2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

Stealthy strategies for deception in hypergames with asymmetric information

Bahman Gharesifard   Jorge Cortés

Abstract— **This paper considers games with incomplete asymmetric information, where one player (the deceiver) has privileged information about the other (the mark) and intends to employ it for belief manipulation. We use hypergames to represent the asymmetric information available to players and assume a probabilistic model for the actions of the mark. This framework allows us to formalize various notions of deception in a precise way. We provide a necessary condition and a sufficient condition for deceivability when the deceiver is allowed to reveal information to the mark as the game evolves. For the case when the deceiver acts stealthily, i.e., restricts her actions to those that do not contradict the belief of the mark, we are able to fully characterize when deception is possible. Moreover, we design the `worst-case max-strategy` that, when such a sequence of deceiving actions exists, is guaranteed to find it. An example illustrates our results.**

I. INTRODUCTION

Informational asymmetries in strategic scenarios provide opportunities for manipulating beliefs or inducing certain desired perceptions. In this paper, we consider a class of games where one player (the deceiver) wishes to misrepresent certain information in order to gain a strategic advantage over the opponent (the mark). In our framework, the deceiver can anticipate the effect that her actions will have on the mark's belief structure. In this sense, the deception goal can be understood as steering the evolution of a particular dynamical system into a desired set of outcomes. Scenarios of interest includes bargaining, cybersecurity, military operations, and human behavior modeling.

Literature review: In strategic scenarios with informational asymmetries [1], players may decide not to disclose some information (passive deception) or lie about a value of interest to the opponent (active deception). Within the context of games of incomplete information, deception has not been studied in a systematic way with the exception of a few references. [2] demonstrates that the inconsistent structure of beliefs can lead to counterintuitive behaviors. [3] studies deception via strategic communication, in which a 'sophisticated' player sends either truthful or false messages to the opponents. [4] investigates the vulnerability of strategic decision makers to persuasion. The recent work [5] constructs a theory of deception for games with incomplete information where players form expectations about the average behavior of the other players based on past histories. [6], [7] consider scenarios where one player has access to certain information and can distort it before it is passed on to others. In this paper, we make use of hypergames [8], [9], [10], since they provide a natural framework for modeling strategic situations with asymmetric information among players. Early references on deception in dynamic games with imperfect information include [11], [12]. The works [13], [14], [15] provide examples of how informational asymmetries can be used to induce false perceptions in the opponent and lead to strategic deception. The works [16], [17] provide deception-robust schemes for a class of discrete dynamic stochastic games under imperfect observations.

The authors are with the Department of Mechanical and Aerospace Engineering, University of California, San Diego, California, USA, {bgharesifard,cortes}@ucsd.edu

Statement of contributions: We consider games of incomplete information where players have different perceptions about the scenarios they are involved in. We study a class of 2-player hypergames where the deceiver has full information about the mark's game and intends to induce a certain belief in her. The mark is rational, observes the actions taken by the deceiver and assumes she acts rationally (although she may not), and updates her perception about the opponent's preferences accordingly. From the deceiver's viewpoint, the mark's actions are rational and probabilistic. This framework sets the stage for the first contribution of the paper, which is the introduction of precise notions of deception to capture different forms of belief manipulation. These notions allow us to identify a necessary condition and a sufficient condition for deceivability on the mark's belief structure. Next, we study scenarios where the deceiver purposefully restricts her set of actions to those that do not contradict the mark's belief structure. We term these actions stealthy and fully characterize when deception via such actions is possible. Our third contribution is the design of the `worst-case max-strategy` that, given a desired deception objective, determines a stealthy sequence of actions that achieves it. An example illustrates the main results. Proofs are omitted for space reasons and will appear elsewhere.

II. PRELIMINARIES

We denote the set of real and positive real numbers by $\mathbb{R}$ and $\mathbb{R}_{>0}$, respectively. We denote by $\mathbb{Z}_{\geq 0}$ and $\mathbb{Z}_{\geq 1}$ the set of nonnegative and positive integers, respectively. A nonempty set X along with a preorder $\succeq$, i.e., a reflexive and transitive binary relation, is called a *directed set* if for every pair of elements in X there exists an upper bound with respect to the preorder. We use $\sigma = (x_1, x_2, \dots)$, where $x_1, x_2, \dots \in X$, to denote a sequence of elements in X. Note that a finite sequence of $k \in \mathbb{Z}_{\geq 1}$ elements is simply a k-tuple.

A. Graph theory

A *digraph* G is a pair (V, E), where V is a finite set, called the vertex set, and $E \subseteq V \times V$, called the edge set. Given an edge $(u, v) \in E$, u is an *in-neighbor* of v and v is an *out-neighbor* of u. The set of in-neighbors and out-neighbors of v are denoted, respectively, by $\mathcal{N}^{\text{in}}(v)$ and

$\mathcal{N}^{\text{out}}(v)$. The *in-degree* and *out-degree* of v are the number of in-neighbors and out-neighbors of v, respectively. $\mathcal{A}$ is an adjacency matrix for $G = (V, E)$ if the following holds: for each $v_i, v_j \in V$, $a_{ij} > 0$ iff $(v_i, v_j) \in E$. A *(directed) path* is an ordered sequence of vertices so that any two consecutive vertices are an edge of the digraph. A *cycle* in a digraph is a directed path that starts and ends at the same vertex and has no other repeated vertex. A digraph is called *acyclic* if it does not contain any cycle.

