On Transformations among Opacity Notions*

Jiří Balun
Faculty of Science, Palacky University
Olomouc, Czechia
jiri.balun01@upol.cz

Tomáš Masopust
Faculty of Science, Palacky University
Olomouc, Czechia
tomas.masopust@upol.cz

***Abstract*—Opacity is a property asking whether a system may reveal its secret to a passive observer who knows the structure of the system but has only limited observations of its behavior. Several notions of opacity have been studied. Similarities among the opacity notions have been investigated via transformations, which have many potential applications. We investigate K-step opacity (K-SO), a notion that generalizes both current-state opacity and infinite-step opacity, and asks whether the intruder cannot decide, at any instant, whether or when the system was in a secret state during the last K observable steps. We provide new polynomial-time transformations among K-SO and other opacity notions. Our results lead, among others, to the general solution of an open problem concerning the computational complexity of the verification of K-SO.**

***Index Terms*—Discrete-event systems, opacity, transformations**

I. Introduction

Properties keeping some information secret include, among others, anonymity [1], noninterference [2], secrecy [3], security [4], and opacity [5]. Opacity is an information-flow property asking whether a system prevents an intruder from revealing the secret. The intruder is a passive observer with the knowledge of the structure of the system but with only limited observation of its behavior. Intuitively, the intruder estimates the behavior of the system, and the system is opaque if, for every secret behavior, there is a non-secret behavior that looks the same to the intruder. Secret is modeled as a set of secret states or as a set of secret behaviors. The former leads to the state-based opacity of Bryans et al. [6], [7], while the latter leads to the language-based opacity of Badouel et al. [8] and Dubreil et al. [9]. See Jacob et al. [10] for more details.

Several notions of opacity have been discussed, including language-based opacity (LBO), initial-state opacity (ISO), current-state opacity (CSO), K-step opacity (K-SO), and infinite-step opacity (INSO). While initial-state opacity prevents the intruder from revealing, at any instant, whether the system started in a secret state, CSO prevents the intruder only from revealing whether the current state of the system is secret. The intruder may, however, realize in the future that the system was in a secret state. For example, if the intruder estimates that the system is in one of two possible states, and the next step proceeds by an observable event enabled only in one of the states, the intruder reveals the state in which the system was one step ago. This problem led to the introduction of K-SO [11], [12], a notion requiring that the intruder cannot ascertain the secret in the current state and K subsequent observable steps.

An interesting question is how the opacity notions are related to each other. The question has been investigated via transformations among the notions [10], [13], [14], which are of interest from both practical and theoretical perspectives.

To illustrate a few practically oriented applications, we start with the results of deeper understanding of the notions, which allowed us to design faster verification algorithms [14], discover that every system satisfying CSO can be transformed to an equivalent system satisfying CSO with a single secret state, or transform K-SO to K'-SO for any K and K' (Section III).

Second, the transformations allow us to use the verification algorithms for one notion to verify another notion. For example, we can transform the problem to verify K-SO of a given system to the problem to verify CSO of the transformed system. This application is of interest, even though there are direct and possibly faster algorithms verifying other opacity notions than the methods based on the transformations, because it may be practically easier, cheaper, and more efficient to develop, optimize, and maintain a verification tool for one notion, say CSO, than for all the notions. Moreover, the transformations from one notion to another are structural, easily doable by polynomial-time algorithms, while the tools implementing verification algorithms are quite involved, implementing exponential-time algorithms that do not scale well, depending therefore on the use of efficient and nontrivial data structures for symbolic computations (such as OBDDs, etc.).

Another interesting, practically motivated application of the transformations is an automatic modification of a system to a higher level of confidentiality. For example, imagine a system that satisfies CSO. Since the applicability and usage of the system develops, at some point, CSO may not be sufficient any longer, and K-SO is required instead. It would be practically very useful to have a tool transforming the system satisfying CSO to an equivalent system satisfying K-SO. Unfortunately, current transformations are not suitable for such an application, and further research is needed. In fact, some of the current transformations may, in a sense, be used with the help of other mechanisms, such as supervisors or controllers protecting the resulting system from reaching states out of the behavior of the original system, or with the help of hand-made modifications

Supported in part by the Ministry of Education, Youth and Sports under the INTER-EXCELLENCE project LTAUSA19098 and by the Palacky University Olomouc under the grant IGA PrF 2022 018. T. Masopust is also with the Institute of Mathematics of the Czech Academy of Sciences supported by the Czech Science Foundation grant GC19-06175J and by RVO 67985840.

by the system designer. To make this approach fully automatic is, however, a challenging open problem.

From the theoretical point of view, the main and most important application of the transformations is the classification of problems wrt their complexity. The transformations serve as a tool to transfer the complexity results among the notions. For example, Corollary 3 states that deciding CSO for systems with a single secret state is as hard as deciding CSO for general systems. In other words, any attempt to improve the efficiency of the verification algorithms by decreasing the number of secret states in the considered systems will not be successful.

Another theoretic application of the transformations tells us that the known fact that deciding CSO is PSPACE-complete even for systems modeled by DFAs with only three events, one of which is unobservable [15], transfers directly to the fact that the problem of deciding K-SO, K $\in \mathbb{N}_\infty$, is PSPACE-complete even for systems modeled by DFAs with a single secret state and only three events, one of which is unobservable. Stated differently, the efficiency of the algorithms cannot be improved by considering only systems with a limited number of secret states and/or with a limited number of observable events.

