arXiv:0706.2746v1 [cs.DM] 19 Jun 2007

Abstract Storage Devices

Robert König[*]   Ueli Maurer[†]   Stefano Tessaro[‡]

Abstract

A quantum storage device differs radically from a conventional physical storage device. Its state can be set to any value in a certain (infinite) state space, but in general every possible read operation yields only partial information about the stored state.

The purpose of this paper is to initiate the study of a combinatorial abstraction, called *abstract storage device* (ASD), which models deterministic storage devices with the property that only partial information about the state can be read, but that there is a degree of freedom as to which partial information should be retrieved.

This concept leads to a number of interesting problems which we address, like the reduction of one device to another device, the equivalence of devices, direct products of devices, as well as the factorization of a device into primitive devices. We prove that every ASD has an equivalent ASD with minimal number of states and of possible read operations. Also, we prove that the reducibility problem for ASD's is $\mathcal{NP}$-complete, that the equivalence problem is at least as hard as the graph isomorphism problem, and that the factorization into binary-output devices (if it exists) is unique.

Keywords: Discrete Structures, Storage Devices, $\mathcal{NP}$-Completeness, Computational Complexity, Factorizations.

1 Introduction

1.1 Motivation

The term storage device is conventionally used for a physical device with a *write* and a *read* operation which can store data reliably, i.e., with the property that the read operation yields an exact copy of the data previously written into the device. In this paper, we consider a generalized type of storage devices for which the write operation consists of setting the device's state to some value in

---

[*]Centre for Quantum Computation, University of Cambridge, United Kingdom, E-mail: r.t.koenig@damtp.cam.ac.uk

[†]Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland, E-mail: maurer@inf.ethz.ch

[‡]Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland, E-mail: tessaros@inf.ethz.ch

the state space, and the subsequent read operation consists of performing some measurement and provides some (usually only partial) information about the state.

Such a storage device is a relevant special case of a general physical system. The state of such a system can in general not be measured exactly. This may be due to intrinsic reasons. For example, it is inherently impossible to perfectly measure a quantum state[1]. Also, practical constraints (like the required efficiency) may impose an unavoidable inaccuracy to the measurement of the state. For instance, a tape only allows to efficiently retrieve its content *locally* by sequentially accessing the small portion of it being of interest.

The task of a conventional storage device (e.g., a hard disc) is to store information reliably. The design goal of such a system is therefore to define a finite subset of its state space (as large as possible) such that the available read operation allows to distinguish different such states with negligible error probability. For this reason, a conventional storage device is characterized by its *storage capacity*, i.e., the number of bits that can be stored reliably in it.

Here, we take a more general approach to storage devices, by modeling explicitly the fact that, on one hand, a read operation provides only partial information about the state, but that, on the other hand, many different such read operations can be available. We typically assume that only one of these operations can be performed, but that the choice is free.

There are different motivations for considering such a setting. A first motivation is *quantum cryptography* or, more precisely, *privacy amplification*, the last step of a quantum key agreement protocol (see [6]). In simplified terms, an adversary is assumed to have access to a bit string S of length n, shared by the legitimate users, and can store information about S in a 2^k-dimensional quantum device, where $k < n$. Since the (reliable) storage capacity of the device is only k, the adversary cannot store S perfectly. Later, the legitimate users select a hash function h from n bits to t bits (where $t < k$) at random from a class of such functions, and the adversary can now perform a measurement of the quantum state, *depending* on the choice of h. In this context, the goal is to prove that every such measurement yields only a negligible amount of information about $h(S)$. One can naturally generalize the setting of privacy amplification to other types of storage devices.

As an additional motivating example, one can consider the following game: An entity, say Alice, is given access to an n-bit string $s = [s_1, \ldots, s_n]$ about which she stores partial information. Later, she will learn a function f drawn from a given set and will have to guess the output $f(s)$. For example, this set of functions might consist of all linear predicates $a_1 s_1 + \cdots + a_n s_n \pmod 2$ for some $a_1, \ldots, a_n \in \{0, 1\}$. A natural question one may ask is finding the minimal amount of reliable storage required to win this game. More generally, one may be interested in deciding whether keeping information about s in a certain storage device suffices to succeed in the game. Also, one may even want to compare such games in the sense of determining whether one game is strictly

---

[1]unless it is known to be one of a set of orthogonal states

more difficult than another one. Similar games, which may be of independent interest, occur in the security analyses of certain cryptographic schemes.

The purpose of this paper is to initiate the study of a combinatorial abstraction, called *abstract storage device (ASD)*, which models the described property that only partial information about the state can be read, but that there is a degree of freedom as to which partial information should be retrieved. Both generalized storage devices as well as the above game can be described as an ASD. Here we only consider *deterministic* storage devices, i.e., we analyze the case with no error probability. This is similar in spirit to the investigation of the *zero-error capacity* [8] in communication theory. Like there, the treatments of the zero-error and the negligible-error cases are quite different and deserve separate investigation.

A natural problem related to the above game is *reducibility* of devices, which asks for deciding whether a certain device can be implemented by a second one. Additionally, this concept directly implies a notion of *equivalence* for devices.

In many branches of science, a common approach to analyze complex objects is to represent such objects as compositions of simpler and better-understood ones. From a mathematical point of view, product factorizations of discrete structures have been studied in many forms in the past, for instance in the context of graph products and of finite relational structures (see [4, 5] for respective surveys). Along similar lines, one can introduce *direct products* of ASD's and study direct product factorizations into simpler primitive devices.

1.2   Contributions and Outline of This Paper

The main contribution of this paper is the introduction of abstract storage devices (ASD). Section 3.1 presents this abstraction and gives some examples. There, we also define direct products of ASD's. Moreover, we state the problems of reducibility and equivalence of ASD's in Section 3.2.

We prove in Section 3.3 that every ASD has an equivalent ASD which has both a minimal number of states *and* a minimal number of possible read operations, and we discuss properties of such devices with respect to reducibility and equivalence.

Also, we present and analyze relevant quantities related to ASD's. The *storage capacity* provides a measure of the amount of information that can be reliably stored in a device, while the *state complexity* characterizes the minimal amount of reliable storage needed to simulate the device. Finally, the *perfectness index* of an ASD's is the minimal number of read operations needed to entirely retrieve the state of a device. These quantities yield easily-verifiable necessary conditions for reducibility, and Section 3.4 is devoted to their discussion.

In Section 4, we prove the general problem of deciding reducibility of ASD's to be $\mathcal{NP}$-complete, whereas deciding equivalence of ASD's is shown to be at least as difficult as deciding the isomorphism of graphs. Furthermore, the latter problem is unlikely to be $\mathcal{NP}$-complete, as its $\mathcal{NP}$-completeness would imply a collapse of the polynomial hierarchy.

3

The last section (Section 5) addresses the direct product factorization of ASD's. We prove that every device admits a unique factorization in terms of binary devices, if such a factorization exists. This result can be seen as a first step towards answering the general question of the existence of unique factorizations into (prime) ASD's, which we state as an open problem.

Relevant basic facts about set partitions and the partition lattice are briefly reviewed in Section 2.

2 Preliminaries

Throughout this paper, we make use of capital calligraphic letters to denote sets. An (undirected) *graph* is an ordered pair $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of *vertices*, and $\mathcal{E} \subseteq \binom{\mathcal{V}}{2}$ is the set of *edges* of $\mathcal{G}$.

A *(set) partition* π of a set $\mathcal{S}$ is a family $\{\mathcal{B}_1, \ldots, \mathcal{B}_k\}$ of disjoint subsets of $\mathcal{S}$, called *blocks*, with the property that $\bigcup_{i=1}^{k} \mathcal{B}_i = \mathcal{S}$. We write $s \equiv_{\pi} t$ whenever both elements $s, t \in \mathcal{S}$ are in the same block of π. Moreover, we denote by $\Pi(\mathcal{S})$ the set of partitions of $\mathcal{S}$. We say that $\pi \in \Pi(\mathcal{S})$ *refines* $\pi' \in \Pi(\mathcal{S})$, denoted $\pi \sqsubseteq \pi'$, if for all $\mathcal{B} \in \pi$ there exists a $\mathcal{B}' \in \pi'$ such that $\mathcal{B} \subseteq \mathcal{B}'$. Recall that $(\Pi(\mathcal{S}); \sqsubseteq)$ is a bounded lattice (cf. e.g. [3]), with the minimal element being $id_{\mathcal{S}} = \{\{s\} \mid s \in \mathcal{S}\}$ and the maximal element being $\{\mathcal{S}\}$. The *meet* of $\pi, \pi' \in \Pi(\mathcal{S})$ is the partition $\pi \wedge \pi' = \{\mathcal{B} \cap \mathcal{B}' \mid \mathcal{B} \in \pi, \mathcal{B}' \in \pi', \mathcal{B} \cap \mathcal{B}' \neq \emptyset\}$, whereas their *join* $\pi \vee \pi'$ is such that $x \equiv_{\pi \vee \pi'} y$ if and only if we can find a sequence of elements $x = x_0, x_1, \ldots, x_r = y$ (for some r) such that $x_i \equiv_{\pi} x_{i+1}$ or $x_i \equiv_{\pi'} x_{i+1}$ holds for all $i = 0, \ldots, r-1$. For a set Π of partitions, we generally write $\bigwedge \Pi = \bigwedge_{\pi \in \Pi} \pi$ and $\bigvee \Pi = \bigvee_{\pi \in \Pi} \pi$. Also, such a set Π is called an *antichain* if $\pi \not\sqsubseteq \pi'$ for all distinct $\pi, \pi' \in \Pi$.

