Solving security models with perfect observability

Paolo Zappala, Amal Benhamiche, Matthieu Chardy, Francesco De Pellegrini, Rosa Figueiredo

Solving security models with perfect observability

Paolo Zappala[1,2], Amal Benhamiche[1], Matthieu Chardy[1], Francesco De Pellegrini[2], and Rosa Figueiredo[2]

[1] Orange Innovation, Orange, 44 Avenue de la République, Châtillon, 92320, France
{name.surname}@orange.com
[2] LIA, Avignon Université, 301 Rue Baruch de Spinoza, Avignon, 84140, France
{name.surname}@univ-avignon.fr

Abstract. Sequential models with perfect observability represent situations in which communication is public and observable by all the agents. Such models are applied within different domains of security, such as intrusion detection, blockchain protocols and wiretap channels. The extensive-form game is the representation used to identify the solution of these models. To date, the literature provides methods to identify specific solutions for small-size extensive-form games. We provide the first method to identify all solutions that is also scalable with the size of the games.

Keywords: Security models · Extensive-form games · Perfect observability.

1 Introduction

In this work we consider security models whose main assumption is perfect observability. In this context, the agents involved can observe each other's actions and react accordingly. Let us provide some examples of applications:

- an *intruder attack* [2]; when a user attacks a target system, she performs some actions that are observed by the latter. The back-and-forth of inputs and outputs provided by the user and the system can be represented by a model with perfect observability;
- a *blockchain protocol* [11]; one of the main features of blockchain is that all valid actions must be observable by all the nodes; thus any attack to a blockchain protocol can be modeled within a framework of perfect observability;
- a *wiretap channel* [5]; when a malicious user tries and intercepts a communication, she has perfect observation of the actions of the two agents involved in the broadcast;
- an *ephemeral network* [7]; in ephemeral networks the local revocation of a malicious node is determined with a vote in sequence;
- an *attack-defense tree* [3]; this category of models describes security weaknesses of a system and the possible countermeasures.

Extensive-form games. The common representation of models with perfect observability is the *extensive-form game with perfect information* [4]. In a game, a finite set of agents, called *players*, observe in turns each other's actions and pick one of the possible subsequent actions available to them. Every player picks a *strategy*, i.e., she selects an action whenever it is due during the game. The standard solution concept is the *Nash equilibrium* (NE) [6], i.e., a combination of strategies such that no player has an incentive to change their own unilaterally. The number of strategies grows exponentially in the size of the extensive form game [12], which makes brute-force algorithms not viable in large games. Every game admits at least one specific NE, called *subgame perfect equilibrium* (SPE) [8]. Since this specific equilibrium can be computed recursively with the backward induction algorithm, it is often used as the solution of reference of the game (cf., e.g., [7]).

Actually, the choice to limit the set of solutions to the SPE is forced by the absence of practical methods to compute the other Nash equilibria, and it is not supported by further assumptions. In ephemeral networks, the local revocation is assumed to be modeled according to the SPE, even if it is understood that there are possibly many other outcomes [7]. In blockchain protocols, only the Nash equilibria with given properties are selected [11], but no method is provided to compute them in large instances.

Contribution. In this work, we provide a method to enumerate all the Nash equilibria of an extensive-form game. To our knowledge, it is the first of its kind that can be applied to any game, no matter what is its structure or its utility function. Moreover, differently from the backward induction, that provides the SPE, our method does not have a recursive structure and it can be parallelized. This allows it to be deployed also in large games. In Section 2 we introduce extensive-form games and Nash equilibria. In Section 3 we provide a more compact definition of the games and show the method for the enumeration of the Nash equilibria. In Section 4 we prove that the method does identify the Nash equilibria. Section 5 ends the paper with perspective on further applications.

2 Extensive-form games

In this section we provide the definitions for extensive-form games with perfect information [1]. In order to express the observability of the actions, we consider extensive-form games in finite number of stages, that are set in chronological order. At every stage there exists a designated player $i \in \mathcal{I}$ who observes a *history* h', i.e., the sequence of actions occurring up to that stage. We denote by $\mathcal{I}$ the set of players of the game. At a give stage, the designated player has available a set of actions $\mathcal{A}(h')$. We denote by $P(h')$ the designated player observing the history h'. When the set of available actions is empty ($\mathcal{A}(h') = \emptyset$) the game ends, i.e., the sequence of actions leading to this stage h' corresponds to an *outcome* of the game. We call H' the set of histories and $H \subset H'$ the set of the outcomes. Every outcome is evaluated by every player $i \in \mathcal{I}$ through a function, called *utility function*, $u_i : H \to \mathbb{R}$. We also write $h_A \succ_i h_B$ for $h_A, h_B \in H$

when $u_i(h_A) > u_i(h_B)$, or $h_A \sim_i h_B$ when $u_i(h_A) = u_i(h_B)$. Let us denote by $h' + h'' = (a_1, a_2, \ldots, a_{m'}, b_1, b_2, \ldots, b_{m''})$ the concatenation of two vectors of actions $h' = (a_1, a_2, \ldots, a_{m'})$ and $h'' = (b_1, b_2, \ldots, b_{m''})$. We also denote by $h''' = h' \cap h''$ the lowest common prefix of the two vectors of actions h' and h'', shortly referred as *prefix* in the following. The full definition of extensive-form game is therefore:

Definition 1 (extensive-form game). *An extensive-form game is a tuple* $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$*, where:*

- $\mathcal{I} = \{1, \ldots, N\}$ *is the set of players;*
- H' *is the set of histories with* $\emptyset \in H'$*;*
- $\mathcal{A} : h' \in H' \to A$ *is a function that provides for every history a set of actions* A*, i.e., for all* $a \in A$*, we have* $h' + (a) \in H'$*;*
- $H = \{h \in H' | \mathcal{A}(h) = \emptyset\} \subset H'$ *is the set of outcomes;*
- $P : H' \setminus H \to \mathcal{I}$ *is a function that indicates which player* $P(h') \in \mathcal{I}$ *acts after observing the history* $h' \in H' \setminus H$*;*
- $u = (u_i)_{i \in \mathcal{I}}$*, with* $u_i : H \to \mathbb{R}$ *the utility function of player* $i \in \mathcal{I}$*.*

Remark. Since in the literature the representation of the game is the game-tree of possible histories, it is customary to call a *node* a history observed by a player. Analogously, we alternatively call an outcome the final node (or *leaf*) and the vector of actions leading to it.

Every agent has a strategy for every scenario she may have to face. Formally, a strategy is a function that maps every history observed by a player to an action.

Definition 2 (strategy). *Given a game* $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$ *and a player* $i \in \mathcal{I}$*, let* $H'_{P=i} = \{h' \in H' \setminus H | P(h) = i\}$ *be the histories at which the player* i *acts. A strategy* $s_i \in S_i$ *is a function* $s_i : h' \in H'_{P=i} \mapsto a \in \mathcal{A}(h')$ *that maps every observed history* $h' \in H'_{P=i}$ *to one of the actions* $a \in \mathcal{A}(h')$ *available to the player.*

We call *strategy profile* a N-tuple of strategies $s = \langle s_1, s_2, \ldots, s_N \rangle$, one for each player. We denote by $S = S_1 \times S_2 \times \cdots \times S_N$ the set of all strategy profiles. If every player chooses a strategy, one single action is picked at every history; therefore, given a strategy profile, the actions chosen by the players lead to a single outcome. We denote by $s \mapsto h$ the outcome $h \in H$ of a strategy profile $s \in S$. When a player picks a strategy, she limits the set of possible outcomes. We define such specific set in Definition 3.