In particular, a direct application of polynomial-time transformations provided in this paper is that the existing complexity results for K-SO (and hence also INSO and CSO, cf. [14, Table 1]) hold for systems that do not have neutral states (states that are neither secret nor non-secret) and where the parameter K is represented in binary. These results significantly improve the known results [14], where the transformations heavily rely on the existence of neutral states, although their existence is not practically justified, and, mainly, the transformations there are, in fact, exponential if the value of K is exponential.

It is worth noticing that the complexity analysis of Balun and Masopust [14] states that the problem of verifying K-SO is PSPACE-complete only if the parameter K is constant or its value is very small, meaning that the value of K is at most polynomial wrt the size of the input system. In detail, the analysis does not consider the parameter K as part of the input of the decision procedure, and the existing transformations are, in fact, exponential wrt the length of the binary representation of the parameter K. Namely, the complexity of verifying K-SO is open if the input to the problem is not only the system, but also the parameter K in a standard binary representation commonly used for the representations of numbers in computers. The same actually applies to Saboori's [16] proof showing that verifying K-SO is NP-hard. Hence the complexity of deciding whether, given a number K represented in binary and a system, the system is K-SO is an open problem.

In this paper, we design new polynomial-time transformations of K-SO to CSO, and vice versa, which are polynomial in both the size of the system and the length of the binary encoding of the parameter K. We then use our transformations to answer the previous open problem by showing that deciding K-SO is PSPACE-complete even if K is considered to be a part of the input represented in binary.

Another problem with the existing transformations between K-SO and other notions of opacity is that they do not work if neutral states are not admitted in the system. Neutral states are states that are neither secret nor nonsecret. Our new transformations fix this issue, and work independently on whether neutral states are admitted or not.

All the missing details and proofs omitted for space reasons can be found in preprint [17], on which this paper is based.

II. Preliminaries

We assume that the reader is familiar with discrete-event systems [18]. For a set S, $|S|$ denotes the cardinality of S and 2^S its power set. An alphabet Σ is a finite nonempty set of events. A string over Σ is a sequence of events; the empty string is denoted by ε. The set of all finite strings over Σ is denoted by Σ^*. A language L over Σ is a subset of Σ^*. The set of prefixes of strings of L is the set $\overline{L} = \{u \mid \exists v \in \Sigma^*, uv \in L\}$. For $u \in \Sigma^*$, $|u|$ is the length of u.

A *nondeterministic finite automaton* (NFA) over an alphabet Σ is a structure $G = (Q, \Sigma, \delta, I, F)$, where Q is a finite set of states, $I \subseteq Q$ is a set of initial states, $F \subseteq Q$ is a set of marked states, and $\delta \colon Q \times \Sigma \to 2^Q$ is a transition function that can be extended to $2^Q \times \Sigma^*$ by induction. The set $L_m(G, I) = \{w \in \Sigma^* \mid \delta(I, w) \cap F \neq \emptyset\}$ is the language *marked* by G, and $L(G, I) = \{w \in \Sigma^* \mid \delta(I, w) \neq \emptyset\}$ is the language *generated* by G. For $S \subseteq \Sigma^*$, we write $\delta(Q, S) = \cup_{s \in S} \delta(Q, s)$. The NFA G is *deterministic* (DFA) if $|I| = 1$ and $|\delta(q, a)| \leq 1$ for every $q \in Q$ and $a \in \Sigma$.

A *discrete-event system* (DES) G over Σ is an NFA over Σ together with the partition of Σ into Σ_o and Σ_{uo} of *observable* and *unobservable events*, respectively. If the marked states are irrelevant, we omit them and simply write $G = (Q, \Sigma, \delta, I)$.

A *projection* $P \colon \Sigma^* \to \Sigma_o^*$ is a morphism with $P(a) = \varepsilon$ if $a \in \Sigma_{uo}$, and $P(a) = a$ if $a \in \Sigma_o$. The action of P on a string $a_1 \cdots a_n$, $P(a_1 \cdots a_n) = P(a_1) \cdots P(a_n)$, is to erase unobservable events. It can be readily extended to languages.

An *observer of G with respect to projection P* is a reachable part of a DFA constructed, by the standard subset construction, from the (extended) NFA obtained from G by replacing every transition label a by $P(a)$. For more details, see [18] or [19].

Let $\mathbb{N}$ be the set of non-negative integers, and let $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$. Given a DES $G = (Q, \Sigma, \delta, I)$ and $K \in \mathbb{N}_\infty$, G is *K-step opaque* with respect to secret states Q_S, non-secret states Q_{NS}, and projection $P \colon \Sigma^* \to \Sigma_o^*$ if for every string $st \in L(G)$ with $|P(t)| \leq K$ and $\delta(\delta(I, s) \cap Q_S, t) \neq \emptyset$, there is $s't' \in L(G)$ such that $P(s) = P(s')$, $P(t) = P(t')$, and $\delta(\delta(I, s') \cap Q_{NS}, t') \neq \emptyset$. Two special cases of K-step opacity include 0-step opacity aka *current-state opacity*, and ∞-step opacity aka *infinite-step opacity* [12], which, for a DES with n states, coincides with $(2^n - 2)$-step opacity [20].

