Symmetry in Information Flow

Jeffrey Kane and Pavel Naumov

Department of Mathematics and Computer Science
McDaniel College, Maryland, USA
{jmk001,pnaumov}@mcdaniel.edu

Abstract

The article investigates information flow properties of symmetric multi-party protocols. It gives a sound and complete axiomatic system for properties of the functional dependence predicate that are common to all protocols with the same group of symmetries.

1. Introduction

1.1. Symmetric Protocols

In this article we study properties of information flow under symmetric protocols. An example of such a protocol is the parity encryption protocol illustrated in Figure 1. Under this protocol, party p sends a binary message

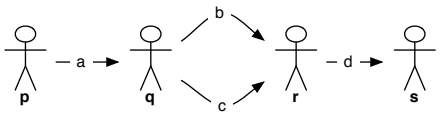

Figure 1: Parity Protocol.

a to a party q. Then q encodes it into b using random encryption key c in such a way that $a \equiv b + c \pmod 2$. It sends both the encrypted message b and the key c to party r. Party r decrypts message using formula $d \equiv b + c \pmod 2$ and sends the result to party s. This protocol is symmetric in the sense that if $a = x$, $b = y$, $c = z$, $d = t$ is a valid set of values under this

protocol, then so is $a = x$, $b = z$, $c = y$, $d = t$. We will formally express it by saying that permutation

$$\sigma = \begin{pmatrix} a & b & c & d \\ a & c & b & d \end{pmatrix}$$

is a symmetry of the protocol. We will also use a graphical way to describe symmetry σ as shown in Figure 2.

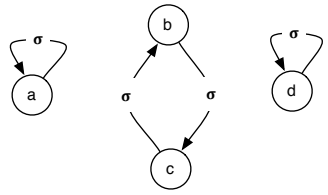

Figure 2: Symmetry σ of the Parity Protocol.

Another example of a symmetric protocol is an anonymous vote protocol. If a, b, and c represent votes of three different parties and m the majority vote, then if $a = x$, $b = y$, $c = z$, $m = t$ is a valid set of values, then so is $a = y$, $b = z$, $c = y$, $m = t$ or any other permutation of these values that preserves m. Using the language of abstract algebra, symmetries of this protocol are all permutations in the *stabilizer subgroup* of the element m.

In general, we specify symmetries of an information flow protocol by giving a group of permutations under which the protocol is invariant in the described above sense. The formal definition will be given in Section 3 below. Properties of symmetry in information [13] and especially in applications to model checking [7] have been studied before.

1.2. Functional Dependence

The properties of information flow protocols between different pieces of information, from now on referred to as secrets, can be studied in different languages. The language is specified by the choice of the predicate(s) it is using. A natural example of such predicate that we will be using in this article is *functional dependence*, which we denote by $a \rhd b$. It means that the value of secret a reveals the value of secret b. A more general form of functional dependence is functional dependence between sets of secrets. If A

and B are two sets of secrets, then $A \rhd B$ means that, together, the values of all secrets in A reveal the values of all secrets in B. Armstrong [1] presented the following sound and complete axiomatization of this relation:

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

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 dependence. Naumov and Nicholls axiomatized a related relation of rationally functional dependence in strategic games [14].

Another natural relation between secrets is the "nondeducibility" predicate introduced by Sutherland [15]. Halpern and O'Neill [5] proposed a closely-related notion called f-secrecy. More and Naumov [10] studied this relation between sets of secrets. A logical system that combines independence and functional dependence predicates was described by Kelvey, More, Naumov, and Sapp [6]. The relation on secrets, "secret a knows at least as much about secret c as secret b does" was axiomatized by More, Naumov, Nicholls, and Yang [12]. The properties of the information flow predicates that are specific to topological structure of the communication network have been also previously studied [3, 8, 9, 11].

In this article we study properties of functional dependence between single secrets in symmetric protocols. For example, consider a broadcasting protocol where party p upon receiving a message a sends messages b and c to parties q and r respectively. We first assume that p sends identical, but possibly different from a, messages b and c. This protocol has a symmetry σ depicted in Figure 3. It is clear that under this protocol $b \rhd c$. Note however,

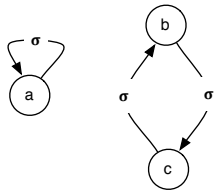

Figure 3: Symmetry σ of the Broadcast Protocol.

that if one considers another protocol, under which messages b and c do not have to be identical, then property $b \rhd c$ is no longer true in spite of the fact that the new protocol has the same symmetry σ. Thus, this property is specific to a protocol, not to the symmetry. In this article we study properties of the functional dependence between single secrets that are common to all protocols with the same group of symmetries. An example of such property for the group generated by symmetry σ depicted in Figure 3 is $b \rhd c \rightarrow c \rhd b$. This property is an instance of the Symmetry axiom in our logical system.