The *direct product* of the partitions $\pi \in \Pi(\mathcal{S})$ and $\pi' \in \Pi(\mathcal{S}')$ is the partition $\pi \times \pi' = \{\mathcal{B} \times \mathcal{B}' \mid \mathcal{B} \in \pi, \mathcal{B}' \in \pi'\} \in \Pi(\mathcal{S} \times \mathcal{S}')$. In particular, we have $(s, s') \equiv_{\pi \times \pi'} (t, t')$ if and only if $s \equiv_{\pi} s'$ and $t \equiv_{\pi'} t'$ for all $s, t \in \mathcal{S}$, $s', t' \in \mathcal{S}'$. Let now $\pi, \rho \in \Pi(\mathcal{S})$, $\pi', \rho' \in \Pi(\mathcal{S}')$ be partitions. Then, both equalities $(\pi \wedge \rho) \times (\pi' \wedge \rho') = (\pi \times \pi') \wedge (\rho \times \rho')$ and $(\pi \vee \rho) \times (\pi' \vee \rho') = (\pi \times \pi') \vee (\rho \times \rho')$ hold. Furthermore, $\pi \times \pi' \sqsubseteq \rho \times \rho'$ is satisfied if and only if $\pi \sqsubseteq \pi'$ and $\rho \sqsubseteq \rho'$. We refer the reader to Appendix A for a proof of these facts.

Given sets $\mathcal{S}, \mathcal{S}'$, a partition $\pi \in \Pi(\mathcal{S}')$, and some function $\phi : \mathcal{S} \to \mathcal{S}'$, we define $\pi \circ \phi \in \Pi(\mathcal{S})$ as the partition such that $x \equiv_{\pi \circ \phi} y$ if and only if $\phi(x) \equiv_{\pi} \phi(y)$ for all $x, y \in \mathcal{S}$. Notice that $(\pi \circ \phi) \wedge (\pi' \circ \phi) = (\pi \wedge \pi') \circ \phi$, and $(\pi \circ \phi) \vee (\pi' \circ \phi) = (\pi \vee \pi') \circ \phi$. Moreover, the *kernel (partition)* of a function $f : \mathcal{X} \to \mathcal{Y}$ is $\ker(f) = \{f^{-1}(\{y\}) \mid y \in \mathrm{range}(f)\}$. Given a further function $\phi : \mathcal{S} \to \mathcal{X}$, we have $\ker(f \circ \phi) = \ker(f) \circ \phi$.

Finally, recall that a k-variate *lattice polynomial* p in the variables $x_1, \ldots, x_k$ is a formal expression of the form either (i) x_i for $i = 1, \ldots, k$, or (ii) one of $q(x_1, \ldots, x_k) \wedge q'(x_1, \ldots, x_k)$ and $q(x_1, \ldots, x_k) \vee q(x_1, \ldots, x_k)$ for k-variate lattice polynomials q, q'. Given partitions $\pi_1, \ldots, \pi_k, \rho_1, \ldots, \rho_k$ such that $\pi_i \sqsubseteq \rho_i$ for $i = 1, \ldots, k$, then $p(\pi_1, \ldots, \pi_k) \sqsubseteq p(\rho_1, \ldots, \rho_k)$ holds for every k-variate lattice polynomial p.

3 Abstract Storage Devices

3.1 Definition

In the following, we look at storage devices used by two entities, called the *writer* and the *reader*, respectively[2]. The writer writes to such a device by selecting a state s from the *state space* of the device. The reader subsequently chooses a (possibly randomized) function g mapping states to output symbols from a set of possible such mappings, and obtains the output $g(s)$. Note, however, that the actual labeling of the outputs is irrelevant, as long as the reader knows a complete description of the function to be read out. In particular, as we only focus on devices whose behavior is entirely *deterministic*, we abstract from the notion of an output domain and we solely describe the kernel partitions of the functions of the storage device. This allows us to formulate the following combinatorial abstraction of deterministic devices.

Definition 1. An *abstract storage device (ASD)* D is a pair $D = \left(\mathcal{S}^D, \Pi^D\right)$, where $\mathcal{S}^D$ is a set called the *state space of D*, and Π^D is a family of partitions of $\mathcal{S}^D$, called the *partition set of D*.

For an ASD D, a *write operation* of the writer consists in selecting a state $s \in \mathcal{S}^D$, and in a subsequent *read operation* the reader selects a partition $\pi \in \Pi^D$ and learns the (unique) block $\mathcal{B} \in \pi$ such that $s \in \mathcal{B}$. We assume that a single read operation is performed. Furthermore, in the following, we are going to focus on ASD's with finite state space and partition set.

Whenever $id_{\mathcal{S}^D} \in \Pi^D$, the reader can distinguish any pair of states with a single read operation. In this case, D is called *perfect*, and it is called *non-perfect* otherwise. If the partition set contains only the trivial partition $\{\mathcal{S}^D\}$, the ASD is called *trivial*. Moreover, it is called *r-regular* if $|\pi| = r$ for all $\pi \in \Pi^D$. In particular, 2-regular ASD's are also called *binary*.

The following are examples of ASD's.

Perfect device. For a given set $\mathcal{X}$, the ASD $C_{\mathcal{X}}$ has state space $\mathcal{X}$ and its state can be retrieved perfectly, that is, $\Pi^D = \{id_{\mathcal{X}}\}$. The special case where $\mathcal{X} = \{1, \ldots, m\}$ for $m \in \mathbb{N}$ is denoted as C_m.

Projective device. For $i \in \{1, \ldots, n\}$, we denote by $p_i : \{0,1\}^n \to \{0,1\}$ the function such that $p_i(x_1, \ldots, x_n) = x_i$ for all $(x_1, \ldots, x_n) \in \{0,1\}^n$. The *projective device* P_n has state space $\mathcal{S}^{P_n} = \{0,1\}^n$ and its partition set is $\Pi^{P_n} = \{\ker(p_i) \,|\, i = 1, \ldots, n\}$. This device is similar to the *1-out-of-n oblivious transfer (OT)* primitive considered in cryptography (introduced in [7]). One may also extend this device to allow for retrieving any $k < n$ consecutive bits of the state. Such a device could be used to model a tape-based storage device.

---

[2]These entities are not necessarily distinct in a physical sense.

Linear device. The *linear device* $L_{n,k}$ where $n \geq k$ is the ASD having state space $\mathcal{S}^{L_{n,k}} = \{0,1\}^n$, and the partition set is the set of the kernel partitions of all linear maps $\{0,1\}^n \to \{0,1\}^k$. We denote by L_n the binary ASD $L_{n,1}$.

One way of constructing a complex device from simpler devices is the parallel composition of two ASD's to obtain a new ASD modeling a setting where the reader and the writer use both devices in a *non-adaptive* fashion. That is, if D has state s and D' has state s', the reader first selects *both* partitions $\pi \in \Pi^D$ and $\pi' \in \Pi^{D'}$, and only subsequently learns the unique blocks $\mathcal{B} \in \pi$, $\mathcal{B}' \in \pi'$ such that $s \in \mathcal{B}$ and $s' \in \mathcal{B}'$.

Definition 2. The *direct product* $D \times D'$ of the ASD's D, D' is the ASD with $\mathcal{S}^{D \times D'} = \mathcal{S}^D \times \mathcal{S}^{D'}$ and $\Pi^{D \times D'} = \{\pi \times \pi' \mid \pi \in \Pi^D, \pi' \in \Pi^{D'}\}$.

For example, since $id_{\mathcal{S}^D \times \mathcal{S}^{D'}} = \pi \times \pi'$ holds if and only if $\pi = id_{\mathcal{S}^D}$ and $\pi' = id_{\mathcal{S}^{D'}}$, we immediately see that $D \times D'$ is perfect if and only if both D and D' are perfect.

In general, we may want to look at more than a single read operation. For an integer $k \geq 1$ and an ASD D, we denote as $D^{(k)}$ the ASD with $\mathcal{S}^{D^{(k)}} = \mathcal{S}^D$ and $\Pi^{D^{(k)}} = \left\{ \bigwedge_{i=1}^k \pi_i \;\middle|\; \pi_i \in \Pi^D, i = 1, \ldots, k \right\}$. It models the scenario where the reader is allowed to perform (at most) k non-adaptive read operations, i.e. given state $s \in \mathcal{S}^D$, it first chooses k partitions $\pi_1, \ldots, \pi_k \in \Pi^D$ to be retrieved, and only subsequently learns the corresponding blocks $\mathcal{B}_1 \in \pi_1, \ldots, \mathcal{B}_k \in \pi_k$ such that $s \in \bigcap_{i=1}^k \mathcal{B}_i$.

Note that both the direct product and the device $D^{(k)}$ can be extended to allow for adaptive read operations, as it essentially suffices to consider all partitions induced by every possible (deterministic) retrieval strategy. However, we do not address this case in this paper.

3.2 Reducibility and Equivalence

In the problem of reducibility of ASD's, we want to decide whether an ASD D can be implemented by a second ASD D'. This is formalized by the following definition.

Definition 3. We say that an ASD D is *reducible* to an ASD D', denoted $D \leq D'$, if there exist functions $\phi : \mathcal{S}^D \to \mathcal{S}^{D'}$ and $\alpha : \Pi^D \to \Pi^{D'}$ such that $\alpha(\pi) \circ \phi \sqsubseteq \pi$ for all $\pi \in \Pi^D$. Such a pair of functions (ϕ, α) is called a *reduction of D to D'*.

In order to clarify this concept, consider the following abstraction in terms of ASD's of the game introduced in Section 1.1. The writer and the reader are given an ASD D' as well as the description of a further ASD D. The writer is told an arbitrary state $s \in \mathcal{S}^D$ and selects the state $\phi(s) \in \mathcal{S}^{D'}$ for D'. Later, an arbitrary partition $\pi \in \Pi^D$ is revealed to the reader, and it performs a read operation for a partition $\alpha(\pi) \in \Pi^{D'}$. The goal is to find appropriate functions $\phi : \mathcal{S}^D \to \mathcal{S}^{D'}$ and $\alpha : \Pi^D \to \Pi^{D'}$ such the reader can *perfectly* guess

6

the unique block $\mathcal{B} \in \pi$ such that $s \in \mathcal{B}$ from the result of retrieving $\alpha(\pi)$ from D'. If such functions exist, the writer and the reader can simulate D using D'. Note that the ASD D itself can alternatively be seen as the specification of a particular game the writer and the reader try to win by using the ASD D'.

