Pavel Naumov

Independence in Information Spaces

Abstract. Three different types of interdependence between pieces of information, or "secrets", are discussed and compared. Two of them, functional dependence and nondeducibility, have been studied and axiomatized before. This article introduces a third type of interdependence and provides a complete and decidable axiomatization of this new relation.

1. Introduction

In this article we study interdependence between pieces of information. We call such pieces *secrets*. More formally, we will later define an *information space* as an arbitrary set of outcomes and secrets as functions on information space. This makes information space analogous to probability space and secrets analogous to random variables. However, unlike probability space, information space does not have a measure associated with it.

Let A and B be two sets of secrets. The simplest example of interdependency between A and B is *functional dependency* relation. We denote it as $A \rhd B$. It means that secrets in set A reveal the secrets in set B. Armstrong [1] presented the following sound and complete axiomatization of this relation:

1. *Reflexivity*: $A \rhd B$, if $A \supseteq B$,
2. *Augmentation*: $A \rhd B \to A, C \rhd B, C$,
3. *Transitivity*: $A \rhd B \to (B \rhd C \to A \rhd C)$,

where here and everywhere below A, B denotes the union of sets A and B. The above axioms are known in database literature as Armstrong's axioms [4, p. 81]. Beeri, Fagin, and Howard [2] suggested a variation of Armstrong's axioms that describe properties of multi-valued dependency.

Another example of interdependency between sets of secrets A and B is when sets A and B both reveal a common secret c. For instance, if one picks two random pages from the same book, then there will be no way to reconstruct one page from just looking at the other. These two pages, however, will be interdependent since they at least share the language in which they are both written. In this example, A and B are sets of data on each page and c is the language of the book. In a relational database, A

Studia Logica (2012) 0: 1–21

and B are sets of attributes and c is an attribute from the intersections of closures of A and B. For any sets of secrets A and B, if such secret c *does not* exist, then we will say that sets of secrets A and B are *independent*. This is the relation that we study in this article. There is a caveat, however. If we allow c to be a constant function on outcomes, then its value is revealed by each set. Hence, no independent sets of secrets would exist. Note that constant secret is not really a "secret" in common sense, because its value is known a priori. We will call such secrets *public knowledge* and will adjust the definition of independence to require secret c not to be public knowledge. We denote the independence relation defined this way by $A \mid B$. Our main result is the following complete and decidable axiomatization of this relation:

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

Finally, there is one more, weaker, type of interdependency, when sets of secrets A and B might not reveal any common non-trivial secret c, but there is a certain combination of values of A that is not compatible with a specific combination of values of B. For example, consider a relational database of people that has boolean attributes a = "born on Saturday" and b = "born on Sunday". These attributes are interdependent in this weaker sense, because the same person can not be born on two different days of week. However, as we will show later in this article, if any other attribute in the same database is functionally determined by a and is also functionally determined by b, then this attribute is the same for all people. If even this, weak, interdependence between two sets of secrets does not hold, then we will say that these two sets are *strongly independent*. We denote strong independence between two sets of secrets by $A \parallel B$. This relation for two single secrets was introduced by Sutherland [15] and is also known as *nondeducibility* in the study of information flow. Halpern and O'Neill [6] proposed a closely related notion called f-secrecy. A sound and complete axiomatization of the strong independence relation between sets was given by More and Naumov [10] in this journal:

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. *Public Knowledge*: $A \parallel B \to (C \parallel C \to A \parallel B, C)$,
5. *Exchange*: $A \parallel B, C \to (B \parallel C \to A, B \parallel C)$.

Essentially the same axioms were shown to provide a complete axiomatization of the independence relation between random variables in probability theory [5], noninterference relation in concurrency theory [13], and Nash equilibrium interchangeability in game theory [14]. More, Naumov, and Donders [12, 11, 3] gave a complete axiomatization of the strong independence relation between single secrets if secrets are generated over a collaboration network with a fixed topology. A complete logical system that describes the connection between relations $\parallel$ and $\rhd$ on single secrets is described by Kelvey, More, Naumov, and Sapp [7].

Most of the article is focused on axiomatization of independence relation. We start, however, by comparing independence and strong independence. In the conclusion, we will discuss a property that connects these two relations.

2. Information Space

Definition 1. *Information space is an arbitrary non-empty set, whose elements will be referred to as "outcomes".*

For the birthday example above, we can formally specify the set of outcomes as {"Workday", "Saturday", "Sunday"}. However, we will find it technically more convenient to define outcomes in the "birthday information space" as the set of boolean pairs in which at least one element is zero:

$$\mathcal{I}_b = \{(x, y) \in \{0, 1\}^2 \mid x \cdot y = 0\},$$

where the first component shows if the birthday is on Saturday and the second if it is on Sunday. Since birthday can not be simultaneously on Saturday and Sunday, we exclude pair $(1, 1)$.

Definition 2. *A "secret" over an information space is a function defined on the information space. Constant functions of this type are called "public knowledge".*

In the birthday example, let secrets α and β be the first and the second projection functions on $\mathcal{I}_b$.

Definition 3. *Set of secrets $\{\alpha_1, \ldots, \alpha_n\}$ reveals, over an information space $\mathcal{I}$, secret β if there is a function $f(x_1, \ldots, x_n)$ such that*

$$f(\alpha_1(x), \ldots, \alpha_n(x)) = \beta(x)$$

for each outcome $x \in \mathcal{I}$.

We are ready now to give the main definition of this work. Two sets of secrets, over an information space, are independent if the only secrets that they both reveal are public knowledge. This can also be stated as

DEFINITION 4. *Sets of secrets $A = \{\alpha_1, \dots, \alpha_n\}$ and $B = \{\beta_1, \dots, \beta_k\}$ are independent over an information space $\mathcal{I}$ if and only if for each two functions f and g on $\mathcal{I}$ if $f(\alpha_1(t), \dots, \alpha_n(t)) = g(\beta_1(t), \dots, \beta_k(t))$ for each $t \in \mathcal{I}$, then $f(\alpha_1(t), \dots, \alpha_n(t))$ is a constant function of t.*

Next, we will prove the result promised in the introduction.

THEOREM 1. *The singleton sets of secrets $\{\alpha\}$ and $\{\beta\}$ over information space $\mathcal{I}_b$ are independent.*

PROOF. Suppose that there are functions f and g such that $f(\alpha(z)) = g(\beta(z))$ for each $z \in \mathcal{I}_p$. We will prove that $f(\alpha(z))$ is a constant function on $\mathcal{I}_b$. Assume the opposite: $f(\alpha(z_1)) \neq f(\alpha(z_2))$ for some $z_1, z_2 \in \mathcal{I}_b$. Let $z_1 = (x_1, y_1)$ and $z_2 = (x_2, y_2)$. Note that $(x_1, 0)$ and $(x_2, 0)$ are also elements of $\mathcal{I}_b$, because $x_1 \cdot 0 = 0$ and $x_2 \cdot 0 = 0$. Thus,

$$\begin{aligned} &f(\alpha(z_1)) = f(pr_1(x_1, y_1)) = f(x_1) = f(pr_1(x_1, 0)) = f(\alpha(x_1, 0)) = \\ &= g(\beta(x_1, 0)) = g(pr_2(x_1, 0)) = g(0) = g(pr_2(x_2, 0)) = g(\beta(x_2, 0)) = \\ &= f(\alpha(x_2, 0)) = f(pr_1(x_2, 0)) = f(x_2) = f(pr_1(x_2, y_2)) = f(\alpha(z_2)). \end{aligned}$$

Therefore, $f(\alpha(z_1)) = f(\alpha(z_2))$, which is a contradiction. ∎

DEFINITION 5. *Sets of secrets $A = \{\alpha_1, \dots, \alpha_n\}$ and $B = \{\beta_1, \dots, \beta_k\}$ are strongly independent over an information space $\mathcal{I}$ if for each $x, y \in \mathcal{I}$ there is $z \in \mathcal{I}$ such that $\alpha_i(z) = \alpha_i(x)$ for each $i \leq n$ and $\beta_j(z) = \beta_j(y)$ for each $j \leq k$.*

