Universiteit Utrecht

Artificial Intelligence

7.5 ECTS

Modal Circuits

Author:
Tjeu Hendriks

Student number:
3974685

Supervisor:
Benjamin G. Rin

Second corrector:
Rosalie Iemhoff

July 7, 2017

Summary

It is well known that Boolean logic circuits are functionally equivalent to propositional logic. This thesis develops an extension of Boolean logic circuits that are functionally equivalent to modal logic with Kripke semantics. We call these circuits *modal circuits*. We first define how modal circuits work with a series of definitions. Then we prove that modal circuits are functionally equivalent to modal logic with Kripke semantics. Using these circuits, we also define a modal analogue of Boolean circuit satisfiability, called *MCSAT*. We show that the well known PSPACE-complete problem of modal satisfiability (*MSAT*) is polynomial time reducible to *MCSAT*.

Contents

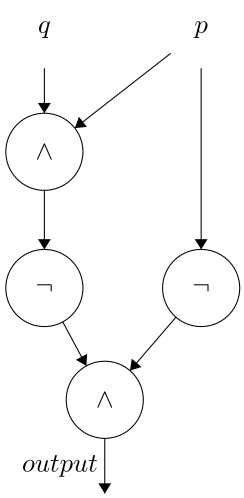
Part I
Introduction

In 1838 George Boole[1] began to develop a system what can be found in his book "An Investigation of the laws of thought".[1] This system is now known as Boolean logic. In 1938 Claude Shannon[2] expanded on this idea by developing a theoretical system in which electrical switches could represent Boolean logic.[2] Nowadays, circuits using these switches are known as Boolean circuits. We now understand the definition of a Boolean circuit as described in Micheal Sipser's book "Introduction to the Theory of Computation"[3]. In this book, circuits are represented as follows: "*a collection of gates and inputs connected by wires. Cycles aren't permitted. Gates take three forms: AND gates, OR gates, and NOT gates.*"[3]

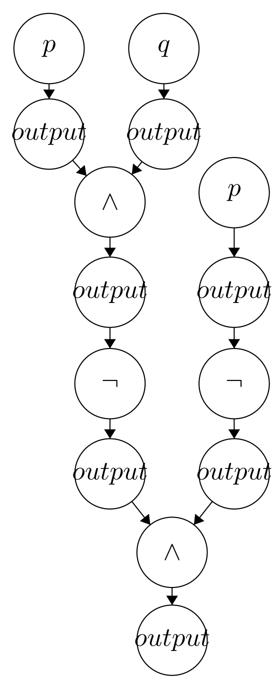
In part II, we will look at an addition to these Boolean circuits. These extended circuits will be called modal circuits. The addition will allow modal circuits to represent modal logic as well as Boolean logic. For the modal circuits, we shall only define the $\neg$ (NOT) gate, the $\wedge$ (AND) gate and the $\Box$ (BOX) gate. These three connectives are a functionally complete set for modal logic. In other words, by combining these three connectives you can create all other connectives, e.g. $\diamond$ is the same as $\neg\Box\neg$. In this paper, we will present modal circuits with "output nodes" between the gate nodes as an aid for presentation.

Example 1. *Let $\neg(p \wedge q) \wedge \neg p$ be a propositional formula. Then the Boolean circuit and the modal circuit will be displayed like this:*

Boolean circuit:



modal circuit:



[1]Boole, George. An Investigation of the Laws of Thought on Which Are Founded the Mathematical Theories of Logic and Probabilities. p.48 - p.58.
[2]Shannon, Claude E. "A Symbolic Analysis of Relay and Switching Circuits." Electrical Engineering 57.12. p.475.
[3]Sipser, Michael. Introduction to the Theory of Computation. p.380.

There is one difference between the structures. Between every gate and at the root of the structure there exists an *output* node. This difference will not affect the workings of the circuit. The *output* nodes exist as placeholders for values of sub circuits of modal circuits.

