Knowledge in Communication Networks

Pavel G. Naumov* Jia Tao*

January 28, 2016

Abstract

The article investigates epistemic properties of information flow under communication protocols with a given topological structure of the communication network. The main result is a sound and complete logical system that describes all such properties. The system consists of a variation of the multi-agent epistemic logic S5 extended by a new network-specific Gateway axiom.

1 Introduction

In this article we study epistemic properties of communication protocols. Consider, for example, a protocol $\mathcal{P}_1$ between agents p, q, u, and v. Under this protocol, agent p communicates to agent q a message over a secure communication channel m. Next, agent q must communicate the same message over insecure channels to agent u. To achieve this, agent q chooses a random one-time encryption pad ("key") and computes a ciphertext as a bit-wise sum of the message and the key modulo 2. Agent q then sends the key and the ciphertext to agent u over insecure channels k and c accordingly. Finally, agent u, upon receiving the key and the ciphertext, computes a bit-wise sum of these two strings modulo 2 and communicates the result over a secure channel m' to agent v.

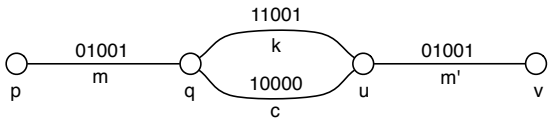

Figure 1: Run r_1 of protocol $\mathcal{P}_1$.

* Department of Computer Science, Illinois Wesleyan University, Bloomington, Illinois, the United States, pavel@pavelnaumov.com

* Department of Computer Science, The College of New Jersey, Ewing, New Jersey, the United States, taoj@tcnj.edu

A *run* of a protocol is an assignment of values to all communication channels that satisfy the restrictions imposed by the protocol. An example of a run r_1 of protocol $\mathcal{P}_1$ is depicted in Figure 1. Note that for any run satisfying the restrictions of $\mathcal{P}_1$, the value of channel m is the same as the value of channel m'. Thus, any outside observer who can eavesdrop on channel m under run r_1 would be able to learn that channel m' has a value of 01001 on this run. Using epistemic modal logic notations[1], we write this as

$$r_1 \Vdash \Box_m(m' = 01001).$$

At the same time, since there is no connection between the values of the ciphertext c and the original message m, an external observer eavesdropping on channel c would not be able to deduce the value of channel m':

$$r_1 \Vdash \neg\Box_c(m' = 01001). \tag{1}$$

Similarly,

$$r_1 \Vdash \neg\Box_k(m' = 01001). \tag{2}$$

We now consider a variation of protocol $\mathcal{P}_1$ that we call $\mathcal{P}_2$. Under the second protocol agents q and u are allowed to make a mistake in at most one bit during the encryption and the decryption stages respectively. In other words, the Hamming distance between the value of channel c and the bit-wise sum of values of channels m and k is no more than one. Similarly, the Hamming distance between the value of channel m' and the bit-wise sum of values of channels c and k is no more than one. An example of a run r_2 of protocol $\mathcal{P}_2$ is depicted on Figure 2.

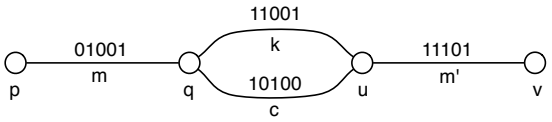

Figure 2: Run r_2 of protocol $\mathcal{P}_2$.

Note that run r_1 is also a valid run of protocol $\mathcal{P}_2$. Thus, an external observer eavesdropping on channel m on run r_2 is not able to distinguish run r_2 from run r_1. Hence, such an observer would not be able to conclude that the value of m' is 11101. Therefore, under protocol $\mathcal{P}_2$,

$$r_2 \Vdash \neg\Box_m(m' = 11101).$$

At the same time, an external observer eavesdropping on channel m on run r_2 of protocol $\mathcal{P}_2$ should be able to conclude that the value of channel m' is *not*

[1]Similarly to Kane and Naumov [1], we interpret modality $\Box_m$ as "any outside observer who can eavesdrop on channel m knows that ...", instead of more traditional "agent m knows that ..." [2].

01110 because the Hamming distance between 01001 and 01110 is three and, according to the restrictions of protocol $\mathcal{P}_2$, errors could be introduced in at most two bits during the encryption and the decryption stages combined:

$$r_2 \Vdash \Box_m(m' \neq 01110).$$

We now consider another variation of protocol $\mathcal{P}_1$ that we call $\mathcal{P}_3$, see Figure 3. The original message m in this protocol is first encrypted into a cyphertext c using a key k, then it is recovered as m', then again encrypted and recovered as m''. A single bit-error could be introduced by each encryption and decryption stage. Thus, the Hamming distance between strings m and m'' could be at most four. Figure 3 shows a possible run r_3 of this protocol.

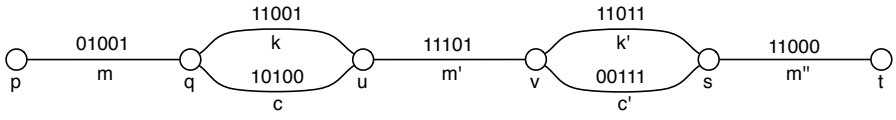

Figure 3: Run r_3 of protocol $\mathcal{P}_3$.

An external observer eavesdropping on channel m on run r_3 under $\mathcal{P}_3$ would not be able to know the exact value of m'. However, it would know that the value of channel m' is at a Hamming distance no more than two from the value of m. Note that the Hamming distance between the value of m and the string 10110 is five. Thus, due to the triangle inequality, the observer would be able to conclude that the Hamming distance between the value of m' and the string 10110 is at least three. Based on this, the observer would be able to conclude that any other observer eavesdropping on channel m' should know that the value of m'' is *not* equal to 10110:

$$r_3 \Vdash \Box_m\Box_{m'}(m'' \neq 10110).$$

So far we have discussed epistemic properties of individual runs. A property which is true on one run does not have to be true on another. For example, the above formula $\Box_m\Box_{m'}(m'' \neq 10110)$ is not true on any run in which the value of channel m is 10110. However, a similar property is true on all runs of protocol $\mathcal{P}_3$:

$$(m = 01001) \rightarrow \Box_m\Box_{m'}(m'' \neq 10110). \tag{3}$$

Another property true for all runs of protocol $\mathcal{P}_3$ is

$$\Box_{m'}(m \neq 00000) \rightarrow \Box_{m'}(m'' \neq 00000). \tag{4}$$

Indeed, the assumption $\Box_{m'}(m \neq 00000)$ tells us that an observer of channel m' on the current run can conclude that $m \neq 00000$. Since at most two mistakes can be introduced between channels m and m', we can conclude that the

message that the observer sees on channel m' contains at least three digits of 1. Therefore, for a similar reason, this observer will conclude that $m'' \neq 00000$.

A property true for all runs of one protocol does not have to be true for all runs of some other protocols. For example, property (3) is false under protocol where up to two bits could be corrupted during each encryption and each decryption stage. Property (4) is not true under a protocol where agents q and u, unlike agents s and t, are not allowed to make mistakes.

In this article we study epistemic properties common to all protocols that have the same topological structure[2] of communication networks. Consider, for example, property

$$\Box_m(m'' \neq 00000) \rightarrow \Box_{m'}(m'' \neq 00000). \tag{5}$$

We will see later in this article that this property is true for each protocol where, as in Figure 3, communication between channels m and m'' happens only through channel m'.

The above formula (5) involves inequality. Neither inequality nor equality is a part of the language of our system. We only allow propositional symbols as atomic statements. An example of an epistemic property common to all protocols with the network topology depicted in Figure 3 expressible in our language is:

$$\Box_m\Box_{m''}\varphi \rightarrow \Box_{m'}\Box_{m''}\varphi. \tag{6}$$

Informally, this property states that if any observer eavesdropping on channel m is able to deduce that any other observer eavesdropping on channel m'' can conclude that some property φ is true, then the same deduction can be made by any observer eavesdropping on channel m' on the same run. This property, as shown in Example 3, is a special case of our Gateway axiom. We prove the soundness of Gateway axiom with respect to a formally defined semantics in Section 6.

Another, perhaps surprising, example of a property common to all protocols with the network topology depicted in Figure 3 is:

$$\Box_{m'}(\Box_m\varphi \vee \Box_{m''}\psi) \rightarrow \Box_{m'}\Box_m\varphi \vee \Box_{m'}\Box_{m''}\psi. \tag{7}$$

Generally speaking, the knowledge of a disjunction of two formulas does not imply the knowledge of either of the two disjuncts. The above formula, however, states that this is true when the disjunct talks about the knowledge of observers located on different sides of channel m'. In Section 5, we prove a more general form of property (7).

An epistemic logic for reasoning about communication graphs was proposed by Pacuit and Parikh [3]. Their language consists of two different modalities: an epistemic modality K_a labeled by an agent a and a modality $\Box$ interpreted as "after any sequence of communications under the given protocol it is true that". They discussed logical principles specific to a given network topology

[2]As we formally define in the next section, the topological structure of a communication network is an undirected graph with multiple edges.

and even gave, in the introduction, a principle similar to our Gateway axiom. However, they did not provide a complete axiomatization of their logical system for a specific topology, even though they proved its decidability.

Kane and Naumov [1] proposed a similar logical system whose language contains only epistemic modality. They eliminated modality "after any sequence of communications" by assuming that all statements refer to the final knowledge after the communication. In this simplified setting they have been able to prove completeness theorem, but only for the case of linear communication networks.

This article extends Kane and Naumov's work from linear communication chains to arbitrary connected graphs. The logical system introduced in [1] contained two principles capturing topology of linear communication chains: Gateway axiom and Disjunction axiom, similar to properties (6) and (7) above. The more general version of Gateway axiom described in the current article no longer requires Disjunction property as a separate axiom. Instead, we prove this property from the more general version of Gateway axiom in Lemma 2. More importantly, the proof of the completeness theorem for non-linear graphs is completely different from the proof of completeness for linear communication chains. In the case of the proof of completeness for linear communication chains, if an observer of channel m knows certain information about channel m', then it is enough to simply pass this information along the interval between channels m and m'. However, the same technique does not apply to non-linear graphs. As we have demonstrated with protocol $\mathcal{P}_1$ and properties (1) and (2), in non-linear graphs an observer of channel m might know certain information about channel m' without anyone between them knowing this information. To be able to prove completeness for non-linear graphs we introduce a new *network flow* construction described in Section 7.

An applied value of the result in this article is in providing a uniform protocol design procedure for communication networks. Namely, suppose that one needs to design a protocol for a network that satisfies security conditions $\varphi_1,\dots,\varphi_n$ expressed in our modal language. Assume additionally that the physical layout (topological structure) of the network is given and can not be changed. In such a setting, the protocol designer should be able to either (i) derive formula $\bigwedge_{i\leq n}\varphi_i\to\bot$ in our logical system and, thus, prove that the specification of the protocol can not be met, or (ii) use the construction from our proof of completeness to produce a protocol that satisfies each of the desired conditions $\varphi_1,\dots,\varphi_n$.

Tao, Slutzki, and Honavar [4] introduced a conceptual logical framework for answering queries without revealing secrecy to multiple querying agents where there is a set of secrets that need to be protected against each of these agents. The communication between agents is modeled using a graph. The focus of their work is on a privacy-preserving algorithm, not on an axiomatic system.

This article is also related to the works on information flow on graphs [5, 6, 7, 8, 9, 10], that study properties of nondeducibility, functional dependency, common knowledge, and fault tolerance predicates. Unlike those works, this article is using a modal language.

The article is organized as follows. Section 2 introduces relevant terminology

from graph theory. Section 3 defines the formal syntax and the semantics for our logical system, which is introduced in Section 4. Section 5 illustrates our logical system by giving several examples of formal proofs in this system. Some of these examples are used later in the proof of completeness. The soundness of the system is established in Section 6. The rest of the article is dedicated to the proof of completeness in Section 7. The proof starts with an informal discussion of a network flow protocol. It continues to formalize the network flow protocol as a canonical communication protocol over the graph. Finally, multiple instances of the canonical protocol are aggregated together to show the completeness of the logical system. Section 8 concludes the article.

2 Graph Theory Preliminaries

We study epistemic properties common to all protocols with the same topology of a channel network. Under such a protocol, multiple messages can be sent over the same channel. A *value of a channel* is the set of all messages communicated through the channel, possibly in both directions. We specify the network topology as an undirected graph in which vertices represent agents and edges represent communication channels between agents. In this section we introduce graph terminology used throughout the rest of the article.

Graph (V, E) contains a set of vertices V and a set of edges E with an incidence relation between them. We allow loops and multiple edges between the same pair of vertices. We write $e \in Edge(v_0, v_1)$ to state that edge $e \in E$ is one of (possibly multiple) edges between vertices $v_0 \in V$ and $v_1 \in V$. By $Inc(v)$ we denote the set of all edges incident to vertex $v \in V$. By $Inc(e)$ we denote the set consisting of the two ends of edge $e \in E$. For example, $Inc(q) = \{m, k, c\}$ and $Inc(k) = \{q, u\}$ in Figure 3.

Let $e \in E$ be an edge of a graph (V, E) incident to a vertex $v \in V$. If edge e is removed from the graph, remaining graph $(V, E \setminus \{e\})$ might have up to two connected components. By C^v_{-e} we denote the *connected component* of the graph $(V, E \setminus \{e\})$ that contains vertex v. Note that in some cases component C^v_{-e} might be equal to the entire graph $(V, E \setminus \{e\})$. For the graph in Figure 3, component $C^u_{-m'}$ consists of vertices p, q, and u as well as edges m, k, and c. For the same graph, component C^u_{-k} contains all vertices of the original graph and all edges of that graph except for edge k.

A *path* is a sequence $e_0, v_1, e_1, \ldots, v_k, e_k$ such that $k \geq 0$, $e_0, \ldots, e_k$ are distinct edges, and $v_1, \ldots, v_k$ are distinct vertices of the graph such that $e_i, e_{i+1} \in Inc(v_{i+1})$ for each $0 \leq i < k$. In Figure 3, sequence k, u, m', v, c' and one-element sequence c are both examples of paths. A *circular path* is defined similarly except for edges e_0 and e_k being the same.

Definition 1 *Edge g is a gateway between sets of edges A and B of a graph if each path that starts with an edge in set A and ends with an edge in set B contains the edge g.*

For example, edge m' is a gateway between sets of edges $\{m, k\}$ and $\{k', c'\}$ in Figure 3. Note that in the above definition edge g can belong to either or both of the sets A and B. In Figure 3, edge k is a gateway between singleton set $\{k\}$ and set $\{m, m''\}$.

3 Syntax and Semantics

In this section we define the language and the formal semantics of our logical system. These definitions presuppose a fixed *signature* of the communication network.

Definition 2 *A signature Sig is an arbitrary triple* $Sig = (V, E, \{P_e\}_{e \in E})$, *such that* (V, E) *is a connected graph and* $\{P_e\}_{e \in E}$ *is a family of disjoint sets of propositions.*

Informally, propositions in set P_e are atomic statements about values of the communication channel e.

Different connected components of a disconnected graph can not exchange any information between them, so, for the sake of simplicity, we have chosen to restrict our system to connected graphs.

We next define the language of our logical system.

Definition 3 *For every signature Sig, let* $\Phi(Sig)$ *be the minimal set of formulas such that*

1. $\bot \in \Phi(Sig)$,
2. $P_e \subseteq \Phi(Sig)$ *for every* $e \in E$,
3. *if* $\varphi, \psi \in \Phi(Sig)$, *then* $\varphi \to \psi \in \Phi(Sig)$,
4. *if* $e \in E$ *and* $\varphi \in \Phi(Sig)$, *then* $\Box_e \varphi \in \Phi(Sig)$.

We assume that connectives $\neg$, $\wedge$, and $\vee$ are defined through $\to$ and $\bot$ in the usual way.

Informally, a protocol is specified by giving a range of values[3] for each edge ("communication channel") and establishing dependencies between the values of the edges. These dependencies are "enforced" by vertices ("agents"), and, thus, each such condition only involves edges incident to a vertex. For this reason we refer to these conditions as "local". For example, for protocol $\mathcal{P}_1$ in the introduction, the local condition enforced by vertex q is $c = m \oplus k$, where $m \oplus k$ is a *bit-wise exclusive or* of binary strings transmitted over channels m and k. For protocols $\mathcal{P}_2$ and $\mathcal{P}_3$, the local condition at vertex q is $h(c, m \oplus k) \leq 1$, where $h(\cdot, \cdot)$ denotes the Hamming distance between any two binary strings of the same length. The local condition for vertex p under all three of the above

[3]Each value represents the collection of all messages sent through the channel on a given run.

protocols is the constant *true*. In the formal definition below, a local condition is treated not as a Boolean function but rather as a set of tuples on which this function is true.