B. Markov chains

We recall here some basic notions from Markov chains following [18]. We denote by $(\Omega, \mathcal{F}, \mathbb{P})$ a *probability space*, where Ω is a countable set, $\mathcal{F}$ is a σ-algebra over Ω, and $\mathbb{P}$ is a probability measure. An *E-valued random* variable is a measurable mapping $X : (\Omega, \mathcal{F}, \mathbb{P}) \to (E, \mathcal{E})$, where $\mathcal{E}$ is a σ-algebra over E and $(E, \mathcal{E})$ is a measurable space. A *Markov chain* is a sequence of random variables $(X_1, X_2, \ldots)$ such that, for all $n \in \mathbb{Z}_{\geq 1}$ and $x \in \Omega$,

$$\mathbb{P}(X_{n+1} = x \,|\, X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) = \mathbb{P}(X_{n+1} = x \,|\, X_n = x_n).$$

The *probability transition kernel* $T_{\mathbb{P}}$ is

$$T_{\mathbb{P}}(x_i, x_j) = \mathbb{P}(X_{n+1} = x_i \,|\, X_n = x_j),$$

where $x_i, x_j \in \Omega$. Note that for every $x \in \Omega$, $T_{\mathbb{P}}(x, .)$ is also a probability measure on Ω. One can inductively define

$$T^k_{\mathbb{P}}(x_i, x_j) := \mathbb{P}(X_{n+k} = x_i \,|\, X_n = x_j).$$

If there exists $k \in \mathbb{Z}_{\geq 1}$ such that $T^k_{\mathbb{P}}(x_i, x_j) > 0$, the state x_i is *reachable* from x_j (or, equivalently, that x_j *communicates* with x_i). We denote the set of all states reachable from x_j, with respect to the transition probability $T_{\mathbb{P}}$, by

$$\mathcal{R}_{T_{\mathbb{P}}}(x_j) = \{x_i \in \Omega \mid \exists k_i \in \mathbb{Z}_{\geq 1},\ T^{k_i}_{\mathbb{P}}(x_i, x_j) > 0\}.$$

C. Hypergame theory

We consider games with inconsistent perceptions across the players in the framework of hypergames [19], [8], [9]. A 0-level hypergame is simply a *(finite) game*, i.e., a triplet $\mathbf{G} = (V, \mathbf{S}_{\text{outcome}}, \mathbf{P})$, where V is a set of $n \in \mathbb{Z}_{\geq 1}$ players, $\mathbf{S}_{\text{outcome}} = S_1 \times \ldots \times S_n$ is the outcome set with finite cardinality $N = |\mathbf{S}_{\text{outcome}}| \in \mathbb{Z}_{\geq 1}$ and $\mathbf{P} = (P_1, \ldots, P_n)$, with $P_i = (x_1, \ldots, x_N)^T \in \mathbf{S}_p$ the preference vector of player v_i, $i \in \{1, \ldots, n\}$. Here, S_i is a finite set of actions available to player $v_i \in V$ and $\mathbf{S}_p \subset \mathbf{S}^N_{\text{outcome}}$ is the set of all elements in $\mathbf{S}^N_{\text{outcome}}$ with pairwise different entries. We denote by π_i the projection of $\mathbf{S}_{\text{outcome}}$ onto S_i.

A *n-person* 1*-level hypergame* is a set $H^1 = \{\mathbf{G}_1, \ldots, \mathbf{G}_n\}$, where $\mathbf{G}_i = (V, (\mathbf{S}_{\text{outcome}})_i, \mathbf{P}_i)$, for $i \in \{1, \ldots, n\}$, is the subjective finite game of player $v_i \in V$, and V is a set of n players; $(\mathbf{S}_{\text{outcome}})_i = S_{1i} \times \ldots \times S_{ni}$, with S_{ji} the finite set of strategies available to v_j, as perceived by v_i; $\mathbf{P}_i = (P_{1i}, \ldots, P_{ni})$, with P_{ji} the preference vector of v_j, as perceived by v_i. In a 1-level hypergame, each player $v_i \in V$ plays the game $\mathbf{G}_i$ with the perception that she is playing a game with complete information. The definition of 1-level hypergame can be extended to higher-order hypergames as follows: a *n-person k-level hypergame*, $k \geq 1$, is a set $H^k = \{H^{k_1}_1, \ldots, H^{k_n}_n\}$, where $k_i \leq k - 1$ and at least one k_i is equal to $k - 1$.

1) Stability and equilibria: Here we recall the notion of stability for 2-person 1-level hypergames. This class of hypergames is the simplest one that explicitly models the perception of players about their opponents' preferences (the reader is referred to [8] for the extension to higher-order hypergames). Let $H^1 = \{H^0_A, H^0_B\}$. Here, $H^0_A = (\mathrm{P}_{AA}, \mathrm{P}_{BA})$ is the 0-level hypergame for player A, where P_{AA} and P_{BA} are, respectively, the preferences of A and B perceived by A. The same convention holds for $H^0_B = (\mathrm{P}_{AB}, \mathrm{P}_{BB})$. For simplicity, the 0-level hypergames have the same set of outcomes $\mathbf{S}_{\text{outcome}}$. We denote by $\succeq_{\mathrm{P}_{IJ}}$ the binary relation on $\mathbf{S}_{\text{outcome}}$ induced by P_{IJ}, where $I, J \in \{A, B\}$. For convenience, we let $\mathbf{S}_{\text{outcome}}|_{\pi_I(x)} = \{y \in \mathbf{S}_{\text{outcome}} \mid \pi_I(y) = \pi_I(x)\}$ and refer to it as a restricted outcome set. We also use I' to denote the opponent of I in $\{A, B\}$. We assign $\mathrm{rank}(x, \mathrm{P}_{IJ}) \in \mathbb{R}_{>0}$ to each outcome $x \in \mathbf{S}_{\text{outcome}}$ such that $\mathrm{rank}(y, \mathrm{P}_{IJ}) > \mathrm{rank}(x, \mathrm{P}_{IJ})$ iff $x \succ_{\mathrm{P}_{IJ}} y$ (players prefer the outcomes with lower ranks). We use the set $\{1, \ldots, |\mathbf{S}_{\text{outcome}}|\}$ to rank the outcomes. Given two distinct outcomes $x, y \in \mathbf{S}_{\text{outcome}}$, y is an *improvement* from x for $I \in \{A, B\}$, perceived by $J \in \{A, B\}$ in H^0_J, iff $\pi_{I'}(y) = \pi_{I'}(x)$ and $y \succ_{\mathrm{P}_{IJ}} x$. $x \in \mathbf{S}_{\text{outcome}}$ is called *rational* for $I \in \{A, B\}$, as perceived by $J \in \{A, B\}$ in H^0_J, if there exists no improvement from x for I. The common notion of rationality in hypergames is the notion of sequential rationality [20], [9], [21]. An outcome $x \in \mathbf{S}_{\text{outcome}}$ is *sequentially rational* for $I \in \{A, B\}$ with respect to H^0_J, $J \in \{A, B\}$, iff for each improvement y for I, perceived by J in H^0_J, there exists an improvement z for I', perceived by J in H^0_J, such that $x \succ_{\mathrm{P}_{IJ}} z$. Whenever this holds, we say that the improvement z from y for I' *sanctions* the improvement y from x for I in H^0_J. By definition, a rational outcome is also sequentially rational. An outcome $x \in \mathbf{S}_{\text{outcome}}$ is *unstable* for player I with respect to H^0_J if it is not sequentially rational for player I, as perceived by player J and is an *equilibrium of* H^0_J if it is sequentially rational for both J and J', perceived by J. An outcome x is an *equilibrium of* H^1 if it is sequentially rational for A in H^0_A and also for B in H^0_B. Note that x can be an equilibrium for H^1 and not an equilibrium of H^0_A.

