Game Semantics for the Geiger-Paz-Pearl Axioms of Independence

Pavel Naumov and Brittany Nicholls

Department of Mathematics and Computer Science
McDaniel College, Westminster, Maryland 21157, USA

{pnaumov,brn002}@mcdaniel.edu

Abstract. The paper analyzes interdependencies between strategies of players in a Nash equilibrium using independence relation between two sets of players. A sound and complete axiomatization of this relation is given. It has been shown previously that the same axiomatic system describes independence in probability theory, information flow, and concurrency theory.

1 Introduction

In this paper, we show that the same logical principles describe independence in four different settings: probability, information flow, concurrency, and game theory.

Independence in Probability Theory. Two events are called independent in probability theory if the probability of their intersection is equal to the product of their probabilities. It is believed [6] that this notion was first introduced by de Moivre [2, 3]. If $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$ are two disjoint sets of random variables with finite ranges of values, then these two sets of variables are called independent if for any values $v_1, \dots, v_n$ and any values $w_1, \dots, w_m$, events $\bigwedge_{i \le n}(a_i = v_i)$ and $\bigwedge_{i \le m}(b_i = w_i)$ are independent. We write $A \parallel B$ to denote this relation. This definition can be generalized to independence of sets of variables with infinite ranges through the independence of appropriate σ-algebras.

A complete axiomatization of propositional properties of the independence relation between two sets of random variables was given by Geiger, Paz, and Pearl[1] [7]:

1. Empty Set: $A \parallel \varnothing$,
2. Symmetry: $A \parallel B \to B \parallel A$,
3. Monotonicity: $A \parallel B, C \to A \parallel B$,
4. Exchange: $A, B \parallel C \to (A \parallel B \to A \parallel B, C)$,

where here and everywhere below A, B means the union of sets A and B. Furthermore, Studený [13] showed that *conditional* probabilistic independence does not have a complete finite axiomatization.

[1] The axiom names shown here are ours.

Independence in Information Flow. Sutherland [14] introduced a relation between two pieces of information, which we will call "secrets", that later became known as the "nondeducibility" relation. Two secrets are in this relation if any possible value of the first secret is consistent with any possible value of the second secret. More and Naumov [11] generalized this relation to a relation $A \parallel B$ between two sets of secrets and called it independence: sets of secrets A and B are independent if each possible combination of the values of secrets in A is consistent with each possible combination of the values of secrets in B. More and Naumov [11] have shown that the same system of Geiger-Paz-Pearl axioms is sound and complete with respect to defined this way semantics of secrets[2].

Cohen [1] presented a related notion called *strong dependence*. More recently, Halpern and O'Neill [8] introduced f-secrecy to reason about multiparty protocols. In our notation, f-secrecy is a version of the nondeducibility predicate whose left or right side contains a certain function of the secret rather than the secret itself. More, Naumov, and Donders also axiomatized a variation of the independence relation between secrets over graphs [9, 5] and hypergraphs [10].

Independence in Concurrency Theory. The third semantics for the Geiger-Paz-Pearl axioms of independence was proposed by More, Naumov, and Sapp [12]. Under this semantics, independence is interpreted as "non-interference" between two sets of concurrent processes. A set of processes A interferes with a set of processes B if these two sets can reach a deadlocked state where either set A or set B is not internally deadlocked. For example, if p_1, p_2, p_3, p_4, p_5 are five philosophers seating at a table with five forks in the Dijkstra's [4] dining philosopher problem, then neither set $\{p_1, p_2, p_3\}$ nor set $\{p_4, p_5\}$ can deadlock by itself (if the other philosophers leave the table). However, the complete set $\{p_1, p_2, p_3, p_4, p_5\}$ can deadlock. Thus, using our notations we can say that statement $\{p_1, p_2, p_3\} \parallel \{p_4, p_5\}$ is false.

More, Naumov, and Sapp [12] have shown that the same system of axioms 1-4 is sound and complete with respect to this concurrency semantics.

Independence in Game Theory. In this paper we consider interdependencies between strategy choices of players in a multi-player game. If no assumptions are made about the players, then each of them can choose any available strategy and, thus, there is no interdependency between these choices. If, however, a player is assumed to be rational, then her choice of strategy might depend on the choices made by the other players. There are different possible ways to formally capture the rationality of the player. In this paper we express rationality of all players in the game through the requirement that strategies of all players are in a Nash equilibrium.

For example, in the United States, people walk on the right side of a hallway or a sidewalk. In Japan, however, people walk on the left side. There is no

[2] As long as the same secret can not appear simultaneously on the left and right hand side of the independence symbol. Otherwise, one more axiom should be added to achieve completeness.

law enforcing this in either of the two countries, but walking on the same side as the other pedestrians is a Nash equilibrium in the multi-player coordination game played by the pedestrians in both of these countries. By observing a single pedestrian in a hallway, one can predict the side of the hallway the next pedestrian will walk on, without a priori knowledge of the countries in which the observation takes place. This is an example of an interdependency between strategies in Nash equilibria of a strategic game.