Definition 3 (outcomes of a strategy). *Given a game* $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$ *and a strategy* $s_i \in S_i$ *of a player* $i \in \mathcal{I}$*, the set of outcomes* $H(s_i) \subset H$ *of strategy* s_i *is*

$$H(s_i) = \{h \in H | \exists s' \in S, s'_i = s_i, s' \mapsto h\}.$$

We also write $H(\langle s_j \rangle_{j \in J}) := \cap_{j \in J} H(s_j)$ to indicate the possible outcomes of a vector of strategies $\langle s_j \rangle_{j \in J}$ for some players $J \subset \mathcal{I}$. We write $\langle s_j \rangle_{j \in J} = s_{-i}$

ALGORITHM 1: Backward induction (BI)

Input: A game $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$ and its root $h^0 = \emptyset \in H'$.
Output: The set of subgame perfect equilibria SPE.
if $|H| = 1$ **then**
  $SPE = H$;
else
  $i = P(h^0)$; // The player acting at the root
  $\langle \Gamma^k, SPE^k, h'_k \rangle_{a_k \in \mathcal{A}(h^0)} \leftarrow \emptyset$;
  for $a_k \in \mathcal{A}(h^0)$ **do**
    $\Gamma^k = \Gamma(h^0 + (a_k))$; // The subgame that follows actions a_k
    $SPE^k = BI(\Gamma^k)$;
    $h'_k \in \arg\min_{h' \in SPE^k} u_i(h')$; // The lowest utility u_i a SPE can achieve in Γ^k
  end
  $SPE = \{h \in \cup SPE^k | \forall k, h \succeq_i h'_k\}$; // Outcome h is preferred by player i to any other SPE
end

when $J = \mathcal{I} \setminus \{i\}$. Clearly for a strategy profile $s \in S$ the set $H(s) = \{h\}$ is a singleton. Furthermore, with some abuse of notation, let $u_i(s) := u_i(s \mapsto h)$ denote the utility of player i under a certain strategy profile s. A strategy profile is a Nash equilibrium if no player can increase her utility by changing unilaterally her strategy.

Definition 4 (Nash equilibrium). *Given a game $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$, a strategy profile $\langle \overline{s}_i \rangle_{i \in \mathcal{I}}$ is a Nash equilibrium if for every $i \in \mathcal{I}$ and for all $s_i \in S_i$ it holds $u_i(\overline{s}_i, \overline{s}_{-i}) \geq u_i(s_i, \overline{s}_{-i})$.*

One method to identify all Nash equilibria is to list all the strategies and verify the condition of Definition 4. However, the number of strategies is often exponential in the number of outcomes [12]. Therefore, when the game is large and has a significant amount of outcomes, brute force is nowhere used as a method to identify the Nash equilibria.

The most known algorithm to identify Nash equilibria in extensive-form games is the backward induction (BI, cf. Algorithm 1). However, the backward induction algorithm provides only a specific subset of Nash equilibria, i.e., the *subgame perfect equilibria* (SPE). A subgame perfect equilibrium is a Nash equilibrium for every *subgame* [8], i.e., the part of the tree having one of the node of the game as root. Every extensive-form game with perfect recall and perfect information admits a subgame perfect equilibrium. The backward induction selects, starting from the leaves of the tree, the outcomes that are most favourite by the player acting at a given node. The value of the corresponding outcomes thus propagates upwards towards the root of the tree as exemplified next.

Example. Let us consider the game Γ represented by tree of Fig. 1a. The preferences of the players w.r.t. the outcomes are indicated in the caption. Let

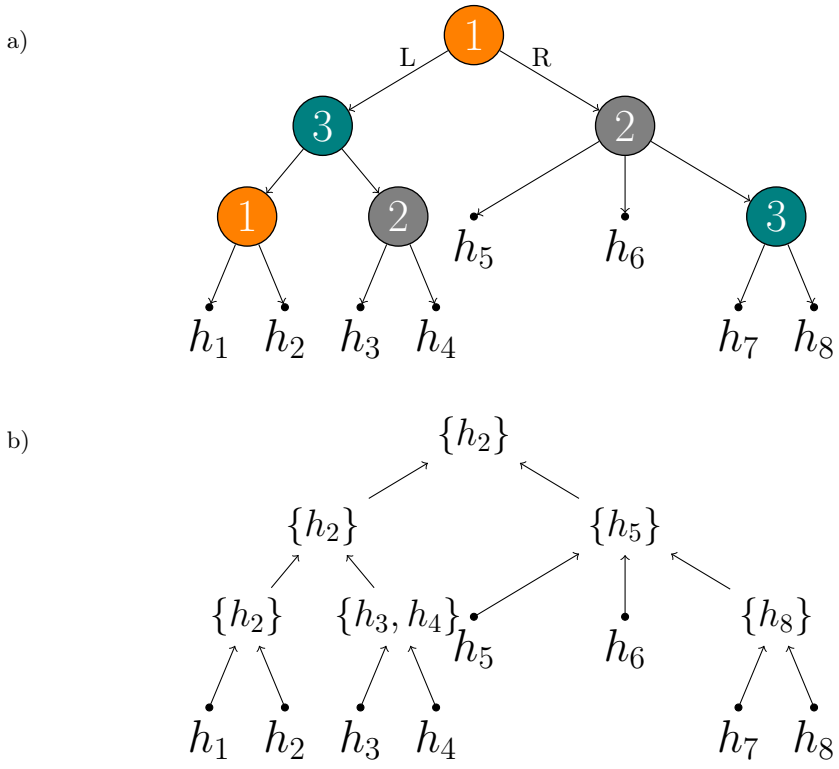

Fig. 1. Example. a) 3-player game in extensive form. Preferences of the players over the outcomes are respectively: $u_1 : h_6 \succ_1 h_7 \succ_1 h_8 \succ_1 h_3 \succ_1 h_4 \succ_1 h_2 \succ_1 h_1 \succ_1 h_5$, $u_2 : h_5 \succ_2 h_8 \succ_2 h_7 \succ_2 h_6 \succ_2 h_2 \succ_2 h_3 \sim_2 h_4 \succ_2 h_1$ and $u_3 : h_8 \succ_3 h_7 \succ_3 h_6 \succ_3 h_2 \succ_3 h_5 \succ_3 h_3 \succ_3 h_1 \succ_3 h_4$. b) Application of the backward induction to the game. The subgame perfect equilibrium of the game is h_2.

us compute the subgame perfect equilibria of the game by applying the BI algorithm. The computation are shown in Fig. 1b. The algorithm starts from the leaves of the tree. Player 1 prefers h_2 to h_1 ($h_2 \succ_1 h_1$), player 2 has no strict preference between h_3 and h_4 ($h_3 \sim_2 h_4$) and player 3 prefers h_8 to h_7 ($h_8 \succ_3 h_7$). The outcomes h_2, $\{h_3, h_4\}$ and h_8 are the SPE of the respective subgames. At the second stage of the tree, players 3 and 2 prefer respectively h_2 to h_3 and h_4 ($h_2 \succ_3 h_3 \sim_3 h_4$), h_5 to h_6 and h_8 ($h_5 \succ_2 h_8 \succ_2 h_6$). Finally, at the root of the tree, player 1 prefers h_2 to h_5 ($h_2 \succ_1 h_5$). The (here unique) subgame perfect equilibrium of the game is h_2.

Subgame perfect equilibria have two drawbacks. On one side, they do not always represent the Nash equilibrium that most fits a real-case scenario [9]. On the other side, they can only be identified by a recursive algorithm which is not practical when the game is too large.

Outcomes of Nash equilibria. The method presented hereafter let us identify the outcomes of all Nash equilibria. Let us consider a strategy profile $s \in S$. We recall that its realisation is the only element $h \in H$ belonging to the set of its possible outcomes $H(s)$. For any strategy profile originated by a unilateral deviation $s' \in S$ it must hold $s'_i \neq s_i$ and $s'_{-i} = s_{-i}$ for one and only one $i \in \mathcal{I}$. Therefore the realisation of any possible unilateral deviation, namely $h' \in H$, belongs to the set of possible outcomes $H(s_{-i})$ of the strategies $s_{-i} \in S_{-i} = \times_{j \in \mathcal{I} \setminus \{i\}} S_j$ of all players but the one deviating $i \in \mathcal{I}$. Formally, the realisation of a Nash equilibrium over the sets of outcomes is characterized by the following

Lemma 1. *Given a game $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$, an outcome $h \in H$ is a realisation of a Nash equilibrium if and only if there exists a strategy profile $s \in S$ such that $H(s) = \{h\}$ and for each $i \in \mathcal{I}$ and $h' \in H(s_{-i})$ it holds $u_i(h) \geq u_i(h')$.*

Proof. The direct implication is obvious. For the converse let us consider the strategy profile $s \in S$ whose existence is assumed in the statement. Observe that

$$H(s_{-i}) \setminus \{h\} = \{h' \in H | \exists s'_i \in S_i, s = \langle s_i, s_{-i} \rangle \mapsto h', h' \neq h\}$$

is the set of the outcomes of the strategy profiles of type s' where $s' = \langle s'_i, s_{-i} \rangle$, $s'_i \neq s_i$, i.e., of strategy profiles which are unilateral deviations from s. Hence, for any such strategy profile it holds $u_i(s'_i, s_{-i}) = u_i(h') \leq u_i(h) = u_i(s_i, s_{-i})$. □

3 Method to identify Nash equilibria

In this section we provide a graph-based method to identify all Nash equilibria. We focus on a target outcome $h \in H$ and we discuss whether it is the realisation of a Nash equilibrium or not. Since the target h can be chosen among all the outcomes of the game, without exceptions, it is possible to identify all the equilibria of the game. We need first to introduce some mathematical tools to analyse extensive-form games and then we use them to introduce the new algorithm. Section 4 will be devoted to the proof that the algorithm provides positive answer if and only if h is the realisation of a Nash equilibrium.