2) H-digraphs: The notion of H-digraph encodes the stability information of hypergames. Formally, the *H-digraph* associated to H^0_A is $\mathcal{G}_{H^0_A} = (\mathbf{S}_{\text{outcome}}, \mathcal{E}_{H^0_A})$, where there exists an edge $(x, y) \in \mathcal{E}_{H^0_A}$ iff either there exists an improvement y from x for A for which there is no sanction of B in H^0_A, or there exists an improvement y from x for B for which there is no sanction of A in H^0_A. One can similarly construct $\mathcal{G}_{H^0_B}$. By definition, an outcome x is sequentially rational for A (respectively for B) iff $\mathcal{N}^{\text{out}}(x) \cap \mathbf{S}_{\text{outcome}}|_{\pi_B(x)} = \emptyset$ (respectively $\mathcal{N}^{\text{out}}(x) \cap \mathbf{S}_{\text{outcome}}|_{\pi_A(x)} = \emptyset$). Moreover, an outcome is an equilibrium for H^0_A iff its out-degree in the associated H-digraph is zero.

3) Learning in hypergames: Suppose players A and B take actions that change the outcome from x to y. If A can perfectly observe B's action and believes that the opponent is rational, she concludes that B prefers $(\pi_A(x), \pi_B(y))$ over x. Therefore, A can incorporate this information into her hypergame and update her perception about the preferences of B. Here, we recall a method called *swap learning* to do this, see [19]. These notions can similarly be defined for B.

We start by an algebraic construction. Let V be a set of cardinality N and let $W \subset V^N$ with pairwise different elements. For $x_1, x_2 \in V$, let $\text{swap}_{x_1 \mapsto x_2} : W \to W$ be

$$(\text{swap}_{x_1 \mapsto x_2}(v))_k = v_k \quad \text{if } v_k \neq x_1, x_2,$$

$$(\text{swap}_{x_1 \mapsto x_2}(v))_i = \begin{cases} v_j & \text{if } v_i = x_1, v_j = x_2 \text{ and } i < j, \\ v_i & \text{if } v_i = x_1, v_j = x_2 \text{ and } i > j, \end{cases}$$

$$(\text{swap}_{x_1 \mapsto x_2}(v))_j = \begin{cases} v_i & \text{if } v_i = x_1, v_j = x_2 \text{ and } i < j, \\ v_j & \text{if } v_i = x_1, v_j = x_2 \text{ and } i > j. \end{cases}$$

We refer to $\text{swap}_{x_1 \mapsto x_2}$ as the *x_1 to x_2 swap map*. The *swap learning maps* $\mathbf{Sw}^A_{x,y} : \mathbf{S}_{\mathrm{P}} \to \mathbf{S}_{\mathrm{P}}$ for A is given by $\mathbf{Sw}^A_{x,y}(\mathrm{P}) = \text{swap}_{x \mapsto (\pi_A(x), \pi_B(y))}(\mathrm{P})$. One can show [19] that if players are rational, swap learning is guaranteed to decrease the mismatch between a player's perception and the true payoff structure of other players. When the outcome changes from x to y and A updates her perception via swap learning, her H-digraph changes from $\mathcal{G}_{H^0_A}$ to $\mathbf{Sw}^A_{x,y}(\mathcal{G}_{H^0_A})$. Similarly, if players A and B repeatedly take actions such that the hypergame outcomes are $\sigma = (x_1, \ldots, x_n)$, then the associated H-digraph of A is denoted $\mathbf{Sw}^A_{x_1,\sigma}(\mathcal{G}_{H^0_A})$, where

$$\mathbf{Sw}^A_{x_1,\sigma} = \mathbf{Sw}^A_{x_1,x_2} \circ \mathbf{Sw}^A_{x_2,x_3} \circ \cdots \circ \mathbf{Sw}^A_{x_{n-1},x_n}.$$

We denote by $\mathbf{Sw}^A_{x_1,\sigma}(\mathcal{E}_{H^0_A})$ the edge set of $\mathbf{Sw}^A_{x_1,\sigma}(\mathcal{G}_{H^0_A})$.

III. Problem statement

In this paper, we consider 2-person 2-level hypergame. We assume B has perfect knowledge about the preferences of A, while A perfectly observes the actions of B and uses the swap learning map to update her perception. We focus on swap learning, although the analysis could also be carried out for other learning mechanisms. Formally, the situation described above corresponds to a 2-person 2-level hypergame $H^2 = \{H^0_A, H^1_B\}$, with $H^1_B = \{H^0_{AB}, H^0_{BB}\}$ such that $H^0_{AB} = H^0_A$. Since $H^0_{BB} = H^0_B$, we actually have $H^2 = \{H^0_A, \{H^0_A, H^0_B\}\}$. Because of the special form of H^2, the equilibria of H^2, as defined in [8], are exactly the same as the equilibria of $H^1_B = \{H^0_A, H^0_B\}$.

We assume that players take their actions sequentially, one after each other. This assumption matches up with the notion of sequential rationality and guarantees that the repeated play of any 0-level hypergame converges to an equilibrium [22]. Note that scenarios where one players takes multiple actions before the other player acts can also be accommodated.