The Symmetry axiom is a very general principle, which is not specific to the functional dependence predicate. It is true for any predicate on a symmetric domain. An example of a property specific to the functional dependence predicate for the group generated by symmetry σ is $a \rhd b \rightarrow b \rhd c$. Indeed, since a is a fixed point of this symmetry the only way for a to reveal value of b is when values of b and c are equal. In this case, $b \rhd c$. This property is an instance of the Stability axiom in our logical system. Our main result is a completeness of the logical system that contains the Symmetry and Stability axioms and two additional not-symmetry-related properties of functional dependence.

2. Group Theory Terminology

In this section we review group theory vocabulary used throughout the rest of the paper.

In abstract algebra, a group is a pair $G = (\Sigma, \cdot)$, where Σ is an arbitrary set and $\cdot$ is an associative binary operation on Σ such that Σ contains an identity element and an inverse element for each element of Σ.

In this article, for any fixed set S by a group acting on S we mean an arbitrary set of permutations G of S (bijections from S onto S) such that

1. G is closed with respect to composition $\circ$,
2. G contains identity function,
3. if $\sigma \in G$, then $\sigma^{-1} \in G$.

By orbit $Orbit_G(s)$ of element $s \in S$ with respect to group G we mean the set $\{\sigma(s) \mid \sigma \in G\}$. By a stabilizer set G_s of an element s we mean the set $\{\sigma \in G \mid \sigma(s) = s\}$. It is easy to see that G_s is a subgroup of G.

3. Syntax and Semantics

In this section we give a formal definition of a protocol symmetric with respect to a particular group of symmetries.

Definition 1. *For any set S (of "secrets"), let $\Phi(S)$ be the minimal set of formulas such that*

1. $\bot \in \Phi(S)$,
2. $a \rhd b \in \Phi(S)$ *for each* $a, b \in S$,
3. $\phi \to \psi \in \Phi(S)$ *for each* $\phi, \psi \in \Phi(S)$.

Definition 2. *Let S be any set and G be any group acting on S. A symmetric protocol $\mathcal{P}$ over (S, G) is a pair (V, R) such that*

1. $V(a)$ *is a set (of "values" of secret a), such that* $V(\sigma(a)) \subseteq V(a)$ *for all* $a \in S$ *and all* $\sigma \in G$.
2. R *is a set of functions ("runs") r on S such that*
   (a) $r(a) \in V(a)$ *for each* $a \in S$,
   (b) $r \circ \sigma \in R$ *for each* $r \in R$ *and each* $\sigma \in G$.

The next definition is the core definition of this article. Part 2 of this definition formally specifies relation $a \rhd b$ between two secrets.

Definition 3. *For any protocol $\mathcal{P} = (V, R)$ over (S, G) and any formula $\phi \in \Phi(S)$, truth relation $\mathcal{P} \vDash \phi$ is defined recursively as follows:*

1. $\mathcal{P} \nvDash \bot$,
2. $\mathcal{P} \vDash a \rhd b$ *if and only if for any runs* $r_1, r_2 \in R$, *if* $r_1(a) = r_2(a)$, *then* $r_1(b) = r_2(b)$,
3. $\mathcal{P} \vDash \phi \to \psi$ *if and only if* $\mathcal{P} \nvDash \phi$ *or* $\mathcal{P} \vDash \psi$.

4. Axioms

In this section we introduce a logical system for properties of functional dependence in a protocol with a given group of symmetries G acting on the set of secrets S. The axioms of our logical system are:

1. Reflexivity: $a \rhd a$,
2. Transitivity: $a \rhd b \to (b \rhd c \to a \rhd c)$,
3. Symmetry: $a \rhd b \to \sigma(a) \rhd \sigma(b)$,

4. Stability: $a \rhd b \to b \rhd \sigma(b)$, where $\sigma \in G_a$.

We write $\vdash_G \phi$ if formula $\phi \in \Phi(S)$ is provable from the above axioms and propositional tautologies in the language $\Phi(S)$ using the modus ponens inference rule. We write $X \vdash_G \phi$ if formula ϕ is provable in our logical system using an additional set of axioms X.

5. Examples

In this section we give several examples of proofs in our formal system. Soundness and completeness of the system will be shown later.

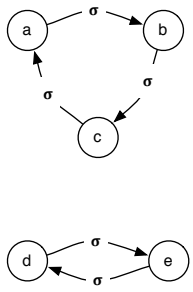

Figure 4: $\langle\sigma\rangle$ acting on $\{a, b, c, d, e\}$.

As common in abstract algebra, by $\langle\sigma_1, \ldots, \sigma_n\rangle$ we denote the group generated by symmetries $\sigma_1, \ldots, \sigma_n$.

