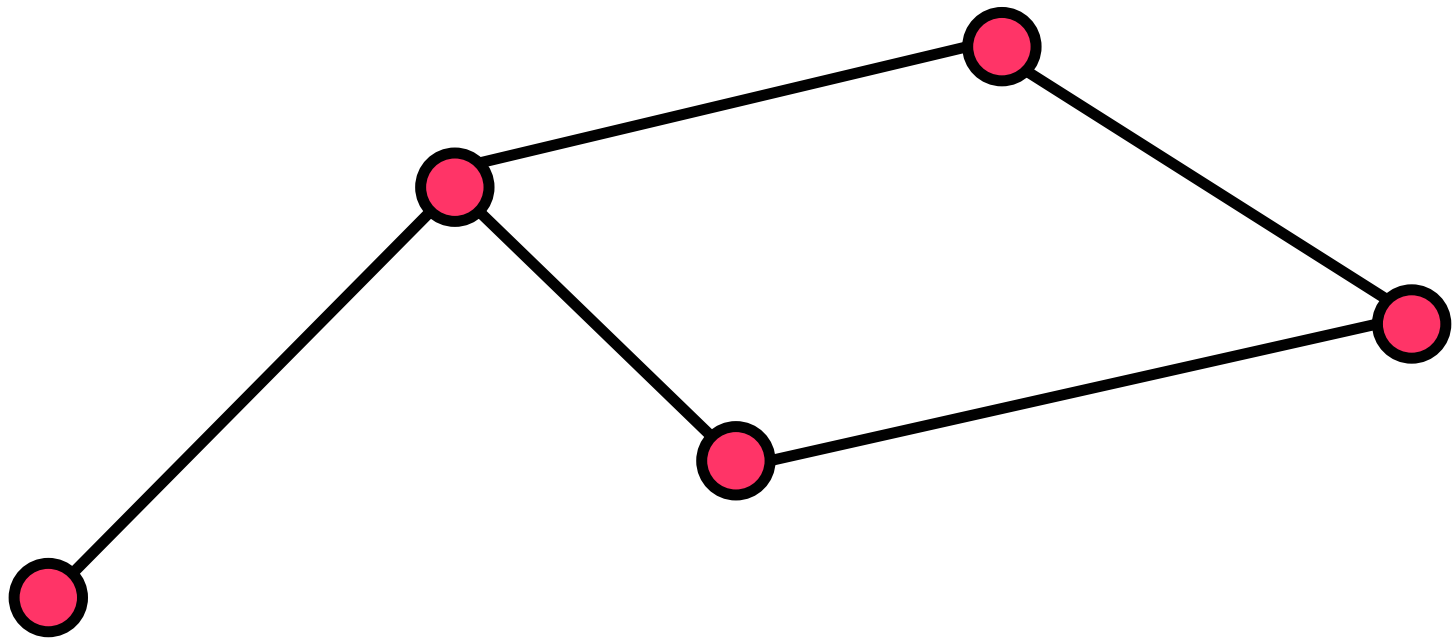
Theorem. ASD Reducibility is $\mathcal{NP}$-complete.

Proof Idea

- Reducibility is in $\mathcal{NP}$ (witness = reduction)
- (Complexity-theoretic) reduction from CLIQUE
- $\forall\ G = (V, E)$ construct graph device $D = D(G)$

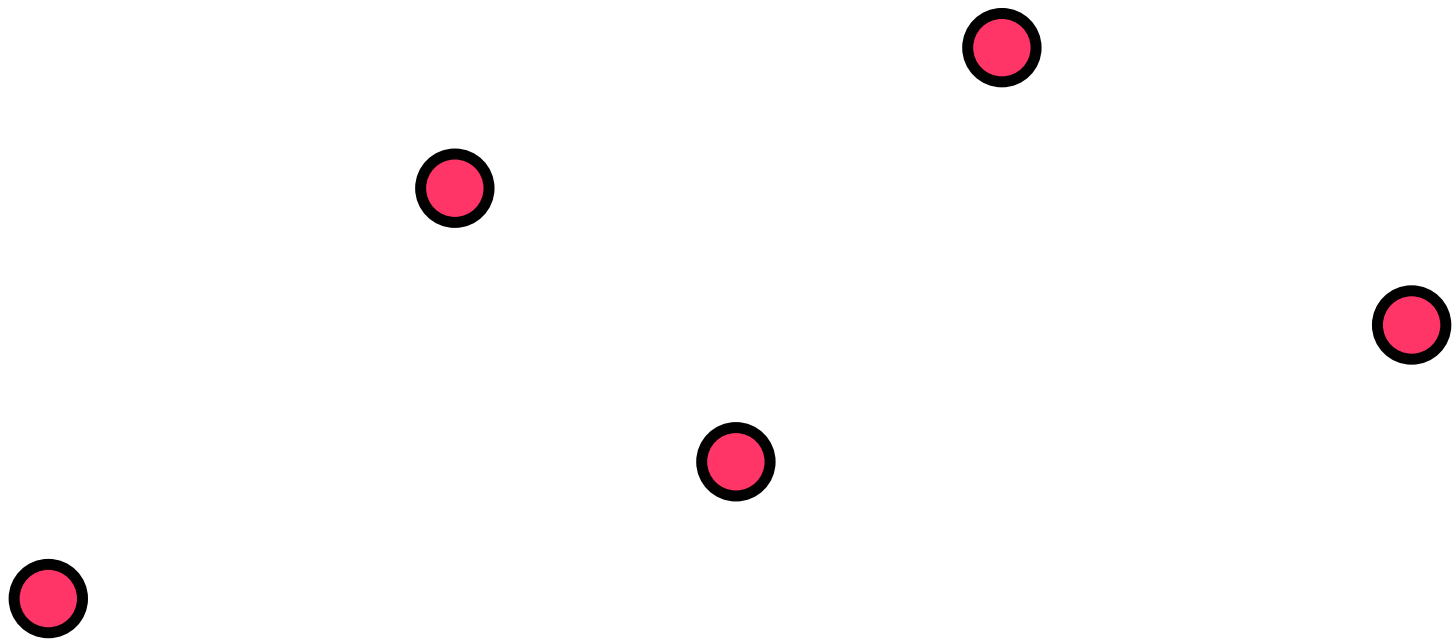
NP-Completeness – Graph Devices

Undirected graph $G = (V, E)$, $|V| \geq 4$.