The $\Box$ gate is the only difference that will have functional consequences. Because of the $\Box$ gate, the inputs of the modal circuits will have to represent Kripke models as defined by Saul Kripke[4][4]. The inputs cannot only be a 1 or a 0 as they would be in Boolean circuits. Because every atomic proposition has its own valuation for every world in a Kripke model, the inputs of a modal circuit have to be able contain multiple valuations per input node. These inputs will be presented as nested sets of valuations calculated with an algorithm to represent Kripke models. This algorithm is described in part II, section 2. Outputs of modal circuits will have to represent the truth value of a modal formula for a specific world. We will also present these outputs as nested sets of truth values. Commonly this will be a singleton, since we are most of the time interested in the valuation of a formula in one world.

Throughout part II there are a few definitions of algorithms used for modal circuits. To explain the use of these algorithms, a running example will be given right after these algorithms.This running example will use the modal formula $\neg\Box(p \wedge \Box q)$.

In part III, we will look at the connection between modal circuits and modal logic. We will first define what the satisfiability of modal circuits entails. Then we will prove that the modal satisfiability problem is polynomial time reducible to the satisfiability problem for modal circuit.[5] Because Michael Fischer and Richard Ladner[5] have proven in 1979 that the modal satisfiability problem is PSPACE-complete, we will prove that certain modal circuit satisfiability problems are PSPACE-hard.[6]

In part IV, we will reflect on this paper. We will discuss the consequences of this paper and give some problems considering modal circuits that are not solved in this paper.

In this paper, we will see quite a few conventions. p and q are used as atomic propositions. ϕ, ψ and χ are used as modal formulas. α, β and γ are used as propositional formulas. In this paper, you will sometimes see a symbol with a subscript i after the use of an enumeration. Then the i denotes and element of that enumeration. This can be seen in example 2.

Example 2. *In the sentence "$\langle \mathcal{I}_1, ..., \mathcal{I}_n \rangle$ is a well formed input set iff $\mathcal{I}_1, ..., \mathcal{I}_n$ are well formed input sets such that each non-empty $\mathcal{I}_i$ has the same rank for $n \geq 0$." [7] $\mathcal{I}_i$ is an element of $\mathcal{I}_1, ..., \mathcal{I}_n$.*

Throughout this paper we will see different uses of the word "correspondence". First, modal formulas can correspond to modal circuits. This is the same correspondence as in example 1 where $\neg(p \wedge q) \wedge \neg p$ corresponds to the modal circuit presented in the example. Second, sets of worlds and sets of values can correspond to models. This means that a certain model is used in the creation of a set of worlds or a set of valuations. How this creation happens will be defined in the paper. Finally, sets of worlds can correspond to sets of valuations. This correspondence will be formally defined in the paper.

[4] Kripke, Saul A. "Semantical Analysis of Modal Logic I Normal Modal Propositional Calculi." Zeitschrift Für Mathematische Logik Und Grundlagen Der Mathematik 9.5-6. p.68 - p.69

[5] The modal satisfiability problem is defined like this: Given a modal formula ϕ, does there exists a model and a world in that model where ϕ is True;
The definition of polynomial time reducibility is defined in Sipser's book "Introduction to the Theory of Computation" on page 300

[6] Fischer, Michael J., and Richard E. Ladner. "Propositional Dynamic Logic of Regular Programs." Journal of Computer and System Sciences 18.2. p.209

[7] As seen on page 4. of this paper

Part II
Formal definition of modal circuits

1 Definition well formed modal circuits

In this section we will first define the valuation function $\mathcal{V}$. Secondly we will define what a *well formed input set* is. Finally we will use these two definitions to define what a *well formed modal circuit* is.

Definition 1. *The* ***valuation function*** $\mathcal{V} : \mathcal{L} \rightarrow \{True, False\}$ *is the function that evaluates propositional formulas and returns True or False depending on the truth value of the formula.*[8]

Definition 2. *A* ***well formed input set*** $\mathcal{I}$ *is recursively defined as follows:*

1. $\langle \mathcal{V}(p_1), ..., \mathcal{V}(p_n) \rangle$ *is a well formed input set iff* $p_1, ..., p_n$ *are atomic propositions for* $n \geq 0$.
2. $\langle \mathcal{I}_1, ..., \mathcal{I}_n \rangle$ *is a well formed input set iff* $\mathcal{I}_1, ..., \mathcal{I}_n$ *are well formed input sets such that each non-empty* $\mathcal{I}_i$ *has the same rank for* $n \geq 0$.[9]
3. *An input set is well formed iff it follows the rules above.*