We say that two players in a multi-player strategy game are independent if knowledge of the first player's strategy in a Nash equilibrium does not reveal anything about the strategy of the second player in the same equilibrium. In other words, for any choice of a strategy for the first player that appears in at least one Nash equilibrium and for any choice of a strategy for the second player that appears in at least one Nash equilibrium, there is a Nash equilibrium that uses both of these strategies. Independence can be defined not just between two single players, but also between two *sets* of players. We say that two disjoint sets of players A and B are independent if for any two Nash equilibria e_1 and e_2 of the game, there is a Nash equilibrium e such that (i) each player in set A uses the same strategy in equilibria e_1 and e and (ii) each player in set B uses the same strategy in equilibria e_2 and e. We denote this relation by $A \parallel B$.

In this paper we will show that the same axioms 1-4 give a sound and complete axiomatization of properties of independence between sets of players in strategic games. It is easy to see that any strategic game could be viewed as an information flow protocol. Thus, soundness of these axioms in the game setting trivially follows from their soundness in the information flow setting. The main technical contribution of this work is the proof of completeness. More and Naumov [11] have shown that if a formula is not provable from axioms 1-4, then there is an information flow protocol for which this formula is false. In this paper we show that such protocol can be described in terms of a strategic game. The significant implication of this result is that *the same non-trivial set of axioms captures the properties of independence in four different settings: probability, information flow, concurrency, and game theory.*

In the conclusion we discuss what appears to be a more general independence relation $A_1 \parallel A_2 \parallel \cdots \parallel A_n$ between several sets of players. We will show, however, that this relation can be expressed through independence between just two sets of players.

2 Semantics

Strategic games are usually defined by specifying for each player either a total preference order on the outcomes or, equivalently, a pay-off function on the outcomes. We have chosen the second approach since it results in a slightly simpler presentation of our main result.

Definition 1. *A strategic game is a triple* $G = (P, \{S_p\}_{p \in P}, \{u_p\}_{p \in P})$*, where*

1. *P is a non-empty finite set of "players".*

2. *S_p is a non-empty set of "strategies" of a player $p \in P$. Elements of the cartesian product $\prod_{p \in P} S_p$ are called "strategy profiles".*
3. *u_p is a "pay-off" function from strategy profiles into the set of real numbers.*

For any tuple $a = \langle a_i \rangle_{i \in I}$, any $i_0 \in I$ and any value b, by $\langle a_i \rangle_{i \in I}[i_0 \mapsto b]$ we mean the tuple a in which i_0-th component is changed from a_{i_0} to b. In the game theory literature the same modified tuple is sometimes denoted by (a_{-i_0}, b).

Definition 2. *Nash equilibrium of a strategic game $G = (P, \{S_p\}_{p \in P}, \{u_p\}_{p \in P})$, is a strategy profile $\langle s_p \rangle_{p \in P}$ such that*

$$u_p(\langle s_p \rangle_{p \in P}[p_0 \mapsto s_0]) \leq u_p(\langle s_p \rangle_{p \in P}) \tag{1}$$

for any $p_0 \in P$ and any $s_0 \in S_{p_0}$.

Alternatively, one can define *strict* Nash equilibrium by replacing relation $\leq$ in inequality (1) with strict inequality sign $<$. The soundness and completeness theorems in this paper are true for both types of equilibria. The set of all Nash equilibria of a game G is denoted by $NE(G)$. Next, we formally define the set of all formulas that we consider.

Definition 3. *For any finite set of players P, the set of formulas $\Phi(P)$ is defined recursively: (i) $\bot \in \Phi(P)$, (ii) $(A \parallel B) \in \Phi(P)$, where A and B are two disjoint subsets of P, (iii) $\phi \to \psi \in \Phi(P)$, where $\phi, \psi \in \Phi(P)$.*

If $x = \langle x_i \rangle_{i \in I}$ and $y = \langle y_i \rangle_{i \in I}$ are two tuples such that $x_a = y_a$ for any $a \in A$, then we write $x \equiv_A y$. We use this notation to define truth relation $G \vDash \phi$ between a game G and a formula ϕ:

Definition 4. *For any game $G = (P, \{S_p\}_{p \in P}, \{u_p\}_{p \in P})$ and any formula $\phi \in \Phi(P)$, binary relation $G \vDash \phi$ is defined as follows:*

1. *$G \nvDash \bot$,*
2. *$G \vDash \phi \to \psi$ if and only if $G \nvDash \phi$ or $G \vDash \psi$,*
3. *$G \vDash A \parallel B$ if and only if for any $e_1, e_2 \in NE(G)$ there is $e \in NE(G)$ such that $e_1 \equiv_A e \equiv_B e_2$.*

The third part of the above definition is the key definition of this paper. It formally specifies independence of two sets of players in a strategic game.