Definition 3.1 (Admissible sequence): A sequence of outcomes $\sigma = (x_0, x_1, x_2, \ldots)$ in $\mathbf{S}_{\text{outcome}}$ is *admissible* if $\pi_I(x_{2i}) = \pi_I(x_{2i+1})$, and $\pi_{I'}(x_{2i+1}) = \pi_{I'}(x_{2i+2})$, for all $i \in \mathbb{Z}_{\geq 0}$, where $I \in \{A, B\}$. The set of all admissible sequences on $\mathbf{S}_{\text{outcome}}$ is denoted by $\mathscr{S}_{\text{adm}}(\mathbf{S}_{\text{outcome}})$.

When convenient, we use the notation σ_B and σ^B to denote admissible sequences where B is the first and last, respectively, to take an action. The notation σ^B_B then means that B is the first and last to take an action. Similar notations can be defined for A. Given an admissible sequence $\sigma = (x_0, x_1, \ldots, x_k)$, $k \in \mathbb{Z}_{\geq 1}$, we say that $z \in \mathbf{S}_{\text{outcome}}$ is aligned with σ at time i if $z = x_i$. In this paper, without loss of generality, we assume that B is the first to take an action. We start by introducing some basic notions.

A. Modeling player actions via probability distributions

Although player B has complete information about A's game, she does not know the strategy that A follows to decide her actions. Formally, this can be captured by assigning a probability distribution to the edges of the H-digraph of A. Let $\mathbb{P}_{AB}(X_{n+1} = y \mid X_n = x)$, for $y \in \mathbf{S}_{\text{outcome}}|_{\pi_B(x)}$, denote the probability that the outcome of the hypergame changes from x to y by the action $\pi_A(y)$ of A, as perceived by B. Given what B knows about A's game, we have that for all $(x, y) \notin \mathcal{E}_{H^0_A}$, $\mathbb{P}_{AB}(X_{n+1} = y \mid X_n = x) = 0$. Note that, for all $x \in \mathbf{S}_{\text{outcome}}$, $\sum_{y \in \mathbf{S}_{\text{outcome}}|_{\pi_B(x)}} \mathbb{P}_{AB}(X_{n+1} = y \mid X_n = x) = 1$. The probability distribution $\mathbb{P}_{AB}$ is selected by B by applying some rule (e.g., 'assign more probability to the most preferred outcome') to the H-digraph of the opponent. The results of the paper are independent of the specific rule used and so we leave it unspecified.

Player B can choose her own actions based on her preferences in any way she sees fit. For later use, We formally describe this via a probability distribution $\mathbb{P}_B$ on any action $\pi_B(y)$ which changes the outcome from x to y. Note that this can, in particular, be a vector with one entry of 1 and the rest 0, and that it can be re-selected at each round of the game. Since players only use the current state of the game to decide about their next action, the sequence of repeated outcomes of the game is a Markov chain, possibly time-varying as the H-digraph of A can evolve with time.

B. Notions of deception

Here, we introduce several definitions to capture different forms of deception. The first definition encodes a situation where the deceiver wishes to make sure that the mark will not take a certain action from a given outcome.

Definition 3.2 (Edge-deceivability): Suppose players A and B play sequentially a hypergame $H^2 = \{H^0_A, H^1_B\}$, with $H^0_{AB} = H^0_A$. An edge $(x, y) \in \mathcal{E}_{H^0_A}$, $\pi_B(x) = \pi_B(y)$, is *deceivable* by B in H^0_A from $x_0 \in \mathbf{S}_{\text{outcome}}$ if there exists an admissible sequence of outcomes $\sigma_B = (x_0, x_1, x_2, \ldots, x_{2k+1})$, $k \in \mathbb{Z}_{\geq 0}$, where

(i) $(x_{2i-1}, x_{2i}) \in \mathbf{Sw}^A_{x_{2i-2},x_{2i-1}} \circ \cdots \circ \mathbf{Sw}^A_{x_0,x_1}(\mathcal{E}_{H^0_A})$ and
(ii) $T_{\mathbb{P}_{AB}}(x_{2i}, x_{2i-1}) > 0$,

for all $i \in \{1, \ldots, k\}$, such that $(x, y) \notin \mathbf{Sw}^A_{x,\sigma_B}(\mathcal{E}_{H^0_A})$. We refer to σ_B a *deceiving sequence* and say that 'B deceives A' if the hypergame evolves according to σ_B. We denote by $E^{B,x_0}_{\text{dec}}(H^0_A) \subseteq \mathcal{E}_{H^0_A}$ the set of all deceivable edges by B in H^0_A from x_0. We say that (x, y) is *surely deceivable* by B in H^0_A from x_0 if it is deceivable with probability one and we denote the set of all such edges by $E^{B,x_0}_{\text{sdec}}(H^0_A) \subseteq \mathcal{E}_{H^0_A}$.

Let us elaborate more on the properties of the deceiving sequence σ_B in the above definition. (i) states that A uses her updated H-digraph and takes an action to shift the outcome to a sanction-free improvement. (ii) states that B perceives a positive probability to the actions of A contained in σ_B. There is an abuse of notation due to the fact that $\mathbb{P}_{AB}$ can change with the evolution of the H-digraph. Also, here we have assumed that B takes the last action. This is without loss of generality; if the edge (x, y) is deceived by B, it remains deceived afterwards, unless B reveals new information.

Definition 3.3: (Strong edge-deceivability): The edge (x, y) is *strong deceivable* by B in H_A^0 if it is deceivable from any outcome $x_0 \in \mathbf{S}_{\text{outcome}}$ and is *surely strong deceivable* if it is strong deceivable with probability one. The set of strong deceivable and surely strong deceivable edges are denoted, respectively, by $E^B_{\text{stdec}}(H_A^0)$ and $E^B_{\text{sstdec}}(H_A^0)$.

Note that Definitions 3.2 and 3.3 are a stepping stone towards the deceiver being able to make sequentially rational an (in principle) unstable outcome for the mark. In this paper, we restrict our attention to the problem of edge-deceivability.