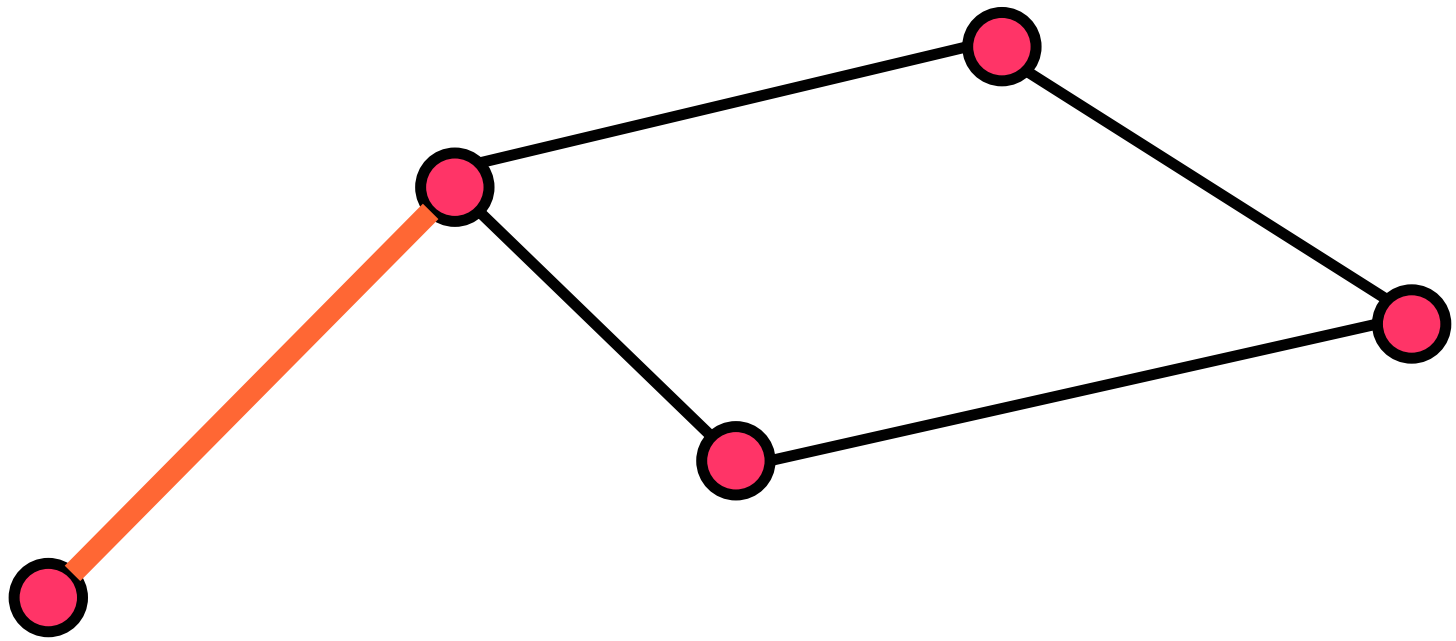
NP-Completeness – Graph Devices

Undirected graph $G = (V, E)$, $|V| \geq 4$.



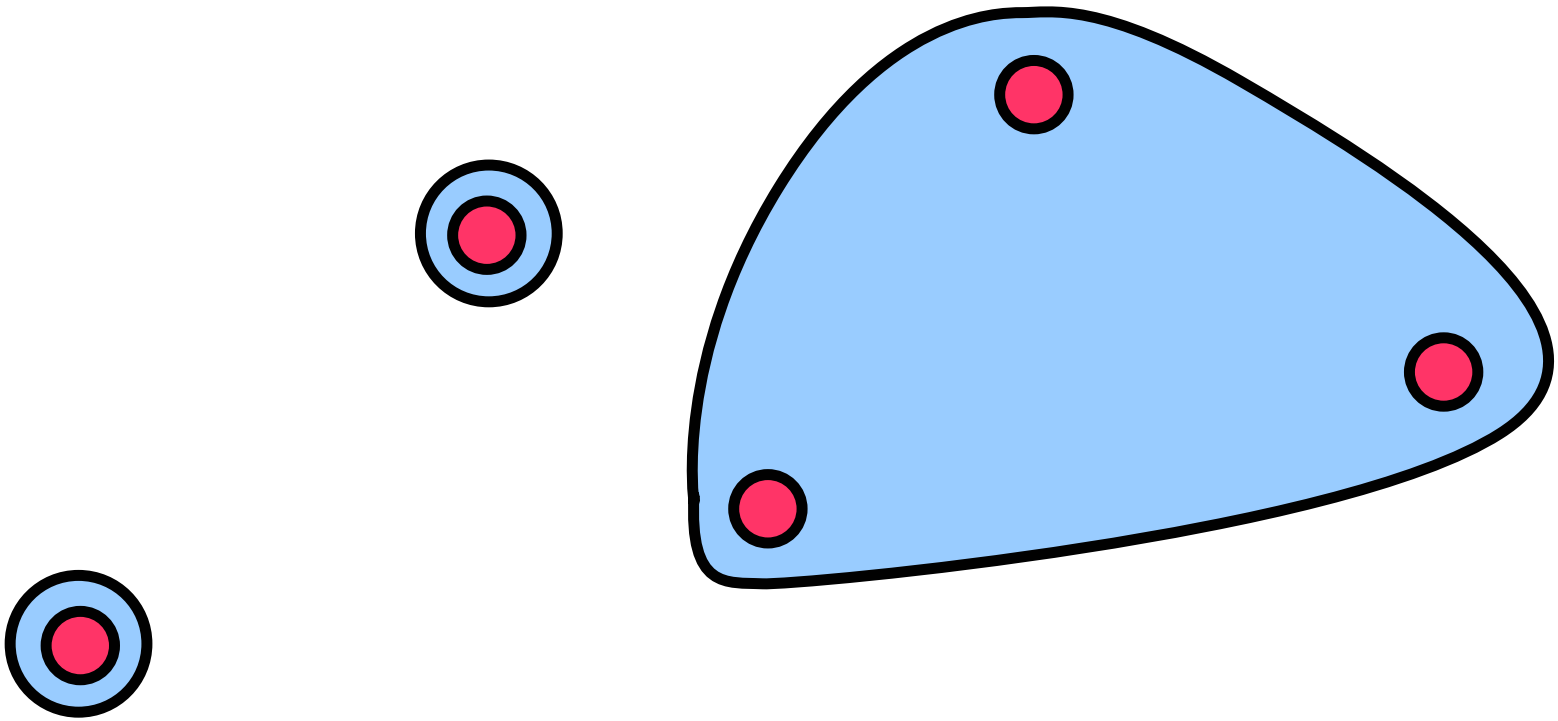
NP-Completeness – Graph Devices

Undirected graph $G = (V, E)$, $|V| \geq 4$.



