Department of Computer Science,
University of Otago

Te Whare Wānanga o Otāgo

Technical Report OUCS-2002-01

Keeping secrets with public communication

Author:

Hans van Ditmarsch

Status: accepted for *LOFT 5 conference*

Department of Computer Science,
University of Otago, PO Box 56, Dunedin, Otago, New Zealand

http://www.cs.otago.ac.nz/trseries/

Keeping secrets with public communication

Hans van Ditmarsch*

Abstract

Given some deal of cards, it is possible to communicate your hand to another player without yet another player learning any of your cards. Every solution to this problem consists of a sequence of *safe communications*, an interesting new form of update. Certain unsafe communications turn out to be *unsuccessful updates*. Each communication can be about a set of alternative card deals only, and even about a set of alternatives to your own hand only. We solve a specific cards problem and summarily discuss some combinatorial issues that are not of logical interest. Generalizations appear to be relevant to cryptology.

1 Introduction

Consider the following problem:

> *From a pack of seven known cards two players each draw three cards and a third player gets the remaining card. How can the players with three cards openly (publicly) inform each other about their cards, without the third player learning from any of their cards who holds it?*

This seven cards problem was originally presented at the Moscow Mathematics Olympiad in 2000. A solution and a procedural requirement for it are presented in [MM01], and various solutions are found in [vD01a, vD02].

Note that we assume faultless communication: we do not study transmission protocols, but communication protocols, as used in cryptology and coding theory. Also, besides being public, all announcements are assumed to be truthful.

In the next section we introduce a logic to describe such problems and relevant structures to interpret it in. In section 3 we describe in the defined logic the formal requirements for a solution. In section 4 we present various solutions for this specific seven cards problem. In section 5 we summarily present some generalizations, which are all of combinatorial interest and outside the scope of this contribution.

*Computer Science, University of Otago, New Zealand, hans@cs.otago.ac.nz

2 Logic and structure

A card deal d is a function from cards Q to players N. In a state where no communications have been made, we may assume that it is commonly known that all cards are different, how many cards each player holds, and that players only can see their own cards. Two deals are the same for an agent if he holds the same cards in both, which induces an equivalence relation on deals. The size $\sharp d$ of a deal of cards d lists for each player (in bold) how many cards he holds.

Example 1 (The seven cards problem) *In the seven cards problem, call the players Anne (or a), Bill (or b) and Crow (or c). Anne and Bill are the players holding three cards. Name the cards* $0, 1, 2, 3, 4, 5, 6$*. Assume that the actual card deal is: Anne holds* $0, 1, 2$*, Bill holds* $3, 4, 5$*, and Crow holds 6.*

We informally write $012|345|6$ *for that deal d, its size is* $\mathbf{3}|\mathbf{3}|\mathbf{1}$*, for player a deals* $012|345|6$ *and* $012|346|5$ *are the same, and* $d^{-1}(a) = \{0, 1, 2\}$*.*

Given a set of agents and a set of atoms, an epistemic update language $\mathcal{L}$ with common knowledge [vBDvE$^+$02, vD00] has basic constructs $p, \neg\varphi, (\varphi \wedge \psi), K_n\varphi, C\varphi, [\psi]\varphi$, where $[\psi]$ stands for truthful public update with ψ.[1] We interpret the language on equivalence ($S5$) models $M = \langle W, \sim, V\rangle$ where W is a domain of (factual / world) states, $\sim$ is a function from agents n to equivalence relations $\sim_n$ on W, and V, the valuation, is a function from atoms p to subsets V_p of W. The combination of a model with a factual state is an *information state* (M, w). The interpretation of an update is defined as

$$M, w \models [\psi]\varphi \text{ iff } M, w \models \psi \text{ implies } (M_\psi, w) \models \varphi$$

where M_ψ is the restriction of M, including access $\sim$, to those states where ψ holds, i.e.:

$$\mathcal{D}(M_\psi) = \{v \in \mathcal{D}(M) \mid M, v \models \psi\}$$

The interpretation of other constructs is standard [FHMV95]. Slightly abusing the language, when φ is the update formula, we call $[\varphi]$ the update. Some simple properties and concepts for update logic are (for – elementary – proofs of Proposition 1 and 2, see the appendix):

