Correctness of the Chord Protocol

Article · September 2017

5 authors, including:

Some of the authors of this publication are also working on these related projects:

Biomechanical feedback in sports and rehabilitation View project

Biofeedback View project

CORRECTNESS OF THE CHORD PROTOCOL

BOJAN MARINKOVIĆ, ZORAN OGNJANOVIĆ, PAOLA GLAVAN, ANTON KOS,
AND ANTON UMEK

ABSTRACT. Internet of Things (IoT) can be seen as a cooperation of the various heterogeneous devices with limited performances, that participate in the same system. By they nature, these devices can be very distributed. The core of every IoT system is its discovery and control service. The Chord protocol is one of the first, simplest and most popular distributed protocol and can be use as a backbone of the discovery and control services of an IoT system. In this paper we prove the correctness of the Chord protocol using the logic of time and knowledge. We consider Chord actions that maintain ring topology with the additional assumption the nodes are not allowed to fail or leave.

Keywords: IoT, DHT, Chord, correctness, temporal logic, epistemic logic

1. INTRODUCTION

Internet of Things (IoT) paradigm can be defined as [1]: "The pervasive presence around us of a variety of things or objects which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals." In this framework the smart objects, which are connected by an Internet-like structure, are able to communicate and exchange information and to enable new forms of interaction among things and people [5]. The core of every IoT system consists of its discovery and control service. Usually, the objects which participate in an IoT system have limited computing power, memory and power supply. It is the common thing that various heterogeneous devices participate in the same IoT system. Ordinarily, these devices are highly distributed, so they participate in a distributed, i.e. Peer-to-Peer (P2P), system.

In a homogeneous decentralized P2P system [16], many nodes (peers) execute the same application, and have equal rights during that execution. They might join or leave system at any time. In such a framework processes are dynamically distributed to peers, with no centralized control. Thus, P2P systems have no inherent bottlenecks and can potentially scale very well. Also, those systems are resilient to failures, attacks, etc., since there are no nodes which perform the critical functions of the systems. The main applications of P2P-systems involve: file sharing, redundant storage, real-time media streaming, etc.

P2P systems are frequently implemented in a form of overlay networks [20], a structure that is totally independent of the underlying network that is actually connecting devices. Overlay networks represent a logical look on organization of the system resources. Some of the overlay networks are realized in the form of a Distributed Hash Tables (DHTs), which provides a lookup service similar to a hash table; $\langle key, value \rangle$ pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Note that *key* is

not used as a cryptographic notion, but (following the common practice in DHT-related papers) to represent identifiers of objects. Responsibility for maintaining the mapping from keys to values is distributed among the peers, in such a way that any change in the set of participants causes a minimal amount of disruption. The Chord protocol [17, 18, 19] is one of the first, simplest and most popular DHTs. The paper [17] which introduces Chord was recently awarded the SIGCOMM 2011 Test-of-Time Award.

Because of the simplicity and popularity of the Chord protocol, it was used for the realization of the discovery and/or control service of IoT systems described in [4, 5, 6, 15, 22].

As we mentioned above, the discovery and control services are cores of an IoT system, and because of that, in this paper we will prove the correctness of the Chord protocol using the logic of time and knowledge. We consider the case when the nodes are not allowed to fail or leave and concern Chord actions that maintain ring topology.

We are aware of only a few attempts to formally verify behavior of DHTs and particularly Chord [2, 3, 9, 10, 23]. We consider them below and compare with our approach.

The rest of the paper is organized in the following way: in Section 2 we consider other approaches for proving the correctness of the Chord protocol and clearly present the contributions of this paper; Section 3 presents a short description of the Chord protocol; in Section 4 we present a logical framework which will be used to prove the correctness of the maintenance of the ring topology of the Chord protocol with the respect of the fact that nodes are not allowed to departure the system after they join it; the proof is given in Section 5; we conclude with Section 6. In A we provide detailed proofs of most lemmas and theorems from the paper.

2. Related Work and Contributions

2.1. **Related Work.** The Chord protocol is introduced in [17, 18, 19]. The papers analyze the protocol, its performance and robustness under the assumption that the nodes and keys are randomly chosen, and give several theorems that involve the phrase *with high probability*, for example: "With high probability, the number of nodes that must be contacted to find a successor in a N-node network is $O(\log N)$".

The only statement in the papers [17, 18, 19] which avoids the mentioned phrase about high probability is Theorem IV.3. It corresponds to our Lemma 5 and proves that inconsistent states produced by executing several concurrent joins of the new nodes are transient, i.e., that after the last node joins the network will form a cycle. More general sequences of concurrent joining and leaving are considered in [10], where a lower bound of the rate at which nodes need to maintain the system such that it works correctly is given with high probability. In this paper we are not considering possible failures and leaves of the nodes. Our intention is that include this segment in our future work.

Anyway, it is not quite clear how to compare these two approaches (deterministic and probabilistic), but in our opinion there is benefit from both of them. One can argue that the probabilistic approach, i.e. providing lower bounds of probabilities, is useful to study robustness of protocols. On the other hand, it will be useful to describe sequences of actions leading to (un)stable states of Chord networks, to be able to analyze properties of systems that incorporate Chord and assume its

correctness, as it is the case with the discovery and/or control service of an IoT system.

In [9] the theory of stochastic processes is used to estimate the probability that a Chord network is in a particular state. In [2, 3] Chord's stabilization algorithm is modelled using the π-calculus and it's correctness is established by proving the equivalence of the corresponding specification and implementation. Possible departures of nodes from a network are not examined in this approach. In [23] the Alloy formal language is used to prove correctness of the pure join model. The same formalization present several counterexamples to correctness of Chord ring-maintenance in the general case.

In [7] a joint frame for reasoning about knowledge and linear time is presented, and the proof of weak completeness for a logic which combines expressions about knowledge with linear time is provided.

As we mentioned in Introduction using DHT or Chord in IoT domain is not a novelty [4, 5, 6, 15, 22]. In [4] authors proposed distributed control plane. They consider the problem how to deliver control messages to the devices that are in sleeping mode most of the time. Proposed DHT algorithm is Chord. The paper [5] introduce scalable, self-configuring and automated service and resource discovery mechanism based on structured DHT architecture. The article [6] presents comparison of the discovery service mechanisms in IoT domain, both traditional and distributed approaches. In [15] authors give the description of a novel discovery service for IoT which adopts DHT approach with multidimensional search domain. Authors of [22] presented discovery service for objects carrying RFID tags based on double Chord ring. In all these articles, the correctness of the Chord protocol was accepted for granted.

2.2. **Contributions.** In this paper we:

- provide axiomatization and prove the soundness, strong completeness and decidability of the logic of time and knowledge;
- describe the Chord protocol using the logic of time and knowledge;
- prove the correctness of the maintenance of the ring topology of the Chord protocol with the respect of the fact that nodes are not allowed to departure the system after they join it.

This work is motivated by the importance of the discovery and control service of an IoT system and the obvious fact that errors in concurrent systems are difficult to reproduce and find merely by program testing. This proof could be, also, the foundation for the formal proof created using a formal proof assistant (like, Coq or Isabelle/HOL).

3. Chord Protocol

The papers [17, 18, 19] introduce the Chord protocol and give the specification of it in C++-like pseudo-code. They present the correctness, performance and robustness of the Chord protocol. Here, we will provide a short description of it.

A number of nodes running the Chord protocol form a ring-shaped network. The main operation supported by Chord is mapping the given key onto a node using consistent hashing.The consistent hashing [8] provides load-balancing, i.e., every node receives roughly the same number of keys, and only a few keys are required to be moved when nodes join and leave the network. Chord networks are overlay

systems. Thus, each node in a network, that consists of N-nodes, needs "routing" information about only a few other nodes, $O(\log N)$, and resolves all lookups via $O(\log N)$ messages to other nodes.
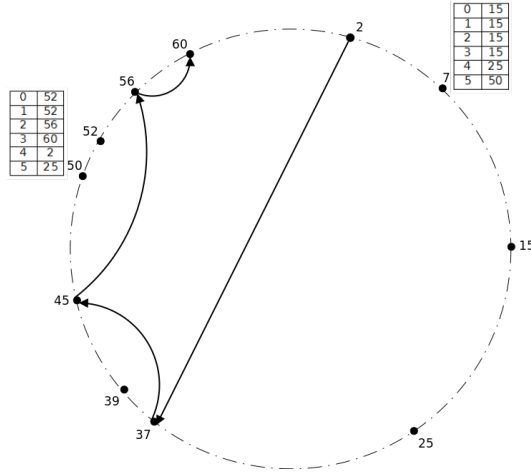

FIGURE 1. Chord lookup procedure

As it is shown, the Chord's stabilization algorithm maintains good lookup performance despite continuous failure and joining of nodes. When the network is not stable, i.e., the corresponding "routing" information is out of date since nodes join and leave arbitrarily, the performance degrades.

Identifiers are assigned to nodes and keys by the consistent hash function. The identifier for a node or a key, $hash(node)$ or $hash(key)$, is produced by hashing IP of the node, or the value of the key. The length of identifiers, for example m bits), must guarantee that the probability that two objects of the same type are assigned same identifiers is negligible. Identifiers are ordered in an identifier circle modulo 2^m. Then, the key k is assigned to the node such that $hash(node) = hash(key)$. If such a node does not exist, the key is assigned to the first node in the circle whose identifier is greater than $hash(key)$.

Every node possesses information on its current successor and predecessor nodes in the identifier circle. To accelerate the lookup procedure, a node also maintains routing information in the form of the so-called *Finger Table* with up to m entries. The ith entry in the table at the node n contains the identifier of the first node s that succeeds n by at least 2^{i-1} in the identifier circle, i.e., $s = successor(n+2^{i-1})$, where $1 \leqslant i \leqslant m$, and all arithmetic is preformed modulo 2^m. Figure 1 presents Finger tables of nodes n_7 and n_{50}.

One node can be aware of only a few other nodes in the system, like node n_7 from Figure 1 knows for the existence of only 3 other nodes. Some other can have different node identifier in almost every entry in its Finger table, like node n_{50} from Figure 1.

During the lookup procedure, a node forwards a query to the largest element of the Finger table which is smaller than the key used in the query, respect to the used arithmetics. In the example illustrated with Figure 1, if n_2 is looking for the responsible node for the key with identifier 57, it will forward this query to node

n_{37}, the closes node from its finger table. After, that this query will be forwarded to n_{45} and n_{56}, until it finally ends at n_{60}. The answer if n_{60} contains the key and respected value with identifier 57 will be returned to node that started query, in this case n_2.

The stabilization procedure implemented by Chord must guarantee that each node's finger table, predecessor and successor pointers are up to date. The procedure runs periodically in the background at each node. To increase robustness, each Chord node can create a successor list of size r, containing the node's first r successors.
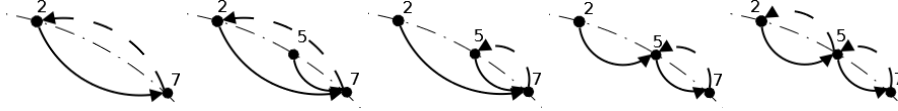

FIGURE 2. Stabilization during the joining of a new node

Figure 2 illustrates the process of joining of the node n_5 between nodes n_2 and n_7. As a first step n_5 will set its successor to n_7. During the stabilization process n_7 will set its predecessor to n_5, then n_2 will set its successor to n_5 and, finally, n_5 will set its predecessor to n_2.

Beside the mapping of keys onto the set of nodes, the only other operations realized by Chord are adding a node to network or removing a node from a network. When a node n joins an existing network, certain keys previously assigned to n's successor now become assigned to n. When a node n leaves the network regularly, it notifies its predecessor and successor and reassigns all of its keys to the successor.

4. Logic of Time and Knowledge

As we mentioned in the previous Section, a system which runs the Chord protocol is a dynamic multi-agent system, where every agent has it own partial view of the surrounding environment. To be able to reason about such system, we need to introduce a framework for formal description of changes of the knowledge of an agent during the time. In this section we present logic of time and knowledge.