THEOREM 2. *The singleton sets of secrets $\{\alpha\}$ and $\{\beta\}$ are not strongly independent over information space $\mathcal{I}_b$.*

PROOF. Assume that the sets $\{\alpha\}$ and $\{\beta\}$ are strongly independent over $\mathcal{I}_b$. Consider the outcomes $(1, 0) \in \mathcal{I}_b$ and $(0, 1) \in \mathcal{I}_b$. By the definition of strong independence, there must exist $(z_1, z_2) \in \mathcal{I}_b$ such that $\alpha(z_1, z_2) = \alpha(1, 0)$ and $\beta(z_1, z_2) = \beta(0, 1)$. Hence, $z_1 = 1$ and $z_2 = 1$. At the same time, $(1, 1) \notin \mathcal{I}_b$, which is a contradiction. ∎

THEOREM 3. *If two sets of secrets are strongly independent over an information space, then they are independent over the same information space.*

PROOF. Let sets of secrets $A = \{\alpha_1, \ldots, \alpha_n\}$ and $B = \{\beta_1, \ldots, \beta_k\}$ be strongly independent over an information space $\mathcal{I}$. We need to prove that A and B are independent over $\mathcal{I}$. Assume the opposite. Then, there are functions f and g such that for each $x \in \mathcal{I}$,

$$f(\alpha_1(x), \ldots, \alpha_n(x)) = g(\beta_1(x), \ldots, \beta_k(x))$$

and $f(\alpha_1(x), \ldots, \alpha_n(x))$ is not a constant function of x. In other words, there are $x_1, x_2 \in \mathcal{I}$ such that

$$f(\alpha_1(x_1), \ldots, \alpha_n(x_1)) \neq f(\alpha_1(x_2), \ldots, \alpha_n(x_2)). \tag{1}$$

Since A and B are strongly independent, there must be $z \in \mathcal{I}$ such that $\alpha_i(z) = \alpha_i(x_1)$ for each $i \leq n$ and $\beta_j(z) = \beta_j(x_2)$ for each $j \leq k$. Note now that

$$\begin{aligned} f(\alpha_1(x_1), \ldots, \alpha_n(x_1)) = f(\alpha_1(z), \ldots, \alpha_n(z)) = g(\beta_1(z), \ldots, \beta_k(z)) = \\ = g(\beta_1(x_2), \ldots, \beta_k(x_2)) = f(\alpha_1(x_2), \ldots, \alpha_n(x_2)). \end{aligned}$$

This is a contradiction with equality (1). ∎

Theorems 1, 2, and 3, taken together, show that strong independence, as a relation, is *stronger* than independence. A complete axiomatization of strong independence is given by More and Naumov [10]. In the rest of this article we give a complete axiomatization of the independence relation.

3. Language and Semantics

Throughout this article we will assume a fixed infinite set of "secret variables": $a, b, c, \ldots$. We will use letters $A, B, C \ldots$ to represent finite sets of secret variables. The atomic formulas of the language of secrets are $A \mid B$, where A and B are *finite* sets of secret variables. An arbitrary formula in a language of secrets is a propositional formula built out of atomic formulas. We will assume that only implication $\rightarrow$ and false $\bot$ are primitive propositional connectives. As usual, the other propositional connectives can be defined through the primitive ones.

DEFINITION 6. *A semantics of secrets is a pair $\langle \mathcal{I}, \star \rangle$, where $\mathcal{I}$ is an arbitrary information space and $\star$ is a mapping of secret variables into secrets over $\mathcal{I}$. If A is a finite set of secret variables, then by $A^\star$ we mean set $\{a^\star \mid a \in A\}$.*

DEFINITION 7. *A semantics $\langle \mathcal{I}, \star \rangle$ is called finite if set $\mathcal{I}$ is finite.*

Definition 8. *For any semantics of secrets $\mathcal{S} = \langle \mathcal{I}, \star \rangle$, and an arbitrary formula ϕ in the language of secrets we define relation $\mathcal{S} \vDash \phi$ as follows:*

1. $\mathcal{S} \nvDash \bot$,
2. $\mathcal{S} \vDash A \,|\, B$ *if and only if sets* $A^\star$ *and* $B^\star$ *are independent,*
3. $\mathcal{S} \vDash A \to B$ *if and only if* $\mathcal{S} \nvDash A$ *or* $\mathcal{S} \vDash B$.

4. Logic of Secrets

In this section we describe a formal logical system for independence relation $A \,|\, B$. This system, like earlier systems defined by Armstrong [1], More and Naumov [8, 9] and by Kelvey, More, Naumov, and Sapp [7], belongs to the set of deductive systems that capture properties of secrets. In general, we refer to such systems as *logics of secrets*. Since this article is focused on only one such system, here we call it *the Logic of Secrets*.

Definition 9. *Logic of Secrets, in additional to propositional tautologies in the language of secrets and Modus Ponens inference rules, contain the following axiom schemata:*

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

Recall from the introduction that comma is a meta notation for the union of the two sets of secret variables. The first three axioms are self-explanatory. To understand the fourth axiom, notice that, by Definition 4, $C \,|\, C$ means that C can only reveal public knowledge and, thus, must be public knowledge by itself.

5. Soundness

Theorem 4 (Empty Set). *$\mathcal{S} \vDash A \,|\, \varnothing$, for each semantics of secrets $\mathcal{S}$ and each finite set of secret variables A.*

Proof. Let $\mathcal{S} = \langle \mathcal{I}, \star \rangle$ and $A = \{a_1, \dots, a_n\}$. Consider any n-argument functions f and 0-argument (thus, constant) function g such that

$$f(a_1^\star(x), \dots, a_n^\star(x)) = g$$

for each outcome x. We need to show that $f(a_1^\star(x), \dots, a_n^\star(x))$ is a constant as a function of x, which is true due to the above equality. ∎

THEOREM 5 (Symmetry). *$\mathcal{S} \vDash A \,|\, B \to B \,|\, A$, for each semantics of secrets $\mathcal{S}$ and each two finite sets of secret variables A and B.*

PROOF. Let $\mathcal{S} = \langle \mathcal{I}, \star \rangle$, $A = \{a_1, \ldots, a_n\}$, and $B = \{b_1, \ldots, b_k\}$. Assume $\mathcal{S} \vDash A \,|\, B$. We will show that $\mathcal{S} \vDash B \,|\, A$. Consider any functions f and g such that $f(b_1^\star(x), \ldots, b_k^\star(x)) = g(a_1^\star(x), \ldots, a_n^\star(x))$ for each outcome x. We need to show that $f(b_1^\star(x), \ldots, b_k^\star(x))$ is a constant as a function of x. Indeed, notice that above equality can be written as $g(a_1^\star(x), \ldots, a_n^\star(x)) = f(b_1^\star(x), \ldots, b_k^\star(x))$. By the assumption $\mathcal{S} \vDash A \,|\, B$, we can conclude that $g(a_1^\star(x), \ldots, a_n^\star(x))$, as a function of x, is constant. Thus, $f(b_1^\star(x), \ldots, b_k^\star(x))$, as a function of x, is also constant. ∎

THEOREM 6 (Monotonicity). *$\mathcal{S} \vDash A \,|\, B, C \to A \,|\, B$, for each semantics of secrets $\mathcal{S}$ and each finite sets of secret variables A, B, and C.*

