Knowledge and games: theory and implementation

Witzel, S.A.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

Download date: 04 Aug 2019
Chapter 1

Guarding common knowledge

1.1 Introduction

1.1.1 Motivation

As described in the Introduction chapter, our goal is a distributed implementation of a game-theoretic algorithm (see, e.g., [72] for a discussion of the interface between game theory and distributed computing). In this chapter, we lay the technical foundations to support such an implementation from a distributed computing point of view.

Two important issues in the domain of game theory are knowledge, especially common knowledge, and symmetry between the players, also called anonymity. We describe these issues and the connections to distributed computing in the following two paragraphs, before we motivate our choice of process calculus and the overall goal of the chapter.

Common knowledge and synchronization. The concept of common knowledge, first introduced by Lewis [92] building on ideas of Schelling [134], has been a topic of much research in distributed computing [73] as well as in game theory [12]. When do processes or players “know” some fact, mutually know that they know it, mutually know that they mutually know that they know it, and so on ad infinitum? And how crucial is the difference between arbitrarily, but finitely deep mutual knowledge and the limit case of real common knowledge?

In the area of distributed computing, the classical example showing that the difference is indeed essential is the scenario of coordinated attack described in the Introduction chapter. The game-theoretic incarnation of the underlying issue is the electronic mail game by Rubinstein [129] (see [102] for a more recent treatment).

The basic insight of these examples is that two agents who communicate through an unreliable channel can never achieve common knowledge, and that
their behavior under finite mutual knowledge can be strikingly different.

These issues have been analyzed in detail by Fagin et al. [60], in particular in a separately published part [73], including a variant where communication is reliable, but message delivery takes an unknown amount of time. Even in that variant, which has also been looked at by Parikh and Ramanujam [116], it is shown that only finite mutual knowledge can be attained.

However, in a synchronous communication act, sending and receiving of a message is, by definition, performed simultaneously. In that way, the agents obtain not only the pure factual information content of the message, but the sender also knows that the receiver has received the message, the receiver knows that the sender knows that, and so on ad infinitum. The communicated information immediately becomes common knowledge.

Attaining common knowledge and achieving synchronization between processes are thus closely related. Furthermore, synchronization is in itself an important subject (see, e.g., [135]).

**Symmetry and peer-to-peer networks.** In game theory, it is usually assumed that players are anonymous and treated on an equal footing in the following sense: Any differences between them are only induced by the payoff structure and the information state in a given game, while their names do not play a role and no player is a priori distinguished from the others [106, 103]. If we want to set up a system that allows processes to incarnate players in any given game, we need to make sure that those processes are on an equal footing in a corresponding sense. Even though the interaction structures we introduce later can take any form, we need to be prepared for cases where the communication infrastructure is in a certain sense symmetric. Such symmetric settings, as we see in this chapter, constitute the crucial cases from the technical viewpoint of an implementation.

In distributed computing, a corresponding kind of symmetry among processes is often a desideratum. Reasons to avoid a predetermined assignment of roles to processes or a centralized coordinator include fault tolerance, modularity, and load balancing [3].

We consider symmetry on two levels. Firstly, we assume communication networks used by the processes to be symmetric to some extent in order not to discriminate single processes a priori on a topological level; we formalize this requirement by defining peer-to-peer networks. These networks are a special case of the interaction structures we use in Chapters 2 and 3, but our results carry over, as we discuss in Section 1.5. Secondly, processes in symmetric positions of the network should have equal possibilities of behavior; this we formalize in a semantic symmetry requirement on the possible computations.

---

1Please note that we are not dealing with fashionable incarnations such as file-sharing networks, but merely use this name for a mathematical notion of a network consisting of directly connected peers “treated on an equal footing”, i.e., not having a client-server structure or otherwise pre-determined roles.
1.1. Introduction

Communicating Sequential Processes (CSP). Since we are interested in synchronization and common knowledge, a process calculus which supports synchronous communication through primitive statements clearly has some appeal. We focus on one of the prime examples of such calculi, namely CSP, introduced by Hoare [79] and later revised [80, 136]. It allows synchronous communication by means of deterministic statements on the one hand and non-deterministic alternatives on the other hand, where the communication statements occur in so-called guards.

CSP has been implemented in various programming languages, among the best-known of which is Occam [82]. We thus have at our disposal a theoretical framework and programming tools which in principle could give us synchronization and common knowledge “for free”.

However, symmetric situations are a reliable source of impossibility results, see [63] for a recent collection. There exist different dialects of CSP, which differ in what communication statements are allowed to appear in guards. We define the relevant dialects later on, for now suffice it to say that the dialect CSP\textsubscript{in} which was, for implementation-related reasons [33], chosen to be the theoretical foundation of Occam is more sensitive to symmetric situations than the general form CSP\textsubscript{io}. This has been proved formally by Bougé [29].

CSP\textsubscript{in} has been used throughout the history of Occam, up to and including its latest variant Occam-π [150]. This restriction to CSP\textsubscript{in} generally tends to be the case for implementations of CSP. One notable exception is a recent extension of JCSP, a Java\textsuperscript{TM} implementation of CSP, by Welch et al. [151].

Some of the restrictions resulting in CSP\textsubscript{in} can in practice be overcome by using helper processes such as buffers [84]. It is conceivable that such processes could be used as mediators to coordinate and establish direct and synchronous communication among the main processes. Therefore, our goal is to formalize the concepts mentioned above, extend the notion of peer-to-peer networks by allowing helper processes, and examine whether synchronization is feasible in either of these two dialects of CSP. We come to the result that, while it can (straightforwardly) be obtained in CSP\textsubscript{io}, it is impossible to do so in CSP\textsubscript{in}. For the setting of this dissertation, we thus need to use one of the rare more general implementations such as JCSP.

1.1.2 Related work

We extend work by Bougé [29], where a semantic characterization of symmetry for CSP is given and fundamental possibility and impossibility results for the problem of electing a leader in networks of symmetric processes are proved for various dialects of CSP. More recently, this has inspired a similar work by Palamidessi [110] on the more expressive π-calculus, but the possibility of adding helper processes is explicitly excluded.

There has been research on how to circumvent problems resulting from the
restrictions of CSP. However, solutions are typically concerned only with the factual content of messages and do not preserve synchronicity and the common knowledge creating effect of communication, for example by relaying communication through buffers [84].