4.1. **Syntax.**

Let $\mathbb{N}$ be the set of non-negative integers. We denote $\mathbf{N} = \{n_0, \ldots n_{m-1}\}$, where $m \in \mathbb{N}$, and then let $\mathbf{N_1} = \mathbf{N} \cup \{u\}$ be the set of propositional variables.

The set *For* of all formulas is the smallest superset of $\mathbf{N_1}$ which is closed under the following formation rules:

- $\langle \phi, \psi \rangle \mapsto \phi * \psi$ where $* \in \{\succ, \prec\}$ and $\phi, \psi \in \mathbf{N_1}$,
- $\langle \phi, \psi, \varphi \rangle \mapsto \phi \mathtt{M} \langle \psi, \varphi \rangle$ where $\phi, \psi, \varphi \in \mathbf{N}$,
- $\psi \mapsto *\psi$ where $* \in \{\neg, \bigcirc, \bullet, \mathtt{K}_i\}$,
- $\langle \phi, \psi \rangle \mapsto \phi * \psi$ where $* \in \{\wedge, \mathtt{U}, \mathtt{S}\}$.

The operators $\succ$ and $\prec$ represent relations successor and predecessor of a node. The tip of the "arrow" is pointing to the node with "greater" identifier, with respect to the ordering determined by the ring shaped Chord network. We will use abbreviation $n_i \succ^2 n_k$ for $n_i, n_k \in N$ iff there is an $n_j \in N$ such that $n_i \succ n_j$ and $n_j \succ n_k$, and $n_k \prec^2 n_i$ for $n_i, n_k \in N$ iff there is an $n_j \in N$ such that $n_k \prec n_j$ and

$n_j \prec n_i$. Similarly, we can define $n_j \succ^i n_k$, as well as $n_j \prec^i n_k$ for $n_j, n_k \in N$ and $0 < i < m$. Figure 3 illustrates the relations $\succ$, $\prec$ (Figure 3a) and $\succ^i$ (Figure 3b).

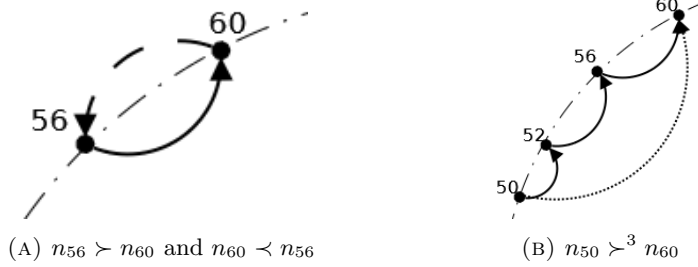(A) $n_{56} \succ n_{60}$ and $n_{60} \prec n_{56}$ (B) $n_{50} \succ^3 n_{60}$

FIGURE 3. Examples of $\succ$, $\prec$ and $\succ^i$

The operators $\neg$ and $\wedge$ represent standard logical negation and conjunction. The operators $\bigcirc$, $\bullet$, $\mathtt{U}$ and $\mathtt{S}$ are standard temporal operators Next, Previous, Until and Since. The operator $\mathtt{K}_i$ represents the knowledge of the agent i.

The remaining logical and temporal connectivities $\vee$, $\rightarrow$, $\leftrightarrow$, $\mathtt{F}$, $\mathtt{G}$, $\mathtt{P}$, $\mathtt{H}$ are defined in the usual way:

- $\phi \vee \psi =_{def} \neg(\neg\phi \wedge \neg\psi)$,
- $\phi \rightarrow \psi =_{def} \neg\phi \vee \psi$,
- $\phi \leftrightarrow \psi =_{def} (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$,
- $\mathtt{F}\psi =_{def} (\psi \rightarrow \psi)\mathtt{U}\psi$,
- $\mathtt{G}\psi =_{def} \neg\mathtt{F}\neg\psi$,
- $\mathtt{P}\psi =_{def} (\psi \rightarrow \psi)\mathtt{S}\psi$,
- $\mathtt{H}\psi =_{def} \neg\mathtt{P}\neg\psi$,
- $\bigcirc^0\psi =_{def} \psi; \bigcirc^{n+1}\psi = \bigcirc\bigcirc^n\psi, n \geqslant 0$,
- $\bullet^0\psi =_{def} \psi; \bullet^{n+1}\psi = \bullet\bullet^n\psi, n \geqslant 0$.

Nonempty sets of formulas will be called theories.

In this paper we will consider time flow which is isomorphic to the set $\mathbb{N}$. We will take into account both future and past. Since we are dealing with a multi-agent system were agents have to share knowledge among them the obvious choice is to use the logic of time and knowledge, similarly like in [7].

We define $\Phi_k(\tau, (\theta_j)_{j\in\mathbb{N}})$ as a k-nested implication for the knowledge of an agent i and for formula τ based on the sequence of formulas $(\theta_j)_{j\in\mathbb{N}}$ in the following recursive way:

$$\Phi_0(\tau, (\theta_j)_{j\in\mathbb{N}}) = \theta_0 \rightarrow \tau,$$

$$\Phi_{k+1}(\tau, (\theta_j)_{j\in\mathbb{N}}) = \theta_{k+1} \rightarrow \mathtt{K}_i\Phi_k(\tau, (\theta_j)_{j\in\mathbb{N}}), \text{ for some } 0 \leqslant i < m.$$

For example, $\Phi_3(\tau, (\theta_j)_{j\in\mathbb{N}}) = \theta_3 \rightarrow \mathtt{K}_i(\theta_2 \rightarrow \mathtt{K}_j(\theta_1 \rightarrow \mathtt{K}_i(\theta_0 \rightarrow \tau))), 0 \leqslant i, j < m$. This definition follows the form of probabilistic k-nested implication presented in [12, 21].

4.2. Semantics.

We will defined models as Kripke's structures.

Definition 1. *A model $\mathcal{M}$ is any tuple $\langle R, W, \pi, \mathcal{K} \rangle$ such that*

- *Set of all possible runs R:*

- $r^j = \{\langle x_0^{j,t}, \dots, x_{m-1}^{j,t}\rangle | t = 0, 1, 2 \dots\}, x_i^{j,t} \in \{\top, \bot\},$
- $R = \{r^j; j = 0, 1, \dots\},$
- *Restriction: if* $x_i^{j,t} = \top$ *then* $x_i^{j,t+1} = \top$
- *W set of time instances (the time flow isomorphic to $\mathbb{N}$),*
- $\pi : R \times W \times \mathbf{N_1} \to \{\top, \bot\}$ *truth assignment, such that:*
  - $\pi(r^j, t, n_l) = x_l^{j,t},$
  - $\pi(r^j, t, u) = \top$
- $\mathcal{K}$ *possibility relations:* $\mathcal{K}_i \subset (R \times W)^2$: $\langle r^j, t\rangle \mathcal{K}_i \langle r^{j'}, t'\rangle$ *iff* $x_i^{j,t} = x_i^{j',t'}$.

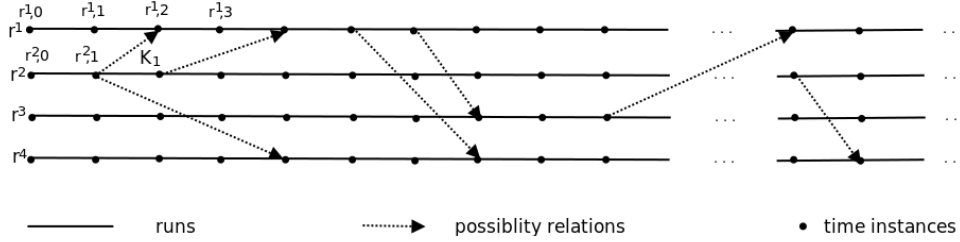FIGURE 4. Kripke model

Figure 4 illustrates a Kripke model which contains the runs r^1, r^2, r^3, r^4, where r^1 is the sequence of $\langle r^1, 0\rangle$, $\langle r^1, 1\rangle$, $\langle r^1, 2\rangle$, etc. and similarly for other runs. In this model, for example $\langle r^2, 1\rangle \mathcal{K}_1 \langle r^2, 2\rangle$, etc.

An $n_i \in \mathbf{N}$ is *true* in the time instant t in the run r^j ($x_i^{j,t} = \top$) if the Chord network node i is active in the corresponding realization of the network. We define the set of propositional variables which represent the active nodes of Chord network as $\mathbf{N_a} = \{n_i | n_i \text{ is } true\}$. For $n_i, n_j, n_k \in \mathbf{N}$ we define the relation $\mathtt{M}$ which represents the fact that n_i is the member of the ring interval $(n_j, n_k]$ as: $n_i \mathtt{M} \langle n_j, n_k\rangle$ is *true* iff

- $j = k,$
- $j < k$ and $j < i \leqslant k,$
- $k < j$ and $\neg(k < i \leqslant j).$

4.3. **Satisfiability relation.** A formula is satisfiable if it is possible to find an interpretation, i.e. model, that makes that formula true.

Definition 2. *Let* $\mathcal{M} = \langle R, W, \pi, \mathcal{K}\rangle$ *be any model. The satisfiability relation* $\models$ *(formula α is satisfied in a time instance of a run $R \times W \models \alpha$) is defined recursively as follows:*

1. $\langle r^j, t\rangle \models n$ *iff* $\pi(r^j, t, n) = true, n \in \mathbf{N_1}$
2. $\langle r^j, t\rangle \models \alpha \wedge \beta$ *iff* $\langle r^j, t\rangle \models \alpha$ *and* $\langle r^j, t\rangle \models \beta$
3. $\langle r^j, t\rangle \models \neg\alpha$ *iff not* $\langle r^j, t\rangle \models \alpha$ *(* $\langle r^j, t\rangle \not\models \alpha$ *)*
4. $\langle r^j, t\rangle \models \bigcirc\alpha$ *iff* $\langle r^j, t+1\rangle \models \alpha$
5. $\langle r^j, t+1\rangle \models \bullet\alpha$ *iff* $\langle r^j, t\rangle \models \alpha$
6. $\langle r^j, 0\rangle \models \bullet\alpha$
7. $\langle r^j, t\rangle \models \alpha\mathtt{U}\beta$ *iff there is a $i \geqslant 0$ such that $\langle r^j, t+i\rangle \models \beta$, and for every k, such that $0 \leqslant k < i$, $\langle r^j, t+k\rangle \models \alpha$*
8. $\langle r^j, t\rangle \models \alpha\mathtt{S}\beta$ *iff there is a $0 \leqslant i \leqslant t$ such that $\langle r^j, t-i\rangle \models \beta$, and for every k, such that $0 \leqslant k < i$, $\langle r^j, t-k\rangle \models \alpha$*

(9) $\langle r^j, t \rangle \models \mathrm{K}_i \alpha$ *iff* $\langle r^{j'}, t' \rangle \models \alpha$ *for all* $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$

(10) $\langle r^j, t \rangle \models n_i \succ n_j$ *iff*

    (a) $i = j$ *and* $\langle r^j, t \rangle \models n_i \wedge \mathrm{K}_i(\bigwedge_{n_j \in \mathbf{N} \setminus \{n_i\}} \neg n_j)$

    (b) $i < j \leqslant m$ *and* $\langle r^j, t \rangle \models n_i \wedge n_j \wedge \mathrm{K}_i(\bigwedge_{k=i+1}^{j-1} \neg n_k) \wedge \mathrm{K}_i n_j$

    (c) $j < i < m$ *and* $\langle r^j, t \rangle \models n_i \wedge n_j \wedge \mathrm{K}_i(\bigwedge_{k=i+1}^{m} \neg n_k) \wedge \mathrm{K}_i(\bigwedge_{k=1}^{j-1} \neg n_k) \wedge \mathrm{K}_i n_j$

    (d) $j < i$ *and* $i = m$ *and* $\langle r^j, t \rangle \models n_i \wedge n_j \wedge \mathrm{K}_i(\bigwedge_{k=1}^{j-1} \neg n_k) \wedge \mathrm{K}_i n_j$