It is easy to see that the condition $\alpha(\pi) \circ \phi \sqsubseteq \pi$ must hold. Otherwise, there would be $s, s' \in \mathcal{S}^D$ such that $s \not\equiv_\pi s'$, but $\phi(s) \equiv_{\alpha(\pi)} \phi(s')$, and hence s and s' could not be distinguished. Conversely, if $\alpha(\pi) \circ \phi \sqsubseteq \pi$, then given state $s \in \mathcal{S}^D$ and $\mathcal{B}' \in \alpha(\pi)$ such that $\phi(s) \in \mathcal{B}'$, there exists a unique block $\mathcal{B} \in \pi$ such that $s \in \mathcal{B}$. Hence, Definition 3 expresses the precise condition in order for ϕ and α to be a winning strategy in the game.

Reducibility is a reflexive and transitive relation. However, it is not antisymmetric, and thus it is only a *quasi-order* on the set of ASD's. In this respect, we say that two ASD's D, D' are *equivalent*, denoted $D \equiv D'$, if both $D \leq D'$ and $D' \leq D$ hold. The relation $\equiv$ is an equivalence relation and reducibility implicitly defines a partial order on its equivalence classes.

The following proposition relates reducibility to direct products and multiple read operations.

Proposition 1. *Let D, D', E, E' be ASD's.*

(i) *If $D \leq D'$ and $E \leq E'$, then $D \times E \leq D' \times E'$.*

(ii) *If $D \leq D'$, then $D^{(k)} \leq D'^{(k)}$.*

Proof. The first claim is obvious. For the second one, let (ϕ, α) be a reduction of D to D'. Define $\tilde{\alpha} : \Pi^{D^{(k)}} \to \Pi^{D'^{(k)}}$ such that $\tilde{\alpha}(\bigwedge_{i=1}^k \pi_i) = \bigwedge_{i=1}^k \alpha(\pi_i)$. Then, $(\phi, \tilde{\alpha})$ reduces $D^{(k)}$ to $D^{(k')}$, since $\tilde{\alpha}(\bigwedge_{i=1}^k \pi_i) \circ \phi = \left(\bigwedge_{i=1}^k \alpha(\pi_i)\right) \circ \phi = \bigwedge_{i=1}^k (\alpha(\pi_i) \circ \phi) \sqsubseteq \bigwedge_{i=1}^k \pi_i$. $\qquad\square$

The perhaps most natural question related to storage devices is to determine how many bits of information can be reliably stored in it with the guarantee of no errors at read out. This quantity can be expressed in terms of the largest perfect device that can be reduced to the considered device.

Definition 4. The *storage capacity* of an ASD D is $C(D) = \max\{\log m \mid C_m \leq D, m \in \mathbb{N}\}$.

Equivalence of ASD's captures that two ASD's D and D' such that $D \equiv D'$ have the same behavior. As an example, it is clear that $D \times D' \equiv D' \times D$, and that $D \times (D' \times D'') \equiv (D \times D') \times D''$, that is, the direct product is commutative and associative with respect to equivalence. The direct product of $D_1, \ldots, D_n$ is thus simply written as $\times_{i=1}^n D_i$, and $D^k = \times_{i=1}^k D$ for any device D. Finally, notice that $D \times E \equiv D$ holds for any trivial device E.

3.3 Minimality

In this section, we have a closer look at the equivalence relation $\equiv$ and at the inner structure of its equivalence classes. In particular, we are interested in

the minimal number of states and partitions needed in order to implement the functionality of a certain ASD.

Definition 5. An ASD D is *state-minimal* if there is no equivalent device D' with $|\mathcal{S}^{D'}| < |\mathcal{S}^D|$. Furthermore, D is *partition-minimal* if there is no equivalent device D' with $|\Pi^{D'}| < |\Pi^D|$. Finally, we say that D is *minimal* if D is both state and partition-minimal.

For every ASD D there exist by definition equivalent ASD's D' and D'' such that D' is state-minimal and D'' is partition minimal. However, it is not clear whether an equivalent ASD exists that satisfies both, i.e., which is minimal. This is shown in the following theorem, which also provides an equivalent characterization of state and partition-minimality.

Theorem 2. *For an ASD D we have the following.*

(i) *D is state-minimal if and only if for all pairs of distinct states $s, s' \in \mathcal{S}^D$ there exists a set partition $\pi \in \Pi^D$ such that $s \not\equiv_\pi s'$. In particular, this holds if and only if $\bigwedge \Pi^D = id_{\mathcal{S}^D}$.*

(ii) *D is partition-minimal if and only if Π^D is an antichain (with respect to $\sqsubseteq$).*

Furthermore, for every ASD D, there exists a minimal ASD $D' \equiv D$.

Proof. We prove the two parts of the theorem separately.

(i) Assume that D is a state-minimal ASD and that there are distinct states $s_1, s_2 \in \mathcal{S}^D$ such that for all $\pi \in \Pi^D$ we have $s_1 \equiv_\pi s_2$. Construct a new ASD D' as follows. We define $\mathcal{S}^{D'} := \mathcal{S}^D - \{s_2\}$ and $\Pi^{D'} := \{\pi \circ \psi \mid \pi \in \Pi^D\}$ where $\psi : \mathcal{S}^{D'} \to \mathcal{S}^D$ is such that $\psi(s) = s$. Clearly, $D' \leq D$. On the other hand, one can easily see that $D \leq D'$: Define a function $\phi : \mathcal{S}^D \to \mathcal{S}^{D'}$ as

$$\phi(s) := \begin{cases} s, & \text{if } s \in \mathcal{S}^{D'}, \\ s_1, & \text{if } s = s_2, \end{cases}$$

and let α be such that $\alpha(\pi) = \pi \circ \psi$. Then (ϕ, α) is a reduction of D to D' as $\alpha(\pi) \circ \phi = \pi \circ (\psi \circ \phi) \sqsubseteq \pi$ because of the choice of s_1 and s_2.

For the converse, assume that for an ASD D we have for every pair of distinct states $s, s' \in \mathcal{S}^D$ a partition $\pi \in \Pi^D$ such that $s \not\equiv_\pi s'$. Assume now that D is not state-minimal. That is, there is a device D' with $|\mathcal{S}^{D'}| < |\mathcal{S}^D|$ and $D' \equiv D$. Let (ϕ, α) be a reduction of D to D'. There must be two states $s_1, s_2 \in \mathcal{S}^D$ such that $\phi(s_1) = \phi(s_2)$, and hence for all $\pi' \in \Pi^{D'}$ we have $\phi(s_1) \equiv_{\pi'} \phi(s_2)$. In particular, let $\pi \in \Pi^D$ be such that $s_1 \not\equiv_\pi s_2$. Then $\pi' \circ \phi \not\sqsubseteq \pi$ for all $\pi' \in \Pi^{D'}$, and thus $D \not\leq D'$.

It is straightforward to verify that $\bigwedge \Pi^D = id_{\mathcal{S}^D}$ holds if and only if for all $s, s' \in \mathcal{S}^D$ there exists $\pi \in \Pi^D$ such that $s \not\equiv_\pi s'$.

8

(ii) Assume that D is a partition-minimal ASD and that Π^D is not an antichain. That is, there exist distinct $\pi_1, \pi_2 \in \Pi^D$ such that $\pi_1 \sqsubseteq \pi_2$. We build a new device D' with $\mathcal{S}^{D'} := \mathcal{S}^D$ and $\Pi^{D'} := \Pi^D - \{\pi_2\}$. Clearly, we have $D' \leq D$. Furthermore, define $\phi : \mathcal{S}^D \to \mathcal{S}^{D'}$ as the identity and $\alpha : \Pi^D \to \Pi^{D'}$ such that

$$\alpha(\pi) := \begin{cases} \pi, & \text{if } \pi \in \Pi^{D'}, \\ \pi_1, & \text{if } \pi = \pi_2, \end{cases}$$

for all $\pi \in \Pi^D$. This implies that $\alpha(\pi) = \alpha(\pi) \circ \phi \sqsubseteq \pi$ for all $\pi \in \Pi^D$, and thus $D \leq D'$. Consequently, $D' \equiv D$. However, $|\Pi^{D'}| = |\Pi^D| - 1$, which contradicts the fact that D is partition-minimal.

For the converse, assume that Π^D is an antichain. Without loss of generality let D be state-minimal. Towards a contradiction, additionally assume that D is not partition minimal, that is, there is D' such that $D' \equiv D$ and $|\mathcal{S}^D| = |\mathcal{S}^{D'}|$ but $|\Pi^{D'}| < |\Pi^D|$. In particular, let (ϕ', α') and (ϕ'', α'') be reductions of D to D' and of D' to D, respectively. Note that $|\text{range}(\alpha')| \leq |\Pi^{D'}| < |\Pi^D|$ by our assumption. Moreover, let $\phi := \phi'' \circ \phi'$ and $\alpha := \alpha'' \circ \alpha'$. Then, (ϕ, α) is a reduction of D to itself where the function α is not injective, since $|\text{range}(\alpha)| \leq |\text{range}(\alpha')| < |\Pi^D|$. Moreover, as D is state-minimal, ϕ is a permutation of $\mathcal{S}^D$. (Otherwise, one would easily be able to build an equivalent ASD with fewer states, hence contradicting state-minimality.) Since α is not injective, there are distinct $\pi_1, \pi_2 \in \Pi^D$ such that $\alpha(\pi_1) = \alpha(\pi_2)$. Additionally, we have $\alpha(\pi_1) \circ \phi \sqsubseteq \pi_1$ as well as $\alpha(\pi_1) \circ \phi = \alpha(\pi_2) \circ \phi \sqsubseteq \pi_2$, and therefore $\alpha(\pi_1) \circ \phi \sqsubseteq \pi_1 \wedge \pi_2$. Also, since α maps partitions of D to partitions of D, for all integers $k \geq 1$, we have

$$\alpha^k(\pi_1) \circ \phi^k \sqsubseteq \pi_1 \wedge \pi_2. \tag{1}$$

Because of our assumption, $\{\pi_1, \pi_2\}$ is an antichain, and therefore, $\pi_1 \wedge \pi_2 \notin \{\pi_1, \pi_2\}$, which implies $\pi_1 \wedge \pi_2 \sqsubset \pi_1$ and $\pi_1 \wedge \pi_2 \sqsubset \pi_2$. Using this fact, for all integers $k \geq 1$, we see that $\alpha^k(\pi_1) \notin \{\pi_1, \pi_2\}$ since

$$|\alpha^k(\pi_1)| = |\alpha^k(\pi_1) \circ \phi^k| \geq |\pi_1 \wedge \pi_2| > \max\{|\pi_1|, |\pi_2|\}.$$

However, there has to exist an integer k' such that $\phi^{k'}$ is the identity permutation. By plugging k' into (1) we obtain

$$\alpha^{k'}(\pi_1) \sqsubseteq \pi_1 \wedge \pi_2 \sqsubset \pi_1,$$

which contradicts the fact that Π^D is an antichain.