Example 1. *If group $G = \langle\sigma\rangle$ is acting, as shown in Figure 4, on set $\{a, b, c, d, e\}$, then $\vdash_G a \rhd d \to e \rhd d$.*

Proof. Assume that $a \rhd d$. Note that $\sigma^3 \in G_a$. Thus, by the Stability axiom, $d \rhd \sigma^3(d)$. In other words, $d \rhd e$. By the Symmetry axiom, $\sigma(d) \rhd \sigma(e)$. Therefore, $e \rhd d$. □

Example 2. *If group $G = \langle\sigma, \tau\rangle$ is acting, as shown in Figure 5, on set $\{a, b, c, d\}$, then $\vdash_G a \rhd c \to c \rhd a$.*

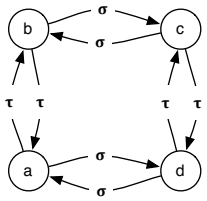

Figure 5: $\langle \sigma, \tau \rangle$ acting on $\{a, b, c, d\}$.

Proof. Assume $a \rhd c$. Thus[1], $(\sigma \circ \tau)a \rhd (\sigma \circ \tau)c$, by the Symmetry axiom. In other words, $c \rhd a$. □

Example 3. *If group $G = \langle \sigma, \tau \rangle$ is acting, as shown in Figure 6, on set $\{a, b, c, d, e, f, g, h, i\}$, then*

$$\vdash_G a \rhd f \to f \rhd e.$$

Proof. Note that $\sigma \circ \tau \in G_a$. Thus,

$$\vdash_G a \rhd f \to f \rhd (\sigma \circ \tau)f$$

by the Stability axiom. Hence, $\vdash_G a \rhd f \to f \rhd e$. □

The next two propositions are theorems provable in our system. We will refer to them later.

Proposition 1. $\vdash_G \sigma(a) \rhd a \to \sigma^k(a) \rhd a$, *for any non-negative integer k, any $\sigma \in G$, and any $a \in S$.*

Proof. Meta induction on parameter k. If $k = 0$, then

$$\vdash_G \sigma(a) \rhd a \to \sigma^k(a) \rhd a$$

by the Reflexivity axiom.

Next, assume that

$$\vdash_G \sigma(a) \rhd a \to \sigma^k(a) \rhd a$$

[1]We assume that $(f \circ g)(x) = f(g(x))$.

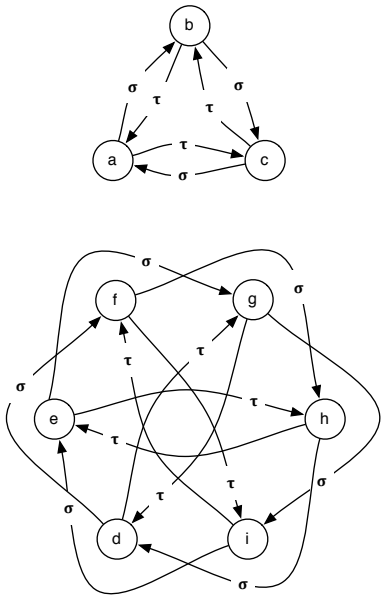

Figure 6: $\langle \sigma, \tau \rangle$ acting on $\{a, b, c, d, e, f, g, h, i\}$.

for $k \geq 0$. Thus, by the Symmetry axiom,

$$\vdash_G \sigma(a) \rhd a \to \sigma^{k+1}(a) \rhd \sigma(a).$$

Therefore, by the Transitivity axiom,

$$\vdash_G \sigma(a) \rhd a \to \sigma^{k+1}(a) \rhd a.$$

□

Proposition 2. *If $Orbit_G(b)$ is finite and $a \in Orbit_G(b)$, then $\vdash a \rhd b \to b \rhd a$.*

Proof. Let $a = \sigma(b)$. Consider sequence

$$b, \sigma(b), \sigma^2(b), \sigma^3(b), \ldots.$$

Due to set $Orbit(b)$ being finite, there must exist $i > j \geq 0$ such that $\sigma^i(b) = \sigma^j(b)$. Thus,

$$\sigma^{i-j}(b) = b. \tag{1}$$

Assumptions $a = \sigma(b)$ and $a \rhd b$ imply that $\sigma(b) \rhd b$. Hence, by Proposition 1, $\sigma^{i-j-1}(b) \rhd b$. Thus, $\sigma^{i-j}(b) \rhd \sigma(b)$ by the Symmetry axiom. Then $b \rhd \sigma(b)$, by equation (1). Therefore, $b \rhd a$ by the choice of σ. □