(11) $\langle r^j, t \rangle \models n_j \prec n_i$ *iff*

    (a) $i = j$, $t \neq 0$ *and* $\langle r^j, t \rangle \models n_i \wedge \mathrm{K}_i(\bigwedge_{n_k \in \mathbf{N} \setminus \{n_i\}} \neg n_k)$

    (b) $i < j \leqslant m$ *and* $\langle r^j, t \rangle \models n_i \wedge n_j \wedge \mathrm{K}_i(\bigwedge_{k=i+1}^{j-1} \neg n_k) \wedge \mathrm{K}_i n_j$

    (c) $j < i < m$ *and* $\langle r^j, t \rangle \models n_i \wedge n_j \wedge \mathrm{K}_i(\bigwedge_{k=i+1}^{m} \neg n_k) \wedge \mathrm{K}_i(\bigwedge_{k=1}^{j-1} \neg n_k) \wedge \mathrm{K}_i n_j$

    (d) $j < i$ *and* $i = m$ *and* $\langle r^j, t \rangle \models n_i \wedge n_j \wedge \mathrm{K}_i(\bigwedge_{k=1}^{j-1} \neg n_k) \wedge \mathrm{K}_i n_j$

    (e) $n_i = u$ *and* $\langle r^j, t \rangle \models \neg n_j \vee (n_j \wedge (\bullet(\neg \mathrm{K}_k(n_k \succ n_j))))$

4.4. **Axiomatization.**

The axioms of our theory are all instances of the following schemata:

A1   instances of tautologies

AT1 $\neg \bigcirc \alpha \leftrightarrow \bigcirc \neg \alpha$

AT2 $\bigcirc(\alpha \to \beta) \to (\bigcirc \alpha \to \bigcirc \beta)$

AT3 $\alpha \mathrm{U} \beta \leftrightarrow \beta \vee (\alpha \wedge \bigcirc(\alpha \mathrm{U} \beta))$

AT4 $\alpha \mathrm{U} \beta \to \mathrm{F} \beta$

AT5 $\bullet(\alpha \to \beta) \to (\bullet \alpha \to \bullet \beta)$

AT6 $\alpha \mathrm{S} \beta \leftrightarrow (\bullet \bot \wedge \beta) \vee (\neg \bullet \bot \wedge (\beta \vee (\alpha \wedge \bullet(\alpha \mathrm{S} \beta))))$

AT7 $\alpha \mathrm{S} \beta \to \mathrm{P} \beta$

AT8 $\alpha \leftrightarrow \bigcirc \bullet \alpha$

AT9 $\alpha \leftrightarrow \bullet \bot \vee (\bullet \neg \bot \wedge \bullet \bigcirc \alpha)$

AT10 $\mathrm{P} \bot$

AT11 $n_i \to \mathrm{G} n_i$

AK1 $\varphi \leftrightarrow \mathrm{K}_i \varphi$, $\varphi = \pm n_i$

AK2 $(\mathrm{K}_i \alpha \wedge \mathrm{K}_i(\alpha \to \beta)) \to \mathrm{K}_i \beta$

AK3 $\mathrm{K}_i \alpha \to \alpha$

AK4 $\mathrm{K}_i \alpha \to \mathrm{K}_i \mathrm{K}_i \alpha$

AK5 $\neg \mathrm{K}_i \alpha \to \mathrm{K}_i \neg \mathrm{K}_i \alpha$

AS1 $n_i \succ n_j \to \bigwedge_{n_k \in \mathbf{N_1} \setminus \{n_j\}} \neg(n_i \succ n_k), n_i, n_j \in \mathbf{N}$

AS2 $n_i \prec n_j \to \bigwedge_{n_k \in \mathbf{N_1} \setminus \{n_j\}} \neg(n_i \prec n_k), n_i, n_j \in \mathbf{N}$

AS3 $n_i \prec n_j \to \bigwedge_{n_k \in \mathbf{N_1} \setminus \{n_i\}} \neg(n_k \prec n_j), n_i, n_j \in \mathbf{N}$

AS4 $n_i \prec n_j \to n_j \succ n_i, n_i, n_j \in \mathbf{N}$

AS5 $n_i \succ n_j \to \mathrm{K}_i(n_i \succ n_j), n_i, n_j \in \mathbf{N}$

AS6 $((n_i \succ n_j) \wedge n_k \mathrm{M} \langle n_i, n_j \rangle \wedge \bigcirc(\neg \mathrm{K}_i n_k)) \to \bigcirc(n_i \succ n_j), n_i, n_j, n_k \in \mathbf{N}$

Inference rules:

MP   from α and $\alpha \to \beta$ infer β

RTN   from α infer $\bigcirc \alpha$

RKN   from α infer $\mathrm{K}_i \alpha$

RI   from $\Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1} \beta), (\theta_j)_{j \in \mathbb{N}})$ for all $i \geqslant 0$ infer $\Phi_k(\neg(\alpha \mathrm{U} \beta), (\theta_j)_{j \in \mathbb{N}})$

[AT1 – AT10] are standard axioms of the linear temporal logic. [AT11] takes into consideration specificity of our model and the restriction that when some n_i become $\top$, then it will never be $\bot$. While [AK1] takes into consideration specificity of our model, [AK2 – AK5] are standard axioms for reasoning about knowledge.

[AS1] says that a node can have only one successor. [AS2] says that a node can be predecessor of only one node. [AS3] says that a node can have only one predecessor. [AS4] says that if a node is predecessor of some other node, that other node has to be its successor. [AS5] says that if a node n_i has the successor n_j than it knows that n_j is its successor. [AS6] says when the current successor will be the successor in the next time instance.

[MP] is modus ponens, [RTN] and [RKN] resemble necessitations,and [RI] is the infinitary inference rule that characterize the Until operator.

4.5. **Soundness, Completeness and Decidability.**

In this part we will prove that our system is sound, complete and decidable. Informally speaking, the soundness means that we cannot prove anything that is wrong, the completeness means that we can prove everything that is right, and the decidability means that there is an effective method for determining whether arbitrary formula is a theorem of our logical system.

The inference relation $\vdash$ is defined as follows:

Definition 3. *We say that α is syntactical consequence of a set of formulas T (or that α is deducible or derivable from T) and write $T \vdash \alpha$ iff there exists an at most countably infinite sequence of $\alpha_0, \ldots, \alpha_\phi$ such that $\alpha_\phi = \alpha$ and for all $\beta \leqslant \phi$, α_β is an instance of some axiom, $\alpha_\beta \in T$, or α_β can be obtained from some previous members of the sequence by an application of some inference rule. A formula α is a theorem ($\vdash \alpha$) if it is deducible from the empty set. The rules [RTN] and [RKN] can be applied only to theorems.*

Definition 4. *A set T is inconsistent iff $T \vdash \perp$, otherwise it is consistent. A set T of formulae is maximal if for every formula α either $\alpha \in T$ or $\neg\alpha \in T$. A set T is deductively closed if for every formula α, if $T \vdash \alpha$, then $\alpha \in T$.*

Theorem 1. *[Soundness] $\vdash \alpha$ implies $\models \alpha$.*

Theorem 2. *Every consistent set of formulas T can be extended to a maximal consistent set T^*.*

Canonical structure. We define a special, so called canonical structure $\mathbb{M}^* = \langle R, W, \pi, \mathcal{K} \rangle$. Let $\mathcal{T}$ be the set of all maximal consistent sets. Let $T \in \mathcal{T}$. We define a run inductively as: $T_j^0 = T$, and $T_j^t = \{\alpha : \bigcirc\alpha \in T_j^{t-1}\}, t > 0$.

We denote:

- $r_t^j = \langle x_0^{j,t}, \ldots, x_{m-1}^{j,t} \rangle$, where $x_l^{j,t} = \top$ if $n_l \in T_j^t$, and $x_l^{j,t} = \perp$ otherwise,
- $r^j = \langle x_0^{j,t}, \ldots, x_{m-1}^{j,t} \rangle, t = 0, 1 \ldots$,
- $R = \{r^j\}$.

Also:

- $\pi(r^j, t, n_l) = x_l^{j,t}$,
- $\langle r^j, t \rangle \mathcal{K}_i \langle r^{j'}, t' \rangle$ iff $n_i \in T_j^t \Leftrightarrow n_i \in T_{j'}^{t'}$.

Theorem 3. *[Strong completeness] Every consistent set of formulas is satisfiable.*

Theorem 4. *$T \models \psi \leftrightarrow T \vdash \psi$.*

Theorem 5 (Decidability theorem). *Checking the satisfiability of a given formula ψ is decidable.*

Proof. In every run at some time instance we will have stationary situation (at least when all possible nodes join the system). Since we do not allow leaving of the nodes, we can apply the ideas from [11, 13, 14] to prove the decidability problem. □

5. Proof of the Correctness

To be able to prove the correctness of the Chord protocol we need to introduce the following definitions:

Definition 5 (Stable pair). *The pair of nodes $\langle n_k, n_l \rangle$ is stable (we denote it with $n_k \between n_l$) at $\langle r^{j'}, t \rangle$ iff $(n_l \succ^{m_1} n_k) \wedge (\bigwedge_{1 \leqslant j \leqslant m_1} \mathrm{K}_{i_j}(n_{i_j} \succ n_{i_{j+1}})) \wedge (n_l \prec^{m_1} n_k) \wedge (\bigwedge_{1 \leqslant j \leqslant m_1} \mathrm{K}_{i_{j+1}}(n_{i_{j+1}} \prec n_{i_j}))$, where $n_{i_j} \in \mathbf{N_a}$.*

Definition 6 (Stable network). *Network is stable (we denote it with $\odot$) at $\langle r^j, t \rangle$ iff $n_k \between n_k$ for all $n_k \in \mathbf{N_a}$.*

We introduce an integer constant $f \in \mathbb{N}$, that will represent fairness condition, i.e. it guarantees that a formula will be realized at maximum of f time instances.

The processes of the Chord network can be describe with:

ρ_S: $\mathrm{H}(\bigwedge_{n_j \in \mathbf{N}} \neg n_j) \wedge n_i \wedge (\bigwedge_{n_j \in \mathbf{N} \setminus \{n_i\}} \neg n_j) \wedge \mathrm{K}_i(n_i \succ n_i) \wedge \mathrm{K}_i(n_i \prec u)$ for one $n_i \in \mathbf{N}$,

$\rho_{J,i}$: $\bullet(\neg n_i) \wedge n_i \wedge \bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_i(n_i \succ n_j) \wedge \mathrm{K}_i(n_i \prec u)$, $n_j \in \mathbf{N_a}, n_i \in \mathbf{N}, i \neq j$,

$\rho_{S1,i,j}$: $(\mathrm{K}_i(n_i \succ n_j) \wedge \mathrm{K}_j(n_j \prec u)) \vee (\mathrm{K}_i(n_i \succ n_j) \wedge \mathrm{K}_j(n_j \prec n_k) \wedge n_i \mathrm{M} \langle n_k, n_j \rangle) \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_j(n_j \prec n_i)$, $n_i, n_k, n_j \in \mathbf{N_a}$,

$\rho_{S2,i,j}$: $\mathrm{K}_i(n_i \succ n_j) \wedge \mathrm{K}_j(n_j \prec n_k) \wedge n_k \mathrm{M} \langle n_i, n_j \rangle \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_i(n_i \succ n_k)$, $n_i, n_k, n_j \in \mathbf{N_a}$.

$[\rho_S]$ describes the start of the new Chord network. $[\rho_{J,i}]$ represents the situation when a new node n_i is joining the existing Chord network, while $[\rho_{S1,i,j}]$ and $[\rho_{S2,i,j}]$ characterize stabilization processes in one Chord network.

