View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by CiteSeerX

Opacity Issues in Games with Imperfect Information

Bastien Maubert
ENS Cachan - Bretagne
Bruz, 35170, France
bastien.maubert@irisa.fr

Sophie Pinchinat
S4, IRISA, Campus de Beaulieu
Rennes, 35042, France
sophie.pinchinat@irisa.fr

Laura Bozzelli
Technical University of Madrid (UPM)
28660 Boadilla del Monte, Madrid, Spain
laura.bozzelli@fi.upm.es

We study in depth the class of games with opacity condition, which are two-player games with imperfect information in which one of the players only has imperfect information, and where the winning condition relies on the information he has along the play. Those games are relevant for security aspects of computing systems: a play is *opaque* whenever the player who has imperfect information never "knows" for sure that the current position is one of the distinguished "secret" positions. We study the problems of deciding the existence of a winning strategy for each player, and we call them the *opacity-violate problem* and the *opacity-guarantee problem*. Focusing on the player with perfect information is new in the field of games with imperfect-information because when considering classical winning conditions it amounts to solving the underlying perfect-information game. We establish the EXPTIME-completeness of both above-mentioned problems, showing that our winning condition brings a gap of complexity for the player with perfect information, and we exhibit the relevant *opacity-verify problem*, which noticeably generalizes approaches considered in the literature for opacity analysis in discrete-event systems. In the case of blindfold games, this problem relates to the two initial ones, yielding the determinacy of blindfold games with opacity condition and the PSPACE-completeness of the three problems.

1 Introduction

We described in [14] a class of two-player games with imperfect information that we called *games with opacity condition*. In these games, the players are Robert (for "robber") and Gerald (for "guardian"). Robert has imperfect information as opposed to Gerald who has perfect information. This asymmetric setting is very relevant for the verification of open systems and all the more for security aspects as it captures the intuitive picture of an attacker having only a partial information against a system. The game model we consider relies on the classical imperfect-information arenas, as defined in *e.g.* [16, 1], but it is equipped with a subset of positions that denote confidential information and that we call *secrets*. We focus on the opportunity for Robert to discover some secret, by introducing the property of *opacity*: a play is *opaque* if, at each step of the (infinite) play, the set of positions that are considered possible by Robert does not consist of secrets only. In games with opacity condition, the opacity property is the winning condition for Gerald. Informally, Robert tries to force the game to reach some point when he knows for sure that the current position is a secret, whereas Gerald tries to keep Robert under uncertainty. Note that this winning condition can be seen as a particular epistemic temporal logic statement [10] on an imperfect information arena seen as an epistemic temporal model : this ETL formula is $G\neg K_{Robert} secret$. However, to our knowledge the complexity of deciding the existence of winning strategies for such winning conditions has never been studied in depth.

Our claim that games with opacity condition are natural and adequate models for practical applications is all the more sustained by very recent contributions of the literature [17, 8]. These results mainly arise from the analysis of discrete-event systems and their theory of control, and our games embed some problems studied in this domain, such as the verification of opacity. Our abstract setting provided by

To appear in EPTCS.

© B. Maubert & S. Pinchinat & L. Bozzelli
This work is licensed under the
Creative Commons Attribution License.

the game-theoretical paradigm enables us to focus on essential aspects of the topic, such as synthesizing strategies, and to circumvent the complexity of the problems.

Not surprisingly, games with opacity condition are not determined [14]. We therefore introduced two dual problems: the *opacity-violate problem* and the *opacity-guarantee problem*, that consist of deciding the existence of a winning strategy, respectively for Robert and for Gerald. The opacity-violate problem generalizes the strategy problem in reachability games with imperfect information [16], and so does the opacity-guarantee problem, but putting the emphasize on the player who has perfect information and has the complementary safety objective. The latter is, to our knowledge, never been done, for the following reason. In two-player games with imperfect information, when considering the existence of winning strategies for a player, one can equivalently consider that the opponent has perfect information (see [16]). Thus, when dealing with omega-regular winning conditions in arenas where the imperfect information is asymmetric, focusing on the player with perfect information would amount to solve the underlying perfect-information game. Our case is different : when considering Gerald's point of view, we could indeed equivalently consider that Robert plays with perfect information too, but we cannot give up the imperfect-information setting because the definition of the winning condition itself relies on Robert's information along the play.

Additionally to the two aforementioned problems, we consider the *opacity-verify problem* as an intermediate problem: the question here is to decide whether in a game with opacity condition, all strategies of Gerald are winning. The choice of considering this apparently weird problem is well motivated. Firstly, it is equivalent both to the opacity-guarantee problem and to the complementary of the opacity-violate problem for blindfold games; an immediate consequence is the determinacy of blindfold games with opacity condition. And secondly, it enables us to embed opacity issues in discrete-event systems with a strong language-theoretic feature, addressed earlier in the literature [17, 8].

In this contribution, we consider the three problems of opacity-violate, opacity-guarantee and opacity-verify, keeping in mind that our main attention turns to the opacity-guarantee problem. It is not hard to establish the EXPTIME-completeness of the opacity-violate problem, from a power-set construction inspired by [16] that amounts to solving a reachability perfect-information game, and from the fact that it generalizes imperfect-information games with reachability condition, known to be EXPTIME-complete [16]. Regarding the opacity-guarantee problem, we rely on an earlier power-set construction to reduce this problem to a perfect-information game [14], yielding EXPTIME membership. The EXPTIME-hardness result for this problem, where the main player (Gerald) has perfect information, was unknown until now and relies on a reduction from the empty input string acceptance problem for linearly-bounded alternating Turing machines. The key point is a pioneer encoding of configurations by information sets. Concerning the opacity-verify problem, we prove its PSPACE-completeness, which for the lower bound relies on a reduction similar to the one in [6] from the universality problem for nondeterministic automata [11]. Interestingly, the opacity-verify problem relates the two other problems for the particular case of *blindfold games*, in such a way that those games are determined. We also show that the blindfold setting embraces the language-theoretic approaches for opacity analysis in discrete-event systems [17, 8].

The paper is organized as follows. In Section 2, we define games with opacity condition. In Section 3, we present the opacity-guarantee problem and the opacity-violate problem, and we establish their EXPTIME complexity. We first recall the power-set constructions from [14] yielding the upper bounds, then we show the matching lower bounds. In Section 4, we consider the opacity-verify problem for blindfold games. In this setting, we establish the determinacy and the PSPACE completeness of the three opacity problems. In Section 5, we relate the opacity-verify problem to the language opacity verification of [17, 8]. In Section 6, we discuss complexity aspects of problems regarding Gerald's winning strategies. We conclude in Section 7 by giving some ideas on our current and future work.

2 Games with opacity condition

A *game with opacity condition* over the alphabet Σ and the set of observations Γ is an imperfect information game structure $A = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0, S)$ where V is a finite set of *positions*, $\Delta : V \times \Sigma \to 2^V \backslash \emptyset$ is a *transition function*, $\mathrm{obs} : V \to \Gamma$ is an *observation function*, and $\mathrm{act} : \Gamma \to 2^\Sigma \backslash \emptyset$ assigns to each observation a non-empty set of available actions, so that available actions are identical for observationally equivalent positions. Finally, v_0 is the initial position, and the additional element $S \subseteq V$ in the structure A is a finite set of *secret positions*.