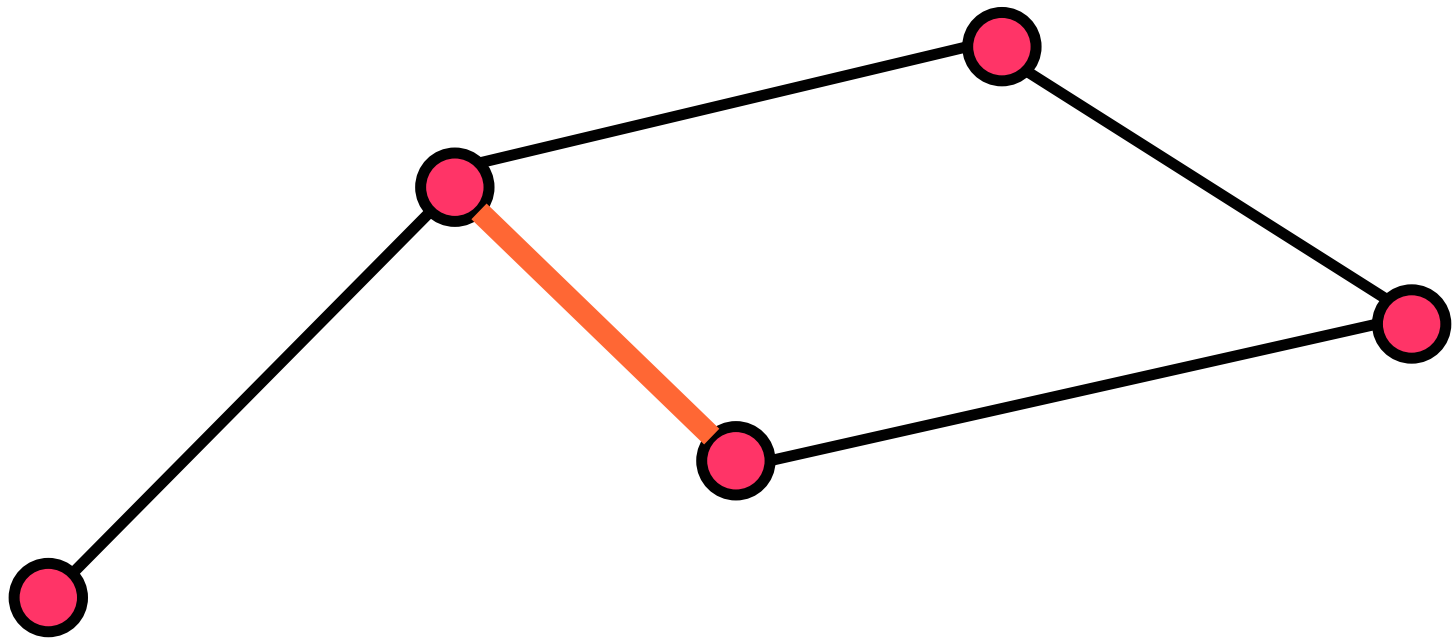
NP-Completeness – Graph Devices

Undirected graph $G = (V, E)$, $|V| \geq 4$.



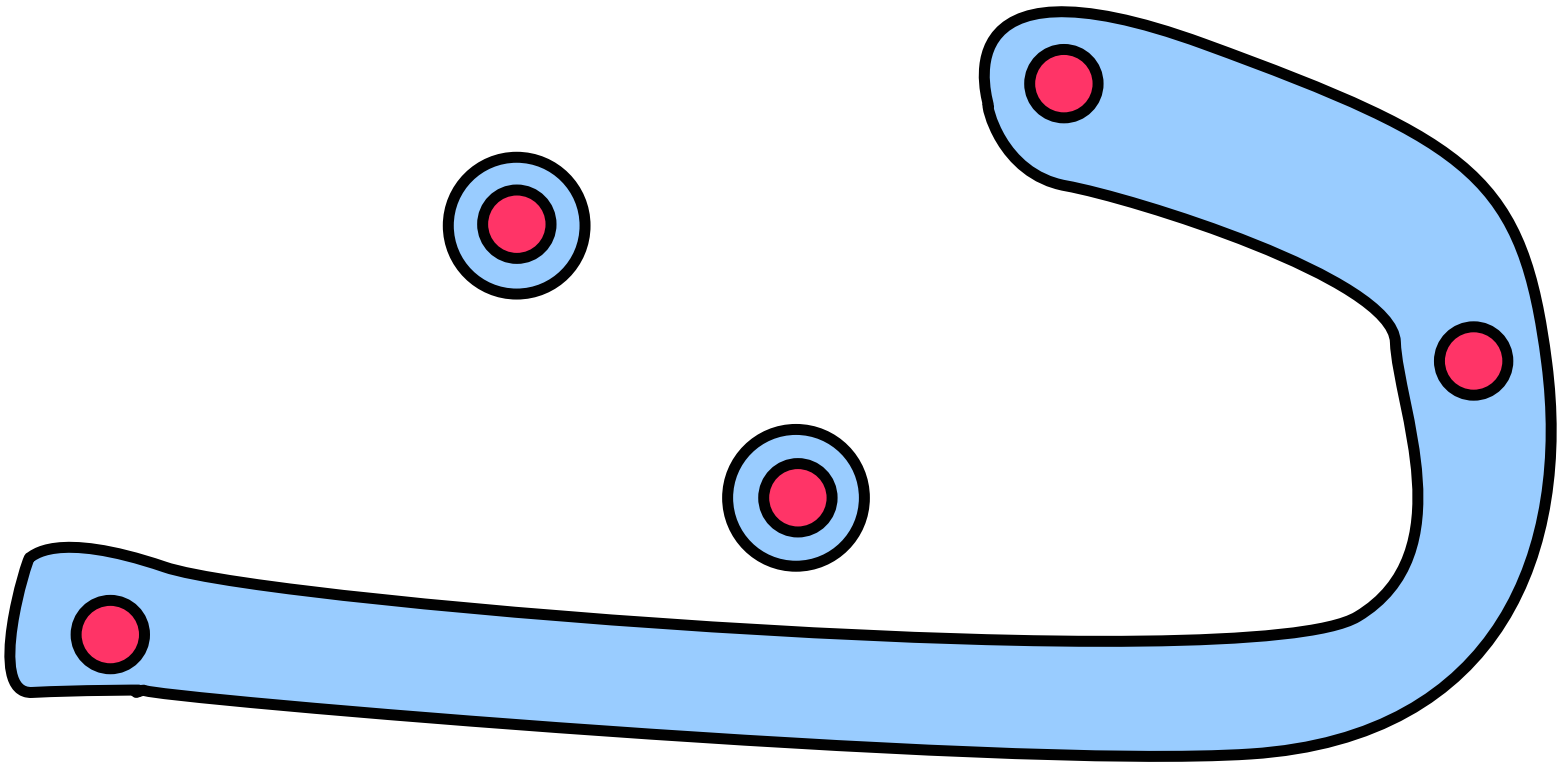
NP-Completeness – Graph Devices

Undirected graph $G = (V, E)$, $|V| \geq 4$.