To be able to describe periodicity of the stabilization process, we introduce the following axioms:

ACF1: $n_i \wedge \rho_S \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S1,i,j}$, $n_i \in \mathbf{N_a}$,

ACF2: $n_i \wedge \rho_S \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S2,i,j}$, $n_i \in \mathbf{N_a}$,

ACF3: $n_i \wedge \rho_{J,i} \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S1,i,j}$, $n_i \in \mathbf{N_a}$,

ACF4: $n_i \wedge \rho_{J,i} \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S2,i,j}$, $n_i \in \mathbf{N_a}$,

ACF5: $n_i \wedge \rho_{S1,i,k} \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S1,i,j}$, $n_i \in \mathbf{N_a}, k \in \{0, m-1\}$,

ACF6: $n_i \wedge \rho_{S2,i,k} \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S2,i,j}$, $n_i \in \mathbf{N_a}, k \in \{0, m-1\}$.

The correctness of the Chord protocol can be proved by the following Lemmas and Theorem.

Lemma 1. *Let a new node start a new Chord network. Then, there is a finite period of time after the network will be stable again, if no other nodes are trying to join in the meanwhile.*

Lemma 2. *Let a new node join a stable Chord network which consists of only one node. Then, there is a finite period of time after the network will be stable again, if no other nodes are trying to join in the meanwhile.*

Proofs of Lemmas 1 and 2 are similar like the proof of Lemma 3.

Lemma 3. *Let a peer join a Chord network, between two nodes which constitute a stable pair, such that the second node is the successor of the first node. Then, there is a finite period of time after the starting pair will be stable again, if no other nodes are trying to join in the meanwhile.*

Lemma 4. *Let a peer join a Chord network, between two nodes which constitute a stable pair. Then, there is a finite period of time after the starting pair will be stable again, if no other nodes are trying to join in the meanwhile.*

Proof. Since one new node is joining the stable pair, we can choose two nodes which are each others successor and predecessor and the new node is joining between them, so we can apply Lemma 3. □

Lemma 5. *Let a Chord network contain a stable pair. If a sequence of nodes join between the nodes that constitute this stable pair, then there is a finite period of time after the starting pair will be stable again.*

Proof. If we assume that all nodes that want to join the network have different successors, by Lemma 4 the statement holds.

If this is not the case, we can assume that $n_i \pitchfork n_k$ and that set of nodes $j_1, j_2, \ldots$, such that $i \leqslant \ldots \leqslant j_2 \leqslant j_1 \leqslant k$, are joining this stable pair. Then, we can apply Lemma 4 on the tuples $\langle i, j_1, k \rangle$, $\langle i, j_2, j_1 \rangle$, $\ldots$. This process will have as a result $n_i \pitchfork n_k$, again. □

Theorem 6. $\vdash \neg \circledcirc \to \mathsf{F} \circledcirc$

Proof. The unstable state can be reached only by joining of the new nodes, and, since we do not allow node failures, this theorem is the corollary of Lemmas 1 – 5. □

6. Conclusion

The core part of the every IoT system are its discovery and control services. In the distributed environment, these services can be realized using the Chord protocol.

In this paper we provide the axiomatization and prove the soundness, strong completeness and decidability of the logic of time and knowledge. Using this framework, we prove the correctness of the maintenance of the ring topology of the Chord protocol with the respect of the fact that nodes are not allowed to departure the system after they join it.

Our plan is to continue our research to prove the correctness in the general case. Also, one of the possible directions for further work is to apply the similar technique to describe other DHT protocols and other cloud processes.

Another challenge could be to verify the given proof in one of the formal proof assistants (e.g., Coq, Isabelle/HOL). It might also produce a certified program implementation from the proof of correctness.

Appendix A. Proofs

Theorem 1. *[Soundness]* $\vdash \alpha$ *implies* $\models \alpha$.

Proof.   AT1 $\neg \bigcirc \alpha \leftrightarrow \bigcirc \neg \alpha$

$\langle r^j, t \rangle \models \neg \bigcirc \alpha$ iff $\langle r^j, t \rangle \not\models \bigcirc \alpha$ iff

$\langle r^j, t+1 \rangle \not\models \alpha$ iff $\langle r^j, t+1 \rangle \models \neg \alpha$ iff

$\langle r^j, t \rangle \models \bigcirc \neg \alpha$

   AT2 $\bigcirc(\alpha \rightarrow \beta) \rightarrow (\bigcirc \alpha \rightarrow \bigcirc \beta)$

$\langle r^j, t \rangle \models \bigcirc(\alpha \rightarrow \beta)$ iff $\langle r^j, t+1 \rangle \models \alpha \rightarrow \beta$ iff $\langle r^j, t+1 \rangle \models \neg \alpha \vee \beta$ iff

$\langle r^j, t+1 \rangle \models \neg \alpha$ or $\langle r, t+1 \rangle \models \beta$ iff

$\langle r^j, t \rangle \models \neg \bigcirc \alpha$ or $\langle r, t \rangle \models \bigcirc \beta$ if

$\langle r^j, t \rangle \models \neg \bigcirc \alpha \vee \bigcirc \beta$ iff

$\langle r^j, t \rangle \models \bigcirc \alpha \rightarrow \bigcirc \beta$

   AT3 $\alpha \mathtt{U} \beta \leftrightarrow \beta \vee (\alpha \wedge \bigcirc(\alpha \mathtt{U} \beta))$

$\langle r^j, t \rangle \models \alpha \mathtt{U} \beta$ iff

$\langle r^j, t+i \rangle \models \beta, i \geqslant 0$ and $\langle r^j, t+k \rangle \models \alpha$ and $0 \leqslant k < i$ iff

$\langle r^j, t \rangle \models \beta$ or $\langle r^j, t+i \rangle \models \beta, i > 0$ and $\langle r^j, t+k \rangle \models \alpha$ and $0 \leqslant k < i$ iff

$\langle r^j, t \rangle \models \beta$ or $\langle r^j, t \rangle \models \alpha$ and $\langle r, t+i \rangle \models \beta$ and $\langle r^j, t+k \rangle \models \alpha$ and $1 \leqslant k < i$ iff

$\langle r^j, t \rangle \models \beta$ or $\langle r^j, t \rangle \models \alpha$ and $\langle r, t+i-1 \rangle \models \beta$ and $\langle r, t+k-1 \rangle \models \alpha$ and $0 \leqslant k-1 < i-1$ iff

$\langle r^j, t \rangle \models \beta$ or $\langle r^j, t \rangle \models \alpha$ and $\langle r^j, t \rangle \models \bigcirc(\alpha \mathtt{U} \beta)$ iff

$\langle r^j, t \rangle \models \beta \vee (\alpha \wedge \bigcirc(\alpha \mathtt{U} \beta))$

   AT4 $\alpha \mathtt{U} \beta \rightarrow \mathtt{F} \beta$

$\langle r^j, t \rangle \models \alpha \mathtt{U} \beta$ iff

$\langle r^j, t+i \rangle \models \beta, i \geqslant 0$ and $\langle r, t+k \rangle \models \alpha$ and $0 \leqslant k < i$ if

$\langle r^j, t+i \rangle \models \beta$ and exists $i \geqslant 0$ iff

$\langle r^j, t \rangle \models \mathtt{F} \beta$

[AT5 – AT7] similarly like [AT2 – AT4] regarding the sub-case $\langle r^j, 0 \rangle$.

   AT8 $\alpha \leftrightarrow \bigcirc \bullet \alpha$

$\langle r^j, t \rangle \models \alpha$ iff $\langle r^j, t+1 \rangle \models \bullet \alpha$ iff $\langle r^j, t \rangle \models \bigcirc \bullet \alpha$

[AT9] similarly like [AT8], regarding the sub-case $\langle r^j, 0 \rangle$.

AT10 $\mathtt{P} \bot$

$\langle r^j, t \rangle \models \mathtt{P} \bot$ iff $\langle r^j, 0 \rangle \models \bullet \bot$

AT11 $n_i \rightarrow \mathtt{G} n_i$

Because of the restriction if $x_i^{j,t} = \top$ then $x_i^{j,t+1} = \top$.

   AK1 $\varphi \leftrightarrow \mathtt{K}_i \varphi$, $\varphi = \pm n_i$

$\langle r^j, t \rangle \models \varphi$ iff

$\langle r^{j'}, t' \rangle \models \varphi$ and all $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ iff

$\langle r^j, t \rangle \models \mathtt{K}_i \varphi$

   AK2 $(\mathtt{K}_i \alpha \wedge \mathtt{K}_i(\alpha \rightarrow \beta)) \rightarrow \mathtt{K}_i \beta$

$\langle r^j, t \rangle \models \mathtt{K}_i \alpha \wedge \mathtt{K}_i(\alpha \rightarrow \beta)$ iff

$\langle r^j, t \rangle \models \mathtt{K}_i \alpha$ and $\langle r^j, t \rangle \models \mathtt{K}_i(\alpha \rightarrow \beta)$ iff

$\langle r^{j'}, t' \rangle \models \alpha$ for all $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ and $\langle r', t' \rangle \models \alpha \rightarrow \beta$ for all $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ iff

$\langle r^{j'}, t' \rangle \models \alpha \wedge (\alpha \rightarrow \beta)$ for all $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ if

$\langle r^{j'}, t' \rangle \models \beta$ for all $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ iff

$\langle r^j, t \rangle \models \mathtt{K}_i \beta$

   AK3 $\mathtt{K}_i \alpha \rightarrow \alpha$

$\langle r^j, t \rangle \models \mathtt{K}_i \alpha$ iff

$\langle r^{j'}, t' \rangle \models \alpha$ and $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ then

$\langle r^j, t \rangle \models \alpha$

AK4 $\mathsf{K}_i \alpha \rightarrow \mathsf{K}_i \mathsf{K}_i \alpha$

$\langle r^j, t \rangle \models \mathsf{K}_i \alpha$ iff

$\langle r^{j'}, t' \rangle \models \alpha$ and $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ then

$\langle r^{j''}, t'' \rangle \models \alpha$ and $\langle r^{j''}, t'' \rangle \in \mathcal{K}_i(\langle r^{j'}, t' \rangle)$ iff

$\langle r^{j'}, t' \rangle \models \mathsf{K}_i \alpha$ and $\langle r^{j'}, t' \rangle \in \mathcal{K}_i(\langle r^j, t \rangle)$ iff

$\langle r^j, t \rangle \models \mathsf{K}_i \mathsf{K}_i \alpha$

AK5 $\neg \mathsf{K}_i \alpha \rightarrow \mathsf{K}_i \neg \mathsf{K}_i \alpha$

Similarly like [AK4]

AS1 $n_i \succ n_j \rightarrow \bigwedge_{n_k \in \mathbf{N_1} \setminus \{n_j\}} \neg(n_i \succ n_k), n_i, n_j \in \mathbf{N}$

Let $\langle r^l, t \rangle \models n_i \succ n_j$.

If $i = j$, by the definition of $n_i \succ n_i$ we have that

$$\langle r^l, t \rangle \models n_i \wedge \mathsf{K}_i(\bigwedge_{n_j \in \mathbf{N} \setminus \{n_i\}} \neg n_j),$$

and by [AK3] and [A1] we have that

$$\langle r^l, t \rangle \models \bigwedge_{n_j \in \mathbf{N} \setminus \{n_i\}} \neg n_j$$

so, there is no candidate $n_k \in \mathbf{N_1} \setminus \{n_i\}$ such that $n_i \succ n_k$.

Let $i \neq j$ and let

$$\langle r^l, t \rangle \models n_i \succ n_{j'}$$

and $i < j' < j \leqslant m$. Then, by the definition of $\succ$ relation we have

$$n_i \succ n_{j'} \rightarrow \mathsf{K}_i n_{j'},$$

and

$$n_i \succ n_j \rightarrow \mathsf{K}_i\left(\bigwedge_{k=i+1}^{j-1} \neg n_k\right).$$

Last two facts are in contradiction.

Similarly in all other cases.

AS2 $n_i \prec n_j \rightarrow \bigwedge_{n_k \in \mathbf{N_1} \setminus \{n_j\}} \neg(n_i \prec n_k), n_i, n_j \in \mathbf{N}$

Similarly like [AS1].