One of the features of extensive-form games with perfect information is that, given two outcomes, there is only one player who can determine which of the two can be selected. For instance, in the game of Fig. 1 it is player 1 who determines whether h_3 or h_6 is attained. Indeed, if player 1 selects action L at the root, h_6 cannot be reached. On the other hand, if player 1 chooses action R, h_3 will not be reached. Since the Nash equilibrium relies on the concept of unilateral deviation, we mark this definition:

$$I : H \times H \to \mathcal{I} \text{ where } I(h, h') = P(h \cap h').$$

The function $I : H \times H \to \mathcal{I}$ maps the pair of outcomes $h, h' \in H$ with $h \neq h'$ to the player $I(h, h')$ that separates their paths from the root of the game tree. We recall that $h \cap h'$ is the node that separates the paths from the root to respectively h and h'. In the example, $I(h_3, h_6) = 1$.

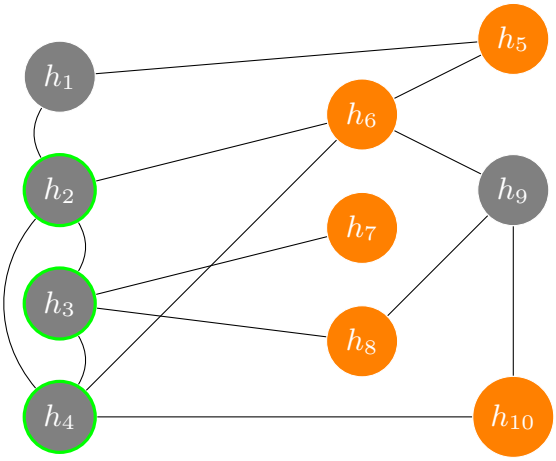

Fig. 2. Problem of the maximal excluding clique $[MC]$. Let us consider problem $[MC]$ with $H = \{h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, h_9, h_{10}\}$ and $X = \{h_5, h_6, h_7, h_8, h_{10}\}$. A vertex set that induces a maximal clique and solves $[MC]$ is $\mathcal{C} = \{h_2, h_3, h_4\}$.

The second definition to be introduced comes from graph theory [11]. The problem of the maximal excluding clique requires to identify a maximal excluding clique on a subset of vertices of the graph. We recall that a maximal clique is a clique that is not a subset of any another clique.

Problem 1. **[MC] Existence of a maximal clique excluding a set of vertices**
Input. $\langle H, E, X\rangle$ defining a graph $\langle H, E\rangle$ and a subset of vertices $X \subset H$.
Output. Is there a vertex set $C \subset H \setminus X$ that induces a maximal clique on $\langle H, E\rangle$?

Example. Let us consider the graph of Fig. 2. The set of vertices is $H = \{h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, h_9, h_{10}\}$. The set of vertices to be excluded is $X = \{h_5, h_6, h_7, h_8, h_{10}\}$. The problem of the maximal excluding clique require to determine if there exists a maximal clique in $H \setminus X$. A set of vertices that solves $[MC]$ is $\mathcal{C} = \{h_2, h_3, h_4\}$, because they induce a maximal clique on the graph.

Provided the aforementioned definitions, we can thus introduce Algorithm 2 to determine whether a target outcome is a Nash equilibrium.

Having fixed the target outcome $h \in H$, Algorithm 2 partitiones the remaining outcomes $h' \in H \setminus \{h\}$ according to the player $I(h, h')$ that separates the path from the root to them. We can thus define define the *set of potential deviations* of a given player $i \in \mathcal{I}$ from h

$$H_i = \{h' \in H \setminus \{h\} | i = I(h, h')\}.$$

Example. Let us fix the target outcome $h = h_3$ in Fig. 1. The set of potential deviations are respectively $H_1 = \{h_5, h_6, h_7, h_8\}$, $H_2 = \{h_4\}$ and $H_3 = \{h_1, h_2\}$.

ALGORITHM 2: (NE) Determining whether an outcome is a realisation of a Nash equilibrium

Input: A game Γ, the set of its outcomes H, the function $I : H \times H \to \mathcal{I}$ and an outcome $h \in H$.
Output: Is h a realisation of a Nash equilibrium?
$boolean = True$; `// A boolean value determining whether` h `is a realisation of a NE`
for $i \in \mathcal{I}$ **do**
  $H_i \leftarrow \{h' \in H \setminus \{h\} | I(h, h') = i\}$;
  $X_i \leftarrow \{h' \in H_i | u_i(h) < u_i(h')\}$;
  $E|_{H_i} = \{(h, h') \in H_i | I(h, h') = i\}$;
  if *Output of Problem 1 with input* $\langle H_i, X_i, E|_{H_i}\rangle$ *is negative* **then**
    $boolean = False$;
  end
end

If there is a unilateral deviation of a player $i \in \mathcal{I}$, it reaches an outcome belonging to the set H_i. Whether the player i has an incentive to deviate to an element $h' \in H_i$, it depends exclusively on the value of the utility $u_i(h')$. Indeed, if $u_i(h) < u_i(h')$, player i has an incentive to deviate from h to h', otherwise it does not. The set of potential deviations for which player i has an incentive to deviate is thus

$$X_i = \{h' \in H_i | u_i(h) < u_i(h')\}.$$

Example. Given $h = h_3$ the target outcome of the game of Fig. 1. The sets of outcomes for which a player has an incentive to deviate are respectively $X_1 = \{h_6, h_7, h_8\}$, $X_2 = \emptyset$ and $X_3 = \{h_2\}$.

The sets H_i are *potential* deviations, i.e., player i can *possibly* deviate to one of the outcomes belonging to H_i. However, player i can reach an outcome $h' \in H_i$ only if the other players have a multistrategy that leads to h'. If none of the outcomes reachable for player i do not belong to X_i, then she does not have any incentive to deviate to them. For instance, in the game of Fig. 1 player 1 can unilaterally deviate from h_3 to h_8 if both player 2 and 3 go right.

We devote Section 4 to the construction of such multistrategies. We later show that all the outcomes reachable for a player i must have the property that is her the player deviating the paths from the root to them. Formally, given $\mathcal{C} \subset H_i$ the outcomes reachable for player i, then for all $h', h'' \in \mathcal{C}$ it holds $I(h', h'') = i$. Moreover, as we show in the next section, such property is maximal, i.e., there is no other outcome that can be added to $\mathcal{C}$ such that the property still holds.

The formal representation of this property is the undirected graph having the outcomes H_i as vertices and $E|_{H_i} = \{(h, h') \in H_i | I(h, h') = i\}$ as edges. The sets of outcomes reachable for player i form maximal cliques over such graph $\langle H_i, E|_{H_i}\rangle$. Finally, Algorithm 2 determines for all $i \in \mathcal{I}$ whether there is a set $\mathcal{C} \subset H_i \setminus X_i$ forming a maximal clique on $\langle H_i, E|_{H_i}\rangle$. As we show in Section 4,

this property is sufficient and necessary for the players not to have an incentive to deviate unilaterally and thus for h to be a realisation of a Nash equilibrium.

Example. Let us apply Algorithm 2 to discuss if h_3 is the realisation of a Nash equilibrium. Let us fix $i = 1$: we have $H_1 = \{h_5, h_6, h_7, h_8\}$ and $X_1 = \{h_6, h_7, h_8\}$. Since for all $h' \in X_1$ we have that $I(h_5, h') \neq 1 = i$, the set $\{h_5\}$ solves Problem 1. Let us now consider $i = 2$; since $H_2 = \emptyset$, Problem 1 has trivially positive answer. Finally, let $i = 3$: we have $H_3 = \{h_1, h_2\}$ and $X_3 = \{h_2\}$. Since $I(h_1, h_2) = 1 \neq 3 = i$, we have that $\{h_1\}$ solves Problem 1 with positive answer. Therefore h_3 is a realisation of a Nash equilibrium. The backward induction algorithm could not identify such outcome, because it is not a subgame perfect equilibrium (cf. Section 2).