Next, we will show that Proposition 2 is false without the assumption that $Orbit_G(b)$ is finite. The example of the protocol for which this proposition does not hold can be constructed using a variation of Hilbert's infinite Grand Hotel. We will assume that the hotel has a countably infinite set of rooms numbered by all integers: $\ldots, -2, -1, 0, 1, 2, \ldots$. Each room is occupied by a guest and each guest knows names of all guests in the rooms with numbers no higher than hers. Thus, for example, guest in the room 27 knows who occupies rooms 27, 26, 25, and so on. Let secret s_i represent the knowledge of the guest in the room $i \in \mathbb{Z}$. Note that $s_{i+1} \rhd s_i$ is true, but $s_i \rhd s_{i+1}$ is false. Different runs of this protocol correspond to different room assignments to the guest of the hotel. Consider symmetry σ of this protocol such that $\sigma(s_i) = s_{i+1}$. This provides an infinite "counterexample" to Proposition 2.

In the next two examples we assume that σ is function $x/2$ on real numbers. Thus, group $G = \langle\sigma\rangle$ acts on the set $S = \mathbb{R}$ of all real numbers.

Example 4. *For any $n \geq 0$,*

$$\vdash_G \frac{1}{2} \rhd 1 \to \frac{1}{2^n} \rhd 1.$$

Proof. See Proposition 1. □

Example 5. *For any integer n,*

$$\vdash_G 0 \rhd 1 \to 1 \rhd \frac{1}{2^n}.$$

Proof. Note that $\sigma^n \in G_0$. Thus, by the Stability axiom, $\vdash_G 0 \rhd 1 \to 1 \rhd \frac{1}{2^n}$. □

6. Soundness

Theorem 1. *If $\vdash_G \phi$, then $\mathcal{P} \vDash \phi$, for any group G acting on set S, any $\phi \in \Phi(S)$, and any protocol $\mathcal{P}$ over (S, G).*

Proof. We will prove soundness of each axiom as a separate lemma. Each of the individual proofs relies upon Definition 3.

Lemma 1 (reflexivity). *$\mathcal{P} \vDash a \rhd a$ for each protocol $\mathcal{P}$ over (S, G) and each $a \in S$.*

Proof. If $r_1(a) = r_2(a)$, then $r_1(a) = r_2(a)$. □

Lemma 2 (transitivity). *For any secrets $a, b, c \in S$ and any protocol $\mathcal{P}$ over (S, G), if $\mathcal{P} \vDash a \rhd b$ and $\mathcal{P} \vDash b \rhd c$, then $\mathcal{P} \vDash a \rhd c$.*

Proof. Suppose that $r_1(a) = r_2(a)$, then, by the first assumption, $r_1(b) = r_2(b)$. Therefore, by the second assumption, $r_1(c) = r_2(c)$. □

Lemma 3 (symmetry). *For any protocol $\mathcal{P}$ over (S, G), any secrets $a, b \in S$, and any symmetry $\sigma \in G$, if $\mathcal{P} \vDash a \rhd b$, then $\mathcal{P} \vDash \sigma(a) \rhd \sigma(b)$.*

Proof. Suppose that $r_1(\sigma(a)) = r_2(\sigma(a))$. Thus, $(r_1 \circ \sigma)(a) = (r_2 \circ \sigma)(a)$. Hence, by the assumption of the lemma, $(r_1 \circ \sigma)(b) = (r_2 \circ \sigma)(b)$. Therefore, $r_1(\sigma(b)) = r_2(\sigma(b))$. □

Lemma 4 (stability). *For any protocol $\mathcal{P} = (V, R)$ over (S, G), any secrets $a, b \in S$, and any symmetry $\sigma \in G_a$, if $\mathcal{P} \vDash a \rhd b$, then $\mathcal{P} \vDash b \rhd \sigma(b)$.*

Proof. We first will show that for any run $r \in R$:

$$r(b) = r(\sigma(b)). \tag{2}$$

Indeed, $a = \sigma(a)$ because $\sigma \in G_a$. Thus, $r(a) = r(\sigma(a))$. In other words, $r(a) = (r \circ \sigma)(a)$. Hence, by the assumption of the lemma, $r(b) = (r \circ \sigma)(b)$. Therefore, $r(b) = r(\sigma(b))$.

To finish the proof of the lemma, suppose that $r_1(b) = r_2(b)$. Hence, $r_1(\sigma(b)) = r_2(\sigma(b))$ by the equation (2). □
This concludes the proof of Theorem 1. □

7. Completeness

Theorem 2. *For any group G acting on set S and any $\phi \in \Phi(S)$, if $\nvdash_G \phi$, then there is a protocol $\mathcal{P}$ over (S, G) such that $\mathcal{P} \not\models_G \phi$.*

We start the proof of the completeness theorem with several technical definitions and lemmas. The proof of the theorem itself appears in Section 7.3.