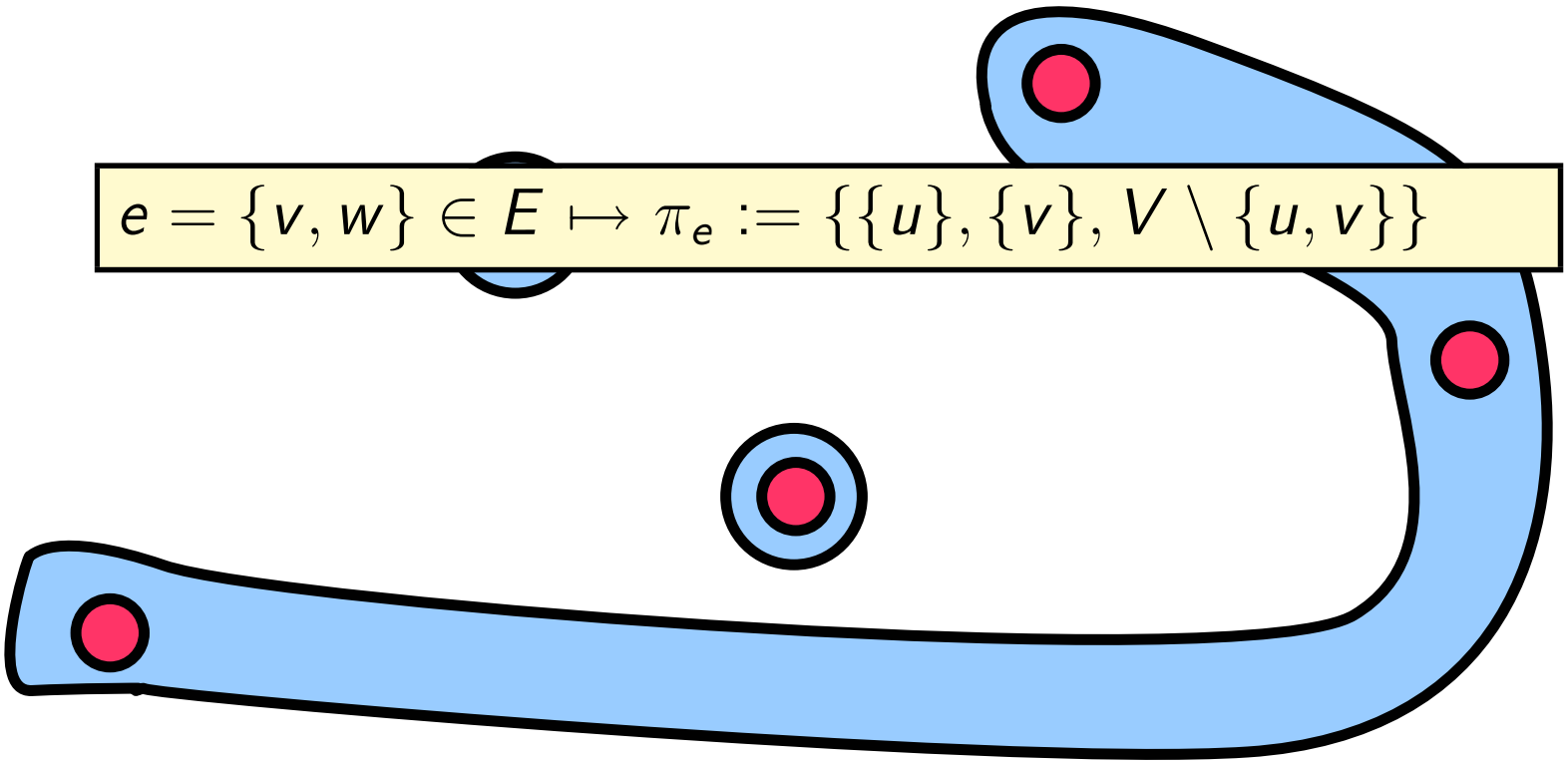
NP-Completeness – Graph Devices

Undirected graph $G = (V, E)$, $|V| \geq 4$.



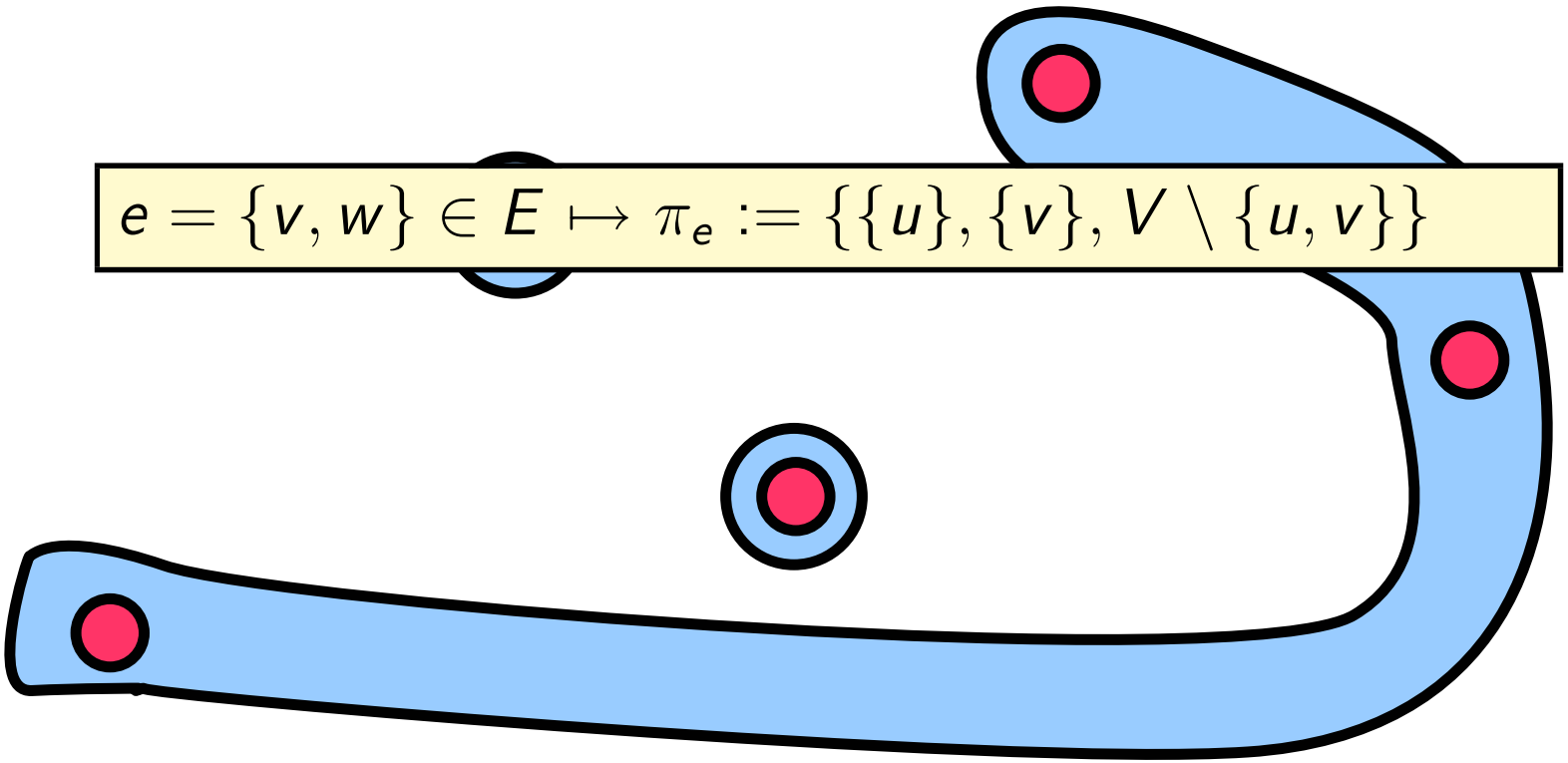
NP-Completeness – Graph Devices

Undirected graph $G = (V, E)$, $|V| \geq 4$.