Recall that each atomic proposition p in set P_e is viewed as proposition "about" the value of channel e. In what follows, by $\pi(p)$ we informally mean the set of all values of channel e for which proposition p is true.

Definition 4 *A protocol over a signature* $(V, E, \{P_e\}_{e\in E})$ *is a tuple* $(\{W_e\}_{e\in E}, \{L_v\}_{v\in V}, \pi)$ *such that*

1. *for every edge* $e \in E$, *set* W_e *is an arbitrary set of values,*
2. *for every* $v \in V$, *set* $L_v \subseteq \prod_{e\in Inc(v)} W_e$ *specifies local conditions at vertex* v,
3. *for every* $p \in P_e$, *function* π *is such that* $\pi(p) \subseteq W_e$. *We denote* $\pi(p)$ *by* p^π.

Definition 5 *A run of a protocol* $(\{W_e\}_{e\in E}, \{L_v\}_{v\in V}, \pi)$ *is an arbitrary tuple* $\langle w_e\rangle_{e\in E} \in \prod_{e\in E} W_e$ *such that* $\langle w_e\rangle_{e\in Inc(v)} \in L_v$ *for every* $v \in V$.

Definition 6 *For any two tuples* $r = \langle w_e\rangle_{e\in E}$ *and* $r' = \langle w'_e\rangle_{e\in E}$ *and any* $f \in E$, *we write* $r =_f r'$ *if* $w_f = w'_f$.

Corollary 1 *Relation* $r =_e r'$ *is an equivalence relation.* ⊠

The formal semantics of our logical system is defined in terms of runs of a protocol, rather than in more common terms of epistemic worlds of a Kripke model. Note, however, that any protocol can be viewed as a Kripke model in which runs of the protocol are epistemic worlds and equality of runs on a given channel c is the indistinguishability relation $\sim_c$ on epistemic worlds.

Definition 7 *For every signature* $Sig = (V, E, \{P_e\}_{e\in E})$, *every* $\varphi \in \Phi(Sig)$, *every protocol* $\mathcal{P} = (\{W_e\}_{e\in E}, \{L_v\}_{v\in V}, \pi)$ *over graph* (V, E), *and every run* $r = \langle w_e\rangle_{e\in E}$ *of* $\mathcal{P}$, *relation* $r \Vdash \varphi$ *is defined recursively as:*

1. $r \nVdash \bot$,
2. $r \Vdash p$ *if* $w_e \in p^\pi$, *where* $p \in P_e$,
3. $r \Vdash \psi \to \chi$ *if* $r \nVdash \psi$ *or* $r \Vdash \chi$,
4. $r \Vdash \Box_e\psi$ *if* $r' \Vdash \psi$ *for every run* r' *of* $\mathcal{P}$ *such that* $r' =_e r$.

For any signature Sig and any set of edges T, by $\Phi(Sig, T)$ we mean the set of all formulas in $\Phi(Sig)$ in which all outermost modalities are labeled only by edges in T and all atomic propositions outside of scopes of all modalities belong to $\bigcup_{t\in T} P_t$. For example, $\Box_a\Box_b\varphi \to \Box_c\psi \in \Phi(Sig, \{a, c\})$. Also, if $p \in P_a$ and $q \in P_b$, then $\Box_b p \to q \in \Phi(Sig, \{b\})$. We use this notation to state our Gateway axiom in the next section. Below is the formal definition of this notation.

Definition 8 *For every signature* $Sig = (V, E, \{P_e\}_{e \in E})$ *and every* $T \subseteq E$*, let* $\Phi(Sig, T)$ *be the minimal set of formulas such that*

1. $\bot \in \Phi(Sig, T)$*,*
2. $P_t \subseteq \Phi(Sig, T)$ *for every* $t \in T$*,*
3. *if* $\varphi, \psi \in \Phi(Sig, T)$*, then* $\varphi \to \psi \in \Phi(Sig, T)$*,*
4. *if* $t \in T$ *and* $\varphi \in \Phi(Sig)$*, then* $\Box_t \varphi \in \Phi(Sig, T)$*.*

Note that in item 4 above, formula φ is an element of set $\Phi(Sig)$ rather than set $\Phi(Sig, T)$.

4 Logical System

In this section we specify the axioms and the inference rules of our logical system for a given signature $Sig = (V, E, \{P_e\}_{e \in E})$. Our logical system, in addition to propositional tautologies in language $\Phi(Sig)$, contains the following axioms:

1. Truth: $\Box_e \varphi \to \varphi$, where $\varphi \in \Phi(Sig)$,
2. Positive Introspection: $\Box_e \varphi \to \Box_e \Box_e \varphi$, where $\varphi \in \Phi(Sig)$,
3. Negative Introspection: $\neg \Box_e \varphi \to \Box_e \neg \Box_e \varphi$, where $\varphi \in \Phi(Sig)$,
4. Distributivity: $\Box_e(\varphi \to \psi) \to (\Box_e \varphi \to \Box_e \psi)$, where $\varphi, \psi \in \Phi(Sig)$,
5. Gateway: $\Box_e(\varphi \to \psi) \to (\varphi \to \Box_g \psi)$, where $e \in A$, $\varphi \in \Phi(Sig, A)$, $\psi \in \Phi(Sig, B)$, and edge g is a gateway between sets of edges $A \subseteq E$ and $B \subseteq E$.

Note that axioms of Truth, Positive Introspection, Negative Introspection, and Distributivity are identical to the corresponding axioms of multi-agent epistemic logic S5. Thus, our logical system can be viewed as an extension of S5 by Gateway axiom.

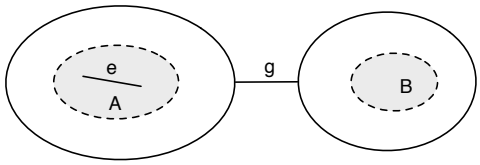

Figure 4: Edge g is a gateway between sets of edges A and B.

Figure 4 illustrates the setting for Gateway axiom. To explain the intuition behind Gateway axiom, let us first consider the special case of this axiom when

formula φ is a propositional tautology. In this case, Gateway axiom can be reduced to $\Box_e\psi \to \Box_g\psi$, which means that if an agent eavesdropping on channel e knows something about the channels in set B, then an agent eavesdropping on gateway channel g must also know this. Intuitively, this claim is true because the information about channels in set B can only reach the observer of channel e by flowing through the gateway channel g. However, to the best of our knowledge, Gateway axiom in this reduced form $\Box_e\psi \to \Box_g\psi$ does not yield a complete logical system. To achieve the completeness, we need a slightly more general principle that takes into account the "local" information about channels on the same side of the gateway as channel e. In Gateway axiom $\Box_e(\varphi \to \psi) \to (\varphi \to \Box_g\psi)$ the local information is captured by formula φ.

We write $\vdash_{Sig} \varphi$ if formula φ is provable in our logical system for signature Sig using Modus Ponens and Necessitation inference rules:

$$\frac{\varphi, \qquad \varphi \to \psi}{\psi} \qquad\qquad \frac{\varphi}{\Box_e\varphi}$$

where $\varphi, \psi \in \Phi(Sig)$ and $e \in E$. We write $X \vdash_{Sig} \varphi$ if formula φ is provable in our logical system from the set of assumptions X using only Modus Ponens rule. We omit subscript Sig when its value is clear from the context.

5 Examples

The soundness and the completeness of our logical system will be established in the next two sections. In this section we give several examples of formal proofs in this system. Among these examples there are several lemmas that will be used later in the proof of completeness.

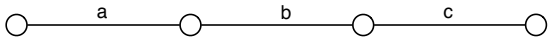

Figure 5: Three-Channel Linear Communication Network.

Example 1 *For any signature* $Sig = (V, E, \{P_e\}_{e\in E})$ *and any* $\varphi \in \Phi(Sig)$ *where* (V, E) *is the graph depicted in Figure 5,*

$$\vdash_{Sig} \Box_a(\Box_b\varphi \vee \Box_c\varphi) \to \Box_b\varphi.$$

In other words, if an observer eavesdropping on channel a knows that an observer eavesdropping on channel b knows φ *or an observer eavesdropping on channel c knows* φ*, then the observer eavesdropping on channel b must know* φ*.*

Proof. Formula $\Box_c\varphi \to \varphi$ is an instance of Truth axiom. Thus, by Necessitation inference rule, $\vdash \Box_b(\Box_c\varphi \to \varphi)$. Hence, by Distributivity axiom and Modus Ponens inference rule,

$$\vdash \Box_b\Box_c\varphi \to \Box_b\varphi. \tag{8}$$

At the same time note that edge b is a gateway between sets $\{a, b\}$ and $\{c\}$. Additionally, $\neg\Box_b\varphi \in \Phi(Sig, \{a, b\})$ and $\Box_c\varphi \in \Phi(Sig, \{c\})$. Thus, by Gateway axiom, $\vdash \Box_a(\neg\Box_b\varphi \to \Box_c\varphi) \to (\neg\Box_b\varphi \to \Box_b\Box_c\varphi)$. Hence, using statement (8) and the laws of propositional logic, $\vdash \Box_a(\neg\Box_b\varphi \to \Box_c\varphi) \to (\neg\Box_b\varphi \to \Box_b\varphi)$. Note that formula $(\neg\Box_b\varphi \to \Box_b\varphi) \to \Box_b\varphi$ is a propositional tautology. Thus, $\vdash \Box_a(\neg\Box_b\varphi \to \Box_c\varphi) \to \Box_b\varphi$. Finally, recall that disjunction $\Box_b\varphi \vee \Box_b\varphi$ is an abbreviation for $\neg\Box_b\varphi \to \Box_b\varphi$. Therefore, $\vdash \Box_a(\Box_b\varphi \vee \Box_c\varphi) \to \Box_b\varphi$. ⊠

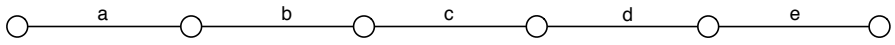

Figure 6: Five-Channel Linear Communication Network.

In what follows, we denote by $\top$ the propositional tautology $\bot \to \bot$.

Example 2 *For any signature* $Sig = (V, E, \{P_e\}_{e\in E})$ *and any* $\varphi \in \Phi(Sig)$ *where* (V, E) *is the graph depicted in Figure 6,*

$$\vdash_{Sig} \Box_a\Box_e\Box_c\varphi \to \Box_b\Box_d\varphi.$$

Proof. By Truth axiom, $\vdash \Box_c\varphi \to \varphi$. Thus, $\vdash \Box_d(\Box_c\varphi \to \varphi)$ by Necessitation inference rule. Hence, by Distributivity axiom and Modus Ponens rule,

$$\vdash \Box_d\Box_c\varphi \to \Box_d\varphi. \tag{9}$$

At the same time, formula $\Box_c\varphi \to (\top \to \Box_c\varphi)$ is a propositional tautology. Thus, by Necessitation rule, $\vdash \Box_e(\Box_c\varphi \to (\top \to \Box_c\varphi))$. By Distributivity axiom and Modus Ponens inference rule,

$$\vdash \Box_e\Box_c\varphi \to \Box_e(\top \to \Box_c\varphi). \tag{10}$$

Similarly, one can show that

$$\vdash \Box_a\Box_d\varphi \to \Box_a(\top \to \Box_d\varphi). \tag{11}$$

Since edge d is a gateway between the sets of edges $\{e\}$ and $\{c\}$, $\top \in \Phi(Sig, \{e\})$, and $\Box_c\varphi \in \Phi(Sig, \{c\})$, by Gateway axiom, $\vdash \Box_e(\top \to \Box_c\varphi) \to (\top \to \Box_d\Box_c\varphi)$. Hence, using statement (9), statement (10) and the propositional reasoning, $\vdash \Box_e\Box_c\varphi \to \Box_d\varphi$. Thus, by Necessitation inference rule, $\vdash \Box_a(\Box_e\Box_c\varphi \to \Box_d\varphi)$. Then, by Distributivity axiom and Modus Ponens inference rule,

$$\vdash \Box_a\Box_e\Box_c\varphi \to \Box_a\Box_d\varphi. \tag{12}$$

Since edge b is a gateway between sets of edges $\{a\}$ and $\{d\}$, $\top \in \Phi(Sig, \{a\})$, and $\Box_d\varphi \in \Phi(Sig, \{d\})$, by Gateway axiom, $\vdash \Box_a(\top \to \Box_d\varphi) \to (\top \to \Box_b\Box_d\varphi)$. Therefore, using statement (11), statement (12), and the propositional reasoning, $\vdash \Box_a\Box_e\Box_c\varphi \to \Box_b\Box_d\varphi$. ⊠

We next prove formula (6) stated in Section 1.

Example 3 *For any signature* $Sig = (V, E, \{P_e\}_{e \in E})$ *and any* $\varphi \in \Phi(Sig)$*, where* $G = (V, E)$ *is the graph depicted in Figure 3,*

$$\vdash_{Sig} \Box_m \Box_{m''} \varphi \to \Box_{m'} \Box_{m''} \varphi.$$

Proof. Formula $\Box_{m''}\varphi \to (\top \to \Box_{m''}\varphi)$ is a propositional tautology in language $\Phi(Sig)$. Thus, by Necessitation inference rule, we have $\vdash \Box_m(\Box_{m''}\varphi \to (\top \to \Box_{m''}\varphi))$. By Distributivity axiom and Modus Ponens inference rule,

$$\vdash \Box_m(\Box_{m''}\varphi) \to \Box_m(\top \to \Box_{m''}\varphi)). \tag{13}$$

Note now that edge m' is a gateway between sets of edges $\{m\}$ and $\{m''\}$. Also, $\top \in \Phi(Sig, \{m\})$ and $\Box_{m''}\varphi \in \Phi(Sig, \{m''\})$. Thus, by Gateway axiom, $\vdash_G \Box_m(\top \to \Box_{m''}\varphi) \to (\top \to \Box_{m'}\Box_{m''}\varphi)$. Hence, using statement (13), by the laws of propositional logic, $\vdash_G \Box_m\Box_{m''}\varphi \to (\top \to \Box_{m'}\Box_{m''}\varphi)$. Therefore, again using propositional logic, $\vdash_G \Box_m\Box_{m''}\varphi \to \Box_{m'}\Box_{m''}\varphi$. ⊠

Instead of proving property (7) from the introduction, in Lemma 2 we prove a slightly more general statement that later will be used in the proof of completeness. The proof of Lemma 2 relies on the following auxiliary lemma. Figure 4 illustrates the settings of both of these lemmas.

Lemma 1 $\vdash \Box_e(\varphi \vee \psi) \to (\varphi \vee \Box_g\psi)$*, where edge* g *is a gateway between sets of edges* A *and* B*,* $e \in A$*,* $\varphi \in \Phi(Sig, A)$*, and* $\psi \in \Phi(Sig, B)$*.*

Proof. Recall that $\varphi \vee \psi$ is an abbreviation for $\neg\varphi \to \psi$. Thus, we need to show that $\vdash \Box_e(\neg\varphi \to \psi) \to (\neg\varphi \to \Box_g\psi)$, which is an instance of Gateway axiom. ⊠

Lemma 2 $\vdash \Box_g(\varphi \vee \psi \vee \chi) \to (\varphi \vee \Box_g\psi \vee \Box_g\chi)$*, where edge* g *is a gateway between sets* A *and* B*,* $\varphi \in \Phi(Sig, \{g\})$*,* $\psi \in \Phi(Sig, A)$*, and* $\chi \in \Phi(Sig, B)$*.*

Proof. Note first that g is a gateway between sets $A \cup \{g\}$ and B. Thus, by Lemma 1,

$$\vdash \Box_g(\varphi \vee \psi \vee \chi) \to \varphi \vee \psi \vee \Box_g\chi.$$

Hence, by the laws of propositional logic,

$$\vdash \Box_g(\varphi \vee \psi \vee \chi) \to \varphi \vee \Box_g\chi \vee \psi.$$

By Necessitation inference rule,

$$\vdash \Box_g(\Box_g(\varphi \vee \psi \vee \chi) \to \varphi \vee \Box_g\chi \vee \psi).$$

By Distributivity axiom and Modus Ponens rule,

$$\vdash \Box_g\Box_g(\varphi \vee \psi \vee \chi) \to \Box_g(\varphi \vee \Box_g\chi \vee \psi).$$

By Positive Introspection axiom,

$$\vdash \Box_g(\varphi \vee \psi \vee \chi) \to \Box_g(\varphi \vee \Box_g\chi \vee \psi). \tag{14}$$

Second, note that edge g is also a gateway between sets $\{g\}$ and A. Thus, again by Lemma 1,

$$\vdash \Box_g(\varphi \vee \Box_g\chi \vee \psi) \to \varphi \vee \Box_g\chi \vee \Box_g\psi.$$

Hence, taking into account statement (14),

$$\vdash \Box_g(\varphi \vee \psi \vee \chi) \to \varphi \vee \Box_g\chi \vee \Box_g\psi,$$

which by the laws of propositional logic is equivalent to

$$\vdash \Box_g(\varphi \vee \psi \vee \chi) \to \varphi \vee \Box_g\psi \vee \Box_g\chi.$$

⊠

Next, we continue with two more auxiliary lemmas. Lemma 4 is also used in the proof of completeness. Lemma 3 is referred to in the proof of Lemma 4.