7.1. Protocol $\mathcal{P}_b$

Let X be any subset of $\Phi(S)$ and b be any element of S. In this section we will define protocol $\mathcal{P}_b$. Later we will prove the completeness theorem by combining such protocols for all $b \in S$.

Orbits partition set S into disjoint subsets. We pick a unique representative from each orbit. If $a \in S$, then the unique representative of $Orbit_G(a)$ is denoted by $\hat{a}$. We will next define $V(a)$ for each element $a \in S$. Elements from the same orbit will have the same set $V(a)$.

Definition 4. *Let $V(a)$ be the set of functions v on set $Orbit_G(b)$ such that for any z,*

$$v(z) \in \begin{cases} \{0,1\} & \text{if } X \vdash \hat{a} \rhd z, \\ \{0\} & \text{otherwise.} \end{cases}$$

Lemma 5. *$V(\sigma(a)) = V(a)$ for each $a \in S$ and each $\sigma \in G$.* □

Definition 5. *A function r is a run if and only if for all $a_1, a_2 \in S$, all $z_1, z_2 \in Orbit_G(b)$, and all $\sigma_1, \sigma_2 \in G$ if*

1. $a_1 = \sigma_1(\widehat{a_1})$,
2. $a_2 = \sigma_2(\widehat{a_2})$,
3. $\sigma_1(z_1) = \sigma_2(z_2)$,
4. $X \vdash \widehat{a_1} \rhd z_1$,
5. $X \vdash \widehat{a_2} \rhd z_2$,

then $r(a_1)(z_1) = r(a_2)(z_2)$.

Lemma 6. *If $r \in R$, then $r \circ \mu \in R$ for each $\mu \in G$.*

Proof. Suppose that for some $a_1, a_2 \in S$, some $z_1, z_2 \in Orbit_G(b)$, and some $\sigma_1, \sigma_2 \in G$:

$$a_1 = \sigma_1(\widehat{a_1}), \qquad a_2 = \sigma_2(\widehat{a_2}), \qquad \sigma_1(z_1) = \sigma_2(z_2),$$
$$X \vdash \widehat{a_1} \rhd z_1, \qquad X \vdash \widehat{a_2} \rhd z_2.$$

We will prove that $r(\mu(a_1))(z_1) = r(\mu(a_2))(z_2)$. Indeed, $\widehat{\mu(a_1)} = \widehat{a_1}$, because $\mu(a_1) \in Orbit(a_1)$. Similarly, $\widehat{\mu(a_2)} = \widehat{a_2}$. Thus,

$$a_1 = \sigma_1(\widehat{\mu(a_1)}), \quad a_2 = \sigma_2(\widehat{\mu(a_2)}), \quad \sigma_1(z_1) = \sigma_2(z_2),$$
$$X \vdash \widehat{\mu(a_1)} \rhd z_1, \qquad X \vdash \widehat{\mu(a_2)} \rhd z_2.$$

Hence,

$$\mu(a_1) = \mu(\sigma_1(\widehat{\mu(a_1)})), \quad \mu(a_2) = \mu(\sigma_2(\widehat{\mu(a_2)})),$$
$$\mu(\sigma_1(z_1)) = \mu(\sigma_2(z_2)),$$
$$X \vdash \widehat{\mu(a_1)} \rhd z_1, \quad X \vdash \widehat{\mu(a_2)} \rhd z_2.$$

Thus, by the assumption $r \in R$ and Definition 5,

$$r(\mu(a_1))(z_1) = r(\mu(a_2))(z_2).$$

□

This completes the definition of the protocol $\mathcal{P}_b$.

Lemma 7. *If $X \vdash c \rhd d$, then $\mathcal{P}_b \vDash c \rhd d$, for each $c, d \in S$.*

Proof. Let r_1, r_2 be two valid runs of the protocol $\mathcal{P}_b$. Suppose that $r_1(c) = r_2(c)$. We will show that $r_1(d) = r_2(d)$. Let z be any element of $Orbit_G(b)$. It will be sufficient to show that $r_1(d)(z) = r_2(d)(z)$. If $X \nvdash \hat{d} \rhd z$, then, by Definition 4, $r_1(d)(z) = 0 = r_2(d)(z)$.