Problem 1 is solved with the following linear system [12]:

$$\begin{aligned} x_{h'} + x_{h''} &\leq 1 \quad h', h'' \in H_i \setminus X_i, (h', h'') \notin E \\ \sum_{h' : (h', h'') \notin E} x_{h'} &\geq 1 \quad \forall h'' \in X_i \\ x_{h'} &\in \{0, 1\} \quad \forall h' \in H_i \setminus X_i. \end{aligned}$$

Complexity. We recall that an enumeration of the Nash equilibria in practice cannot be done with brute force, because it require to list an exponential number of strategies. On the other hand, Algorithm 2 can be represented with an undirected graph with $|H|$ vertices and $O(|H|^2)$ edges. The function $I : H \times H \to \mathcal{I}$ requires to always compare two paths whose length depends on the depth of the tree, which is always lower than the number of outcomes $O(|H|)$ [12]. Differently from brute force methods, Algorithm 2 relies on a representation which is scalable with the size of the game.

Parallelizable. Beside brute-force algorithms, the only method to compute at least one Nash equilibrium is the backward induction [8], which identifies the subgame perfect equilibria of the game. Such method is recursive and thus cannot be parallelized. Moreover, there is no way to simplify the algorithm, since every node must be explored [10]. On the other hand, Algorithm 2 can be parallelized and relies on Problem 1, whose complexity varies with the structure of the tree and the value of utility function [12]. Empirical results show that in two-player games Problem 1 is trivial in the majority of cases [12].

Applications. Let us consider some examples of extensive-form games with perfect information introduced in Section 1:

- an *intruder attack* [2]; intrusion detection is modeled with a zero-sum game, whose goal is to avoid that the intruder wins; our method allows to analyse every outcome corresponding to an attack carried out with success and prove that they are not equilibria;
- a *blockchain protocol* [11]; the method of analysis of blockchains requires to assess the properties of a single outcome [11], i.e., the one corresponding to the protocol's outcome. Such result is often not corresponding to the subgame perfect equilibrium. Algorithm 2 provides a method to analyse it without building the tree of the game nor computing other equilibria;

- a *wiretap channel* [5]; results in the literature provide only the subgame perfect equilibrium, while Algorithm 2 allows to compute all equilibria; because of space limits, we leave this computation to future works;
- an *ephemeral network* [7]; the analysis of the vote in sequence in ephemeral networks relies on the subgame perfect equilibrium; however, in reality the players can create coalitions which correspond to different equilibria; Algorithm 2 allows to compute such equilibria;
- an *attack-defense tree* [3]; similarly to the intrusion detection, the game is zero-sum and thus the analysis can be performed for the cases that the attacks are carried out with success.

4 Technical analysis of the method

In this section we show that Algorithm 2 determines if an outcome $h \in H$ is the realisation of a Nash equilibrium.

The proof relies on Lemma 1. First, we characterise the outcomes of a strategy $H(s_i)$ (cf. Definition 3), given a strategy $s_i \in S_i$ of a player $i \in \mathcal{I}$. The function $I : H \times H \to \mathcal{I}$, which is key for Algorithm 2, characterises the outcomes of the strategies.

Theorem 1. *Given a game $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$ and two outcomes $h, h' \in H$, the following three propositions are equivalent:*

1. *$i = P(h \cap h')$;*
2. *There is no $s_i \in S_i$ such that $h, h' \in H(s_i)$;*
3. *There exists a set of strategies $s_{-i} \in S_{-i}$ such that $h, h' \in H(s_{-i})$.*

Proof. Let us represent outcomes h and h' as the two sequences of actions leading to them, i.e., $h = (a_k)_{k \in \{1,\dots,K\}}$ and $h' = (a'_k)_{k \in \{1,\dots,K'\}}$, respectively. We denote h^r and h'^r the histories which are the prefix of size r of h and h', respectively. By definition the prefix $h \cap h'$, of size $\overline{r}$, is the history such that $h^r = h'^r$ for $r \leq \overline{r}$ and $h^{\overline{r}+1} \neq h'^{\overline{r}+1}$.

(1) $\Rightarrow$ (3). Let us consider strategy profile $s = \langle s_j \in S_j \rangle_{j \in \mathcal{I}}$ defined as follows: $s_j(h^r) = a_{r+1}$ and $s_j(h'^r) = a'_{r+1}$ for all $r \neq \overline{r}$ such that respectively $P(h^r) = j$ or $P(h'^r) = j$. For all other nodes of the game tree, the actions are chosen at random. Let us consider two strategies $s_i, s'_i \in S_i$ of player $i = P(h \cap h')$ and such that $s_i(a_{\overline{r}}) = a_{\overline{r}+1}$ and $s'_i(a'_{\overline{r}}) = a'_{\overline{r}+1}$. By construction $\langle s_1, \dots, s_i, \dots, s_N \rangle \mapsto h$ and $\langle s_1, \dots, s'_i, \dots, s_N \rangle \mapsto h'$ and thus for all $j \neq i$ it holds $h, h' \in H(s_j)$.

(2) $\Rightarrow$ (1). We prove it by contradiction. If $P(h \cap h') = j \neq i$ we would have that, since (1) $\Rightarrow$ (3), there exists $s_i \in S_i$ such that $h, h' \in H(s_i)$, against the assumptions in (2).

(3) $\Rightarrow$ (2). If there is a strategy $s_i \in S_i$ such that $h, h' \in H(s_i)$, then we have $\{h, h'\} \subseteq H(s)$, i.e., strategy profile $\langle s_i, s_{-i} \rangle$ would have more than one outcome, which is absurd. □

In order to define the set of possible outcomes $H(s_i)$ of a strategy $s_i \in S_i$ of a player $i \in \mathcal{I}$, it is possible to use directly function I to select which elements

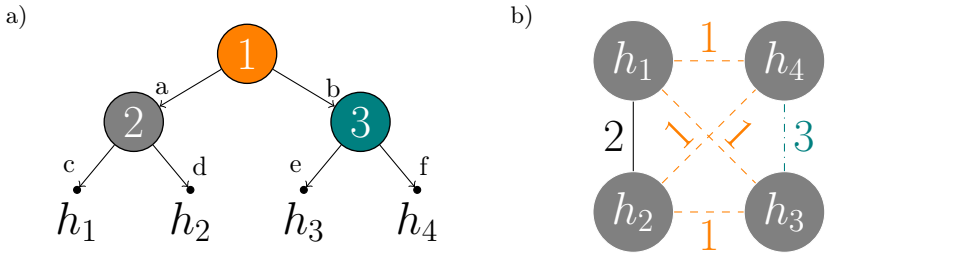

Fig. 3. Example of graph form. a) Game in extensive form. b) Game in graph form.

$h \in H$ can or cannot belong to $H(s_i)$. We therefore represent the game as a complete graph whose vertex set is made by the outcomes H and each edge $(h, h') \in H^2$ is labeled with the label of player $I(h, h')$.

Definition 5. *Given an extensive-form game $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u \rangle$ the graph form $\langle H, I, u \rangle$ is described by the complete edge-labeled graph with vertex set H, where every edge $(h, h') \in H^2$ with $h \neq h'$ has label $I(h, h') = P(h \cap h') \in \mathcal{I}$ and the utility function $u : H \to \mathbb{R}^N$.*

Example. Let us observe the game of Fig. 3 with its graph form. In this game each player acts at only one node, therefore we represent with s^a the strategy that chooses action a. The paths from the root to outcomes h_1 and h_3 are split by player 1, who can choose whether to go left (strategy s^a) or to go right (strategy s^b). We thus write $I(h_1, h_3) = 1$ and we assign the label 1 to arc (h_1, h_3). Analogously, the paths belonging to outcomes h_3 and h_4 are split by player 3 who can go either left (strategy s^e) or right (strategy s^f). Therefore we write $I(h_3, h_4) = 3$, assigning label 3 to arc (h_3, h_4).

Now, we define the set of outcomes of a strategy by using the function $I : H \times H \to \mathcal{I}$. According to Theorem 1, the graph form contains all the possible values of function $I(h, h')$ for every couple of outcomes $(h, h') \in H \times H$ of the game.

Let us analyse our example and then conclude how to characterize the set of outcomes of a strategy directly on the graph of the game.