The same focus on factual information holds for general research on synchronizing processes with asynchronous communication. For example, in [135] one goal is to ensure that a writing process knows that no other process is currently writing; whether this is common knowledge, is not an issue.

The problem of coordinated attack has also been studied for models in which processes run synchronously [63]; however, the interesting property of CSP is that processes run asynchronously, which is more realistic in physically distributed systems, and synchronize only at communication statements.

Since we focus on the communication mechanisms, our results carry over to other formalisms with synchronous communication facilities comparable to those of CSP.

1.1.3 Plan of the chapter

In Section 1.2 we give a short description of CSP and the dialects that we are interested in, define some basic concepts from graph theory, and recall the required notions and results for symmetric electoral systems by Bougé [29].

In Section 1.3 we set the stage by first formally defining the problem of pairwise synchronization that we examine. Subsequently, we give a formalization of peer-to-peer networks which ensures a certain kind of symmetry on the topological level, and describe in what ways we want to allow them to be extended by helper processes. Finally, we adapt a concept from [29] to capture symmetry on the semantic level.

Section 1.4 contains two positive results and the main negative result saying that pairwise synchronization of peer-to-peer networks of symmetric processes is not obtainable in CSP, even if we allow extensions through buffers or similar helper processes which might mediate between the main processes.

Section 1.5 offers a concluding discussion.

1.2 Preliminaries

We briefly review the required concepts and results from the CSP calculus in Section 1.2.1, from graph theory in Section 1.2.2, and from [29] in Section 1.2.3. For more details see [79, 117, 29].
1.2. Preliminaries

1.2.1 CSP

A CSP process consists of a sequential program which can use, besides the usual local statements (e.g. assignments or expression evaluations involving its local variables), two communication statements:

- $P! \text{message}$ to send (output) the given message to process $P$;
- $P? \text{variable}$ to receive (input) a message from process $P$ and store it in the given (local) variable.

Communication is synchronous, i.e., send and receive instructions block until their counterpart is available, at which point the message is transferred and both participating processes continue execution. Note that the communication partner $P$ is statically defined in the program code.

There are two control structures containing guarded commands, see Figure 1.1. A guard is a Boolean expression over local variables (which, if omitted, is taken to be true), optionally followed by a communication statement. A guard is open if its Boolean expression evaluates to true and its communication statement, if any, can currently be performed. A guard is closed if its Boolean expression evaluates to false. Note that a guard can thus be neither open nor closed.

\[
\begin{align*}
\&\text{guard}_1 \to \text{command}_1 \\
\&\text{guard}_2 \to \text{command}_2 \\
\&\vdots \\
\&\text{guard}_k \to \text{command}_k
\end{align*}
\]

(a) Non-deterministic selection

\[
\begin{align*}
\&\text{guard}_1 \to \text{command}_1 \\
\&\text{guard}_2 \to \text{command}_2 \\
\&\vdots \\
\&\text{guard}_k \to \text{command}_k
\end{align*}
\]

(b) Non-deterministic repetition

Figure 1.1: Control structures in CSP.

The selection statement fails and execution is aborted if all guards are closed. Otherwise execution is suspended until there is at least one open guard. Then one of the open guards is selected non-deterministically, the required communication (if any) performed, and the associated command executed.

The repetition statement keeps waiting for, selecting, and executing open guards and their associated commands until all guards are closed, and then exits normally; that is, program execution continues at the next statement.

We sometimes use the following abbreviation to denote multiple branches of a control structure (for some finite set $X$):

\[
\Box_{x \in X} \text{guard}_x \to \text{command}_x
\]

Various dialects of CSP can be distinguished according to what kind of communication statements are allowed to appear in guards. Specifically, in $CSP_m$ only input statements are allowed, and in $CSP_{i/o}$ both input and output statements

\[
\Box_{x \in X} \text{guard}_x \to \text{command}_x
\]
Chapter 1. Guarding common knowledge

are allowed (within the same control structure). For technical reasons, CSP\textsubscript{m} has been suggested from the beginning [79] and is indeed commonly used for implementations, as mentioned in Section 1.1.1.

1.2.1. Definition. A communication graph (or network) is a directed graph without self-loops. A process system (or simply system) \(\mathcal{P}\) with communication graph \(G = (V, E)\) is a set of component processes \(\{P_v\}_{v \in V}\) such that for all \(v, w \in V\), if the program run by \(P_v\) (respectively \(P_w\)) contains an output command to \(P_w\) (respectively input command from \(P_v\)) then \((v, w) \in E\). In that case we say that \(G\) admits \(\mathcal{P}\). We identify vertices \(v\) and associated processes \(P_v\) and use them interchangeably.

1.2.2. Example. Figure 1.2 shows a simple network \(G\) with the vertex names written inside the vertices, and a CSP\textsubscript{i/o} program run by two processes which make up a system \(\mathcal{P} := \{P_0, P_1\}\). Obviously, \(G\) admits \(\mathcal{P}\). The intended behavior is that the processes send each other, in non-deterministic order, a message containing their respective process name. Since communication is synchronous, it is guaranteed that both processes execute each communication statement synchronously at the time when the message is transmitted. In a larger context, executing this code fragment would have the effect that the participating processes synchronize, i.e., wait for each other and jointly perform the communication. In terms of knowledge, this fact as well as the transmitted message (which can of course be more interesting than just the process names) become common knowledge between the processes.

\[
\begin{align*}
&\text{recd} := \text{false} \\
&\text{sent} := \text{false}
\end{align*}
\]

(a) Network \(G\)

\[
\begin{array}{c}
0 \quad 1 \\
\end{array}
\]

\([\neg \text{recd} \land P_{i+1} ? x \rightarrow \text{recd} := \text{true} \\
\quad \square \neg \text{sent} \land P_{i+1} ! i \rightarrow \text{sent} := \text{true}]
\]

(b) Program of process \(P_i\)

Figure 1.2: Network and program run by \(P_0\) and \(P_1\) in Example 1.2.2. Addition within process names here and in all further example programs is modulo 2.