AS3 $n_i \prec n_j \rightarrow \bigwedge_{n_k \in \mathbf{N_1} \setminus \{n_i\}} \neg(n_k \prec n_j), n_i, n_j \in \mathbf{N}$

Similarly like [AS1].

AS4 $n_i \prec n_j \rightarrow n_j \succ n_i, n_i, n_j \in \mathbf{N}$

Let $\langle r^l, t \rangle \models n_i \prec n_j$.

If $i = j$, by the definition of $n_i \prec n_i$ we have that

$$\langle r^l, t \rangle \models n_i \wedge \mathsf{K}_i(\bigwedge_{n_j \in \mathbf{N} \setminus \{n_i\}} \neg n_j),$$

so we have $\langle r^l, t \rangle \models n_i \succ n_j$.

Let $i \neq j$ and $j < i \leqslant m$, then

$$\langle r^l, t \rangle \models n_j \wedge n_i \wedge \mathsf{K}_j\left(\bigwedge_{k=j+1}^{i-1} \neg n_k\right) \wedge \mathsf{K}_j n_i,$$

which means that:

$$\langle r^l, t \rangle \models n_j \succ n_i.$$

Similarly in all other cases.

AS5 $n_i \succ n_j \to \mathtt{K}_i(n_i \succ n_j), n_i, n_j \in \mathbf{N}$

Suppose opposite, that

$$\langle r^l, t \rangle \models (n_i \succ n_j) \wedge \neg \mathtt{K}_i(n_i \succ n_j).$$

Then we have:

$$\langle r^l, t \rangle \models n_i \succ n_j \text{ and } \langle r^l, t \rangle \models \neg \mathtt{K}_i(n_i \succ n_j)),$$

and

$$\langle r^l, t \rangle \not\models \mathtt{K}_i(n_i \succ n_j).$$

By [AK3], we have that:

$$\langle r^l, t \rangle \not\models n_i \succ n_j,$$

which cannot hold.

AS6 $((n_i \succ n_j) \wedge n_k \mathtt{M}\langle n_i, n_j \rangle \wedge \bigcirc(\neg \mathtt{K}_i n_k)) \to \bigcirc(n_i \succ n_j), n_i, n_j, n_k \in \mathbf{N}$

Let $\langle r^{j'}, t \rangle \models ((n_i \succ n_j) \wedge n_k \mathtt{M}\langle n_i, n_j \rangle \wedge \bigcirc(\neg \mathtt{K}_i n_k))$, and suppose that $\langle r^{j'}, t+1 \rangle \not\models (n_i \succ n_j)$. Without loss of generality we can assume that $j < i \leqslant m - 1$. The, by the definition of $\succ$ and $\mathtt{M}$ we have that

$$(1) \qquad \langle r^{j'}, t \rangle \models n_i \wedge n_j \wedge \mathtt{K}_i(\bigwedge_{l=i+1}^{j-1} \neg n_l) \wedge \bigcirc \mathtt{K}_i(\bigwedge_{l=i+1}^{j-1} \neg n_l) \wedge \mathtt{K}_i n_j.$$

From $\langle r^{j'}, t+1 \rangle \not\models (n_i \succ n_j)$ we can conclude that for some $k, i < k < j$ $\langle r^{j'}, t+1 \rangle \models (n_i \succ n_k)$. By the definition of $\succ$:

$$\langle r^{j'}, t+1 \rangle \models n_i \wedge n_k \wedge \mathtt{K}_i(\bigwedge_{l=i+1}^{k-1} \neg n_l) \wedge \mathtt{K}_i n_k,$$

which is in contradiction with (1).

[MP], [RTN] and [RKN] in standard way (see [11, 13, 14])

RI from $\Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j \in \mathbb{N}})$ for all $i \geqslant 0$ infer $\Phi_k(\neg(\alpha \mathtt{U} \beta), (\theta_j)_{j \in \mathbb{N}})$

We show that [RI] produces valid formula for a valid set of premises by induction on k. Suppose that

$$\langle r^{j'}, t \rangle \models \Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j \in \mathbb{N}}), \text{ for } i \geqslant 0.$$

Then

$$\langle r^{j'}, t \rangle \models \Phi_k(\neg(\alpha \mathtt{U} \beta), (\theta_j)_{j \in \mathbb{N}})$$

by following: Induction base.

$k = 0$:

Note that:

if $\langle r^{j'}, t \rangle \not\models \theta_0 \to \neg(\alpha \mathtt{U} \beta)$ then

$\langle r^{j'}, t \rangle \models \theta_0 \wedge (\alpha \mathtt{U} \beta)$ iff

$\langle r^{j'}, t \rangle \models \theta_0$ and $\langle r^j, t \rangle \models \alpha \mathtt{U} \beta$ iff

$$(2) \qquad \langle r^{j'}, t \rangle \models \theta_0 \text{ and } \langle r^{j'}, t+i_0 \rangle \models \beta \text{ and } \langle r^{j'}, t+l \rangle \models \alpha, 0 \leqslant l < i_0$$

$$\langle r^{j'}, t \rangle \models \{\theta_0 \to \neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta) | i \geqslant 0\} \text{ iff}$$

$$(3) \quad \langle r^{j'}, t \rangle \models \neg\theta_0 \text{ and } (\langle r^{j'}, t+i \rangle \not\models \beta \text{ and } \langle r^{j'}, t+l \rangle \not\models \alpha, 0 \leqslant l < i \text{ for all } i \geqslant 0$$

which in contradiction with (2).

Inductive step.

Let $\langle r^{j'}, t\rangle \models \Phi_{k+1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ for $i \geqslant 0$, i.e.

$$\langle r^{j'}, t\rangle \models \theta_{k+1} \to K_{e_k}\Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$$

for $i \geqslant 0$ and $0 \leqslant e_k < m$. Let us assume opposite, that

$$\langle r^{j'}, t\rangle \not\models \Phi_{k+1}(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}}), \text{ i.e.}$$

$$\langle r^{j'}, t\rangle \models \theta_{k+1} \wedge \neg\Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}}).$$

Also, we have:

$$\langle r^{j'}, t\rangle \models K_{e_k}\Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$$

for $i \geqslant 0$. For every $\langle r^{j''}, t'\rangle \in \mathcal{K}_{e_k}(\langle r^{j'}, t\rangle)$ we have that:

$$\langle r^{j''}, t'\rangle \models \Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$$

and by induction hypothesis

$$\langle r^{j''}, t'\rangle \models \Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}}).$$

Therefore:

$$\langle r^{j'}, t\rangle \models K_{e_k}\Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}})$$

which is a contradiction.

$\square$

Theorem 7 (Deduction theorem). *$T \cup \{\varphi\} \vdash \psi$ implies $T \vdash \varphi \to \psi$.*

Proof. If ψ is an axiom or $\psi \in T$, then $T \vdash \psi$, so since $T \vdash \psi \to (\varphi \to \psi)$ [A1] by [MP] $T \vdash \varphi \to \psi$. If $\varphi = \psi$ then $T \vdash \varphi \to \varphi$ [A1].

If ψ is a theorem then, $\vdash \bigcirc\psi$. By weakening $T \vdash \bigcirc\psi$, so $T \vdash \varphi \to \bigcirc\psi$. Similarly for [RKN] rule.

Let us assume that ψ if obtained from $T \cup \{\varphi\}$ using [RI] rule, i.e. $\psi = \Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}})$. Then we have:

$T, \varphi \vdash \Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$,

$T \vdash \varphi \to \Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$, by induction hypothesis,

$T \vdash \varphi \to (\theta_k \to K_{e_k}\Phi_{k-1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}}))$, $0 \leqslant e_k < m$, by the definition of Φ_k

$T \vdash (\varphi \wedge \theta_k) \to K_{e_k}\Phi_{k-1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$, by propositional tautology $(p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r)$.

If we denote by $(\bar{\theta}_j)_{j\in\mathbb{N}}$ the sequence which coincides everywhere with $(\theta_j)_{j\in\mathbb{N}}$ for $j \neq k$, with the exception that $\bar{\theta}_k \equiv \varphi \wedge \theta_k$ we get that:

$T \vdash \bar{\theta}_k \to K_{e_{k-1}}\Phi_{k-1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\bar{\theta}_j)_{j\in\mathbb{N}})$,

$T \vdash \Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^{l}\alpha) \wedge \bigcirc^{i+1}\beta), (\bar{\theta}_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$,

$T \vdash \Phi_k(\neg(\alpha U\beta), (\bar{\theta}_j)_{j\in\mathbb{N}})$ by application of [RI]

$T \vdash (\varphi \wedge \theta_k) \to K_{e_{k-1}}\Phi_{k-1}(\neg(\alpha U\beta), (\bar{\theta}_j)_{j\in\mathbb{N}})$

$T \vdash \varphi \to (\theta_k \to K_{e_{k-1}}\Phi_{k-1}(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}}))$

$$T \vdash \varphi \to \Phi_k(\neg(\alpha \mathtt{U} \beta), (\theta_j)_{j \in \mathbb{N}))$$
$$T \vdash \varphi \to \psi.$$

$\square$

Definition 7. *For a given set of formulae T we define set $*T = \{*\alpha | \alpha \in T\}$ and $* \in \{\mathtt{K}_i, \bigcirc, \bullet\}, 0 \leqslant i < m$. Also, for a given set of formulae T we define set $\mathtt{K}_i^-(T) = \{\alpha | \mathtt{K}_i \alpha \in T\}$.*

Lemma 6. *Let α, β be formulae:*

LF1 $\vdash \mathtt{G}\alpha \leftrightarrow \alpha \wedge \bigcirc \mathtt{G}\alpha$,

LP1 $\vdash \mathtt{H}\alpha \leftrightarrow \alpha \wedge \bullet \mathtt{H}\alpha$,

LF2 $\vdash \mathtt{G} \bigcirc \alpha \leftrightarrow \bigcirc \mathtt{G}\alpha$,

LP2 $\vdash \mathtt{H}\bullet\alpha \leftrightarrow \bullet \mathtt{H}\alpha$,

LF3 $(\bigcirc\alpha \to \bigcirc\beta) \to \bigcirc(\alpha \to \beta)$,

LP3 $(\bullet\alpha \to \bullet\beta) \to \bullet(\alpha \to \beta)$,

LF4 $(\bigcirc\alpha \wedge \bigcirc\beta) \leftrightarrow \bigcirc(\alpha \wedge \beta)$,

LP4 $(\bullet\alpha \wedge \bullet\beta) \leftrightarrow \bullet(\alpha \wedge \beta)$,

LF5 $(\bigcirc\alpha \vee \bigcirc\beta) \leftrightarrow \bigcirc(\alpha \vee \beta)$,

LP5 $(\bullet\alpha \vee \bullet\beta) \leftrightarrow \bullet(\alpha \vee \beta)$,

LF6 $\mathtt{G}\alpha \vdash \bigcirc^i\alpha$, $i \geqslant 0$,

LP6 $\mathtt{H}\alpha \vdash (\bullet\bot \wedge \alpha) \vee \bullet^i\alpha$, $i \geqslant 0$,

LF7 *if* $\vdash \alpha$ *then* $\vdash \mathtt{G}\alpha$,

LP7 *if* $\vdash \alpha$ *then* $\vdash \mathtt{H}\alpha$,

LF8 *if* $T \vdash \alpha$, *where T is a set of formulae, then* $\bigcirc T \vdash \bigcirc\alpha$,

LP8 *if* $T \vdash \alpha$, *where T is a set of formulae, then* $\bullet T \vdash \bullet\alpha$,

LF9 *for* $j \geqslant 0$, $\bigcirc^j\beta, \bigcirc^0\alpha, \ldots, \bigcirc^{j-1}\alpha \vdash \alpha \mathtt{U}\beta$,

LP9 *for* $j \geqslant 0$, $\bullet^j\beta, \bullet^{j-1}\alpha, \ldots, \bullet^0\alpha \vdash \alpha \mathtt{S}\beta$,

LK *if* $T \vdash \gamma$, *where T is a set of formulae, then* $\mathtt{K}_e T \vdash \mathtt{K}_e\gamma$ *for any* $0 \leqslant e < m$.