III. Transformations

We construct new transformations of K-SO to CSO, and vice versa. Compared with the existing transformations, which are exponential wrt the standard binary representation of the parameter K, the new transformations are polynomial wrt the binary representation of K. For the transformations of CSO to other opacity notions, we refer to [13], [14].

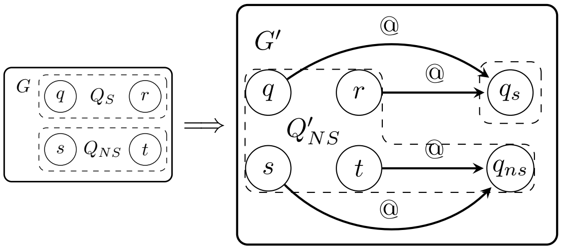

Figure 1. Transforming CSO to K-SO for any K $\in \mathbb{N}_\infty$.

Construction 1. *Let $G = (Q, \Sigma, \delta, I)$ be a DES with secret states Q_S, non-secret states Q_{NS}, and $P \colon \Sigma^* \to \Sigma_o^*$. We construct a DES $G' = (Q \cup \{q_s, q_{ns}\}, \Sigma \cup \{@\}, \delta', I)$ where @ is a new observable event and q_s and q_{ns} are new states. The transition function δ' is initialized as δ of G and further extended as follows, see Figure 1 for an illustration: (i) for every $q \in Q_S$, we add $(q, @, q_s)$ to δ'; (ii) for every $q \in Q_{NS}$, we add $(q, @, q_{ns})$ to δ'. We define $P' \colon (\Sigma \cup \{@\})^* \to (\Sigma_o \cup \{@\})^*$, secret states $Q'_S = \{q_s\}$, and non-secret states $Q'_{NS} = Q_S \cup Q_{NS} \cup \{q_{ns}\}$.*

We can now state the following.

Theorem 2. *A DES G is CSO wrt Q_S, Q_{NS}, and P iff G' created by Construction 1 is K-SO wrt Q'_S, Q'_{NS}, and P'.* □

The transformation is doable in polynomial time, does not depend on K, and does not use neutral states. However, it introduces a new observable event. In fact, the number of observable events in G' can be reduced in polynomial time to two [17]. Since, in addition, the transformation reduces CSO to K-SO with a single secret state, we have that the problem is difficult even if the number of secret states and observable events is very small. Consequently, we can now answer the open problem concerning the complexity of deciding K-SO if K is given as part of the input represented in binary.

Corollary 3. *Given a parameter $K \in \mathbb{N}_\infty$ represented in binary, and a system G. Deciding whether G satisfies K-SO is* PSPACE*-complete. The problem remains* PSPACE*-complete even if G is very restricted, namely, if it has a single secret state and only two observable events.* □

The lower-bound complexity, i.e., PSPACE-hardness, follows from the polynomial-time reduction from CSO to K-SO described by Construction 1. The fact that K-SO can be verified in polynomial space with respect to both the size of the system and the length of the binary encoding of K can be proved either directly, or it follows from the polynomial-time reduction of K-SO to CSO described by Construction 9.

We further mention, referring to [17], that a direct transformation preserving a single observable event that does not admit neutral states may be designed. This transformation is of particular interest in, e.g., the Brandin-Wonham timed DES framework, where the single observable event represents the tick of a global clock, while all the other events are local.

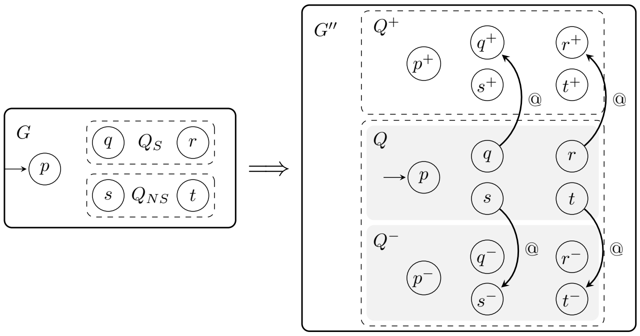

Figure 2. Automaton G'' of the first step transforming K-SO to CSO.

Theorem 4. *A DES G with a single observable event is CSO wrt Q_S, Q_{NS}, and P iff G' constructed in [17] having a single observable event is K-SO wrt Q'_S, Q'_{NS}, and P'.* □

We now proceed to the transformation of INSO to CSO.

Construction 5. *Let $G = (Q, \Sigma, \delta, I)$ be a DES with secret states Q_S, non-secret states Q_{NS}, and $P \colon \Sigma^* \to \Sigma_o^*$. We construct a DES $G'' = (Q \cup Q^+ \cup Q^-, \Sigma \cup \{@\}, \delta', I)$ by creating two disjoint copies of G, denoted by G^+ and G^-, with state sets $Q^+ = \{q^+ \mid q \in Q\}$ and $Q^- = \{q^- \mid q \in Q\}$, and with an additional observable event @ that connects G to G^+ and G^- by the transitions $(q, @, q^+)$, for every $q \in Q_S$, and $(q, @, q^-)$, for every $q \in Q_{NS}$. Secret states are $Q''_S = Q^+$ and non-secret states are $Q''_{NS} = Q \cup Q^-$, see Figure 2.*

The idea of the construction is that if G is K-SO, and hence CSO, then the state estimate of G contains a non-secret state whenever it contains a secret state. Hence, being in a secret (and hence also non-secret) state, the new @-transitions move the computation to both copies G^+ and G^-. In these copies, we verify that if G can make k steps from the secret state (in G^+), it can also make k steps from the corresponding non-secret state (in G^-). This is verified using CSO by considering the states of G^+ secret and of G^- non-secret, which requires that every move in G^+ be accompanied by a move in G^-.