Example. For the game of Fig. 3a let us enlist all the strategies, their possible outcomes and then observe the corresponding labelling on the graph. Player 1 has two strategies: s^a and s^b. If player 1 picks strategy s^a the only possible outcomes are $H(s^a) = \{h_1, h_2\}$, while if she picks strategy s^b we have $H(s^b) = \{h_3, h_4\}$. Player 2 has two strategies: s^c and s^d. If player 2 chooses strategy s^c, she limits the possible outcomes to $H(s^c) = \{h_1, h_3, h_4\}$, while if she chooses s^d we have $H(s^d) = \{h_2, h_3, h_4\}$. Finally for player 3 we have that $H(s^e) = \{h_1, h_2, h_3\}$ and $H(s^f) = \{h_1, h_2, h_4\}$. Let us consider the graph form depicted in Fig. 3b and remove all arcs with the same label $i \in \mathcal{I}$. Formally, let us define the graph $\langle H, E|_{\neq i} \rangle$ for each player $i \in \mathcal{I}$, with $E|_{\neq i} = \{(h, h') \in H^2 : I(h, h') \neq i\}$ excluding all the arcs $(h, h') \in E$ such that $I(h, h') = i$. Let us consider $i = 1$ and observe the strategies $s_1 = s^a$ and $s_1 = s^b$. Their outcomes $H(s^a) = \{h_1, h_2\}$ and

$H(s^b) = \{h_3, h_4\}$ form cliques over $\langle H, E|_{\neq 1}\rangle$. This is compliant with Theorem 1, for which given a strategy s_i for all elements $h, h' \in H(s_i)$ we have that $I(h, h') \neq i$ and thus $(h, h') \in E|_{\neq i}$. Moreover, as proved next, we conclude that such cliques are maximal.

The above argument can be made stronger: not only the outcomes of a strategy $s_i \in S_i$ form a maximal clique over $\langle H, E|_{\neq i}\rangle$, but also for every set $C \subset H$ inducing a maximal clique on $\langle H, E|_{\neq i}\rangle$ there is a corresponding strategy $s_i \in S_i$ with such set of outcomes $C = H(s_i)$.

Lemma 2. *Given an extensive-form game $\Gamma = \langle \mathcal{I}, \mathcal{A}, H', H, P, u\rangle$ and its graph form $\langle H, I, u\rangle$, let us consider $\langle H, E|_{\neq i}\rangle$ the graph with H as vertices and $E|_{\neq i} = \{(h, h') \in H^2, I(h, h') \neq i\}$ for some player $i \in \mathcal{I}$. There is a bijection between the set of maximal cliques of $\langle H, E|_{\neq i}\rangle$ and the set of the set of outcomes of the player's strategies $H(S_i) = \{H(s_i)|s_i \in S_i\}$.*

Proof. Let $C \subset H$ induce a maximal clique on graph $\langle H, E|_{\neq i}\rangle$. Let us define a strategy $s_i \in S_i$ such that $C \subset H(s_i)$. We use the same constructive argument as done in Theorem 1: for all $h \in C$, and for all k-prefix h^k such that $P(h^k) = i$, we can fix $s_i(h^k) = a_k$ such that $h^k + (a_k) = h^{k+1}$; indeed, since C is a clique, for every other $h' \in C$ such that h^k is a prefix of h' we have that h^{k+1} is a prefix also for h'. For all remaining nodes of the tree, actions can be fixed at random. Let $h'' \in H \setminus C$: by construction there is $h \in C$ such that $I(h, h') = i$, so that $h'' \notin H(s_i)$ and thus $H(s_i) = C$.

We now prove the opposite, i.e., the outcomes of a strategy of player $i \in \mathcal{I}$ define a maximal clique over $\langle H, E|_{\neq i}\rangle$. Consider a strategy $s_i \in S_i$ and the set of its outcomes $H(s_i)$. We apply Theorem 1: for every $h, h' \in H(s_i)$ it holds $I(h, h') \neq i$. By definition, all the elements $h, h' \in H(s_i)$ are connected in $\langle H, E|_{\neq i}\rangle$, i.e., $H(s_i)$ forms a clique. If this clique is not maximal, there exists $C \subset H$ with $H(s_i) \subsetneq C$ that induces a maximal clique over $\langle H, E|_{\neq i}\rangle$. As done before, we define $s'_i \in S_i$ a strategy such that $H(s'_i) = C$. We have thus $H(s_i) \subsetneq H(s'_i)$. This is absurd. Indeed, since $s_i \neq s'_i$, there exists $h^k \in H(s'_i)$ with $P(h^k) = i$ such that $s_i(h^k) \neq s'_i(h^k)$. Let us consider an element $h \in H(s_i)$ such that $h^k + s_i(h^k)$ is a prefix of h: such element exists because the subgame Γ^k starting from node $h^k + s_i(h^k)$ must be not empty. We have that $h \in H(s_i)$ and $h \notin H(s'_i)$, hence proving the contradiction. □

The above result characterises the players' strategies in terms of a structural property of the graph form of the game. Let us recall that Lemma 1 defines a realisation of the Nash equilibria over the set of outcomes of the strategies, which are then characterised on the graph in Lemma 2. We combine the two lemmas to discuss over the graph whether a candidate outcome $h \in H$ is the realisation of a Nash equilibrium $s \in S$.

Theorem 2. *Given a game in its graph form $\langle H, I, u\rangle$, let us consider $\langle H, E|_{\neq i}\rangle$ defined for each player $i \in \mathcal{I}$. An outcome $h \in H$ is a realisation of a Nash equilibrium if and only if there are sets $\{C_i \subset H\}_{i\in\mathcal{I}}$ that induce maximal cliques respectively over the graphs $\{\langle H, E|_{\neq i}\rangle\}_{i\in\mathcal{I}}$ such that:*

i. $h \in \cap_{i \in \mathcal{I}} C_i$;
ii. $\forall h' \in H \setminus \{h\}$ *and* $i = I(h, h')$ *at least one of the two conditions holds: a)* $u_i(h) \geq u_i(h')$ *or b)* $h' \notin \cap_{j \in \mathcal{I} \setminus \{i\}} C_j$.

Proof. Let us consider a strategy $s \in S$ as for Lemma 1. First, for all $i \in \mathcal{I}$ it must hold $h \in H(s_i)$. Second, for any other outcome $h' \neq h$, if $I(h, h') = i$ we have that $h \in H(s_i)$ implies that $h' \notin H(s_i)$ (cf. Theorem 1). Therefore the only condition that allows $h' \in H(s_{-i}) = \cap_{j \in \mathcal{I} \setminus \{i\}} H(s_j)$ is that $I(h, h') = i$. Any outcome $h' \neq h$ must thus fulfill at least one of the two conditions: a) $u_i(h) \geq u_i(h')$ no matter if $h \in \cap_j H(s_j)$ or not, or b) $h' \notin \cap_j H(s_j)$. Finally, from Lemma 2 we know that the existence of every set $H(s_i)$ depends on the existence of a set $C_i = H(s_i)$ that forms a maximal clique on graph $\langle H, E|_{\neq i} \rangle$. □

Example. Let us apply Theorem 2 to the graph of Fig. 3b for outcome $h_2 \in H$. Three cliques have to be identified C_1, C_2 and C_3. The only set inducing a maximal clique on $\langle H, E|_{\neq 1} \rangle$ such that h_2 belongs to it is $C_1 = \{h_1, h_2\}$. Analogously, the only maximal clique on $\langle H, E|_{\neq 2} \rangle$ including h_2 is $C_2 = \{h_2, h_3, h_4\}$. Finally, the maximal cliques on $\langle H, E|_{\neq 3} \rangle$ are $C_3 = \{h_1, h_2, h_3\}$ and $C_3 = \{h_1, h_2, h_4\}$. Therefore $h_1 \in C_1 \cap C_3$ and the condition $u_2(h_2) \geq u_2(h_1)$ is necessary. On the other hand, either $h_3 \in C_2 \cap C_3$ and $h_4 \in C_2$ or $h_4 \in C_2 \cap C_3$ and $h_3 \in C_2$. One of the two conditions between $u_1(h_2) \geq u_1(h_3)$ and $u_1(h_2) \geq u_1(h_4)$ must be fulfilled. Finally, h_2 is a realisation of a Nash equilibrium if and only if $u_2(h_2) \geq u_2(h_1)$ and either $u_1(h_2) \geq u_1(h_3)$ or $u_1(h_2) \geq u_1(h_4)$.

We now state a property of the graph of the game, which will be helpful in the following arguments.

Lemma 3 (Triangle property). *Given a game in its graph form* $\langle H, I, u \rangle$ *let us consider three outcomes* $h, h', h'' \in H$. *If* $I(h, h'') \neq I(h'', h')$, *then either* $I(h, h') = I(h, h'')$ *or* $I(h, h') = I(h'', h')$.