Proof. LF1 $\vdash \mathtt{G}\alpha \leftrightarrow \alpha \wedge \bigcirc \mathtt{G}\alpha$

$\vdash \neg(\top\mathtt{U}\neg\alpha) \leftrightarrow \neg(\neg\alpha \vee (\top \wedge \bigcirc(\top\mathtt{U}\neg\alpha)))$ (by definition of $\mathtt{G}$ and [AT4])

$\vdash \neg(\top\mathtt{U}\neg\alpha) \leftrightarrow \alpha \wedge (\bot \vee \bigcirc\neg(\top\mathtt{U}\neg\alpha))$ (by [AT1])

$\vdash \neg(\top\mathtt{U}\neg\alpha) \leftrightarrow \alpha \wedge \bigcirc\neg(\top\mathtt{U}\neg\alpha)$ (property of $\vee$)

$\vdash \mathtt{G}\alpha \leftrightarrow \alpha \wedge \bigcirc \mathtt{G}\alpha$ (by definition of $\mathtt{G}$)

LF2 – LF7 The proofs are the consequences of the temporal part of the above axiomatization.

LF8 if $T \vdash \alpha$, where T is a set of formulae, then $\bigcirc T \vdash \bigcirc\alpha$

We will prove this by the induction on the length of the proof of α from T.

Suppose that α is obtained by the inference rule [MP] from $\beta \to \alpha$ and β. Then we have:

$\bigcirc T \vdash \bigcirc(\beta \to \alpha)$ (induction hypothesis)

$\bigcirc T \vdash \bigcirc(\beta \to \alpha) \to (\bigcirc\beta \to \bigcirc\alpha)$ [AT2]

$\bigcirc T \vdash \bigcirc\beta \to \bigcirc\alpha$ [MP]

$\bigcirc T \vdash \bigcirc\beta$ (induction hypothesis)

$\bigcirc T \vdash \bigcirc\alpha$ [MP]

Similarly we can prove the case when α is obtained using [RTN] and [RKN].

Suppose that $\alpha = \Phi_k(\neg(\gamma\mathtt{U}\beta), (\theta_j)_{j \in \mathbb{N}}) = \theta_k \to \mathtt{K}_i\Phi_{k-1}(\neg(\gamma\mathtt{U}\beta), (\theta_j)_{j \in \mathbb{N}})$ is obtained by the inference rule [RI]. Then:

for $0 \leqslant e < m, i \geqslant 0$, $\bigcirc T \vdash \bigcirc \Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \gamma) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$, by induction hypothesis

for $0 \leqslant e < m, i \geqslant 0$, $\bigcirc T \vdash \bigcirc(\theta_k \to \mathtt{K}_e\Phi_{k-1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}}))$, by definition of Φ_k

for $0 \leqslant e < m, i \geqslant 0$, $\bigcirc T \vdash \bigcirc(\theta_k \to \mathtt{K}_e\Phi_{k-1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})) \to (\bigcirc\theta_k \to \bigcirc\mathtt{K}_e\Phi_{k-1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha)\wedge\bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}}))$ [AT2]

for $0 \leqslant e < m, i \geqslant 0$, $\bigcirc T \vdash \bigcirc\theta_k \to \bigcirc\mathtt{K}_e\Phi_{k-1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ [MP]

for $0 \leqslant e < m$, $\bigcirc T \vdash (\bigcirc\theta_k \to \bigcirc\mathtt{K}_e\Phi_{k-1}(\neg(\gamma\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}}))$ [RI]

for $0 \leqslant e < m$, $\bigcirc T \vdash (\bigcirc\theta_k \to \bigcirc\mathtt{K}_e\Phi_{k-1}(\neg(\gamma\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}})) \to \bigcirc(\theta_k \to \mathtt{K}_e\Phi_{k-1}(\neg(\gamma\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}}))$ (LF3)

for $0 \leqslant e < m$, $\bigcirc T \vdash \bigcirc(\theta_k \to \mathtt{K}_e\Phi_{k-1}(\neg(\gamma\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}})$ [MP]

$\bigcirc T \vdash \bigcirc\Phi_k(\neg(\gamma\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}})$, by definition of Φ_k.

LF9 for $j \geqslant 0$, $\bigcirc^j\beta, \bigcirc^0\alpha, \ldots, \bigcirc^{j-1}\alpha \vdash \alpha\mathtt{U}\beta$

By propositional reasoning we can obtain:

$$\bigcirc^j\beta, \bigcirc^0\alpha, \ldots \bigcirc^{j-1}\alpha \vdash \beta \vee (\alpha \wedge (\bigcirc\beta \vee (\bigcirc\alpha \wedge (\ldots (\bigcirc^{j-1}\beta \vee (\bigcirc^{j-1}\alpha \wedge$$
$$(\bigcirc^j\beta \vee (\bigcirc^j\alpha \wedge \bigcirc^{j+1}(\alpha\mathtt{U}\beta)))))) \ldots))).$$

Since

$$\vdash \beta \vee (\alpha \wedge (\bigcirc\beta \vee (\bigcirc\alpha \wedge (\ldots (\bigcirc^{j-1}\beta \vee (\bigcirc^{j-1}\alpha \wedge (\bigcirc^j\beta \vee (\bigcirc^j\alpha \wedge \bigcirc^{j+1}(\alpha\mathtt{U}\beta)))))) \ldots))) \to \alpha\mathtt{U}\beta$$

can be gained using [AT3], we have

$$\bigcirc^j\beta, \bigcirc^0\alpha, \ldots, \bigcirc^{j-1}\alpha \vdash \alpha\mathtt{U}\beta.$$

LP1 – LP9 The proofs are similar to the [LF1 – LF9] respectively.

LK if $T \vdash \gamma$, where T is a set of formulae, then $\mathtt{K}_e T \vdash \mathtt{K}_e\gamma$ for any $0 \leqslant e < m$

We use the transfinite induction on the length of proof $T \vdash \gamma$. Suppose that $T \vdash \gamma$ where $\gamma \equiv \Phi_k(\neg(\alpha\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}}))$ is obtained using [RI] rule. Then:

$T \vdash \Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ for all $i \geq 0$

$\mathtt{K}_e T \vdash \mathtt{K}_e\Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha)\wedge\bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ by induction hypothesis,

$\mathtt{K}_e T \vdash \top \to \mathtt{K}_e\Phi_k(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha) \wedge \bigcirc^{i+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$

$\mathtt{K}_e T \vdash \Phi_{k+1}(\neg((\bigwedge_{l=0}^{i} \bigcirc^l \alpha)\wedge\bigcirc^{i+1}\beta), (\bar{\theta}_j)_{j\in\mathbb{N}})$ where $(\bar{\theta}_j)_{j\in\mathbb{N}}$ is a nested $k+1$-sequence such that $\bar{\theta}_{k+1} \equiv \top$, and which coincides everywhere with $(\bar{\theta}_j)_{j\in\mathbb{N}}$ for $j \neq k+1$

$\mathtt{K}_e T \vdash \Phi_{k+1}(\neg(\alpha\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}}))$ by [RI]

$\mathtt{K}_e T \vdash \top \to \mathtt{K}_e\Phi_k(\neg(\alpha\mathtt{U}\beta), (\theta_j)_{j\in\mathbb{N}}))$

$\mathtt{K}_e T \vdash \top \to \mathtt{K}_e\gamma$

$\mathtt{K}_e T \vdash \mathtt{K}_e\gamma$

$\square$

Theorem 2. *Every consistent set of formulas T can be extended to a maximal consistent set T^*.*

Proof. Let us assume that $For = \{\alpha_i | i \geqslant 0\}$ is the set of all formulas. The maximally consistent set T^* is defined recursively, as follows:

(1) $T_0 = T$,

(2) If α_i is consistent with T_i then $T_{i+1} = T_i \cup \{\alpha_i\}$,

(3) If α_i is not consistent with T_i and has form $\Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}})$ then

$$T_{i+1} = T_i \cup \{\neg\alpha_i, \neg\Phi_k(\neg((\bigwedge_{l=0}^{n_0} \bigcirc^l\alpha) \wedge \bigcirc^{n_0+1}\beta), (\theta_j)_{j\in\mathbb{N}})\}$$

where n_0 is a positive integer such that T_{i+1} is consistent,
(4) Otherwise $T_{i+1} = T_i$,
(5) $T^* = \bigcup_{n\geqslant 0} T_n$.

The set T_{i+1} obtained by the steps 2 or 4 is obviously consistent. Let us consider the step 3.

If we suppose that $\neg\Phi_k(\neg((\bigwedge_{l=0}^n \bigcirc^l\alpha) \wedge \bigcirc^{n+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ is not consistent with T_i for every $n \geqslant 0$ then by Deduction theorem, $T_i \vdash \Phi_k(\neg((\bigwedge_{l=0}^n \bigcirc^l\alpha)\wedge\bigcirc^{n+1}\beta), (\theta_j)_{j\in\mathbb{N}})$ for every $n \geqslant 0$, and by [RI] we have $T_i \vdash \Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}})$ which contradicts the assumption. Thus, the set T_i obtained by the step 3 is also consistent. Also, the construction guarantees that for each $\alpha \in For$, either $\alpha \in T^*$ or $\neg\alpha \in T^*$.

To prove that that T^* is deductively closed it is sufficient to prove that it is closed under the inference rules. We will only prove closeness under the inference rule [RI] since the other cases are straightforward.

Suppose that $\Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}}) \notin T^*$, while $\Phi_k(\neg((\bigwedge_{l=0}^n \bigcirc^l\alpha)\wedge\bigcirc^{n+1}\beta), (\theta_j)_{j\in\mathbb{N}}) \in T^*$ for every $n \geqslant 0$. By maximality of T^*, $\neg\Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}}) \in T^*$. If $\alpha_i = \Phi_k(\neg(\alpha U\beta), (\theta_j)_{j\in\mathbb{N}})$, then, by the construction of T^* there is n_0 such that $\neg\Phi_k(\neg((\bigwedge_{l=0}^{n_0} \bigcirc^l\alpha)\wedge\bigcirc^{n_0+1}\beta), (\theta_j)_{j\in\mathbb{N}}) \in T_i$ which contradicts the fact that $\Phi_k(\neg((\bigwedge_{l=0}^n \bigcirc^l\alpha)\wedge\bigcirc^{n+1}\beta), (\theta_j)_{j\in\mathbb{N}}) \in T^*$ for every $n \geqslant 0$. □

Lemma 7. T_j^t *is a maximal consistent set.*

Proof. The proof is by induction on t. By hypothesis, T_j^0 is maximal and consistent. Let $t \geqslant 0$ and T_j^t be maximal and consistent.

Suppose that T_j^{t+1} is not maximal. There is a formula α such that $\{\alpha, \neg\alpha\} \cap T_j^{t+1} = \varnothing$. Consequently, $\{\bigcirc\alpha, \bigcirc\neg\alpha\} \cap T_j^t = \varnothing$. Thus, we have that $\{\bigcirc\alpha, \neg\bigcirc\alpha\} \cap T_j^t = \varnothing$ which is in contradiction with the maximality of T_j^t.

Suppose that T_j^{t+1} is not consistent, i.e. $T_j^{t+1} \vdash \alpha \wedge \neg\alpha$, for any formula α. By [LF8], $\bigcirc T_j^{t+1} \vdash \bigcirc(\alpha \wedge \neg\alpha)$ and $T_j^t \vdash \bigcirc(\alpha \wedge \neg\alpha)$. By [LF4] and [AT1] we can show that $T_j^t \vdash \bigcirc\alpha \wedge \neg\bigcirc\alpha$, which is in contradiction with consistency of T_j^t. □

Theorem 3. *[Strong completeness] Every consistent set of formulas is satisfiable.*

Proof. We prove that $\gamma \in T_j^t$ iff $\langle r^j, t \rangle \models \gamma$ by induction on complexity of γ.