Proposition 1 (Combining two updates) *For all formulas in the language,* $[\varphi \wedge [\varphi]\psi]\chi$ *is equivalent to* $[\varphi][\psi]\chi$*.*

Definition 1 (Unsuccessful update) *Given an information state* (M, w)*, an unsuccessful update is a formula* φ *such that* $M, w \models [\varphi]\neg\varphi$*.*

The best-known example of an unsuccessful update is 'nobody knows whether (s)he is muddy' in the Muddy Children problem, in the last round [FHMV95]. The term is introduced in [Ger99] and used in [vD00]. Updates with common knowledge are always successful:

[1] One may allow sequences of and nondeterministic choice between updates as well, defined by abbreviation as, respectively, $[\varphi\ ;\ \psi]\chi :\leftrightarrow [\varphi][\psi]\chi$ and $[\varphi \cup \psi]\chi :\leftrightarrow [\varphi]\chi \wedge [\psi]\chi$.

Proposition 2 (Common knowledge updates are successful) *For all formulas in the language,* $[C\varphi]C\varphi$ *is valid.*

For card deals, the agents are the players, and atoms q_n describe that player n holds card q. The information of the players in a given card deal d is represented by an information state $(I_{\sharp d}, d)$ (in the precise sense that any other information state representing the same information is bisimilar to it), where the domain of $I_{\sharp d}$ consists of all deals of the same size as d, where the equivalences $\sim_n$ are induced by n holding the same cards in different deals, and where the valuation $V_{d'}$ of atoms in a factual state corresponds to the deal d' of the same size as d, that it represents. The (atomic) description δ_d of a deal d is the conjunction of atoms or their negations according to V_d, and the description δ^n_d of the hand of n, is the conjunction of the atoms involving agent n. For details, see [vDvdHK02].

Example 2 $(I_{\sharp 012|345|6}, 012|345|6)$ *is the initial information state for the seven cards problem. The atomic description of that deal is* $\delta_{012|345|6} := 0_a \wedge 1_a \wedge 2_a \wedge \neg 3_a \wedge ... \wedge \neg 0_b \wedge ...$, *and the hand of player a is described by* $\delta^a_{012|345|6} := 0_a \wedge 1_a \wedge 2_a \wedge \neg 3_a \wedge \neg 4_a \wedge \neg 5_a \wedge \neg 6_a$. *For* $\delta^a_{012|345|6}$ *we also write* 012_a, *etc. Some typical formulas satisfied in the initial information state* $(I_{\sharp 012|345|6}, 012|345|6)$ *are:* $K_a 0_a$ *(Anne knows that she holds card 0),* $K_b \neg K_a 3_b$ *(Bill knows that Anne doesn't know that he holds card 3), and* $C \bigvee_{i \neq j \neq k \in \{0,\cdots,6\}} K_a ijk_a$ *(It is common knowledge that Anne knows her own hand of cards).*

We are now ready to do battle with the seven cards problem.

3 Safe communications

The constraints that (at least) have to be satisfied are: Anne knows Bill's cards (aknowsbs), Bill knows Anne's cards (bknowsas), and Crow doesn't know any of Anne's or Bill's cards (¬cknowsany).

Definition 2 (Necessary requirements) *Let* $d : Q \to N$ *be a card deal involving at least three players,* $a, b \in N$, *and* $O := N \setminus \{a, b\}$ *(for* Others*). Necessary requirements for an exchange of secrets are:*

$$\begin{array}{ll} \mathsf{aknowsbs} & \bigvee_{\sharp d' = \sharp d} K_a \delta^b_{d'} \\ \mathsf{bknowsas} & \bigvee_{\sharp d' = \sharp d} K_b \delta^a_{d'} \\ \mathsf{cknowsany} & \bigvee_{q \in Q \setminus d^{-1}(O)} \bigvee_{c \in O} (K_c q_a \vee K_c q_b) \end{array}$$

Further, post := aknowsbs ∧ bknowsas ∧ cknowsany. These requirements are necessary, but not sufficient. We illustrate their weakness by means of some examples, that also uncover other phenomena.