PROOF. Let $\mathcal{S} = \langle \mathcal{I}, \star \rangle$, $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_k\}$, and $C = \{c_1, \ldots, c_m\}$. Assume $\mathcal{S} \vDash A \,|\, B, C$. We will show that $\mathcal{S} \vDash A \,|\, B$. Consider any functions f and g such that $f(a_1^\star(x), \ldots, a_n^\star(x)) = g(b_1^\star(x), \ldots, b_k^\star(x))$ for each outcome x. We need to show that $f(a_1^\star(x), \ldots, a_n^\star(x))$ is a constant as a function of x. Indeed, define function $h(y_1, \ldots, y_k, z_1, \ldots, z_m)$ to be equal to $g(y_1, \ldots, y_k)$ for each $y_1, \ldots, y_k$. Thus,

$$\begin{aligned} f(a_1^\star(x), \ldots, a_n^\star(x)) &= g(b_1^\star(x), \ldots, b_k^\star(x)) = \\ &= h(b_1^\star(x), \ldots, b_k^\star(x), c_1^\star(x), \ldots, c_m^\star(x)) \end{aligned}$$

for each output $x \in \mathcal{I}$. Therefore, by the assumption $\mathcal{S} \vDash A \,|\, B, C$, function $f(a_1^\star(x), \ldots, a_n^\star(x))$ must be a constant function of x. ∎

THEOREM 7 (Public Knowledge). *$\mathcal{S} \vDash A \,|\, B \to (C \,|\, C \to A \,|\, B, C)$, for each semantics of secrets $\mathcal{S}$ and each finite sets of secret variables A, B, and C.*

PROOF. Let $\mathcal{S} = \langle \mathcal{I}, \star \rangle$, $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_k\}$, and $C = \{c_1, \ldots, c_m\}$. Assume $\mathcal{S} \vDash A \,|\, B$ and $\mathcal{S} \vDash C \,|\, C$. We will show that $\mathcal{S} \vDash A \,|\, B, C$. First, consider function f that returns the tuple constructed out of its n arguments:

$$f(x_1, \ldots, x_m) = \langle x_1, \ldots, x_m \rangle.$$

Note that by reflexivity of equality,

$$f(c_1^\star(x), \ldots, c_m^\star(x)) = f(c_1^\star(x), \ldots, c_m^\star(x))$$

for each outcome $x \in \mathcal{I}$. Thus, by assumption $\mathcal{S} \vDash C \,|\, C$, function

$$f(c_1^\star(x), \ldots, c_m^\star(x)) = \langle c_1^\star(x), \ldots, c_m^\star(x) \rangle$$

must be a constant. This, in turn, is possible only if each of the functions $c_1^\star(x), \dots, c_m^\star(x)$ is a constant (in other words, public knowledge). We will refer to values of these constant functions as $\gamma_1, \dots, \gamma_m$.

We are now ready to prove that $\mathcal{S} \vDash A \,|\, B, C$. Indeed, consider any functions f and g such that

$$f(a_1^\star(x), \dots, a_n^\star(x)) = g(b_1^\star(x), \dots, b_k^\star(x), c_1^\star(x), \dots, c_m^\star(x))$$

for each outcome x. We will prove that $f(a_1^\star(x), \dots, a_n^\star(x))$ is a constant function of x.

$$h(x_1, \dots, x_k) = g(x_1, \dots, x_k, \gamma_1, \dots, \gamma_m)$$

and note that

$$\begin{aligned} f(a_1^\star(x), \dots, a_n^\star(x)) &= g(b_1^\star(x), \dots, b_k^\star(x), c_1^\star(x), \dots, c_m^\star(x)) = \\ &= g(b_1^\star(x), \dots, b_k^\star(x), \gamma_1, \dots, \gamma_m) = h(b_1^\star(x), \dots, b_k^\star(x)). \end{aligned}$$

for each $x \in \mathcal{I}$. Thus, by assumption $\mathcal{S} \vDash A \,|\, B$, function $f(a_1^\star(x), \dots, a_n^\star(x))$ must be a constant function of x. ■

6. Completeness

We start the completeness proof by describing two auxiliary semantics $\mathcal{S}(a)$ and $\mathcal{S}(A, B)$ multiple instances of which later will be combined into a "canonical" semantics needed for the completeness theorem.

6.1. Semantics $\mathcal{S}(a)$

Definition 10. *For any secret variable a, let information space $\mathcal{I}(a)$ be two-element set $\{0, 1\}$.*

Definition 11. *Let $\star$ be the following mapping of a secret variable v into a secret over $\mathcal{I}(a)$:*

$$v^\star(x) = \begin{cases} x & \text{if } v = a, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 12. *Let semantics of secrets $\mathcal{S}(a)$ be $\langle \mathcal{I}(a), \star \rangle$.*

Theorem 8. *$\mathcal{S}(a) \vDash A \,|\, B$ if and only if $a \notin A \cap B$.*

PROOF. ($\Rightarrow$) : Assume that $a \in A \cap B$. We will show that $\mathcal{S}(a) \not\models A \,|\, B$. Indeed, let $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_k\}$, and $a = a_i = b_j$ for some i and j. Consider functions $f(x_1, \ldots, x_n) = x_i$ and $g(y_1, \ldots, y_k) = y_j$. Thus, for each $x \in \mathcal{I}(a)$,

$$f(a_1^\star(x), \ldots, a_n^\star(x)) = a_i^\star(x) = a^\star(x)$$

and

$$g(b_1^\star(x), \ldots, b_k^\star(x)) = b_j^\star(x) = a^\star(x).$$

Hence, $f(a_1^\star(x), \ldots, a_n^\star(x)) = g(b_1^\star(x), \ldots, b_k^\star(x))$ for each $x \in \mathcal{I}(a)$. We are just left to show that $f(a_1^\star(x), \ldots, a_n^\star(x))$ is not a constant function of x, which is true because

$$f(a_1^\star(1), \ldots, a_n^\star(1)) = a^\star(1) = 1 \neq 0 = a^\star(0) = f(a_1^\star(0), \ldots, a_n^\star(0)).$$

($\Leftarrow$) : Assume that $a \notin A \cap B$. Without loss of generality, let $a \notin B$. Suppose that for some functions f and g and each $x \in \mathcal{I}(a)$,

$$f(a_1^\star(x), \ldots, a_n^\star(x)) = g(b_1^\star(x), \ldots, b_k^\star(x)).$$

We will show that $f(a_1^\star(x), \ldots, a_n^\star(x))$ is a constant function of x. Indeed, since $a \notin B$, for each $x \in \mathcal{I}(a)$,

$$f(a_1^\star(x), \ldots, a_n^\star(x)) = g(b_1^\star(x), \ldots, b_k^\star(x)) = g(0, \ldots, 0).$$

Thus, $f(a_1^\star(x), \ldots, a_n^\star(x))$ is a constant function of x. ■

6.2. Semantics $\mathcal{S}(A, B)$

DEFINITION 13. *Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_k\}$ be two non-empty disjoint sets of secret variables, information space $\mathcal{I}(A, B)$ is defined as follows:*

$$\mathcal{I}(A, B) = \{(x_1, \ldots, x_n, y_1, \ldots, y_k) \in \{0,1\}^{n+k} \mid \bigvee_{i=1}^{n} x_i = \bigvee_{j=1}^{k} y_j\}.$$

In the above definition, disjunction $\vee$ is defined in the standard way as the maximum of the arguments boolean arguments.

DEFINITION 14. *Let $\star$ be the following mapping of a secret variables v into secrets over $\mathcal{I}(A, B)$:*

$$v^\star(x_1, \ldots, x_n, y_1, \ldots, y_k) = \begin{cases} x_i & \text{if } v = a_i, \\ y_j & \text{if } v = b_j, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 15. *Let $\mathcal{S}(A,B)$ be semantics $\langle \mathcal{I}(A,B), \star\rangle$.*

Although throughout the most of this article we use comma to denote the union of the two sets of secret variables, in the theorem below, which refers to the union and the intersection at the same time, we revert to the more common notation $\cup$ for the union to go along with standard notation $\cap$ for the intersection.