In a game $A = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0, S)$, the players are Gerald and Robert. A play is an infinite sequence of rounds, and in each round $i \geq 1$, Robert chooses an action $a_i \in \mathrm{act}(\mathrm{obs}(v_{i-1}))$, Gerald chooses the new position $v_i \in \Delta(v_{i-1}, a_i)$, and Robert observes $\mathrm{obs}(v_i)$. A *play* in A is an infinite sequence $\rho = v_0 a_1 v_1 \ldots \in v_0(\Sigma V)^\omega$ that results from an interaction of Robert and Gerald in this game.

We now extend obs to plays by letting $\mathrm{obs}(v_0 a_1 v_1 a_2 v_2 \ldots) := v_0 a_1 \gamma_1 a_2 \gamma_2 \ldots$ with $\gamma_i = \mathrm{obs}(v_i)$ for each $i \geq 1$. The imperfect information setting leads Robert to partially observe a play ρ as $\mathrm{obs}(\rho)$. Note that since the initial position is a part of the description of the arena, it is known by Robert.

For every natural number $k \in \mathbb{N}$ and play ρ, we denote by $\rho^k \in v_0(\Sigma V)^k$ the k-th prefix of ρ, defined by $\rho^k := v_0 a_1 v_1 \ldots a_k v_k$, with the convention that $\rho^0 = v_0$. We denote by ρ^+ an arbitrary prefix of ρ.

Since the information revealed to Robert is based on observations, a strategy of Robert in A is a mapping of the form $\alpha : v_0(\Sigma\Gamma)^* \to \Sigma$ such that for any play prefix ρ^k ending in observation γ, $\alpha(\mathrm{obs}(\rho^k)) \in \mathrm{act}(\gamma)$. On the contrary Gerald has perfect information on how the play progresses, so a strategy of Gerald in A is a mapping of the form $\beta : v_0(\Sigma V)^*\Sigma \to V$ such that for any play prefix ρ^k ending in position v, for all a in $\mathrm{act}(\mathrm{obs}(v))$, $\beta(\rho^k a) \in \Delta(v, a)$.

Given strategies α and β of Robert and of Gerald respectively, we say that a play $\rho = v_0 a_1 v_1 \ldots$ is *induced by* α if $\forall k \geq 1$, $a_k = \alpha(\mathrm{obs}(\rho^{k-1}))$, and ρ is *induced by* β if $\forall k \geq 1$, $v_k = \beta(\rho^{k-1} a_k)$. We also note $\alpha\widehat{\ }\beta$ the only play induced by α and by β.

In the following, an observation γ might be interpreted as the set of positions it denotes, namely $\mathrm{obs}^{-1}(\gamma)$.

Let us fix a play $\rho = v_0 a_1 v_1 a_2 v_2 \ldots$. Note that every k-th prefix of ρ characterizes a unique *information set* $I(\rho^k) \subseteq V$ consisting of the set of positions that Robert considers possible in the game after k rounds. Formally, information sets can be defined inductively as follows.

Definition 1 *For every play $\rho = v_0 a_1 v_1 a_2 v_2 \ldots$, we let $I(\rho^0) := \{v_0\}$ and $I(\rho^{k+1}) := \Delta(I(\rho^k), a_{k+1}) \cap \mathrm{obs}(v_{k+1})$, for $k \in \mathbb{N}$.*

We now define the opacity property:

Definition 2 *For a given set of secret positions $S \subseteq V$, a play ρ satisfies* the opacity property for *S, or is S-*opaque*, if:*

$$\forall k \in \mathbb{N}, I(\rho^k) \not\subseteq S$$

Informally, the opacity condition means that Robert never knows with certainty that the current position is a secret, because there is always one of the positions he considers possible that is not a secret. In a *game with opacity condition*, the opacity property is the winning condition for Gerald, *i.e* S-opaque plays are winning for Gerald, and the other ones are winning for Robert.

Remark 1 *The definition of the arena and of the opacity condition are slightly different from the ones in [14] : originally Robert's aim was to reach a singleton information set. We introduce here the set of secret positions and define the winning condition accordingly because it makes these games closer to the intuition behind opacity. Anyway the results established in [14] still hold in this setting, and adapting the proofs is straightforward.*

3 Opacity-violate and opacity-guarantee problems

It is well known that perfect-information games are determined [13], and that imperfect-information games are not determined in general. We recall that a game is *determined* if each position is winning for one of the two players.

We proved the following result in [14]:

Theorem 1 *Games with opacity condition are not determined in general.*

This result leads to introduce two dual problems. We remind that α (resp. β) stands for a strategy of Robert (resp. Gerald). We first consider Robert's point of view.

Definition 3 *Given a game with opacity condition* $A = (V, \Delta, \text{obs}, \text{act}, v_0, S)$*, the* opacity-violate problem *is to decide whether the following property holds:*

$$\exists \alpha, \forall \beta,\ \alpha\widehat{\ }\beta \text{ is not } S\text{-opaque}$$

We now consider Gerald's dual point of view.

Definition 4 *Given a game with opacity condition* $A = (V, \Delta, \text{obs}, \text{act}, v_0, S)$*, the* opacity-guarantee problem *is to decide whether the following property holds:*

$$\exists \beta, \forall \alpha,\ \alpha\widehat{\ }\beta \text{ is } S\text{-opaque}$$

Remark 2 *It is important to comment on Definition 4 regarding the universal quantification over Robert's strategies. As defined, this quantification ranges over observation based strategies only. The opacity-guarantee problem would however be equivalent if this quantification ranged over the wider set of perfect information strategies, as already argumented by Reif in [16] : along a play, Robert's possible behaviors are not restricted by observation-based strategies.*

In the rest of this section we prove the following result:

Theorem 2 *The opacity-violate and opacity-guarantee problems are EXPTIME-complete.*

In the following, we adopt the classic convention that the size of a game is the size of its arena, *i.e.* the number of positions.

3.1 Power-set constructions for upper bounds

We recall the power-set constructions of [14] that lead to equivalently solve perfect information games.

We first address the opacity-violate problem. Since we consider the point of view of the player with imperfect information, this problem is close to problems usually studied in games with imperfect information. This is why we can easily rely on previous work on the topic to study its complexity. We remind the construction from [14], which is strongly inspired from the one described by Reif in [16] :

Let $A = (V, \Delta, \text{obs}, \text{act}, v_0, S)$ be a game with opacity condition. We define a reachability perfect-information game $\widetilde{A}$, where the players are Roberta and SuperGeraldine[1]. A position of $\widetilde{A}$ is either I where I is a reachable information set in A - it is a position of Roberta -, or (I, a) where I is a reachable information set in A and $a \in \text{act}(I)$ [2] - it is a position of SuperGeraldine.

[1] We use the superlative "Super" here because in general the winning strategies of SuperGeraldine do not reflect any winning strategy of Gerald in A. She has "more power" than Gerald.

[2] $\text{act}(I)$ makes sense because an information set is always a subset of a single observation.

The game is played as follows. It starts in the initial position $I_0 := \{v_0\}$ of Roberta. In a position I, Roberta chooses $a \in \mathrm{act}(I)$ and moves to position (I,a). Next, let O be the set of reachable observations from I by a. SuperGeraldine chooses a next information set $\Delta(I,a) \cap \gamma$, where γ ranges over O. In $\widetilde{A}$, a play $I_0(I_0,a_1)I_1(I_1,a_2)\ldots$ is winning for Roberta if it reaches a position of the form I with $I \subseteq S$, otherwise it is winning for SuperGeraldine.