First consider the sequence:

Anne says: "I don't have 6" and Bill says: "Neither have I." (i)

After the first announcement cknowsany holds, and after both announcements post holds. This is not a good solution, because the underlying protocol that Anne apparently executes might as well have resulted in Anne saying that she doesn't have 4, after which Crow knows that, so cknowsany holds. We will come back to this later.

The bad solution in [MM01] is:

> *Anne says "If you don't have* 0*, then I have* $\{0,1,2\}$*" and Bill says "If you don't have* 3*, then I have* $\{3,4,5\}$*".* (ii)

Indeed, update of the current information state $(I_{\mathbf{3|3|1}}, 012|345|6)$ with $[\neg 0_b \to 012_a]$ and subsequently with $[\neg 3_a \to 345_b]$ results in an information state where Crow cannot distinguish the actual deal of cards $012|345|6$ from the deal $345|012|6$ (and various other deals), so that $\neg$cknowsany holds; aknowsbs and bknowsas also hold. Is this a fair treatment of the information? The announcements have been processed as if they have been made by an *insider*, a virtual player who can look in everybody's cards, or differently said, a player whose accessibility on the information state is the identity relation.

One should of course use that Anne *knows* what she says, which makes her announcement more informative than that of an insider. As it is common knowledge that Anne initially doesn't know any of Bill's cards, she can only truthfully announce "If you don't have 0, then I have $\{0,1,2\}$", if she actually holds $\{0,1,2\}$. In other words: update $[K_a(\neg 0_b \to 012_a)]$ can only be executed in a state where 012_a holds, therefore after that update c knows all of a's cards, so definitely cknowsany is true. A further update $[K_b(\neg 3_a \to 345_b)]$ results in a state where it is common knowledge that $012|345|6$ is the deal of cards.

It is obvious that players' announcements should be based on their knowledge. It is less obvious why the following is also a bad solution:

> *Anne says "I have* $\{0,1,2\}$*, or I haven't got any of these cards" and Bill says "I have* $\{3,4,5\}$*, or I haven't got any of these cards".* (iii)

After an update of $(I_{\mathbf{3|3|1}}, 012|345|6)$ with first $[K_a(012_a \vee (\neg 0_a \wedge \neg 1_a \wedge \neg 2_a))]$ $(=: [K_a\mathsf{first}])$ and then $[K_b(345_b \vee (\neg 3_b \wedge \neg 4_b \wedge \neg 5_b))]$, it still holds that both $012|345|6$ and $345|012|6$ are the same for Crow, so $\neg$cknowsany holds. Further, unlike in (i), Anne's announcement seems 'safe' in (iii) in the sense that no other execution of the underlying protocol would have resulted in Crow learning any of her cards. However, *Crow doesn't know that*, and, surprisingly, Crow may use *that* to derive further knowledge: it may reason from the assumption that Anne wouldn't dare making an unsafe communication. To be precise: Anne knows that after her announcement Crow doesn't know any of her cards, so we do not just update with $[K_a\mathsf{first}]$ but with $[K_a\mathsf{first} \wedge [K_a\mathsf{first}]\neg\mathsf{cknowsany}]$. And in all deals d' that are the same for Crow as $012|345|6$ after update $[K_a\mathsf{first}]$, announcement of first *could* have been informative for Crow, so $\neg$cknowsany doesn't hold in d' in that information state, so $K_a\mathsf{first} \wedge [K_a\mathsf{first}]\neg\mathsf{cknowsany}$ doesn't hold in $(I_{\mathbf{3|3|1}}, d')$, so updating with *that* we end up with the singleton information state that consists of $012|345|6$ only, where Crow knows all of Anne's

cards! We now have:

$$I_{\mathbf{3|3|1}}, 012|345|6 \models [K_a \mathsf{first} \wedge [K_a \mathsf{first}] \neg \mathsf{cknowsany}] \mathsf{cknowsany}$$