Lemma 3.4 (Deceivability inclusions): For all $x_0 \in \mathbf{S}_{\text{outcome}}$, the following inclusions hold

$$E^B_{\text{sstdec}}(H_A^0) \subseteq E^{B,x_0}_{\text{sdec}}(H_A^0),\ E^B_{\text{stdec}}(H_A^0) \subseteq E^{B,x_0}_{\text{dec}}(H_A^0).$$

We are now ready to formally state the problem we set out to study. Consider $H^2 = \{H_A^0, H_B^1\}$, with $H_{AB}^0 = H_A^0$. We wish to provide answers to the following two problems:

(i) given $(x, y) \in \mathcal{E}_{H_A^0}$, with $\pi_B(x) = \pi_B(y)$, what are the set of outcomes $x_0 \in \mathbf{S}_{\text{outcome}}$ from which the edge is (surely/strongly) deceivable by B?

(ii) given an answer to the previous question, design an strategy that B can implement in order to deceive A.

IV. When is it possible to perform deception?

In this section, we identify a necessary condition and a sufficient condition for the notions of deceivability introduced in Section III-B. We also define a class of admissible sequences of outcomes, termed stealthy, and characterize conditions for deceivability that are both necessary and sufficient when the allowable sequences are restricted to this family.

A. Necessary and sufficient conditions for deceivability

We first identify a necessary condition for deceivability.

Lemma 4.1: (Necessary condition for edge-deceivability): Let $x_0 \in \mathbf{S}_{\text{outcome}}$ and assume $(x, y) \in E^{B,x_0}_{\text{dec}}(H_A^0)$. Then

$$\mathsf{H}^A_{\text{dec}}(x, y) = \{u \in \mathbf{S}_{\text{outcome}}|_{\pi_A(y)} \mid u \prec_{\mathrm{P}_{AA}} x\} \neq \emptyset.$$

We also have the following result for sure deceivability.

Lemma 4.2: (Sufficient conditions for surely deceivability): Let $(x, y) \in \mathcal{E}_{H_A^0}$, $\pi_B(x) = \pi_B(y)$, and suppose $\mathsf{H}^A_{\text{dec}}(x, y) \neq \emptyset$. Then $(x, y) \in E^{B,\tilde{y}}_{\text{sdec}}(H_A^0)$, for all $\tilde{y} \in \mathsf{T}^A_{\text{dec}}(y) = \{w \in \mathbf{S}_{\text{outcome}}|_{\pi_A(y)} \mid w \succeq_{\mathrm{P}_{BA}} y\}$.

B. Stealthy sequences of actions

If B takes an action not aligned with the perception of A, and A updates her perception (using for instance swap learning), then the structure of the H-digraph of A will change. Therefore, for B, the complexity of selecting a sequence of actions to deceive the opponent greatly grows with the length of the sequence. Here, instead, we focus on a particular family of sequences, which we term *stealthy*, that B can employ to achieve her goal without revealing any information to A, up to the moment that the 'deceiving action' takes place. Let us formally define this notion.

Definition 4.3: (Stealthy sequence): An admissible sequence of outcomes $\sigma_B = (x_0, x_1, \ldots, x_k)$, is *stealthy* if $(x_i, x_{i+1}) \in \mathcal{E}_{H_A^0}$, for all $i < k-1$, and $(x_{k-1}, x_k) \notin \mathcal{E}_{H_A^0}$.

A consequence of the definition is that, if $\sigma_B = (x_0, x_1, \ldots, x_k)$, $k \in \mathbb{Z}_{\geq 1}$, is a stealthy sequence, then $\mathbf{Sw}^A_{x_{i-1},x_i}(\mathcal{E}_{H_A^0}) = \mathcal{E}_{H_A^0}$, for all $i \in \{1, \ldots, k-1\}$, i.e., A does not see her perception contradicted when the outcomes of the game correspond to σ_B. Moreover, at the last outcome, $\mathbf{Sw}^A_{x_{k-1},x_k}(\mathcal{E}_{H_A^0}) = \mathbf{Sw}^A_{x_0,\sigma_B}(\mathcal{E}_{H_A^0}) \neq \mathcal{E}_{H_A^0}$.

Note that with this definition, the probability distribution $\mathbb{P}_{AB}$ does not change when the games is played according to a stealthy sequence. This definition motivates us to define the set $\mathscr{S}^{\mathbb{P}_{AB}}_{\text{adm}}(\mathbf{S}_{\text{outcome}}) \subseteq \mathscr{S}_{\text{adm}}(\mathbf{S}_{\text{outcome}})$ with

$$\mathscr{S}^{\mathbb{P}_{AB}}_{\text{adm}}(\mathbf{S}_{\text{outcome}}) = \{(x_0, x_1, x_2, \ldots) \in \mathscr{S}_{\text{adm}}(\mathbf{S}_{\text{outcome}}) \mid T_{\mathbb{P}_{AB}}(x_{i+1}, x_i) > 0, \forall i \in \mathbb{Z}_{\geq 0}, \pi_B(x_i) = \pi_B(x_{i+1})\}.$$

If $\sigma \in \mathscr{S}^{\mathbb{P}_{AB}}_{\text{adm}}(\mathbf{S}_{\text{outcome}})$, we call σ a $\mathbb{P}_{AB}$-*admissible sequence*. With this definition, B perceives a positive probability to the actions of A contained in σ. From now on, when we use the term 'stealthy sequence' we mean '$\mathbb{P}_{AB}$-admissible stealthy sequence'.

Theorem 4.4: (Necessary and sufficient conditions for deceivability via stealthy sequences): Let $x_0 \in \mathbf{S}_{\text{outcome}}$ and $(x, y) \in \mathcal{E}_{H_A^0}$, $\pi_B(x) = \pi_B(y)$. The following are equivalent:

(i) (x, y) is deceivable from x_0 via a stealthy sequence;

(ii) $\mathsf{H}^A_{\text{dec}}(x, y) \neq \emptyset$ and

$$\mathcal{T}^A_{\text{dec}}(y, x_0) = \mathsf{T}^A_{\text{dec}}(y) \cap \big(\{x_0\} \cup \mathcal{R}_{T_{\mathbb{P}_{AB}} T_{\mathbb{P}_B}}(x_0)\big) \neq \emptyset,$$

for a probability distribution $\mathbb{P}_B$ such that $\mathbb{P}_B(X_{n+1} = z \mid X_n = r) > 0$ for any $(r, z) \in \mathcal{E}_{H_A^0}$.