Notice that G'' can be constructed in polynomial-time using no neutral states. The construction of G'' is already suitable to verify INSO of G by checking CSO of G''.

Theorem 6 (Transforming INSO to CSO)**.** *A DES G is INSO wrt Q_S, Q_{NS}, and P iff G'' created by Construction 5 is CSO wrt Q''_S, Q''_{NS}, and $P'' \colon (\Sigma \cup \{@\})^* \to (\Sigma_o \cup \{@\})^*$.* □

Although G'' resulting from Construction 5 can verify INSO of G by checking CSO of G'', it is not suitable to verify K-SO; indeed, G'' verifies any number of steps from the visited secret state rather than at most K steps. To overcome this issue, we extend Construction 5 by adding a counter that allows us to count up to K observable events from a visited secret state.

Construction 7. *For the counter, we use the automaton $\mathcal{A}_K$ constructed in Appendix A, which is of size polynomial in the logarithm of K, its unique initial state is denoted by q_0, and*

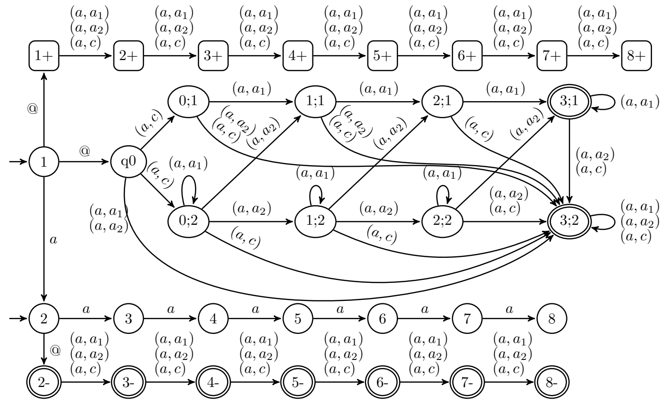

Figure 3. The DES G''' of the transformation of 6-SO to CSO with neutral states; secret states are squared and non-secret states are marked.

its observer has a unique path of length K consisting solely of non-marked states, while all the other states are marked.

However, the automata G, G^+, G^- of Construction 5 are over the alphabet Σ, while $\mathcal{A}_K$ is over Γ, which is disjoint from Σ. Hence, we change the alphabets of the automata to

$$\Sigma' = \Sigma \cup (\Sigma_o \times \Gamma)\,.$$

Namely, in G^+ and G^-, we replace every observable *transition (p,σ,q) by $|\Gamma|$ transitions $(p,(\sigma,\gamma),q)$, for every $\gamma \in \Gamma$, and denote the results by $\tilde{G}^+$ and $\tilde{G}^-$. Similarly, in $\mathcal{A}_K$, we replace every transition (p,γ,q) by $|\Sigma_o|$ transitions $(p,(\sigma,\gamma),q)$, for every observable $\sigma \in \Sigma_o$, and denote the result by $\tilde{\mathcal{A}}_K$.*

We admit, for a moment, neutral states, and construct the NFA G''' as a disjoint union of G, $\tilde{G}^+$, $\tilde{G}^-$, and $\tilde{\mathcal{A}}_K$, together with transitions $(q,@,q^+)$, $(q,@,q_0)$, for every $q \in Q_S$, where q_0 is the initial state of $\tilde{\mathcal{A}}_K$, and $(q,@,q^-)$, for every $q \in Q_{NS}$. Secret states are $Q'''_S = Q^+$ and non-secret states are $Q'''_{NS} = Q^- \cup \{$marked states of $\tilde{\mathcal{A}}_K\}$. The other states are neutral.

The construction transforms the K-SO problem of G to the CSO problem of G'''.

Theorem 8 (K-SO to CSO with neutral states)**.** *A DES G is K-SO wrt Q_S, Q_{NS}, and P iff the DES G''' created by Construction 7 from the DES G is CSO wrt Q'''_S, Q'''_{NS}, and $P''' \colon (\Sigma' \cup \{@\})^* \to (\Sigma_o \cup \{@\} \cup \Sigma_o \times \Gamma)^*$.* □

To illustrate Construction 7, we transform the 6-SO problem of $G = (\{1,\dots,8\},\{a\},\delta,\{1,2\})$ with $\delta(i,a) = \{i+1\}$, $i = 1,\dots,7$, $Q_S = \{1\}$, and $Q_{NS} = \{2\}$. Notice that G is 6-SO, since we can make six steps from both states 1 and 2. To encode K $= 6$, the transformation uses $\mathcal{A}_6 = \mathcal{A}_{2,2}$ (see Appendix A), and results in G''' of Figure 3, where all non-secret states are marked. The minimized observer of G''' is shown in Figure 4. Since every state of the observer reachable by a string containing @ is marked, it has to contain a non-secret state of G, that is, G''' is CSO.