3 Axioms

Definition 5. *The logic of information flow, in addition to propositional tautologies and the Modus Ponens inference rule, consists of the following axioms:*

1. *Empty Set: $A \parallel \varnothing$,*
2. *Symmetry: $A \parallel B \to B \parallel A$,*
3. *Monotonicity: $A \parallel B, C \to A \parallel B$,*
4. *Exchange: $A, B \parallel C \to (A \parallel B \to A \parallel B, C)$.*

Recall from the introduction that these axioms first appeared in a work on independence of random variables in probability theory by Geiger, Paz, and Pearl [7].

4 Soundness

Theorem 1. *For any finite set of parties P and any $\phi \in \Phi(P)$, if $\vdash \phi$, then $G \vDash \phi$ for any game $G = (P, \{S_p\}_{p\in P}, \{u_p\}_{p\in P})$.*

Proof. It will be sufficient to verify that $G \vDash \phi$ for each axiom ϕ of the logic of information flow. Soundness of the Modus Ponens rule is trivial.

Empty Set Axiom. Consider any two Nash Equilibria $e_1, e_2 \in NE(G)$. Let $e = e_2$. It is easy to see that $e \equiv_\varnothing e_1$ and $e \equiv_A e_2$.

Monotonicity Axiom. Consider any two Nash Equilibria $e_1, e_2 \in NE(G)$. If $e \equiv_{A,B} e_1$ and $e \equiv_C e_2$, then $e \equiv_A e_1$ and $e \equiv_C e_2$.

Exchange Axiom. Consider any two Nash Equilibria $e_1, e_2 \in NE(G)$. By the assumption that $A \parallel B$, there is a Nash equilibrium $e_3 \in NE(G)$ such that $e_3 \equiv_A e_1$ and $e_3 \equiv_B e_2$. Since $D \parallel C$, there is a Nash equilibrium $e_4 \in NE(G)$ such that $e_4 \equiv_D e_2$ and $e_4 \equiv_C e_1$. Finally, by the assumption the $A, B \parallel C, D$, there is a Nash equilibrium $e \in NE(G)$ such that $e \equiv_{A,B} r_e$ and $e \equiv_{C,D} e_4$. Thus, $e \equiv_A e_3 \equiv_A e_1$, $e \equiv_C e_4 \equiv_C e_1$, $e \equiv_B e_3 \equiv_B e_2$, and $e \equiv_D e_4 \equiv_D e_2$. Therefore, $e \equiv_{A,C} e_1$ and $e \equiv_{B,D} e_2$. □

5 Completeness

In this section we will prove the completeness of the Geiger-Paz-Pearl axioms with respect to the strategic game semantics. This result is stated in Theorem 2. We start, however, with a sequence of lemmas in which we assume a fixed finite set of parties P and a fixed maximal consistent set of formulas $X \subseteq \Phi(P)$.

5.1 Critical Sets

The key to understanding axioms 1-4 is the notions of critical pair and critical set. Below is their combined definition and their basic properties. Later we will define a separate strategic game for each critical subset of P.

Definition 6. *A set $C \subseteq P$ is called critical if there is a disjoint partition $C_1 \sqcup C_2$ of C, called a "critical partition", such that*

1. $X \nvdash C_1 \parallel C_2$,
2. $X \vdash C_1 \cap D \parallel C_2 \cap D$, *for any* $D \subsetneq C$.

Lemma 1. *Any critical partition is a non-trivial partition.*

Proof. It will be sufficient to prove that for any set A, we have $X \vdash A \parallel \varnothing$ and $X \vdash \varnothing \parallel A$. The first statement is an instance of the Empty Set axiom, the second statement follows from the Empty Set and the Symmetry axioms. □

Lemma 2. *$X \nvdash A \parallel B$, for any non-trivial (but not necessarily critical) partition $A \sqcup B$ of a critical set C.*

Proof. Suppose $X \vdash A \parallel B$ and let $C_1 \sqcup C_2$ be a critical partition of C. By the Monotonicity and Symmetry axioms, $X \vdash A \cap C \parallel B \cap C$. Thus,

$$X \vdash A \cap C_1, A \cap C_2 \parallel B \cap C_1, B \cap C_2. \tag{2}$$

Since $A \sqcup B$ is a non-trivial partition of C, sets A and B are both non-empty. Thus, $A \subsetneq C$ and $B \subsetneq C$. Hence, by the definition of a critical set, $X \vdash A \cap C_1 \parallel A \cap C_2$ and $X \vdash B \cap C_1 \parallel B \cap C_2$.