1.2.3. Definition. A state of a system \(\mathcal{P}\) is the collection of all component processes’ (local) variables together with their current execution positions. A computation step is a transition from one state to another, involving either one component process executing a local statement, or two component processes jointly executing a pair of matching (send and receive) communication statements. The possible next computation steps are thus determined by the current state of the system.

A computation is a maximal sequence of computation steps, i.e., a sequence which is not a prefix of any other sequence of computation steps. A computation
• is **properly terminated** if all component processes have completed their last instruction,

• **diverges** if it is infinite, and

• is in **deadlock** if it is finite but not properly terminated.

1.2.4. **Example.** Figure 1.3 shows a computation of the system from Figure 1.2. It is finite and both processes reach the end of their respective program, so it is properly terminated. Note that the exact order in which, for example, the processes get to initialize their local variables is non-deterministic, so there are other computations with these steps exchanged. Only certain restrictions to the order apply, e.g. that the steps within one process are ordered corresponding to its program, or that both processes must have evaluated the Boolean guards before they can participate in the subsequent communication.

\[
\begin{align*}
P_0 &: \text{assign false to } recd \\
P_1 &: \text{assign false to } recd \\
P_1 &: \text{assign false to } sent \\
P_0 &: \text{assign false to } sent \\
P_1 &: \text{evaluate Boolean guards} \\
P_2 &: \text{evaluate Boolean guards} \\
P_0, P_1 &: \text{send 0 from } P_0 \text{'s variable } x \\
P_0 &: \text{assign true to } sent \\
P_0 &: \text{evaluate Boolean guards} \\
P_1 &: \text{assign true to } recd \\
P_1 &: \text{evaluate Boolean guards} \\
P_0, P_1 &: \text{send 1 from } P_1 \text{'s variable } x \\
P_1 &: \text{assign true to } sent \\
P_0 &: \text{assign true to } recd \\
P_0 &: \text{evaluate Boolean guards and exit repetition} \\
P_1 &: \text{evaluate Boolean guards and exit repetition}
\end{align*}
\]

Figure 1.3: A properly terminating computation of the system from **Example 1.2.2.**

1.2.2 **Graph theory**

We state some fundamental notions concerning directed finite graphs, from here on simply referred to as **graphs.**
1.2.5. **Definition.** Two vertices \( a, b \in V \) of a graph \( G = (V, E) \) are **strongly connected** if there are paths from \( a \) to \( b \) and from \( b \) to \( a \) consisting of edges in \( E \). \( G \) is strongly connected if all pairs of vertices are.

Two vertices \( a, b \in V \) are **directly connected** if \((a, b) \in E \) or \((b, a) \in E \); \( G \) is directly connected if all pairs of vertices are. \( \square \)

1.2.6. **Definition.** An **automorphism** of a graph \( G = (V, E) \) is a permutation \( \sigma \) of \( V \) such that for all \( v, w \in V \),

\[
(v, w) \in E \text{ implies } (\sigma(v), \sigma(w)) \in E.
\]

The **automorphism group** \( \Sigma_G \) of a graph \( G \) is the set of all automorphisms of \( G \). The least \( p > 0 \) with \( \sigma^p = \text{id} \) is called the **period** of \( \sigma \), where by \text{id} we denote the identity function defined on the domain of whatever function it is compared to.

The **orbit** of \( v \in V \) under \( \sigma \in \Sigma_G \) is \( O^\sigma_v := \{\sigma^p(v) | p \geq 0\} \). An automorphism \( \sigma \) is **well-balanced** if the orbits of all vertices have the same cardinality, or alternatively, if for all \( p \geq 0 \),

\[
\sigma^p(v) = v \text{ for some } v \in V \text{ implies } \sigma^p = \text{id}.
\]

We usually consider the (possibly empty) set \( \Sigma_G^{wb} \setminus \{\text{id}\} \) of **non-trivial** well-balanced automorphisms of a graph \( G \), that is those with period greater than 1.

A subset \( W \subseteq V \) is called **invariant** under \( \sigma \in \Sigma_G \) if \( \sigma(W) = W \), i.e., if \( W \) is an orbit under \( \sigma \); it is called invariant under \( \Sigma_G \) if it is invariant under all \( \sigma \in \Sigma_G \). \( \square \)

1.2.7. **Example.** Figure 1.4 shows two graphs \( G \) and \( H \) and automorphisms \( \sigma \in \Sigma_G \) with period 3 and \( \tau \in \Sigma_H \) with period 2. Both are well-balanced since, e.g., \( O^\sigma_1 = O^\sigma_3 = \{1, 3\} \) and \( O^\tau_2 = O^\tau_4 = \{2, 4\} \) all have the same cardinality. We have \( \Sigma_H = \{\text{id}, \tau\} \), so \( \{1, 3\} \) and \( \{2, 4\} \) are invariant under \( \Sigma_H \).

![Figure 1.4: Two graphs with non-trivial well-balanced automorphisms, indicated by gray, bent arrows.](image-url)
1.2.3 Symmetric electoral systems

We take over the semantic definition of symmetry from Bougé [29]. As discussed there, syntactic notions of symmetry are difficult to formalize properly; requiring that “all processes run the same program” does not do the job. We skip some formal details which we are not going to use. The interested reader is referred to [29].

1.2.8. Definition (adapted from [29, Definition 2.2.2]). A system $\mathcal{P}$ with communication graph $G = (V, E)$ is symmetric if for each automorphism $\sigma \in \Sigma_G$ and each computation $C$ of $\mathcal{P}$, there is a computation $C'$ of $\mathcal{P}$ satisfying the following condition: For each $v \in V$, process $P_{\sigma(v)}$ performs the same steps in $C'$ as $P_v$ in $C$, modulo changing via $\sigma$ the process names occurring in the computation (e.g. as communication partners).

The intuitive interpretation of this symmetry notion is as follows. Any two processes which are not already distinguished by the communication graph $G$ itself, i.e., which are related by some automorphism, must have equal possibilities of behavior. That is, whatever behavior one process exhibits in some particular possible execution of the system (i.e., in some computation), the other process must exhibit in some other possible execution of the system, localized to its position in the graph by appropriate process renaming. Taken back to the syntactic level, this is the case, for example, if both processes run the same program, which does not make use of any externally given distinctive features like an ordering on the process names.