Theorem 9. *For any finite sets of secrets A, B, C, and D,*

$$\mathcal{S}(A,B) \vDash C \cap (A \cup B) \,|\, D \cap (A \cup B) \to C \,|\, D.$$

Proof. Assume that $\mathcal{S}(A,B) \vDash C \cap (A \cup B) \,|\, D \cap (A \cup B)$. Let $C = \{c_1, \dots, c_p\}$, $D = \{d_1, \dots, d_q\}$ and $C \cap (A \cup B) = \{c_1, \dots, c_{p'}\}$, $D \cap (A \cup B) = \{d_1, \dots, d_{q'}\}$ for some $p' \le p$ and $q' \le q$. Suppose also that f and g are any two functions such that for each outcome $t \in \mathcal{I}(A,B)$,

$$f(c_1^\star(t), \dots, c_p^\star(t)) = g(d_1^\star(t), \dots, d_q^\star(t)) \tag{2}$$

We will show that $f(c_1^\star(t), \dots, c_p^\star(t))$ is a constant as a function of t. Indeed, define functions

$$f'(t_1, \dots, t_{p'}) = f(t_1, \dots, t_{p'}, 0, \dots, 0),$$

$$g'(t_1, \dots, t_{q'}) = g(t_1, \dots, t_{q'}, 0, \dots, 0).$$

Note that, according to equation (2), for each outcome $t \in \mathcal{I}(A,B)$

$$\begin{aligned} &f'(c_1^\star(t), \dots, c_{p'}^\star(t)) = f(c_1^\star(t), \dots, c_{p'}^\star(t), 0, \dots, 0) = \\ &= g(d_1^\star(t), \dots, d_{q'}^\star(t), 0, \dots, 0) = g'(d_1^\star(t), \dots, d_{q'}^\star(t)). \end{aligned}$$

Thus, we can use assumption $\mathcal{S}(A,B) \vDash C \cap (A \cup B) \,|\, D \cap (A \cup B)$ to conclude that $f'(c_1^\star(t), \dots, c_{p'}^\star(t))$ is a constant function of t. Recall now that by Definition 14, $c_i^\star(t) = 0$ for each $i \ge p'$ and $d_j^\star(t) = 0$ for each $j \ge q'$. Hence, for each outcome $t \in \mathcal{I}(A,B)$,

$$f(c_1^\star(t), \dots, c_p^\star(t)) = f(c_1^\star(t), \dots, c_{p'}^\star(t), 0, \dots, 0) = f'(c_1^\star(t), \dots, c_{p'}^\star(t)).$$

Therefore, $f(c_1^\star(t), \dots, c_p^\star(t))$ is also a constant function of t. ∎

Theorem 10. *$\mathcal{S}(A,B) \nvDash A \,|\, B$.*

PROOF. Let $f(t_1,\dots,t_n) = \bigvee_{i\le n} t_i$ and $g(t_1,\dots,t_k) = \bigvee_{i\le k} t_i$. Note that for each outcome $t = (x_1,\dots,x_n,y_1,\dots,y_k) \in \mathcal{I}(A,B)$,

$$f(a_1^\star(t),\dots,a_n^\star(t)) = f(x_1,\dots,x_n) = \bigvee_{i=1}^{n} x_i =$$
$$= \bigvee_{j=1}^{k} y_j = g(y_1,\dots,y_k) = g(b_1^\star(t),\dots,b_k^\star(t)).$$

We only need to show that $f(a_1^\star(t),\dots,a_n^\star(t))$, as a function of t, is not a constant on set $\mathcal{I}(A,B)$. Indeed, consider $t_0 = (0,\dots,0)$ and $t_1 = (1,\dots,1)$. Note that $t_0, t_1 \in \mathcal{I}(A,B)$ because sets A and B, by Definition 13, are non-empty. At the same time,

$$f(a_1^\star(t_0),\dots,a_n^\star(t_0)) = f(0,\dots,0) = \bigvee_{i=1}^{n} 0 = 0$$

and

$$f(a_1^\star(t_1),\dots,a_n^\star(t_1)) = f(1,\dots,1) = \bigvee_{i=1}^{n} 1 = 1.$$

■

THEOREM 11. *Let A_1,A_2 be two disjoint subsets of A and B_1, B_2 be two disjoint subsets of B, if both A_1 and B_1 are not empty, then $\mathcal{S}(A,B) \vDash A_1, B_1 \,|\, A_2, B_2$.*

PROOF. Suppose that $A_1 = \{a_1,\dots,a_{n_1}\}$, $A_2 = \{a_{n_1+1},\dots,a_{n_2}\}$, $B_1 = \{b_1,\dots,b_{k_1}\}$, and $B_2 = \{b_{k_1+1},\dots,b_{k_2}\}$. Let f and g be any two functions such that

$$f(a_1^\star(t),\dots,a_{n_1}^\star(t),b_1^\star(t),\dots,b_{k_1}^\star(t)) = \\ g(a_{n_1+1}^\star(t),\dots,a_{n_2}^\star(t),b_{k_1+1}^\star(t),\dots,b_{k_2}^\star(t)) \tag{3}$$

for each $t \in \mathcal{I}_2(A,B)$. We will show that

$$f(a_1^\star(t),\dots,a_{n_1}^\star(t),b_1^\star(t),\dots,b_{k_1}^\star(t)),$$

as a function of t, is a constant. Assume the opposite. Let there be $t', t'' \in \mathcal{I}(A,B)$ such that

$$f(a_1^\star(t'),\dots,a_{n_1}^\star(t'),b_1^\star(t'),\dots,b_{k_1}^\star(t')) \neq \\ f(a_1^\star(t''),\dots,a_{n_1}^\star(t''),b_1^\star(t''),\dots,b_{k_1}^\star(t'')). \tag{4}$$

Let $t' = (x'_1, \dots, x'_n, y'_1, \dots, y'_k)$ and $t'' = (x''_1, \dots, x''_n, y''_1, \dots, y''_k)$. Since A_1 and B_1 are both not empty, $n_1 > 1$ and $k_1 > 1$. Thus, we can define

$$\begin{array}{rcl} u & = & (1, x'_2, \dots, x'_n, 1, y'_2, \dots, y'_k) \\ v & = & (1, x'_2, \dots, x'_{n_1}, x''_{n_1+1}, \dots, x''_n, 1, y'_2, \dots, y'_{k_1}, y''_{k_1+1}, \dots, y''_k). \end{array}$$

Note that $u, v \in \mathcal{I}(A, B)$ because

$$1 \vee x'_2 \vee \dots \vee x'_n = 1 = 1 \vee y'_2 \vee \dots \vee y'_k,$$

$$1 \vee x'_2 \vee \dots \vee x'_{n_1} \vee x''_{n_1+1} \vee \dots \vee x''_n = 1 = 1 \vee y'_2 \vee \dots \vee y'_{k_1} \vee y''_{k_1+1} \vee \dots \vee y''_k.$$

Therefore, by multiple application of (3),

$$\begin{array}{rl} & f(a^\star_1(t'), \dots, a^\star_{n_1}(t'), b^\star_1(t'), \dots, b^\star_{k_1}(t')) = \\ = & g(a^\star_{n_1+1}(t'), \dots, a^\star_{n_2}(t'), b^\star_{k_1+1}(t'), \dots, b^\star_{k_2}(t')) = \\ = & g(x'_{n_1+1}, \dots, x'_{n_2}, y'_{k_1+1}, \dots, y'_{k_2}) = \\ = & g(a^\star_{n_1+1}(u), \dots, a^\star_n(u), b^\star_{k_1+1}(u), \dots, b^\star_{k_2}(u)) = \\ = & f(a^\star_1(u), \dots, a^\star_{n_1}(u), b^\star_1(u), \dots, b^\star_{k_1}(u)) = \\ = & f(1, x'_2, \dots, x'_{n_1}, 1, y'_2, \dots, y'_{k_1}) = \\ = & f(a^\star_1(v), \dots, a^\star_{n_1}(v), b^\star_1(v), \dots, b^\star_{k_1}(v)) = \\ = & g(a^\star_{n_1+1}(v), \dots, a^\star_{n_2}(v), b^\star_{k_1+1}(v), \dots, b^\star_{k_2}(v)) = \\ = & g(x''_{n_1+1}, \dots, x''_{n_2}, y''_{k_1+1}, y''_{k_2}) = \\ = & g(a^\star_{n_1+1}(t''), \dots, a^\star_{n_2}(t''), b^\star_{k_1+1}(t''), \dots, b^\star_{k_2}(t'')) = \\ = & f(a^\star_1(t''), \dots, a^\star_{n_1}(t''), b^\star_1(t''), \dots, b^\star_{k_1}(t'')). \end{array}$$