Note that $A \cap C$ is not empty since $A \sqcup B$ is a non-trivial partition of C. Thus, either $A \cap C_1$ or $A \cap C_2$ is not empty. Without loss of generality, assume that $A \cap C_1 \neq \varnothing$. From (2) and our earlier observation that $X \vdash A \cap C_1 \parallel A \cap C_2$, the Exchange axiom yields

$$X \vdash A \cap C_1 \parallel A \cap C_2, B \cap C_1, B \cap C_2.$$

By the Symmetry axiom,

$$X \vdash A \cap C_2, B \cap C_1, B \cap C_2 \parallel A \cap C_1. \tag{3}$$

The assumption $A \cap C_1 \neq \varnothing$ implies that $(A \cap C_2) \cup (B \cap C_1) \cup (B \cap C_2) \subsetneq C$. Hence, by the definition of a critical set,

$$X \vdash B \cap C_1 \parallel A \cap C_2, B \cap C_2.$$

By Symmetry axiom,

$$X \vdash A \cap C_2, B \cap C_2 \parallel B \cap C_1.$$

From (3) and the above statement, using the Exchange axiom,

$$X \vdash A \cap C_2, B \cap C_2 \parallel A \cap C_1, B \cap C_1.$$

Since $A \sqcup B$ is a partition of C, we can conclude that $X \vdash C_2 \parallel C_1$. By the Symmetry axiom, $X \vdash C_1 \parallel C_2$, which contradicts the assumption that $C_1 \sqcup C_2$ is a critical partition. □

Lemma 3. *For any two disjoint subsets $A, B \subseteq P$, if $X \nvdash A \parallel B$, then there is a critical partition $C_1 \sqcup C_2$, such that $C_1 \subseteq A$ and $C_2 \subseteq B$.*

Proof. Consider the partial order $\preceq$ on set $2^A \times 2^B$ such that $(E_1, E_2) \preceq (F_1, F_2)$ if and only if $E_1 \subseteq F_1$ and $E_2 \subseteq F_2$. Define

$$\mathcal{E} = \{(E_1, E_2) \in 2^A \times 2^B \mid X \nvdash E_1 \parallel E_2\}.$$

$X \nvdash A \parallel B$ implies that $(A, B) \in \mathcal{E}$. Thus, $\mathcal{E}$ is a non-empty finite set. Take (C_1, C_2) to be a minimal element of set $\mathcal{E}$ with respect to partial order $\preceq$. □

5.2 Parity Game

For any subset $Q \subseteq P$, we define "parity" game $PG(Q)$. Later we will consider such games only for Q which are critical subsets of P. For now, however, Q is just an arbitrary subset of P.

We start with an informal description of the parity game. Players in set Q will be referred to as "active" players, since they will be able to influence outcome of the game. Players in the set $P \setminus Q$ are "passive": they get a pay-off, but can not influence its amount. Each active player picks an integer number. If the sum of all picked numbers is even, then pay-off of each player in set P is zero. If the sum of all picked numbers is odd, then each player in the set P gets one dollar.

In the formalization of this game below, we assume that players only pick numbers from the set $\{0, 1\}$ and that passive players always pick number 0.

Definition 7. *For any set of parties $Q \subseteq P$, by parity game $PG(Q)$ we mean game $(P, \{S_p\}_{p\in P}, \{u_p\}_{p\in P})$ such that*

1. *set of strategies of party $p \in P$ is*

$$S_p = \begin{cases} \{0,1\} & \text{if } p \in Q, \\ \{0\} & \text{otherwise.} \end{cases}$$

2. *pay off function u_p is the same for all players $p \in P$. We denote it simply by u. Value of $u(\langle s_p\rangle_{p\in P})$ is either 0 or 1 in such a way that*

$$u(\langle s_p\rangle_{p\in P}) \equiv \sum_{p\in P} s_p \pmod 2.$$

Lemma 4.

$$NE(PG(Q)) = \{\langle s_p\rangle_{p\in P} \in \prod_{p\in P} S_p \mid \sum_{p\in P} s_p \equiv 1 \pmod 2\}.$$

Proof. Follows from Definition 2 and Definition 7. □

Lemma 5. *If set Q is not empty, then game $PG(Q)$ has at least one Nash equilibrium.*

Proof. Let $q_0 \in Q$. Consider strategy profile $\langle e_p\rangle_{p\in P}$ such that

$$e_p = \begin{cases} 1 & \text{if } p = q_0, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 4, $\langle e_p\rangle_{p\in P} \in NE(PG(Q))$. □

Lemma 6. *If A and B are two disjoint subsets of Q, then $PG(Q) \not\models A \parallel B$ if and only if $A \sqcup B$ is a non-trivial partition of the set Q.* □

Proof. ($\Rightarrow$) : Suppose that $A \sqcup B$ is not a non-trivial partition of Q. There are three possible cases to consider:
Case I: A is empty. Thus, $PG(P) \vDash A \parallel B$ due to soundness of the Empty Set and Symmetry axioms (See Theorem 1).
Case II: B is empty. Thus, $PG(P) \vDash A \parallel B$ due to soundness of the Empty Set axiom.
Case III: there is $q_0 \in Q \setminus (A \cup B)$. Let e', e'' be any two Nash equilibria of the game $PG(Q)$. We will show that there is $e \in NE(PG(Q))$ such that $e' \equiv_A e \equiv_B e''$. Indeed, consider strategy profile $\langle e_p \rangle_{p \in P}$ such that

$$e_p \equiv \begin{cases} e'_p & \text{if } p \in A, \\ e''_p & \text{if } p \in B, \\ 1 + \sum_{a \in A} e'_a + \sum_{b \in B} e''_b & \text{if } p = q_0, \\ 0 & \text{otherwise.} \end{cases} \pmod 2$$