We will now assume that

$$X \vdash \hat{d} \rhd z. \tag{3}$$

Let $c = \sigma_1(\hat{c})$ and $d = \sigma_2(\hat{d})$ for some $\sigma_1, \sigma_2 \in G$. Next, we will use Definition 5 to show that

$$r_1(c)(\sigma_1^{-1}(\sigma_2(z))) = r_1(d)(z) \tag{4}$$
$$r_2(c)(\sigma_1^{-1}(\sigma_2(z))) = r_2(d)(z) \tag{5}$$

To do so, we need to verify conditions 1.-5. of Definition 5:

1. $c = \sigma_1(\hat{c})$ by the choice of σ_1.
2. $d = \sigma_2(\hat{d})$ by the choice of σ_2.
3. $\sigma_1(\sigma_1^{-1}(\sigma_2(z))) = (\sigma_1 \circ \sigma_1^{-1})(\sigma_2(z)) = \sigma_2(z)$.
4. By the Symmetry axiom, assumption (3) implies that $X \vdash \sigma_2(\hat{d}) \rhd \sigma_2(z)$. Thus, $X \vdash d \rhd \sigma_2(z)$ by the choice of σ_2. By the Transitivity axiom and the assumption of the lemma, $X \vdash c \rhd \sigma_2(z)$. Hence, $X \vdash \sigma_1(\hat{c}) \rhd \sigma_2(z)$, by the choice of σ_1. By the Symmetry axiom, $X \vdash \sigma_1^{-1}(\sigma_1(\hat{c})) \rhd \sigma_1^{-1}(\sigma_2(z))$. Hence, $X \vdash \hat{c} \rhd \sigma_1^{-1}(\sigma_2(z))$.
5. By the assumption (3), $X \vdash \hat{d} \rhd z$.

Finally, note that equations (4) and (5) together with assumption $r_1(c) = r_2(c)$ imply that $r_1(d)(z) = r_2(d)(z)$. □

Definition 6. *Let $r_0(c)(z) = 0$ for each $c \in S$ and each $z \in Orbit_G(b)$.*

Lemma 8. *r_0 is a run of the protocol $\mathcal{P}_b$.*

Proof. See Definition 5. □

Definition 7. *For each $c = \sigma(\hat{c}) \in S$ and each $z \in Orbit_G(b)$, let*

$$r_1(c)(z) = \begin{cases} 1 & \text{if } X \vdash \sigma(z) \rhd b \text{ and } X \vdash \hat{c} \rhd z, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 9. *Function r_1 is well-defined.*

Proof. Suppose that $\sigma_1(\hat{c}) = \sigma_2(\hat{c})$. We will show that if $X \vdash \sigma_1(z) \rhd b$ and $X \vdash \hat{c} \rhd z$, then $X \vdash \sigma_2(z) \rhd b$.

Assumption $\sigma_1(\hat{c}) = \sigma_2(\hat{c})$ implies that $\hat{c} = \sigma_2^{-1}(\sigma_1(\hat{c}))$. Thus, by the assumption $X \vdash \hat{c} \rhd z$ and the Stability axiom, $X \vdash z \rhd \sigma_2^{-1}(\sigma_1(z))$. Hence, by the Symmetry axiom, $X \vdash \sigma_2(z) \rhd \sigma_1(z)$. Therefore, $X \vdash \sigma_2(z) \rhd b$ by the Transitivity axiom and the assumption $X \vdash \sigma_1(z) \rhd b$. □

Lemma 10. *r_1 is a run of the protocol $\mathcal{P}_b$.*

Proof. Consider any $a_1, a_2 \in S$, any $z_1, z_2 \in Orbit_G(b)$, and any $\sigma_1, \sigma_2 \in G$ such that

1. $a_1 = \sigma_1(\widehat{a_1})$,
2. $a_2 = \sigma_2(\widehat{a_2})$,
3. $\sigma_1(z_1) = \sigma_2(z_2)$,
4. $X \vdash \widehat{a_1} \rhd z_1$,
5. $X \vdash \widehat{a_2} \rhd z_2$.

We will show that $r_1(a_1)(z_1) = r_1(a_2)(z_2)$. By Definition 7, it will be sufficient that if either the value of $r_1(a_1)(z_1)$ or the value of $r_1(a_2)(z_2)$ is equal to 1, then the other value is also equal to 1. Without loss of generality, suppose that $r_1(a_1)(z_1) = 1$. Thus, by Definition 7, $X \vdash \sigma_1(z_1) \rhd b$. Hence, by the assumption 3. above, $X \vdash \sigma_2(z_2) \rhd b$. Then, taking into account assumption 5. and Definition 7, we have $r_1(a_2)(z_2) = 1$. □

Lemma 11. *If $X \nvdash a \rhd b$, then $r_1(a)(z) = 0$ for each $a \in S$ and each $z \in Orbit_G(b)$.*

Proof. Suppose there are $a \in S$ and $z \in Orbit_G(b)$ such that $r_1(a)(z) = 1$. Let $a = \sigma(\hat{a})$ for some $\sigma \in G$. Hence, $X \vdash \sigma(z) \rhd b$ and $X \vdash \hat{a} \rhd z$, by Definition 7. By the Symmetry axiom, $X \vdash \sigma(\hat{a}) \rhd \sigma(z)$. Hence, $X \vdash a \rhd \sigma(z)$. Therefore, by the Transitivity axiom, $X \vdash a \rhd b$. □

Lemma 12. $r_1(b)(\hat{b}) = 1$.