- $\gamma \in \mathbf{N}$. This is immediate consequence of the definition of π.
- The proof in the cases when γ is a negation or a conjunction is standard.
- $\gamma = \bigcirc\alpha$.
  $\langle r^j, t \rangle \models \bigcirc\alpha$ iff $\langle r^j, t+1 \rangle \models \alpha$ iff $\alpha \in T_j^{t+1}$ iff $\bigcirc\alpha \in T_j^t$
- $\gamma = \alpha U\beta$.
  Suppose that $\langle r^j, t \rangle \models \alpha U\beta$. There is some $i \geqslant 0$ such that $\langle r, t+i \rangle \models \beta$ and for every l, $0 \leqslant l < i$, $\langle r^j, t+l \rangle \models \alpha$. By the induction hypothesis, $\beta \in T_j^{t+i}$, for $i \geqslant 0$, and $\alpha \in T_j^{t+l}$, for $0 \leqslant l < i$. By the construction of $\mathbb{M}^*$, we have $\bigcirc^i\beta \in T_j^t$, for $i \geqslant 0$, and $\bigcirc^l\alpha \in T_j^t$, for $0 \leqslant l < i$. Thus, by [L9], we have that $\alpha U\beta \in T_j^t$.

For the other direction, assume that $\alpha \mathsf{U} \beta \in T_j^t$. By construction of the model $\mathbb{M}^*$, for some $i \geqslant 0, \bigcirc^i \beta \in T_j^t$, i.e. $\beta \in T_j^{t+i}$. Let $i_0 = \min\{i : \bigcirc^i \beta \in T_j^t\}$. If $i_0 = 0$, $\beta \in T_j^t$, and by the induction hypothesis $\langle r^j, t \rangle \models \beta$. It follows that $\langle r^j, t \rangle \models \alpha \mathsf{U} \beta$. Thus, suppose that $i_0 > 0$. For every i such that $0 \leqslant i < i_0$, $\bigcirc^i \beta \notin T_j^t$, i.e. $\beta \notin T_j^{t+i}$. So we have that $\alpha \mathsf{U} \beta \in T_j^t$ and $\beta \vee (\alpha \wedge (\bigcirc \beta \vee (\bigcirc \alpha \wedge \ldots \wedge (\bigcirc^{i_0 - 1} \beta \vee (\bigcirc^{i_0 - 1} \alpha \wedge \bigcirc^{i_0}(\alpha \mathsf{U} \beta) \ldots) \in T_j^t$. It follows that for every $i < i_0$, $\bigcirc^i \alpha \in \langle r^j, t \rangle$, $\alpha \in \langle r^j, t + i \rangle$, and by the induction hypothesis $\langle r^j, t + i \rangle \models \alpha$. From $\langle r^j, t + i_0 \rangle \models \beta$, it follows that $\langle r^j, t \rangle \models \alpha \mathsf{U} \beta$.

- $\gamma = \bullet \alpha$.
  - $t = 0$

    If $\bullet \alpha \in T_j^0$ by definition we have $\langle r^j, 0 \rangle \models \bullet \alpha$.

    Also, if $\langle r^j, 0 \rangle \models \bullet \alpha$ then $\bullet \bot \in T_j^0$, so: $\vdash \bot \to \alpha$ iff $\vdash \bullet(\bot \to \alpha)$ iff $\vdash \bullet \bot \to \bullet \alpha$ iff $\bullet \bot \vdash \bullet \alpha$ iff $\bullet \alpha \in T_j^0$
  - $t > 0$

    $\bullet \alpha \in T_j^t$ iff $\bigcirc \bullet \alpha \in T_j^{t-1}$ iff $\alpha \in T_j^{t-1}$ iff $\langle r^j, t-1 \rangle \models \alpha$ iff $\langle r^j, t \rangle \models \bullet \alpha$
- $\gamma = \alpha \mathsf{S} \beta$.
  - $t = 0$

    If $\alpha \mathsf{S} \beta \in T_j^0$, by [AT6] $\beta \in T_j^0$, thus $\langle r^j, 0 \rangle \models \alpha \mathsf{S} \beta$.

    If $\langle r^j, 0 \rangle \models \alpha \mathsf{S} \beta$ then $\langle r^j, 0 \rangle \models \beta$ and $\beta, \bullet \bot \in T_j^0$, thus by [AT6] $\alpha \mathsf{S} \beta \in T_j^0$.
  - $t > 0$

    Suppose that $\langle r^j, t \rangle \models \alpha \mathsf{S} \beta$. There is some $0 \leqslant i \leqslant t$ such that $\langle r^j, t - i \rangle \models \beta$ and for every l, $0 \leqslant l < i$, $\langle r^j, t - l \rangle \models \alpha$. Thus, $\beta \in T_j^{t-i}$, for $0 \leqslant i \leqslant t$, and $\alpha \in T_j^{t-l}$, for $0 \leqslant l < i$. By the construction of $\mathbb{M}^*$, we have $\bullet^i \beta \in T_j^t$, for $0 \leqslant i \leqslant t$, and $\bullet^l \alpha \in T_j^t$, for $0 \leqslant l < i$. Thus, by [LP9], we have that $\alpha \mathsf{S} \beta \in T_j^t$.

    Contrariwise, $\alpha \mathsf{S} \beta \in T_j^t$. By [AT6] we have that $\alpha \wedge \bullet(\alpha \mathsf{S} \beta)) \in T_j^t$. If $\beta \in T_j^t$ then $\langle r^j, t \rangle \models \beta$ and consequently $\langle r^j, t \rangle \models \alpha \mathsf{S} \beta$. Otherwise, if $\beta \notin T_j^t$ then $\alpha \in T_j^t$ and $\bullet(\alpha \mathsf{S} \beta) \in T_j^t$. By [LF8] $\bigcirc \bullet(\alpha \mathsf{S} \beta) \in T_j^{t-1}$, and by [AT8] $\alpha \mathsf{S} \beta \in T_j^{t-1}$. For some $k < t$, we have $\langle r^j, t \rangle \models \bullet^k \beta$ and $\langle r^j, t \rangle \models \bullet^l \alpha$, for $0 \leqslant l < k$. Thus, we have that $\langle r^j, t \rangle \models \alpha \mathsf{S} \beta$.
- $\gamma = \mathsf{K}_i \alpha$.

  Suppose $\mathsf{K}_i \alpha \in T_j^t$, then $\alpha \in \mathsf{K}_i^-(T_j^t)$. Also, $T_j^t \supset \mathsf{K}_i(\mathsf{K}_i^-(T_j^t))$, so for each $\langle r^{j'}, t' \rangle$ such that $\langle r^j, t \rangle \mathcal{K}_i \langle r^{j'}, t' \rangle$ (by the definition of relation $\mathcal{K}_i$), $\langle r^{j'}, t' \rangle \models \alpha$. By induction hypothesis (α is subformula of $\mathsf{K}_i \alpha$), we have that $\langle r^j, t \rangle \models \mathsf{K}_i \alpha$.

  Conversely, let $\langle r^j, t \rangle \models \mathsf{K}_i \alpha$ and assume the opposite, i.e. that $\mathsf{K}_i \alpha \notin T_j^t$. Then $\mathsf{K}_i^-(T_j^t) \cup \{\neg \alpha\}$ is consistent. Otherwise, by Deduction theorem $\mathsf{K}_i^-(T_j^t) \vdash \alpha$, by [LK], and $T_j^t \supset \mathsf{K}_i(\mathsf{K}_i^-(T_j^t)) \vdash \mathsf{K}_i \alpha$, by maximality of T_j^t, and $\mathsf{K}_i \alpha \in T_j^t$ which is a contradiction. Thus, $\mathsf{K}_i^-(T_j^t) \cup \{\neg \alpha\}$ can be extended to a maximal consistent set $T_{j'}^{t'}$, and:

$$n_i \in T_j^t \Rightarrow \mathsf{K}_i n_i \in T_j^t \Rightarrow n_i \in \mathsf{K}_i(T_j^t) \Rightarrow n_i \in T_{j'}^{t'}.$$

Similarly, for $\neg n_i \in T_j^t$. Thus, we have $\langle r^j, t \rangle \mathcal{K}_i \langle r^{j'}, t' \rangle$. Since $\neg \alpha \in T_{j'}^{t'}$, then $\langle r^{j'}, t' \rangle \models \neg \alpha$ by induction hypothesis, so $\langle r^{j'}, t' \rangle \not\models \alpha$, which is a contradiction.

$\square$

Lemma 3. *Let a peer join a Chord network, between two nodes which constitute a stable pair, such that the second node is the successor of the first node. Then, there is a finite period of time after the starting pair will be stable again, if no other nodes are trying to join in the meanwhile.*

Proof. Let us assume that $n_i, n_j \in \mathbf{N_a}$ and $n_i \mathbin{\text{\reflectbox{m}}} n_j$, i.e. $(n_i \succ n_j) \wedge (n_j \prec n_i)$ and that n_k tries to join that stable pair. Let us denote

$$\alpha = \bullet(n_i \mathbin{\text{\reflectbox{m}}} n_j) \wedge \rho_{J,k} \bigwedge_{n_l \in I} \bigwedge_{t=0}^{5f} \bigcirc^t \neg n_l, I = \{n_l | n_l \mathtt{M} \langle n_i, n_j \rangle, n_k \neq n_l, n_j \neq n_l\}$$

.

We have,

(by AS6) (1)

$\quad \alpha \vdash \mathtt{K}_i(n_i \succ n_j) \wedge \mathtt{K}_j(n_j \prec n_i) \wedge n_k \mathtt{M} \langle n_i, n_j \rangle \wedge n_k$

(by definition of $\wedge$ and 1) (2a)

$\quad \alpha \vdash \mathtt{K}_i(n_i \succ n_j)$

(by definition of $\wedge$ and 1) (2b)

$\quad \alpha \vdash \mathtt{K}_j(n_j \prec n_i)$

(by definition of $\wedge$ and 1) (2c)

$\quad \alpha \vdash n_k \mathtt{M} \langle n_i, n_j \rangle$

(by definition of $\wedge$ and 1) (2d)

$\quad \alpha \vdash n_k$

(by definition of α) (2e)

$\quad \alpha \vdash \rho_{J,k}$

(by 2d, 2e) (2f)

$\quad \alpha \vdash n_k \wedge \rho_{J,k}$

(by definition of $\rho_{J,k}$) (3)

$$\alpha \vdash \rho_{J,k} \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \mathtt{K}_k(n_k \succ n_j)$$

(by MP, 2e, 3) (4)

$$\alpha \vdash \bigvee_{l=0}^{f} \bigcirc^l \mathtt{K}_k(n_k \succ n_j)$$

(by definition of AS6,4) (5)

$$\alpha \vdash \bigvee_{l=0}^{f} \bigcirc^l \mathtt{K}_k(n_k \succ n_j) \rightarrow \bigcirc^f \mathtt{K}_k(n_k \succ n_j),$$

(by MP, 4, 5) (6)

$\quad \alpha \vdash \bigcirc^f \mathtt{K}_k(n_k \succ n_j)$

[ACF3] (7)

$$\alpha \vdash n_k \wedge \rho_{J,k} \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \rho_{S1,k,j}$$

(by MP, 2f,7) (8a)

$$\alpha \vdash \bigvee_{l=0}^{f} \bigcirc^l \rho_{S1,k,j}$$

(by AS6) (8b)

$$\alpha \vdash \bigcirc^f \rho_{S1,k,j}$$

(by 8b) (9a)

$$\alpha \vdash \bigcirc^f((\mathtt{K}_k(n_k \succ n_j) \wedge \mathtt{K}_j(n_j \prec n_i) \wedge n_k\mathtt{M}\langle n_i, n_j\rangle) \rightarrow \bigvee_{l=0}^{f} \bigcirc^l \mathtt{K}_j(n_j \prec n_k))$$