Let $\mathfrak{I}$ *denote the class of all well formed input sets.*

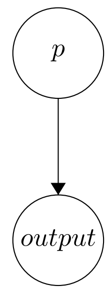
Example 3. *Let* p, q, r *be atomic propositions. Then examples of well formed input sets are*
$\langle \mathcal{V}(p), \mathcal{V}(q), \mathcal{V}(r) \rangle$
$\langle \langle \mathcal{V}(p), \mathcal{V}(q) \rangle, \langle \mathcal{V}(q), \mathcal{V}(r) \rangle, \langle \rangle \rangle$
$\langle \langle \langle \mathcal{V}(r) \rangle, \langle \rangle \rangle, \langle \langle \mathcal{V}(p), \mathcal{V}(q), \mathcal{V}(r) \rangle \rangle, \langle \rangle \rangle$

Input sets are the inputs for a modal circuit, just as 1's and 0's are inputs for Boolean circuits. Since, in a Kripke model, every atomic proposition can have a different valuation for every world, the inputs for modal circuits have to be able to contain different valuations. This problem is solved by having sets of valuations for every atomic proposition. The nesting of input sets represents the structure of a Kripke model in relation to the modal circuit. The algorithm to create input sets representing Kripke models is defined in section 2.

A **well formed modal circuit** is defined recursively as a directed vertex-labeled tree-like graph. In this graph, we only have interest in the labeling of the leaves of the tree. We will call these leaves input nodes. The labels of the input nodes will be atomic propositions. Other nodes are divided into two types: gate nodes and output nodes. Gate nodes are labeled by $\neg$, $\wedge$ and $\Box$. Output nodes are labeled *output*. The root of the tree is called the final output node. Note that two or more input nodes can have the same labeling. The modal circuits will now be recursively defined as follows:

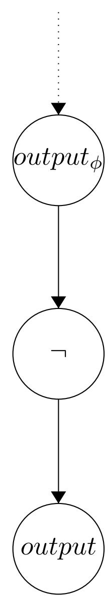
[8] In this paper, we will use $\mathcal{L}$ as the class of all propositional formulas
[9] Here we understand rank in the standard set-theoretic way, except with $\langle , \rangle$ instead of $\{ , \}$

1. Atomic propositions:



is a well formed modal circuit iff p is a label of an input node.

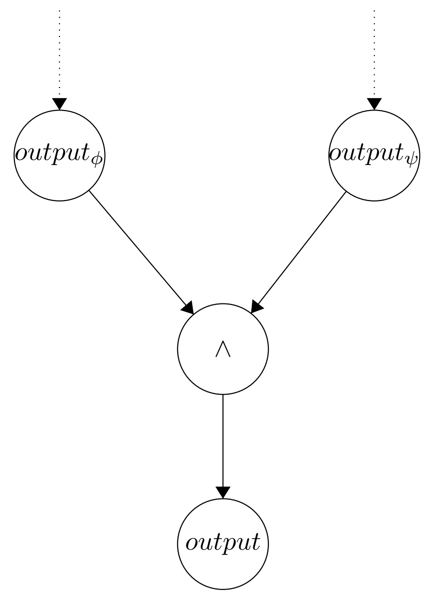
2. Negations:



is a well formed modal circuit iff the node labeled $output_\phi$ is an output node in a well formed modal circuit. [10]

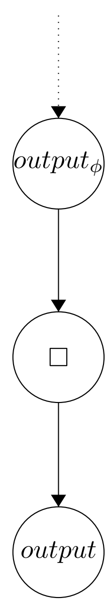
[10] Throughout the paper, the dotted arrow will be used as an abbreviation for the rest of the modal circuit that is connected to the node the arrow points at

3. Conjunctions:



is a well formed modal circuit iff the node labeled $output_\phi$ and the node labeled $output_\psi$ are output nodes in well formed modal circuits.

4. Box operators:



is a well formed modal circuit iff the node labeled $output_\phi$ is an output node in a well formed modal circuit.