Lemma 3 $\vdash \varphi \to \Box_e\varphi$ *for each* $\varphi \in \Phi(Sig, \{e\})$.

Proof. Formula $\varphi \to \varphi$ is a tautology. Thus, by Necessitation inference rule, $\vdash \Box_e(\varphi \to \varphi)$. Note that e is a gateway between sets $\{e\}$ and $\{e\}$. By Gateway axiom, $\vdash \Box_e(\varphi \to \varphi) \to (\varphi \to \Box_e\varphi)$. Therefore, $\vdash \varphi \to \Box_e\varphi$. ⊠

Lemma 4 *If* $X \subseteq \Phi(Sig, \{e\})$ *and* $\varphi \in \Phi(Sig)$, *then* $X \vdash \varphi$ *implies* $X \vdash \Box_e\varphi$.

Proof. Suppose that $X \subseteq \Phi(Sig, \{e\})$ and $X \vdash \varphi$ where $\varphi \in \Phi(Sig)$, then there is a finite subset $\{\psi_1, \psi_2, \ldots, \psi_n\}$ of X such that $\psi_1, \psi_2, \ldots, \psi_n \vdash \varphi$. Hence, by Deduction theorem for propositional logic, we have $\vdash \psi_1 \to (\psi_2 \to \ldots(\psi_n \to \varphi)\ldots)$. By Necessitation rule, $\vdash \Box_e(\psi_1 \to (\psi_2 \to \ldots(\psi_n \to \varphi)\ldots))$. Applying Distributivity axiom and Modus Ponens n times, we have $\Box_e\psi_1, \Box_e\psi_2, \ldots, \Box_e\psi_n \vdash \Box_e\varphi$. Hence, by Lemma 3, $\psi_1, \psi_2, \ldots, \psi_n \vdash \Box_e\varphi$. Therefore, $X \vdash \Box_e\varphi$. ⊠

6 Soundness

In this section we prove the soundness of our logical system with respect to runs of a protocol $\mathcal{P}$ over a signature $Sig = (V, E, \{P_e\}_{e\in E})$. The soundness of propositional tautologies and Modus Ponens inference rule is straightforward. Below we prove the soundness of Necessitation inference rule and of each axiom as a separate lemma.

Lemma 5 (Necessitation) *If* $e \in E$ *and* $r \Vdash \varphi$ *for each run* r *of protocol* $\mathcal{P}$, *then* $r \Vdash \Box_e\varphi$ *for each run* r *of protocol* $\mathcal{P}$.

Proof. Let r be a run of protocol $\mathcal{P}$. To show that $r \Vdash \Box_e\varphi$, consider any run r' of protocol $\mathcal{P}$ such that $r' =_e r$. It is sufficient to prove that $r' \Vdash \varphi$, which is true due to the assumption of the lemma. ⊠

Lemma 6 (Truth) *For every $e \in E$, every formula $\varphi \in \Phi(Sig)$, and every run r of protocol $\mathcal{P}$, if $r \Vdash \Box_e \varphi$, then $r \Vdash \varphi$.*

Proof. Assume that $r \Vdash \Box_e \varphi$. Thus, by Definition 7, $r' \Vdash \varphi$ for every run r' of protocol $\mathcal{P}$ such that $r' =_e r$. In particular, $r \Vdash \varphi$. ⊠

Lemma 7 (Positive Introspection) *For every $e \in E$, every formula $\varphi \in \Phi(Sig)$, and every run r of protocol $\mathcal{P}$, if $r \Vdash \Box_e \varphi$, then $r \Vdash \Box_e \Box_e \varphi$.*

Proof. Assume that $r \Vdash \Box_e \varphi$. Let r' be any run of protocol $\mathcal{P}$ such that $r' =_e r$. We need to show that $r' \Vdash \Box_e \varphi$. Consider any run r'' of protocol $\mathcal{P}$ such that $r'' =_e r'$. We need to show that $r'' \Vdash \varphi$. Indeed, $r'' =_e r' =_e r$ due to the choice of r' and r''. Hence, $r'' \Vdash \varphi$ by the assumption $r \Vdash \Box_e \varphi$. ⊠

Lemma 8 (Negative Introspection) *For every $e \in E$, every formula $\varphi \in \Phi(Sig)$, and every run r of protocol $\mathcal{P}$, if $r \Vdash \neg \Box_e \varphi$, then $r \Vdash \Box_e \neg \Box_e \varphi$.*

Proof. Assume that $r \Vdash \neg \Box_e \varphi$. Then there is a run r' of protocol $\mathcal{P}$ such that $r' =_e r$ and $r' \nVdash \varphi$. Consider now any run r'' of protocol $\mathcal{P}$ such that $r'' =_e r$. It is sufficient to show that $r'' \Vdash \neg \Box_e \varphi$, which is true because $r' =_e r =_e r''$ and $r' \nVdash \varphi$. ⊠

The proof of the soundness of Gateway axiom relies on the following technical lemma.

Lemma 9 *For every set $F \subseteq E$, every formula $\varphi \in \Phi(Sig, F)$, and every two runs r and r' of protocol $\mathcal{P}$, if $r =_e r'$ for all $e \in F$, then $r \Vdash \varphi$ if and only if $r' \Vdash \varphi$.*

Proof. We prove this by induction on the structural complexity of formula φ. The base case is when φ is a propositional variable $p \in P_e$ for some $e \in E$. By Definition 7, $r \Vdash p$ is equivalent to $w_e \in p^\pi$, which, due to $w_e = w'_e$, in turn is equivalent to $w'_e \in p^\pi$. The latter is equivalent to $r' \Vdash p$, again by Definition 7.

The induction step involves the following cases:

1. Suppose that φ is of the form $\neg\psi$. By Definition 7, $r \Vdash \varphi$ is equivalent to $r \nVdash \psi$. By the induction hypothesis, $r \nVdash \psi$ is equivalent to $r' \nVdash \psi$, which, by Definition 7, is equivalent to $r' \Vdash \neg\psi$.

2. Suppose that φ is of the form $\psi \to \chi$. By Definition 7, $r \Vdash \psi \to \chi$ is equivalent to the disjunction of $r \nVdash \psi$ and $r \Vdash \chi$, which is equivalent to the disjunction of $r' \nVdash \psi$ and $r' \Vdash \chi$ by the induction hypothesis. The latter is equivalent to $r' \Vdash \psi \to \chi$ by Definition 7.

3. Suppose that φ is of the form $\Box_e \psi$. By Definition 7, $r \Vdash \Box_e \psi$ if and only if $r'' \Vdash \psi$ for every r'' such that $r'' =_e r'$. Since $r' =_e r$, the latter statement is equivalent to $r'' \Vdash \psi$ for every r'' such that $r'' =_e r'$. By Definition 7, the latter is equivalent to $r' \Vdash \Box_e \psi$.

⊠

Lemma 10 (Gateway) *For every run $r = \langle w_e \rangle_{e \in E}$ of protocol $\mathcal{P}$, every gateway g between sets of edges A and B, every $a \in A$, and every $\varphi \in \Phi(Sig, A)$, $\psi \in \Phi(Sig, B)$, if $r \Vdash \Box_a(\varphi \to \psi)$ and $r \Vdash \varphi$, then $r \Vdash \Box_g \psi$.*

Proof. Consider any run $r' = \langle w'_e \rangle_{e \in E}$ of protocol $\mathcal{P}$ such that $r' =_g r$. It suffices to show that $r' \Vdash \psi$. Consider a graph $G' = (V, E \setminus \{g\})$. Due to the assumption that g is a gateway A and B, graph G' consists of two connected components C_A and C_B such that all edges in set A belong to the component C_A and all edges in set B belong to the component C_B. Let r^+ be a tuple $\langle w^+_e \rangle_{e \in E}$ such that

$$w^+_e = \begin{cases} w_e & \text{if } e \in C_A \cup \{g\}, \\ w'_e & \text{if } e \in C_B \cup \{g\}. \end{cases}$$

Note that tuple r^+ is well defined due to the assumption that $r' =_g r$.

Claim 1 *Tuple r^+ is a run of protocol $\mathcal{P}$.*

Proof. We need to show that r^+ satisfies local conditions of protocol $\mathcal{P}$ at any vertex $v \in V$. If $v \in C_A$, then $w^+_e = w_e$ for each $e \in Inc(v)$ by the choice of $\langle w^+_e \rangle_{e \in E}$. Hence, $\langle w^+_e \rangle_{e \in Inc(v)} = \langle w_e \rangle_{e \in Inc(v)} \in L_v$. The case $v \in C_B$ is similar. ⊠

We are ready to finish the proof of the lemma. Note that $r^+ =_a r$ by the choice of $\langle w^+_e \rangle_{e \in E}$ and the assumption $a \in A$. Thus, $r^+ \Vdash \varphi \to \psi$ by the assumption $r \Vdash \Box_a(\varphi \to \psi)$. At the same time, $r^+ \Vdash \varphi$ by Lemma 9 and the assumption $r \Vdash \varphi$. Hence, $r^+ \Vdash \psi$ by Definition 7. Therefore, $r' \Vdash \psi$ by the same Lemma 9 and the assumption $\psi \in \Phi(Sig, B)$. ⊠

7 Completeness

In this section we prove the completeness of our logical system with respect to the formal semantics defined in Section 3.

In general, to prove a completeness theorem for a logical system, for any statement not provable in this system, one needs to describe how to construct a model in which this statement is false. In our case, for each formula φ not provable in our logical system, we construct a protocol ("Kripke model") and a run ("epistemic world") of this protocol on which formula φ is not satisfied. This protocol will be obtained by *aggregating* simpler *canonical* protocols. Each canonical protocol synchronizes information known to different observers. For example, if an observer a knows that an observer b knows ψ, then one of the canonical protocols guarantees that observer b indeed knows ψ.

The construction of such canonical protocols is based on the network flow protocol [11, p.708]. Information flow has many properties similar to that of

network flow. In fact, network flow is sometimes used to communicate information. For example, the hydraulic brake system in modern cars uses the flow of the brake fluid to communicate a braking signal from the brake pedal to the wheels. In a more general setting, one can consider a closed system of water pipes with several faucets and several sinks. If one of the faucets is pumping water into the system (somebody knows formula δ), then at least one of the sinks must be leaking the water (forcing formula δ to be true). We will use such pipe systems to communicate information between different edges of the graph.

In this section we first informally discuss network flow protocols in more details. Next, we define "canonical" protocols that formalize network flow protocol in the form needed for our proof of completeness. Finally, to finish the proof of completeness, we aggregate multiple canonical protocols into a single one.

7.1 Network Flow Protocol

Consider an example of a network of six pipes depicted in Figure 7. Assume that this network has two sink faucets located at edges d and f. Furthermore, let us assume that

1. water can leak from the network only through faucets on edges d and f,
2. water does not have to leak even if the faucet is open, and
3. all pipes can (but do not have to) add water into the system by pumping it in the middle of the pipes.

Throughout this section, atomic propositions p and q denote the statements "faucet on the edge d is open" and "faucet on the edge f is open", respectively.

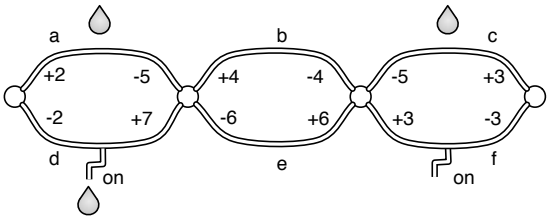

Figure 7: Run r_1 of a network flow protocol.

We show the flow in the network by assigning a real number f_u^e to each end u of each pipe e in the network. The *positive* number denotes the speed (volume per time unit) with which water is *coming into* the pipe through this end and *negative* number shows the speed with which water is *leaving* the pipe through that end.

So far, we assume that no water can be added at a vertex. Thus, the sum of all values at each vertex is zero. Any such valid assignment of the flow values to the ends of all pipes defines a run of the network flow protocol.

An example of a run r_1 is also shown on Figure 7. On this run pipes a and c add water into the system, both sink faucets are open, but only edge d leaks water. Note that an external observer of pipe a would see that the sum of flow values on edge a is negative. This means that water is added into the system. Thus, the observer would be able to conclude that at least one of the sink faucets is open: $r_1 \Vdash \Box_a(p \vee q)$. However, this observer will not be able to deduce exactly which faucet is open: $r_1 \Vdash \neg\Box_a p \wedge \neg\Box_a q$. Also, an external observer of pipe d will see that the sum of the two flow values at the ends of this pipe is positive and, thus, faucet on the pipe d is leaking. Hence, $r_1 \Vdash \Box_d p$ and so $r_1 \Vdash \Box_d(p \vee q)$.

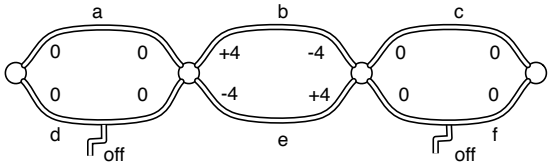

Figure 8: Run r_2 of a network flow protocol.

We now argue that $r_1 \Vdash \neg\Box_b(p \vee q)$. Indeed, any external observer of pipe b will not be able to distinguish run r_1 from run r_2 depicted in Figure 8 because they have the same flow values at both ends of pipe b. Run r_2 has a circular flow through pipes b and e, with both faucets being closed. Since $r_2 \nVdash p \vee q$ and the observer of pipe b can not distinguish between runs r_1 and r_2, it follows that $r_1 \Vdash \neg\Box_b(p \vee q)$. Similarly, another run could be constructed to show that $r_1 \Vdash \neg\Box_e(p \vee q)$.

Before continuing with the next example, let us introduce a notion of a *bridge* edge of a graph, which is related but not identical to the earlier introduced notion of a gateway edge between two sets of edges.

Definition 9 *An edge b is a bridge in a connected graph (V, E), if graph $(V, E \setminus \{b\})$ is not connected.*

For any given graph, by $\mathcal{B}$ we mean the set of all bridges of this graph. For example, for the graph depicted in Figure 3, set $\mathcal{B}$ is $\{m, m', m''\}$.

The main difference between a gateway and a bridge is that a gateway between sets is defined assuming two given sets. Bridge is a specific type of an edge. It's definition does not depend on the choice of any specific sets. Furthermore, a gateway does not have to be a bridge. For example, for any edges e and f, of an arbitrary graph, edge e is a gateway between set $\{e\}$ and set $\{f\}$ even if edge e is not a bridge.

The graph in Figure 8 has no bridges. As we show next, the epistemic properties of the network flow protocol are different for edges that are bridges and edges that are not bridges. Let r_3 be the run of the network flow protocol depicted in Figure 9, where pipe b is a bridge. Note that although no additional water is pumped into pipe b, an external observer of pipe b would be able to conclude that the faucet at edge d is open because such an observer would notice a right-to-left water flow on pipe b. In other words, $r_3 \Vdash \Box_b p$.

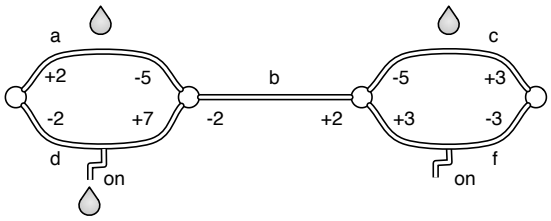

Figure 9: Run r_3 of a network flow protocol.

These examples show that in order for an observer of a non-bridge edge to be able to deduce disjunction $p \vee q$, this edge must be pumping water into the system. In the case over a bridge, however, it is sufficient to have a non-zero flow of the bridge in either of the two directions. This distinction between bridges and non-bridges under the network flow protocol will lead to two different corresponding cases in the definition of our canonical protocol (see Definition 11).

The network flow protocol, as described above, has a peculiar property. Namely, since water could be pumped into the system only through edges, an external observer of bridge b under run r_3 will not only be able to deduce that p is true, but also to conclude that either an external observer of pipe c or an external observer of pipe f must know that $p \vee q$ is true: $r_3 \Vdash \Box_b(\Box_c(p \vee q) \vee \Box_f(p \vee q))$. Indeed, an external observer of pipe b would conclude that water is pumped into the system either at pipe c or at pipe f and, thus, either $\Box_c(p \vee q)$ or $\Box_f(p \vee q)$. To prove the completeness theorem for our logical system, we need a slightly more general class of flow protocols for which this property is not necessarily true. Namely, we allow additional water to be pumped into the system not only at pipes, but also at the vertices. The sink faucets, however, are still located only in the middle of the pipes. Under the modified network flow protocol, the statement $r_3 \Vdash \Box_b(\Box_c(p \vee q) \vee \Box_f(p \vee q))$ is no longer true because an external observer of pipe b can not distinguish run r_3 from run r_4 of the modified protocol depicted in Figure 10 and because $r_4 \Vdash \neg\Box_c(p \vee q)$ and $r_4 \Vdash \neg\Box_f(p \vee q)$.