Theorem 3 *[14] Robert has a winning strategy in A, if and only if, Roberta has a winning strategy in the perfect-information game $\widetilde{A}$.*

Due to nondeterminacy (Theorem 1), the opacity-guarantee problem has to be studied on its own. We remind the power-set construction for the opacity-guarantee problem described in [14], that leads to a safety perfect-information game $\widehat{A}$. In this game, unlike in $\widetilde{A}$, we maintain an extra information on how Gerald is playing in A. The players in $\widehat{A}$ are SuperRoberta[3] and Geraldine. A position in $\widehat{A}$ is either of the form (I,v) where I is a reachable information set in A, and $v \in I$ - it is a position of SuperRoberta -, or of the form (I,v,a) where I is a reachable information set in A, $v \in I$, and $a \in \mathrm{act}(I)$ - it is a position of Geraldine. The initial position is $(\{v_0\},v_0)$. In position (I,v), SuperRoberta chooses $a \in \mathrm{act}(I)$, and moves to (I,v,a). In position (I,v,a), Geraldine chooses $v' \in \Delta(v,a)$ and moves to (I',v') where $I' = \Delta(I,a) \cap \mathrm{obs}(v')$. In $\widehat{A}$, a play $(I_0,v_0)(I_0,v_0,a_1)(I_1,v_1)\ldots$ is winning for SuperRoberta if it reaches a position (I,v) with $I \subseteq S$, otherwise it is winning for Geraldine.

Theorem 4 *[14] Gerald has a winning strategy in A, if and only if, Geraldine has a winning strategy in the perfect-information game $\widehat{A}$.*

It is well known that perfect-information reachability games and perfect-information safety games are solvable in PTIME. Since the constructions of $\widetilde{A}$ and $\widehat{A}$ involve a single exponential blow-up, it follows from Theorems 3 and 4 that the opacity-violate and opacity-guarantee problems are in EXPTIME.

3.2 Matching lower bounds

We prove here that the opacity-violate and the opacity-guarantee problems are EXPTIME-hard.

First, EXPTIME-hardness of the opacity-violate problem is proved by a reduction from reachability imperfect-information games of [16]. Recall that a *reachability imperfect-information game* is a game of imperfect information $A = (V,F,\Delta,\mathrm{obs},\mathrm{act},v_0)$ over Σ and Γ with a distinguished set of *target observations* $F \subseteq \Gamma$ that Robert aims at reaching.

Theorem 5 *[16] Solving reachability imperfect-information games is* EXPTIME-*complete.*

The reduction is straightforward. Let $A = (V,F,\Delta,\mathrm{obs},\mathrm{act},v_0)$ be a reachability imperfect-information game over Σ and Γ. We define the game with opacity condition $A' := (V,\Delta,\mathrm{obs},\mathrm{act},v_0,S)$ over Σ and Γ, where $S = \bigcup_{\gamma \in F} \gamma$. It is easy to see that solving the reachability imperfect-information game A is equivalent to solving the opacity-violate problem in the game A' : a winning strategy for Robert to reach F in A is also a winning strategy for Robert in A', and vice versa (remember that the information set is always a subset of the current observation).

We now show that the opacity-guarantee problem is EXPTIME-hard by a polynomial-time reduction from the acceptance problem of the empty input string for *linearly-bounded alternating* Turing Machines (TM) with a binary branching degree, which is EXPTIME-complete [5]. The key idea is to encode TM configurations by the information sets.

[3] we use the superlative "Super" as, contrary to what Roberta could do in the game $\widetilde{A}$, SuperRoberta can take advantage of the extra information.

In the rest of this section, we fix such a TM machine $\mathcal{M} = (B, Q = Q_\forall \cup Q_\exists \cup \{q_{acc}, q_{rej}\}, q_0, \delta)$, where B is the input alphabet, $Q_\exists$ (resp. $Q_\forall$) is the set of existential (resp. universal) states, $q_0 \in Q$ is the initial state, $q_{acc} \notin Q_\forall \cup Q_\exists$ is the (terminal) accepting state, $q_{rej} \notin Q_\forall \cup Q_\exists$ is the (terminal) rejecting state, and $\delta : (Q_\forall \cup Q_\exists) \times B \to (Q \times B \times \{+1,-1\}) \times (Q \times B \times \{+1,-1\})$ is the transition function. In each non-terminal step (i.e., the current state is in $Q_\forall \cup Q_\exists$), $\mathcal{M}$ overwrites the tape cell being scanned, and the tape head moves one position to the left (-1) or right ($+1$). Let n be the size of $\mathcal{M}$ and $[n] = \{1,\dots,n\}$. We assume that $n > 1$.

Since $\mathcal{M}$ is linearly bounded, we can assume that $\mathcal{M}$ uses exactly n tape cells when started on the *empty* input string ε. Hence, a configuration (of $\mathcal{M}$ over ε) is a word $C = w_1\,(q,b)\,w_2 \in B^* \cdot (Q \times B) \cdot B^*$ of length exactly n denoting that the tape content is $w_1\,b\,w_2$, the current state is q, and the tape head is at position $|w_1|+1$. The initial configuration C_{init} is given by $(q_0, \sqcup)\,\sqcup^{n-1}$, where $\sqcup$ is the blank symbol. Moreover, without loss of generality, we assume that when started on C_{init}, no matter what are the universal and existential choices, $\mathcal{M}$ always *halts* by reaching a terminal configuration C, i.e. such that the associated state, written $q(C)$, is in $\{q_{acc}, q_{rej}\}$ (this assumption is standard, see [5]). For a non-terminal configuration $C = w_1\,(q,b)\,w_2$ (i.e. such that $q \in Q_\exists \cup Q_\forall$), we denote by $succ_L(C)$ (resp. $succ_R(C)$) the successor of C obtained by choosing the left (resp. the right) triple in $\delta(q,b)$. An *accepting computation tree* of $\mathcal{M}$ over ε is a finite tree T whose nodes are labeled by configurations and such that the root is labeled by C_{init}, the leaves are labeled by accepting configurations C, i.e. $q(C) = q_{acc}$, each internal node x is labeled by a non-terminal configuration C, and: (1) if C is existential (i.e., $q(C) \in Q_\exists$), then x has exactly one child whose label is one of the two successors of C, and (2) if C is universal (i.e., $q(C) \in Q_\forall$), then x has exactly two children corresponding to the two successors $succ_L(C)$ and $succ_R(C)$ of C. We construct a game with opacity condition $A_{\mathcal{M}}$ such that Gerald has a winning strategy in $A_{\mathcal{M}}$ if, and only if, there is an accepting computation tree of $\mathcal{M}$ over ε (Theorem 6). Hence, EXPTIME-hardness of the opacity-guarantee problem follows.

In the game $A_{\mathcal{M}}$, the tape content can be retrieved from the current information set (of size n), and the remaining information about the current configuration is available in each position of the information set. A step of the machine is simulated by two rounds of the game: in the first round, depending on whether the current state is universal or existential, Robert simulates the universal choice of the next configuration or Gerald simulates the existential choice, and the second round simulates the updating of the configuration of the machine.
Here, we describe the construction of the game $A_{\mathcal{M}} = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0, S)$.