The choice of $\mathbb{P}_B$ in Theorem 4.4(ii) ensures that all actions of B are considered when determining if a stealthy sequence exists to deceive A. Once such sequence is found, B will assign probability one to each of the actions for her prescribed in the sequence (cf. Section V).

Theorem 4.4 shows that, given $x_0 \in \mathbf{S}_{\text{outcome}}$, any action of B from $\mathcal{T}^A_{\text{dec}}(y, x_0)$ to $\mathsf{H}^A_{\text{dec}}(x, y)$ removes the edge (x, y) from the H-digraph $\mathcal{G}_{H_A^0}$. Thus, if these two sets are nonempty, finding a stealthy sequence is equivalent, by definition of $\mathcal{T}^A_{\text{dec}}(y, x_0)$, to finding a path in $\mathcal{G}_{H_A^0}$ that reaches $\mathcal{T}^A_{\text{dec}}(y, x_0)$ from x_0. One can characterize the set of all initial outcomes from which the edge (x, y) is deceivable as

$$\mathcal{I}^A_{\text{dec}}(x, y) = \{x_0 \in \mathbf{S}_{\text{outcome}} \mid \mathsf{H}^A_{\text{dec}}(x, y), \mathcal{T}^A_{\text{dec}}(y, x_0) \neq \emptyset\}.$$

V. The `worst-case max-strategy`

Here, we provide an algorithmic approach that can be used by B to determine a stealthy sequence to deceive A. Consider the scenario described in Section III. Suppose at time $t \geq 0$ the outcome of the 2-person 2-level hypergame is $\mathbf{x}(t)$. Without loss of generality, assume that B takes actions when $t \in 2\mathbb{Z}_{\geq 0}$ and A takes actions when $t \in 2\mathbb{Z}_{\geq 0}+1$. In this situation, Theorem 4.4 characterizes the edges of the H-digraph of A that are deceivable by B via a stealthy sequence. To model the fact that the outcome of the hypergame is influenced by the actions of A, let us introduce the map $\Phi_{\mathbb{P}_{AB}} : \mathscr{S}^{\mathbb{P}_{AB}}_{\text{adm}}(\mathbf{S}_{\text{outcome}}) \to \mathbb{R}$,

$$\Phi_{\mathbb{P}_{AB}}(x_0,\dots,x_k) = \sum_{\substack{i=0 \\ \pi_B(x_i)=\pi_B(x_{i+1})}}^{k-1} \ln\left(T_{\mathbb{P}_{AB}}(x_{i+1},x_i)\right). \quad (1)$$

This map captures the probability of reaching an outcome via a $\mathbb{P}_{AB}$-admissible sequence. In this scenario, after making sure that the necessary condition for deception is satisfied, a reasonable strategy for B at each round is to take an action that maximizes the minimum probability of achieving the deception goal. We call this strategy the `worst-case max-strategy` and formally describe it in Algorithm 1.

Algorithm 1: `worst-case max-strategy`

Input: $\mathcal{G}_{H^0_A}$, $\mathbb{P}_{AB}$, $(x,y) \in \mathcal{E}_{H^0_A}$, $x_0 \in \mathbf{S}_{\text{outcome}}$, $\mathcal{N}^{\text{out}}(x_0) \cap \mathbf{S}_{\text{outcome}}|_{\pi_A(x_0)} \neq \emptyset$
Initialization: $\alpha^{\text{maxmin}} = -\infty$, $\sigma_B = \emptyset$, $\mathbf{x}(0) = x_0$

check $\mathsf{H}^A_{\text{dec}}(x,y) \neq \emptyset$; else, announce (x,y) not deceivable
at time: $t \in 2\mathbb{Z}_{\geq 0}$
if $\mathbf{x}(t) \in \mathsf{T}^A_{\text{dec}}(y)$ **then**
    take action that makes $\mathbf{x}(t+1) \in \mathsf{H}^A_{\text{dec}}(x,y)$
else
    if $\sigma_B \neq \emptyset$ and $\mathbf{x}(t)$ is aligned with σ_B **then**
        take action prescribed by σ_B
    else
        foreach $w \in \mathbf{S}_{\text{outcome}}|_{\pi_A(\mathbf{x}(t))}$, $(\mathbf{x}(t), w) \in \mathcal{E}_{H^0_A}$ **do**
            $\alpha^{\text{min}} = +\infty$
            foreach $\tilde{y} \in \mathsf{T}^A_{\text{dec}}(y)$ **do**
                if there is path in $\mathcal{G}_{H^0_A}$ from w to $\tilde{y}$ **then**
                    find σ^A_A from w to $\tilde{y}$ minimizing $\Phi_{\mathbb{P}_{AB}}$
                    if $\Phi_{\mathbb{P}_{AB}}(\sigma^A_A) \leq \alpha^{\text{min}}$ **then**
                        $\alpha^{\text{min}} = \Phi_{\mathbb{P}_{AB}}(\sigma^A_A)$
                    end
                end
            end
            if $\alpha^{\text{min}} \neq +\infty$ and $\alpha^{\text{min}} \geq \alpha^{\text{maxmin}}$ **then**
                $\alpha^{\text{maxmin}} = \alpha^{\text{min}}$, $\eta = \sigma$
            end
        end
        if $\alpha^{\text{maxmin}} \neq -\infty$ **then**
            $\sigma_B = (\mathbf{x}(t), \eta)$ take action prescribed by σ_B
        else
            (x,y) is not deceivable from $\mathbf{x}(t)$
        end
    end
end

The rationale behind its name is made explicit next.

Lemma 5.1: (Algorithm 1 maximizes the minimum probability of deception): The following are equivalent:

(i) $\sigma_B = (x_0, x_1, x_2, \dots, x_{2k}) \in \mathscr{S}^{\mathbb{P}_{AB}}_{\text{adm}}(\mathbf{S}_{\text{outcome}})$, where $k \in \mathbb{Z}_{\geq 1}$, $x_{2k} \in \mathsf{T}^A_{\text{dec}}(y)$, and $(x_i, x_{i+1}) \in \mathcal{E}_{H^0_A}$ for $i \in \{0,\dots,2k-1\}$, is a minimizer of $\Phi_{\mathbb{P}_{AB}}$;
(ii) σ_B corresponds to the longest path from x_0 to $x_{2k} \in \mathsf{T}^A_{\text{dec}}(y)$, in $(\mathbf{S}_{\text{outcome}}, \mathcal{E}_{H^0_A}, \mathcal{A}_{H^0_A})$, where, for $i,j \in \{1,\dots|\mathbf{S}_{\text{outcome}}|\}$, $\mathcal{A}_{H^0_A})_{ij} = |\ln(T_{\mathbb{P}_{AB}}(z_j,z_i))|$, if $\pi_B(z_i) = \pi_B(z_j)$, and is zero otherwise.