7.2 Canonical Protocols

In this section we define canonical protocols based on the network flow construction informally discussed above. The canonical protocols are used later in the proof of completeness. Under a canonical protocol, the value of each edge

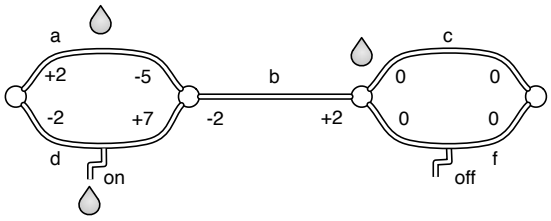

Figure 10: Run r_4 of a network flow protocol.

e contains a maximal consistent subset X^e of $\Phi(Sig, \{e\})$. Informally, set X^e consists of all epistemic facts about an external observer of edge e that are true on a given run. Of course, on the same run, sets X^e for different edges e must be correlated. For example, if set X^e contains formula $\Box_e \Box_h \psi$, then set X^h must contain formula $\Box_h \psi$. In general, if $\Box_e \delta \in X^e$, then formula δ should be, in some sense, "true" on this run. We use network flow to enforce such correlations between sets X^e for different edges e on the same run.

A single canonical protocol is used to only enforce such a correlation for a single formula δ. Thus, each formula δ produces a different canonical protocol. In Section 7.4, we aggregate these canonical protocols into a single protocol. Note that in propositional logic any formula can be written in Disjunctive Normal Form. Any modal formula δ can be shown to be equivalent to $\bigwedge_{i \leq n} \bigvee_{h \in E} \delta_h^i$, where $\delta_h^i \in \Phi(Sig, \{h\})$ for each $i \leq n$ and each $h \in E$. Also note that in the presence of Distributivity axiom and Necessitation inference rule, formula $\Box_e \bigwedge_{i \leq n} \bigvee_{h \in E} \delta_h^i$ is provably equivalent to $\bigwedge_{i \leq n} \Box_e \bigvee_{h \in E} \delta_h^i$. Because of this, in what follows we enforce our correlation between different sets X^e only for formulas δ of the form $\bigvee_{h \in E} \delta_h$, where $\delta_h \in \Phi(Sig, \{h\})$ for each $h \in E$.

Definition 10 *For any signature $Sig = (V, E, \{P_e\}_{e \in E})$, let $\Delta(Sig)$ be the set of all formulas of the form $\bigvee_{e \in E} \delta_e$, where $\delta_e \in \Phi(Sig, \{e\})$ for each $e \in E$.*

The correlation that we intend to enforce is: for all $e \in E$, if $\Box_e \bigvee_{h \in E} \delta_h \in X^e$, then there exist $h \in E$ such that $\delta_h \in X^h$. Instead of defining a single protocol $\mathcal{P}^\delta$ under which this correlation is enforced for each $e \in E$, we define a family of protocols $\{\mathcal{P}_F^\delta\}_{F \subseteq E}$. For each subset $F \subseteq E$, under protocol $\mathcal{P}_F^\delta$ the correlation is enforced only for edges in F.

The enforcement of the desired correlation under protocol $\mathcal{P}_F^\delta$ is achieved by using network the flow construction described in the previous section. Informally, each edge of the graph is viewed as a pipe. In addition to set X^e, the value of each edge e also includes flow values over this edge. As before, sink faucets are placed in the middle of each edge. However, the sink faucet at edge h is open only if $\delta_h \in X^h$. If $\Box_e \delta \in X^e$ and edge e is *not* a bridge, then e is required to "pump" water into the system. The network flow protocol guarantees that if water is pumped into the system, then it must leak through

at least one of the sinks. This implies that if $\Box_e \delta \in X^e$ ("water is pumped in"), then $\delta_h \in X^h$ ("sink is leaking") for at least one disjunct δ_h in formula δ. For the same reason, if $\Box_e \delta \in X^e$ and e is a bridge, then e is required to have a non-zero flow (in either direction).

We now define a canonical protocol $\mathcal{P}_F^\delta$ over a signature $Sig = (V, E, \{P_e\}_{e \in E})$ for each subset $F \subseteq E$ and each $\delta \in \Delta(Sig)$, where δ is of the form $\bigvee_{e \in E} \delta_e$ and $\delta_e \in \Phi(Sig, \{e\})$ for each $e \in E$.

Definition 11 *A value w_e of an edge $e \in Edge(u, u')$ under protocol $\mathcal{P}_F^\delta$ is a tuple $\langle X, \{f_v\}_{v \in Inc(e)} \rangle$ that has the following properties:*

1. *Properties common to all edges.*
   (a) *X is a maximal consistent subset of $\Phi(Sig, \{e\})$,*
   (b) *f_u and $f_{u'}$ are real numbers,*
   (c) *$f_u + f_{u'} > 0$ if and only if $\delta_e \in X$.*
2. *Properties of bridge edges. For each $e \in \mathcal{B}$,*
   (a) *if $\delta_e \notin X$, then $f_u + f_{u'} = 0$,*
   (b) *if $f_u < 0$, then $\Box_e \bigvee_{h \in C_{-e}^u} \delta_h \in X$,*
   (c) *if $e \in F$, $\Box_e \delta \in X$, and $\delta_e \notin X$, then $f_u < 0$ or $f_{u'} < 0$.*
3. *Properties of non-bridge edges. For each $e \in E \setminus \mathcal{B}$,*
   (a) *if $f_u + f_{u'} < 0$, then $\Box_e \delta \in X$,*
   (b) *if $e \in F$, $\Box_e \delta \in X$, and $\delta_e \notin X$, then $f_u + f_{u'} < 0$.*

Valuation. Let π be a function such that, for each $e \in E$ and $p \in P_e$, set p^π contains all values $\langle X, \{f_v\}_{v \in Inc(e)} \rangle$ under protocol $\mathcal{P}_F^\delta$, where $p \in X$.

We now specify local a condition L_u at a vertex u under protocol $\mathcal{P}_F^\delta$. Under the network flow protocol, we allow any vertex u to pump additional water into the system and disallow it to leak water out of the system. This is formally captured by the local condition $\sum_{e \in Inc(u)} f_u^e \geq 0$. At the same time, recall that we use the network flow to enforce property: if $\Box_e \delta \in X^e$, where $\delta = \bigvee_{h \in E} \delta_h$, then $\delta_h \in X^h$ for at least one $h \in E$. Note that if $\delta_h \in X^h$ for at least one $h \in E$, then the property is already true and no additional enforcement is necessary. Because of this, if $\delta_h \in X^h$ for at least one edge h adjacent to vertex u, then we allow the sum $\sum_{e \in Inc(u)} f_u^e$ to be negative. This relaxation of the local condition will be useful later.

Local Conditions. Consider any tuple of values $\langle X^e, \{f_v^e\}_{v \in Inc(e)} \rangle_{e \in Inc(u)}$ under protocol $\mathcal{P}_F^\delta$. This tuple belongs to L_u when the following condition is satisfied: if $\delta_e \notin X^e$ for each $e \in Inc(u)$, then $\sum_{e \in Inc(u)} f_u^e \geq 0$.

This concludes the specification of the family of protocols $\mathcal{P}_F^\delta$. The following corollary directly follows from the above definitions.

Corollary 2 *For any run* $\langle X^e, \{f_u^e\}_{u\in Inc(e)}\rangle_{e\in E}$ *of a protocol* $\mathcal{P}_F^\delta$ *and any real number* $\lambda > 0$*, tuple* $\langle X^e, \{\lambda f_u^e\}_{u\in Inc(e)}\rangle_{e\in E}$ *is a run of protocol* $\mathcal{P}_F^\delta$*.* ⊠

Lemma 11 *Let* $\langle X^e, \{f_u^e\}_{u\in Inc(e)}\rangle_{e\in E}$ *be any run of a protocol* $\mathcal{P}_F^\delta$*. If* $h = (v, v') \in F \cap \mathcal{B}$ *and* $\delta_h \notin X^h$*, then* $f_v^h = 0$ *if and only if* $\Box_h\delta \notin X^h$*.*

Proof. ($\Rightarrow$) : We prove by contrapositive. Suppose that $\Box_h\delta \in X^h$. Then by Definition 11 part 2(c), $f_v^h < 0$ or $f_{v'}^h < 0$. Hence, $f_v^h \neq 0$ or $f_{v'}^h \neq 0$. Note that $f_{v'}^h \neq 0$, by Definition 11 part 2(a), implies that $f_v^h \neq 0$. Therefore, in both cases, $f_v^h \neq 0$.
($\Leftarrow$) : Assume that $f_v^h \neq 0$. By Definition 11 part 2(a), either $f_v^h < 0$ or $f_{v'}^h < 0$. Suppose, without loss of generality, that $f_v^h < 0$. Then, by Definition 11 part 2(b),

$$\Box_h \bigvee_{e\in C_{-h}^v} \delta_e \in X^h. \tag{15}$$

Note that $\bigvee_{e\in C_{-h}^v} \delta_e \to \delta$ is a propositional tautology. Thus, by Necessitation rule,

$$\vdash \Box_h \left(\bigvee_{e\in C_{-h}^v} \delta_e \to \delta \right).$$

Hence, by Distributivity axiom and Modus Ponens rule,

$$\vdash \Box_h \left(\bigvee_{e\in C_{-h}^v} \delta_e \right) \to \Box_h\delta.$$

Thus, $X^h \vdash \Box_h\delta$ from statement (15) and Modus Ponens inference rule. Therefore, $\Box_h\delta \in X^h$ due to the maximality of set X^h. ⊠

7.3 Properties of Canonical Protocols

In this section we prove several technical properties of the canonical protocols that are used in the proof of completeness. To build the intuition, as we proceed, we compare these properties with those of our informal network flow model.

Lemma 12 *For any* $\delta \in \Delta(Sig)$*, if* $F' \subseteq F$*, then each run of protocol* $\mathcal{P}_F^\delta$ *is also a run of protocol* $\mathcal{P}_{F'}^\delta$*.*

Proof. The statement of the lemma immediately follows from the definition of the canonical protocols $\mathcal{P}_F^\delta$. Indeed, the difference between protocol $\mathcal{P}_F^\delta$ and $\mathcal{P}_{F'}^\delta$ is only in parts 2(c) and 3(b) of Definition 11. ⊠

The following theorem formalizes our intuition described earlier that if there is an inflow of water into the system, then there must be at least one open sink for the water to leak.

Theorem 1 *For any $h \in E$ and any run $\langle X^e, \{f^e_u\}_{u\in Inc(e)}\rangle_{e\in E}$ of protocol $\mathcal{P}^{\delta}_{\{h\}}$, if $\square_h\delta \in X^h$, then there is an edge $h' \in E$ such that $\delta_{h'} \in X^{h'}$.*

Proof. Suppose that there is no $h' \in E$ such that $\delta_{h'} \in X^{h'}$. Due to the local conditions of protocol $\mathcal{P}^{\delta}_{\{h\}}$,

$$\sum_{e\in Inc(v)} f^e_v \geq 0, \qquad \text{for each } v \in V. \tag{16}$$

We consider the following two cases separately:
Case I: $h \notin \mathcal{B}$. The sum of flow values over edges can be rearranged to the sum of flow values over vertices. Thus, due to inequality (16),

$$\sum_{e\in Edge(u,u')} (f^e_u + f^e_{u'}) = \sum_{v\in V} \sum_{e\in Inc(v)} f^e_v \geq 0. \tag{17}$$

The assumption that there is no $h' \in E$ such that $\delta_{h'} \in X^{h'}$, together with the assumptions $h \notin \mathcal{B}$ and $\square_h\delta \in X^h$ by part 3(b) of Definition 11, implies that $f^h_v + f^h_{v'} < 0$, where v and v' are the two ends of the edge h. Then, by inequality (17), there must exist $h' \in Edge(u_1, u_2)$ such that $f^{h'}_{u_1} + f^{h'}_{u_2} > 0$. Therefore, $\delta_{h'} \in X^{h'}$ by part 1(c) of Definition 11, which is a contradiction.
Case II: $h \in \mathcal{B}$. By part 2(c) of Definition 11, there is an end u_0 of edge h such that $f^h_{u_0} < 0$, see Figure 11. The sum of the flow values over edges in component $C^{u_0}_{\text{-}h}$ can be rearranged to the sum of the flow values over vertices. Hence, by

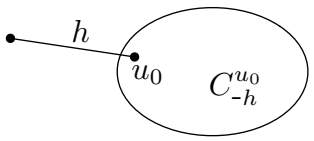

Figure 11: Towards proof of Theorem 1, Case II.

inequality (16),

$$\sum_{e\in Edge(u,u')\cap C^{u_0}_{\text{-}h}} (f^e_u + f^e_{u'}) = \left(\sum_{v\in C^{u_0}_{\text{-}h}} \sum_{e\in Inc(v)} f^e_v \right) - f^h_{u_0} \geq 0 - f^h_{u_0} > 0.$$

Thus, there must exist $h' \in Edge(u_1, u_2) \in C^{u_0}_{\text{-}h}$ such that $f^{h'}_{u_1} + f^{h'}_{u_2} > 0$. Therefore, $\delta_{h'} \in X^{h'}$ by part 1(c) of Definition 11, which is a contradiction. ⊠

Note that in the network flow model the following property holds: if v_1 is one of the vertices of an edge e_0 and the water flows through edge e_0 towards vertex

v_1, then there must exist a sink edge e_k and a path $e_0, v_1, e_1, v_2, e_2, \ldots, v_k, e_k$ such that there is a water flow along this path in the direction from edge e_0 to edge e_k. In our formal setting this property is captured by the following definition and lemma.

Definition 12 *For any maximal consistent set of formulas M, let Γ_M be the set of all paths $e_0, v_1, e_1, v_2, e_2, \ldots, v_k, e_k$, where $k > 0$, such that*

1. $\Box_{e_0} \bigvee_{h \in C^{v_1}_{-e_0}} \delta_h \in M$,
2. $\delta_{e_i} \notin M$, *for each* $0 \leq i < k$,
3. *if* $e_i \in \mathcal{B}$, *then* $\Box_{e_i} \left(\bigvee_{h \in C^{v_{i+1}}_{-e_i}} \delta_h \right) \in M$, *for each* $0 \leq i < k$,
4. $\delta_{e_k} \in M$.

Lemma 13 *For any edge $e \in Edge(u, u')$, if $\Box_e \bigvee_{h \in C^u_{-e}} \delta_h \in M$ and $\delta_e \notin M$, then there is a path in set Γ_M that starts with edge e and continues through vertex u.*

Proof. Let Ω be the set of all such paths $e_0, v_1, e_1, v_2, e_2, \ldots, v_k, e_k$ that $e_0 = e$, $v_1 = u$, $\Box_{e_0}\delta \in M$, and for each $0 \leq i < k$, if $e_i \in \mathcal{B}$, then $\Box_{e_i} \left(\bigvee_{h \in C^{v_{i+1}}_{-e_i}} \delta_h \right) \in M$.

Let C_0 be the set of all edges that belong to at least one path in Ω. Let $C_1, \ldots, C_n$ be the connected components of the graph obtained from component C^u_{-e} by removing all edges in C_0. By the definition of set Ω, for each $0 < i \leq n$ there is an edge g_i in $C_0 \cap \mathcal{B}$, such that

$$\Box_{g_i} \left(\bigvee_{h \in C_i} \delta_h \right) \notin M. \tag{18}$$

Note that edge g_i is the gateway between edges in $C_0 \cup C_1 \cup \cdots \cup C_{i-1} \cup C_{i+1} \cup \cdots \cup C_n$ and C_i. See Figure 12.

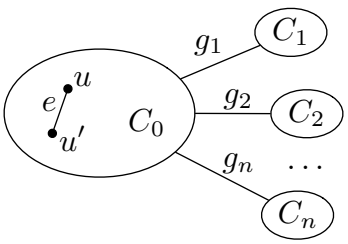

Figure 12: Components and corresponding bridges.