Proof. Let $b = \sigma(\hat{b})$ for some $\sigma \in G$. By the Reflexivity axiom,

$$X \vdash \hat{b} \rhd \hat{b}. \tag{6}$$

By the Symmetry axiom, $X \vdash \sigma(\hat{b}) \rhd \sigma(\hat{b})$, In other words, $X \vdash \sigma(\hat{b}) \rhd b$. Therefore, $r_1(b)(\hat{b}) = 1$ by Definition 7 and statement (6). □

Lemma 13. *If $\mathcal{P}_b \models a \rhd b$, then $X \vdash a \rhd b$, for each $a \in S$.*

Proof. Suppose that there is $a \in S$ such that $X \nvdash a \rhd b$. Consider runs r_0 and r_1 defined above. By Lemma 11 and Definition 6, $r_1(a) = 0 = r_0(a)$. At the same time, $r_0(b)(\hat{b}) = 0 \neq 1 = r_1(b)(\hat{b})$, by Lemma 12 and Definition 6. Therefore, $\mathcal{P}_b \not\models a \rhd b$. □

7.2. Protocol Composition

In this section we introduce a way to combine several different protocols over (S, G) into a single protocol.

Definition 8. *If $\mathcal{P}_1 = (V_1, R_1), \ldots, \mathcal{P}_n = (V_n, R_n)$ are protocols over (S, G), then $\mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ is a protocol (V, R) over (S, G) such that*

1. *$V(a) = V_1(a) \times \cdots \times V_n(a)$, for each $a \in S$,*
2. *R is a set of all functions $r(x) = \langle r_1(x), \ldots, r_n(x)\rangle$ for all $r_1 \in R_1, \ldots, r_n \in R_n$.*

Lemma 14. *Let $\mathcal{P}_1 = (V_1, R_1), \ldots, \mathcal{P}_n = (V_n, R_n)$ be protocols over (S, G) such that set R_k is not empty for each $k \leq n$. Then $\mathcal{P}_1 \times \cdots \times \mathcal{P}_n \vDash c \rhd d$ if and only if $\mathcal{P}_k \vDash c \rhd d$ for each $k \leq n$.*

Proof. ($\Rightarrow$) : Suppose that $r_k^1, r_k^2 \in R_k$ are such that $r_k^1(c) = r_k^2(c)$. We will show that $r_k^1(d) = r_k^2(d)$.

Let (V, R) be protocol $\mathcal{P}_1 \times \cdots \times \mathcal{P}_n$. Consider any runs

$$r_1 \in R_1, \ldots, r_{k-1} \in R_{k-1}, r_{k+1} \in R_{k+1}, \ldots, r_n \in R_n.$$

Let $r^1, r^2 \in R$ be such that for each $x \in S$

$$r^1(x) = \langle r_1(x), \ldots, r_{k-1}(x), r_k^1(x), r_{k+1}(x), \ldots, r_n(x)\rangle,$$

$$r^2(x) = \langle r_1(x), \ldots, r_{k-1}(x), r_k^2(x), r_{k+1}(x), \ldots, r_n(x)\rangle.$$

Note that $r_k^1(c) = r_k^2(c)$ implies that $r^1(c) = r^2(c)$. Hence, by the assumption of the lemma, $r^1(d) = r^2(d)$. Therefore, $r_k^1(d) = r_k^2(d)$.
($\Leftarrow$) : Suppose that $r^1, r^2 \in R$ are such that $r^1(c) = r^2(c)$. We will show that $r^1(d) = r^2(d)$. Let

$$r^1(x) = \langle r_1^1(x), \ldots, r_n^1(x)\rangle,$$

$$r^2(x) = \langle r_1^2(x), \ldots, r_n^2(x)\rangle.$$

Assumption $r^1(c) = r^2(c)$ implies that $r_k^1(c) = r_k^2(c)$ for each $k \leq n$. Thus, by the assumption of the lemma, $r_k^1(d) = r_k^2(d)$ for each $k \leq n$. Therefore, $r^1(d) = r^2(d)$. □

7.3. Completeness: final steps

We are now ready to finish the proof of the completeness theorem that has been stated earlier as Theorem 2.

Proof. Assume that $\nvdash_G \phi$. Let X be a maximal consistent subset of $\Phi(S)$ that contains $\neg\phi$. Let $S = \{b_1, \ldots, b_n\}$. For each $i \leq n$ consider defined above protocol $\mathcal{P}_{b_i}$ and define $\mathcal{P} = \mathcal{P}_{b_1} \times \cdots \times \mathcal{P}_{b_n}$.