Note that, in Lemma 5.1, (i) is equivalent to stating that σ_B is a minimizer of $\Pi^k_{i=1} T_{\mathbb{P}_{AB}}(x_{2i}, x_{2i-1})$, and (ii) implies that finding solutions to the `worst-case max-strategy` is equivalent to finding a longest path on a digraph.

Remark 5.2: (Complexity of Algorithm 1): The digraph $(\mathbf{S}_{\text{outcome}}, \mathcal{E}_{H^0_A}, \mathcal{A}_{H^0_A})$ was recently shown in [22] to be acyclic, and therefore, the problem of finding a longest path is well-posed and can be solved efficiently. •

Algorithm 1 is complete, in the following sense.

Theorem 5.3: (Surely deceivable edges via `worst-case max-strategy`): The edge $(x,y) \in \mathcal{E}_{H^0_A}$, $\pi_B(x) = \pi_B(y)$, is surely deceivable from $x_0 \in \mathbf{S}_{\text{outcome}}$ via a stealthy sequence of B iff $\mathsf{H}^A_{\text{dec}}(x,y) \neq \emptyset$ and either $x_0 \in \mathsf{T}^A_{\text{dec}}(y)$ or

$$\max_{x_1 \in \mathbf{S}_{\text{outcome}}|_{\pi_A(x_0)}} \min_{\sigma_B} \Phi_{\mathbb{P}_{AB}}(\sigma_B) = 0,$$

where $\sigma_B = (x_0, x_1, x_2, \dots, x_{2k}) \in \mathscr{S}^{\mathbb{P}_{AB}}_{\text{adm}}(\mathbf{S}_{\text{outcome}})$, $k \in \mathbb{Z}_{\geq 1}$, $x_{2k} \in \mathsf{T}^A_{\text{dec}}(y)$, $(x_i, x_{i+1}) \in \mathcal{E}_{H^0_A}$, $i \in \{0,\dots,2k-1\}$.

Remark 5.4 (Strong deceivability): The execution of the `worst-case max-strategy` from all the outcomes in $\mathbf{S}_{\text{outcome}}$ fully characterizes the set $\mathcal{I}^A_{\text{dec}}(x,y)$. Note that, by definition, $\mathcal{I}^A_{\text{dec}}(x,y) = \mathbf{S}_{\text{outcome}}$ iff (x,y) is strongly deceivable via a stealthy sequence. •

VI. An Example

Consider a 2-level $H^2 = \{H^0_A, H^1_B\}$ between A and B, with $H^0_{AB} = H^0_A$ and outcome set $\mathbf{S}_{\text{outcome}} = S_A \times S_B = \{1,\dots,50\}$, where S_A and S_B are the action sets of A and B, respectively, and $|S_A| = 5$ and $|S_B| = 10$. The preference vectors P_{AA} and P_{BA} are shown in Figure 1. The H-digraph

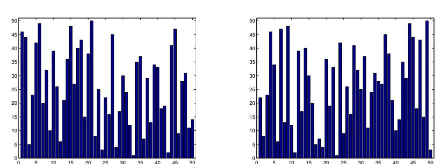

Fig. 1. Preference vectors P_{AA} (left) and P_{BA} (right). The horizontal axis shows the outcomes and the vertical axis shows the rank of outcomes.

$\mathcal{G}_{H^0_A}$ is shown in Figure 2(left). Regarding the actions of A, player B perceives that outcomes with lower rank in P_{AA} have higher probability of occurring. Formally, B assigns

$$T_{\mathbb{P}_{AB}}(j,i) = \frac{50 - \text{rank}(j, \mathrm{P}_{AA})}{\sum_{l \in \mathcal{N}^{\text{out}}(i) \cap \mathbf{S}_{\text{outcome}}|_{\pi_B(i)}} (50 - \text{rank}(l, \mathrm{P}_{AA}))},$$

to the event that the outcome changes from i to j by the action $\pi_A(j)$ of A, where $j \in \mathbf{S}_{\text{outcome}}|_{\pi_B(i)}$.

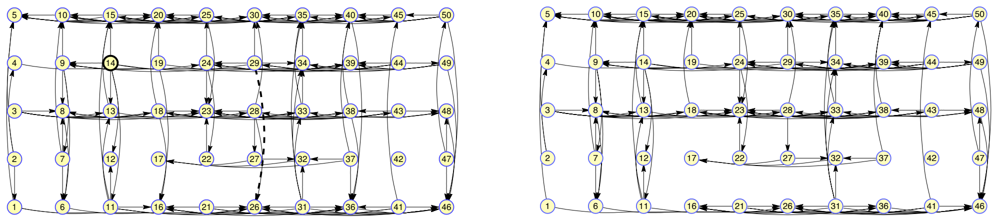

Fig. 2. H-digraphs $\mathcal{G}_{H_A^0}$ (left) and $\mathbf{Sw}_{36,11}^A(\mathcal{G}_{H_A^0})$ (right). Player A plays rows, B plays columns, and P_{AA} and P_{BA} are given in Figure 1.