(by AT2, 9a) (9b)

$$\alpha \vdash \circ^f((\mathtt{K}_k(n_k \succ n_j) \wedge \mathtt{K}_j(n_j \prec n_i) \wedge n_k\mathtt{M}\langle n_i, n_j\rangle)) \rightarrow \circ^f(\bigvee_{l=0}^{f} \bigcirc^l \mathtt{K}_j(n_j \prec n_k))$$

(by AS6, 6) (10a)

$$\alpha \vdash \circ^f \mathtt{K}_k(n_k \succ n_j)$$

(by AS6, 2b) (10b)

$$\alpha \vdash \circ^f \mathtt{K}_k(n_j \prec n_i)$$

(by AS6, 2c) (10c)

$$\alpha \vdash \circ^f(n_k\mathtt{M}\langle n_i, n_j\rangle)$$

(by LF4, 10a, 10b, 10c) (11)

$$\alpha \vdash \circ^f(\mathtt{K}_k(n_k \succ n_j) \wedge \mathtt{K}_j(n_j \prec n_i) \wedge n_k\mathtt{M}\langle n_i, n_j\rangle)$$

(by MP, 9,11) (12)

$$\alpha \vdash \circ^f(\bigvee_{l=0}^{f} \bigcirc^l \mathtt{K}_j(n_j \prec n_k))$$

(by definition of $\bigcirc$, AS6, 12) (13)

$$\alpha \vdash \circ^{2f} \mathtt{K}_j(n_j \prec n_k)$$

(by $n_i \in \mathbf{N_a}$ and ACF2 or ACF4) (14)

$$\alpha \vdash \bigvee_{l=f}^{2f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S2,i,j}$$

(by definition of $\vee$,14) (15a)

$$\alpha \vdash \bigvee_{l=f}^{2f} \bigcirc^l \rho_{S2,i,k}$$

(by definition AS6,15a) (15b)

$$\alpha \vdash \bigcirc^{2f} \rho_{S2,i,k}$$

(by 15b) (16a)

$$\alpha \vdash \bigcirc^{2f}(\mathrm{K}_i(n_i \succ n_j) \wedge \mathrm{K}_j(n_j \prec n_k) \wedge n_k\mathrm{M}\langle n_i, n_j\rangle) \to \bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_i(n_i \succ n_k))$$

(by AT2, 16a) (16b)

$$\alpha \vdash \bigcirc^{2f}(\mathrm{K}_i(n_i \succ n_j) \wedge \mathrm{K}_j(n_j \prec n_k) \wedge n_k\mathrm{M}\langle n_i, n_j\rangle)) \to \bigcirc^{2f}(\bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_i(n_i \succ n_k))$$

(by AS6, 2a) (17a)

$$\alpha \vdash \bigcirc^{2f}\mathrm{K}_i(n_i \succ n_j)$$

(by AS6, 13) (17b)

$$\alpha \vdash \bigcirc^{2f}\mathrm{K}_j(n_j \prec n_k)$$

(by AS6, 2c) (17c)

$$\alpha \vdash \bigcirc^{2f}(n_k\mathrm{M}\langle n_i, n_j\rangle)$$

(by LF4, 17a, 17b, 17c) (18)

$$\alpha \vdash \bigcirc^{2f}(\mathrm{K}_i(n_i \succ n_j) \wedge \mathrm{K}_j(n_j \prec n_k) \wedge n_k\mathrm{M}\langle n_i, n_j\rangle)$$

(by MP, 16b,18) (19)

$$\alpha \vdash \bigcirc^{2f}(\bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_i(n_i \succ n_k))$$

(by definition of $\bigcirc$, AS6,19) (20)

$$\alpha \vdash \bigcirc^{3f}\mathrm{K}_i(n_i \succ n_k),$$

(by $n_i \in \mathbf{N_a}$ and ACF1 or ACF3) (21)

$$\alpha \vdash \bigvee_{l=3f}^{4f} \bigcirc^l \bigvee_{j=0}^{m-1} \rho_{S1,i,j}$$

(by definition of $\vee$,21) (22a)

$$\alpha \vdash \bigvee_{l=3f}^{4f} \bigcirc^l \rho_{S1,i,k}$$

(by definition AS6, 22a) (22b)

$$\alpha \vdash \bigcirc^{4f} \rho_{S1,i,k}$$

(by 22b) (23a)

$$\alpha \vdash \bigcirc^{4f}(\mathrm{K}_i(n_i \succ n_k) \wedge \mathrm{K}_k(n_k \prec u) \wedge n_k\mathrm{M}\langle n_i, n_j\rangle) \to \bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_k(n_k \prec n_i))$$

(by definition of AT2, 23a) (23b)

$$\alpha \vdash \bigcirc^{4f}(\mathrm{K}_i(n_i \succ n_k) \wedge \mathrm{K}_k(n_k \prec u) \wedge n_k\mathrm{M}\langle n_i, n_j\rangle)) \to \bigcirc^{4f}(\bigvee_{l=0}^{f} \bigcirc^l \mathrm{K}_k(n_k \prec n_i))$$

(by AS6, 29) (24a)

$$\alpha \vdash \bigcirc^{4f}\mathrm{K}_i(n_i \succ n_k)$$

(by AS6, 2e) (24b)

$$\alpha \vdash \bigcirc^{4f}\mathrm{K}_k(n_k \prec u)$$

(by AS6, 2c) (24c)
$$\alpha \vdash \bigcirc^{4f}(n_k \text{M}\langle n_i, n_j \rangle)$$
(by LF4, 24a, 24b, 24c) (25)
$$\alpha \vdash \bigcirc^{4f}(\text{K}_i(n_i \succ n_k) \wedge \text{K}_k(n_k \prec u) \wedge n_k \text{M}\langle n_i, n_j \rangle)$$
(by MP, 23b,25) (26)
$$\alpha \vdash \bigcirc^{4f}(\bigvee_{l=0}^{f} \bigcirc^l \text{K}_k(n_k \prec n_i))$$
(by definition of $\bigcirc$, AS6,26) (27)
$$\alpha \vdash \bigcirc^{5f} \text{K}_k(n_k \prec n_i)$$
(by AS6, 6) (28)
$$\alpha \vdash \bigcirc^{5f} \text{K}_k(n_k \succ n_j)$$
(by AS6, 13) (29)
$$\alpha \vdash \bigcirc^{5f} \text{K}_j(n_j \prec n_k)$$
(by AS6, 20) (30)
$$\alpha \vdash \bigcirc^{5f} \text{K}_i(n_i \succ n_k)$$
(by AS6, 27) (31)
$$\alpha \vdash \bigcirc^{5f} \text{K}_k(n_k \prec n_i)$$
(by LF4, 28, 29, 30, 31) (32)
$$\alpha \vdash \bigcirc^{5f}(\text{K}_k(n_k \succ n_j) \wedge \text{K}_j(n_j \prec n_k) \wedge \text{K}_i(n_i \succ n_k) \wedge \text{K}_k(n_k \prec n_i))$$
(by definition of ⋒) (33)
$$\alpha \vdash \bigcirc^{5f}(n_i ⋒ n_j)$$

$\square$

Acknowledgment

References

[1] L. Atzori, A. Iera, G. Morabito. *The Internet of things: A survey.* In *Computer Networks*, 54.15, 2787–2805, 2010.

[2] R. Bakhshi, D. Gurov. *Verification of Peer-to-peer Algorithms: A Case Study.* Technical report, ICT, 2006.

[3] R. Bakhshi, D. Gurov. *Verification of Peer-to-peer Algorithms: A Case Study.* In *Electronic Notes in Theoretical Computer Science* (ENTCS), Volume 181, 35–47, 2007.

[4] J. J. Bolonio, M. Urueña, G. Camarillo. *A Distributed Control Plane for the Internet of Things Based on a Distributed Hash Table.* In *Mobile Networks and Management*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 125, 108–121, 2013.

[5] S. Cirani, L. Davoli, G. Ferrari, R. Léone, P. Medagliani, M. Picone, L. Veltri. *A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things.* In *IEEE Internet of Things Journal*, Vol. 1, No. 5, 508–521, 2014.

[6] S. Evdokimov, B. Fabian, S. Kunz, N. Schoenemann. *Comparison of Discovery Service Architectures for the Internet of Things.* In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, 2010.

[7] R. Fagin, J. Y. Halpern, Y. Moses, M. Y. Vardi. *Reasoning About Knowledge.* The MIT Press, Cambridge, Massachusetts, 1995.

[8] D. R. Karger, E. Lehman, F. T. Leighton, R. Panigrahy, M. S. Levine, D. Lewin. *Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web.* In *Proceedings of STOC'97*, pages 654–663, 1997.

[9] S. Krishnamurthy, S. El-Ansary, E. Aurell, S. Haridi. *A Statistical Theory of Chord Under Churn.* In *4th International Workshop on Peer-To-Peer Systems*, pages 93–103, 2005.

[10] D. Liben-Nowell, H. Balakrishnan, D. R. Karger. *Analysis of the Evolution of Peer-to-Peer Systems.* In *Proc. 21st ACM Symp. Principles of Distributed Computing (PODC)*, pages 233–242, 2002.

[11] B. Marinković, Z. Ognjanović, D. Doder, A. Perović. *A Propositional Linear Time logic with Time Flow Isomorphic to ω^2.* In *Journal of Applied Logic*, 12(2), 208 − 229, 2014.

[12] M. Milošević, Z. Ognjanović. *A First-Order Conditional Probability Logic With Iterations.* In *Publication de L'Institute Matematique*, n.s. 93 (107), 19–27, 2013.

[13] Z. Ognjanović. *Discrete Linear-time Probabilistic Logics: Completeness, Decidability and Complexity.* In *Journal of Logic Computation*, Vol. 16, No. 2, 257–285, 2006.

[14] Z. Ognjanović, D. Doder, Z. Marković. *A Branching Time Logic with Two Types of Probability Operators.* In *Fifth International Conference on Scalable Uncertainty Management SUM-2011*, Springer LNCS 6929, 219–232, 2011.

[15] F. Paganelli, D. Parlanti. *A DHT-Based Discovery Service for the Internet of Things.* In *Journal of Computer Networks and Communications*, doi:10.1155/2012/107041, 2012.

[16] R. Rodrigues, P. Druschel. *Peer-to-Peer Systems* In *Communications of the ACM*, Vol. 53 Issue 10, pages 72–82, October 2010.

[17] I. Stoica, R. Morris, D. Karger, M. Kaashoek, H. Balakrishnan. *Chord: A Scalable Peer-to-Peer Lookup service for Internet Applications.* In *ACM SIGCOMM*, pages 149–160, 2001.

[18] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, H. Balakrishnan. *Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications.* MIT Technical report, TR-819, 2001.

[19] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, H. Balakrishnan. *Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications.* In *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, 17 − 32, 2003.

[20] I. Taylor. *From P2P to Web Services and Grids.* Springer-Verlag, 2005.

[21] S. Tomović, Z. Ognjanović, D. Doder. *Probabilistic Common Knowledge Among Infinite Number of Agents.* In *ECSQARU 2015*, LNCS 9161, 496 − 505, 2015/

[22] D. Xu, Z. Wu, Z. Wu, Q. Zhang, L. Qin, J. Zhou. *Internet of Things: Hotspot-based Discovery Service Architecture with Security Mechanism.* In *International Journal of Network Security*, Vol. 17, No. 2, 208–216, 2015.

[23] P. Zave. *Using Lightweight Modeling to Understand Chord.* In ACM SIGCOMM Computer Communication Review, Vol. 42, Issue 2, pages 50–57, April 2012.

Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Serbia
E-mail address: `bojanm@mi.sanu.ac.rs`

Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Serbia
E-mail address: `zorano@mi.sanu.ac.rs`

Faculty of Mechanical Engineering and Naval Architecture, University of Zagreb, Zagreb, Croatia
E-mail address: `pglavan@fsb.hr`

Faculty of Electrical Engineering, University of Ljubljana, Ljubljana, Slovenia
E-mail address: `anton.kos@fe.uni-lj.si`

Faculty of Electrical Engineering, University of Ljubljana, Ljubljana, Slovenia
E-mail address: `anton.umek@fe.uni-lj.si`