NP-Completeness – Graph Devices

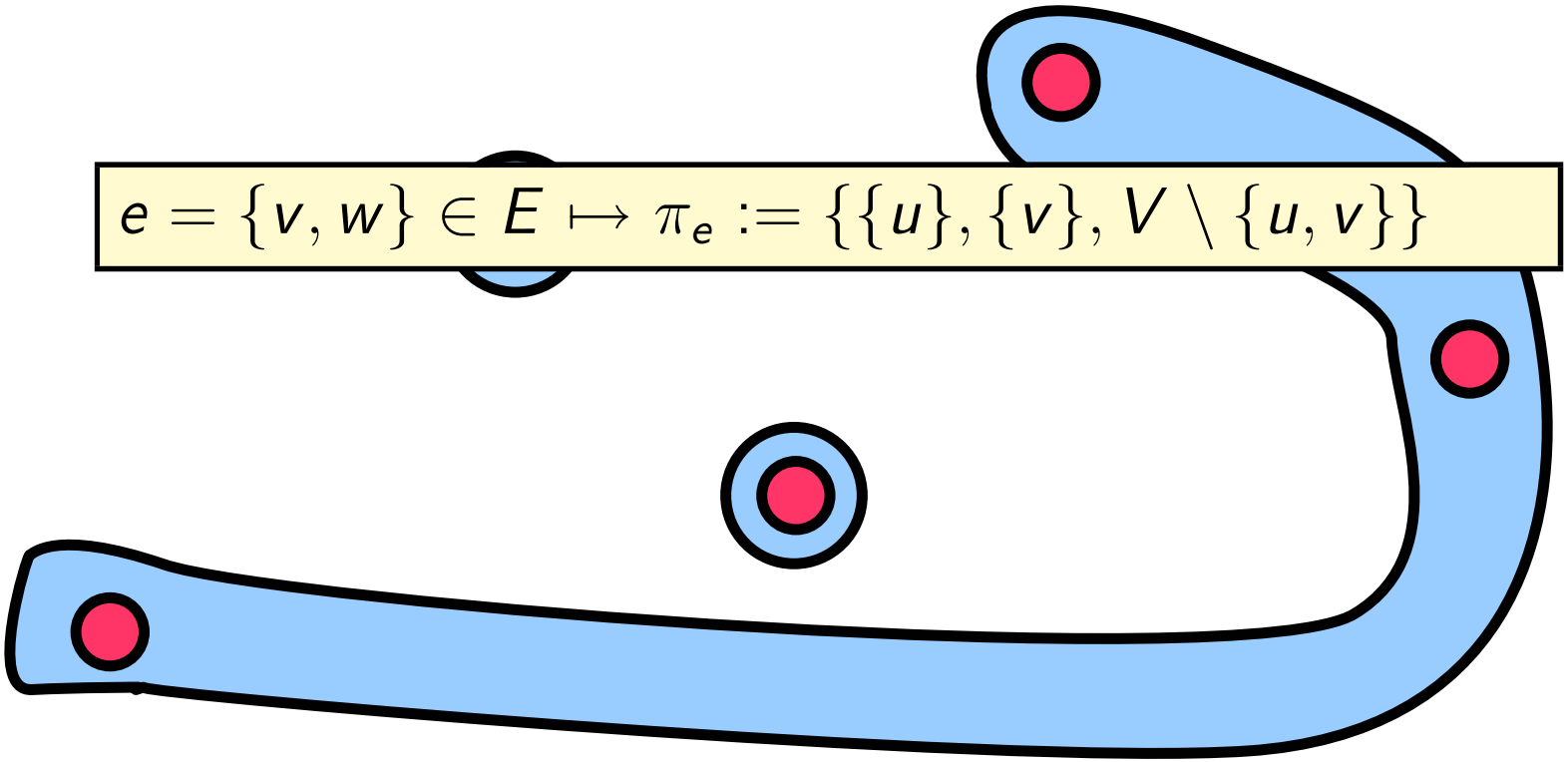
Undirected graph $G = (V, E)$, $|V| \geq 4$.



$$e = \{v, w\} \in E \mapsto \pi_e := \{\{u\}, \{v\}, V \setminus \{u, v\}\}$$

Lemma. G' contained in $G \iff D(G') \leq D(G)$

Undirected graph $G = (V, E)$, $|V| \geq 4$.



Lemma. G' contained in $G \iff D(G') \leq D(G)$

Corollary. G contains k-CLIQUE $\iff D(K_k) \leq D(G)$

ASD Reducibility – Some Challenges

$$L_2 \times L_3 \times L_2 \overset{?}{\leq} L_2 \times L_5$$

$$L_3 \times L_2 \overset{?}{\leq} L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \overset{?}{\leq} L_4 \times L_4$$

ASD Reducibility – Some Challenges

$$L_2 \times L_3 \times L_2 \overset{?}{\leq} L_2 \times L_5$$

$$L_3 \times L_2 \overset{?}{\leq} L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \overset{?}{\leq} L_4 \times L_4$$

ASD Reducibility – Some Challenges

$$L_2 \times L_3 \times L_2 \overset{?}{\leq} L_2 \times L_5$$

Storage Capacity. $C(D) := \max\{\log s \mid C_s \leq D\}$.

$$L_5 \times L_3 \overset{.}{\leq} L_4 \times L_4$$

ASD Reducibility – Some Challenges

$$L_2 \times L_3 \times L_2 \overset{?}{\leq} L_2 \times L_5$$

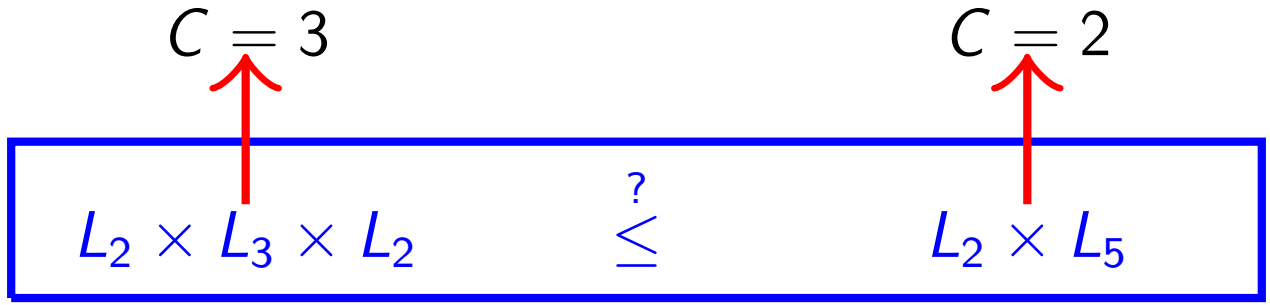
Storage Capacity. $C(D) := \max\{\log s \mid C_s \leq D\}$.

$$L_5 \times L_3 \overset{\cdot}{<} L_4 \times L_4$$

Properties.

- $D \leq D' \Longrightarrow C(D) \leq C(D')$
- $C(D \times D') = C(D) + C(D')$
- $C(L_n) = 1$

ASD Reducibility – Some Challenges



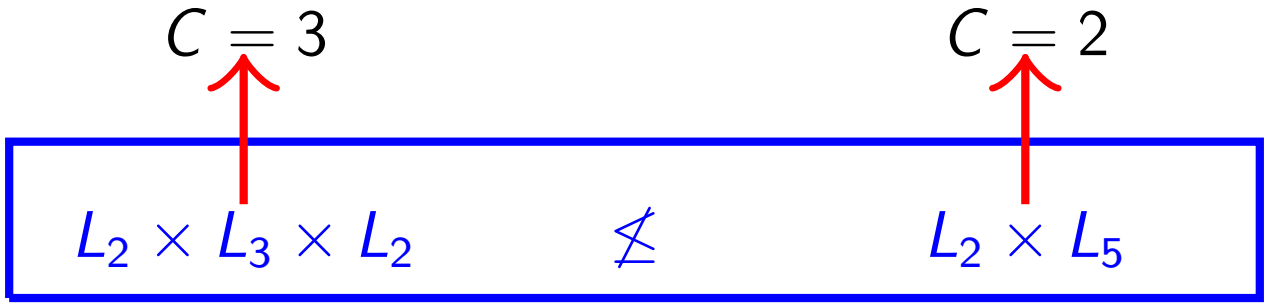
Storage Capacity. $C(D) := \max\{\log s \mid C_s \leq D\}$.

$L_5 \times L_3 \overset{\cdot}{<} L_4 \times L_4$

Properties.

- $D \leq D' \Longrightarrow C(D) \leq C(D')$
- $C(D \times D') = C(D) + C(D')$
- $C(L_n) = 1$

ASD Reducibility – Some Challenges



Storage Capacity. $C(D) := \max\{\log s \mid C_s \leq D\}$.

$L_5 \times L_3 \quad < \quad L_4 \times L_4$

Properties.