1. $V = \{v_0, safe_L, safe_R, safe_{choice}\} \cup \big(([n] \times B) \times ([n] \times Q \times B) \times \{L, R, choice\}\big)$.
2. $\mathrm{obs} : V \to \Gamma = \{\gamma_0, \gamma_{choice}, \gamma_L, \gamma_R\}$ is defined by

$$\mathrm{obs}(v) \;=\; \begin{cases} \gamma_0 & \text{if } v = v_0 \\ \gamma_L & \text{if } v \in \{safe_L\} \cup \big(([n] \times B) \times ([n] \times Q \times B) \times \{L\}\big) \\ \gamma_R & \text{if } v \in \{safe_R\} \cup \big(([n] \times B) \times ([n] \times Q \times B) \times \{R\}\big) \\ \gamma_{choice} & \text{otherwise.} \end{cases}$$

3. $\mathrm{act} : \Gamma \to \Sigma = \{\forall_L, \forall_R, \exists\} \cup B$ is defined by

$$\mathrm{act}(\gamma) \;=\; \begin{cases} \Sigma & \text{if } \gamma = \gamma_0 \\ \{\forall_L, \forall_R, \exists\} & \text{if } \gamma = \gamma_{choice} \\ B & \text{otherwise.} \end{cases}$$

4. $S = ([n] \times B) \times ([n] \times \{q_{rej}\} \times B) \times \{choice\}$.

We delay the formal definition of $\Delta : V \times \Sigma \to 2^V \setminus \emptyset$ after informally describing the running of the game.

A configuration C is encoded by an *information set* $I_f(C)$ of the form

$$\{((1,b_1),(i,q(C),b_i),f),\ldots,((n,b_n),(i,q(C),b_i),f)\}$$

where $f \in \{L,R,choice\}$, i is the position of the tape cell of C being scanned, and for each $1 \le j \le n$, b_j is the content of the j-th cell. For each $f \in \{L,R,choice\}$, $I_f(C)$ is called the f*-code* of C, and during a play, the current information set is of the form $I_f(C)$ for some reachable configuration C of the machine, unless Robert happened to have made some *deviating* move which does not simulate the dynamics of $\mathscr{M}$. We capture this deviation by making Robert lose: technically, the play enters one of the *safe* positions $safe_L, safe_R$, or $safe_{choice}$ that do not belong to the set S of secrets; then, once a safe position is reached, only other safe positions can be reached, yielding Gerald to win, whatever Robert does in the future. Note that for each $f \in \{L,R\}$, $I_f(C)$ does not violate the opacity condition for S, and $I_{choice}(C)$ violates the opacity condition for S if, and only if, C is rejecting (i.e. $q(C) = q_{rej}$). For all $q \in Q_\exists \cup Q_\forall$ and $b \in B$, we denote by $\delta_L(q,b)$ (resp. $\delta_R(q,b)$) the left (resp. right) triple in $\delta(q,b)$. The behavior of $A_{\mathscr{M}}$ is as follows:

First round: From the initial position v_0, whatever Robert and Gerald choose, the information set at the end of the first round is $I_{choice}(C_{init})$, the *choice*-code of the initial configuration.

The current information set is $I_{choice}(C)$ for some terminal configuration C: If C is rejecting, then $I_{choice}(C) \subseteq S$ and Gerald loses. Otherwise, $I_{choice}(C) \not\subseteq S$ and independently of the move of Robert, the play reaches a safe position $safe_{dir}$ for some $dir \in \{L,R\}$ and Gerald wins.

As we shall see, there remain only two cases, which in turn simulate a complete step of $\mathscr{M}$.

The current information set is $I_{choice}(C)$ for some non-terminal configuration C:
Let $v = ((k,b_k),(i,q(C),b_i),choice)$ be the current position (corresponding to some position in $I_{choice}(C)$). From obs(v), Robert can only choose actions in $\{\exists,\forall_L,\forall_R\}$. There are again two cases.

- *C is existential (note that this information is contained in the position v).* Moves $\forall_L$ and $\forall_R$ of Robert are deviating and the play reaches one of the safe positions $safe_L$ or $safe_R$, thus Gerald wins. If instead Robert's move is $\exists$, the following move $dir \in \{L,R\}$ of Gerald aims at simulating the existential choice of $\mathscr{M}$ in the configuration configuration C. The reached position is then $v' = ((k,b_k),(i,q(C),b_i),dir)$.
- *C is universal*. The move $\exists$ of Robert is deviating and the following move of Gerald can lead only to $safe_L$ or $safe_R$, which makes him win. Instead Robert's move $\forall_{dir} \in \{\forall_L,\forall_R\}$ simulates the universal choice of $\mathscr{M}$ in the configuration C. Next, Gerald's move is unique and leads to the position $v' = ((k,b_k),(i,q(C),b_i),dir)$.

Whatever the type of the configuration C was, by letting the observation classes split positions with different values of dir (see the definition of obs above), the information set after the move of Gerald becomes $I_{dir}(C)$, unless Robert's move was deviating.

The current information set is $I_{dir}(C)$ with $dir \in \{L,R\}$, for some non-terminal configuration C:
Let the current position be $v = ((k,b_k),(i,q(C),b_i),dir) \in I_{dir}(C)$, and let $\delta_{dir}(q(C),b_i) = (q_{dir},b_{dir},\theta_{dir})$. The value $j = i + \theta_{dir}$ represents the position of the cell being scanned in the next configuration $succ_{dir}(C)$; note that the value j is easily computable from the current position v. In order however to complete the step of the machine and to reach the information set $I_{choice}(succ_{dir}(C))$, the value of b_j must be provided by the game. Therefore, we let b_j be the only non-deviating move of Robert from position $v \in I_{dir}(C)$, among the possible moves in B.

From position $v = ((k, b_k), (i, q(C), b_i), dir)$, the above behavior is implemented as follows. Let b be the action chosen by Robert. If $k \notin \{i, j\}$, tape cell k is unchanged by the step of the machine, hence the only possible move of Gerald leads to $((k, b_k), (j, q_{dir}, b), choice)$. If $k = i$, tape cell i is overwritten, hence the move of Gerald is unique and leads to $((i, b_{dir}), (j, q_{dir}, b), choice)$. Finally, if $k = j$, there are two cases. If $b = b_j$, then Gerald can only move to $((j, b_j), (j, q_{dir}, b_j), choice)$ which updates the data for the next configuration $succ_{dir}(C)$, otherwise the move b ($\neq b_j$) of Robert is deviating (and the play reaches a safe position).

We can now formally define the moves in $A_{\mathscr{M}}$, by letting $\Delta : V \times \Sigma \to 2^V \setminus \emptyset$ be:

Case $v = v_0$**:**

$$\Delta(v, a) = \{((h, ␣), (1, q_0, ␣), choice) \mid h \in [n]\}$$

Case $v = safe_{choice}$**:**

$$\Delta(v, a) = \{safe_{dir} \mid dir \in \{L, R\}\}$$

Case $v = safe_{dir}$, where $dir \in \{L, R\}$:

$$\Delta(v, a) = \{safe_{choice}\}$$

Case $v = ((h, b), (i, q, b'), choice)$**:**

$$\Delta(v, a) = \begin{cases} \{((h, b), (i, q, b'), dir) \mid dir \in \{L, R\}\} & \text{if } a = \exists \text{ and } q \in Q_\exists \\ \{((h, b), (i, q, b'), L)\} & \text{if } a = \forall_L \text{ and } q \in Q_\forall \\ \{((h, b), (i, q, b'), R)\} & \text{if } a = \forall_R \text{ and } q \in Q_\forall \\ \{safe_{dir} \mid dir \in \{L, R\}\} & \text{otherwise} \end{cases}$$