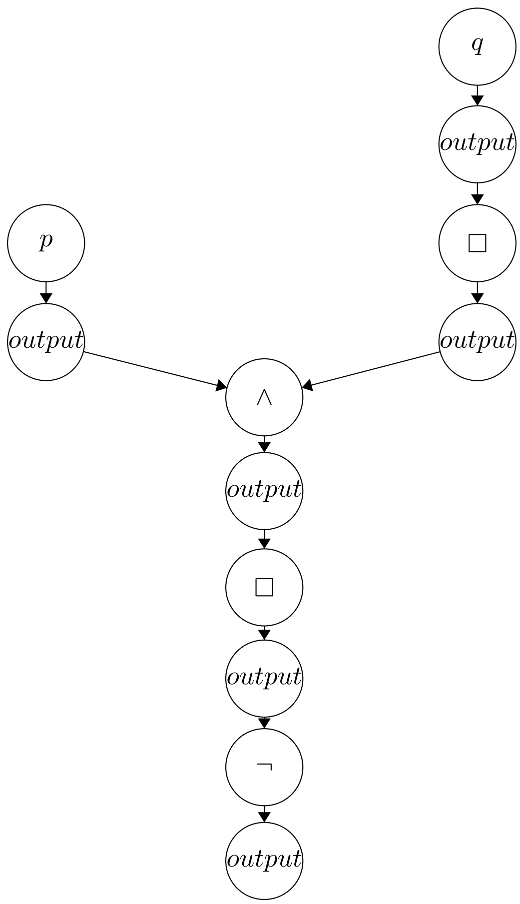
5. For every output node it holds that the output node is accessed by exactly one node.
6. A modal circuit is well formed iff every node in the modal circuit follows the rules above.

Definition 3. *$\mathcal{C}_\phi$ is a modal circuit corresponding to a modal formula ϕ.*

Definition 4. *Let ϕ' be any sub formula of ϕ. Then we define that $\mathcal{N}_{\phi'}$ is the final output node of the modal sub circuit corresponding to ϕ'.*

Converting modal formulas into modal circuits is done in the same way as propositional formulas are converted to Boolean circuits (i.e., the circuit is isomorphic to the formula's syntactic tree). Note that, as in the Boolean case, there is a bijection between modal circuits and modal formulas.

Running example 1. *Let $\neg\Box(p \wedge \Box q)$ be a modal formula. Then the modal circuit corresponding to this formula is:*



2 Creating input sets representing models

In this section, we define the notion of *world sets* and two functions, $\textcircled{\blacksquare}$ and $\mathcal{SET}_{\mathcal{M}}$. Then we define the rules for creating input sets using this notion and these functions. Throughout this paper, let $\mathcal{M} = \{\mathcal{W}, \mathcal{R}, \mathcal{V}, \tau\}$ be any Kripke model.

A world set is a variant of input sets. A world set looks almost the same as an input set. The difference is that the most nested elements of the sets are worlds instead of valuations. These world sets are used in the algorithm for creating input sets.

Definition 5. *A* ***well formed world set*** *W is recursively defined as follows:*

1. *$\langle w_1, ..., w_n\rangle$ is a well formed world set iff $w_1, ..., w_n \in \mathcal{W}$ for $n \geq 0$.*
2. *$\langle W_1, ..., W_n\rangle$ is a well formed world set iff $W_1, ..., W_n$ are well formed world sets such that each non-empty W_i has the same rank for $n \geq 0$.*
3. *a world set is well formed iff it follows the rules above.*

Let $\mathbb{W}_{\mathcal{M}}$ denote the class of all well formed world sets whose worlds are in $\mathcal{W}$.

Example 4. *Let w_1, w_2, w_3 be worlds in model $\mathcal{W}$. Then examples of well formed world sets are $\langle w_1, w_2, w_3\rangle$,*
$\langle\langle w_1, w_2\rangle, \langle w_3, w_3\rangle, \langle\rangle\rangle$,
$\langle\langle\langle w_3\rangle, \langle\rangle\rangle, \langle\langle w_1, w_2, w_2\rangle\rangle, \langle\rangle\rangle$

In definition 6 we will borrow the $\{element \mid condition\}$ notation from set theory.[11] Despite the use of ordered sets, this notation will not be problematic because the order of the elements satisfying the condition will not matter when using this function.