Note that by the proofs of (i) and (ii) we see that, given an ASD D, one can iteratively construct a state-minimal ASD D' such that $D' \equiv D$. Furthermore, one can construct out of D' a partition-minimal ASD $D'' \equiv D' \equiv D$ such that $|\mathcal{S}^{D'}| = |\mathcal{S}^{D''}|$. Hence D'' is minimal, and this concludes the proof of Theorem 2. $\square$

As an example, observe that the projective device P_n is state minimal. Indeed, given distinct $x, x' \in \{0,1\}^n$, there exists a component i such that $x_i \neq x'_i$, and thus $x \not\equiv_{\ker(p_i)} x'$. This also implies that the linear device L_n is state-minimal. Furthermore, every r-regular device (for some r) is necessarily partition-minimal, since any two partitions with the same number of blocks are either equal or incomparable (with respect to $\sqsubseteq$).

The following lemma provides some properties of minimal devices with respect to device reducibility.

Lemma 3. *(i) If D, D' are state-minimal and (ϕ, α) reduces D to D', then ϕ is injective. In particular, $|\mathcal{S}^D| \leq |\mathcal{S}^{D'}|$.*

(ii) If D, D' are both r-regular for some r (and hence partition minimal) and (ϕ, α) reduces D to D', then α is injective. In particular, $|\Pi^D| \leq |\Pi^{D'}|$.

(iii) If D, D' are both state-minimal (partition-minimal), then the direct product $D \times D'$ is state-minimal (partition-minimal).

Proof. To prove (i), assume that there are indeed $s_0, s_1 \in \mathcal{S}^D$ such that $\phi(s_0) = \phi(s_1)$, then there exists a partition $\pi \in \mathcal{S}^D$ such that $s_0 \not\equiv s_1$, while for all $\pi' \in \Pi^{D'}$ we have $s_0 \equiv_{\pi' \circ \phi} s_1$ and hence $\pi' \circ \phi \not\sqsubseteq \pi$.

For (ii), assume that α is not an injection, then there exists $\pi_0 \neq \pi_1 \in \Pi^D$ such that $\alpha(\pi_1) = \alpha(\pi_2)$. That is $\alpha(\pi_1) \circ \phi \sqsubseteq \pi_1 \wedge \pi_2$. But then $|\alpha(\pi_1) \circ \phi| \geq |\pi_1 \wedge \pi_2| > r$, since Π^D is an antichain. However, this contradicts the fact that $|\alpha(\pi_1) \circ \phi| \leq r$.

Finally, in order to prove (iii), let D, D' be state-minimal. Then $\bigwedge \Pi^{D \times D'} = \left(\bigwedge \Pi^D\right) \times \left(\bigwedge \Pi^{D'}\right) = id_{\mathcal{S}^D} \times id_{\mathcal{S}^{D'}} = id_{\mathcal{S}^{D \times D'}}$, and thus $D \times D'$ is state-minimal by Theorem 2. Furthermore, let D, D' be partition-minimal, and assume $D \times D'$ is not. Then there exist distinct $\pi \times \pi', \rho \times \rho' \in \Pi^{D \times D'}$ such that $\pi \times \pi' \sqsubseteq \rho \times \rho'$. But then $\pi \sqsubseteq \rho$ and $\pi' \sqsubseteq \rho'$. Since $\pi \neq \rho$ or $\pi' \neq \rho'$ holds, at least one of D and D' is not partition-minimal. $\square$

It also turns out that equivalence of devices is easier to characterize in the minimal case.

Proposition 4. *Let D, D' be minimal ASD's. Then $D \equiv D'$ if and only if there exist bijections $\phi : \mathcal{S}^D \to \mathcal{S}^{D'}$ and $\alpha : \Pi^D \to \Pi^{D'}$ such that $\pi = \alpha(\pi) \circ \phi$ for all $\pi \in \Pi^D$, or, equivalently, $\pi' = \alpha^{-1}(\pi') \circ \phi^{-1}$ for all $\pi' \in \Pi^{D'}$.*

Proof. Clearly, if such bijections exist, then $D \equiv D'$. Now, assume that $D \equiv D'$, then there exists a reduction (ϕ, α) of D to D'. Note that ϕ must be a bijection by Lemma 3. Furthermore, α must also be a bijection, otherwise there would be an equivalent ASD with fewer partitions, contradicting the partition-minimality of D.

Assume towards a contradiction that there is $\pi \in \Pi^D$ such that $\alpha(\pi) \circ \phi \sqsubset \pi$. Note that since $D' \leq D$, there exists a reduction (ϕ', α') of D' to D where ϕ' and α' are both bijections. Consequently, there exists a reduction $(\tilde{\phi}, \tilde{\alpha})$ from D to itself where $\tilde{\phi} := \phi' \circ \phi$ and $\tilde{\alpha} := \alpha' \circ \alpha$ are permutations of $\mathcal{S}^D$ and Π^D,

respectively. Moreover, for all $k \geq 1$, we have $\tilde{\alpha}^k(\pi) \circ \tilde{\phi}^k \sqsubseteq \tilde{\alpha}(\pi) \circ \tilde{\phi} \sqsubseteq \alpha(\pi) \circ \phi \sqsubseteq \pi$. Thus, by choosing $k \geq 1$ such that $\tilde{\phi}^k$ is the identity permutation, we obtain a contradiction to the partition-minimality of D. $\square$

For example, given ASD's D, D', where $\Pi^D = \{\pi_1, \ldots, \pi_k\}$, as well as a k-variate lattice polynomial p, Proposition 4 implies that $p(\alpha(\pi_1) \circ \phi, \ldots, \alpha(\pi_k) \circ \phi) = p(\alpha(\pi_1), \ldots, \alpha(\pi_k)) \circ \phi = p(\pi_1, \ldots, \pi_k)$. As ϕ is a bijection, in order to prove that $D \not\equiv D'$ it is sufficient to find a k-variate lattice polynomial p such that $|p(\pi_1, \ldots, \pi_k)| \neq |p(\alpha(\pi_1), \ldots, \alpha(\pi_k))|$.

3.4 Necessary Conditions for Reducibility

In this section, we discuss easily characterizable necessary conditions for reducibility. Let $\mathcal{D}$ be a set of ASD's and let $f : \mathcal{D} \to \mathbb{R}$ be a function. We say that f is *order-preserving on* $\mathcal{D}$ if $D \leq D'$ implies $f(D) \leq f(D')$ for all ASD's $D, D' \in \mathcal{D}$. In particular, note that $f(D) = f(D')$ whenever $D \equiv D'$. Such a function yields a necessary condition for reducibility. In the following paragraphs, we discuss three order-preserving functions.

Storage capacity. The storage capacity (cf. Section 3.2) is order-preserving on the set of all ASD's: Given D, D' such that $D \leq D'$, let m be maximal such that $C_m \leq D$. By transitivity we have $C_m \leq D'$, and hence $\log m = C(D) \leq C(D')$. The storage capacity is easy to compute, as stated in the following proposition, which also provides properties with respect to direct products and multiple read operations.

Proposition 5. *(i)* $C(D) = \max_{\pi \in \Pi^D} \log |\pi|$ *for all ASD's D.*

(ii) $C(D \times D') = C(D) + C(D')$ *for all ASD's D, D'.*

(iii) For all $k \geq 1$, we have $C(D^{(k)}) \leq k \cdot C(D)$ for all ASD's D.

The first claim follows from the simple observation that $C_m \leq D$ holds if and only if there exists $\pi \in \Pi^D$ such that $|\pi| \geq m$. The simple proofs of (ii) and (iii) are omitted.

For instance, $C(D) = \log r$ for every r-regular ASD D. Furthermore, the storage capacity allows us to easily see that $L_2 \times L_2 \times L_2 \not\leq L_3 \times L_3$, since $C(L_2 \times L_2 \times L_2) = 3 \cdot C(L_2) = 3$, but $C(L_3 \times L_3) = 2 \cdot C(L_3) = 2$.

State complexity. The *state complexity* $\sigma(D)$ of an ASD D provides the minimal number of states that are necessary in order to reproduce the behavior of D, that is, $\sigma(D) = \min_{E \equiv D} \log |\mathcal{S}^E|$. The state complexity is order-preserving: Given devices D, D', let E, E' be state-minimal such that $D \equiv E$ and $D' \equiv E'$. Since $D \leq D'$, we have $E \leq E'$ by transitivity, and by Lemma 3 this implies $\sigma(D) = \log |\mathcal{S}^E| \leq \log |\mathcal{S}^{E'}| = \sigma(D')$. Furthermore, $\sigma(D \times D') = \sigma(D) + \sigma(D')$ by Lemma 3.

Note that $D \leq C_{2^{\sigma(D)}}$, whereas Lemma 3 yields $D \not\leq C_{m'}$ for all $m' < 2^{\sigma(D)}$. For this reason, we obtain $\sigma(D) = \min\{\log m \mid m \in \mathbb{N}, D \leq C_m\}$. Therefore,

11

the state complexity $\sigma(D)$ provides the minimal amount of reliable storage in terms of bits needed to win the game (in the sense of Section 3.2) described by the ASD D.