Note that

$$\sum_{p \in P} e_p = e_{q_0} + \sum_{a \in A} e_a + \sum_{b \in B} e_b \equiv 1 + \sum_{a \in A} e'_a + \sum_{b \in B} e''_b + \sum_{a \in A} e'_a + \sum_{b \in B} e''_b \equiv 1 \pmod 2.$$

Therefore, by Lemma 4, $e \in NE(PG(Q))$.
($\Leftarrow$) : Suppose that $PG(P) \vDash A \parallel B$ and $A \sqcup B$ is a non-trivial partition of Q. Let $a_0 \in A$ and $b_0 \in B$. Consider strategy profiles $e^A = \langle e^A_p \rangle_{p \in P}$ and $e^B = \langle e^B_p \rangle_{p \in P}$ such that

$$e^A_p \equiv \begin{cases} 1 \text{ if } p = a_0, \\ 0 \text{ otherwise} \end{cases}$$

and

$$e^B_p \equiv \begin{cases} 1 \text{ if } p = b_0, \\ 0 \text{ otherwise.} \end{cases}$$

By Lemma 4, $e^A, e^B \in NE(PG(Q))$. By assumption $PG(Q) \vDash A \parallel B$ there must be $e \in NE(PG(Q))$ such that $e^A \equiv_A e \equiv_B e^B$. Since $A \sqcup B$ is a partition of Q, we have

$$\sum_{p \in P} e_p = \sum_{a \in A} e_a + \sum_{b \in B} e_b = \sum_{a \in A} e^A_a + \sum_{b \in B} e^B_b = e^A_{a_0} + e^B_{b_0} = 1 + 1 \equiv 0 \pmod 2.$$

Contradiction with Lemma 4. □

5.3 Game Composition

Informally, by a composition of several games we mean a game in which each of the composed games is played independently. Pay-off of any player is defined as the sum of the pay-offs in the individual games.

Definition 8. *Let $\{G^i\}_{i\in I} = \{(P, \{S^i_p\}_{p\in P}, \{u^i_p\}_{p\in P})\}_{i\in I}$ be a finite family of strategic games between the same set of players P. By product game $\prod_i G^i$ we mean game $(P, \{S_p\}_{p\in P}, \{u_p\}_{p\in P})$ such that*

1. $S_p = \prod_i S^i_p$,
2. $u_p(\langle\langle s^i_p\rangle_{i\in I}\rangle_{p\in P}) = \sum_i u^i_p(\langle s^i_p\rangle_{p\in P})$.

Lemma 7.

$$NE\left(\prod_i G^i\right) = \prod_i NE(G^i).$$

Proof. First, assume that $\langle e_p\rangle_{p\in P} = \langle\langle e^i_p\rangle_{i\in I}\rangle_{p\in P} \in NE\left(\prod_i G^i\right)$. We will need to show that $\langle e^i_p\rangle_{p\in P} \in NE(G^i)$ for any $i \in I$. Indeed, suppose that for some $i_0 \in I$, some $p_0 \in P$, and some $s_0 \in S_{p_0}$ we have

$$u^{i_0}_{p_0}(\langle e^{i_0}_p\rangle_{p\in P}[p_0 \mapsto s_0]) > u^{i_0}_{p_0}(\langle e^{i_0}_p\rangle_{p\in P}). \tag{4}$$

Define strategy profile $\langle \hat{e}_p\rangle_{p\in P} = \langle\langle \hat{e}^i_p\rangle_{i\in I}\rangle_{p\in P}$ of the game $\prod_i G^i$ as follows:

$$\hat{e}^i_p \equiv \begin{cases} s_0 & \text{if } i = i_0 \text{ and } p = p_0, \\ e^i_p & \text{otherwise.} \end{cases}$$

Note that, taking into account inequality (4),

$$\begin{aligned} u_{p_0}(\langle \hat{e}_p\rangle_{p\in P}) &= \sum_{i\in I} u^i_{p_0}(\langle \hat{e}^i_p\rangle_{p\in P}) = u^{i_0}_{p_0}(\langle \hat{e}^{i_0}_p\rangle_{p\in P}) + \sum_{i\neq i_0} u^i_{p_0}(\langle \hat{e}^i_p\rangle_{p\in P}) = \\ &= u^{i_0}_{p_0}(\langle e^{i_0}_p\rangle_{p\in P}[p_0 \mapsto s_0]) + \sum_{i\neq i_0} u^i_{p_0}(\langle e^i_p\rangle_{p\in P}) > \\ &> u^{i_0}_{p_0}(\langle e^{i_0}_p\rangle_{p\in P}) + \sum_{i\neq i_0} u^i_{p_0}(\langle e^i_p\rangle_{p\in P}) = \\ &= \sum_i u^i_{p_0}(\langle e^i_p\rangle_{p\in P}) = u_{p_0}(\langle e_p\rangle_{p\in P}), \end{aligned}$$

which is a contradiction with the assumption that $\langle e_p\rangle_{p\in P}$ is a Nash equilibrium of the game $\prod_i G^i$.