Definition 6. *The function $\textcircled{\blacksquare} : \mathbb{W}_{\mathcal{M}} \to \mathbb{W}_{\mathcal{M}}$ is recursively defined as follows:*

1. *$\textcircled{\blacksquare}(\langle w_1, ..., w_n\rangle) = \langle\langle w_i | (w_1, w_i) \in \mathcal{R}\rangle, ..., \langle w_i | (w_n, w_i) \in \mathcal{R}\rangle\rangle$ for $n \geq 0$.*
2. *$\textcircled{\blacksquare}(\langle W_1, ..., W_n\rangle) = \langle\textcircled{\blacksquare}(W_1), ..., \textcircled{\blacksquare}(W_n)\rangle$ for $n \geq 0$.*

We may abbreviate $\textcircled{\blacksquare}(W)$ by $\textcircled{\blacksquare}W$.

Definition 7. *The function $\mathcal{SET}_{\mathcal{M}} : \mathbb{W}_{\mathcal{M}} \times \mathcal{L}_p \to \mathfrak{I}$ is recursively defined as follows:* [12]

1. *$\mathcal{SET}_{\mathcal{M}}(\langle w_1, ..., w_n\rangle, p) = \langle\mathcal{V}(p_{w_1}), ..., \mathcal{V}(p_{w_n})\rangle$ where p_{w_i} is True iff $\mathcal{M}, w_i \models p$ for $n \geq 0$.*
2. *$\mathcal{SET}_{\mathcal{M}}(\langle W_1, ..., W_n\rangle, p) = \langle\mathcal{SET}_{\mathcal{M}}(W_1, p), ..., \mathcal{SET}_{\mathcal{M}}(W_n, p)\rangle$ for $n \geq 0$.*

We may abbreviate $\mathcal{SET}_{\mathcal{M}}$ by $\mathcal{SET}$ when the Kripke model is obvious.

Given $\mathcal{M}$ we now associate, for every non-gate node $\mathcal{N}$, an element $S_{\mathcal{M},\mathcal{N}} \in (\mathbb{W}_{\mathcal{M}} \cup \mathfrak{I})$ at $\mathcal{N}$. With the algorithm we will arrange it so that for every input node $\mathcal{N}$, $S_{\mathcal{M},\mathcal{N}} \in \mathfrak{I}$, and that for every output node $\mathcal{N}$ $S_{\mathcal{M},\mathcal{N}} \in \mathbb{W}_{\mathcal{W}}$. We will abbreviate $S_{\mathcal{M},\mathcal{N}_\phi}$ by $\mathcal{W}_\phi$. We will commonly start by setting $\mathcal{W}_\phi = \langle\tau\rangle$, because we are often interested in the value of a formula at the actual world τ. However, the definition below works for any arbitrary world set. Define $S_{\mathcal{M},\mathcal{N}_1}$ (respectively $S_{\mathcal{M},\mathcal{N}_3}$), the set corresponding to $\mathcal{M}$ at node $\mathcal{N}_1$ (respectively $\mathcal{N}_3$), by these rules:

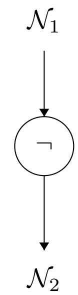
[11] An example of this notation from set theory can be found in Sipser's book "Introduction to the Theory of Computation" on page 7.

[12] In this paper, we will use $\mathcal{L}_p$ as the class of atomic propositions

1. If the circuit contains:

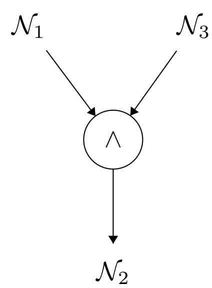
   and $\mathcal{N}_1$ is an input node labeled by any atomic proposition p, then $S_{\mathcal{M},\mathcal{N}_1} = \mathcal{SET}(S_{\mathcal{M},\mathcal{N}_2}, p)$.

2. If the circuit contains:



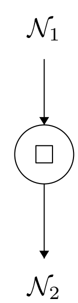
   then $S_{\mathcal{M},\mathcal{N}_1} = S_{\mathcal{M},\mathcal{N}_2}$.