This is an interesting new type of unsuccessful update. It is apparently not safe enough that Anne only makes announcements where Crow doesn't get to know any of her cards: Crow may use *exactly* that to derive Anne's cards. It illustrates as well that post is not a sufficiently strong postcondition to require for a solution of the cards problem. We should instead require common knowledge of it: $C\mathsf{post}$. And on top of that, *common knowledge* of Crow's ignorance must be an invariant under the execution of any communication of a protocol. Otherwise, (i) would be a solution of the problem, as $C\mathsf{post}$ holds after it, but after the first of its two announcements $\neg\mathsf{cknowsany}$ holds but $C\neg\mathsf{cknowsany}$ doesn't hold.

We summarize our results:

Definition 3 (Communicative updates)

$[\varphi]$	*announcement of φ (by an outsider)*
$[K_n\varphi]$	*communication of φ (by player n)*
$[K_n\varphi \wedge [K_n\varphi]C\neg\mathsf{cknowsany}]$	*safe communication of φ (by player n)*

By proposition 1, a safe communication $[K_n\varphi \wedge [K_n\varphi]C\neg\mathsf{cknowsany}]$ is equivalent to the sequence of two updates $[K_n\varphi][C\neg\mathsf{cknowsany}]$. Also, after any sequence of safe communications $C\neg\mathsf{cknowsany}$ holds. This is because

$$M, w \models [K_n\varphi \wedge [K_n\varphi]C\neg\mathsf{cknowsany}]C\neg\mathsf{cknowsany}$$

is equivalent to

$$M, w \models [K_n\varphi][C\neg\mathsf{cknowsany}]C\neg\mathsf{cknowsany}$$

which follows from

$$M_{K_n\varphi}, w \models [C\neg\mathsf{cknowsany}]C\neg\mathsf{cknowsany}$$

which is an instance of proposition 2.

Merely requiring that aknowsbs and bknowsas hold after a sequence of announcements may be dangerous, for the same reason as for $\neg$cknowsany: if this is not commonly known, one of a or b making this information public may change the information state into one where some others have learnt one of a's or b's cards.

If in (iii) the announcements are interpreted as communications but not as safe communications, in the resulting information state aknowsbs and bknowsas both hold but are not commonly known: if Anne makes aknowsbs public (update [aknowsbs]), then Crow can derive the entire deal of cards! In order to reach a 'stable solution', where no player can learn from other players announcing their knowledge of the requirements, we have to require that *common knowledge* of aknowsbs and bknowsas is reached:

Definition 4 (Exchange of secrets) *Given deal d of cards (for at least three players), an* exchange of secrets *between two players a and b is a finite sequence $[\pi]$ of safe communications $[\pi_1], \cdots, [\pi_n]$ by a and/or b such that $I_{\sharp d}, d \models C\mathsf{post}$.*

An even different perspective appears: Given that the information state $(I_{\sharp d}, d)$ has a characteristic formula $\delta_d \wedge C\mathsf{kgames}$, where kgames is a description of the model $I_{\sharp d}$ in multiagent epistemic logic *without* update operators [vDvdHK02], an exchange of secrets π corresponds to the validity of the *epistemic correctness statement*:

$$(\delta_d \wedge C\mathsf{kgames}) \rightarrow [\pi]C\mathsf{post}$$

The sufficient requirements may correspond to a procedural requirement that is given in [MM01]. The authors have provided me with a partial translation of their original work, in Russian [Mak01]. The infinitary flavour of what they define as a 'protocol' possibly corresponds to the fixed-point character of common knowledge.