Next, assume that $\{\langle e^i_p\rangle_{p\in P}\}_{i\in I}$ is such a set that for any $i \in I$,

$$\langle e^i_p\rangle_{p\in P} \in NE(G^i) \tag{5}$$

We will prove that $\langle\langle e^i_p\rangle_{i\in I}\rangle_{p\in P} \in NE\left(\prod_i G^i\right)$. Indeed, consider any p_0 and any $\langle s^i_0\rangle_{i\in I} \in \prod_{i\in I} S^i_{p_0}$. By assumption (5) and Definition 2, for any $i \in I$

$$u^i_{p_0}(\langle e^i_p\rangle_{p\in P}[p_0 \mapsto s^i_0]) \leq u^i_{p_0}(\langle e^i_p\rangle_{p\in P}).$$

Thus,

$$\begin{aligned} u_{p_0}(\langle\langle e^i_p\rangle_{i\in I}\rangle_{p\in P}[p_0 \mapsto \langle s^i_0\rangle_{i\in I}]) &= \sum_{i\in I} u^i_{p_0}(\langle e^i_p\rangle_{p\in P}[p_0 \mapsto s^i_0]) \leq \\ &\leq \sum_{i\in I} u^i_{p_0}(\langle e^i_p\rangle_{p\in P}) = u_{p_0}(\langle\langle e^i_p\rangle_{i\in I}\rangle_{p\in P}). \end{aligned}$$

Therefore, $\langle\langle e_p^i\rangle_{i\in I}\rangle_{p\in P} \in NE\left(\prod_i G^i\right)$. □

Lemma 8. *For any disjoint subsets A and B of the set P, if each of the games $\{G_i\}_{i\in I}$ has at least one Nash equilibrium, then*

$$\prod_i G^i \vDash A \parallel B \qquad \textit{iff} \qquad \forall i\,(G^i \vDash A \parallel B).$$

Proof. ($\Rightarrow$) : By the assumption of the theorem, for any $i \in I$ there is at least one Nash equilibrium $\langle e_p^i\rangle_{p\in P}$ of the game G^i. Suppose that $\prod_i G^i \vDash A \parallel B$ and consider any $i_0 \in I$. We will prove that $G^{i_0} \vDash A \parallel B$. Indeed, let $f = \langle f_p\rangle_{p\in P} \in NE(G^{i_0})$ and $g = \langle g_p\rangle_{p\in P} \in NE(G^{i_0})$. We will construct $h = \langle h_p\rangle_{p\in P} \in NE(G^{i_0})$ such that $f \equiv_A h \equiv_B g$. To construct such equilibrium, consider strategy profiles $\hat{f} = \langle\langle \hat{f}_p^i\rangle_{i\in I}\rangle_{p\in P}$ and $\hat{g} = \langle\langle \hat{g}_p^i\rangle_{i\in I}\rangle_{p\in P}$ for the game $\prod_i G^i$ such that

$$\hat{f}_p^i = \begin{cases} f_p & \text{if } i = i_0 \\ e_p^i & \text{otherwise} \end{cases} \tag{6}$$

and

$$\hat{g}_p^i = \begin{cases} g_p & \text{if } i = i_0 \\ e_p^i & \text{otherwise} \end{cases} \tag{7}$$

By Lemma 7, $\hat{f}, \hat{g} \in NE(\prod_i G^i)$. Thus, by assumption $\prod_i G^i \vDash A \parallel B$, there must be $\hat{h} \in NE(\prod_i G^i)$ such that

$$\hat{f} \equiv_A \hat{h} \equiv_B \hat{g} \tag{8}$$

Define strategy profile h for the game G^{i_0} to be $\langle h_p^{i_0}\rangle_{p\in P}$. By Lemma 7, $h \in NE(G^{i_0})$. From statements (8), (6), and (7), it follows that $f \equiv_A h \equiv_B g$.

($\Leftarrow$) : Assume that $\forall i\,(G^i \vDash A \parallel B)$. Let $f = \langle\langle f_p^i\rangle_{i\in I}\rangle_{p\in P} \in NE(\prod_i G^i)$ and $g = \langle\langle g_p^i\rangle_{i\in I}\rangle_{p\in P} \in NE(\prod_i G^i)$. We will show that there is $e \in NE(\prod_i G^i)$ such that $f \equiv_A e \equiv_B g$. Indeed, by Lemma 7, $\langle f_p^i\rangle_{p\in P} \in NE(G^i)$ and $\langle g_p^i\rangle_{p\in P} \in NE(G^i)$ for any $i \in I$. Thus, by the assumption, for any $i \in I$ there is $\langle e_p^i\rangle_{p\in P} \in NE(G^i)$ such that $\langle g_p^i\rangle_{p\in P} \equiv_A \langle e_p^i\rangle_{p\in P} \equiv_B \langle g_p^i\rangle_{p\in P}$. Thus,

$$\langle\langle f_p^i\rangle_{i\in I}\rangle_{p\in P} \equiv_A \langle\langle e_p^i\rangle_{i\in I}\rangle_{p\in P} \equiv_B \langle\langle g_p^i\rangle_{i\in I}\rangle_{p\in P}.$$