The following formula is a propositional tautology:

$$\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=1}^{n}\bigvee_{h\in C_i}\delta_h\right).$$

Thus, by Necessitation inference rule,

$$\vdash\Box_e\left(\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=1}^{n}\bigvee_{h\in C_i}\delta_h\right)\right).$$

By Distributivity axiom,

$$\vdash\Box_e\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\Box_e\left(\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=1}^{n}\bigvee_{h\in C_i}\delta_h\right)\right).$$

By Lemma 1 and laws of propositional logic,

$$\vdash\Box_e\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\left(\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=2}^{n}\bigvee_{h\in C_i}\delta_h\right)\right)\vee\Box_{g_1}\left(\bigvee_{h\in C_1}\delta_h\right).$$

By Necessitation rule,

$$\vdash\Box_e\left(\Box_e\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\left(\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=2}^{n}\bigvee_{h\in C_i}\delta_h\right)\right)\vee\Box_{g_1}\left(\bigvee_{h\in C_1}\delta_h\right)\right).$$

By Distributivity axiom,

$$\vdash\Box_e\Box_e\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\Box_e\left(\left(\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=2}^{n}\bigvee_{h\in C_i}\delta_h\right)\right)\vee\Box_{g_1}\left(\bigvee_{h\in C_1}\delta_h\right)\right).$$

By Positive Introspection axiom,

$$\vdash\Box_e\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\Box_e\left(\left(\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=2}^{n}\bigvee_{h\in C_i}\delta_h\right)\right)\vee\Box_{g_1}\left(\bigvee_{h\in C_1}\delta_h\right)\right).$$

By Lemma 1 and the laws of propositional logic,

$$\vdash\Box_e\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\left(\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=3}^{n}\bigvee_{h\in C_i}\delta_h\right)\vee\left(\bigvee_{i=1}^{2}\Box_{g_i}\left(\bigvee_{h\in C_i}\delta_h\right)\right)\right).$$

By repeating the previous steps $n-2$ more times,

$$\vdash\Box_e\left(\bigvee_{h\in C^u_{\sim_e}}\delta_h\right)\to\left(\left(\bigvee_{h\in C_0}\delta_h\right)\vee\left(\bigvee_{i=1}^{n}\Box_{g_i}\left(\bigvee_{h\in C_i}\delta_h\right)\right)\right).$$

Since, $\Box_e \left(\bigvee_{h \in C^u_{\text{-}e}} \delta_h \right) \in M$ and set M is a maximal consistent set of formulas,

$$\left(\bigvee_{h \in C_0} \delta_h \right) \vee \left(\bigvee_{i=1}^{n} \Box_{g_i} \left(\bigvee_{h \in C_i} \delta_h \right) \right) \in M.$$

Due to (18) and the maximality of set M, there must exist an edge $h \in C_0$ such that $\delta_h \in M$. By the definition of C_0, there is a path $e, v_1, e_1, v_2, e_2, \ldots, v_k, e_k$ in Ω containing h. Let e_m be the first edge along this path such that $\delta_{e_m} \in M$. Note that $e_m \neq e$ because $\delta_e \notin M$ by the assumption of the claim. Then, $e, v_1, e_1, v_2, e_2, \ldots, v_m, e_m$ is the required path in Γ. $\boxtimes$

Another property that holds for the network flow is: if water is pumped into an edge e_0, then there must exist a sink edge e_k and a path $e_0, v_1, e_1, \ldots, v_k, e_k$ such that there is a water flow along this path in the direction from edge e_0 to edge e_k. We capture this property in the canonical protocol case by the following lemma.

Lemma 14 *For any edge $e \in E$, and any $\delta \in \Delta(Sig)$, if $\Box_e \delta \in M$ and $\delta_e \notin M$, then there is a path in set Γ_M that starts with edge e.*

Proof. Let $e \in Edge(u, u')$. There are two cases:
Case I: $e \in E \setminus \mathcal{B}$. Note that e is a gateway between sets $\{e\}$ and $E \setminus \{e\}$. Then, by Lemma 1,

$$\vdash \Box_e \left(\delta_e \vee \bigvee_{h \in C^u_{\text{-}e}} \delta_h \right) \rightarrow \left(\delta_e \vee \Box_e \bigvee_{h \in C^u_{\text{-}e}} \delta_h \right) \tag{19}$$

At the same time, component $C^u_{\text{-}e}$ contains all edges of the graph except for edge e due to the assumption $e \in E \setminus \mathcal{B}$. Thus,

$$\delta \rightarrow \delta_e \vee \bigvee_{h \in C^u_{\text{-}e}} \delta_h$$

is a propositional tautology. Hence, by Necessitation inference rule,

$$\vdash \Box_e \left(\delta \rightarrow \delta_e \vee \bigvee_{h \in C^u_{\text{-}e}} \delta_h \right).$$

By Distributivity axiom and Modus Ponens inference rule,

$$\vdash \Box_e \delta \rightarrow \Box_e \left(\delta_e \vee \bigvee_{h \in C^u_{\text{-}e}} \delta_h \right).$$

Using statement (19) and the laws of propositional logic,

$$\vdash \Box_e \delta \rightarrow \delta_e \vee \Box_e \bigvee_{h \in C^u_{\text{-}e}} \delta_h.$$

Recall that $\Box_e\delta \in M$ and $\delta_e \notin M$. Thus, $\Box_e \bigvee_{h\in C^u_{-e}} \delta_h \in M$, due to the maximality and the consistency of set M. Then, the required follows from Lemma 13.
Case II: $e \in \mathcal{B}$. Thus, edge e is a gateway between edges of the component C^u_{-e} and edges of the component $C^{u'}_{-e}$. Thus, by Lemma 2,

$$\vdash \Box_e \left(\delta_e \vee \bigvee_{h\in C^u_{-e}} \delta_h \vee \bigvee_{h\in C^{u'}_{-e}} \delta_h \right) \rightarrow \left(\delta_e \vee \Box_e \bigvee_{h\in C^u_{-e}} \delta_h \vee \Box_e \bigvee_{h\in C^{u'}_{-e}} \delta_h \right). \quad (20)$$

At the same time, notice that the formula

$$\delta \rightarrow \delta_e \vee \bigvee_{h\in C^u_{-e}} \delta_h \vee \bigvee_{h\in C^{u'}_{-e}} \delta_h$$

is a propositional tautology. Thus, by Necessitation inference rule,

$$\vdash \Box_e \left(\delta \rightarrow \delta_e \vee \bigvee_{h\in C^u_{-e}} \delta_h \vee \bigvee_{h\in C^{u'}_{-e}} \delta_h \right).$$

By Distributivity axiom and Modus Ponens inference rule,

$$\vdash \Box_e\delta \rightarrow \Box_e \left(\delta_e \vee \bigvee_{h\in C^u_{-e}} \delta_h \vee \bigvee_{h\in C^{u'}_{-e}} \delta_h \right).$$

Using statement (20) and the laws of propositional logic,

$$\vdash \Box_e\delta \rightarrow \delta_e \vee \Box_e \bigvee_{h\in C^u_{-e}} \delta_h \vee \Box_e \bigvee_{h\in C^{u'}_{-e}} \delta_h.$$

Recall that $\Box_e\delta \in M$ and $\delta_e \notin M$. Thus, $\Box_e \bigvee_{h\in C^u_{-e}} \delta_h \in M$ or $\Box_e \bigvee_{h\in C^{u'}_{-e}} \delta_h \in M$, due to the maximality and the consistency of set M. In either case, the required follows from Lemma 13. ⊠

In general, the completeness of a modal logic is often proven through a construction that converts a maximal consistent set of formulas into a world of a "canonical" model for this set of formulas. In our case, the canonical model is represented by protocol $\mathcal{P}^\delta_E$. Instead of a Kripke world, we construct a special run of this protocol. The construction is done recursively for an arbitrary $\mathcal{P}^\delta_F$ in the theorem below. Informally, in term of the network flow model, the theorem states that for any maximal consistent set of formulas X there is a network flow on the graph that satisfies this set of formulas.

Theorem 2 *For every $\delta \in \Delta(Sig)$ every $F \subseteq E$ and every maximal consistent set M there is a run $r = \langle X^e, \{f^e_u\}_{u\in Inc(e)}\rangle_{e\in E}$ of protocol $\mathcal{P}^\delta_F$ such that for each $e \in E$, we have $X^e = M \cap \Phi(Sig, \{e\})$.*

Proof. We prove the theorem by induction on the size of set F.

If $F = \varnothing$, for each $e \in E$ and each $u \in Inc(e)$, let

$$f_u^e = \begin{cases} 1, & \text{if } \delta_e \in X^e, \\ 0, & \text{otherwise.} \end{cases}$$

Claim 2 *Tuple $\langle X^e, \{f_u^e\}_{u \in Inc(e)} \rangle_{e \in E}$ is a run of protocol $\mathcal{P}_{\varnothing}^{\delta}$.*

Proof. The claim immediately follows from Definition 11 and the definition of local conditions of protocol $\mathcal{P}_{\varnothing}^{\delta}$ on page 20. ⊠

Next, assume that $F = F' \cup \{h\}$. By the induction hypothesis, there is a run $r = \langle X^e, \{f_u^e\}_{u \in Inc(e)} \rangle_{e \in E}$ of protocol $\mathcal{P}_{F'}^{\delta}$ such that $X^e = M \cap \Phi(Sig, \{e\})$ for each $e \in E$. If $\Box_h \delta \notin X^h$ or $\delta_h \in X^h$, then, by Definition 11, run r is a run of protocol $\mathcal{P}_F^{\delta}$. Suppose now that $\Box_h \delta \in X^h$ and $\delta_h \notin X^h$. Let λ be any positive real number such that

$$\lambda > |f_u^e|$$

for each $e \in E$ and each $u \in Inc(e)$. By the assumption $\Box_h \delta \in X^h$ and Lemma 14, there is a path $e_0, v_1, e_1, v_2, e_2, \ldots, v_k, e_k$ in Γ_M such that $e_0 = h$. Let v_0 be the end of edge h different from v_1 and let v_{k+1} be the end of edge e_k different from v_k. We next define a tuple $\widehat{r} = \langle X^e, \{\widehat{f}_u^e\}_{u \in Inc(e)} \rangle_{e \in E}$, for which we consider two cases, see Figures 13 and 14:

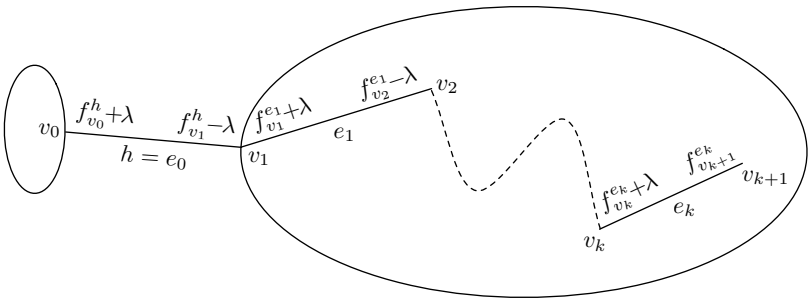

Figure 13: Definition of $\widehat{f}_u^e$ if $h \in \mathcal{B}$.

Case I: If $h \in \mathcal{B}$, then for each $e \in E$ and each $u \in Inc(e)$,

$$\widehat{f}_u^e = \begin{cases} f_u^e + \lambda, & \text{where } e = e_i,\ u = v_i, \text{ and } 0 \le i \le k, \\ f_u^e - \lambda, & \text{where } e = e_i,\ u = v_{i+1}, \text{ and } 0 \le i < k, \\ f_u^e, & \text{otherwise.} \end{cases}$$

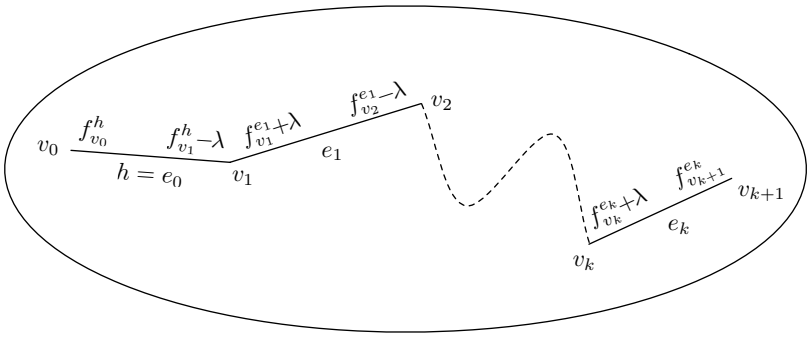

Figure 14: Definition of $\widehat{f}^e_u$ if $h \in E \setminus \mathcal{B}$.

Case II: If $h \in E \setminus \mathcal{B}$, then for each $e \in E$ and each $u \in Inc(e)$,

$$\widehat{f}^e_u = \begin{cases} f^e_u + \lambda, & \text{where } e = e_i,\ u = v_i, \text{ and } 0 < i \le k, \\ f^e_u - \lambda, & \text{where } e = e_i,\ u = v_{i+1}, \text{ and } 0 \le i < k, \\ f^e_u, & \text{otherwise.} \end{cases}$$

This defines tuple $\widehat{r}$.

Claim 3 *$\widehat{f}^e_u + \widehat{f}^e_{u'} = f^e_u + f^e_{u'}$, for each $e \in Edge(u, u') \in E \setminus \{e_0, e_k\}$.*

Proof. If $e = e_i$ for some $0 < i < k$, then

$$\widehat{f}^e_u + \widehat{f}^e_{u'} = \widehat{f}^e_{v_i} + \widehat{f}^e_{v_{i+1}} = f^e_{v_i} + \lambda + f^e_{v_{i+1}} - \lambda = f^e_{v_i} + f^e_{v_{i+1}} = f^e_u + f^e_{u'}.$$

Otherwise, $\widehat{f}^e_u = f^e_u$ and $\widehat{f}^e_{u'} = f^e_{u'}$. Thus, $\widehat{f}^e_u + \widehat{f}^e_{u'} = f^e_u + f^e_{u'}$. ⊠

Claim 4 *Tuple $\widehat{r}$ is a run of protocol $\mathcal{P}^\delta_F$.*

Proof. We need to verify that the tuple $\widehat{r}$ satisfies the conditions of Definition 11 and the local conditions of the run $\mathcal{P}^\delta_F$ on page 20. Below by v_{k+1} we denote the end of edge e_k different from vertex v_k. We start with conditions of Definition 11.

1(c) Due to Claim 3 and the assumption that r is a run of protocol $\mathcal{P}^\delta_{F'}$, we only need to verify condition 1(c) for edges e_0 and e_k.

We first verify this condition for edge e_0. Note that $e_0 = h$. Thus, $\delta_{e_0} \notin X^{e_0}$ due to our assumption. Hence, $f^{e_0}_{v_0} + f^{e_0}_{v_1} \le 0$, because run r satisfies condition 1(c) of Definition 11.

If $e_0 \in \mathcal{B}$, then

$$\widehat{f}^{e_0}_{v_0} + \widehat{f}^{e_0}_{v_1} = f^{e_0}_{v_0} + \lambda + f^{e_0}_{v_1} - \lambda = f^{e_0}_{v_0} + f^{e_0}_{v_1} \le 0.$$

If $e_0 \notin \mathcal{B}$, then, since $\lambda > 0$,

$$\widehat{f}^{e_0}_{v_0} + \widehat{f}^{e_0}_{v_1} = f^{e_0}_{v_0} + f^{e_0}_{v_1} - \lambda < f^{e_0}_{v_0} + f^{e_0}_{v_1} \leq 0.$$

In either case, we have $\delta_{e_0} \notin X^{e_0}$ and $\widehat{f}^{e_0}_{u} + \widehat{f}^{e_0}_{u'} \leq 0$. Thus, condition 1(c) is satisfied.

Next, we verify this condition for the edge e_k. Note that $\delta_{e_k} \in X^{e_k}$, by Definition 12. Thus, we only need to show that $\widehat{f}^{e_k}_{v_k} + \widehat{f}^{e_k}_{v_{k+1}} > 0$. Indeed, $f^{e_k}_{v_k} + f^{e_k}_{v_{k+1}} > 0$ because run r satisfies condition 1(c). Thus, since $\lambda > 0$,

$$\widehat{f}^{e_k}_{v_k} + \widehat{f}^{e_k}_{v_{k+1}} = f^{e_k}_{v_k} + \lambda + f^{e_k}_{v_{k+1}} > f^{e_k}_{v_k} + f^{e_k}_{v_{k+1}} > 0.$$

2(a) Due to Claim 3 and the assumption that r is a run of protocol $\mathcal{P}^{\delta}_{F'}$, we again only need to verify condition 2(a) for edges e_0 and e_k.

We first verify this condition for edge e_0. Note that $\delta_{e_0} \notin X^{e_0}$ by condition 2 of Definition 12. Since run r satisfies the condition 2(c) of Definition 11, we have $f^{e_0}_{v_0} + f^{e_0}_{v_1} = 0$. Hence,

$$\widehat{f}^{e_0}_{v_0} + \widehat{f}^{e_0}_{v_1} = f^{e_0}_{v_0} + \lambda + f^{e_0}_{v_1} - \lambda = f^{e_0}_{v_0} + f^{e_0}_{v_1} = 0.$$

For edge e_k this condition is vacuously true because $\delta_{e_k} \in X^{e_k}$ due to condition 4 of Definition 12.