If we remove state 8 from G together with the corresponding transitions, then G is not 6-SO, since we can make six steps from secret state 1, but only five steps from the corresponding non-secret state 2. The transformation results in G''' that coincides with the automaton of Figure 3 disregarding states 8, 8^+, 8^-, and corresponding transitions. The minimized observer is shown in Figure 5, where state 4, corresponding to state $\{7^+,(2;1),(2;2)\}$, is secret and reachable by the string $@(a,c)(a,a_1)(a,a_1)(a,a_2)(a,a_1)(a,a_2)$, i.e., G''' is not CSO.

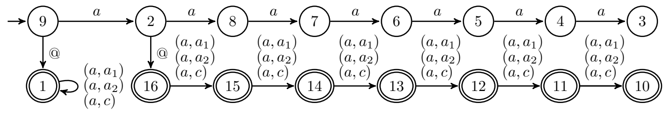

Figure 4. The minimized observer of G''' of Figure 3.

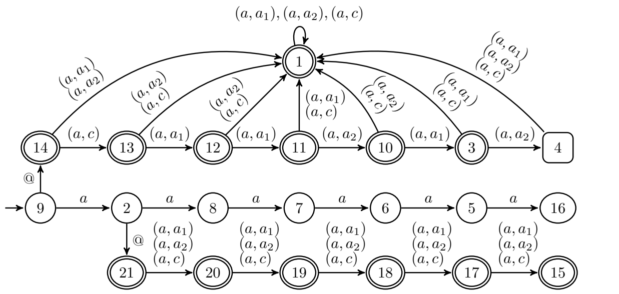

Figure 5. The minimized observer of G''' of Figure 3 disregarding states 8, 8^+, 8^-, and corresponding transitions.

Finally, we describe the transformation of K-SO to CSO without using neutral states.

Construction 9. *We consider Construction 7, make all states of $\tilde{G}^+$ both initial and marked, and synchronize the computations of $\tilde{G}^+$ and $\tilde{\mathcal{A}}_K$ by their synchronous product $\tilde{G}^+ \| \tilde{\mathcal{A}}_K$. Now, we construct a DES G' as a disjoint union of G, $\tilde{G}^-$, and $\tilde{G}^+ \| \tilde{\mathcal{A}}_K$, connected together by transitions $(q,@,(q^+,q_0))$, for every $q \in Q_S$, and $(q,@,q^-)$, for every $q \in Q_{NS}$. The secret states of G' are the non-marked states of $\tilde{G}^+ \| \tilde{\mathcal{A}}_K$. All the other states are non-secret.*

The transformation can be done in polynomial time in the system size and the binary encoding of K. How to reduce the number of observable events can be found in [17]. We can thus state the following result.

Theorem 10 (K-SO to CSO without neutral states)**.** *A DES G is K-SO wrt Q_S, Q_{NS}, and P iff the DES G' created by Construction 9 from the DES G is CSO wrt Q'_S, Q'_{NS}, and $P' \colon (\Sigma' \cup \{@\})^* \to (\Sigma_o \cup \{@\} \cup \Sigma_o \times \Gamma)^*$.* □

To illustrate Construction 9, we again transform the 6-SO problem $G = (\{1,\dots,8\},\{a\},\delta,\{1,2\})$ with state 1 secret and the other states non-secret, and $\delta(i,a) = \{i+1\}$, $i = 1,\dots,7$. The transformation results in G' depicted in Figure 6, using again the NFA $\mathcal{A}_6$. The minimized observer of G' is depicted in Figure 7. Since every state of the observer reachable by a string containing @ is marked, it has to contain a non-secret state of G, that is, G' is CSO.

If we remove state 8 from G together with the corresponding transitions, the transformation results in the DES G' that coincides with the NFA of Figure 6 without states containing

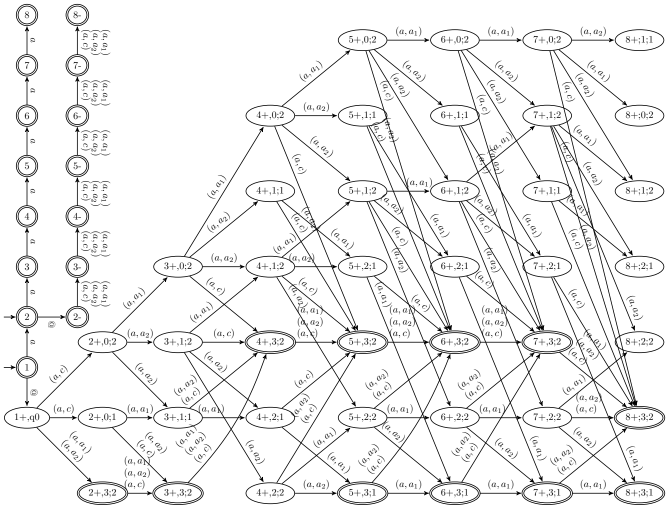

Figure 6. DES G' with a relevant part of $\tilde{G}^+ \| \tilde{\mathcal{A}}_6$; non-secret states are marked, other states are secret.

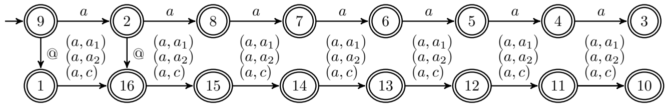

Figure 7. The minimized observer of G'.