3.1 Normal form of safe communications

So a safe communication of φ is an update $[K_n\varphi \wedge [K_n\varphi]C\neg\mathsf{cknowsany}]$. What can we say about φ itself? As we haven't put any restrictions on φ, anything appears to go: 'I have one of the cards d, e, and f', 'My hand is one of $\{0,1,2\}$ and $\{0,3,4\}$ and ...', 'The deal of cards is either 012|345|6 or 345|012|6', 'I don't know the cards of player b yet', 'If I have card 2, then you have card 4', etc. For the information states we consider, such announcements can be greatly standardized:

Proposition 3 (Alternative deals) *In any information state resulting from updates in the initial information state for a deal of cards, every announcement is equivalent to one about alternative deals.*

Proof. Let φ be an announcement in the initial information state $(I_{\sharp d}, d)$. As all states d' in $(I_{\sharp d}, d)$ represent *different* card deals, it holds that $(I_{\sharp d}, d) \models \varphi \leftrightarrow \bigvee_{d' \in (I_{\sharp d})_\varphi} \delta_{d'}$ (where, as before, $\mathcal{D}((I_{\sharp d})_\varphi) = \{d \in I_{\sharp d} \mid I_{\sharp d}, d \models \varphi\}$). In other words, φ has the same informational content as the announcement "my deal is one of the set $(I_{\sharp d})_\varphi$". By (natural) induction, we can extend any number of such announcements with another one. ⊣

Proposition 4 (Alternative hands) *In any information state resulting from updates in the initial information state for a deal of cards, every communication is equivalent to an announcement about alternative hands for that player.*

Proposition 4 and its proof, that is omitted, are by Ben Handley. The essential part of the (adaptation of the) proof is the following. Because players only say what they know (to be true), every announcement by some player is interpreted as a *game action* in the sense of [vD01b]. I.e., its denotation is a set of deals that is a union of $\sim_n$ equivalence classes for that player n, for the current information state.

We continue with the presentation of solutions for the seven cards problem.

4 Solutions for the seven cards problem

Given that we now know the constraints, what are the solutions (exchanges of secrets)? We know four. The part for Anne varies, for Bill it always suffices to announce Crow's card, or alternatively to copy the protocol (*any* protocol) of Anne. We leave out the details:

- MOD
  Anne announces the sum of her cards modulo 7 (in this case: '3').
- SUM
  Anne renames the cards $1, 2, 3, 4, 5, 6, 7$ such that the sum of her hand is 12.
- DNF
  Anne says: "My hand is one of 012, 034, 056, 135, 146, 236, 245."
- CNF
  Anne says: "I hold a card from all of: 012, 034, 056, 135, 146, 236, 245".

In SUM, Anne is doing this *openly*. It will be common knowledge that the sum of Anne's cards is 12. For deal 012|345|6 she could (e.g.) have said: "rename 0 to 3 and 1 to 7 and keep the rest as it is". In CNF, read 'at least one card' for 'a card'.

For details of MOD, see [MM01, vD02]. The relation between MOD and SUM is obvious. However, SUM *only* works for sum 12, whereas MOD works for any sum modulo 7, not just sum 5. From proposition 4 follows that CNF must be just as informative in the given information state as some alternative announcement about alternative hands: DNF is that alternative. In this particular case DNF and CNF are even logically equivalent. DNF (CNF) is just one of twelve executions of a nondeterministic protocol. The seven triples can be seen as corresponding to all seven lines of a projective geometric plane for seven points, as long as one line corresponds to the actual hand. The symmetry apparent in DNF is an automorphism property of that plane. MOD can *not* be extended to DNF (i.e. there are *not* two appropriate triples), and DNF cannot be weakened by adding *any* single other hand of Anne (such as 345, to give an example that may puzzle the reader). Each such addition will result in Crow deriving the entire deal of cards.

5 Combinatorics and generalizations

Given an arbitrary deal of cards, can two players communicate their hands without the remaining players getting to know any of their cards, or not? Although there are some remaining issues of logical interest, this is a largely combinatorial problem (apparently related to 'block design' [GGL96]) that can be studied entirely independently from the declarative logical constraints. Those mainly

served the purpose of analyzing puzzling (because of the unsuccessful updates involved) non-solutions.