Contradiction with (4). ∎

THEOREM 12. *Let A_1,A_2 be two disjoint subsets of A and B_1, B_2 be two disjoint subsets of B. If $A_1 \cup A_2$ is a proper subset of A and $B_1 \cup B_2$ is a proper subset of B, then $\mathcal{S}(A, B) \vDash A_1, B_1 \,|\, A_2, B_2$.*

PROOF. Assume $a \in A \setminus (A_1 \cup A_2)$ and $b \in B \setminus (B_1 \cup B_2)$. By Theorem 11, $\mathcal{S}(A, B) \vDash a, A_1, b, B_1 \,|\, A_2, B_2$. By soundness of Symmetry axiom (Theorem 5), $\mathcal{S}(A, B) \vDash A_2, B_2 \,|\, a, A_1, b, B_1$. By soundness of Monotonicity axiom (Theorem 6), $\mathcal{S}(A, B) \vDash A_2, B_2 \,|\, A_1, B_1$. Again by soundness of Symmetry axiom, $\mathcal{S}(A, B) \vDash A_1, B_1 \,|\, A_2, B_2$. ∎

THEOREM 13. *Let A_1,A_2 be two disjoint subsets of A and B_1, B_2 be two disjoint subsets of B. If $A_1 \cup A_2$ is a proper subset of A, then $\mathcal{S}(A, B) \vDash A_1, B_1 \,|\, A_2, B_2$.*

PROOF. If $B_1 \cup B_2$ is a proper subset of B, then statement of the theorem follows from Theorem 12. Thus, we will assume that $B_1 \cup B_2 = B$. Since B is not empty, either B_1 or B_2 is also not empty. Without loss of generality (due to soundness of Symmetry axiom), we will assume that B_1 is not empty. Let $a \in A \backslash (A_1 \cup A_2)$. By Theorem 11, $\mathcal{S}(A, B) \vDash a, A_1, B_1 \mid A_2, B_2$. By soundness of Symmetry and Monotonicity axioms, $\mathcal{S}(A, B) \vDash A_1, B_1 \mid A_2, B_2$. ■

THEOREM 14. *Let A_1,A_2 be two disjoint subsets of A and B_1, B_2 be two disjoint subsets of B. If $\mathcal{S}(A, B) \nvDash A_1, B_1 \mid A_2, B_2$, then one of the following conditions is true:*

1. *$A = A_1$ and $B = B_2$ or*
2. *$A = A_2$ and $B = B_1$.*

PROOF. By Theorem 13, $A_1 \cup A_2 = A$ and $B_1 \cup B_2 = B$. Consider expression $A_1, B_1 \mid A_2, B_2$. If left-hand side of this expression contains mix of secret variables from both set A and set B, then, by Theorem 11, $\mathcal{S}(A, B) \vDash A_1, B_1 \mid A_2, B_2$. Contradiction. Similarly, if right-hand side of this expression contains mix of secret variables from A and B, then, by soundness of Symmetry axiom and by Theorem 11, $\mathcal{S}(A, B) \vDash A_1, B_1 \mid A_2, B_2$. Contradiction. Thus, neither of the two sides contains a mix of secret variables from both set A and set B. Note that sets A and B can not be on the same side of the expression due to soundness of Empty Set axiom (Theorem 4). Therefore, sets A and B are on two different sides of the expression. ■

6.3. Semantics Composition

In this section we will define composition of semantics. This is an operation on semantics that will be used later to combine multiple instances of semantics $\mathcal{S}(a)$ and $\mathcal{S}(A, B)$ into a single "canonical" semantics.

DEFINITION 16. *Let $\mathcal{S}_1 = \langle \mathcal{I}_1, \star_1 \rangle, \ldots, \mathcal{S}_n = \langle \mathcal{I}_n, \star_n \rangle$ be a finite set of semantics. We define composition of these semantics $\mathcal{S} = \langle \mathcal{I}, \star \rangle$ as follows:*

1. *$\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_n$,*
2. *$v^\star(\langle x_1, \ldots, x_n \rangle) = \langle v^{\star_1}(x_1), \ldots, v^{\star_n}(x_n) \rangle$.*

THEOREM 15. *Composition of a finite number of finite semantics is a finite semantics.*

THEOREM 16. *If $\mathcal{S}$ is a composition of semantics $\mathcal{S}_1, \ldots, \mathcal{S}_n$ and A and B are finite sets of secret variables, then $\mathcal{S} \vDash A \mid B$ if and only if $\mathcal{S}_i \vDash A \mid B$ for each $i \leq n$.*

PROOF. Assume that $A = \{a_1, \dots, a_m\}$ and $B = \{b_1, \dots, b_k\}$.
($\Rightarrow$) : Suppose $\mathcal{S} \vDash A \,|\, B$. We need to show that $\mathcal{S}_i \vDash A \,|\, B$, where i is an arbitrary index. Indeed, Let f and g be two functions such that for each outcome $t \in \mathcal{I}_i$

$$f(a_1^{\star_i}(t), \dots, a_m^{\star_i}(t)) = g(b_1^{\star_i}(t), \dots, b_k^{\star_i}(t))$$

We need to show that $f(a_1^{\star_i}(t), \dots, a_m^{\star_i}(t))$ is a constant function of t. To do this, define function F and G as follows:

$$F(u_1, \dots, u_m) = f(pr_i(u_1), \dots, pr_i(u_n)),$$

$$G(u_1, \dots, u_k) = g(pr_i(u_1), \dots, pr_i(u_k)),$$

where $pr_i(u)$ is the projection function that returns i-th component of a tuple. Note that for each $\langle t_1, \dots, t_n\rangle \in \mathcal{I}$,

$$\begin{aligned} F(a_1^\star(\langle t_1, \dots, t_n\rangle), \dots, a_m^\star(\langle t_1, \dots, t_n\rangle)) = \\ F(\langle a_1^{\star_1}(t_1), \dots, a_1^{\star_n}(t_n)\rangle, \dots, \langle a_m^{\star_1}(t_1), \dots, a_m^{\star_n}(t_n)\rangle) = \\ f(a_1^{\star_i}(t_i), \dots, a_m^{\star_i}(t_i)) = g(b_1^{\star_i}(t_i), \dots, b_k^{\star_i}(t_i)) = \\ G(\langle b_1^{\star_1}(t_1), \dots, b_1^{\star_n}(t_n)\rangle, \dots, \langle b_k^{\star_1}(t_1), \dots, b_k^{\star_n}(t_n)\rangle) = \\ G(b_1^\star(\langle t_1, \dots, t_n\rangle), \dots, b_k^\star(\langle t_1, \dots, t_n\rangle)). \end{aligned}$$