Perfectness index. The *perfectness index* $i(D)$ of a device D is the minimal integer k such that $D^{(k)}$ is perfect, if such k exists. Otherwise, $i(D) = \infty$. Thus, $i(D)$ provides the minimal number of read operations needed to retrieve the state perfectly. If $i(D)$ is finite, then in particular $i(D) \leq |\Pi^D|$, and by Theorem 2 $i(D)$ is bounded if and only if D is state-minimal. In the following, for an integer m, consider the set of ASD's $\mathcal{D}_m$ such that for all $D \in \mathcal{D}_m$ we have $|\mathcal{S}^D| = m$.

Proposition 6. *Let $D, D' \in \mathcal{D}_m$ for some m be such that $D \leq D'$. Then, $i(D) \geq i(D')$. That is, $D \mapsto -i(D)$ is an order-preserving function on $\mathcal{D}_m$.*

Proof. If $i(D) = \infty$ holds, the claim is trivially satisfied. Therefore, assume that $i(D)$ is finite, and, towards a contradiction, that $D \leq D'$, but $i(D) < i(D')$. There is an integer $k \geq 1$ such that $D^{(k)}$ is perfect, but $D'^{(k)}$ is not. Thus, $id_{\mathcal{S}^D} \in \Pi^{D^{(k)}}$, but $id_{\mathcal{S}^{D'}} \notin \Pi^{D'^{(k)}}$. Since $|\mathcal{S}^D| = |\mathcal{S}^{D'}| = m$, for all possible $\phi : \mathcal{S}^D \to \mathcal{S}^{D'}$ there is no partition $\pi' \in \Pi^{D'^{(k)}}$ such that $\pi' \circ \phi \sqsubseteq id_{\mathcal{S}^D}$. Hence $D^{(k)} \not\leq D'^{(k)}$, which contradicts $D \leq D'$ according to Proposition 1. $\square$

One can easily verify that $i(\times_{i=1}^{n} D_i) = \max_{1 \leq i \leq n} i(D_i)$ for any ASD's $D_1, \ldots, D_n$. Furthermore, $i(L_n) = n$, since exactly n distinct, linearly independent, linear predicates have to be read out to learn the state. As an example, consider the ASD's $L_4 \times L_2$ and $L_3 \times L_3$. By the above, we have $i(L_4 \times L_2) = 4$, and $i(L_3 \times L_3) = 3$. Therefore, $L_3 \times L_3 \not\leq L_4 \times L_2$ by Proposition 6.

The presented quantities are related by the following proposition.

Proposition 7. *For all ASD's D, we have $\sigma(D) \leq i(D) \cdot C(D)$.*

Proof. The claim is trivially true if $i(D) = \infty$. Otherwise, we just combine the facts that $\sigma(D) \leq C(D^{(i(D))}) = \log |\mathcal{S}^D|$ and that $C(D^{(i(D))}) \leq i(D) \cdot C(D)$. $\square$

4 Complexity of Reducibility and Equivalence

We investigate the computational complexity of deciding reducibility and equivalence of ASD's. Both problems are obviously in $\mathcal{NP}$, since given a reduction (ϕ, α) reducibility can be verified in polynomial-time (in the numbers of states and partitions)[3], and hence also equivalence (by giving two corresponding reductions). In this section, we prove the following theorem.

Theorem 8. *Reducibility of ASD's is $\mathcal{NP}$-complete. Furthermore, deciding equivalence of ASD's is at least as hard as deciding graph isomorphism.*

---

[3]We assume some canonical encoding of ASD's.

First, we briefly recall some graph-theoretic notions. A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is *isomorphic* to $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$, denoted $\mathcal{G} \cong \mathcal{G}'$, if there exists a bijection $\phi : \mathcal{V} \to \mathcal{V}'$ such that $\{v, w\} \in \mathcal{E}$ if and only if $\{\phi(v), \phi(w)\} \in \mathcal{E}'$. Furthermore, $\mathcal{G}$ is a *subgraph* of $\mathcal{G}'$ if $\mathcal{V} \subseteq \mathcal{V}'$ and $\mathcal{E} \subseteq \mathcal{E}'$. Finally, $\mathcal{G}$ is *contained* in $\mathcal{G}'$, denoted $\mathcal{G} \preceq \mathcal{G}'$, if there exists a subgraph $\mathcal{H}$ of $\mathcal{G}$ such that $\mathcal{G} \cong \mathcal{H}$. Let $\mathcal{K}_k$ be the complete graph on k vertices. The *k-clique problem* consists in deciding, given a graph $\mathcal{G}$, whether $\mathcal{K}_k \preceq \mathcal{G}$. For arbitrary k, this is a well-known $\mathcal{NP}$-complete problem.

In order to prove Theorem 8, we introduce a class of ASD's representing graphs. For a given graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, we define its *graph device* $D(\mathcal{G})$ as the 3-regular ASD such that $\mathcal{S}^{D(\mathcal{G})} = \mathcal{V}$ and $\Pi^{D(\mathcal{G})} = \{\pi_e \mid e \in \mathcal{E}\}$, where for $e = \{u, v\} \in \mathcal{E}$, we have $\pi_e = \{\{u\}, \{v\}, V - \{u, v\}\}$. Note that graph devices are only meaningful if $|\mathcal{V}| \geq 4$, since in the case where $|\mathcal{V}| = 3$, all edges define the same partition.

For instance, if one takes the complete graph $\mathcal{K}_k$ (for $k \geq 4$), the resulting graph device $D(\mathcal{K}_k)$ has state space $\{1, \ldots, k\}$ and all its partitions are of the form $\{\{i\}, \{j\}, \{1, \ldots, k\} - \{i, j\}\}$ for all $i < j$, $i, j \in \{1, \ldots, k\}$.

The following result can easily be verified using Theorem 2.

Lemma 9. *The ASD $D(\mathcal{G})$ is minimal for all graphs $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $|\mathcal{V}| \geq 4$ and no isolated[4] vertices.*

The following lemma is the central point in the proof of Theorem 8.

Lemma 10. *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ be graphs with no isolated vertices such that $\min\{|\mathcal{V}|, |\mathcal{V}'|\} \geq 4$. Then, $\mathcal{G} \preceq \mathcal{G}'$ if and only if $D(\mathcal{G}) \leq D(\mathcal{G}')$.*

Proof. For notational convenience, let $\Pi^{D(\mathcal{G})} = \{\pi_e \mid e \in \mathcal{E}\}$ and $\Pi^{D(\mathcal{G}')} = \{\pi'_{e'} \mid e' \in \mathcal{E}'\}$. If $\mathcal{G} \preceq \mathcal{G}'$, then there is an injective map $\phi : \mathcal{V} \to \mathcal{V}'$ such that, for all $u, v \in \mathcal{V}$, $\{u, v\} \in \mathcal{E}$ implies $\{\phi(u), \phi(v)\} \in \mathcal{E}'$. That is, for all $e \in \mathcal{E}$, we have $\pi'_{\phi(e)} \in \Pi^{D(\mathcal{G}')}$. Construct a map $\alpha : \Pi^{D(\mathcal{G})} \to \Pi^{D(\mathcal{G}')}$ such that for all $e \in \mathcal{E}$, we set $\alpha(\pi_e) = \pi'_{\phi(e)}$. One can now easily see that for all $e \in \mathcal{E}$, we have $\pi_e = \pi'_{\phi(e)} \circ \phi$, and thus (ϕ, α) reduces $D(\mathcal{G})$ to $D(\mathcal{G}')$.

For the converse, assume that $D(\mathcal{G}) \leq D(\mathcal{G}')$, and let (ϕ, α) be a reduction of $D(\mathcal{G})$ to $D(\mathcal{G}')$. Since both graphs have at least four vertices $D(\mathcal{G})$ and $D(\mathcal{G}')$ are both state-minimal by Lemma 9, and therefore the function ϕ is injective by Lemma 3. For all $e \in \mathcal{E}$, there is $e' \in \mathcal{E}'$ such that $\alpha(\pi_e) = \pi_{e'}$ and such that $\pi_e = \pi'_{e'} \circ \phi$. For all $e = \{v, w\}$, this means that $\phi(v) \not\equiv_{\pi'_{e'}} \phi(w)$, and that the remaining block of $\pi'_{e'}$ contains at least two elements. Thus, $e' = \{\phi(v), \phi(w)\}$, and since $e' \in \mathcal{E}'$, we have $\mathcal{G} \preceq \mathcal{G}'$. □

Given a graph $\mathcal{G}$ with at least four vertices, none of which is isolated, as well as an integer $k \geq 4$, in order to decide whether $\mathcal{G}$ contains a k-clique, one simply constructs the ASD's $D(\mathcal{K}_k)$ and $D(\mathcal{G})$, and checks whether $D(\mathcal{K}_k) \leq D(\mathcal{G})$.

---

[4]A vertex $v \in \mathcal{V}$ is *isolated* if there exists no $e \in \mathcal{E}$ such that $v \in e$.

It is easy to see that the reduction is polynomial-time, and this implies $\mathcal{NP}$-completeness[5]. Lemma 10 also implies that $D(\mathcal{G}) \equiv D(\mathcal{G}')$ if and only if $\mathcal{G} \cong \mathcal{G}'$ for any two graphs $\mathcal{G}, \mathcal{G}'$ as in the statement of the lemma. Hence, deciding equivalence of ASD's is at least as difficult as deciding graph isomorphism, since deciding isomorphism is clearly not (computationally) easier when restricted to such graphs. This completes the proof of Theorem 8.

We conclude this section by noting that one can provide a simple two-round interactive proof for the problem of deciding non-equivalence of ASD's (see Appendix B). This means that deciding non-equivalence is in the complexity class $\mathcal{IP}(2)$, and hence also in $\mathcal{AM}$ [2]. For this reason, if the problem of deciding equivalence of ASD's were $\mathcal{NP}$-complete, we would have $\mathcal{NP} \subseteq$ co-$\mathcal{AM}$, and it is well-known [1] that this implies a collapse of the polynomial hierarchy $\mathcal{PH}$ to its second level. Therefore, it is very unlikely that deciding device equivalence is $\mathcal{NP}$-complete.