Sizes of deals for which there is an exchange of secrets (between the two players with the largest number of cards) include **4|2|1** and **4|7|2**. If there is a solution for size **x|y|z**, then there is one for size **x|y|z-1**. In the second case, the first player introduces a virtual extra card for the third player.

A general treatment is relevant for cryptology. E.g. in public key cryptography, others cannot discover the secrets that are exchanged, because it is *too difficult* to solve a large prime factorization. Here, other players cannot discover the secrets that are exchanged, because it is *impossible*.

A further generalization is the following. Given a distributed (interpreted) system [FHMV95], can two agents communicate their local state to each other without the remaining agents getting to know those local states? Note that the postcondition is slightly weaker than for the cards problem: we may now learn *some* of the cards of the communicating players, but not *all* of them. E.g., in 012|345|6, Anne announcing that she has card 0 is a safe communication. But what should she or Bill say next?

We conclude with some tentative results and conjectures:

Proposition 5 (Decision procedure for an exchange of secrets) *Given a deal of cards and two players, it can be determined whether there is an exchange of secrets.*

Proof. Let $d \in N^C$ be a deal of cards, let $a, b \in N$. The following crude algorithm computes whether there exists an exchange of secrets (between a and b); all exchanges of secrets, if there are any, are found this way:

Start with the current set of relevant deals equal to all deals of that size: $D := \mathcal{D}(I_{\sharp d})$. For both player a and player b, for every subset $D' \subseteq D$ containing d that is a union of $\sim_a$ equivalence classes (or, respectively, $\sim_b$ equivalence classes), check whether $I_{\sharp d}{\restriction}D', d \models C\neg\mathsf{cknowsany}$. If not, discard that subset. If so, check whether $I_{\sharp d}{\restriction}D', d \models C(\mathsf{aknowsbs} \wedge \mathsf{bknowsas})$. If so, we have found an exchange of secrets. If not, set $D := D'$ and repeat the procedure. ⊣

Conjecture 6 (Completion) *If an exchange of secrets exists, every sequence of safe communications can be extended to an exchange of secrets.*

Conjecture 7 (One round solution) *If an exchange of secrets exists, there is one consisting of only two safe communications (namely one by each of the involved players).*

There is some suggestive evidence that conjecture 7 might hold: if any update is allowed, and secrecy is no issue, n agents can pool their distributed knowledge in a maximum of n communications. In the case of card deals this may be done by each but the last player saying what their cards are (which makes $n-1$ communications).

These combinatorial issues are still under investigation. Work in progress by and with Ben Handley is foreseen to be completed at some later stage.

References

[FHMV95] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning about Knowledge*. MIT Press, Cambridge MA, 1995.

[Ger99] J.D. Gerbrandy. *Bisimulations on Planet Kripke*. PhD thesis, University of Amsterdam, 1999. ILLC Dissertation Series DS-1999-01.

[GGL96] R. L. Graham, M. Grotschel, and L. Lovasz, editors. *Handbook of Combinatorics*. MIT Press, Cambridge MA, 1996.

[Mak01] K. Makarychev. Logicheskie voprosy peredachi informacii (logical issues of information transmission). Master's thesis, Moscow State University, 2001. Diplomnaja rabota, part 1.

[MM01] K.S. Makarychev and Yu.S. Makarychev. The importance of being formal. *Mathematical Intelligencer*, 23(1):41–42, 2001.

[vBDvE+02] J.F.A.K. van Benthem, P. Dekker, J. van Eijck, M. de Rijke, and Y. Venema. *Logic in Action*. ILLC, Amsterdam, 2002.

[vD00] H.P. van Ditmarsch. *Knowledge games*. PhD thesis, University of Groningen, 2000. ILLC Dissertation Series DS-2000-06.

[vD01a] H.P. van Ditmarsch. Killing cluedo. *Natuur & Techniek*, 69(11):32–40, 2001.