3. I the circuit contains:



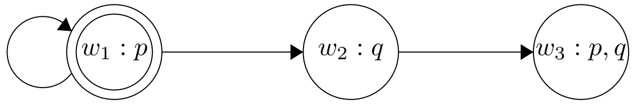
   then $S_{\mathcal{M},\mathcal{N}_1} = S_{\mathcal{M},\mathcal{N}_2} = S_{\mathcal{M},\mathcal{N}_3}$.

4. If the circuit contains:

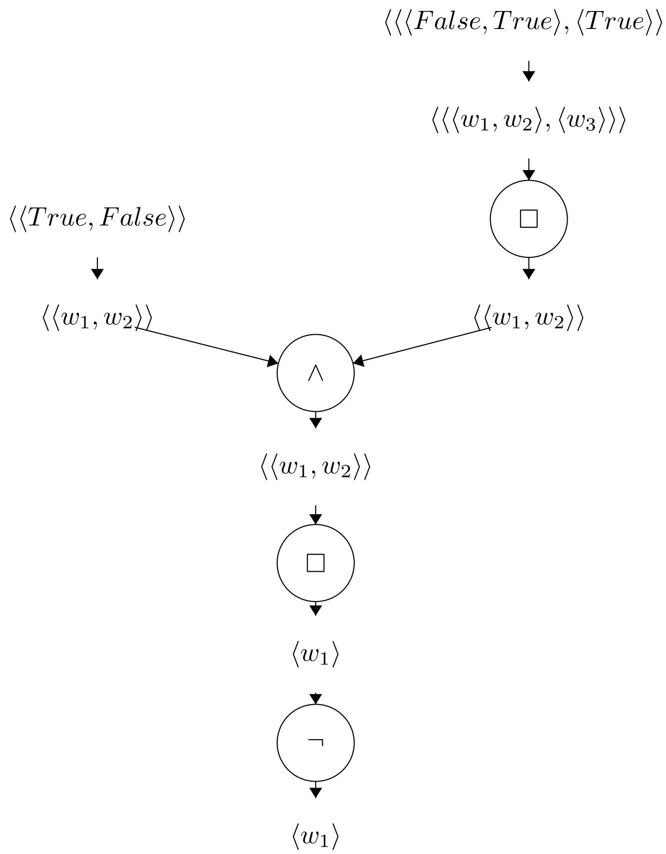


   then $S_{\mathcal{M},\mathcal{N}_1} = \textcircled{$\blacksquare$} S_{\mathcal{M},\mathcal{N}_2}$.

Running example 2. *Let $\neg\Box(p \wedge \Box q)$ be a modal formula and let the Kripke model $\mathcal{M}$ be:*



If we want to know whether $\mathcal{M}, \tau \models \neg\Box(p \wedge \Box q)$, then we calculate the input sets from the root of the modal circuit corresponding to the formula using the algorithm like this:



3 Calculating values of output nodes

In this section, we define the notion of a well formed output set, which is similar to an input set except with (possibly) non-atomic propositions as the most nested elements. Then we define a notion of position and the notion of correspondence between output sets and world sets. With these notions, we will define one function, $\ominus$, and two partial functions, $\circledwedge$ and $\boxdot_{\mathcal{M}}$. Finally we will define the rules for calculating output sets using this notion and these functions.

Definition 8. *The* ***value*** *of an output node is a well formed output set $\mathcal{O}$. A* ***well formed output set*** *$\mathcal{O}$ is recursively defined as follows:*

1. *$\langle \mathcal{V}(\alpha_1), ..., \mathcal{V}(\alpha_n)\rangle$ is a well formed output set iff $\alpha_1, ..., \alpha_n$ are propositional formulas for $n \geq 0$.*
2. *$\langle \mathcal{O}_1, ..., \mathcal{O}_n\rangle$ is a well formed output set iff $\mathcal{O}_1, ..., \mathcal{O}_n$ are well formed output sets such that each non-empty $\mathcal{O}_i$ has the same rank for $n \geq 0$.*
3. *an output set is well formed iff it follows the rules above.*

Let $\mathbb{O}$ denote the class of all well formed output sets.