1.2.9. Example. The system from Figure 1.2 is symmetric. It is easy to see that, for example, if we swap all 0s and 1s in the computation shown in Figure 1.3, we still have a computation of $\mathcal{P}$. Note that programs are allowed to access the process names, and indeed they do; however, they do not, for example, use their natural order to determine which process sends first.

1.2.10. Example. On the other hand, consider the system $\mathcal{Q} = \{Q_0, Q_1\}$ running the program in Figure 1.5. There is obviously a computation where $Q_0$ sends its process name 0 to $Q_1$; since the two vertices of the communication graph are related by an automorphism, symmetry would require that there also be a computation where $Q_1$ sends its process name 1 to $Q_0$. However, such a computation does not exist due to the use of the process name for determining the communication role, so the system is not symmetric.

$$
\begin{align*}
\begin{bmatrix}
i = 0 & \rightarrow & Q_{i+1} ! i \\
\square i = 1 & \rightarrow & Q_{i+1} ? x
\end{bmatrix}
\end{align*}
$$

Figure 1.5: Asymmetric program run by $Q_0$ and $Q_1$ in Example 1.2.10.
Chapter 1. Guarding common knowledge

We now recall a classical problem for networks of processes, pointed out by Le Lann [90].

1.2.11. Definition (from [29, Definition 1.2.1]). A system $P$ is an electoral system if

(i) all computations of $P$ are properly terminating and

(ii) each process of $P$ has a local variable leader, and at the time of termination all these variables contain the same value, the name of some process $P \in P$.

We now restate the impossibility result which our work builds on, combining a graph-theoretical characterization with the symmetry notion and electoral systems.

1.2.12. Theorem (from [29, Theorem 3.3.2]). Suppose a network $G$ admits some well-balanced automorphism $\sigma$ different from id. Then $G$ admits no symmetric electoral system in CSP$_m$.

1.3 Setting the stage

1.3.1 Pairwise synchronization

Intuitively, if we look at synchronization as part of a larger system, a process is able to synchronize with another process if it can execute an algorithm such that a direct communication (of any message) between the two processes takes place. This may be the starting point of some communication protocol to exchange more information, or simply be taken as an event creating common knowledge about the processes’ current progress of execution.

Communication in CSP always involves exactly two processes and facilities for synchronous broadcast do not exist, thus synchronization is inherently pairwise only. This special case is interesting nevertheless and has been used as a setting to examine knowledge-related issues, e.g., by Parikh and Krasucki [115]. Note that JCSP supports broadcasts as an extension of communication to multiple recipients, and as such can accommodate the interaction structures we deal with in Chapters 2 and 3.

Focusing on the synchronization algorithm, we want to guarantee that it allows all pairs of processes to synchronize. To this end, we require existence of a system where in all computations, all pairs of processes synchronize. Most probably, in a real system not all pairs of processes need to synchronize in all executions. However, if one has an algorithm which in principle allows that, then one could certainly design a system where they actually do; and, vice versa, if one has a system which is guaranteed to synchronize all pairs of processes, then one can
obviously use its algorithms to synchronize any given pair. Therefore we use the following formal notion.

**1.3.1. Definition.** A system $\mathcal{P}$ of processes (pairwise) synchronizes $Q \subseteq \mathcal{P}$ if all computations of $\mathcal{P}$ are finite and properly terminating and contain, for each pair $P_a, P_b \in Q$, at least one direct communication from $P_a$ to $P_b$ or from $P_b$ to $P_a$.

**1.3.2. Example.** The system from Figure 1.2 synchronizes $\{P_0, P_1\}$.

Note that the program considered so far is not a valid CSP$_m$ program, since an output statement appears within a guard. If we want to restrict ourselves to CSP$_m$ (for example, to implement the program in Occam), we have to get rid of that statement. Attempts to simply move it out of the guard fail since the symmetric situation inevitably leads to a system which may deadlock.

To see this, consider the system $\mathcal{P}' = \{P_0', P_1'\}$ with the program shown in Figure 1.6. There is no guarantee that not both processes enter the second clause of the repetition at the same time, since it is now only guarded by a local variable, and then block forever at the output statement, waiting for each other to become ready for input. A standard workaround [84] for such cases is to introduce buffer processes mediating between the main processes, in our case resulting in the extended system $\mathcal{R} = \{R_0, R_0', R_1, R_1'\}$ shown in Figure 1.7.

```
recd := false
sent := false
*[ ¬recd ∧ P'_{i+1} ? x → recd := true
\Box ¬sent → P'_{i+1}! i; sent := true ]
```

Figure 1.6: Program of process $P'_i$ potentially causing deadlock.

```
recd := false
sent := false
*[ ¬recd ∧ R'_{i+1} ? x → recd := true
\Box ¬sent → R'_{i+1}! i; sent := true ]
```

(a) Program of main process $R_i$ (b) Program of buffer process $R'_i$

(c) Underlying communication network

Figure 1.7: Extended system with main processes $R_0$ and $R_1$ and buffer processes $R'_0$ and $R'_1$ together with the underlying communication network.
Chapter 1. Guarding common knowledge

While the actual data transmitted between the main processes remains the same, this system obviously cannot synchronize \( \{ R_0, R_1 \} \), since there is not even a direct link in the communication network. This removes the synchronizing and common knowledge creating effects of communication. Even though a buffer might notify its main process when its message is delivered, then notify the communication partner about the notification, and so on, synchronicity is not restored and mutual knowledge only attained to a finite (if arbitrarily high) level, as seen in the coordinated attack example discussed in the Introduction chapter.

The obvious question now is: Is it possible to change the program or use buffer or other helper processes in more complicated and smarter ways to negotiate between the main processes and aid them in establishing direct communications?

To attack this question, in the following Section 1.3.2 we formalize the kind of communication networks we are interested in and define how they may be extended in order to allow for helper processes without affecting the symmetry inherent in the original network.

1.3.2 Peer-to-peer networks

The idea of peer-to-peer networks is to have nodes which can communicate with each other directly and on an equal footing, i.e., there is no predetermined client/server architecture or central authority coordinating the communication. We first formalize the topological prerequisites for this, and then adapt the semantic symmetry requirement to our setting.