2(b) By the definition of $\widehat{r}$, for each edge $b \in \mathcal{B} \setminus \{e_0, \ldots, e_k\}$, and each vertex $u \in Inc(b)$, we have $\widehat{f}^{b}_{u} = f^{b}_{u}$. Thus, $\widehat{r}$ on any such edge satisfies condition 2(b) of Definition 11 because run r does.

We next show that condition 2(b) is satisfied for each e_i such that $e_i \in \mathcal{B}$ and $0 \leq i \leq k$. Indeed, consider any $u \in Inc(e_i)$ and suppose that $\widehat{f}^{e_i}_{u} < 0$.

If $u = v_i$, then, since $\lambda > 0$,

$$f^{e_i}_{u} = f^{e_i}_{v_i} = \widehat{f}^{e_i}_{v_i} - \lambda < \widehat{f}^{e_i}_{u} < 0.$$

Thus, $\square_{e_i} \bigvee_{e \in C^{u}_{\bar{e}_i}} \delta_e \in X^{e_i}$ because run r satisfies condition 2(b) of Definition 11.

If $u = v_{i+1}$ and $i < k$, then condition 2(b) is satisfied due to condition 3 of Definition 12.

Finally, if $i = k$ and $u = v_{k+1}$, then $\widehat{f}^{e_i}_{u} = f^{e_i}_{u}$ by the definition of $\widehat{r}$. Thus, condition 2(b) is satisfied by run $\widehat{r}$ because it is satisfied by run r.

2(c) By the definition of $\widehat{r}$, for each edge $b \in \mathcal{B} \setminus \{e_0, \ldots, e_k\}$, and each vertex $u \in Inc(b)$, we have $\widehat{f}^{b}_{u} = f^{b}_{u}$. Thus, $\widehat{r}$ on any such edge satisfies condition 2(c) of Definition 11 because run r does.

We will next show that condition 2(c) is satisfied for each e_i such that $e_i \in \mathcal{B}$ and $0 \leq i < k$. Indeed, note that $\lambda > |f^{e_i}_{v_{i+1}}|$ due to the choice of λ. Thus

$$\widehat{f}^{e_i}_{v_{i+1}} = f^{e_i}_{v_{i+1}} - \lambda < 0.$$

Finally, note that when $i = k$, we have $\delta_{e_k} \in X^{e_k}$. Therefore, condition 2(c) is vacuously true.

3(a) Due to Claim 3 and the assumption that r is a run of protocol $\mathcal{P}^{\delta}_{F'}$, we again only need to verify condition 3(a) for edges e_0 and e_k.

Note that $\square_h \delta \in X^h$ by our assumption. Recall that $e_0 = h$. Thus, $\square_{e_0} \delta \in X^{e_0}$. Therefore, condition 3(a) is satisfied for edge e_0.

By condition 4 of Definition 12, $\delta_{e_k} \in X^{e_k}$. Thus, as we have shown in the case 1(c) above, $\widehat{f}^{e_k}_{v_k} + \widehat{f}^{e_k}_{v_{k+1}} > 0$. Therefore, condition 3(a) is vacuously true for edge e_k.

3(b) Due to Claim 3 and the assumption that r is a run of protocol $\mathcal{P}^{\delta}_{F'}$, we again only need to verify condition 3(b) for edges e_0 and e_k.

Note that $\delta_h \notin X^h$ by our assumption. Recall that $e_0 = h$. Thus, $\delta_{e_0} \notin X^{e_0}$. Since r is a run of protocol $\mathcal{P}^{\delta}_{F'}$, by condition 1(c) of Definition 11, we have $f^{e_0}_{v_0} + f^{e_0}_{v_1} \leq 0$. Hence, due to $\lambda > 0$,

$$\widehat{f}^{e_0}_{v_0} + \widehat{f}^{e_0}_{v_1} = f^{e_0}_{v_0} + f^{e_0}_{v_1} - \lambda \leq 0 - \lambda < 0.$$

Therefore, condition 3(b) is satisfied for edge e_0. By condition 4 of Definition 12, $\delta_{e_k} \in X^{e_k}$. Thus, condition 3(b) is vacuously true for edge e_k.

To show that local conditions (see page 20) are satisfied at any vertex $u \in V$, it is sufficient to show that

$$\sum_{e \in Inc(u)} \widehat{f}^{e}_{u} \geq \sum_{e \in Inc(u)} f^{e}_{u}.$$

Consider first the case when $u = v_0$ and $e_0 \in \mathcal{B}$. Since it has been assumed (see page 6) that vertices along any path do not repeat and because $\lambda > 0$,

$$\sum_{e \in Inc(v_0)} \widehat{f}^{e}_{v_0} = \widehat{f}^{e_0}_{v_0} + \sum_{e \in Inc(v_0) \setminus \{e_0\}} \widehat{f}^{e}_{v_0} = f^{e_0}_{v_0} + \lambda + \sum_{e \in Inc(v_0) \setminus \{e_0\}} f^{e}_{v_0}$$
$$= \sum_{e \in Inc(v_0)} f^{e}_{v_0} + \lambda > \sum_{e \in Inc(v_0)} f^{e}_{v_0}.$$

Next, consider the case when vertex $u = v_i$ for some $0 < i \leq k$. Then,

$$\sum_{e \in Inc(v_i)} \widehat{f}^{e}_{v_i} = \widehat{f}^{e_{i-1}}_{v_i} + \widehat{f}^{e_i}_{v_i} + \sum_{e \in Inc(v_i) \setminus \{e_{i-1}, e_i\}} \widehat{f}^{e}_{v_i}$$
$$= f^{e_{i-1}}_{v_i} - \lambda + f^{e_i}_{v_i} + \lambda + \sum_{e \in Inc(v_i) \setminus \{e_{i-1}, e_i\}} f^{e}_{v_i} = \sum_{e \in Inc(v_i)} f^{e}_{v_i}.$$

Otherwise, the sum $\sum_{e \in Inc(u)} \widehat{f}_u^e$ and the sum $\sum_{e \in Inc(u)} f_u^e$ are equal because they consist of equal terms. ⊠
This concludes the proof of Theorem 2. ⊠

The previous theorem constructs a run ("epistemic world") that matches a maximal consistent set M on all edges. The next theorem enhances the claim of the previous theorem by adding an additional condition on the run being constructed. Namely, if h is a given edge of the graph and r is a given run of the protocol, then the desired run $\widehat{r}$ can be constructed not only to match set M on all edges, but also to satisfy the equation $\widehat{r} =_h r$. The theorem assumes, of course, that run r itself matches set M on edge h. In terms of the network flow model, the theorem states that if there is a network flow that satisfies local properties $M \cap \Phi(Sig, \{h\})$ at a given edge h, then this network flow can be modified to match properties in M globally (on all edges of the graph). The proof of the theorem below explains how the water can be re-routed through the graph to achieve the desired outcome.

Theorem 3 *For each $h \in E$, each run $r = \langle X^e, \{f_u^e\}_{u \in Inc(e)} \rangle_{e \in E}$ of protocol $\mathcal{P}_E^\delta$, and each maximal consistent set M such that $X^h = M \cap \Phi(Sig, \{h\})$, there is a run*

$$\widehat{r} = \langle \widehat{X}^e, \{\widehat{f}_u^e\}_{u \in Inc(e)} \rangle_{e \in E}$$

of protocol $\mathcal{P}_E^\delta$ such that

1. *$\widehat{X}^e = M \cap \Phi(Sig, \{e\})$ for each $e \in E$,*
2. *$\widehat{r} =_h r$.*

Proof. By Theorem 2, there is a run $r' = \langle Y^e, \{\ell_u^e\}_{u \in Inc(e)} \rangle_{e \in E}$ of protocol $\mathcal{P}_E^\delta$ such that $Y^e = M \cap \Phi(Sig, \{e\})$ for each $e \in E$. We will show how this run can be modified to obtain the desired run $\widehat{r}$, by considering several possible cases.
Case I: if $\delta_h \in M$, then define $\widehat{r}$ to be the tuple $\langle Y^e, \{\widehat{f}_u^e\}_{u \in Inc(e)} \rangle_{e \in E}$, where

$$\widehat{f}_u^e = \begin{cases} f_u^h, & \text{if } e = h, \\ \ell_u^e, & \text{otherwise.} \end{cases}$$

Claim 5 *$\widehat{r}$ is a run of protocol $\mathcal{P}_E^\delta$ and $\widehat{r} =_h r$.*

Proof. We need to verify that tuple $\widehat{r}$ satisfies conditions of Definition 11 and the local conditions of protocol $\mathcal{P}_E^\delta$ on page 20.

We start with the conditions of Definition 11 for an arbitrary edge $e \in E$. If $e = h$, then $\widehat{r} =_e r$, and thus tuple $\widehat{r}$ satisfies the conditions of Definition 11 on edge e because run r does. Similarly, if $e \neq h$, then $\widehat{r} =_e r'$, and thus tuple $\widehat{r}$ satisfies the conditions of Definition 11 on edge e because run r' does.

We now show that tuple $\widehat{r}$ vacuously satisfies local conditions of protocol $\mathcal{P}_E^\delta$ at any vertex $v \in V$. If $v \notin Inc(h)$, then $\widehat{r} =_e r'$ for each $e \in Inc(v)$. Thus, tuple $\widehat{r}$ satisfies local conditions of protocol $\mathcal{P}_E^\delta$ because run r' does. If $v \in Inc(h)$, then tuple $\widehat{r}$ vacuously satisfies local conditions of protocol $\mathcal{P}_E^\delta$ because $\delta_h \in M$.

The condition $\widehat{r} =_h r$ is satisfied because (i) $Y^h = M \cap \Phi(Sig, \{h\}) = X^h$ and (ii) $\widehat{f}^h_u = f^h_u$ for each $u \in Inc(h)$. ⊠

Case II: if $\delta_h \notin M$ and $h \in E \setminus \mathcal{B}$. Let $h \in Edge(v_0, v_1)$. Since $h \notin \mathcal{B}$, there is a circular path $h = e_0, v_1, e_1, v_2, \ldots, v_{k-1}, e_{k-1}, v_k, e_k = h$. By Definition 9, $e_i \notin \mathcal{B}$ for each $0 \leq i < k$. We will now further split this case into two subcases:

Subcase IIa: If $\Box_h \delta \notin M$, then define $\widehat{r}$ to be tuple $\langle Y^e, \{\widehat{f}^e_u\}_{u \in Inc(e)} \rangle_{e \in E}$, see Figure 15, where

$$\widehat{f}^e_u = \begin{cases} \ell^e_u + f^h_{v_0} - \ell^h_{v_0}, & \text{if } e = e_i,\ u = v_i, \text{ and } 0 \leq i < k, \\ \ell^e_u + f^h_{v_1} - \ell^h_{v_1}, & \text{if } e = e_i,\ u = v_{i+1}, \text{ and } 0 \leq i < k, \\ \ell^e_u, & \text{otherwise.} \end{cases}$$

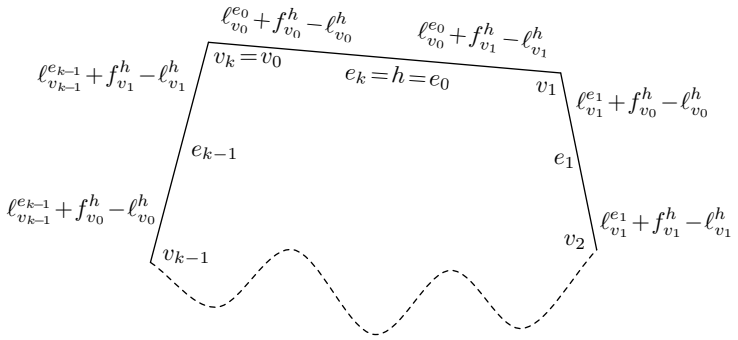

Figure 15: Subcase IIa.

Claim 6 *$\widehat{f}^{e_i}_{v_i} + \widehat{f}^{e_i}_{v_{i+1}} = \ell^{e_i}_{v_i} + \ell^{e_i}_{v_{i+1}}$ and $\widehat{f}^{e_i}_{v_{i+1}} + \widehat{f}^{e_{i+1}}_{v_{i+1}} = \ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}}$, for each $0 \leq i < k$.*

Proof. By condition 1(c) of Definition 11, the assumption $\delta_h \notin M$ implies that $f^h_{v_0} + f^h_{v_1} \leq 0$ and $\ell^h_{v_0} + \ell^h_{v_1} \leq 0$. By condition 3(a) of the same definition, the assumption $\Box_h \delta \notin M$ implies that $f^h_{v_0} + f^h_{v_1} \geq 0$ and $\ell^h_{v_0} + \ell^h_{v_1} \geq 0$. Thus, $f^h_{v_0} + f^h_{v_1} = 0$ and $\ell^h_{v_0} + \ell^h_{v_1} = 0$. Therefore,

$$\begin{aligned} \widehat{f}^{e_i}_{v_i} + \widehat{f}^{e_i}_{v_{i+1}} = \ell^{e_i}_{v_i} + f^h_{v_0} - \ell^h_{v_0} + \ell^{e_i}_{v_{i+1}} + f^h_{v_1} - \ell^h_{v_1} = \ell^{e_i}_{v_i} + \ell^{e}_{v_{i+1}} + \\ (f^h_{v_0} + f^h_{v_1}) - (\ell^h_{v_0} + \ell^h_{v_1}) = \ell^{e_i}_{v_i} + \ell^{e}_{v_{i+1}} + 0 - 0 = \ell^{e_i}_{v_i} + \ell^{e_i}_{v_{i+1}}, \end{aligned}$$

and

$$\begin{aligned} \widehat{f}^{e_i}_{v_{i+1}} + \widehat{f}^{e_{i+1}}_{v_{i+1}} = \ell^{e_i}_{v_{i+1}} + f^h_{v_1} - \ell^h_{v_1} + \ell^{e_{i+1}}_{v_{i+1}} + f^h_{v_0} - \ell^h_{v_0} = \ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}} + \\ (f^h_{v_0} + f^h_{v_1}) - (\ell^h_{v_0} + \ell^h_{v_1}) = \ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}} + 0 - 0 = \ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}}. \end{aligned}$$

⊠

Claim 7 *$\widehat{r}$ is a run of protocol $\mathcal{P}_E^\delta$ and $\widehat{r} =_h r$.*

Proof. We need to verify that the tuple $\widehat{r}$ satisfies the conditions of Definition 11 and the local conditions of protocol $\mathcal{P}_E^\delta$ on page 20.

We start with the conditions of Definition 11 for an arbitrary edge $e \in E$. If $e = e_i$ for some $0 \le i < k$, then, due to the path being circular, $e \notin \mathcal{B}$. Thus, all applicable conditions from Definition 11 are satisfied for tuple $\widehat{r}$ because they are satisfied for run r' and due to the equality $\widehat{f}^{e_i}_{v_i} + \widehat{f}^{e_i}_{v_{i+1}} = \ell^{e_i}_{v_i} + \ell^{e_i}_{v_{i+1}}$ established in Claim 6. If $e \ne e_i$ for all $0 \le i < k$, then the required is true because $\widehat{r} =_e r'$.

We now show that tuple $\widehat{r}$ satisfies local conditions of protocol $\mathcal{P}_E^\delta$ at any vertex $v \in V$. If $v = v_{i+1}$ for some $0 \le i < k$, then $\widehat{f}^{e_i}_{v_{i+1}} + \widehat{f}^{e_{i+1}}_{v_{i+1}} = \ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}}$ by Claim 6. Thus, $\sum_{e \in Inc(v_{i+1})} \widehat{f}^{e}_{v_{i+1}} = \sum_{e \in Inc(v_{i+1})} \ell^{e}_{v_{i+1}}$. If $v \ne v_{i+1}$ for all $0 \le i < k$, then $\widehat{r} =_e r'$ for all $e \in Inc(v)$. In either of these two cases, tuple $\widehat{r}$ satisfies the local conditions of protocol $\mathcal{P}_E^\delta$ at vertex $v \in V$ because run r' satisfies these conditions.