Case $v = ((h, b), (i, q, b'), dir)$, where $dir \in \{L, R\}$, $q \notin \{q_{rej}, q_{acc}\}$, and $\delta_{dir}(q, b') = (q_{dir}, b_{dir}, \theta_{dir})$:

$$\Delta(v, a) = \begin{cases} \{((h, b), (i + \theta_{dir}, q_{dir}, a), choice)\} & \text{if } a \in B \text{ and } h \notin \{i, i + \theta_{dir}\} \\ \{((h, b_{dir}), (i + \theta_{dir}, q_{dir}, a), choice)\} & \text{if } a \in B \text{ and } h = i \\ \{((h, b), (i + \theta_{dir}, q_{dir}, b), choice)\} & \text{if } a = b \text{ and } h = i + \theta_{dir} \\ \{safe_{choice}\} & \text{otherwise} \end{cases}$$

Case $v = ((h, b), (i, q, b'), dir)$, where $dir \in \{L, R\}$ and $q \in \{q_{rej}, q_{acc}\}$:

$$\Delta(v, a) = \{((h, b), (i, q, b'), choice)\}$$

This achieves the construction of the game $A_{\mathscr{M}}$ which satisfies the following result:

Theorem 6 **[2]** *There is an accepting computation tree of $\mathscr{M}$ over ε if, and only if, there is a winning strategy of Gerald in the game $A_{\mathscr{M}}$.*

4 Blindfold games with opacity condition

We recall that a game with imperfect information is *blindfold* if all positions have the same observation.

Lemma 7 *Let $A = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0)$ be a blindfold game with imperfect information over Σ and $\Gamma = \{\gamma\}$. For every play prefix $\rho^n = v_0 a_1 v_1 \ldots a_n v_n$, $I(\rho^n) = \Delta(\{v_0\}, a_1 \ldots a_n)$.*

The proof is trivial, by applying the definition of the information set.

In blindfold games Robert cannot base the choice of his actions on anything because he sees nothing of what Gerald does. So a strategy for Robert is just an infinite sequence of actions. More formally:

Lemma 8 *Let $A = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0)$ be a blindfold game with imperfect information over Σ and $\Gamma = \{\gamma\}$, let α be a strategy for Robert, then there exists $a_1 a_2 a_3 \ldots \in \Sigma^\omega$ such that for all strategies β and β' for Gerald,* $\mathrm{obs}(\alpha\widehat{\ }\beta) = \mathrm{obs}(\alpha\widehat{\ }\beta') = v_0 a_1 \gamma a_2 \gamma \ldots$

In the rest of this section we prove the following two theorems:

Theorem 9 *Blindfold games with opacity condition are determined.*

Theorem 10 *For blindfold games with opacity condition, the opacity-guarantee problem and the opacity-violate problem are* PSPACE*-complete.*

Both theorems are proved by considering a third problem: the *opacity-verify problem* which addresses the strong ability for Gerald to win the game. We define this problem and establish its PSPACE-completeness in the general setting of games with opacity condition and also in the particular case of blindfold games (Theorem 11). We finally compare it to the opacity-violate and opacity-guarantee problems for blindfold games (Theorem 14).

Definition 5 *Given a game with opacity condition $A = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0, S)$, the* opacity-verify problem *is to decide whether the following property holds:*

$$\forall \beta, \forall \alpha,\ \alpha\widehat{\ }\beta \text{ is } S\text{-opaque} \tag{1}$$

If Property (1) holds, any strategy β of Gerald is a winning-strategy. Otherwise, there exists a play in the game that is not S-opaque.

Theorem 11 *The opacity-verify problem is* PSPACE*-complete, even for blindfold games.*

For the PSPACE membership, we design an algorithm that decides whether there exists a losing play for Gerald, which is clearly equivalent to deciding whether there exists a strategy of Gerald that is not winning. The algorithm runs in NPSPACE, hence in PSPACE [18], by nondeterministically choosing the moves for Robert and Gerald, and by updating the current information set of Robert at each round. Since information sets are subsets of the set of positions, if there are n positions, we need $O(n)$ space to run this algorithm. The PSPACE-hardness of the opacity-verify problem results from a reduction from the universality problem for a complete nondeterministic finite automaton (NFA), known to be PSPACE-complete [19]. This reduction was initially inspired by [7] but is in fact a variant of the one in [6].

We recall that a NFA $\mathscr{A} = (Q, \Sigma, \Delta, Q_0, Q_f)$ is a nondeterministic finite automaton with states Q, alphabet Σ, transition relation $\Delta : Q \times \Sigma \to 2^Q$ and sets of (respectively) initial and accepting states Q_0 and Q_f. A NFA $\mathscr{A}$ is complete if for every state q and letter a, $\Delta(q,a) \neq \emptyset$. The *language* $\mathscr{L}(\mathscr{A}) \subseteq \Sigma^*$ of $\mathscr{A}$ is the set of words $w \in \Sigma^*$ such that $\Delta(Q_0, w) \cap Q_f \neq \emptyset$. The universality problem is to decide whether $\mathscr{A}$ accepts all possible finite words, *i.e* $\mathscr{L}(\mathscr{A}) = \Sigma^*$.

Given a complete NFA $\mathscr{A} = (Q, \Sigma, \Delta, Q_0, Q_f)$, define the blindfold game with opacity condition $A_{\mathscr{A}} = (Q \cup \{q_0\}, \Delta', \mathrm{obs}, \mathrm{act}, q_0, S)$ over Σ and $\Gamma = \{\gamma\}$, with $q_0 \notin Q$, as follows:

$$S = Q \backslash (Q_f \cup \{q_0\}) \qquad \mathrm{act}(\gamma) = \Sigma \qquad \forall q \in Q \cup \{q_0\}, \mathrm{obs}(q) = \gamma$$

$$\forall a \in \Sigma, \Delta'(q,a) = \begin{cases} Q_0 & \text{if } q = q_0 \\ \Delta(q,a) & \text{otherwise} \end{cases}$$

Since, firstly, q_0 is not reachable after the first move, secondly, $\Delta'(q,a) = \Delta(q,a)$ for $q \neq q_0$ and finally, $\Delta'(q_0,a) = Q_0$ for all a, we obtain from lemma 7 the following corollary :

Corollary 12 *For each play prefix in $A_{\mathscr{A}}$ of the form $\rho^n = q_0 a_1 \dots a_n q_n$ ($n \geq 1$), $I(\rho^n) = \Delta(Q_0, a_2 \dots a_n)$.*

One may note that the aim of the initial position q_0 is to initialise Robert's information set to Q_0 at the end of the first round.

Proposition 13 *The NFA $\mathscr{A}$ is universal if, and only if, in $A_{\mathscr{A}}$, every strategy of Gerald is winning.*

Proof We start with the right-left implication. Assume that every strategy is winning for Gerald. Take one strategy β, and take a word $w \in \Sigma^*$. Consider a play ρ in which Robert's first moves form the sequence of actions aw, for some a in Σ, and Gerald follows strategy β. This is possible because the underlying automaton is complete. Being ρ induced by the winning strategy β, it is S-opaque, hence in particular $I(\rho^{1+|w|}) \nsubseteq S$. By Corollary 12 we obtain : $\Delta(Q_0,w) \nsubseteq S$, which implies that there exists a position q in $\Delta(Q_0,w)$ that is in Q_f, hence $\mathscr{A}$ accepts w. $\mathscr{A}$ is universal.