1.3.3. Definition. A peer-to-peer network is a communication graph \( G = (V, E) \) with at least two vertices (also called nodes) such that

(i) \( G \) is strongly connected,

(ii) \( G \) is directly connected, and

(iii) we have \( \Sigma^w_G \setminus \{ \text{id} \} \neq \emptyset \).

In this definition,

(i) says that each node has the possibility to contact (at least indirectly) any other node, reflecting the fact that there are no predetermined client/server roles;

(ii) ensures that all pairs of nodes have a direct connection at least in one direction, without which pairwise synchronization by definition would be impossible; and

(iii) requires a kind of symmetry in the network.
1.3. Setting the stage

This last item is implied by the more intuitive requirement that there be some $\sigma \in \Sigma_G$ with only one orbit, i.e., an automorphism relating all nodes to each other and thus making sure that they are topologically on an equal footing. The requirement we use is less restrictive and suffices for our purposes.

1.3.4. Example. See Figure 1.4 for two examples of peer-to-peer networks.

We consider extensions of a peer-to-peer network in order to allow for helper processes while preserving the symmetry inherent in the network. The intuitive background for this kind of extensions is that we view the peers, i.e., the nodes of the original network, as processors each running a main process, while the added nodes can be thought of as helper processes running on the same processor as their respective main process. Communication connections between processors are physically given, while inside a processor they can be created as necessary.

1.3.5. Definition. Let $G = (V, E)$ be a peer-to-peer network, then $G' = (V', E')$ is a symmetry-preserving extension of $G$ iff there is a collection $\{S_v\}_{v \in V}$ partitioning $V'$ such that

(i) for all $v \in V$, we have $v \in S_v$;

(ii) all $v \in V$ and $v' \in S_v \setminus \{v\}$ are strongly connected (possibly via nodes $\not\in S_v$);

(iii) for all $v, w \in V$, $E' \cap (S_v \times S_w) \neq \emptyset$ iff $(v, w) \in E$;

(iv) there is, for each $\sigma \in \Sigma_G$, an automorphism $\iota_\sigma \in \Sigma_{G'}$ extending $\sigma$ such that $\iota_\sigma(S_v) = S_{\sigma(v)}$ for all $v \in V$.

Note that, in general, the collection $\{S_v\}_{v \in V}$ may not be unique. When we refer to it, we implicitly fix an arbitrary one.

Intuitively, these requirements are justified as follows:

(i) Each $S_v$ can be seen as the collection of processes running on the processor at vertex $v$, including its main process $P_v$.

(ii) The main process should be able to communicate (at least indirectly) in both ways with each helper process.

(iii) While communication links within one processor can be created freely, links between processes on different processors are only possible if there is a physical connection, that is a connection in the original peer-to-peer network; also, if there was a connection in the original network, then there should be one in the extension in order to preserve the network structure.

(iv) Lastly, to preserve symmetry, each automorphism of the original network must have an extension which maps all helper processes to the same processor as their corresponding main process.
1.3.6. Example. See Figure 1.8 for an example of a symmetry-preserving extension. Note that condition (iii) of Definition 1.3.5 is liberal enough to allow helper processes to communicate directly with processes running on other processors, and indeed, e.g. 2c has a link to 3. It also allows several communication links on one physical connection, reflected by the fact that there are three links connecting $S_2$ to $S_3$. Furthermore, (ii) is satisfied in that the main processes are strongly connected with their helper processes, although, as e.g. with 2 and 2c, indirectly and through processes on other processors.

![Diagram](image.png)

Figure 1.8: A symmetry-preserving extension (illustrating Definition 1.3.5).

We need the following immediate fact later on.

1.3.7. Fact. As a direct consequence of Definitions 1.3.3 and 1.3.5, any symmetry-preserving extension of a peer-to-peer network is strongly connected.

1.3.3 $G$-symmetry

Corresponding to the intuition of processors with main and helper processes, we weaken Definition 1.2.8 such that only automorphisms are considered which keep the set of main processes invariant and map helper processes to the same processor as their main process. There are cases where the main processor otherwise would be required to run the same program as some helper process.

1.3.8. Definition. A system $\mathcal{P}$ whose communication graph $G'$ is a symmetry-preserving extension of some peer-to-peer network $G = (V,E)$ is called $G$-symmetric if Definition 1.2.8 holds with respect to those automorphisms $\sigma \in \Sigma_{G'}$ satisfying, for all $v \in V$,
(i) $\sigma(V) = V$, and

(ii) $\sigma(S_v) = S_{\sigma(v)}$.

This is weaker than Definition 1.2.8, since there we require the condition to hold for all automorphisms.

1.3.9. Example. To illustrate the impact of $G$-symmetry, Figure 1.9 shows a network $G$ and an extension where symmetry relates all processes with each other. $G$-symmetry disregards the automorphism which causes this and considers only those which keep the set of main processes invariant, i.e., the nodes of the original network $G$, thus allowing them to behave differently from the helper processes.

Note that the main processes do not have a direct connection in the extension, which is permitted by Definition 1.3.5 although it will obviously make it impossible for them to synchronize.

Now that we have formalized peer-to-peer networks and the symmetry-preserving extensions which we want to allow, we are ready to prove positive and negative results about feasibility of pairwise synchronization.

1.4 Results

1.4.1 Positive results

First, we state the intuition foreshadowed in Section 1.3.1, namely that CSP\textsubscript{i/o} does allow for symmetric pairwise synchronization in peer-to-peer networks.

1.4.1. Theorem. Let $G = (V, E)$ be a peer-to-peer network. Then $G$ admits a symmetric system pairwise synchronizing $V$ in CSP\textsubscript{i/o}.
Chapter 1. Guarding common knowledge

Proof. A system which at each vertex $v \in V$ runs the program shown in Figure 1.10 is symmetric and pairwise synchronizes $V$. Each process simply waits for each other process in parallel to become ready to send or receive a dummy message, and exits once a message has been exchanged with each other process. □

\begin{verbatim}
for each $w \in V$ do $\text{sync}_w := \text{false}$
$W_{in} := \{w \in V | (w, v) \in E\}$
$W_{out} := \{w \in V | (v, w) \in E\}$
*[
  $\square_{w \in W_{in}} \neg \text{sync}_w \land P_w ? x \rightarrow \text{sync}_w := \text{true}$
  $\square_{w \in W_{out}} \neg \text{sync}_w \land P_w ! 0 \rightarrow \text{sync}_w := \text{true}$
]*

Figure 1.10: The program run at each vertex $v \in V$ in the proof of Theorem 1.4.1.
\end{verbatim}

As a second result, we show that by dropping the topological symmetry requirement for peer-to-peer networks, under certain conditions we can achieve symmetric pairwise synchronizing systems even in CSP$_m$.