Condition $\widehat{r} =_h r$ is satisfied because (i) $Y^h = M \cap \Phi(Sig, \{h\}) = X^h$, (ii) $\widehat{f}^h_{v_0} = \ell^h_{v_0} + f^h_{v_0} - \ell^h_{v_0} = f^h_{v_0}$, and (iii) $\widehat{f}^h_{v_1} = \ell^h_{v_1} + f^h_{v_1} - \ell^h_{v_1} = f^h_{v_1}$. ⊠

Subcase IIb: If $\square_h \delta \in M$, then $f^h_{v_0} + f^h_{v_1} < 0$ and $\ell^h_{v_0} + \ell^h_{v_1} < 0$ due to condition 3(b) of Definition 11. Let $\lambda = (f^h_{v_0} + f^h_{v_1})/(\ell^h_{v_0} + \ell^h_{v_1})$. Note that $\lambda > 0$. Define $\widehat{r}$ to be the tuple $\langle Y^e, \{\widehat{f}^e_u\}_{u \in Inc(e)} \rangle_{e \in E}$, see Figure 16, where

$$\widehat{f}^e_u = \begin{cases} \lambda(\ell^e_u - \ell^h_{v_0}) + f^h_{v_0}, & \text{if } e = e_i,\ u = v_i, \text{ and } 0 \le i < k, \\ \lambda(\ell^e_u + \ell^h_{v_0}) - f^h_{v_0}, & \text{if } e = e_i,\ u = v_{i+1}, \text{ and } 0 \le i < k, \\ \lambda \ell^e_u, & \text{otherwise.} \end{cases}$$

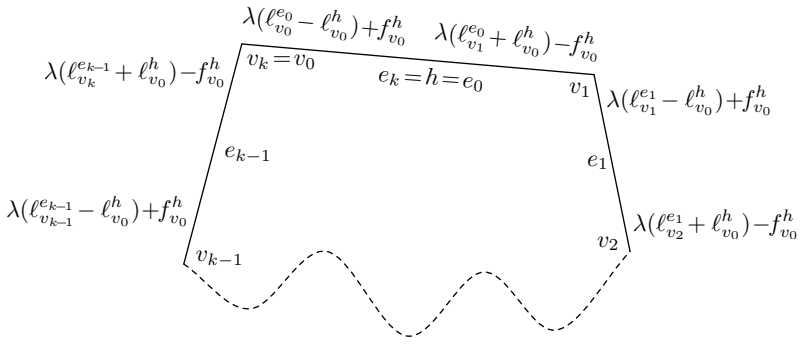

Figure 16: Subcase IIb.

Claim 8 *$\widehat{f}^{e_i}_{v_i} + \widehat{f}^{e_i}_{v_{i+1}} = \lambda(\ell^{e_i}_{v_i} + \ell^{e_i}_{v_{i+1}})$ and $\widehat{f}^{e_i}_{v_{i+1}} + \widehat{f}^{e_{i+1}}_{v_{i+1}} = \lambda(\ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}})$, for each $0 \leq i < k$.*

Proof.

$$\widehat{f}^{e_i}_{v_i} + \widehat{f}^{e_i}_{v_{i+1}} = \lambda(\ell^{e_i}_{v_i} - \ell^h_{v_0}) + f^h_{v_0} + \lambda(\ell^{e_i}_{v_{i+1}} + \ell^h_{v_0}) - f^h_{v_0} = \lambda(\ell^{e_i}_{v_i} + \ell^{e_i}_{v_{i+1}}).$$

Similarly,

$$\widehat{f}^{e_i}_{v_{i+1}} + \widehat{f}^{e_{i+1}}_{v_{i+1}} = \lambda(\ell^{e_i}_{v_{i+1}} + \ell^h_{v_0}) - f^h_{v_0} + \lambda(\ell^{e_{i+1}}_{v_{i+1}} - \ell^h_{v_0}) + f^h_{v_0} = \lambda(\ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}}).$$

⊠

Claim 9 *$\widehat{r}$ is a run of protocol $\mathcal{P}^\delta_E$ and $\widehat{r} =_h r$.*

Proof. We need to verify that tuple $\widehat{r}$ satisfies the conditions of Definition 11 and the local conditions of protocol $\mathcal{P}^\delta_E$ on page 20.

We start with the conditions of Definition 11 for an arbitrary edge $e \in E$. If $e = e_i$ for some $0 \leq i < k$, then $e \notin \mathcal{B}$ since the path is circular. Thus, all applicable conditions from Definition 11 are satisfied for tuple $\widehat{r}$ because they are satisfied for run r' and due to $\lambda > 0$ and the equality $\widehat{f}^{e_i}_{v_i} + \widehat{f}^{e_i}_{v_{i+1}} = \lambda(\ell^{e_i}_{v_i} + \ell^{e_i}_{v_{i+1}})$ established in Claim 8. If $e \neq e_i$ for all $0 \leq i < k$, then the required is true because run r' satisfies the conditions from Definition 11 and $\widehat{f}^e_u =_e \lambda \ell^e_u$ for each $u \in Inc(e)$, where $\lambda > 0$.

We now show that tuple $\widehat{r}$ satisfies the local conditions of protocol $\mathcal{P}^\delta_E$ at any vertex $v \in V$. If $v = v_{i+1}$ for some $0 \leq i < k$, then $\widehat{f}^{e_i}_{v_{i+1}} + \widehat{f}^{e_{i+1}}_{v_{i+1}} = \lambda(\ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}})$ by Claim 8. Thus, $\sum_{e \in Inc(v_{i+1})} \widehat{f}^e_{v_{i+1}} = \lambda \sum_{e \in Inc(v_{i+1})} \ell^e_{v_{i+1}}$. If $v \neq v_{i+1}$ for all $0 \leq i < k$, then $\widehat{f}^e_v = \lambda \ell^e_v$ for all $e \in Inc(v)$. In either of these two cases, tuple $\widehat{r}$ satisfies the local conditions of protocol $\mathcal{P}^\delta_E$ at vertex $v \in V$ because run r' satisfies these conditions and $\lambda > 0$.

The condition $\widehat{r} =_h r$ is satisfied because $Y^h = M \cap \Phi(Sig, \{h\}) = X^h$,

$$\widehat{f}^h_{v_0} = \lambda(\ell^h_{v_0} - \ell^h_{v_0}) + f^h_{v_0} = 0 + f^h_{v_0} = f^h_{v_0},$$

and

$$\widehat{f}^h_{v_1} = \lambda(\ell^h_{v_1} + \ell^h_{v_0}) - f^h_{v_0} = \frac{f^h_{v_0} + f^h_{v_1}}{\ell^h_{v_0} + \ell^h_{v_1}}(\ell^h_{v_1} + \ell^h_{v_0}) - f^h_{v_0} = f^h_{v_0} + f^h_{v_1} - f^h_{v_0} = f^h_{v_1}.$$

⊠

Case III: If $\delta_h \notin M$ and $h \in \mathcal{B}$. Let $h \in Edge(v_0, v_1)$. There are three subcases:

Subcase IIIa: If $f^h_{v_1} \cdot \ell^h_{v_1} = 0$, then $f^h_{v_1} = 0$ or $\ell^h_{v_1} = 0$. Hence, by Lemma 11, $\Box_h \delta \notin X^h$. Thus, again by Lemma 11, $f^h_{v_1} = 0$, $f^h_{v_0} = 0$, $\ell^h_{v_0} = 0$, and $\ell^h_{v_1} = 0$. Furthermore, $Y^h = M \cap \Phi(Sig, \{h\}) = X^h$. Hence, $r =_h r'$. Let $\widehat{r} = r'$.

Subcase IIIb: If $f^h_{v_1} \cdot \ell^h_{v_1} > 0$, then define $\widehat{r}$ to be tuple

$$\langle Y^e, \{(f^h_{v_1}/\ell^h_{v_1})\ell^e_u\}_{u \in Inc(e)}\rangle_{e \in E}.$$

By Corollary 2 and the fact that r' is a run of protocol $\mathcal{P}^\delta_E$, tuple $\widehat{r}$ is a run of protocol $\mathcal{P}^\delta_E$. Since $Y^h = M \cap \Phi(Sig, \{h\}) = X^h$, to show that $\widehat{r} =_h r$, it is sufficient to show that $(f^h_{v_1}/\ell^h_{v_1})\ell^h_{v_1} = f^h_{v_1}$ and $(f^h_{v_1}/\ell^h_{v_1})\ell^h_{v_0} = f^h_{v_0}$. The former is an algebraic identity, the later follows from the equalities $f^h_{v_0} + f^h_{v_1} = 0$ and $\ell^h_{v_0} + \ell^h_{v_1} = 0$, which, in turn, follows from condition 2(a) of Definition 11.

Subcase IIIc: If $f^h_{v_1} \cdot \ell^h_{v_1} < 0$, then $f^h_{v_1} \neq 0$. By Definition 11, part 2(a), it follows that either $f^h_{v_1} < 0$ or $f^h_{v_0} < 0$. We consider the former case, the later one is similar. If $f^h_{v_1} < 0$, then $\Box_h \bigvee_{e \in C^{v_1}_{-h}} \delta_e \in X^h$ by Definition 11, part 2(b). Hence, $\Box_h \bigvee_{e \in C^{v_1}_{-h}} \delta_e \in M$. Thus, $\Box_h \bigvee_{e \in C^{v_1}_{-h}} \delta_e \in Y^h$. By Lemma 13, there is a path $e_0, v_1, e_1, v_2, \ldots, v_k, e_k$ in Γ_M such that $h = e_0$. Let λ be any positive real number such that

$$\lambda > |\ell^e_u|$$

for each $e \in E$ and each $u \in Inc(e)$. Also, let $\mu = f^h_{v_0}/(\ell^h_{v_0} + \lambda)$. Recall that $f^h_{v_1} < 0$. Thus, $f^h_{v_0} > 0$ by condition 2(a) of Definition 11. Additionally, note that $\lambda > |\ell^h_{v_0}|$. Thus, $\mu > 0$.

Define $\widehat{r}$ to be tuple $\langle Y^e, \{\widehat{f}^e_u\}_{u \in Inc(e)}\rangle_{e \in E}$, see Figure 17, where

$$\widehat{f}^e_u = \begin{cases} \mu(\ell^e_u + \lambda), & \text{if } e = e_i,\ u = v_i, \text{ and } 0 \leq i \leq k, \\ \mu(\ell^e_u - \lambda), & \text{if } e = e_i,\ u = v_{i+1}, \text{ and } 0 \leq i < k, \\ \mu\ell^e_u, & \text{otherwise.} \end{cases} \tag{21}$$

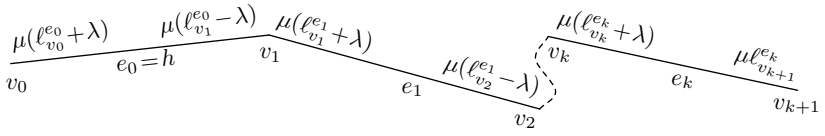

Figure 17: Subcase IIIc, the last vertex of the path, not named in the text, is denoted by v_{k+1} on this figure.

Claim 10 *$\widehat{f}^e_u + \widehat{f}^e_{u'} = \mu(\ell^e_u + \ell^e_{u'})$, for each edge $e \in Edge(u, u') \in E \setminus \{e_k\}$.*

Proof. If $e = e_i$ for some $0 \leq i < k$, then

$$\widehat{f}^{e_i}_{v_i} + \widehat{f}^{e_i}_{v_{i+1}} = \mu(\ell^{e_i}_{v_i} + \lambda) + \mu(\ell^{e_i}_{v_{i+1}} - \lambda) = \mu(\ell^{e_i}_{v_i} + \ell^{e_i}_{v_{i+1}}).$$

If $e \neq e_i$ for all $0 \leq i \leq k$, then $\widehat{f}^e_u + \widehat{f}^e_u = \mu\ell^e_u + \mu\ell^e_{u'} = \mu(\ell^e_u + \ell^e_{u'})$. ⊠

Claim 11 *$\sum_{e\in Inc(u)} \widehat{f}^e_u \geq \mu \sum_{e\in Inc(u)} \ell^e_u$ for each vertex $u \in V$.*

Proof. If $u \neq v_i$ for all $0 \leq i \leq k$, then

$$\sum_{e\in Inc(u)} \widehat{f}^e_u = \sum_{e\in Inc(u)} \mu\ell^e_u = \mu \sum_{e\in Inc(u)} \ell^e_u.$$

If $u = v_{i+1}$ for some $0 \leq i < k$, then

$$\begin{aligned}
\sum_{e\in Inc(u)} \widehat{f}^e_u &= \widehat{f}^{e_i}_{v_{i+1}} + \widehat{f}^{e_{i+1}}_{v_{i+1}} + \sum_{e\in Inc(v_{i+1})\setminus\{e_i,e_{i+1}\}} \widehat{f}^e_{v_{i+1}} \\
&= \mu(\ell^{e_i}_{v_{i+1}} - \lambda) + \mu(\ell^{e_{i+1}}_{v_{i+1}} + \lambda) + \sum_{e\in Inc(v_{i+1})\setminus\{e_i,e_{i+1}\}} \mu\ell^e_{v_{i+1}} \\
&= \mu\left(\ell^{e_i}_{v_{i+1}} + \ell^{e_{i+1}}_{v_{i+1}} + \sum_{e\in Inc(v_{i+1})\setminus\{e_i,e_{i+1}\}} \ell^e_{v_{i+1}}\right) \\
&= \mu \sum_{e\in Inc(v_{i+1})} \ell^e_{v_{i+1}}.
\end{aligned}$$

Finally, if $u = v_0$, then, since $\lambda > 0$ and $\mu > 0$,

$$\begin{aligned}
\sum_{e\in Inc(u)} \widehat{f}^e_u &= \widehat{f}^{e_0}_{v_0} + \sum_{e\in Inc(v_0)\setminus\{e_0\}} \widehat{f}^e_{v_0} \\
&= \mu(\ell^{e_0}_{v_0} + \lambda) + \sum_{e\in Inc(v_0)\setminus\{e_0\}} \mu\ell^e_{v_0} \\
&= \mu\left(\ell^{e_0}_{v_0} + \sum_{e\in Inc(v_0)\setminus\{e_0\}} \ell^e_{v_0}\right) + \mu\lambda \\
&= \mu \sum_{e\in Inc(v_0)} \ell^e_{v_0} + \mu\lambda \\
&> \mu \sum_{e\in Inc(v_0)} \ell^e_{v_0}.
\end{aligned}$$

The last inequality is true because $\lambda > 0$ and $\mu > 0$. ⊠

Claim 12 *$\widehat{r}$ is a run of protocol $\mathcal{P}^\delta_E$ and $\widehat{r} =_h r$.*

Proof. We need to verify that tuple $\widehat{r}$ satisfies the conditions of Definition 11 and the local conditions of protocol $\mathcal{P}^\delta_E$ on page 20. Below by v_{k+1} we denote the end of edge e_k different from vertex v_k. We start with conditions of Definition 11.

1(c) Due to Claim 10 and the assumption that r' is a run of protocol $\mathcal{P}^\delta_E$, we only need to verify condition 1(c) for edge e_k. Note that $\delta_{e_k} \in X^{e_k}$, by Definition 12. Thus, we only need to show that $\widehat{f}^{e_k}_{v_k} + \widehat{f}^{e_k}_{v_{k+1}} > 0$. Indeed,

$\ell^{e_k}_{v_k} + \ell^{e_k}_{v_{k+1}} > 0$ because run r' satisfies condition 1(c). Since $\lambda > 0$ and $\mu > 0$,

$$\widehat{f}^{e_k}_{v_k} + \widehat{f}^{e_k}_{v_{k+1}} = \mu(\ell^{e_k}_{v_k} + \lambda) + \mu\ell^{e_k}_{v_{k+1}} = \mu(\ell^{e_k}_{v_k} + \ell^{e_k}_{v_{k+1}}) + \mu\lambda > \mu(\ell^{e_k}_{v_k} + \ell^{e_k}_{v_{k+1}}) > 0.$$

2(a) Due to Claim 10 and the assumption that r' is a run of protocol $\mathcal{P}^{\delta}_{E}$, we again only need to verify condition 2(a) for edge e_k, which is vacuously true because $\delta_{e_k} \in X^{e_k}$ due to condition 4 of Definition 12.

2(b) By the definition of $\widehat{r}$, for each edge $b \in \mathcal{B} \setminus \{e_0, \ldots, e_k\}$, and each vertex $u \in Inc(b)$, we have $\widehat{f}^{b}_{u} = \mu\ell^{b}_{u}$. Thus, $\widehat{r}$ on any such edge satisfies condition 2(b) of Definition 11 because run r' does and $\mu > 0$.

We next show that condition 2(b) is satisfied for each e_i such that $e_i \in \mathcal{B}$ and $0 \leq i \leq k$. Indeed, consider any $u \in Inc(e_i)$ and suppose that $\widehat{f}^{e_i}_{u} < 0$.

If $u = v_i$, then, since $\lambda > 0$ and $\mu > 0$, from equation (21), we have

$$\ell^{e_i}_{u} = \ell^{e_i}_{v_i} = \frac{\widehat{f}^{e_i}_{v_i}}{\mu} - \lambda < \frac{\widehat{f}^{e_i}_{v_i}}{\mu} < 0.$$

Thus, $\Box_{e_i} \bigvee_{e \in C^{u}_{-e_i}} \delta_e \in X^{e_i}$ because run r' satisfies condition 2(b) of Definition 11.