Suppose the game initially starts at outcome $x_0 = 14$ and B wishes to deceive A by removing the edge $(29, 26) \in \mathcal{E}_{H_A^0}$ via a stealthy sequence. Since $\mathcal{H}_{\text{dec}}^A(29, 26) = \{11, 31, 41\}$, and thus non-empty, the necessary condition of Lemma 4.1 is satisfied. According to Theorem 4.4, we compute $\mathsf{T}_{\text{dec}}^A(26) = \{1, 6, 26, 36\}$. The actions of B from 14 aligned with A's H-digraph are $\mathcal{N}^{\text{out}}(14) \cap \mathbf{S}_{\text{outcome}}|_{\pi_A(14)} = \{9, 24, 39\}$. By executing the `worst-case max-strategy`, B finds that the action that maximizes the minimum probability of reaching any of the outcomes in $\mathsf{T}_{\text{dec}}^A(26)$ is $\pi_B(24)$, where she perceives that the repeated play of the game will reach outcome 36 via the path $\mathfrak{S} = (14, 24, 25, 40, 36)$, with probability 0.52. Note that, by definition, $36 \in \mathcal{T}_{\text{dec}}^A(26, 14)$. If the repeated play goes according to B's perception, after reaching 36, B takes an action that changes the outcome to any of the outcomes in $\mathcal{H}_{\text{dec}}^A(29, 26)$. e.g., if B chooses to take the action $\pi_B(11)$ (note that $(36, 11) \notin \mathcal{E}_{H_A^0}$), then A's H-digraph after updating her perception via swap learning is shown in Figure 2(right). If A takes an action not aligned with the sequence $\mathfrak{S}$ at any round, according to the `worst-case max-strategy`, B will recompute the stealthy sequence and take the ensuing action accordingly.

VII. Conclusions

We have studied scenarios of active deception in 2-person 2-level hypergames with asymmetric information. Using the properties of hypergames encoded in the notion of H-digraph, we have introduced formal notions that capture different forms of deception. We have provided a necessary condition and a sufficient condition for deceivability for the case when the deceiver might take actions that contradict the perception of her opponent about the game. When this is not the case, i.e., if the deceiver acts in a stealthy way and only takes actions aligned with her opponent's perception, we have fully characterized when deception is possible. Finally, we have introduced the `worst-case max-strategy` which maximizes the minimum probability that the deceiver achieves the deception goal. We have shown this algorithm to be complete. Future work will study efficient ways of performing outcome deceivability, the impact of signaling cost on the deceiver's strategies, and the challenging scenario of deception via non-stealthy strategies, where the H-digraph of the opponent might change by the action of the deceiver.

Acknowledgments

This work was supported by AFOSR FA9550-10-1-0499.

References

[1] R. J. Lewicki, D. M. Saunders, and B. Barry, *Negotiation*. New York: McGraw-Hill, 6nd ed., 2010.

[2] D. Teneketzis and D. A. Castañón, "Informational aspects of class of subjective games of incomplete information: static case," *Journal of Optimization Theory & Applications*, vol. 54, no. 2, pp. 413–422, 1987.

[3] V. P. Crawford, "Lying for strategic advantage: Rational and boundedly rational misrepresentation of intentions," *American Economic Review*, vol. 93, pp. 133–149, 2003.

[4] S. Mullainathan, J. Schwartzstein, and A. Shleifer, "Coarse thinking and persuasion," *Quarterly Journal of Economics*, vol. 123, no. 5, pp. 577–619, 2008.

[5] D. Ettinger and P. Jehiel, "A theory of deception," *American Economic Journal: Microeconomics*, vol. 2, pp. 1–20, 2010.

[6] V. J. Baston and F. A. Bostock, "Deception games," *International Journal of Game Theory*, vol. 17, pp. 129–134, 1988.

[7] K. T. Lee and K. L. Teo, "A game with distorted information," *Naval Research Logistics*, vol. 40, pp. 993–1001, 1993.

[8] N. M. Fraser and K. W. Hipel, *Conflict Analysis: Models and Resolutions*. Systems Science and Engineering, Oxford, UK: Elsevier, 1984.

[9] M. Wang, K. W. Hipel, and N. M. Fraser, "Solution concepts in hypergames," *Applied Mathematics and Computation*, vol. 34, pp. 147–171, 1989.

[10] R. Vane and P. Lehner, "Using hypergames to increase planned payoff and reduce risk," *Autonomous Agents and Multi-Agent Systems*, vol. 5, pp. 365–380, 2002.

[11] P. Bernhard, A. L. Colomb, and G. Papavassilopoulos, "Rabbit and hunter game: Two discrete stochastic formulations," *International Journal of Applied Mathematics and Computer Science*, vol. 13, pp. 205–225, 1987.

[12] G. J. Olsder and G. P. Papavassilopoulos, "About when to use a searchlight," *Journal of Mathematical Analysis and Applications*, vol. 136, pp. 466–487, 1988.

[13] D. A. Castañón, P. R. Chandler, and M. Pachter, "A game of deception," in *IEEE Conf. on Decision and Control*, (Paradise Island, Bahamas), pp. 3364–3369, 2004.

[14] J. P. Hespanha, "Application and value of deception," in *Adversarial Reasoning: Computational Approaches to Reading the Opponent's Mind* (A. Kott and W. M. McEneaney, eds.), (Boca Raton, FL), pp. 145–165, Chapman and Hall/CRC, 2007.

[15] D. Li and J. B. C. Jr., "Information, decision-making and deception in games," *Decision Support Systems*, vol. 47, pp. 518–527, 2009.

[16] W. M. McEneaney, "Some classes of imperfect information finite state space stochastic games with finite-dimensional solutions," *Applied Mathematics and Optimization*, vol. 50, no. 2, pp. 87–118, 2004.

[17] W. M. McEneaney and R. Singh, "Robustness against deception," in *Adversarial Reasoning: Computational Approaches to Reading the Opponent's Mind* (A. Kott and W. McEneaney, eds.), (Boca Raton, FL), pp. 167–207, Chapman and Hall/CRC, 2007.

[18] S. Meyn and R. L. Tweedie, *Markov Chains and Stochastic Stability*. Cambridge, UK: Cambridge University Press, 2nd ed., 2009.

[19] B. Gharesifard and J. Cortés, "Evolution of players' misperceptions in hypergames under perfect observations," *IEEE Transactions on Automatic Control*, 2010. Submitted.

[20] D. M. Kreps and R. Wilson, "Sequential equilibria," *Econometrica*, vol. 50, no. 4, pp. 863–894, 1982.

[21] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*. SIAM, 2 ed., 1999.

[22] B. Gharesifard and J. Cortés, "Learning of equilibria and misperceptions in hypergames with perfect observations," in *American Control Conference*, (San Francisco, California), pp. 4045–4050, 2010.