For the other implication, suppose that $\mathscr{A}$ is universal. Let β be a strategy of Gerald, and let ρ be a play induced by β. We prove that ρ is S-opaque. Let $n \in \mathbb{N}$. If $n = 0$, $I(\rho^n) = \{q_0\} \nsubseteq S$. If $n > 0$, there exists w in Σ^* such that $I(\rho^n) = \Delta(Q_0,w)$ (Corollary 12). Since $\mathscr{A}$ is universal it accepts w, hence $\Delta(Q_0,w) \cap Q_f \neq \emptyset$. So $I(\rho^n) \nsubseteq S$, and this finishes the proof. □

Theorem 14 *In the setting of blindfold games with opacity condition, the opacity-verify problem, the opacity-guarantee problem and the complementary of the opacity-violate problem are equivalent.*

Proof Let $A = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0, S)$ be a blindfold game with opacity condition. It is clear that in general,

$$\forall \beta, \forall \alpha,\ \alpha\widehat{\ }\beta \text{ is } S\text{-opaque} \Rightarrow \exists \beta, \forall \alpha,\ \alpha\widehat{\ }\beta \text{ is } S\text{-opaque}$$

We prove the converse in the case of blindfold games. Suppose that there exists a winning strategy β for Gerald. We prove that any strategy β' is also winning.

Let α be a strategy for Robert. Since A is blindfold, by Lemma 8 we have that $\mathrm{obs}(\alpha\widehat{\ }\beta) = \mathrm{obs}(\alpha\widehat{\ }\beta')$, so for every $n \in \mathbb{N}$, $I(\alpha\widehat{\ }\beta'^{\,n}) = I(\alpha\widehat{\ }\beta^n) \nsubseteq S$.

So we have that the opacity-verify problem is equivalent to the opacity-guarantee problem in blindfold games. We now show that the opacity-verify problem is also equivalent to the complementary of the opacity-violate problem (decide whether $\forall \alpha, \exists \beta$ s.t. $\alpha\widehat{\ }\beta$ is S-opaque holds).

Once again one implication is trivial :

$$\forall \beta, \forall \alpha,\ \alpha\widehat{\ }\beta \text{ is } S\text{-opaque} \Rightarrow \forall \alpha, \exists \beta,\ \alpha\widehat{\ }\beta \text{ is } S\text{-opaque}$$

Now the other way. Suppose that for any strategy α there is a strategy β for Gerald such that α loses. Now take any couple of strategies (α, β'). We know that there exists a strategy β such that $\alpha\widehat{\ }\beta$ is S-opaque. But we also know (Lemma 8) that $\mathrm{obs}(\alpha\widehat{\ }\beta) = \mathrm{obs}(\alpha\widehat{\ }\beta')$ because the game is blindfold, so once again for every $n \in \mathbb{N}$, $I(\alpha\widehat{\ }\beta'^n) = I(\alpha\widehat{\ }\beta^n) \nsubseteq S$. □

The idea behind this theorem is that in blindfold games with opacity condition, the outcome of a play does not rely on Gerald's behaviour but only on what Robert plays. Indeed, since he observes nothing of what Gerald does, Robert's information set, and so the winning condition, are only determined by the series of actions he chooses. Thus, these games via a power-set construction can be seen as (reachability) one-player games: each position is a reachable information set I, at each step the unique player (Robert) chooses an action $a \in act(I)$, where I is the current position, and moves to position $\Delta(I,a)$. Therefore, in blindfold games with opacity condition, whether Robert has a winning strategy (*i.e* a winning sequence of actions), or Gerald wins whatever he does.

The determinacy of blindfold games with opacity condition (Theorem 9) is an immediate corollary of the above Theorem 14. Also Theorem 10 results from Theorems 14 and 11.

5 Related work

Opacity has mostly been studied in the framework of discrete-event systems and their theory of control ([17, 8]). It is both interesting and important to know to what extent the classical problems in this field can be embedded into our games. We first describe the discrete-event system setting, next we define the notion of opacity in this framework. We finally propose a translation from the verification of opacity in this setting to the opacity-verify problem in games with opacity condition.

First we recall that a *a deterministic finite automaton (DFA)* is a NFA $\mathscr{A} = (Q, \Sigma, \delta, q_0, Q_f)$ but with a unique initial state q_0 and in which the transition relation $\delta : Q \times \Sigma \to 2^Q$ satisfies $|\delta(q,a)| \leq 1$ for all states q and input symbols a.

The problem of opacity is defined in [8] with regards to a LTS G (labelled transition system, *i.e* a DFA without accepting states) and a confidential predicate ϕ over execution traces of G, representable by a regular language $\mathscr{L}_\phi \subseteq \Sigma^*$ where Σ is the set of events of the transition system. For convenience, we equivalently state it on a DFA $\mathscr{A}_G^\phi$ representing the transition system together with the secret predicate. The automaton $\mathscr{A}_G^\phi$ is simply the synchronized product of G with some complete DFA accepting $\mathscr{L}_\phi$. We denote by $\mathscr{T}(\mathscr{A}) \subseteq \Sigma^*$ the set of execution traces of an automaton $\mathscr{A}$, and by $\mathscr{L}(\mathscr{A})$ the language accepted by $\mathscr{A}$, so we have that $\mathscr{T}(\mathscr{A}_G^\phi) = \mathscr{T}(G)$ and $\mathscr{L}(\mathscr{A}_G^\phi) = \mathscr{T}(G) \cap \mathscr{L}_\phi$. From now on, for a DFA $\mathscr{A}$, a state q and $w \in \mathscr{T}(\mathscr{A})$, $\delta(q,w)$ shall denote the only state it contains.

We consider a subset of events $\Sigma_a \subseteq \Sigma$ which denotes the observation capabilities of a potential attacker of the system, and we let P_{Σ_a} be the *projection* function from Σ^* to Σ_a^*. Two words w and w' are *observationally equivalent* if $P_{\Sigma_a}(w) = P_{\Sigma_a}(w')$. We denote by $[w]_a = P_{\Sigma_a}^{-1}(P_{\Sigma_a}(w))$ the set of words in Σ^* that are observationally equivalent to the word w with regard to Σ_a.

Definition 6 *$\mathscr{L}_\phi$ is* opaque *w.r.t. $\mathscr{T}(G)$ and Σ_a if*

$$\forall w \in \mathscr{T}(G), [w]_a \cap \mathscr{T}(G) \not\subseteq \mathscr{L}_\phi$$

This means that $\mathscr{L}_\phi$ is opaque w.r.t. $\mathscr{T}(G)$ and Σ_a if, and only if, whenever an execution trace of G verifies the confidential predicate ϕ there exists another possible execution trace observationally equivalent that does not verify ϕ.

We take an instance of the opacity verification problem, $\mathscr{A}_G^\phi = (Q, \Sigma, \delta, q_0^G, Q_f)$, and we describe the construction of the game with opacity condition A_G^ϕ such that the following holds.

Theorem 15 *Verifying that $\mathscr{L}_\phi$ is opaque w.r.t $\mathscr{T}(G)$ and Σ_a is equivalent to deciding the opacity-verify problem in A_G^ϕ.*

The construction starts from $\mathscr{A}_G^\phi$ where transitions labelled by events in $\Sigma \backslash \Sigma_a$ are turned into ε-transitions. Then we remove those ε-transitions as described in [11] by taking the ε-closure of the transition function, and we obtain the ε-free nondeterministic finite automaton $\mathscr{A}^\varepsilon = (Q, \Sigma_a, \Delta^\varepsilon, Q_0^\varepsilon, Q_f)$.

In this automaton, transitions are all labelled by observable events. One should think of the nondeterminism in this automaton as the uncertainty the attacker has concerning the behaviour of the system.

More precisely, she does not know when an observable event is triggered whether the system takes "invisible" transitions or not, may it be before, after, or both before and after the observable one.