Thus, $F(a_1^\star(t), \dots, a_m^\star(t)) = G(b_1^\star(t), \dots, b_k^\star(t))$ for each $t \in \mathcal{I}$. Hence, by assumption $\mathcal{S} \vDash A \,|\, B$, function $F(a_1^\star(t), \dots, a_m^\star(t))$, as a function of t is a constant. By Definition 1, sets $\{\mathcal{I}_i\}_i$ are non-empty. Let $t_1^0, \dots, t_{i-1}^0, t_{i+1}^0, \dots, t_n^0$ be arbitrary elements from $\mathcal{I}_1, \dots, \mathcal{I}_{i-1}, \mathcal{I}_{i+1}, \dots, \mathcal{I}_n$. Note that

$$\begin{aligned} f(a_1^{\star_i}(t), \dots, a_m^{\star_i}(t)) = \\ F(a_1^\star(\langle t_1^0, \dots, t_{i-1}^0, t, t_{i+1}^0, \dots, t_n^0\rangle), \dots, a_m^\star(\langle t_1^0, \dots, t_{i-1}^0, t, t_{i+1}^0, \dots, t_n^0\rangle)). \end{aligned}$$

Since $F(a_1^\star(t), \dots, a_m^\star(t))$ is a constant function of $t \in \mathcal{I}$, we can conclude that $f(a_1^{\star_i}(t), \dots, a_m^{\star_i}(t))$ is a constant function of $t \in \mathcal{I}_i$.
($\Leftarrow$) : Suppose that $\forall i\, (\mathcal{S}_i \vDash A \,|\, B)$. Let us consider any two functions $F(u_1, \dots, u_m)$ and $G(u_1, \dots, u_k)$ such that

$$F(a_1^\star(t), \dots, a_m^\star(t)) = G(b_1^\star(t), \dots, b_k^\star(t))$$

for each $t \in \mathcal{I}$. We will need to prove that $F(a_1^\star(t), \dots, a_m^\star(t))$ is a constant function of $t \in \mathcal{I}$. Before doing so, however, we first will introduce a more convenient notations for writing arguments of function F and G. Notice that if $t = \langle t_1, \dots, t_n\rangle$, then, by definition of $\star$, $a_i^\star(t) = \langle a_i^{\star_1}(t_1), \dots, a_i^{\star_n}(t_n)\rangle$.

Thus, $F(a_1^\star(t),\ldots,a_m^\star(t))$ could be viewed as F applied to a list of tuples. We will arrange this list of tuples into a matrix as follows:

$$F(a_1^\star(t),\ldots,a_m^\star(t)) = F\begin{pmatrix} a_1^{\star_1}(t_1) & \ldots & a_1^{\star_n}(t_n) \\ \ldots & \ldots & \ldots \\ a_m^{\star_1}(t_1) & \ldots & a_m^{\star_n}(t_n) \end{pmatrix}.$$

Similarly,

$$G(b_1^\star(t),\ldots,b_k^\star(t)) = G\begin{pmatrix} b_1^{\star_1}(t_1) & \ldots & b_1^{\star_n}(t_n) \\ \ldots & \ldots & \ldots \\ b_k^{\star_1}(t_1) & \ldots & b_k^{\star_n}(t_n) \end{pmatrix}.$$

Assumption $F(a_1^\star(t),\ldots,a_m^\star(t)) = G(b_1^\star(t),\ldots,b_k^\star(t))$ for each $t \in \mathcal{I}$ could now be stated as

$$F\begin{pmatrix} a_1^{\star_1}(t_1) & \ldots & a_1^{\star_n}(t_n) \\ \ldots & \ldots & \ldots \\ a_m^{\star_1}(t_1) & \ldots & a_m^{\star_n}(t_n) \end{pmatrix} = G\begin{pmatrix} b_1^{\star_1}(t_1) & \ldots & b_1^{\star_n}(t_n) \\ \ldots & \ldots & \ldots \\ b_k^{\star_1}(t_1) & \ldots & b_k^{\star_n}(t_n) \end{pmatrix} \tag{5}$$

for each $t = \langle t_1,\ldots,t_n\rangle \in \mathcal{I}$.

Now let us return to the proof. We want to prove that $F(a_1^\star(t),\ldots,a_m^\star(t))$ is a constant function of $t \in \mathcal{I}$. Assume that there are $\langle t_1',\ldots,t_n'\rangle \in \mathcal{I}$ and $\langle t_1'',\ldots,t_n''\rangle \in \mathcal{I}$ such that

$$F\begin{pmatrix} a_1^{\star_1}(t_1') & \ldots & a_1^{\star_n}(t_n') \\ \ldots & \ldots & \ldots \\ a_m^{\star_1}(t_1') & \ldots & a_m^{\star_n}(t_n') \end{pmatrix} \neq F\begin{pmatrix} a_1^{\star_1}(t_1'') & \ldots & a_1^{\star_n}(t_n'') \\ \ldots & \ldots & \ldots \\ a_m^{\star_1}(t_1'') & \ldots & a_m^{\star_n}(t_n'') \end{pmatrix}. \tag{6}$$

Consider the following expression E_i for each $0 \leq i \leq n$:

$$E_i = F\begin{pmatrix} a_1^{\star_1}(t_1') & \ldots & a_1^{\star_i}(t_i') & a_1^{\star_{i+1}}(t_{i+1}'') & \ldots & a_1^{\star_n}(t_n'') \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_m^{\star_1}(t_1') & \ldots & a_m^{\star_i}(t_i') & a_m^{\star_{i+1}}(t_{i+1}'') & \ldots & a_m^{\star_n}(t_n'') \end{pmatrix}.$$

Note from non-equality (6) that the first and the last element of the sequence $E_0,\ldots,E_n$ are not equal. Thus, there must be two adjacent non-equal elements in this sequence. We will assume that $E_{\ell-1} \neq E_\ell$. Consider now function $f(u_1,\ldots,u_m)$, which is equal to

$$F\begin{pmatrix} a_1^{\star_1}(t_1') & \ldots & a_1^{\star_{\ell-1}}(t_{\ell-1}') & u_1 & a_1^{\star_{\ell+1}}(t_{\ell+1}'') & \ldots & a_1^{\star_n}(t_n'') \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\ a_m^{\star_1}(t_1') & \ldots & a_m^{\star_{\ell-1}}(t_{\ell-1}') & u_m & a_m^{\star_{\ell+1}}(t_{\ell+1}'') & \ldots & a_m^{\star_n}(t_n'') \end{pmatrix}.$$

Note that

$$f(a_1^{\star_\ell}(t''_\ell),\dots,a_m^{\star_\ell}(t''_\ell)) = E_{\ell-1} \neq E_\ell = f(a_1^{\star_\ell}(t'_\ell),\dots,a_m^{\star_\ell}(t'_\ell)). \qquad (7)$$

We also will define function $g(u_1,\dots,u_k)$ as

$$F\begin{pmatrix} b_1^{\star_1}(t'_1) & \dots & b_1^{\star_{\ell-1}}(t'_{\ell-1}) & u_1 & b_1^{\star_{\ell+1}}(t''_{\ell+1}) & \dots & a_1^{\star_n}(t''_n) \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ b_k^{\star_1}(t'_1) & \dots & b_k^{\star_{\ell-1}}(t'_{\ell-1}) & u_k & b_k^{\star_{\ell+1}}(t''_{\ell+1}) & \dots & b_k^{\star_n}(t''_n) \end{pmatrix}.$$

Note that for each $t \in \mathcal{I}_\ell$, $\langle t''_1,\dots,t'_{\ell-1},t,t'_{\ell+1},\dots,t'_n\rangle \in \mathcal{I}$. Thus, from equation (5), for each $t \in \mathcal{I}_\ell$,

$$f(a_1^{\star_\ell}(t),\dots,a_m^{\star_\ell}(t)) = g(b_1^{\star_\ell}(t),\dots,b_k^{\star_\ell}(t)).$$

By the assumption, $\forall i\,(\mathcal{S}_i \vDash A \,|\, B)$. In particular, $\mathcal{S}_\ell \vDash A \,|\, B$. Therefore, the above equality implies that $f(a_1^{\star_\ell}(t),\dots,a_m^{\star_\ell}(t))$ must be a constant function of $t \in \mathcal{I}_\ell$. This contradicts statement (7). ■