Example. Let us consider three vertices in the graph of Fig. 3b, for instance vertices h_1, h_2 and h_3. The arcs (h_1, h_3) and (h_2, h_3) have label 1, while the arc (h_1, h_2) has label 2. The outcome h_3 is separated at the root by h_1 and h_2 and therefore shares with them the same label $i = 1$. Being the separation held at the same stage, h_3 must share the same label with h_1 and h_2. With a similar argument it is possible to show that among three outcomes there is always one which is separated by the other two at the same stage. Formally, since it is impossible that three paths in a tree share three different intersections, it is possible to prove that no triangle in the graph of a game has three different labels.

The graph form of a game labels every pair of outcomes with the unique player who can be decisive in choosing among them. In order for an outcome $h \in H$ to be the realisation of a Nash equilibrium (cf. Theorem 2), any possible outcome $h' \in H \setminus \{h\}$ resulting from a deviation in terms of strategies must be either not incentivised, i.e., $u_i(h) \geq u_i(h')$, or not be a realisation of an unilateral deviation, i.e., there are at least two players having strategies that

do not include h' as possible outcome. The first condition is easily verified by checking the values of the utility function for each tagged player i. Let us focus on the second condition: for any other outcome $h' \neq h$ with $I(h,h') = i$ we have to find sets $\{C_j\}_{j\in\mathcal{I}\setminus\{i\}}$ inducing maximal cliques on the respective graphs $\{\langle H|E_{\neq j}\rangle\}_{j\in\mathcal{I}\setminus\{j\}}$ such that for at least one $j \in \mathcal{I}\setminus\{i\}$ we have that $h' \notin H(s_j)$. The aim of the Algorithm 2 is to verify the existence a set of maximal cliques such to prevent that any outcome not meeting the first condition $u_i(h) \geq u_i(h')$ at some player i belongs to the intersection of all cliques but the one corresponding to player i. Algorithm 2 allows, given a game in graph form $\langle H, I, u\rangle$, precisely to determine if an outcome $h \in H$ is the realisation of a Nash equilibrium. In the following paragraphs we develop the steps that lead to the design of the algorithm:

- The graph $\langle H, E\rangle$ is partitioned into subgraphs $\{\langle H_i, E\rangle\}_{i\in\mathcal{I}}$, where $H = \cup_{i\in\mathcal{I}}\{H_i\} \cup \{h\}$ and $H_i = \{h' \in H, I(h,h') = i\}$ are the outcomes of the possible unilateral deviations of player i;
- Any set $C_j \subset H$ inducing a maximal clique over $\langle H, E|_{\neq j}\rangle$ is shown to be a union of sets $C_j = \cup_{i\in\mathcal{I}\setminus\{j\}} C_j|_{H_i}$ inducing maximal cliques over the respective subgraphs $\{\langle H_i, E|_{\neq j}\rangle\}_{i\in\mathcal{I}\setminus\{j\}}$ (cf. Lemma 4); the problem can be thus analysed on every subgraph $\langle H_i, E|_{\neq j}\rangle$;
- The problem of existence of multiple sets $\{C_j|_{H_i} \subset H_i\}_{j\in\mathcal{I}\setminus\{i\}}$ inducing maximal cliques over the respective subgraphs $\{\langle H_i, E|_{\neq j}\rangle\}_{j\in\mathcal{I}\setminus\{i\}}$ is proved to be equivalent to the problem of existence of a set $\mathcal{C}_i \subset H_i$ inducing a maximal clique over $\langle H_i, E|_{=i}\rangle$ (cf. Lemma 5);
- Algorithm 2 thus checks for all $i \in \mathcal{I}$ that on every subgraph $\langle H_i, E|_{=i}\rangle$ there is a set $\mathcal{C}_i \subset H_i$ inducing a maximal clique such that none of the elements that do not meet the first condition $X_i = \{h' \in H_i, u_i(h) < u_i(h')\}$ belong to $\mathcal{C}_i$, i.e., such that $\mathcal{C}_i \cap X_i = \emptyset$ (cf. Problem 1).

Induced subgraphs of deviations. From now on the object of the inquire is a target outcome $h \in H$ and whether or not it is the realisation of some Nash equilibrium $s \in S$. For the sake of example we shall use the graph form of Fig. 4 which corresponds to the game of Fig. 1. Let us group all the outcomes that can be potential unilateral deviations of the same player in the sets H_i. In the following we call alternatively *unilateral deviation* the strategy $s'_i \neq s_i$ that differs from the one used at the Nash equilibrium $s \in S$ and the realisation h' of the new strategy profile $s' = (s'_i, s_{-i}) \mapsto h'$.

In order to simplify the condition of Theorem 2, we analyse the relationship between maximal cliques and the subgraphs induced by sets of possible deviations $\{H_i\}_{i\in\mathcal{I}}$.

Example. Fig. 5 shows the graph of Fig. 4 induced over respectively $H_1 = \{h_5, h_6, h_7, h_8\}$, $H_2 = \{h_4\}$ and $H_3 = \{h_1, h_2\}$. Let us suppose that we are given for all $j \in \mathcal{I}$ the set of outcomes C_j of a strategy $s_j \in S_j$ inducing a maximal clique over graph $\langle H, E|_{\neq j}\rangle$.

The first observation is that, in order for the designated $h \in H$ to be an outcome of the strategy profile $s \in S$, it must hold $h \in C_j$ for every $j \in \mathcal{I}$.

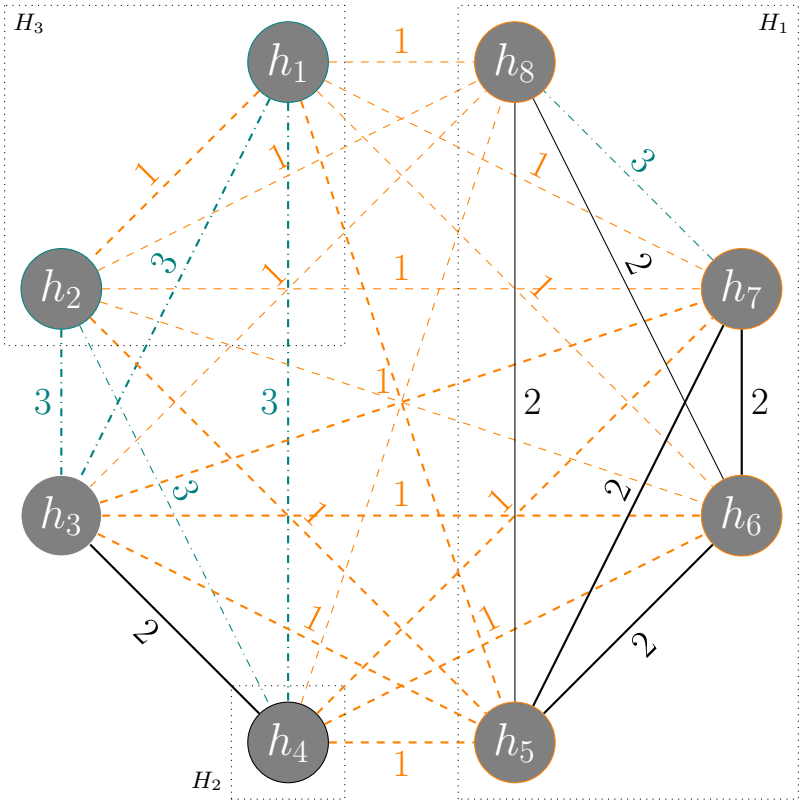

Fig. 4. Graph form of game of Fig. 1. Given $h = h_3$ as target outcome, we have $H_1 = \{h_5, h_6, h_7, h_8\}$, $H_2 = \{h_4\}$ and $H_3 = \{h_1, h_2\}$. In the example the chosen strategy profile $s \in S$ is such that $H(s_1) = C_1 = \{h_1, h_3, h_4\}$, $H(s_2) = C_2 = \{h_1, h_2, h_3, h_5\}$ and $H(s_3) = C_3 = \{h_3, h_4, h_5, h_6, h_7\}$. Preferences of the players over the outcomes are respectively: $u_1 : h_6 \succ_1 h_7 \succ_1 h_8 \succ_1 h_3 \succ_1 h_4 \succ_1 h_2 \succ_1 h_1 \succ_1 h_5$, $u_2 : h_5 \succ_2 h_8 \succ_2 h_7 \succ_2 h_6 \succ_2 h_2 \succ_2 h_3 \sim_2 h_4 \succ_2 h_1$ and $u_3 : h_8 \succ_3 h_7 \succ_3 h_6 \succ_3 h_2 \succ_3 h_5 \succ_3 h_3 \succ_3 h_1 \succ_3 h_4$.

By definition of H_j, we have that $C_j \cap H_j = \emptyset$, because all of its elements are incompatible with h with respect to player i.