5 Binary ASD's and Unique Factorizations

We say that an ASD D has *direct product factorization* $\times_{i=1}^{m} D_i$ if this product is equivalent to D. Furthermore, an ASD D is *prime* if, whenever $D \equiv E \times E'$, then either E or E' is trivial. For example, if D is minimal with a partition $\pi \in \Pi^D$ such that $|\pi| = p$ for a prime number p, then D is prime. Furthermore, every ASD D has a prime factorization with at most $\log |\mathcal{S}^D|$ factors.

In the following, we look at the class $\mathcal{D}_2^{\times}$ of ASD's having (at least one) prime factorization consisting uniquely of binary ASD's. Note that this class is closed under taking direct products. The following lemma provides a strong necessary and sufficient condition for deciding reducibility among members of the class $\mathcal{D}_2^{\times}$ with the same number of states, and such that no perfect factor appears in their binary factorization. The reader is referred to Appendix C for a proof.

Lemma 11. *Let $D_1, \ldots, D_m, D_1', \ldots, D_n'$ be non-perfect state-minimal binary ASD's such that $\prod_{i=1}^{m} |\mathcal{S}^{D_i}| = \prod_{j=1}^{n} |\mathcal{S}^{D_j'}|$. Then $\times_{i=1}^{m} D_i \leq \times_{j=1}^{n} D_j'$ holds if and only if there exists a partition $\{J_1, \ldots, J_m\}$ of the indices $\{1, \ldots, n\}$ such that $D_i \leq \times_{j \in J_i} D_j'$ for all $i \in \{1, \ldots, m\}$.*

As a corollary of this fact, for given linear devices $L_{k_1}, \ldots, L_{k_m}, L_{r_1}, \ldots, L_{r_n}$ with $\sum_{i=1}^{m} k_i = \sum_{j=1}^{n} r_j$, we have $\times_{i=1}^{m} L_{k_i} \leq \times_{j=1}^{n} L_{r_j}$ if and only if $m \leq n$ and there exists a partition $\{J_1, \ldots, J_m\}$ of $\{1, \ldots, n\}$ such that $k_i = \sum_{j \in J_i} r_j$. For instance, one can see that $L_3 \times L_3 \not\leq L_2 \times L_2 \times L_2$. Otherwise, the above would imply that $L_3 \leq L_2$, which is obviously false.

The following theorem makes use of Lemma 11 to show that the factorization in terms of *binary* ASD's in unique.

---

[5]Of course, the k-clique problem is still $\mathcal{NP}$-complete even when imposing $k \geq 4$ and when looking at graphs with no isolated vertices.

Theorem 12. *Let D be an ASD, and assume that $\times_{i=1}^{m} D_i$ is a factorization of D where $D_1, \ldots, D_m$ are* binary. *Then, this factorization is unique (with respect to the set of all factorizations into binary devices), up to order and equivalence of the factors.*

Proof. Let $D_1, \ldots, D_m, D'_1, \ldots, D'_m$ be binary ASD's such that $\times_{i=1}^{m} D_i \equiv \times_{j=1}^{m} D'_j$. In order to prove the theorem, it suffices to show that these factorizations are equivalent, that is, there exists a permutation $\gamma : \{1, \ldots, m\} \to \{1, \ldots, m\}$ such that $D_i \equiv D'_{\gamma(i)}$ for all $i = 1, \ldots, m$. Without loss of generality, assume that all devices are minimal.

First, note that for a minimal binary ASD's D, we have $\bigvee \Pi^D = id_{\mathcal{S}^D}$ whenever D is perfect, whereas $\bigvee \Pi^D = \{\mathcal{S}^D\}$ otherwise. Therefore, if exactly ℓ binary devices in the product $\times_{i=1}^{m} D_i$ are perfect, then $\left| \bigvee \Pi^{\times_{i=1}^{m} D_i} \right| = \left| \times_{i=1}^{m} \left(\bigvee \Pi^{D_i} \right) \right| = 2^{\ell}$. For this reason, both products $\times_{i=1}^{m} D_i$ and $\times_{j=1}^{m} D'_j$ have exactly the same number of perfect binary devices, otherwise they would not be equivalent by Proposition 4. Hence, we can rewrite both products as

$$C \times E_1 \times \cdots \times E_k \equiv C \times E'_1 \times \cdots \times E'_k$$

for some $k \leq m$, non-perfect binary ASD's $E_1, \ldots, E_k, E'_1, \ldots, E'_k$, and a perfect ASD C. By Proposition 4, there exist bijections $\phi : \mathcal{S}^{C \times E_1 \times \cdots \times E_k} \to \mathcal{S}^{C \times E'_1 \times \cdots \times E'_k}$ and $\alpha : \Pi^{E_1 \times \cdots \times E_k} \to \Pi^{E'_1 \times \cdots \times E'_k}$ such that

$$id_{\mathcal{S}^C} \times \pi = (id_{\mathcal{S}^C} \times \alpha(\pi)) \circ \phi \tag{2}$$

for all $\pi \in \Pi^{E_1 \times \cdots \times E_k}$. This in particular implies

$$id_{\mathcal{S}^C} \times \left\{ \mathcal{S}^{E_1 \times \cdots \times E_k} \right\} = \bigvee \Pi^{C \times E_1 \times \cdots \times E_k}$$
$$= \left(\bigvee \Pi^{C \times E'_1 \times \cdots \times E'_k} \right) \circ \phi = \left(id_{\mathcal{S}^C} \times \left\{ \mathcal{S}^{E'_1 \times \cdots \times E'_k} \right\} \right) \circ \phi.$$

For a fix $s \in \mathcal{S}^C$ and any two $e_0, e_1 \in \mathcal{S}^{E_1 \times \cdots \times E_k}$ we have $(s, e_0) \equiv_{\bigvee \Pi^{C \times E_1 \times \cdots \times E_k}} (s, e_1)$ by Proposition 4, and thus $\phi(s, e_0) \equiv_{\bigvee \Pi^{C \times E'_1 \times \cdots \times E'_k}} \phi(s, e_1)$. In order for this to hold, there has to exist $t \in \mathcal{S}^C$ such that $\phi(s, e) = (t, e')$ for all $e \in \mathcal{S}^{\times_{i=1}^{k} E_i}$, where $e' \in \mathcal{S}^{\times_{i=1}^{k} E'_i}$.

Without loss of generality, we can assume that there exists a bijection $\tilde{\phi} : \mathcal{S}^{E_1 \times \cdots \times E_k} \to \mathcal{S}^{E'_1 \times \cdots \times E'_k}$ such that $\phi(s, e) = (s, \tilde{\phi}(e))$, and therefore by (2) we have $id_{\mathcal{S}^C} \times \pi = id_{\mathcal{S}^C} \times (\alpha(\pi) \circ \tilde{\phi})$ for all π. This implies that $\pi = \alpha(\pi) \circ \phi$, and thus $E_1 \times \cdots \times E_k \equiv E'_1 \times \cdots \times E'_k$, again by Proposition 4.

It now suffices to prove that these two last factorizations are equivalent in order to conclude the proof. Note that since all devices are non-perfect, both $\times_{i=1}^{k} E_i \leq \times_{i=1}^{k} E'_i$ and $\times_{i=1}^{k} E'_i \leq \times_{i=1}^{k} E_i$ hold. By Lemma 11, there exist permutations γ, γ' of $\{1, \ldots, k\}$ such that $E_i \leq E'_{\gamma(i)}$ and $E'_j \leq E'_{\gamma'(j)}$. Assume that there is an $i \in \{1, \ldots, k\}$ such that E_i and $E'_{\gamma(i)}$ are not equivalent, i.e., $E'_{\gamma(i)} \not\leq E_i$. Define $\tilde{\gamma} = \gamma' \circ \gamma$. Then, $E_i \leq E'_{\gamma(i)} \leq E_{\tilde{\gamma}^r(i)}$ for all $r > 0$. Since k

15

is finite there exists $r' > 0$ such that $\tilde{\gamma}^{r'}(i) = i$. Therefore, $E_i \equiv E'_{\gamma(i)}$, which is a contradiction. $\square$

An immediate corollary of the theorem is the following.

Corollary 13. *Two products of binary linear devices are equivalent if and only if they consist of exactly the same devices.*

For instance, the corollary immediately yields $L_4 \times L_3 \times L_3 \not\equiv L_4 \times L_4 \times L_2$. Note that this non-equivalence could not be proved using simpler arguments based on order-preserving functions.

We stress that Theorem 12 does not rule out the fact that there might be additional factorizations in terms of non-binary prime ASD's. Indeed, the general question of deciding whether prime factorizations of ASD's are unique appears to be challenging. For instance, it is easy to see that every perfect ASD C_m where $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ for distinct primes $p_1, \ldots, p_r$, and positive integers $\alpha_1, \ldots, \alpha_r$ can be uniquely factorized as $\times_{i=1}^{r} C_{p_i}^{\alpha_i}$. We leave the more general question as an open problem. Note that the problem is related to a line of research investigating unique factorizations of *relational structures* (cf. e.g. [5] for a survey). Even though ASD's are related to relational structures, known results only apply to a weaker form of direct product.

Acknowledgments

References

[1] R. B. Boppana, J. Håstad, and S. Zachos, "Does co-NP have short interactive proofs?," *Inf. Process. Lett.*, vol. 25, no. 2, pp. 127–132, 1987.

[2] S. Goldwasser and M. Sipser, "Private coins versus public coins in interactive proof systems," in *STOC '86: Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pp. 59–68, 1986.

[3] G. Grätzer, *General Lattice Theory*. Basel: Birkhäuser, 1998.

[4] W. Imrich and S. Klavžar, *Product Graphs: Structure and Recognition*. Wiley, 2000.

[5] B. Jónsson, "The unique factorization problem for finite relational structures," *Colloq. Math.*, vol. 14, pp. 1–32, 1966.