1.4.2. Theorem. Let $G = (V, E)$ be a network satisfying only the first two conditions of Definition 1.3.3, i.e., $G$ is strongly connected and directly connected. If $G$ admits a symmetric electoral system and there is some vertex $v \in V$ such that $(v, a) \in E$ and $(a, v) \in E$ for all $a \in V$, then $G$ admits a symmetric system pairwise synchronizing $V$ in CSP$_m$.

Proof. First, the electoral system is run to determine a temporary leader $v'$. When the election has terminated, $v'$ chooses a coordinator $v$ that is directly and in both directions connected to all other vertices, and broadcasts its name. Broadcasting can be done by choosing a spanning tree and transmitting the broadcast information together with the definition of the tree along the tree, as in the proof of [29, Theorem 2.3.1, Phase 2] (the strong connectivity which is required there holds for $G$ by assumption). After termination of this phase, the other processes each send one message to $v$ and then wait to receive commands from $v$ according to which they perform direct communications with each other, while $v$ receives one message from each other process and uses the obtained order to send out the commands.

This can be achieved by running the following program at each process $P_c$, $c \in V$, after having elected the temporary leader $v'$:

- If $c = v'$, choose some $v \in V$ such that $(v, a) \in E$ and $(a, v) \in E$ for all $a \in V$, and broadcast the name $v$; otherwise obtain the broadcast name.

- If $c = v$: 
1.4. Results

- Receive exactly one message from each other process in some non-deterministic order and remember the order:
  \[ W := V \setminus \{v\} \]
  for each \( w \in W \) do \( \text{order}_w := -1 \)
  \( \text{count} := 0 \)
  \[ *[ \square_{w \in W} \text{order}_w = -1 \land P_w ? x \rightarrow \text{order}_w := \text{count} \]
  \( \text{count} := \text{count} + 1 \]

- Issue commands to the other processes according to the obtained order:
  for each \( a, b \in V \setminus \{v\}, a \neq b \) do
    \[ *[ \text{order}_a < \text{order}_b \land (a, b) \in E \rightarrow \]
    \( P_a ! \text{“contact } b\text{”} \)
    \( P_b ! \text{“listen to } a\text{”} \)
    \( \square \text{order}_a \geq \text{order}_b \lor (a, b) \notin E \rightarrow \]
    \( P_a ! \text{“contact } a\text{”} \)
    \( P_b ! \text{“listen to } b\text{”} \]
  \]
done

otherwise (i.e., \( c \neq v \)):
- Send dummy message to \( P_v \):
  \[ P_v ! 0 \]
- Execute the commands from \( v \) until one message has been exchanged with each other process:
  \[ \text{num} := |V \setminus \{c, v\}| \]
  \[ *[ \text{num} > 0 \land P_v ? m \rightarrow \]
  \[ *[ m = \text{“contact } w\text{”} \rightarrow P_w ! 0 \]
  \( \square m = \text{“listen to } w\text{”} \rightarrow P_w ? x \]
  \[ \]
  \[ \text{num} := \text{num} - 1 \]

1.4.3. Example. See Figure 1.11 for an example of a network which admits a symmetric system pairwise synchronizing all its vertices in CSP\(_m\). The fact that the network admits a symmetric electoral system can be established as for [29, Fig. 4]. There the property is used that \( \{1, 2\} \) and \( \{3, 4, 5\} \) are invariant under the network’s automorphism group and the associated processes can thus behave differently; this property is not affected by the edges we have added (note that the edges between the lower nodes are only in one direction).
Chapter 1. Guarding common knowledge

Figure 1.11: A network which by Theorem 1.4.2 admits a symmetric system pairwise synchronizing all its vertices in CSP\(_m\). Note that the connections between vertices 3, 4 and 5 are only in one direction.

This result could be generalized, e.g. by weakening the conditions on \(v\) and taking care that the commands will reach the nodes at least indirectly. Since our main focus is the negative result, we do not pursue this further.

1.4.2 Negative result

In the following we establish the main result of this chapter, saying that, even if we extend a peer-to-peer network \(G\) by helper processes (in a symmetry-preserving way), it is not possible to obtain a network which admits a \(G\)-symmetric system pairwise synchronizing the nodes of \(G\) in CSP\(_m\).

To this end, we derive a contradiction with Theorem 1.2.12 by proving the following intermediate steps (let \(G\) denote a peer-to-peer network and \(G'\) a symmetry-preserving extension):

- **Lemma 1.4.4:** If \(G'\) admits a \(G\)-symmetric system pairwise synchronizing the nodes of \(G\) in CSP\(_m\), it admits a \(G\)-symmetric electoral system in CSP\(_m\).

- **Lemma 1.4.5:** \(G'\) has a non-trivial well-balanced automorphism taken into account by \(G\)-symmetry (i.e., satisfying the two conditions of Definition 1.3.8).

- **Lemma 1.4.7:** We can extend \(G'\) in such a way that there exists a non-trivial well-balanced automorphism (derived from the previous result), \(G\)-symmetry is reduced to symmetry, and admittance of an electoral system is preserved.

1.4.4. **Lemma.** If some symmetry-preserving extension of a peer-to-peer network \(G = (V, E)\) admits a \(G\)-symmetric system pairwise synchronizing \(V\) in CSP\(_m\), then it admits a \(G\)-symmetric electoral system in CSP\(_m\).

**Proof.** The following steps describe the desired electoral system (using the fact that under \(G\)-symmetry processes of nodes \(\in V\) may behave differently from those of nodes \(\notin V\)):

- All processes run the assumed \(G\)-symmetric pairwise synchronization program, with the following modification for the processes in \(\mathcal{P} := \{P_v | v \in V\}\) (intuitively this can be seen as a kind of knockout tournament, similar to the proof of [29, Theorem 4.1.2, Phase 1]):
1.4. Results

- Each of these processes has an additional local variable `winning` initialized to `true`.