We need the following lemma, which is a mere consequence of the construction :

Lemma 16
$$\forall w \in \Sigma_a^*, \Delta^\varepsilon(Q_0^\varepsilon, w) = \{\delta(q_0^G, w') \mid w' \in [w]_a \cap \mathscr{T}(G)\}$$

We can now define the game $A_G^\phi = (V, \Delta, \mathrm{obs}, \mathrm{act}, v_0, S)$ over $\Sigma' = \{\surd\}$ and $\Gamma = \{\gamma_x \mid x \in \Sigma_a\} \cup \{\gamma_\varepsilon\}$:

- $V = Q \times \Sigma_a \cup Q_0^\varepsilon \times \{\varepsilon\} \cup \{v_{init}\}$.
- $\Delta(v, \surd) = \begin{cases} \{(q', y) \mid y \in \Sigma_a, q' \in \Delta^\varepsilon(q, y)\} & \text{if } v = (q, x) \\ \{(q, \varepsilon) \mid q \in Q_0^\varepsilon\} & \text{if } v = v_{init} \end{cases}$
- $\forall (q, x) \in V,\ \mathrm{obs}((q, x)) = \gamma_x$, and $\mathrm{obs}(v_{init}) = \gamma_\varepsilon$
- $\forall v \in V,\ \mathrm{act}(v) = \{\surd\}$
- $S = \{(q_f, x) \mid q_f \in Q_f, x \in \Sigma_a \cup \{\varepsilon\}\}$ and $v_0 = v_{init}$

Remark 3 *Without loss of generality we can assume that in every state q of $\mathscr{A}^\varepsilon$ there exists an event y in Σ_a such that $\Delta^\varepsilon(q, y)$ is not empty. So in every position (q, x) in V, $\Delta((q, x), \surd)$ is not empty, and the game can always continue.*

In this game, Robert is passive. He only observes Gerald, who simulates the system G. If the game is in position (q, x), it represents that we are in state q in the system G, and that the last visible event was x (if $x = \varepsilon$, no observable event happened yet). Robert observes γ_x, *i.e* the only information he gains during a play is the sequence of visible events. When Gerald plays, he chooses a visible event y and a state reachable from q through y in $\mathscr{A}^\varepsilon$, which can be seen as choosing as many invisible transitions in G as he wishes, plus one visible amongst them, y. We shall note $\alpha_\surd$ the only possible strategy for Robert, which is to always play $\surd$.

v_{init} is the initial position, that can never be reached after the first move. It is used to initialize Robert's information set to $Q_0^\varepsilon \times \{\varepsilon\}$ (these are the only reachable positions from v_{init}, and they have the same observation, γ_ε). This represents the set of states in G that are reachable before any observable transition is taken.

We start the proof of Theorem 15 by establishing this central lemma.

Lemma 17 *Let $\rho^{n+1} = v_{init}\surd(q_0, \varepsilon)\surd(q_1, x_1)\dots\surd(q_n, x_n)$ be a prefix of a play, with $n \geq 0$. Then $\{q \mid (q, x_n) \in I(\rho^{n+1})\} = \Delta^\varepsilon(Q_0^\varepsilon, x_1 \dots x_n)$ and for all (q, x) in $I(\rho^{n+1})$, $x = x_n$.*

Proof The latter fact is obvious, from the definition of observations. Considering the former fact, we prove it by induction on n.

$n = 1$ **:** $I(\rho^1) = \Delta(\{v_{init}\}, \surd) \cap \gamma_\varepsilon = \{(q_0, \varepsilon) \mid q_0 \in Q_0^\varepsilon\}$, so $\{q \mid (q, \varepsilon) \in I(\rho^1)\} = Q_0^\varepsilon = \Delta^\varepsilon(Q_0^\varepsilon, \varepsilon)$

$n + 1$ **:**
$$\begin{aligned} \{q \mid (q, x_{n+1}) \in I(\rho^{n+2})\} &= \{q \mid (q, x_{n+1}) \in \Delta(I(\rho^{n+1}), \surd) \cap \mathrm{obs}((q_{n+1}, x_{n+1}))\} \\ &= \{q \mid (q, x_{n+1}) \in \Delta(I(\rho^{n+1}), \surd)\} \\ &= \{q \mid \exists (q', x_n) \in I(\rho^{n+1}), q \in \Delta^\varepsilon(q', x_{n+1})\} \\ &= \{q \mid \exists q' \in \Delta^\varepsilon(Q_0^\varepsilon, x_1 \dots x_n), q \in \Delta^\varepsilon(q', x_{n+1})\} \\ &= \Delta^\varepsilon(Q_0^\varepsilon, x_1 \dots x_{n+1}) \end{aligned}$$

□

We move on to the proof of Theorem 15. Suppose that every strategy β is winning for Gerald. We prove that $\mathscr{L}_\phi$ is opaque w.r.t $\mathscr{T}(G)$ and Σ_a. Take a word w in $\mathscr{T}(G)$. There exists a prefix of a play $\rho^{n+1} = v_{init}\surd(q_0,\varepsilon)\surd(q_1,x_1)\ldots\surd(q_n,x_n)$ such that $x_1\ldots x_n = P_{\Sigma_a}(w)$. So there exists a strategy β such that $\alpha\widehat{\surd}\beta^{n+1} = \rho^{n+1}$. With lemma 17 and 16 we have that $\{q \mid (q,x_n)\in I(\rho^{n+1})\} = \{\delta(q_0^G,w) \mid w \in [x_1\ldots x_n]_a \cap \mathscr{T}(G)\}$. Since β is winning, $\{q \mid (q,x_n)\in I(\rho^{n+1})\} \nsubseteq Q_f$, so there exists w' in $[x_1\ldots x_n]_a \cap \mathscr{T}(G) = [w]_a \cap \mathscr{T}(G)$ such that $\delta(q_0^G,w') \notin Q_f$. This implies that $[w]_a \cap \mathscr{T}(G) \nsubseteq \mathscr{L}_\phi$.

Now suppose that $\mathscr{L}_\phi$ is opaque w.r.t $\mathscr{T}(G)$ and take β a strategy for Gerald in A_G^ϕ, we prove that β is winning. Let $\rho_\beta = \alpha\widehat{\surd}\beta$ be the only possible play induced by β. Take a prefix $\rho_\beta^{n+1} = v_{init}\surd(q_0,\varepsilon)\surd(q_1,x_1)\ldots\surd(q_n,x_n)$ of this play. By Lemma 17 and 16 again, $\{q \mid (q,x_n)\in I(\rho_\beta^{n+1})\} = \{\delta(q_0^G,w) \mid w \in [x_1\ldots x_n]_a \cap \mathscr{T}(G)\}$. Since an information set is never empty, there exists w in $[x_1\ldots x_n]_a \cap \mathscr{T}(G)$, and because $\mathscr{L}_\phi$ is opaque w.r.t $\mathscr{T}(G)$, $[x_1\ldots x_n]_a \cap \mathscr{T}(G) \nsubseteq \mathscr{L}_\phi$. So there exists w' in $[x_1\ldots x_n]_a \cap \mathscr{T}(G)$ such that $\delta(q_0^G,w') = q \notin Q_f$, hence $(q,x_n)\notin S$ and $I(\rho_\beta^n) \nsubseteq S$. β is winning.