[6] R. König, U. Maurer, and R. Renner, "On the power of quantum memory," *IEEE Transactions on Information Theory*, vol. 51, no. 7, pp. 2391–2401, 2005.

[7] M. O. Rabin, "How to exchange secrets with oblivious transfer." Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[8] C. E. Shannon, "The zero-error capacity of a noisy channel," *IEEE Transactions on Information Theory*, vol. 2, pp. 8–19, 1956.

A   Direct Products of Set Partitions

We prove here two facts about direct products of partitions. The first proposition states that one can look at the refinement order component wise.

Proposition 14. *Let $\mathcal{S}, \mathcal{S}'$ be sets, $\pi, \rho \in \Pi(\mathcal{S})$, and $\pi', \rho' \in \Pi(\mathcal{S}')$. Then*

$$(\pi \times \pi') \sqsubseteq (\rho \times \rho') \iff (\pi \sqsubseteq \rho) \wedge (\pi' \sqsubseteq \rho').$$

Proof. The proof follows from the fact that, given sets $\mathcal{B}, \mathcal{B}', \mathcal{C},$ and $\mathcal{C}'$, we have $\mathcal{B} \times \mathcal{B}' \subseteq \mathcal{C} \times \mathcal{C}'$ if and only if $\mathcal{B} \subseteq \mathcal{C}$ and $\mathcal{B}' \subseteq \mathcal{C}'$. If $\pi \sqsubseteq \rho$ and $\pi' \sqsubseteq \rho'$ both hold, then for every $\mathcal{B} \in \pi$, $\mathcal{B}' \in \pi'$ there have to exist $\mathcal{C} \in \rho, \mathcal{C}' \in \rho'$ such that $\mathcal{B} \subseteq \mathcal{C}$ and $\mathcal{B}' \subseteq \mathcal{C}'$, and hence $\mathcal{B} \times \mathcal{B}' \subseteq \mathcal{C} \times \mathcal{C}'$, which implies $(\pi \sqsubseteq \rho)$ and $(\pi' \sqsubseteq \rho')$. Conversely, if $(\pi \times \pi') \sqsubseteq (\rho \times \rho')$, then for every $\mathcal{B} \times \mathcal{B}'$ there is $\mathcal{C} \times \mathcal{C}'$ such that $\mathcal{B} \subseteq \mathcal{B}'$ and $\mathcal{C} \subseteq \mathcal{C}'$. In particular, $\pi \sqsubseteq \rho$ and $\pi' \sqsubseteq \rho'$. □

The second proposition states that the meet (join) of direct product partitions is the direct product of the meets (joins).

Proposition 15. *Let $\mathcal{S}, \mathcal{S}'$ be sets, $\pi, \rho \in \Pi(\mathcal{S})$, and $\pi', \rho' \in \Pi(\mathcal{S}')$. Then*

(i) $(\pi \times \pi') \wedge (\rho \times \rho') = (\pi \wedge \rho) \times (\pi' \wedge \rho')$

(ii) $(\pi \times \pi') \vee (\rho \times \rho') = (\pi \vee \rho) \times (\pi' \vee \rho')$

Proof. For the first statement, we have directly

$$\begin{aligned}
(\pi \times \pi') \wedge (\rho \times \rho') &= \{(\mathcal{B} \times \mathcal{B}') \cap (\mathcal{C} \times \mathcal{C}') \,|\, \mathcal{B} \in \pi, \mathcal{B}' \in \pi', \mathcal{C} \in \rho, \mathcal{C}' \in \rho'\} \\
&= \{(\mathcal{B} \cap \mathcal{C}) \times (\mathcal{B}' \cap \mathcal{C}') \,|\, \mathcal{B} \in \pi, \mathcal{B}' \in \pi', \mathcal{C} \in \rho, \mathcal{C}' \in \rho'\} \\
&= (\pi \wedge \rho) \times (\pi' \wedge \rho').
\end{aligned}$$

To prove the second statement, first note that by definition $\pi \sqsubseteq \pi \vee \rho$ and $\pi' \sqsubseteq \pi' \vee \rho'$, and therefore $\pi \times \pi' \sqsubseteq (\pi \vee \rho) \times (\pi' \vee \rho')$ by Proposition 14. Analogously, $\rho \times \rho' \sqsubseteq (\pi \vee \rho) \times (\pi' \vee \rho')$, which implies $(\pi \times \pi') \vee (\rho \times \rho') \sqsubseteq (\pi \vee \rho) \times (\pi' \vee \rho')$.

Now, let $(s, s'), (t, t') \in \mathcal{S} \times \mathcal{S}'$ be such that $(s, s') \equiv_{(\pi \vee \rho) \times (\pi' \vee \rho')} (t, t')$. This implies that $s \equiv_{\pi \vee \rho} t$ and $s' \equiv_{\pi' \vee \rho'} t'$. There are $y_1, \ldots, y_k \in \mathcal{S}$ with $s = y_1$ and $t = y_k$ such that for all $i = 1, \ldots, k - 1$ we have $y_i \equiv_\pi y_{i+1}$ or $y_i \equiv_\rho y_{i+1}$. Analogously, there are $y_1', \ldots, y_\ell' \in \mathcal{S}'$ with $s' = y_1'$ and $t' = y_\ell'$ such that for all $j = 1, \ldots, \ell - 1$ we have $y_j' \equiv_{\pi'} y_{j+1}'$ or $y_j' \equiv_{\rho'} y_{j+1}'$. In particular, for all $i = 1, \ldots, k-1$ we have $(y_i, s') \equiv_{\pi \times \pi'} (y_{i+1}, s')$ or $(y_i, s') \equiv_{\rho \times \rho'} (y_{i+1}, s')$. Additionally, for all $j = 1, \ldots, \ell - 1$ we have $(t, y_j') \equiv_{\pi \times \pi'} (t, y_{j+1}')$ or $(t, y_j') \equiv_{\rho \times \rho'} (t, y_{j+1}')$. Therefore, $(s, s') \equiv_{(\pi \times \pi') \vee (\rho \times \rho')} (t, t')$. That is, $(\pi \vee \rho) \times (\pi' \vee \rho') \sqsubseteq (\pi \times \pi') \vee (\rho \times \rho')$, and this implies equality. □

17

B   Interactive Proof for Device Non-Equivalence

In this section, we briefly sketch a two-round interactive proof for the problem of non-equivalence of ASD's. The protocol follows the same lines as the one for graph non-isomorphism.

Assume that Alice and Bob are given a pair of ASD's (D_0, D_1), and Alice would like to prove $D_0 \not\equiv D_1$ to Bob. Also, assume without loss of generality that D_0 and D_1 are minimal, and that $\mathcal{S}^{D_0} = \mathcal{S}^{D_1} = \{1, \ldots, n\}$ for some integer n, and $|\Pi^{D_0}| = |\Pi^{D_1}|$. Bob starts the protocol by choosing a bit $b \in \{0, 1\}$ uniformly at random and generates an equivalent device $D \equiv D_b$ uniformly at random. (By Proposition 4, this can be done efficiently by choosing an appropriate pair of permutations (ϕ, α) uniformly at random.). He subsequently sends the description of D to Alice. Finally, Alice returns a bit $b' \in \{0, 1\}$ to Bob, and Bob accepts if and only if $b = b'$.

Whenever $D_0 \not\equiv D_1$ holds, Alice is able to decide whether $D_0 \equiv D$ or $D_1 \equiv D$, and hence to perfectly guess b. However, if $D_0 \equiv D_1$, Alice can make Bob accept with probability at most $\frac{1}{2}$ regardless of her strategy.

C   Proof of Lemma 11

Sufficiency is obvious. To prove the converse, assume that $\times_{i=1}^{m} D_i \leq \times_{j=1}^{n} D'_j$, and let (ϕ, α) be an arbitrary reduction of $\times_{i=1}^{m} D_i$ to $\times_{j=1}^{n} D'_j$. By Lemma 3, the function ϕ is a bijection. In the following, we show that such a ϕ induces a partition of the set of indices $\{1, \ldots, n\}$ as in the statement of the theorem. To do this, we introduce the following function τ: Let $j \in \{1, \ldots, n\}$ and $(s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_n) \in \mathcal{S}^{D'_1} \times \cdots \times \mathcal{S}^{D'_{j-1}} \times \mathcal{S}^{D'_{j+1}} \times \cdots \times \mathcal{S}^{D'_n}$, then we define

$$\tau(j, s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_n) :=$$
$$\{j \mid |\phi_j^{-1}(\{s'_1\} \times \cdots \times \{s'_{j-1}\} \times \mathcal{S}^{D'_j} \times \{s'_{j+1}\} \times \cdots \times \{s'_n\}| > 1\},$$

where ϕ_j^{-1} denotes the j-th component of the output of the function ϕ^{-1}. In other words, the value $\tau(j, s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_n)$ provides the set of indices of the devices in the product $\times_{i=1}^{m} D_i$ for which the state is modified when one goes over all possible states of the ASD D'_j, fixing the states of the remaining ASD's to $s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_n$, and looks at the output of ϕ^{-1}. We start by proving the following claim, which states that for a given $j \in \{1, \ldots, n\}$, arbitrarily modifying the j-th component of a vector in $\mathcal{S}^{D'_1} \times \cdots \times \mathcal{S}^{D'_n}$ only alters a single component of the output with respect to ϕ^{-1}.

Claim 1. For all $j \in \{1, \ldots, n\}$ and $(s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_n) \in \mathcal{S}^{D'_1} \times \cdots \times \mathcal{S}^{D'_{j-1}} \times \mathcal{S}^{D'_{j+1}} \times \cdots \times \mathcal{S}^{D'_n}$, we have $|\tau(j, s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_n)| = 1$.