- $D \leq D' \Longrightarrow C(D) \leq C(D')$
- $C(D \times D') = C(D) + C(D')$
- $C(L_n) = 1$

ASD Reducibility – Some Challenges

$$L_2 \times L_3 \times L_2 \not\leq L_2 \times L_5$$

$$L_3 \times L_2 \overset{?}{\leq} L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \overset{?}{\leq} L_4 \times L_4$$

ASD Reducibility – Some Challenges

Imperfectness Index. $i(D) := \min\{k \mid C_{|\mathcal{S}(D)|} \leq D^{(k)}\}$.

$$L_3 \times L_2 \overset{?}{\leq} L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \overset{?}{\leq} L_4 \times L_4$$

ASD Reducibility – Some Challenges

Imperfectness Index. $i(D) := \min\{k \mid C_{|\mathcal{S}(D)|} \leq D^{(k)}\}$.

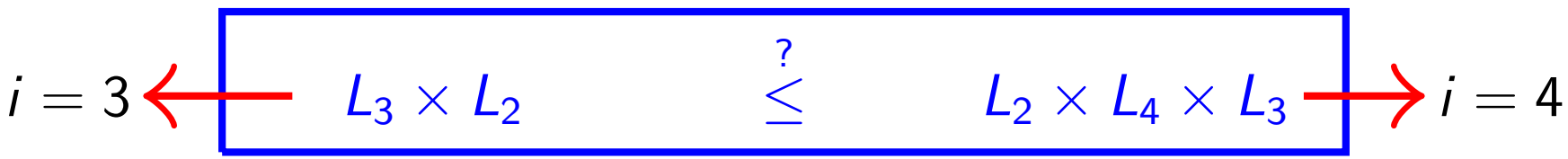
$$L_3 \times L_2 \overset{?}{\leq} L_2 \times L_4 \times L_3$$

Properties.

- $D \leq D' \Longrightarrow i(D) \geq i(D')$
- $i(D \times D') = \max\{i(D), i(D')\}$
- $i(L_n) = n$

ASD Reducibility – Some Challenges

Imperfectness Index. $i(D) := \min\{k \mid C_{|\mathcal{S}(D)|} \leq D^{(k)}\}$.



Properties.

- $D \leq D' \Longrightarrow i(D) \geq i(D')$
- $i(D \times D') = \max\{i(D), i(D')\}$
- $i(L_n) = n$

ASD Reducibility – Some Challenges

Imperfectness Index. $i(D) := \min\{k \mid C_{|\mathcal{S}(D)|} \leq D^{(k)}\}$.

$i = 3$ ← $L_3 \times L_2 \not\leq L_2 \times L_4 \times L_3$ → $i = 4$

Properties.

- $D \leq D' \Longrightarrow i(D) \geq i(D')$
- $i(D \times D') = \max\{i(D), i(D')\}$
- $i(L_n) = n$

ASD Reducibility – Some Challenges

$$L_2 \times L_3 \times L_2 \not\leq L_2 \times L_5$$

$$L_3 \times L_2 \not\leq L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \overset{?}{\leq} L_4 \times L_4$$

Outline

ASD Factorizations

$D_1, \ldots, D_\ell$ **factorization** of D if

$$D \equiv D_1 \times \cdots \times D_\ell.$$

D is **prime** if

$$D \equiv D_1 \times D_2.$$

implies D_1 or D_2 is trivial.

(Open) Question. Is the factorization in prime ASD's unique?

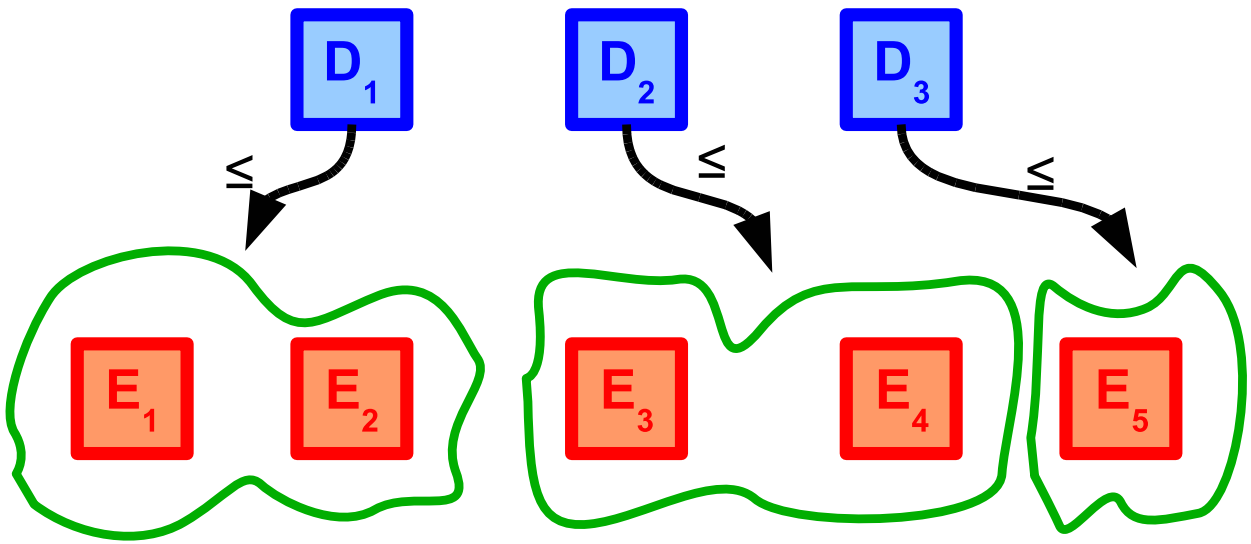
ASD Factorizations – 2

Lemma. $D_1 \times \cdots \times D_m$ and $E_1 \times \cdots \times E_n$ products of binary ASD's with equal total state size.

$$D_1 \times \cdots \times D_m \leq E_1 \times \cdots \times E_n$$

if and only if $\exists$ partition $\{\mathcal{J}_1, \ldots, \mathcal{J}_m\}$ of $\{1, \ldots, n\}$ with

$$D_i \leq \bigtimes_{j \in \mathcal{J}_i} E_j \text{ for all } i = 1, \ldots, m.$$



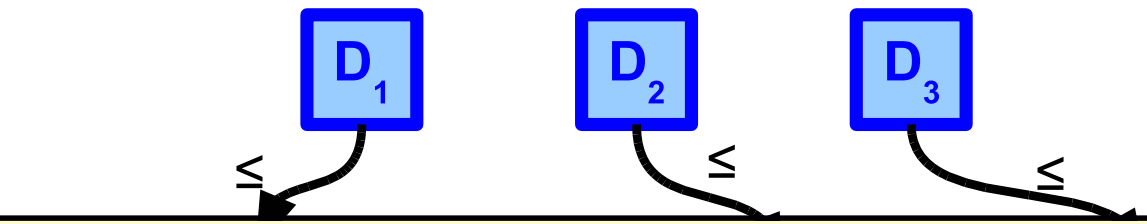
ASD Factorizations – 2

Lemma. $D_1 \times \cdots \times D_m$ and $E_1 \times \cdots \times E_n$ products of binary ASD's with equal total state size.