6.4. Completeness: final arguments

THEOREM 17. *For any finite set of secret variable A,*

$$\vdash \left(\bigwedge_{a\in A} a \,|\, a\right) \to A \,|\, A.$$

PROOF. By Empty Set axiom, $\vdash A \,|\, \varnothing$. By applying Public Knowledge axiom separately for each $a \in A$, we get $\{a \,|\, a\}_{a\in A} \vdash A \,|\, A$. Therefore, by the Deduction theorem for the classical propositional logic, $\vdash \left(\bigwedge_{a\in A} a \,|\, a\right) \to A \,|\, A$. ■

THEOREM 18. *For any formula $A \,|\, B$ and for any finite set of formulas $\{C_i \mid D_i\}_i$, if $\{C_i \mid D_i\}_i \nvdash A \,|\, B$, then there is a semantics $\mathcal{S} = \langle\{\mathcal{I}\},\star\rangle$ such that $\mathcal{S} \vDash C_i \,|\, D_i$ for each i, but, at the same time, $\mathcal{S} \nvDash A \,|\, B$.*

PROOF. We first define set PK (for "public knowledge") as

$$PK = \{a \,:\, \{C_i \mid D_i\}_i \vdash a \,|\, a\}.$$

There are four cases to consider:

1. If $A \cap B \not\subseteq PK$, then there is $a \in A \cap B$ such that $\{C_i \mid D_i\}_i \nvdash a \,|\, a$. Consider semantics $\mathcal{S}(a)$. By Theorem 8, $\mathcal{S}(a) \nvDash A \,|\, B$. We now need to prove that $\mathcal{S}(a) \vDash C_i \,|\, D_i$ for each i. Indeed, suppose that $\mathcal{S}(a) \nvDash C_{i_0} \,|\, D_{i_0}$ for some i_0. By Theorem 8, $a \in C_{i_0} \cap D_{i_0}$. Thus, by Monotonicity axiom and Symmetry axiom, $C_{i_0} \,|\, D_{i_0} \vdash a \,|\, a$. Hence, $\{C_i \mid D_i\}_i \vdash a \,|\, a$. Contradiction.

2. If $B \subseteq PK$, then, by Empty Set axiom, $\vdash A \,|\, (B \setminus PK)$. On the other hand, by Theorem 17, $\{C_i \mid D_i\}_i \vdash (B \cap PK) \,|\, (B \cap PK)$. By Public Knowledge axiom, $\{C_i \mid D_i\}_i \vdash A \,|\, (B \setminus PK), B \cap PK$. In other words, $\{C_i \mid D_i\}_i \vdash A \,|\, B$. Contradiction.

3. If $A \subseteq PK$, then, similarly, by Empty Set axiom, $\vdash B \,|\, (A \setminus PK)$. By Theorem 17, $\{C_i \mid D_i\}_i \vdash (A \cap PK) \,|\, (A \cap PK)$. By Public Knowledge Axiom, $\{C_i \mid D_i\}_i \vdash B \,|\, (A \setminus PK), A \cap PK$. Hence, $\{C_i \mid D_i\}_i \vdash B \,|\, A$. By Symmetry axiom, $\{C_i \mid D_i\}_i \vdash A \,|\, B$. Contradiction.

4. Finally, suppose that $A \setminus PK$ and $B \setminus PK$ are two non-empty disjoint set. Consider semantics $\mathcal{S} = \mathcal{S}(A \setminus PK, B \setminus PK)$. By Theorem 10, $\mathcal{S} \nvDash (A \setminus PK) \,|\, (B \setminus PK)$. By the soundness of Monotonicity and Symmetry axioms (Theorem 6 and Theorem 5), $\mathcal{S} \nvDash A \,|\, B$. We now only need to prove that $\mathcal{S} \vDash C_i \,|\, D_i$ for each i. Assume the opposite. Let there be such i_0 that $\mathcal{S} \nvDash C_{i_0} \,|\, D_{i_0}$.

   LEMMA 1. $C_{i_0} \cap D_{i_0} \subseteq PK$.

   PROOF. Assume that $a \in C_{i_0} \cap D_{i_0}$. Thus, by Monotonicity and Symmetry axioms, $C_{i_0} \,|\, D_{i_0} \vdash a \,|\, a$. Hence $\{C_i \mid D_i\}_i \vdash a \,|\, a$. Therefore, $a \in PK$. ■

   Now let's continue with the proof of the theorem. From assumption $\mathcal{S} \nvDash C_{i_0} \,|\, D_{i_0}$, by Theorem 9,

$$\mathcal{S} \nvDash C_{i_0} \cap ((A \setminus PK) \cup (B \setminus PK)) \,|\, D_{i_0} \cap ((A \setminus PK) \cup (B \setminus PK))$$

   which is equivalent to

$$\mathcal{S} \nvDash C_{i_0} \cap (A \setminus PK), C_{i_0} \cap (B \setminus PK) \,|\, D_{i_0} \cap (A \setminus PK), D_{i_0} \cap (B \setminus PK).$$

   Note that by the lemma, the following two subsets of $A \setminus PK$ are disjoint: $C_{i_0} \cap (A \setminus PK)$ and $D_{i_0} \cap (A \setminus PK)$. Similarly, $C_{i_0} \cap (B \setminus PK)$ and $D_{i_0} \cap (B \setminus PK)$ are disjoint subsets of $B \setminus PK$. Thus, by Theorem 14 from the above statement, either $A \setminus PK = C_{i_0} \cap (A \setminus PK)$ and $B \setminus PK =$

$D_{i_0} \cap (B \setminus PK)$ or $A \setminus PK = D_{i_0} \cap (A \setminus PK)$ and $B \setminus PK = C_{i_0} \cap (B \setminus PK)$. We will consider the former case. The later one could be treated similarly. Statements $A \setminus PK = C_{i_0} \cap (A \setminus PK)$ and $B \setminus PK = D_{i_0} \cap (B \setminus PK)$ imply that $A \setminus PK \subseteq C_{i_0}$ and $B \setminus PK \subseteq D_{i_0}$. Hence, by Monotonicity and Symmetry axioms, $C_{i_0} \,|\, D_{i_0} \vdash A \setminus PK \,|\, B \setminus PK$. Therefore,

$$\{C_i \mid D_i\}_i \vdash A \setminus PK \,|\, B \setminus PK.$$

At the same time, by Theorem 17, $\{C_i \mid D_i\}_i \vdash B \cap PK \,|\, B \cap PK$. Thus, by Public Knowledge axiom,

$$\{C_i \mid D_i\}_i \vdash A \setminus PK \,|\, B \setminus PK, B \cap PK.$$

By Symmetry Axiom,

$$\{C_i \mid D_i\}_i \vdash B \setminus PK, B \cap PK \,|\, A \setminus PK.$$

Again by Theorem 17, $\{C_i \mid D_i\}_i \vdash A \cap PK \,|\, A \cap PK$. Hence, by Public Knowledge axiom,

$$\{C_i \mid D_i\}_i \vdash B \setminus PK, B \cap PK \,|\, A \setminus PK, A \cap PK.$$

Therefore, $\{C_i \mid D_i\}_i \vdash B \,|\, A$. By Symmetry axiom, $\{C_i \mid D_i\}_i \vdash A \,|\, B$. Contradiction with the assumption of the theorem.

■

THEOREM 19 (completeness). *If $\mathcal{S} \vDash \phi$ for each semantics $\mathcal{S}$, then $\vdash \phi$.*

PROOF. Suppose that $\nvdash \phi$. Let V be the finite set of all secret variables that appear in ϕ. Let X be a maximal consistent set of formulas that use only variable from the set V such that X does not contain formula ϕ. Let $\{\neg(A_1 \,|\, B_1), \dots, \neg(A_n \,|\, B_n)\} \cup \{C_1 \,|\, D_1, \dots, C_k \,|\, D_k\}$ be the set of all atomic formulas in the set X. By Theorem 18, for each $i \le n$ there is a semantics $\mathcal{S}_i$ such that $\mathcal{S}_i \nvDash A_i \,|\, B_i$ and, for each $j \le k$, $\mathcal{S}_i \vDash C_j \,|\, D_j$. Let $\mathcal{S}$ be the composition of semantics $\mathcal{S}_1, \dots, \mathcal{S}_n$. By Theorem 16, $\mathcal{S} \nvDash A_i \,|\, B_i$ for each $i \le n$ and $\mathcal{S} \vDash C_j \,|\, D_j$ for each $j \le k$.