Proof. Assume, towards a contradiction, that the claim is false. In particular,

there are states $\tilde{s}^1, \tilde{s}^2 \in \mathcal{S}^{D'_j}$ such that

$$(s_1^1, \ldots, s_m^1) := \phi^{-1}(s'_1, \ldots, s'_{j-1}, \tilde{s}^1, s'_{j+1}, \ldots, s'_n),$$
$$(s_1^2, \ldots, s_m^2) := \phi^{-1}(s'_1, \ldots, s'_{j-1}, \tilde{s}^2, s'_{j+1}, \ldots, s'_n)$$

differ in two components p and q, that is, $s_p^1 \neq s_p^2$ and $s_q^1 \neq s_q^2$. Since $|\mathcal{S}^{D'_j}| \geq 3$ by our assumption, pick an arbitrary third element $\tilde{s}^3 \in \mathcal{S}^{D'_j}$ different from $\tilde{s}^1$ and $\tilde{s}^2$, and define $(s_1^3, \ldots, s_m^3) := \phi^{-1}(s'_1, \ldots, s'_{j-1}, \tilde{s}^3, s'_{j+1}, \ldots, s'_n)$. We look for partitions $\pi_1, \ldots, \pi_m$, where $\pi_i \in \Pi^{D_i}$, such that the vectors $(s_1^1, \ldots, s_n^1)$, $(s_1^2, \ldots, s_n^2)$, and $(s_1^3, \ldots, s_n^3)$ are each in a distinct block of $\pi_1 \times \cdots \times \pi_m$. In order to do so, consider the following two cases:

(i) $s_p^1 = s_p^3$: Choose a partition $\pi_p \in \Pi^{D_p}$ such that $s_p^1 \not\equiv_{\pi_p} s_p^2$ (this exists by state-minimality). Furthermore, there must exist a component $r \neq p$ such that $s_r^1 \neq s_r^3$. Then, simply pick $\pi_r \in \Pi^{D_r}$ such that $s_r^1 \not\equiv_{\pi_r} s_r^3$. All π_i for $i \neq p$ and $i \neq r$ can be chosen arbitrarily. The cases $s_q^1 = s_q^3$, $s_p^2 = s_p^3$, and $s_q^2 = s_q^3$ are analogous. (Notice that these cases are not mutually-exclusive.)

(ii) $s_p^3 \neq s_p^1$, $s_p^3 \neq s_p^2$, $s_q^3 \neq s_q^1$, and $s_q^3 \neq s_q^2$: Choose a partition $\pi_p \in \Pi^{D_p}$ such that $s_p^1 \not\equiv_{\pi_p} s_p^3$. Now, it might be that either $s_p^2 \equiv_{\pi_p} s_p^3$ or $s_p^2 \equiv_{\pi_p} s_p^1$. In the first case, choose $\pi_q \in \Pi^{D_q}$ such that $s_q^2 \not\equiv_{\pi_q} s_q^3$, whereas in the second case choose $\pi_q \in \Pi^{D_q}$ such that $s_q^2 \not\equiv_{\pi_q} s_q^1$. All π_i for $i \neq p$ and $i \neq q$ are chosen arbitrarily.

Since D'_j is binary, there are distinct $u, v \in \{1, 2, 3\}$ such that

$$(s'_1, \ldots, s'_{j-1}, \tilde{s}^u, s'_{j+1}, \ldots, s'_n) \equiv_{\alpha(\pi_1 \times \cdots \pi_m)} (s'_1, \ldots, s'_{j-1}, \tilde{s}^v, s'_{j+1}, \ldots, s'_n).$$

However, we have $(s_1^u, \ldots, s_m^u) \not\equiv_{\pi_1 \times \cdots \times \pi_m} (s_1^v, \ldots, s_m^v)$, and (ϕ, α) cannot be a reduction. $\qquad\square$

We now want to prove that the unique component which varies is independent of the other states.

Claim 2. For all $j \in \{1, \ldots, n\}$ and for all $(s'_{1,1}, \ldots, s'_{1,j-1}, s'_{1,j+1}, \ldots, s'_{1,n})$, $(s'_{2,1}, \ldots, s'_{2,j-1}, s'_{2,j+1}, \ldots, s'_{2,n}) \in \mathcal{S}^{D'_1} \times \cdots \times \mathcal{S}^{D'_{j-1}} \times \mathcal{S}^{D'_{j+1}} \times \cdots \times \mathcal{S}^{D'_n}$, we have

$$\tau(j, s'_{1,1}, \ldots, s'_{1,j-1}, s'_{1,j+1}, \ldots, s'_{1,n}) = \tau(j, s'_{2,1}, \ldots, s'_{2,j-1}, s'_{2,j+1}, \ldots, s'_{2,n}).$$

Proof. We start by assuming that there is a unique component $r \in \{1, \ldots, n\} - \{j\}$ such that $s'_{1,r} \neq s'_{2,r}$. Also, assume without loss of generality that $j \neq n$ and $r = n$. In particular, denote $s'_{j'} := s_{1,j'} = s_{2,j'}$ for all $j' \in \{1, \ldots, n-1\} - \{j\}$. Given two states $s'_{A,j}, s'_{B,j} \in \mathcal{S}^{D'_j}$, we define the following states of $D'_1 \times \cdots \times D'_n$:

$$s'_{1,A} := (s'_1, \ldots, s'_{j-1}, s'_{A,j}, s'_{j+1}, \ldots, s'_{n-1}, s'_{1,n}),$$
$$s'_{1,B} := (s'_1, \ldots, s'_{j-1}, s'_{B,j}, s'_{j+1}, \ldots, s'_{n-1}, s'_{1,n}),$$
$$s'_{2,A} := (s'_1, \ldots, s'_{j-1}, s'_{A,j}, s'_{j+1}, \ldots, s'_{n-1}, s'_{2,n}),$$
$$s'_{2,B} := (s'_1, \ldots, s'_{j-1}, s'_{B,j}, s'_{j+1}, \ldots, s'_{n-1}, s'_{2,n}).$$

Furthermore, using the previous claim, we define

$$\{p_1\} := \tau(j, s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_{n-1}, s'_{1,n})$$
$$\{p_2\} := \tau(j, s'_1, \ldots, s'_{j-1}, s'_{j+1}, \ldots, s'_{n-1}, s'_{2,n}),$$

as well as

$$\{r_A\} := \tau(n, s'_1, \ldots, s'_{j-1}, s_{A,j}, s'_{j+1}, \ldots, s'_{n-1})$$
$$\{r_B\} := \tau(n, s'_1, \ldots, s'_{j-1}, s_{B,j}, s'_{j+1}, \ldots, s'_{n-1}).$$

Finally, we define the following states of $D_1 \times \cdots \times D_m$ making use of ϕ^{-1}:

$$w := \phi^{-1}(s'_{1,A}), x := \phi^{-1}(s'_{1,B}), y := \phi^{-1}(s'_{2,B}), z := \phi^{-1}(s'_{2,A}).$$

We have $w_{p_1} \neq x_{p_1}$ and $x_p = w_p$ for all $p \in \{1, \ldots, m\} - \{p_1\}$. Analogously $y_{p_2} \neq z_{p_2}$ and $y_p = z_p$ for all $p \in \{1, \ldots, m\} - \{p_2\}$. And again, by the same argument, x and y differs only at component r_A, and z and w differ only in component r_B. According to this, there are two ways to modify state w into x. The first one is by changing component p_1. The second one is by going through states z and y, modifying components r_A, p_2, and r_B. Assume, towards a contradiction, that $p_1 \neq p_2$. Since $w_{p_2} = x_{p_2}$, we must have either $r_A = p_2$ and $r_B = p_1$ or $r_A = p_1$ and $r_B = p_2$. If the former holds, we necessarily have $w = y$, while if the latter holds, then $z = x$. In both cases, we have a contradiction with the fact that ϕ is a bijection.

The proof of the claim easily follows by repeating the same argument iteratively for $r \neq n$. $\qquad\square$

Hence, for $j \in \{1, \ldots, n\}$ we are now allowed to denote by $\tau(j)$ the unique component which varies when altering the state of D'_j. Additionally, for $i \in \{1, \ldots, m\}$, we define

$$\rho(i) := \{j \mid \tau(j) = i\}.$$

Note that $\{\rho(i) \mid i = 1, \ldots, m\} = \ker(\tau)$ is a set partition of $\{1, \ldots, n\}$. Now, take a fix $i \in \{1, \ldots, m\}$ and let $\rho(i) = \{j_1, \ldots, j_r\}$. Furthermore, fix states $s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_m$ for the devices $D_1, \ldots, D_{i-1}, D_{i+1}, \ldots, D_m$. The j-th component $\phi_j(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n)$ is constant for all $j \notin \rho(i)$, since for any two states $s', s'' \in \mathcal{S}^{D'_1 \times \cdots \times D'_n}$ differing at two distinct components $p \neq q$ such that $\tau(p) \neq \tau(q)$, the states $\phi^{-1}(s), \phi^{-1}(s')$ differ at both components $\tau(p)$ and $\tau(q)$.

Furthermore, fix arbitrary partitions $\pi_1, \ldots, \pi_{i-1}, \pi_{i+1}, \ldots, \pi_n$ for the devices $D_1, \ldots, D_{i-1}, D_{i+1}, \ldots, D_n$, and finally define

$$\phi^i(s) := (\phi_{j_1}(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n), \ldots, \phi_{j_r}(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n))$$

$$\alpha^i(\pi) := (\alpha_{j_1}(\pi_1, \ldots, \pi_{i-1}, \pi, \pi_{i+1}, \ldots, \pi_n), \ldots, \alpha_{j_r}(\pi_1, \ldots, \pi_{i-1}, \pi, \pi_{i+1}, \ldots, \pi_n)).$$

It is now easy to verify that (ϕ^i, α^i) is a reduction of D_i to $\times_{j \in \rho(i)} D'_j$. If this is not the case, there are distinct states $s_i, s'_i \in D_i$ and $\pi_i \in \Pi^D$ such that $s_i \neq_{\pi_i} s'_i$, but $s_i =_{\alpha^i(\pi_i) \circ \phi^i} s'_i$. By the arguments above, and by the definition of ϕ^i and α^i, this implies that (ϕ, α) is not a reduction.