6 Discussion on complexity

Solving safety games with perfect-information is in PTIME, and solving parity games with perfect information is known to be in $NP \cap$co-NP [12]. However we have seen that deciding whether Gerald, who has perfect-information, has a winning strategy in a game with opacity condition, is EXPTIME-complete, even if we let Robert play with perfect-information (in the sense that his strategies are based on actual prefixes of plays instead of their observation). So the gap between deciding the existence of a winning strategy for a player in perfect-information games and for Gerald in a game with opacity condition does not come from the fact that Robert has imperfect information, but rather from the nature of the winning condition itself, which is based on the notion of information set, and forces Gerald to keep track of what Robert's information set along the game is.

Similarly, verifying that a finite-state strategy is winning in a safety perfect-information game can be done in PTIME, whereas we have shown in [2] that in games with opacity condition, deciding whether a finite-state (and even memoryless) strategy of Gerald is winning is PSPACE-complete in the size of the arena and the memory of the strategy (we define in a classic way the size of the memory of a strategy as the number of states of an I/O automaton realizing the strategy [9]). The idea is that one has to check that the strategy is winning not in all positions, but in all information sets. Concerning the size of the memory needed for Gerald's strategies, we know that an exponential memory is sufficient because if there is a winning strategy there is a memoryless one in the powerset construction. The lower bound for the needed memory is still an open problem.

7 Conclusion and perspectives

Following [14], we have extended the study of games with opacity condition. The opacity condition is an atypical winning condition in imperfect information arenas aiming at capturing security aspects of computer systems. Since games with opacity condition are not determined in general, two dual problems need being considered: the opacity-violate problem and the opacity-guarantee problem, focusing on the player who has imperfect information and on the player who has perfect information respectively. The latter problem is usually equivalent to solving the underlying perfect information game, which explains why it has never been considered; but the fact that our winning condition is based on information sets makes the problem relevant. For both problems, simple power-set constructions apply to convert such games into perfect information ones, that can be solved in polynomial time, hence their upper bound is EXPTIME. On the contrary, the matching EXPTIME lower bound for the opacity-guarantee problem, where the main player has perfect information, was unknown until now and relies on an elegant reduction from the empty input string acceptance problem for linearly-bounded alternating Turing machines. The key point is to encode configurations by information sets. The reduction and its correctness proof are very technical, but we could provide an intuitive informal description.

Finally, we focused on the particular case of blindfold games which offers specific results such as determinacy (Theorem 9) and PSPACE-complete complexities (Theorem 10). The main tool to obtain these results is the opacity-verify problem which addresses the question whether any strategy of Gerald is winning. The fact that blindfold games with opacity condition can be seen as one-player games makes this problem relevant and explains why it is equivalent to the opacity-guarantee problem and to the complement of the opacity-violate problem in the blindfold setting, as we established. We also proved that it is PSPACE-complete, by providing a PSPACE algorithm and a reduction from the nondeterministic finite automata universality problem. The opacity-verify problem is all the more interesting to consider that it naturally demonstrates how the paradigm of opacity condition embraces opacity issues investigated in the recent literature of Control Theory [17, 8].

Games with opacity condition open a novel field in the theoretical aspects of games with imperfect information by putting the emphasis on the player who has perfect information. From this point of view, plethora of questions need being addressed, among which their connection with language-theoretic issues (the synchronizing/directing word problem [3, 15, 4], controller synthesis to enforce the opacity of a language [8]), their logical foundations, and their algorithmic aspects.

Acknowledgements

We are very grateful to the reviewers for relevant comments and suggestions that significantly helped in highlighting the conceptual content of the paper.

References

[1] D. Berwanger & L. Doyen (2008): *On the power of imperfect information*. In: *Proc. of FSTTCS*. Citeseer, pp. 73–82. Available at `http://drops.dagstuhl.de/opus/volltexte/2008/1742`.

[2] Laura Bozzelli, Bastien Maubert & Sophie Pinchinat (2011): *Opacity Issues in Games with Imperfect Information*. Technical Report PI-1978, IRISA.

[3] Ján Černý (1964): *Poznámka k. homogénnym experimentom s konecnými automatmi*. *Mat. fyz. čas SAV* 14, pp. 208–215.

[4] Ján Černý, Alica Pirická & Blanka Rosenauerova (1971): *On directable automata*. *Kybernetica* 7, pp. 289–298.

[5] A.K. Chandra & L.J. Stockmeyer (1976): *Alternation*. In: *17th annual symposium on Foundations of Computer Science*. IEEE, pp. 98–108, doi:`10.1109/SFCS.1976.4`.

[6] M. De Wulf, L. Doyen, T. Henzinger & J.F. Raskin (2006): *Antichains: A new algorithm for checking universality of finite automata*. In: *Computer Aided Verification*. Springer, pp. 17–30.

[7] J. Dubreil (2009): *Monitoring and Supervisory Control for Opacity Properties*. Ph.D. thesis, Université de Rennes 1.

[8] J. Dubreil, P. Darondeau & H. Marchand (2008): *Opacity enforcing control synthesis*. In: *Discrete Event Systems, 2008. WODES 2008. 9th International Workshop on*. IEEE, pp. 28–35, doi:10.1109/WODES.2008.4605918.

[9] S. Dziembowski, M. Jurdzinski & I. Walukiewicz (1997): *How much memory is needed to win infinite games?* In: *Logic in Computer Science, 1997. LICS'97. Proceedings., 12th Annual IEEE Symposium on*. IEEE, pp. 99–110, doi:10.1109/LICS.1997.614939.

[10] J.Y. Halpern & M.Y. Vardi (1989): *The complexity of reasoning about knowledge and time. I. Lower bounds*. *Journal of Computer and System Sciences* 38(1), pp. 195–237, doi:10.1145/12130.12161.

[11] J.E. Hopcroft, R. Motwani & J.D. Ullman (2006): *Automata theory, languages, and computation*. *International Edition* doi:10.1145/568438.568455.

[12] M. Jurdzinski (1998): *Deciding the winner in parity games is in UP [intersection] co-UP*. *Information Processing Letters* 68(3), pp. 119–124, doi:10.1016/S0020-0190(98)00150-1.

[13] D. Martin (1975): *Borel determinacy*. *Annales of Mathematics* 102, pp. 363–371, doi:10.2307/1971035.

[14] B. Maubert & S. Pinchinat (2009): *Games with Opacity Condition*. In: *Proceedings of the 3rd International Workshop on Reachability Problems*. Springer-Verlag, p. 175, doi:10.1007/978-3-642-04420-5_16.

[15] J.E. Pin (1983): *On two combinatorial problems arising from automata theory*. *Ann. Discrete Math* 17, pp. 535–548, doi:10.1016/S0304-0208(08)73432-7.

[16] J.H. Reif (1984): *The complexity of two-player games of incomplete information*. *Journal of computer and system sciences* 29(2), pp. 274–301, doi:10.1016/0022-0000(84)90034-5.

[17] A. Saboori & C.N. Hadjicostis (2008): *Opacity-Enforcing Supervisory Strategies for Secure Discrete Event Systems*. In: *IEEE Conference on Decision and Control (CDC)*. Cancun, Mexico, pp. 889–894, doi:10.1109/CDC.2008.4738646.

[18] Walter J. Savitch (1970): *Relationships between nondeterministic and deterministic tape complexities*. *J. Comput. System. Sci.* 4, pp. 177–192, doi:10.1016/S0022-0000(70)80006-X.

[19] L.J. Stockmeyer & A.R. Meyer (1973): *Word problems requiring exponential time (Preliminary Report)*. In: *Proceedings of the fifth annual ACM symposium on Theory of computing*. ACM, pp. 1–9, doi:10.1145/800125.804029.