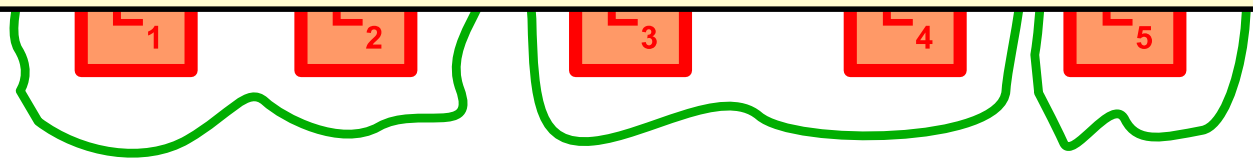
$$D_1 \times \cdots \times D_m \leq E_1 \times \cdots \times E_n$$

if and only if $\exists$ partition $\{\mathcal{J}_1, \ldots, \mathcal{J}_m\}$ of $\{1, \ldots, n\}$ with

$$D_i \leq \bigtimes_{j \in \mathcal{J}_i} E_j \text{ for all } i = 1, \ldots, m.$$



Theorem. The factorization of an ASD D in terms of binary ASD's is unique.



ASD Factorizations – 3

$$L_2 \times L_3 \times L_2 \not\leq L_2 \times L_5$$

$$L_3 \times L_2 \not\leq L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \overset{?}{\leq} L_4 \times L_4$$

ASD Factorizations – 3

$$L_2 \times L_3 \times L_2 \not\leq L_2 \times L_5$$

$$L_3 \times L_2 \not\leq L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \overset{?}{\leq} L_4 \times L_4$$

$L_5 \not\leq L_4 \Rightarrow$ no partition exists

ASD Factorizations – 3

$$L_2 \times L_3 \times L_2 \quad \not\leq \quad L_2 \times L_5$$

$$L_3 \times L_2 \quad \not\leq \quad L_2 \times L_4 \times L_3$$

$$L_5 \times L_3 \quad \not\leq \quad L_4 \times L_4$$

$L_5 \not\leq L_4 \Rightarrow$ no partition exists

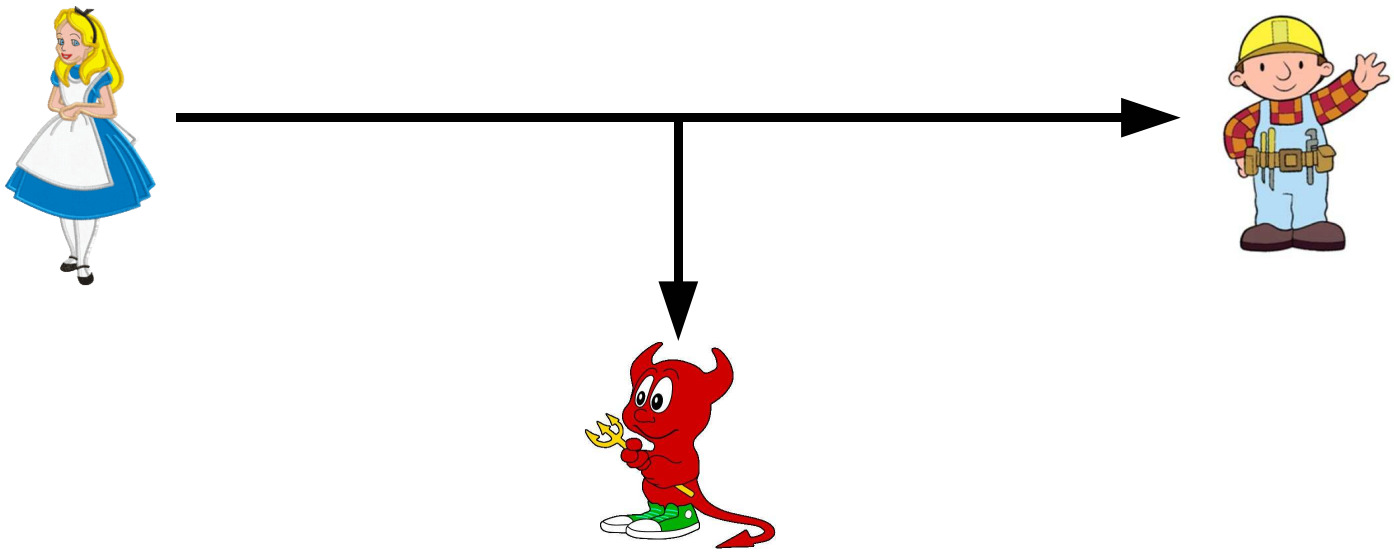
Outline

(Some) Open Problems

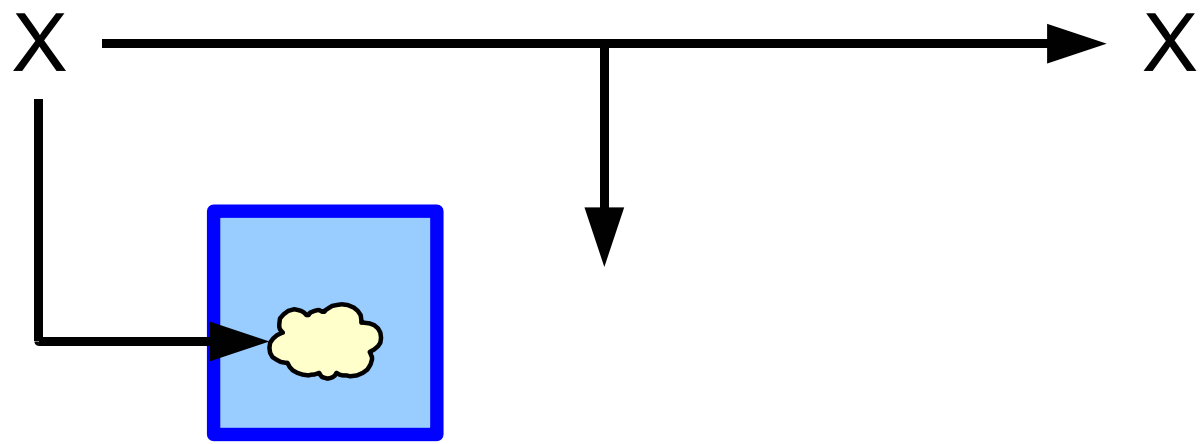
- Study general notions of reducibility
- Framework for probabilistic storage devices
- Show unique factorization theorem for ASD's / find counterexamples
- Find new application scenarios

Questions?