8, 8^+, 8^-, and the corresponding transitions. The minimized observer is shown in Figure 8, where state 4, abbreviating the state $\{(7^+,(2;1)),(7^+,(2;2))\}$ consisting of secret states of $\tilde{G}^+ \| \tilde{\mathcal{A}}_{\mathrm{K}}$, is reachable by the string $@(a,c)(a,a_1)(a,a_1)$ $(a,a_2)(a,a_1)(a,a_2)$, that is, G' is not CSO.

Again, we can provide a direct transformation for systems with one observable event, which is of interest in, e.g., the Brandin-Wonham timed DES framework.

Theorem 11 (K-SO to CSO with a single observable event)**.** *A DES $G = (Q, \Sigma, \delta, I)$ with $\Sigma_o = \{a\}$, secret states Q_S, non-secret states $Q_{NS} = Q - Q_S$, and $P\colon \Sigma^* \to \{a\}^*$ is K-SO wrt Q_S, Q_{NS}, and P iff G is CSO wrt Q'_S, Q'_{NS}, and P, where Q'_S and Q'_{NS} are constructed as follows.*

Let n be the number of states of G. We determine (in linear time) if $P(L(G))$ is finite. If so, we verify K-SO of G in linear time by checking the subsets of states $\delta(I, P^{-1}(a^k))$, for $k \leq n-1$. If G is K-SO, and hence CSO, set $Q'_S = Q_S$ and $Q'_{NS} = Q_{NS}$. If G is not K-SO, set $Q'_{NS} = \emptyset$ and $Q'_S = Q$.

If $P(L(G))$ is infinite, define $Q'_{NS} = \{q \in Q_{NS} \mid \varphi(q) = K\}$, where $\varphi\colon Q \to \{0,\dots,K\}$ assigns to q the maximal $k \in \{0,\dots,K\}$ of observable steps possible from q. Formally, $\varphi(q) = \max\{k \in \{0,\dots,K\} \mid \delta(q, P^{-1}(a^k)) \neq \emptyset\}$. The secret states are $Q'_S = Q - Q'_{NS}$. □

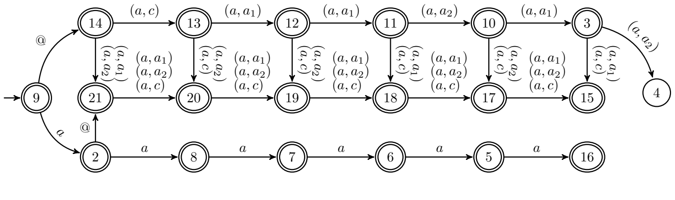

Figure 8. The minimized observer of G' of Figure 6 disregarding states containing 8, 8^+, 8^-, and corresponding transitions.

IV. Conclusions

We designed new transformations of K-SO to CSO, and vice versa, which are polynomial in both the size of the system and the length of the binary encoding of the parameter K, and, in addition, are universal, meaning that they work independently on whether neutral states are allowed in the system or not. We also discussed several challenging applications of the transformations and answered one open problem.

Appendix A
Logarithmic Encoding of a K-Step Counter

We construct an NFA $\mathcal{A}_{\mathrm{K}}$ of size polynomial in the logarithm of K such that the observer of $\mathcal{A}_{\mathrm{K}}$ has a unique path of length K consisting solely of non-marked states, while all the other states are marked.

Lemma 12. *For all integers $k, n \geq 1$, there is an NFA $\mathcal{A}_{k,n}$ with n events and $n(k+2)$ states, such that $\mathcal{A}_{k,n}$ accepts all strings except for all prefixes of a unique string $W_{k,n}$, which is a string of length $\binom{k+n}{k} - 1$.*

Proof. For $k, n \geq 1$, we define the string $W_{k,n}$ over $\Sigma_n = \{a_1,\dots,a_n\}$ by $W_{k,1} = a_1^k$, $W_{1,n} = a_1 a_2 \cdots a_n$, and $W_{k,n} = W_{k,n-1} a_n W_{k-1,n-1} a_n \cdots a_n W_{1,n-1} a_n$. The length of $W_{k,n}$ is $\binom{k+n}{k} - 1$, and a_n appears exactly k times in $W_{k,n}$ [21]. We further set $W_{k,n} = \varepsilon$ whenever $kn = 0$. We construct the NFA $\mathcal{A}_{k,n}$ over Σ_n marking $\underline{\Sigma_n^*} - \underline{\{W_{k,n}\}}$. For $k \geq 0$, $\mathcal{A}_{k,1}$ is the DFA marking $\{a_1\}^* - \underline{\{a_1^k\}}$ consisting of $k+2$ states of the form $(i;1)$, see Figure 9, together with the given transitions. State $(k+1;1)$ is marked, state $(0;1)$ is initial.