LEMMA 2. *For any formula ψ that only uses secret variables from set V,*

$$\psi \in X \text{ if and only if } \mathcal{S} \vDash \psi.$$

PROOF. Induction on the structural complexity of formula ψ. Base case follows from the choice of families of sets A_i, B_i, C_i and D_i. Induction step relies on the maximality and the consistency of the set X. ■

To conclude the proof of the completeness theorem, we only need to notice that $\phi \notin X$ by the choice of X. Hence, by the above lemma, $\mathcal{S} \not\models \phi$. ■

COROLLARY 1. *Logic of Secrets is decidable.*

PROOF. Logic of Secrets has a recursively enumerable axiomatization and is complete with respect to finite models. ■

7. Conclusion

In this article we have described a complete axiomatic systems for the independence relation. This result complements joint work of the author with Sara Miner More [10] on axiomatization of strong independence relation. One also can attempt to construct a single axiomatic system that captures properties of both relations. Of course, such system will include axioms of strong and "weak" independencies. In addition, it will also contain properties relating these two types of independence. A non-trivial example of such property is the following modified form of the Exchange axiom:

$$A \parallel B, C \to (B \,|\, C \to A, B \,|\, C).$$

To prove this property, assume that $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_k\}$, and $C = \{c_1, \ldots, c_m\}$. Consider semantics $\mathcal{S} = \langle \mathcal{I}, \star \rangle$ and suppose that there are functions f and g such that $f(a_1^\star(x), \ldots a_n^\star(x), b_1^\star(x), \ldots, b_k^\star(x)) = g(c_1^\star(x), \ldots, c_m^\star(x))$ for each $x \in \mathcal{I}$. We will need to prove that

$$f(a_1^\star(x), \ldots a_n^\star(x), b_1^\star(x), \ldots, b_k^\star(x))$$

is a constant function of x. By Definition 1, set $\mathcal{I}$ is not empty. Let x_0 be any element of set $\mathcal{I}$.

Consider an arbitrary $x \in \mathcal{I}$. Since $A^\star$ and $B^\star, C^\star$ are strongly independent, there is $y \in \mathcal{I}$ such that $a_i^\star(y) = a_i^\star(x_0)$ for each $i \leq n$ and $b_j^\star(y) = b_j^\star(x)$ for each $j \leq k$ and $c_j^\star(y) = c_j^\star(x)$ for each $j \leq m$. Thus,

$$f(a_1^\star(x_0), \ldots a_n^\star(x_0), b_1^\star(x), \ldots, b_k^\star(x)) = f(a_1^\star(y), \ldots a_n^\star(y), b_1^\star(y), \ldots, b_k^\star(y)) = \\ = g(c_1^\star(y), \ldots, c_m^\star(y)) = g(c_1^\star(x), \ldots, c_m^\star(x)).$$

In other words, if we define $h(t_1, \ldots, t_k) = f(a_1^\star(x_0), \ldots a_n^\star(x_0), t_1, \ldots, t_k)$, then we have $h(b_1^\star(x), \ldots, b_k^\star(x)) = g(c_1^\star(x), \ldots, c_m^\star(x))$ for each $x \in \mathcal{I}$. At the same time, by our assumption, sets $B^\star$ and $C^\star$ are independent. Hence, function $h(b_1^\star(x), \ldots, b_k^\star(x))$ is a constant function of x. Note, however, that

$$\begin{aligned} f(a_1^\star(x), \ldots a_n^\star(x), b_1^\star(x), \ldots, b_k^\star(x)) &= g(c_1^\star(x), \ldots, c_m^\star(x)) = \\ &= h(b_1^\star(x), \ldots, b_k^\star(x)). \end{aligned}$$

Therefore, $f(a_1^\star(x), \dots a_n^\star(x), b_1^\star(x), \dots, b_k^\star(x))$ is also a constant function of x. This concludes the proof. The complete axiomatization of properties connecting independence and strong independence relations remains an open problem.

8. Acknowledgment

The author is grateful to Sara Miner More for the discussions of the two types of independence relation at the initial stages of this work.

References

[1] W. W. Armstrong. Dependency structures of data base relationships. In *Information processing 74 (Proc. IFIP Congress, Stockholm, 1974)*, pages 580–583. North-Holland, Amsterdam, 1974.

[2] Catriel Beeri, Ronald Fagin, and John H. Howard. A complete axiomatization for functional and multivalued dependencies in database relations. In *SIGMOD '77: Proceedings of the 1977 ACM SIGMOD international conference on Management of data*, pages 47–61, New York, NY, USA, 1977. ACM.

[3] Michael S. Donders, Sara Miner More, and Pavel Naumov. Information flow on directed acyclic graphs. In Lev D. Beklemishev and Ruy de Queiroz, editors, *WoLLIC*, volume 6642 of *Lecture Notes in Computer Science*, pages 95–109. Springer, 2011.

[4] Hector Garcia-Molina, Jeffrey Ullman, and Jennifer Widom. *Database Systems: The Complete Book*. Prentice-Hall, second edition, 2009.

[5] Dan Geiger, Azaria Paz, and Judea Pearl. Axioms and algorithms for inferences involving probabilistic independence. *Inform. and Comput.*, 91(1):128–141, 1991.

[6] Joseph Y. Halpern and Kevin R. O'Neill. Secrecy in multiagent systems. *ACM Trans. Inf. Syst. Secur.*, 12(1):1–47, 2008.

[7] Robert Kelvey, Sara Miner More, Pavel Naumov, and Benjamin Sapp. Independence and functional dependence relations on secrets. In *Proceedings of 12th International Conference on the Principles of Knowledge Representation and Reasoning (Toronto, 2010)*, pages 528–533. AAAI, 2010.

[8] Sara Miner More and Pavel Naumov. An independence relation for sets of secrets. In H. Ono, M. Kanazawa, and R. de Queiroz, editors, *Proceedings of 16th Workshop on Logic, Language, Information and Computation (Tokyo, 2009), LNAI 5514*, pages 296–304. Springer, 2009.

[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. An independence relation for sets of secrets. *Studia Logica*, 94(1):73–85, 2010.

[11] Sara Miner More and Pavel Naumov. Hypergraphs of multiparty secrets. *Ann. Math. Artif. Intell.*, 62(1-2):79–101, 2011.

[12] Sara Miner More and Pavel Naumov. Logic of secrets in collaboration networks. *Ann. Pure Appl. Logic*, 162(12):959–969, 2011.

[13] Sara Miner More, Pavel Naumov, and Benjamin Sapp. Concurrency semantics for the Geiger-Paz-Pearl axioms of independence. In Marc Bezem, editor, *Computer Science Logic, 25th International Workshop / 20th Annual Conference of the EACSL, CSL 2011, September 12-15, 2011, Bergen, Norway, Proceedings*, volume 12 of *LIPIcs*, pages 443–457. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2011.

[14] Pavel Naumov and Brittany Nicholls. Game semantics for the Geiger-Paz-Pearl axioms of independence. In *The Third International Workshop on Logic, Rationality and Interaction(LORI-III), LNAI 6953*, pages 220–232. Springer, 2011.

[15] David Sutherland. A model of information. In *Proceedings of Ninth National Computer Security Conference*, pages 175–183, 1986.

Pavel Naumov
McDaniel College
Department of Mathematics and Computer Science
Westminster, Maryland, the United States
pnaumov@mcdaniel.edu