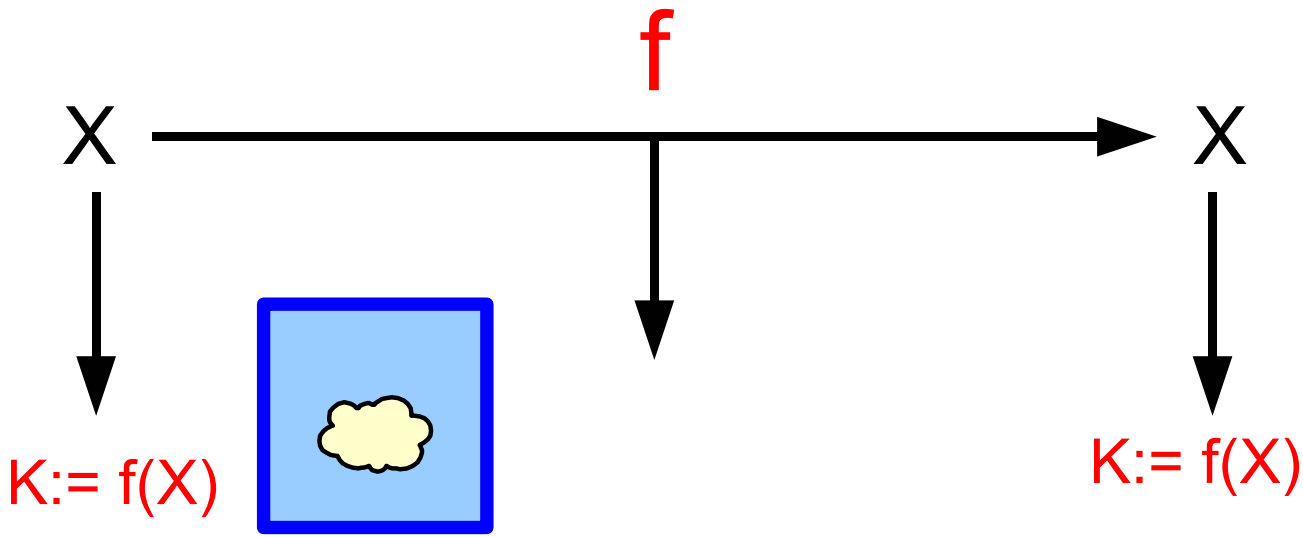
Application: Privacy Amplification



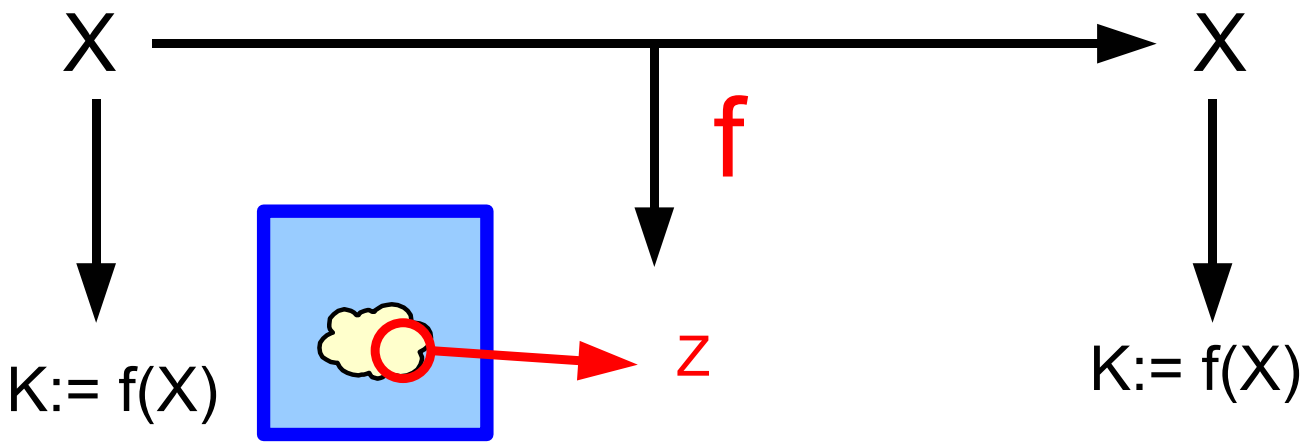
Application: Privacy Amplification



Application: Privacy Amplification

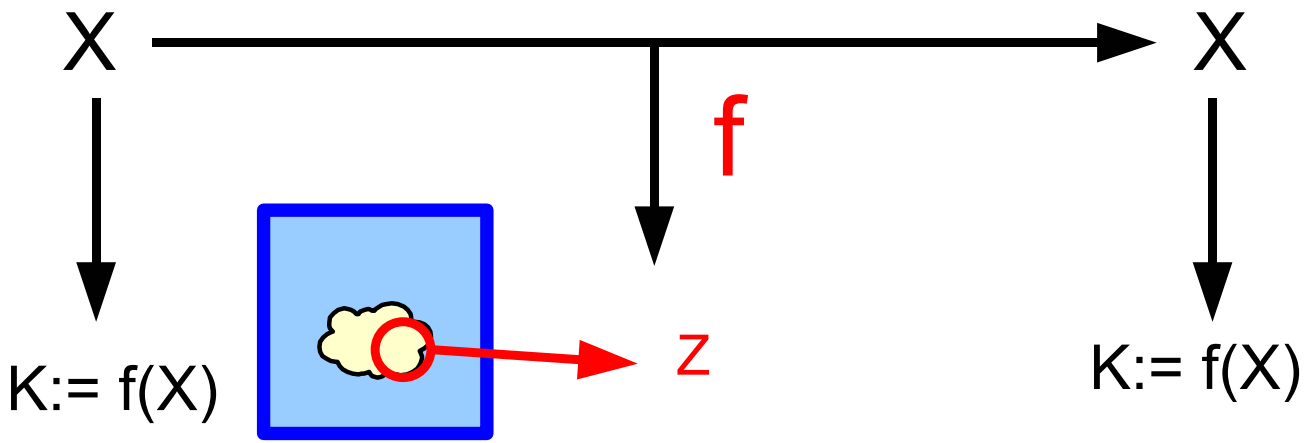


Application: Privacy Amplification



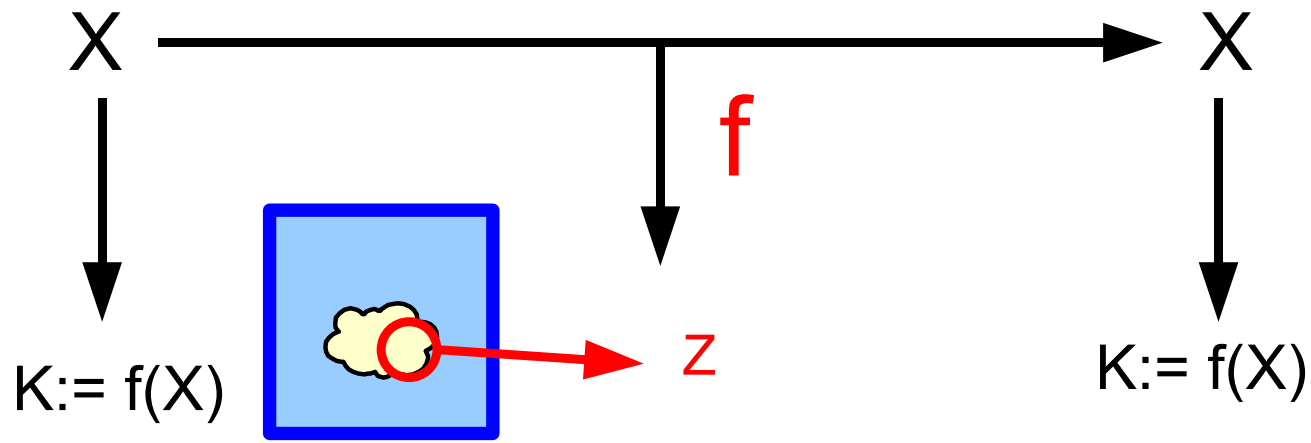
Application: Privacy Amplification

Goal. $\forall$ retrieval ops: Z gives no information about K



Application: Privacy Amplification

Goal. $\forall$ retrieval ops: Z gives no information about K



Previous work

- classical PA [BBR88,BBCM95]
- quantum PA [KMR05,RK05]
- ...

ASD Equivalence – Complexity

Theorem. ASD Equivalence $\mathcal{NP}$-complete $\Rightarrow$ $\mathcal{PH}$ collapses to 2nd level.

ASD Equivalence – Complexity

Theorem. ASD Equivalence $\mathcal{NP}$-complete $\Rightarrow$ $\mathcal{PH}$ collapses to 2nd level.

Remarks

- Similar result as for GI
- Unlikely to be $\mathcal{NP}$-complete