Pick strategy profile e to be $\langle\langle e_p^i\rangle_{i\in I}\rangle_{p\in P}$ and notice that, by Lemma 7, $e \in NE(\prod_i G^i)$. □

5.4 Completeness: the final steps

We are now ready to prove the completeness theorem, which is stated below.

Theorem 2. *For any set of players P and any $\phi \in \Phi(P)$, if $\nvdash \phi$, then there is a game G with set of players P such that $G \nvDash \phi$.*

Proof. Suppose that $\nvdash \phi$ and let X be a maximal consistent set of formulas containing $\neg\phi$. Let $\{C_i\}_{i\in I}$ be the finite set of all critical subsets of P. Let $PG(C_i)$ be the parity game between set of players P. Pick game G to be $\prod_{i\in I} PG(C_i)$.

Lemma 9. *For any disjoint subsets A and B of the set P,*

$$G \vDash A \parallel B \qquad \textit{iff} \qquad A \parallel B \in X.$$

Proof. ($\Rightarrow$) : Assume that $A \parallel B \notin X$. Thus, $X \nvdash A \parallel B$ due to maximality of X. Hence, by Lemma 3, there is a critical set $C \subseteq P$ such that $(A\cap C)\sqcup(B\cap C)$ is a critical partition of C. Thus, by Lemma 1, $(A \cap C) \sqcup (B \cap C)$ is a non-trivial partition of the set C. Hence, by Lemma 6, $PG(C) \nvDash A \cap C \parallel B \cap C$. Thus, due to soundness of the Monotonicity and Symmetry axioms (Theorem 1), $PG(C) \nvDash A \parallel B$. Hence, by Lemma 5 and Lemma 8, $\prod_{i\in I} G^i \nvDash A \parallel B$. In other words, $G \nvDash A \parallel B$.
($\Leftarrow$) : Suppose that $A \parallel B \in X$. Due to Lemma 5 and Lemma 8, it will be sufficient to show that $PG(C_i) \vDash A \parallel B$ for any $i \in I$. Assume that $PG(C^{i_0}) \nvDash A \parallel B$ for some $i_0 \in I$. Thus, due to soundness of Symmetry and Monotonicity axioms, $PG(C_{i_0}) \nvDash A \cap C_{i_0} \parallel B \cap C_{i_0}$. Then, by Lemma 6, $A \cap C_{i_0} \sqcup B \cap C_{i_0}$ is a non-trivial partition of C_{i_0}. Hence, by Lemma 2, $X \nvdash A \cap C_{i_0} \parallel B \cap C_{i_0}$. Therefore, by Monotonicity and Symmetry axioms, $X \nvdash A \parallel B$. □

Lemma 10. *For any formula ψ in $\Phi(P)$,*

$$G \vDash \psi \qquad \textit{iff} \qquad \psi \in X$$

Proof. Induction on the structural complexity of ψ. Base case is proven in Lemma 9. The induction step follows from the maximality and the consistency of the set X. □

To finish the proof of the completeness theorem, note that $\neg\phi \in X$. Thus, $\phi \notin X$ due to consistency of X. Therefore, by Lemma 10, $G \nvDash \phi$. □

6 Conclusion

6.1 An n-ary Independence Relation

In this paper, we have considered the independence relation $A \parallel B$ between two sets of players. This binary relation can be naturally generalized to the n-ary relation

$$A_1 \parallel A_2 \parallel \cdots \parallel A_n$$

between n sets of players by changing part 3 of Definition 4 to

3. $G \vDash A_1 \parallel A_2 \parallel \cdots \parallel A_n$ *if and only if for any* $e_1, e_2, \ldots, e_n \in NE(G)$ *there is* $e \in NE(G)$ *such that* $e \equiv_{A_i} e_i$ *for each* $i \leq n$.

It turns out, however, that the n-ary independence relation can be expressed through the binary independence relation studied in this paper. For example, in the case $n = 3$, the following result holds:

Theorem 3. *For any game* $G = (P, \{S_p\}_{p\in P}, \{u_p\}_{p\in P})$ *and any disjoint subsets* A, B, *and* C *of set the* P,

$$G \vDash (A \parallel B \parallel C) \Longleftrightarrow (A \parallel B, C) \wedge (B \parallel C).$$

Proof. ($\Rightarrow$) : Assume $G \vDash A \parallel B \parallel C$. To prove $G \vDash A \parallel B, C$, consider any two equilibria $e_1, e_2 \in NE(G)$. We will show that there is equilibrium $e \in NE(G)$ such that $e_1 \equiv_A e \equiv_{B,C} e_2$. Indeed, by the assumption, there must be equilibrium $e \in NE(G)$ such that $e \equiv_A e_1$, $e \equiv_B e_2$, and $e \equiv_C e_2$.