Lemma 15. *For each $a, b \in S$,*

$$\mathcal{P} \models a \rhd b \qquad \textit{if and only if} \qquad a \rhd b \in X.$$

Proof. ($\Rightarrow$) : Suppose that $\mathcal{P} \models a \rhd b$. Note that by Lemma 8, each of the protocols $\{\mathcal{P}_{b_i}\}_{i \leq n}$ has at least one run. Thus, by Lemma 14, $\mathcal{P}_{b_i} \models a \rhd b$ for each $i \leq n$. In particular, $\mathcal{P}_b \models a \rhd b$. Hence, by Lemma 13, $X \vdash a \rhd b$. Therefore, $a \rhd b \in X$, due to maximality of set X.
($\Leftarrow$) : Assume that $X \vdash a \rhd b$. Thus, by Lemma 7, $\mathcal{P}_{b_i} \models a \rhd b$ for each $i \leq n$. Note again that by Lemma 8, each of the protocols $\{\mathcal{P}_{b_i}\}_{i \leq n}$ has at least one run. Therefore, by Lemma 14, $\mathcal{P} \models a \rhd b$. □

Lemma 16. *For each $\psi \in \Phi(S)$,*

$$\mathcal{P} \models \psi \qquad \textit{if and only if} \qquad \psi \in X.$$

Proof. Induction on the structural complexity of formula ψ. Case ψ being $\bot$ follows from the assumption of consistency of X and Definition 3. If ψ is an atomic formula $a \rhd b$, then statement of the lemma follows from Lemma 15. The induction step follows from the maximality and consistence of set X in the standard way. □

Recall now that $\neg\phi \in X$. Hence, $\phi \notin X$ due to consistency of X. Therefore, $\mathcal{P} \not\models \phi$ by Lemma 16. This concludes the proof of Theorem 2. □

8. Conclusion

In this article with gave a complete axiomatization of properties of functional dependence in symmetric protocols. We have been assuming that a symmetry is a bijection of the set into itself. In a more general setting,

symmetries can be defined as injections of the set into itself. The set of bijective symmetries forms a group with respect to composition. The injective symmetries only form a monoid (informally, group without inverses). An example of an injective symmetry is an injection of the Sierpinski triangle (see Figure 7) into the upper quarter of the triangle.

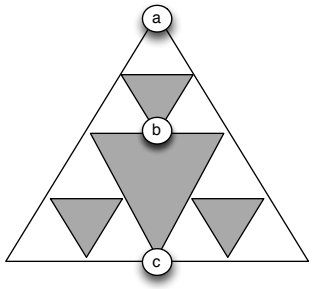

Figure 7: Second iteration of Sierpinski triangle.

It is easy to check that our axioms are sound with respect to such symmetries. Let, for example, a, b, and c be the points of the Sierpinski triangle as shown in Figure 7 and M be the monoid of injective symmetries of the Sierpinski triangle. Then, $\vdash_M a \rhd c \to a \rhd b$ by the Symmetry axiom and $\vdash_M a \rhd c \to c \rhd b$ by the Stability axiom. Since our proof of completeness heavily relies on invertibility of symmetries, axiomatization of all properties of functional dependencies with respect to an arbitrary monoid of injective symmetries remains an open question.

Another open question is an axiomatization of properties of functional dependencies between sets of secrets for a given group of symmetries. Such axiomatization would include Armstrong axiom, the Symmetry axiom, the Stability axiom, and, possibly, some other not yet discovered properties.

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

[6] 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.

[7] Alice Miller, Alastair F. Donaldson, and Muffy Calder. Symmetry in temporal logic model checking. *ACM Comput. Surv.*, 38(3), 2006.

[8] 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.

[9] 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.

[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. The functional dependence relation on hypergraphs of secrets. In João Leite, Paolo Torroni, Thomas

Ågotnes, Guido Boella, and Leon van der Torre, editors, *CLIMA*, volume 6814 of *Lecture Notes in Computer Science*, pages 29–40. Springer, 2011.

[12] Sara Miner More, Pavel Naumov, Brittany Nicholls, and Andrew Yang. A ternary knowledge relation on secrets. In Krzysztof R. Apt, editor, *Proceedings of the 13th Conference on Theoretical Aspects of Rationality and Knowledge (TARK-2011), Groningen, The Netherlands, July 12-14, 2011*, pages 46–54. ACM, 2011.

[13] Fionn Murtagh. Symmetry in data mining and analysis: A unifying view based on hierarchy. *Proceedings of the Steklov Institute of Mathematics*, 265:177–198, 2009. 10.1134/S0081543809020175.

[14] Pavel Naumov and Brittany Nicholls. Rationally functional dependence. In *10th Conference on Logic and the Foundations of Game and Decision Theory (LOFT)*, 2012.

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