If $u = v_{i+1}$ and $i < k$, then condition 2(b) is satisfied due to condition 3 of Definition 12.

Finally, if $i = k$ and $u = v_{k+1}$, then $\widehat{f}^{e_i}_{u} = \mu\ell^{e_i}_{u}$ by the definition of $\widehat{r}$. Thus, condition 2(b) is satisfied by run $\widehat{r}$ because it is satisfied by run r' and since $\mu > 0$.

2(c) By the definition of $\widehat{r}$, for each edge $b \in \mathcal{B} \setminus \{e_0, \ldots, e_k\}$, and each vertex $u \in Inc(b)$, we have $\widehat{f}^{b}_{u} = \mu\ell^{b}_{u}$. Thus, $\widehat{r}$ on any such edge satisfies condition 2(c) of Definition 11 because run r' does and $\mu > 0$.

We will next show that condition 2(c) is satisfied for each e_i such that $e_i \in \mathcal{B}$ and $0 \leq i < k$. Indeed, note that $\lambda > |\ell^{e_i}_{v_{i+1}}|$ due to the choice of λ. Thus

$$\widehat{f}^{e_i}_{v_{i+1}} = \mu(\ell^{e_i}_{v_{i+1}} - \lambda) < 0.$$

Finally, note that when $i = k$, we have $\delta_{e_k} \in X^{e_k}$. Therefore, condition 2(c) is vacuously true.

3(a) Due to Claim 10 and the assumption that r' is a run of protocol $\mathcal{P}^{\delta}_{E}$, we again only need to verify condition 3(a) for edge e_k. By condition 4 of Definition 12, $\delta_{e_k} \in X^{e_k}$. Thus, as we have shown in the case 1(c) above, $\widehat{f}^{e_k}_{v_k} + \widehat{f}^{e_k}_{v_{k+1}} > 0$. Therefore, condition 3(a) is vacuously true for edge e_k.

3(b) Due to Claim 10 and the assumption that r' is a run of protocol $\mathcal{P}^{\delta}_{E}$, we once more only need to verify condition 3(b) for edge e_k. By condition 4 of Definition 12, $\delta_{e_k} \in X^{e_k}$. Thus, condition 3(b) is vacuously true for edge e_k.

The local conditions (see page 20) are satisfied by tuple $\widehat{r}$ at each vertex $u \in V$ because they are satisfied by run r' and due to Claim 11 combined with the fact that $\mu > 0$.

To show that $\widehat{r} =_h r$, first note that $Y^h = M \cap \Phi(Sig, \{h\}) = X^h$. Then, observe that

$$\widehat{f}^h_{v_0} = \mu(\ell^h_{v_0} + \lambda) = \frac{f^h_{v_0}}{\ell^h_{v_0} + \lambda}(\ell^h_{v_0} + \lambda) = f^h_{v_0}.$$

Finally, note that $f^h_{v_0} = -f^h_{v_1}$ and $\ell^h_{v_0} = -\ell^h_{v_1}$ because runs r and r' satisfy condition 2(a) of Definition 11. Thus,

$$\widehat{f}^h_{v_1} = \mu(\ell^h_{v_1} - \lambda) = \frac{f^h_{v_0}}{\ell^h_{v_0} + \lambda}(\ell^h_{v_1} - \lambda) = \frac{-f^h_{v_1}}{-\ell^h_{v_1} + \lambda}(\ell^h_{v_1} - \lambda) = f^h_{v_1}.$$

⊠

This concludes the proof of Theorem 3. ⊠

7.4 Aggregated Protocol

Recall from Section 7.2 that canonical protocol $\mathcal{P}^\delta_E$ has formula δ as a parameter. In this section we introduce a construction that aggregates multiple canonical protocols. One can view a run of the aggregated protocol $\mathcal{P}$ as several runs of different canonical protocols for different values of parameter δ being executed concurrently on different "levels". Also recall that a value of an edge under a canonical protocol consists of a maximal consistent set of formulas and a pair of real numbers (flow values). Although there is no explicit connection between flow values on different levels for the same edge, we assume that maximal consistent sets are the same on all layers for a given edge of the aggregated protocol, see Definition 13.

Definition 13 *A value w_e of an edge $e \in E$ under the aggregated protocol $\mathcal{P}$ is a tuple $\langle X, \{f_{v,\delta}\}_{v \in Inc(e), \delta \in \Delta(Sig)}\rangle$ such that $\langle X, \{f_{v,\delta}\}_{v \in Inc(e)}\rangle$ is a value of edge e under protocol $\mathcal{P}^\delta_E$ for each $\delta \in \Delta(Sig)$.*

Valuation. Let π be a function such that, for each $e \in E$ and $p \in P_e$, set p^π contains all values $\langle X, \{f_{v,\delta}\}_{v \in Inc(e), \delta \in \Delta(Sig)}\rangle$, where $p \in X$.

Local Conditions. A tuple $\langle X^e, \{f^e_{v,\delta}\}_{v \in Inc(e), \delta \in \Delta(Sig)}\rangle_{e \in Inc(u)}$ satisfies the local conditions of protocol $\mathcal{P}$ at vertex u if for each $\delta \in \Delta(Sig)$, the tuple $\langle X^e, \{f^e_{v,\delta}\}_{v \in Inc(e)}\rangle_{e \in Inc(u)}$ satisfies local conditions of protocol $\mathcal{P}^\delta_E$ at vertex u.

This concludes the definition of the aggregated protocol $\mathcal{P}$.

Theorem 4 *If $e \in E$, $\varphi \in \Phi(Sig, \{e\})$, and tuple*

$$r = \langle X^h, \{f^h_{u,\delta}\}_{u \in Inc(h), \delta \in \Delta(Sig)}\rangle_{h \in E}$$

is a run of protocol $\mathcal{P}$, then $r \Vdash \varphi$ if and only if $\varphi \in X^e$.

Proof. We prove the theorem by induction on the structural complexity of formula φ. If φ is a proposition $p \in P_e$, then the required follows from Definition 7 and the definition of valuation function π for protocol $\mathcal{P}$. The cases when φ is constant $\bot$ or an implication $\varphi_1 \to \varphi_2$ follow from Definition 7 and the maximality and the consistency of set X^e in the standard way. Now let φ be of the form $\Box_e\psi$.

($\Rightarrow$) : Suppose that $\bigwedge_i \bigvee_{h\in E} \psi_h^i$ is the conjunctive normal form of $\neg\psi$ such that $\psi_h^i \in \Phi(Sig, \{h\})$ for each $h \in E$. Thus, the following statement can be proven using just the axioms of the propositional logic in language $\Phi(Sig)$

$$\vdash \neg \bigwedge_i \bigvee_{h\in E} \psi_h^i \to \psi. \tag{22}$$

Assume that $\Box_e\psi \notin X^e$. To prove that $r \nVdash \Box_e\psi$, it suffices to show that there is a run $\widehat{r}$ of the canonical protocol $\mathcal{P}_E$ such that $\widehat{r} =_e r$ and $\widehat{r} \Vdash \bigwedge_i \bigvee_{h\in E} \psi_h^i$.

The assumption $\Box_e\psi \notin X^e$ and the maximality of set X^e imply that $X^e \nvdash \Box_e\psi$. Thus, $X^e \nvdash \psi$ by Lemma 4. Hence, set $X^e \cup \{\neg\psi\}$ is consistent. Let M be any maximal consistent extension of $X^e \cup \{\neg\psi\}$. By Theorem 3, for each $\delta \in \Delta(Sig)$ there is a run $\widehat{r}_\delta = \langle \widehat{X}^h, \{\widehat{f}^h_{u,\delta}\}_{u\in Inc(h)}\rangle_{h\in E}$ of the canonical protocol $\mathcal{P}_E^\delta$ such that $\widehat{r} =_e r$ and $\widehat{X}^h = M \cap \Phi(Sig, \{h\})$ for each $h \in E$. Define tuple $\widehat{r}$ to be $\langle \widehat{X}^h, \{\widehat{f}^h_{u,\delta}\}_{u\in Inc(h),\delta\in\Delta(Sig)}\rangle_{h\in E}$. By the definition of protocol $\mathcal{P}$, tuple $\widehat{r}$ is a run of $\mathcal{P}$.

We next show that $\widehat{r} \Vdash \bigwedge_i \bigvee_{h\in E} \psi_h^i$. Suppose the opposite, then there is i_0 such that $\widehat{r} \nVdash \bigvee_{h\in E} \psi_h^{i_0}$. Thus, $\widehat{r} \nVdash \psi_h^{i_0}$ for each $h \in E$. Hence, by the induction hypothesis, $\psi_h^{i_0} \notin \widehat{X}^h$ for each $h \in E$. Recall that $\psi_h^{i_0} \in \Phi(Sig, \{h\})$ and $\widehat{X}^h$ is a maximal consistent subset of $\Phi(Sig, \{h\})$ for each $h \in E$. Thus, $\neg\psi_h^{i_0} \in \widehat{X}^h \subseteq M$ for each $h \in E$. Hence, $\bigwedge_{h\in E} \neg\psi_h^{i_0} \in M$ due to maximality of the set M. Then, $M \vdash \neg \bigvee_{h\in E} \psi_h^{i_0}$. Hence, $M \vdash \neg \bigwedge_i \bigvee_{h\in E} \psi_h^i$. Therefore, $M \vdash \psi$, by statement (22). The latter contradicts the choice of set M being a maximal consistent extension of set $X^e \cup \{\neg\psi\}$.

($\Leftarrow$) : Suppose that $\Box_e\psi \in X^e$. We will show that $r \Vdash \Box_e\psi$. Consider any run $\widehat{r} = \langle \widehat{X}^h, \{\widehat{f}^h_{u,\delta}\}_{u\in Inc(h),\delta\in\Delta(Sig)}\rangle_{h\in E}$ of the aggregated protocol $\mathcal{P}$ such that $\widehat{r} =_e r$. It suffices to prove that $\widehat{r} \Vdash \psi$.

Let $\bigwedge_i \bigvee_{h\in E} \psi_h^i$ be a conjunctive normal form of ψ such that $\psi_h^i \in \Phi(Sig, \{h\})$ for each $h \in E$. Then, for each i, the following statement can be proven using just the axioms of the propositional logic in language $\Phi(Sig)$

$$\vdash \psi \to \bigvee_{h\in E} \psi_h^i.$$

By Necessitation inference rule

$$\vdash \Box_e \left(\psi \to \bigvee_{h\in E} \psi_h^i \right).$$

By Distributivity axiom and Modus Ponens inference rule,

$$\vdash \Box_e \psi \to \Box_e \bigvee_{h \in E} \psi_h^i.$$

Thus, for each i, we have $\Box_e \bigvee_{h \in E} \psi_h^i \in X^e$ due to the assumption $\Box_e \psi \in X^e$ and the maximality of set X^e. Note that $\widehat{X}^e = X^e$ due to the assumption $\widehat{r} =_e r$. Hence, $\Box_e \bigvee_{h \in E} \psi_h^i \in \widehat{X}^e$. Let $\widehat{\delta}$ denote the formula $\bigvee_{h \in E} \psi_h^i$. Recall that $\widehat{r}$ is a run of protocol $\mathcal{P}$. Hence, by the definition of the aggregated protocol, tuple $\langle \widehat{X}^h, \{\widehat{f}^h_{u,\widehat{\delta}}\}_{u \in Inc(h)} \rangle_{h \in E}$ is a run of protocol $\mathcal{P}_E^{\widehat{\delta}}$, and so, by Lemma 12, it is a run of protocol $\mathcal{P}_{\{e\}}^{\widehat{\delta}}$. Then, by Theorem 1, there is an edge $h_0 \in E$ such that $\psi_{h_0}^i \in \widehat{X}^{h_0}$. Thus, by the induction hypothesis, $\widehat{r} \Vdash \psi_{h_0}^i$. Hence, $\widehat{r} \Vdash \bigvee_{h \in E} \psi_h^i$ for each i. Then, $\widehat{r} \Vdash \bigwedge_i \bigvee_{h \in E} \psi_h^i$. Therefore, $\widehat{r} \Vdash \psi$. ⊠

Theorem 5 (completeness) *For any signature Sig and any formula $\varphi \in \Phi(Sig)$, if $\nvdash \varphi$, then there exists a protocol $\mathcal{P}$ over Sig and a run r of $\mathcal{P}$ such that $r \nVdash \varphi$.*

Proof. Suppose that $\nvdash \varphi$. Let M be a maximal consistent subset of $\Phi(Sig)$ containing the formula $\neg\varphi$. Assume that $\bigwedge_i \bigvee_{e \in E} \varphi_e^i$ is the conjunctive normal form of the formula $\neg\varphi$ such that $\varphi_e^i \in \Phi(Sig, \{e\})$ for each i and each $e \in E$. Since $\neg\varphi \in M$, for each i there exists $e_i \in E$ such that $\varphi_{e_i}^i \in M$. By Theorem 2, for each $\delta \in \Delta(Sig)$, there exists a run $r^\delta = \langle X^h, \{f_u^h\}_{u \in Inc(h)} \rangle_{h \in E}$ of the canonical protocol $\mathcal{P}_E^\delta$ such that $X^h = M \cap \Phi(Sig, \{h\})$ for all $h \in E$. Thus, $\varphi_{e_i}^i \in X^{e_i}$ for each i. Consider tuple $r = \langle X^h, \{f^h_{u,\delta}\}_{u \in Inc(h), \delta \in \Delta(Sig)} \rangle_{h \in E}$. By the definition of the aggregated protocol, tuple r is a run of protocol $\mathcal{P}$. Hence, $r \vDash \varphi_{e_i}^i$ for each i, by Theorem 4. Therefore, $r \Vdash \bigwedge_i \bigvee_{e \in E} \varphi_e^i$ and so $r \Vdash \neg\varphi$. ⊠

8 Conclusion

In this article we have developed a formal modal logical framework for reasoning about information flow in communication networks with a fixed topological structure. Our main results are the soundness and the completeness of this logical system. At the core of the proof of the completeness is a well-known network flow protocol. A natural possible extension of this work is to develop a similar system for directed graphs that represent networks with one-way communication channels. Another possible extension is a distributed knowledge system with a modality $\Box_A$ in which the statement $\Box_A \varphi$ is interpreted as "any agent that eavesdrops on all channels in set A knows that φ is true".

Another possible direction for the future work is to develop logical frameworks for reasoning about information flow in more specialized settings. An example of such a setting is the influence flow in social networks. The influence in social networks is usually modeled by a relatively simple and very

specific form of "local conditions" such as those in commonly used threshold model [12, 13, 14, 15, 16, 17]. A logical framework for such a setting is likely to include more powerful version of Gateway axiom. The canonical network construction for the proof of the completeness presented in this article is very unlikely to be adoptable to a much more restricted interpretation of local conditions found in social network.

References

[1] Jeffrey Kane and Pavel Naumov. Epistemic logic for communication chains. In *14th conference on Theoretical Aspects of Rationality and Knowledge (TARK '13), January 2013, Chennai, India*, pages 131–137, 2013.

[2] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about knowledge*. MIT Press, Cambridge, MA, 1995.

[3] Reasoning about communication graphs.

[4] Jia Tao, Giora Slutzki, and Vasant Honavar. A conceptual framework for secrecy-preserving reasoning in knowledge bases. *ACM Trans. Comput. Logic*, 16(1):3:1–3:32, December 2014.

[5] 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.

[6] Sarah Holbrook and Pavel Naumov. Fault tolerance in belief formation networks. In Luis Fariñas del Cerro, Andreas Herzig, and Jérôme Mengin, editors, *JELIA*, volume 7519 of *Lecture Notes in Computer Science*, pages 267–280. Springer, 2012.

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

[8] 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.

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

[10] Jeffrey Kane and Pavel Naumov. The Ryōan-ji axiom for common knowledge on hypergraphs. *Synthese*, 191(14):3407–3426, 2014.

[11] Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. *Introduction to Algorithms*. MIT Press, 3rd edition, 2009.

[12] Thomas W Valente. Social network thresholds in the diffusion of innovations. *Social networks*, 18(1):69–89, 1996.

[13] Michael W Macy. Chains of cooperation: Threshold effects in collective action. *American Sociological Review*, pages 730–747, 1991.

[14] David Kempe, Jon Kleinberg, and Éva Tardos. Maximizing the spread of influence through a social network. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 137–146. ACM, 2003.

[15] Krzysztof R Apt and Evangelos Markakis. Social networks with competing products. *Fundamenta Informaticae*, 129(3):225–250, 2014.

[16] Mark Granovetter. Threshold models of collective behavior. *American journal of sociology*, pages 1420–1443, 1978.

[17] Thomas Schelling. *Micromotives and Macrobehavior*. Norton, 1978.