- After each communication statement with some other $P \in \mathcal{P}$, insert a second communication statement with $P'$ in the same direction:
  
  * If it was a “send” statement, send the value of `winning`.
  * If it was a “receive” statement, receive a Boolean value, and if the received value is `true`, set `winning` to `false`.

Note that, since the program pairwise synchronizes $V$, each pair of processes associated to vertices in $V$ has had a direct communication at the end of execution, and thus there is exactly one process in the whole system which has a local variable `winning` containing `true`.

- After the synchronization program terminates the processes check their local variable `winning`. The unique process that still has value `true` declares itself the leader and broadcasts its name; all processes set their variable `leader` accordingly. As in the proof of Theorem 1.4.2, broadcasting can be done using a spanning tree. The required strong connectivity is guaranteed by Fact 1.3.7.

1.4.5. Lemma. For any symmetry-preserving extension $G' = (V', E')$ of a peer-to-peer network $G = (V, E)$, there is $\sigma' \in \Sigma_{G'}^{wh} \setminus \{\text{id}\}$ such that $\sigma'(V) = V$ and $\sigma'(S_u) = S_{\sigma'(u)}$ for all $u \in V$.

Proof. Take an arbitrary $\sigma \in \Sigma_{G}^{wh} \setminus \{\text{id}\}$ (exists by Definition 1.3.3) and let $\iota$, to save indices, denote the $\iota_\sigma$ required by Definition 1.3.5. If $\iota \in \Sigma_{G'}^{wh} \setminus \{\text{id}\}$ we are done; otherwise we can construct a suitable $\sigma'$ from $\iota$ by “slicing” orbits of $\iota$ which are larger than the period of $\sigma$ into orbits of that size. See Example 1.4.6 for an illustration of the following proof.

Let $p$ denote the period of $\sigma$ and pick an arbitrary $v \in V$. For simplicity, we assume that $\sigma$ has only one orbit; if it has several, the proof extends straightforwardly by picking one $v$ from each orbit and proceeding with them in parallel.

For all $u \in S_v$ let $p_u := |O_u'|$ and note that for all $t \in O_u'$ we have $p_t = p_u$, and $p_u \geq p$ since $\iota$ maps each $S_v$ to $S_{\sigma(v)}$ and these sets are pairwise disjoint. We define $\sigma' : V' \to V'$ as follows:

$$
\sigma'(u) :=
\begin{cases}
\iota^{p_u-p+1}(u) & \text{if } u \in S_v \\
\iota(u) & \text{otherwise.}
\end{cases}
$$

Now we can show that

- $\sigma'(V) = V$, $\sigma' \neq \text{id}$: Follows from $\iota \mid V = \sigma$ and $p_v = p$ and thus $\sigma' \mid V = \sigma$ (where $f \mid X$ denotes the restriction of a function $f$ to the domain $X$)
Definition 1.3.5. We obtain that, for \( \sigma \) with automorphism \( \iota \), we have that \( \sigma'(O_u \cap S_v) = \iota(O_u \cap S_v) \), thus \( \sigma' \) is a permutation of \( V' \) since \( \iota \) is one. Furthermore, for \( t, u \in S_v \), we have \( \iota^{p_u(p_u - 1)}(t) = t \) and \( \iota^{p_u(p_u - 1)}(u) = u \) and therefore

\[
(\sigma'(t), \sigma'(u)) = (\iota^{p_u-1}(t), \iota^{p_u-1}(u)) = (\iota^{p_u-1}(t), \iota^{p_u-1}(u)),
\]

thus \( \sigma' \) also inherits edge-preservation from \( \iota \).

- \( \sigma'(S_u) = S_{\sigma'(u)} \), \( \sigma' \) well-balanced: The above-mentioned fact that for all \( u \in S_v \) we have \( \sigma'(O_u \cap S_v) = \iota(O_u \cap S_v) \), together with (iv) from Definition 1.3.5 implies that also \( \sigma'(S_u) = S_{\sigma(u)} \) for all \( u \in V \). For all \( v' \in V' \), well-balancedness of \( \sigma \) and disjointness of the \( S_u \) imply that \( \sigma'^{q}(v') \neq v' \) for \( 0 < q < p \). On the other hand, since each orbit of \( \sigma \) has size \( p \) and contains exactly one element from \( S_v \) (namely \( v \)), we have that

\[
\sigma'^{p}(v') = \iota^{(p_u-1)+(p-1)}(v') = \iota^p(v') = \iota^{p_u}(v') = v'.
\]

1.4.6. Example. Consider the extended peer-to-peer network \( G' \) shown in Figure 1.12(a) with automorphism \( \iota_\sigma \) as required by Definition 1.3.5. We illustrate the construction of \( \sigma' \) given in the proof of Lemma 1.4.5.

We have \( p = 2 \) (the period of \( \sigma = \iota_\sigma \mid_{\{1,2\}} \)), and we pick vertex \( v = 2 \). For the elements of \( S_2 \), we obtain \( p_2 = p = 2 \) and \( p_{2a} = p_{2b} = p_{2c} = 6 \) since, e.g., \( O_{2a}^\sigma = \{2a, 1a, 2c, 1b, 2b, 1c\} \). Thus \( \sigma' \) is defined as follows:

\[
\sigma'(u) = \begin{cases} 
\iota(u) & \text{if } u = 2 \\
\iota^5(u) & \text{if } u \in S_2 \setminus \{2\} \\
\iota(u) & \text{if } u \in S_1.
\end{cases}
\]

This \( \sigma' \) is depicted in Figure 1.12(b). All orbits have the same cardinality, namely 2, and the remaining claims of Lemma 1.4.5 are also satisfied.