Example. In Fig. 5 we observe $C_1 \cap H_1 = \emptyset$, $C_2 \cap H_2 = \emptyset$ and $C_3 \cap H_3 = \emptyset$. Any set C_j that verifies the assumptions of Theorem 2 includes solely elements of outcome sets H_i for $i \neq j$.

The second observation is that the elements in $C_j \cap H_i$ for any $i \neq j$ form a maximal clique also on the induced graph $\langle H_i, E|_{\neq j} \rangle$, i.e., with H_i as set of vertices and $E|_{\neq j} = \{(h, h') \in H_i^2 | I(h, h') \neq j\}$.

Example. Let us consider $C_3 = \{h_3, h_4, h_5, h_6, h_7\}$ and let us analyse $C_3 \cap H_1$ and $C_3 \cap H_2$. The element h_4 is the only element of $C_3 \cap H_2$ and therefore forms a maximal clique within H_2. The elements $\{h_5, h_6, h_7\} \subset C_3$ belong to

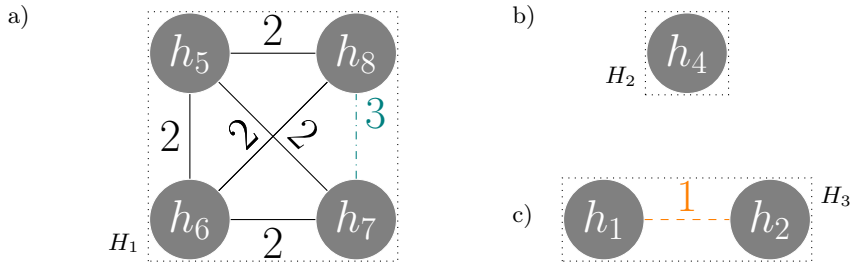

Fig. 5. Induced subgraphs. The candidate outcome is $h = h_3$. We show graph of Fig. 4 induced over a) $H_1 = \{h_5, h_6, h_7, h_8\}$ b) $H_2 = \{h_4\}$ and c) $H_3 = \{h_1, h_2\}$. We recall that the chosen $s \in S$ in the example is such that $H(s_1) = C_1 = \{h_1, h_3, h_4\}$, $H(s_2) = C_2 = \{h_1, h_2, h_3, h_5\}$ and $H(s_3) = C_3 = \{h_3, h_4, h_5, h_6, h_7\}$.

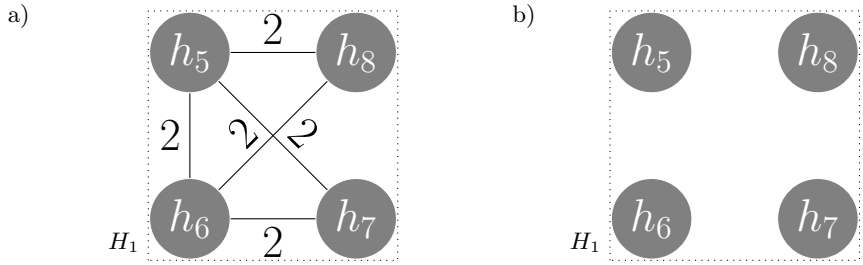

Fig. 6. Removing arcs from a induced graph. a) Induced graph $\langle H_1, E|_{\neq 3}\rangle$ b) Induced graph $\langle H_1, E|_{=1}\rangle$.

$H_1 = \{h_5, h_6, h_7, h_8\}$. Let us observe the induced graph $\langle H_1, E|_{\neq 3}\rangle$ in Fig. 6a. The outcomes h_7 and h_8 are not connected since $I(h_7, h_8) = j = 3$. The elements $C_3 \cap H_1 = \{h_5, h_6, h_7\}$ form indeed a maximal clique within $\langle H_1, E|_{\neq 3}\rangle$.

With the following lemma we show that it is equivalent to look for a maximal clique over the graph $\langle H, E|_{\neq j}\rangle$ and looking for $N-1$ maximal cliques on the $N-1$ respective graphs $\{\langle H_i, E|_{\neq j}\rangle\}_{i \in \mathcal{I}\setminus\{j\}}$.

Lemma 4 (Partition). *Given a game in its graph form $\langle H, I, u\rangle$, a player $i \in \mathcal{I}$ and the graph $\langle H, E|_{\neq j}\rangle$, every set C_j inducing a maximal clique over the graph $\langle H, E|_{\neq j}\rangle$ is the union $C_j = \cup_{i \in \mathcal{I}\setminus\{j\}} C_j|_{H_i}$ of the disjoint sets $C_j|_{H_i} = C_j \cap H_i$ inducing maximal cliques over $\langle H_i, E|_{\neq j}\rangle$.*

Proof. We recall that $H_i = \{h' \in H | I(h, h') = i\}$ is the set of possible deviations from the target outcome $h \in H$. It is enough to prove that within the main graph $\langle H, E|_{\neq j}\rangle$ every two elements $h_{i'}, h_{i''}$ belonging to two different sets of possible deviations, i.e., $h_{i'} \in H_{i'}$ and $h_{i''} \in H_{i''}$ with $i', i'' \in \mathcal{I} \setminus \{j\}$ and $i' \neq i''$, are always connected. Formally, we need to show that it always holds $(h_{i'}, h_{i''}) \in E|_{\neq j}$, i.e., $I(h_{i'}, h_{i''}) \neq j$. Given the designated $h \in H$, we observe that $I(h, h_{i'}) = i'$ and $I(h, h_{i''}) = i''$. For the triangle property of Lemma 3 either $I(h_{i'}, h_{i''}) = i' \neq j$ or $I(h_{i'}, h_{i''}) = i'' \neq j$, which concludes the proof. □

Example. Let us consider again the graph of Fig. 4 with candidate outcome $h = h_3$. Let us characterise a generic maximal clique C_2, i.e., the set of outcomes of a strategy $s_2 \in S_2$ of player $j = 2$ that admits $h_3 \in H(s_2) = C_2$ as possible outcome. By hypothesis we have to fix $h_3 \in C_2$ and $h_4 \notin C_2$, since $H_2 = \{h_4\}$. Let us consider thus $H_1 = \{h_5, h_6, h_7, h_8\}$ and $H_3 = \{h_1, h_2\}$. Given any edge $(h', h'') \in H_1 \times H_3$, the label $I(h', h'') \neq 2$ again from Lemma 3. In this specific case $I(h', h'') = 1$ for every pair of elements. Any candidate strategy $s_2 \in S_2$ for a Nash equilibrium $s \in S$ having $s \mapsto h_3$ as realisation has therefore a set of outcomes $H(s_2) = C_2 = \{h_3\} \cup (C_2|_{H_1}) \cup (C_2|_{H_3})$, where $C_2|_{H_1}$ and $C_2|_{H_3}$ are sets of elements that induce a maximal clique respectively on $\langle H_1, E|_{\neq 2}\rangle$ and $\langle H_3, E|_{\neq 2}\rangle$.

Theorem 2 requires to identify for every $j \in \mathcal{I}$ a maximal clique over the graph $\langle H, E|_{\neq j}\rangle$. Thanks to the latest result, it is possible to check the existence of such maximal clique on every induced graph $\langle H_i, E|_{\neq j}\rangle$. We thus rewrite the necessary and sufficient condition on the induced subgraphs: for all $i \in \mathcal{I}$ there must be a set $C_j|H_i$ inducing a maximal clique for every player $j \in \mathcal{I} \setminus \{i\}$ such that none of the possible deviations $h' \in X_i \subset H_i$ belongs to the intersection of the maximal cliques $\cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i}$.

Example. In Fig. 6a we have that $X_1 = \{h_6, h_7, h_8\}$ and the induced sets over $H_1 = \{h_5, h_6, h_7, h_8\}$ that induce maximal cliques are respectively $C_2|_{H_1} = \{h_5\}$ and $C_3|_{H_1} = \{h_5, h_6, h_7\}$. The property $(\cap_{j\in\mathcal{I}\setminus\{i\}} C_j) \cap X_i = \emptyset$ is fulfilled, since $(C_2 \cap C_3)|_{H_1} = \{h_5\}$ and $X_1 = \{h_6, h_7, h_8\}$ have no elements in common.