To prove $G \vDash B \parallel C$, consider any two equilibria $e_1, e_2 \in NE(G)$. We will show that there is equilibrium $e \in NE(G)$ such that $e_1 \equiv_B e \equiv_C e_2$. Indeed, by the assumption, there must be equilibrium $e \in NE(G)$ such that $e \equiv_A e_1$, $e \equiv_B e_1$, and $e \equiv_C e_2$.
($\Leftarrow$) : Assume $G \vDash A \parallel B, C$ and $G \vDash B \parallel C$. To prove $G \vDash A \parallel B \parallel C$, consider any three equilibria $e_1, e_2, e_3 \in NE(G)$. We will show that there is equilibrium $e \in NE(G)$ such that $e \equiv_A e_1$, $e \equiv_B e_2$, and $e \equiv_C e_3$. Indeed, by the assumption $G \vDash B \parallel C$, there must be equilibrium $e_4 \in NE(G)$ such that $e_2 \equiv_B e_4 \equiv_C e_3$. By the assumption $G \vDash A \parallel B, C$, there must be equilibrium $e \in NE(G)$ such that $e_1 \equiv_A e \equiv_{B,C} e_4$. Therefore, $e \equiv_A e_1$, $e \equiv_B e_4 \equiv_B e_2$, and $e \equiv_C e_4 \equiv_C e_3$. □

6.2 Possible Extensions

In this paper we have defined independence $A \parallel B$ between two sets of rational players through properties of their strategies in a Nash equilibrium. There are several other ways in which independence between groups of players could be specified. One can say that set of players A is independent from set of players B if players in set A will not change their strategies if strategies of players in set B are revealed to them. An alternative is to assume that not only players in set A know strategies of players in set B, but they can dictate the choice of these strategies. Yet another way to define independence is to see if cooperation between coalitions A and B will not increase their pay-off values. In the future work, we would like to give the precise definitions of these types of independence and to study their universal properties.

References

1. Ellis Cohen. Information transmission in computational systems. In *Proceedings of Sixth ACM Symposium on Operating Systems Principles*, pages 113–139. Association for Computing Machinery, 1977.
2. Abraham de Moivre. De mensura sortis seu; de probabilitate eventuum in ludis a casu fortuito pendentibus. *Philosophical Transactions (1683-1775)*, 27:pp. 213–264, 1711.
3. Abraham de Moivre. *Doctrine of Chances*. 1718.
4. Edsger W. Dijkstra. Hierarchical ordering of sequential processes. *Acta Inf.*, 1:115–138, 1971.

5. Michael Donders, Sara Miner More, and Pavel Naumov. Information flow on directed acyclic graphs. In L. Beklemishev and R. de Queiroz, editors, *Proceedings of 18th Workshop on Logic, Language, Information and Computation (Philadelphia, United States)*, pages 95–109. Springer, 2011.
6. Moivre, Abraham, de. In *The New Encyclopædia Britannica*, volume 8, page 226. Encyclopædia Britannica, 15th edition, 1998.
7. Dan Geiger, Azaria Paz, and Judea Pearl. Axioms and algorithms for inferences involving probabilistic independence. *Inform. and Comput.*, 91(1):128–141, 1991.
8. Joseph Y. Halpern and Kevin R. O'Neill. Secrecy in multiagent systems. *ACM Trans. Inf. Syst. Secur.*, 12(1):1–47, 2008.
9. Sara Miner More and Pavel Naumov. On interdependence of secrets in collaboration networks. In *Proceedings of 12th Conference on Theoretical Aspects of Rationality and Knowledge (Stanford University, 2009)*, pages 208–217, 2009.
10. Sara Miner More and Pavel Naumov. Hypergraphs of multiparty secrets. In *11th International Workshop on Computational Logic in Multi-Agent Systems CLIMA XI (Lisbon, Portugal), LNAI 6245*, pages 15–32. Springer, 2010.
11. Sara Miner More and Pavel Naumov. An independence relation for sets of secrets. *Studia Logica*, 94(1):73–85, 2010.
12. Sara Miner More, Pavel Naumov, and Benjamin Sapp. Concurrency semantics for the Geiger-Paz-Pearl axioms of independence. In *20th Conference on Computer Science Logic (CSL 2011)*. Bergen, Norway, September 2011 (to appear).
13. Milan Studený. Conditional independence relations have no finite complete characterization. In *Information Theory, Statistical Decision Functions and Random Processes. Transactions of the 11th Prague Conference vol. B*, pages 377–396. Kluwer, 1990.
14. David Sutherland. A model of information. In *Proceedings of Ninth National Computer Security Conference*, pages 175–183, 1986.