[vD01b] H.P. van Ditmarsch. Knowledge games. *Bulletin of Economic Research*, 53(4):249–273, 2001.

[vD02] H.P. van Ditmarsch. Oplossing van het mysterie (solution of the murder mystery). *Natuur & Techniek*, 70(2):17, 2002.

[vDvdHK02] H.P. van Ditmarsch, W. van der Hoek, and B.P. Kooi. Descriptions of game states. In I. van Loon, G. Mints, and R. Muskens, editors, *Proceedings of LLC9 (2000)*, Stanford, 2002. CSLI Publications. To appear.

Appendix: Proofs

Proof of Proposition 1: For all formulas in the language, $[\varphi \wedge [\varphi]\psi]\chi$ is equivalent to $[\varphi][\psi]\chi$.

Proof. Let M, w be arbitrary. Then:

$$
\begin{array}{l}
M, w \models [\varphi \wedge [\varphi]\psi]\chi \\
\Leftrightarrow \\
M, w \models \varphi \text{ and } M, w \models [\varphi]\psi \text{ implies } M_{\varphi \wedge [\varphi]\psi}, w \models \chi \\
\Leftrightarrow \\
M, w \models \varphi \text{ and } M_\varphi, w \models \psi \text{ implies } M_{\varphi \wedge [\varphi]\psi}, w \models \chi \\
\Leftrightarrow \qquad\qquad\qquad\qquad \text{as } M_{\varphi \wedge [\varphi]\psi} = (M_\varphi)_\psi, \text{ see below} \\
M, w \models \varphi \text{ and } M_\varphi, w \models \psi \text{ implies } (M_\varphi)_\psi, w \models \chi \\
\Leftrightarrow \\
M, w \models \varphi \text{ implies } M_\varphi, w \models [\psi]\chi \\
\Leftrightarrow \\
M, w \models [\varphi][\psi]\chi
\end{array}
$$

We have that $M_{\varphi \wedge [\varphi]\psi} = (M_\varphi)_\psi$, since:

$$
\begin{array}{l}
\mathcal{D}(M_{\varphi \wedge [\varphi]\psi}) \\
= \\
\{v \mid M, v \models \varphi \wedge [\varphi]\psi\} \\
= \\
\{v \mid M, v \models \varphi \text{ and } (M, v \models \varphi \text{ implies } M_\varphi, v \models \psi)\} \\
= \qquad\qquad v \in \mathcal{D}(M_\varphi) \text{ presupposes that } M, v \models \varphi \\
\{v \mid M_\varphi, v \models \psi\} \\
= \\
\mathcal{D}((M_\varphi)_\psi)
\end{array}
$$

⊣

Proof of Proposition 2: For all formulas in the language, $[C\varphi]C\varphi$ is valid.

Proof. Define $\sim_N := (\bigcup_{n \in N} \sim_n)^*$, and $M^w_{\sim_N}$ as the $\sim_N$-generated submodel of M with point w (i.e. with $\mathcal{D}(M^w_{\sim_N}) := \{v \in \mathcal{D}(M) \mid v \sim_N w\}$). Obviously, for all formulas and states, $M, w \models \psi$ iff $M^v_{\sim_N}, w \models \psi$.

Let M, w be arbitrary, and suppose $M, w \models C\varphi$. Let $v \sim_N w$. Then $M, v \models C\varphi$ (using the validity of $C\varphi \to CC\varphi$), and therefore $\mathcal{D}(M^w_{\sim_N}) \subseteq \mathcal{D}(M_{C\varphi})$. Also $M, v \models \varphi$, so $M^v_{\sim_N}, v \models \varphi$, and also $M_{C\varphi}, v \models \varphi$. As $v \in M_{C\varphi}$, it follows that $M_{C\varphi}, w \models C\varphi$. We have now shown that $M, w \models C\varphi$ implies $M_{C\varphi}, w \models C\varphi$, in other words: $M, w \models [C\varphi]C\varphi$. As M and w were arbitrary, it follows that $\models [C\varphi]C\varphi$. ⊣