Let us discuss the properties of the intersection $\cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i}$: these are the possible unilateral deviations of player i, given the strategies of the other players $\cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i} = H(s_{-i})$ for some $s_{-i} \in S_{-i}$. Let us observe that given the possible outcomes $\cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i}$ it is the player $i \in \mathcal{I}$ who chooses which one is to be the deviation. In other words, it is intuitive that for every pair of elements $h, h' \in \cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i}$ it must hold $I(h, h') = i$. Let us show that this property is maximal and thus that identifying an intersection of maximal cliques $\cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i}$ is equivalent to identifying a set $\mathcal{C}_i$ inducing a maximal clique over H_i.

Lemma 5. *Given a game in graph form $\langle H, I, u\rangle$, a player $i \in \mathcal{I}$ and the induced subgraph $\langle H_i, E\rangle$ on the set of possible deviations H_i and a set $\mathcal{C}_i \subset H_i$, the two conditions are equivalent:*

- *$\mathcal{C}_i$ induces a maximal clique over graph $\langle H_i, E|_{=i}\rangle$, where $E|_{=i} = \{(h, h') \in H_i^2 | I(h, h') = i\}$;*
- *There are sets $\{C_j|_{H_i}\}_{j\in\mathcal{I}\setminus\{i\}}$ inducing maximal cliques over the graphs $\{\langle H_i, E|_{\neq j}\rangle\}_{j\in\mathcal{I}\setminus\{i\}}$ such that $\mathcal{C}_i = \cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i}$.*

Proof. For sake of clarity, in the proof we drop the subscript $|_{H_i}$ from $C_j|_{H_i}$.

We first prove the direct implication. Let $\mathcal{C}_i$ induce a maximal clique over $\langle H_i, E|_{=i}\rangle$ and for all $j \in \mathcal{I}\setminus\{i\}$ a set C_j with $\mathcal{C}_i \subset C_j$ induce maximal clique over the graphs $\langle H_i, E|_{\neq j}\rangle$. The sets $\{C_j\}$ are well defined because for all $h', h'' \in \mathcal{C}_i$ it holds $I(h', h'') = i \neq j$. We observe that for every $h', h'' \in \cap_j C_j$ it holds $I(h', h'') = i$ and thus $\mathcal{C}_i \subset \cap_j C_j$. Since $\mathcal{C}_i$ is a maximal clique, $\mathcal{C}_i = \cap_j C_j$.

Now let us prove the opposite, i.e., let us show that $\mathcal{C}_i = \cap_j C_j$ induces a maximal clique over $\langle H_i, E|_{=i}\rangle$. For all $h', h'' \in \mathcal{C}_i$ it holds $I(h', h'') = i$, i.e., $\mathcal{C}_i$ induces a clique on $\langle H_i, E|_{=i}\rangle$. Let us show that it is maximal. By contradiction, there is $\mathcal{C}'_i \supset \mathcal{C}_i$ forming a maximal clique over $\{H_i, E|_{=i}\}$. With a similar argument used for Lemma 2 we prove that this is absurd. □

Let us observe the induced graph $\langle H_1, E|_{=1}\rangle$ of Fig. 6b. There are no edges with label 1 and therefore all the maximal cliques are the single vertices. This means that players 2 and 3 can identify strategies such that player 1 is forced to pick only the vertex chosen by them.

We can thus show that Algorithm 2 determines whether an outcome is a realisation of a Nash Equilibrium or not.

Theorem 3. *Given a game in its graph form $\langle H, I, u\rangle$ and an outcome $h \in H$ as input, Algorithm 2 determines whether h is a realisation of a Nash equilibrium.*

Proof. Let us define the set of possible unilateral deviations $H_i = \{h' \in H, I(h, h') = i\}$, with $H_i = V_i \cup X_i$ as in Algorithm 2. Theorem 2 states that the necessary and sufficient condition for h to be a realisation of a Nash equilibrium is the existence of sets $\{C_i\}_{i\in\mathcal{I}}$ inducing maximal cliques over the respective graphs $\{\langle H, E|_{\neq i}\rangle\}_{i\in\mathcal{I}}$ such that $h \in \cap_{i\in\mathcal{I}} C_i$ and $\cap_{j\in\mathcal{I}\setminus\{i\}} C_j \subset V_i$. The previous results let us simplify such condition up to the excluding clique problem: for sake of clarity, hereafter let us summarise the argument. For Lemma 4 the condition is equivalent to verifying for all $i \in \mathcal{I}$ the existence of sets $\{C_j|_{H_i} \subset H_i\}_{j\in\mathcal{I}\setminus\{i\}}$ inducing maximal cliques over graphs $\{\langle H_i, E|_{\neq j}\rangle\}_{i\in\mathcal{I}}$ such that $\cap_{j\in\mathcal{I}\setminus\{i\}} C_j|_{H_i} \subset V_i$. Finally, for Lemma 5 this condition is equivalent to verifying for all $i \in \mathcal{I}$ the existence of a set $\mathcal{C}_i \subset V_i$ that induces a maximal clique over $\langle H_i, E|_{=i}\rangle$, hence the proof. □

5 Conclusions

In this work, we focused on security models with perfect observability. In the literature, the representation of such models is in the form of an extensive-form game, whose solution concept is the Nash equilibrium. However, to date, such representation is not convenient computationally because, to the best our knowledge, there exist no efficient methods to compute all Nash equilibria of extensive form games. In fact, the only known method in this field is the backward induction algorithm, which provides a subset of Nash equilibria. The lack of other methods for computing Nash equilibria has limited the analysis of security models with perfect observability. In Section 2 we have thus introduced an algorithm to determine whether or not an outcome of the game is the realisation of a pure Nash equilibrium. The algorithm has an efficient representation, i.e., it does not require to enumerate the game strategies. Furthermore, it relies on a graph theoretical problem whose instances are often easy to compute, as verified for the vast majority of outcomes we have tested. Moreover, this algorithm is parallelizable, a condition that is key in order to scale the solution method for larger games.

In Section 2 we have showed how our method applies to provide better insights on several known security models which are solved by means of an extensive-form game representation. Due to space limits, we did not provide the detailed analysis of such models. We plan to apply the proposed algorithm to those classes of problems and to deduce more insights on their solutions as part of future works.

References

1. Alós-Ferrer, C., Ritzberger, K., Alós-Ferrer, C., Ritzberger, K.: Discrete extensive forms. The Theory of Extensive Form Games pp. 131–161 (2016)
2. Kantzavelou, I., Katsikas, S.: A generic intrusion detection game model in it security. In: Trust, Privacy and Security in Digital Business: 5th International Conference, TrustBus 2008 Turin, Italy, September 4-5, 2008 Proceedings 5. pp. 151–162. Springer (2008)
3. Kordy, B., Mauw, S., Melissen, M., Schweitzer, P.: Attack–defense trees and two-player binary zero-sum extensive form games are equivalent. In: Decision and Game Theory for Security: First International Conference, GameSec 2010, Berlin, Germany, November 22-23, 2010. Proceedings 1. pp. 245–256. Springer (2010)
4. Kuhn, H.W., Tucker, A.W.: Contributions to the Theory of Games. No. 28 in II, Princeton University Press (1953)
5. Mukherjee, A., Swindlehurst, A.L.: Jamming games in the mimo wiretap channel with an active eavesdropper. IEEE Transactions on Signal Processing **61**(1), 82–91 (2012)
6. Nash Jr, J.F.: Equilibrium points in n-person games. Proceedings of the national academy of sciences **36**(1), 48–49 (1950)
7. Raya, M., Manshaei, M.H., Félegyházi, M., Hubaux, J.P.: Revocation games in ephemeral networks. In: Proceedings of the 15th ACM conference on Computer and communications security. pp. 199–210 (2008)
8. Selten, R.: Spieltheoretische behandlung eines oligopolmodells mit nachfrageträgheit: Teil i: Bestimmung des dynamischen preisgleichgewichts. Zeitschrift für die gesamte Staatswissenschaft/Journal of Institutional and Theoretical Economics **2**(H.), 301–324 (1965)
9. Selten, R.: The chain store paradox. Theory and decision **9**(2), 127–159 (1978)
10. Szymanik, J.: Backward induction is ptime-complete. In: Logic, Rationality, and Interaction: 4th International Workshop, LORI 2013, Hangzhou, China, October 9-12, 2013, Proceedings 4. pp. 352–356. Springer (2013)
11. Zappalà, P., Belotti, M., Potop-Butucaru, M., Secci, S.: Game theoretical framework for analyzing blockchains robustness. In: 35th International Symposium on Distributed Computing. p. 25 (2021)
12. Zappalà, P., Benhamiche, A., Chardy, M., De Pellegrini, F., Figueiredo, R.: Graph-based approach for enumerating the Nash equilibria of a two-player extensive-form game (May 2023), https://hal.science/hal-04093334, working paper or preprint