We construct $\mathcal{A}_{k,n}$ from $\mathcal{A}_{k,n-1}$ by adding $k+2$ states $(0;n), (1;n), \dots, (k+1;n)$, where $(0;n)$ is added to initial, and $(k+1;n)$ to final states, see Figure 10 for $n=2$; $\mathcal{A}_{k,n}$ has $n(k+2)$ states. We call state $(k+1, n)$ *maximal*. Additional transitions of $\mathcal{A}_{k,n}$ consist of: Self-loops $(i;n) \xrightarrow{a_j} (i;n)$ for $i \in \{0,\dots,k+1\}$ and $a_j \in \{a_1,\dots,a_{n-1}\}$; transitions $(i;n) \xrightarrow{a_n} (i+1;n)$ for $i \in \{0,\dots,k\}$, and the self-loop $(k+1;n) \xrightarrow{a_n} (k+1;n)$; transitions $(i;n) \xrightarrow{a_n} (i+1;m)$ for $i \in \{0,\dots,k\}$ and $m \in \{1,\dots,n-1\}$; and transitions $(i;m) \xrightarrow{a_n} (k+1;n)$ for every $(i;m)$ of $\mathcal{A}_{k,n-1}$ with $i \neq k$. For details, see [17]. □

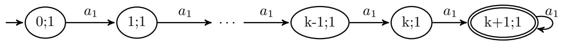

Figure 9. The NFA $\mathcal{A}_{k,1}$ with $k+2$ states.

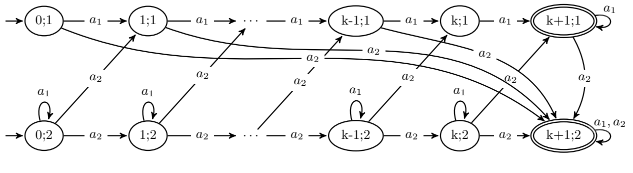

Figure 10. The NFA $\mathcal{A}_{k,2}$ with $2(k+2)$ states.

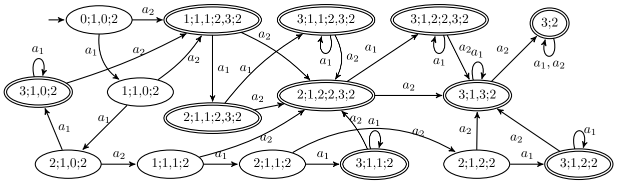

Figure 11. The observer of the NFA $\mathcal{A}_{2,2}$.

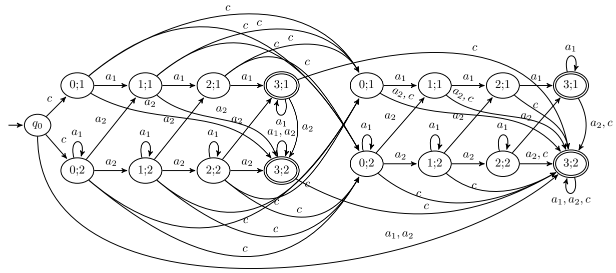

Figure 12. Example for $\mathrm{K} = 12$, which gives $a_2 = 2$, the automaton $\mathcal{A}_{12}$ consisting of two copies of $\mathcal{A}_{2,2}$.

For an illustration, let $k = n = 2$. Then, $W_{2,2} = a_1^2 a_2 a_1 a_2$, NFA $\mathcal{A}_{2,2}$ has 8 states, and the observer of $\mathcal{A}_{2,2}$ in Figure 11 contains a unique path of length $\binom{4}{2} - 1 = 5$ consisting solely of non-marked states while all the other states are marked.

Since $\binom{2n+2}{n+1} = \frac{4n+2}{n+1}\binom{2n}{n}$ and $\binom{2n}{n} \le 4^n$, every natural K can be expressed as $\mathrm{K} = b_n\binom{2n}{n} + b_{n-1}\binom{2n-2}{n-1} + \cdots + b_1\binom{2}{1} + b_0$ for some $n \le \lceil \log_4(\mathrm{K}+1) \rceil$ and $b_i \in \{0,1,2,3\}$, $i = 0,\dots,n$.

For every b_i, $i = n,\dots,0$, we create b_i copies of $\mathcal{A}_{i,i}$ over $\Sigma_i = \{a_1 \dots, a_i\}$, resulting in a sequence of automata $\mathcal{B}_1,\dots,\mathcal{B}_\ell$. We take an event $c \notin \Sigma_n$ and connect $\mathcal{B}_1,\dots,\mathcal{B}_\ell$ to a single automaton $\mathcal{A}_\mathrm{K}$ by c-transitions as follows. For $j = 1,\dots,\ell-1$, we add a c-transition from every non-marked state of $\mathcal{B}_j$ to every initial state of $\mathcal{B}_{j+1}$; from all the other states, the c-transition goes to the maximal state of $\mathcal{B}_\ell$. Finally, we add a new state, q_0, which is the only initial state of $\mathcal{A}_\mathrm{K}$, c-transitions from q_0 to all initial states of $\mathcal{B}_1$, and transitions under all the other events to the maximal state of $\mathcal{B}_\ell$; see Figure 12 for an illustrative example.

The observer of $\mathcal{A}_\mathrm{K}$ has a unique path consisting of non-marked states along the string $(cW_{n,n})^{b_n}(cW_{n-1,n-1})^{b_{n-1}} \dots (cW_{0,0})^{b_0}$ of length $\mathrm{K} = b_n\binom{2n}{n} + b_{n-1}\binom{2n-2}{n-1} + \cdots + b_0\binom{0}{0}$, and the other states are marked. Since every $\mathcal{B}_j$ is of size polynomial in n, $\mathcal{A}_\mathrm{K}$ is of size polynomial in the logarithm of K and its observer has a unique path of length K consisting solely of non-marked states, with all the other states marked.