1.4.7. Lemma. Any symmetry-preserving extension \( G' = (V', E') \) of a peer-to-peer network \( G = (V, E) \) can be extended to a network \( H \) such that

(i) \( \Sigma^{wb}_H \setminus \{\text{id}\} \neq \emptyset \), and

(ii) if \( G' \) admits a \( G \)-symmetric electoral system in \( \text{CSP}_m \), then \( H \) admits a symmetric electoral system in \( \text{CSP}_m \).
1.4. Results

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.12.png}
\caption{An extended peer-to-peer network $G'$ illustrating Lemma 1.4.5.}
\end{figure}

\textbf{Proof.} The idea is to add an “identifying structure” to all elements of $V$, which forces all automorphisms to keep $V$ invariant and map the $S_v$ to each other correspondingly (see Figure 1.13). Formally, let $K = |V'|$ and, denoting the inserted vertices by $i_v \ldots$, for each $v \in V$ let

\[
I_v := \bigcup_{k=1}^{K} \{i_v, k\}
\]

\[
E_v := \{(v, i_v, 1)\} \cup \bigcup_{k=1}^{K-1} \{(i_{v,k}, i_{v,k+1}), (i_{v,k+1}, v)\} \cup \bigcup_{w \in S_v} \{(i_v, K, w)\},
\]

and let

\[
H := (V' \cup \bigcup_{v \in V} I_v, E' \cup \bigcup_{v \in V} E_v).
\]

Now we can prove the two claims as follows.

(i) Let $\sigma \in \Sigma_{G'}^w \setminus \{\text{id}\}$ with $\sigma(V) = V$ and $\sigma(S_v) = S_{\sigma(v)}$ for all $v \in V$ (such a $\sigma$ exists by Lemma 1.4.5). Then we have

\[
\sigma \cup \bigcup_{v \in V} \bigcup_{k=1}^{K} \{i_{v,k} \mapsto i_{\sigma(v),k}\} \in \Sigma_H^w \setminus \{\text{id}\},
\]

and thus $\Sigma_H^w \setminus \{\text{id}\} \neq \emptyset$.

(ii) $H$ is still a symmetry-preserving extension of $G$ via (straightforward) extensions of the $S_v$. The discriminating construction \:\text{notably the fact that the vertices from $V$ now are guaranteed to have more edges than any vertex not in $V$, but still the same number with respect to each other} has the effect that $\Sigma_H$ consists only of extensions, as above, of those $\sigma \in \Sigma_{G'}$ for which $\sigma(V) = V$ and $\sigma(S_v) = S_{\sigma(v)}$ for all $v \in V$. Thus, any $G$-symmetric system with communication graph $H$ is a symmetric system with communication graph $H$. 
Additionally, the set of all $i_{v,k}$ is invariant under $\Sigma_H$ due to the distinctive structure of the $I_v$, thus the associated processes are allowed to differ from those of the remaining vertices. A symmetric electoral system in CSP$_m$ can thus be obtained by running the original $G$-symmetric electoral system on all members of $G'$ and having each $v \in V$ inform $i_{v,1}$ about the leader, while all $i_{v,k}$ simply wait for and transmit the leader information.

Figure 1.13: The network from Figure 1.9, shown with an automorphism disregarded by $G$-symmetry, and the extension given in Lemma 1.4.7 invalidating automorphisms of this kind shown with the only remaining automorphism.

Now we have gathered all prerequisites to prove our main result.

1.4.8. THEOREM. There is no symmetry-preserving extension of any peer-to-peer network $G = (V, E)$ that admits a $G$-symmetric system pairwise synchronizing $V$ in CSP$_m$.

Proof. Assume there is such a symmetry-preserving extension $G'$. Then by Lemma 1.4.4 it also admits a $G$-symmetric electoral system in CSP$_m$. According to Lemma 1.4.7, there is then a network $H$ with $\Sigma_H^{\text{wb}} \setminus \{\text{id}\} \neq \emptyset$ that admits a symmetric electoral system in CSP$_m$. This is a contradiction to Theorem 1.2.12.

1.5 Conclusions

We have provided a formal definition of peer-to-peer networks and adapted a semantic notion of symmetry for process systems communicating via such networks. In this context, we have defined and investigated the existence of pairwise synchronizing systems, which are directly useful because they achieve synchronization, but particularly in our context because they create common knowledge among processes. Focusing on two dialects of the CSP calculus, we have proved the existence of such systems in CSP$_{\text{i/o}}$, as well as the impossibility
of implementing them in CSP, even when we allow additional helper processes. We have also mentioned a recent extension to JCSP to show that, while CSP is less complex and most commonly implemented, implementations of CSP/i/o are feasible and do exist.

A way to circumvent our impossibility result is to remove some requirements. For example, we have provided a construction for non-symmetric systems in CSP. In general, if we give up the symmetry requirement, CSP/i/o can be implemented in CSP, as proved by Bougé [29, p. 197].

Another way is to tweak the definition or the assumptions about common knowledge. Various possibilities have been discussed by Halpern and Moses [73]. By following the eager protocol they propose, common knowledge can eventually be attained, but the trade-off is an indefinite time span during which the knowledge states of the processes are inconsistent. This may not be an option, especially in systems which have to be able to act sensibly and rationally at any time. Alternatively, if messages are guaranteed to be delivered exactly after some fixed amount of time, common knowledge can also be achieved, but this may not be realistic in actual systems. Finally, possibilities to approximate common knowledge are described. Approximate common knowledge or finite mutual knowledge may suffice in settings where the impact decreases significantly as the depth of mutual knowledge increases, as discussed, e.g., by Weinstein and Yildiz [149].

However, if one is interested in symmetric systems and exact common knowledge, as is the case in our Chapters 2 and 3, then these results show that CSP/i/o is a suitable formalism while CSP is insufficient.

Hoare [79] recognized in his initial paper on CSP that the exclusion of output guards reduces expressivity and is programmatically inconvenient. Soon it was deemed technically not justified [22, 33, 64] and removed in later versions of CSP [80, p. 227].

Some existing proposals for implementations of input and output guards and synchronous communication could be criticized for simply shifting the problems to a lower level, notably for not being symmetric themselves or for not even being strictly synchronous in real systems due to temporal imprecision [73]. However, it is often useful to abstract away from implementation issues on the high level of a process calculus or a programming language, as argued in a context similar to ours by Kurki-Suonio [88, Section 10].

We therefore identify JCSP as the most natural platform for the implementation which we discuss in Chapter 3. Since the interaction structures used there generalize our peer-to-peer networks, it is clear that our negative result Theorem 1.4.8 still holds, excluding most other implementations of CSP. Vice versa, JCSP supports broadcasts, i.e., synchronous communication with multiple recipients, and is therefore suitable to implement our positive result Theorem 1.4.1 even in that more general setting.