Lemma 13. *For every natural number K, there is an automaton $\mathcal{A}_K$ of size polynomial in $O(\log K)$ such that the observer of $\mathcal{A}_K$ has a unique path of length K consisting solely of non-marked states, and with all the other states marked.* □

For an illustration, consider $\mathrm{K} = 12 = 2\binom{4}{2} + 0\binom{2}{1} + 0$. We create two copies of $\mathcal{A}_{2,2}$ and connect them by c-transitions as shown in Figure 12. The observer with the unique path of non-marked states of length $\mathrm{K} = 12$ is shown in Figure 13.

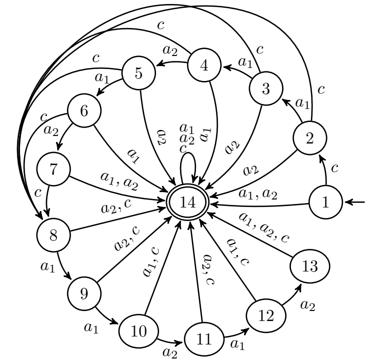

Figure 13. The min. DFA of the observer with the unique path of length 12.

References

[1] S. Schneider and A. Sidiropoulos, "CSP and anonymity," in *Computer Security (ESORICS)*. Springer Berlin Heidelberg, 1996, pp. 198–218.

[2] N. BenHadj-Alouane, S. Lafrance, F. Lin, J. Mullins, and M. Yeddes, "On the verification of intransitive noninterference in mulitlevel security," *IEEE Trans. Syst. Man Cybern.: Syst.*, vol. 35, pp. 948–958, 2005.

[3] R. Alur, P. Černý, and S. Zdancewic, "Preserving secrecy under refinement," in *ICALP*. Springer Berlin Heidelberg, 2006, pp. 107–118.

[4] R. Focardi and R. Gorrieri, "A taxonomy of trace-based security properties for CCS," in *CSFW VII*, 1994, pp. 126–136.

[5] L. Mazaré, "Decidability of opacity with non-atomic keys," in *Formal Aspects in Security and Trust*. Springer-Verlag, 2004, pp. 71–84.

[6] J. W. Bryans, M. Koutny, and P. Y. Ryan, "Modelling opacity using Petri nets," *El. Notes Theor. Comput. Sci.*, vol. 121, pp. 101–115, 2005.

[7] J. W. Bryans, M. Koutny, L. Mazaré, and P. Y. A. Ryan, "Opacity generalised to transition systems," *Int. J. Inf. Secur.*, vol. 7, no. 6, pp. 421–435, 2008.

[8] E. Badouel, M. Bednarczyk, A. Borzyszkowski, B. Caillaud, and P. Darondeau, "Concurrent secrets," *Discrete Event Dyn. Syst.*, vol. 17, no. 4, pp. 425–446, 2007.

[9] J. Dubreil, P. Darondeau, and H. Marchand, "Opacity enforcing control synthesis," in *WODES*, 2008, pp. 28–35.

[10] R. Jacob, J.-J. Lesage, and J.-M. Faure, "Overview of discrete event systems opacity: Models, validation, and quantification," *Annu. Rev. Control*, vol. 41, pp. 135–146, 2016.

[11] A. Saboori and C. N. Hadjicostis, "Notions of security and opacity in discrete event systems," in *IEEE CDC*, 2007, pp. 5056–5061.

[12] ——, "Verification of infinite-step opacity and complexity considerations," *IEEE Trans. Autom. Control*, vol. 57, no. 5, pp. 1265–1269, 2012.

[13] Y.-C. Wu and S. Lafortune, "Comparative analysis of related notions of opacity in centralized and coordinated architectures," *Discrete Event Dyn. Syst.*, vol. 23, no. 3, pp. 307–339, 2013.

[14] J. Balun and T. Masopust, "Comparing the notions of opacity for discrete-event systems," *Discrete Event Dyn. Syst.*, vol. 31, pp. 553–582, 2021.

[15] ——, "On opacity verification for discrete-event systems," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 2075–2080, 2020.

[16] A. Saboori, "Verification and enforcement of state-based notions of opacity in discrete event systems," Ph.D. dissertation, Uni. Illinois at Urbana-Champaign, 2011.

[17] J. Balun and T. Masopust, "K-step opacity in discrete event systems: Verification, complexity, and relations," *CoRR*, vol. abs/2109.02158, 2021. [Online]. Available: https://arxiv.org/abs/2109.02158

[18] C. G. Cassandras and S. Lafortune, Eds., *Introduction to Discrete Event Systems*, 3rd ed. Springer, Cham, 2021.

[19] G. Jirásková and T. Masopust, "On a structural property in the state complexity of projected regular languages," *Theoret. Comput. Sci.*, vol. 449, pp. 93–105, 2012.

[20] X. Yin and S. Lafortune, "A new approach for the verification of infinite-step and K-step opacity using two-way observers," *Automatica*, vol. 80, pp. 162–171, 2017.

[21] T. Masopust and M. Thomazo, "On boolean combinations forming piecewise testable languages," *Theoret. Comput. Sci.*, vol. 682, pp. 165–179, 2017.