As we will see in section 3.2, given a model $\mathcal{M}$ and choice of W_ϕ, we will associate, for every output node $\mathcal{N}$, an element $\mathcal{O}_{\mathcal{M},\mathcal{N}} \in \mathbb{O}$.[13]

Definition 9. *The* ***position*** *of an element x in a world set W or an output set $\mathcal{O}$ is a string $s \in (\mathbb{N} \cup \{\$\})^*$ and is recursively defined as follows:*

1. *The position of x_i in $\langle x_1, ..., x_i, ..., x_n\rangle$ is $\$i$, iff $x_1, ..., x_i, ..., x_n$ are either worlds or valuations for $0 \leq i \leq n$.*
2. *The position of an element x in X_i in $\langle X_1, ..., X_i, ..., X_n\rangle$ is $\$iI$ where I is the position of x in X_i, iff $X_1, ..., X_i, ..., X_n$ are either world sets or output sets for $0 \leq i \leq n$.*

Example 5. *Let $\langle\langle\langle w_1, w_2, w_2\rangle, \langle w_2\rangle, \langle w_1\rangle\rangle, \langle\langle w_2, w_3, w_1\rangle\rangle\rangle$ be a world set. Then the position of the element w_3 is $\$2\$1\$2$.*

Definition 10. *Let α be a propositional formula and let ϕ be a modal formula and let ϕ' be any sub formula of ϕ. A world w in the world set $\mathcal{S}_{\mathcal{M},\mathcal{N}_{\phi'}}$* ***corresponds*** *to the valuation $\mathcal{V}(\alpha)$ in the output set $\mathcal{O}_{\mathcal{M},\mathcal{N}_{\phi'}}$ iff the position of w in $\mathcal{S}_{\mathcal{M},\mathcal{N}_{\phi'}}$ is the same as the position of $\mathcal{V}(\alpha)$ in $\mathcal{O}_{\mathcal{M},\mathcal{N}_{\phi'}}$ and it holds that $\mathcal{M}, w \models \phi'$ iff $\mathcal{V}(\alpha)$ is True.*

Definition 11. *A world set W* ***corresponds*** *to an output set $\mathcal{O}$ iff each element of W corresponds to some unique element of $\mathcal{O}$.*

3.1 Functions on output sets

In the next section there are several definitions of functions. All these functions will be used in the running example after the algorithm in section 3.2.

[13] $\mathcal{W}_\phi$ is the world set chosen to be the root of a modal circuit. Commonly this will be $\langle\tau\rangle$ but for sub circuits other world sets may be needed

Definition 12. *The function* $\ominus : \mathbb{O} \rightarrow \mathbb{O}$ *is recursively defined, on the structure of output sets, as follows:*

1. $\ominus(\langle \mathcal{V}(\alpha_1), ..., \mathcal{V}(\alpha_n)\rangle) = \langle \mathcal{V}(\neg\alpha_1), ..., \mathcal{V}(\neg\alpha_n)\rangle$ *for* $n \geq 0$.
2. $\ominus(\langle \mathcal{O}_1, ..., \mathcal{O}_n\rangle) = \langle \ominus(\mathcal{O}_1), ..., \ominus(\mathcal{O}_n)\rangle$ *for* $n \geq 0$.

We may abbreviate $\ominus(\mathcal{O})$ by $\ominus\mathcal{O}$.

Definition 13. *The partial function* $\owedge : \mathbb{O} \times \mathbb{O} \rightharpoonup \mathbb{O}$ [14] *is recursively defined as follows:*

1. $\owedge(\langle \mathcal{V}(\alpha_1), ..., \mathcal{V}(\alpha_n)\rangle, \langle \mathcal{V}(\beta_1), ..., \mathcal{V}(\beta_n)\rangle) = \langle \mathcal{V}(\alpha_1 \wedge \beta_1), ..., \mathcal{V}(\alpha_n \wedge \beta_n)\rangle$ *for* $n \geq 0$.
2. $\owedge(\langle \mathcal{O}_{1,1}, ..., \mathcal{O}_{1,n}\rangle, \langle \mathcal{O}_{2,1}, ..., \mathcal{O}_{2,n}\rangle) = \langle \owedge(\mathcal{O}_{1,1}, \mathcal{O}_{2,1}), ..., \owedge(\mathcal{O}_{1,n}, \mathcal{O}_{2,n})\rangle$ *for* $n \geq 0$.

Definition 14. *The partial function* $\circledbox_{\mathcal{M}} : \mathbb{O} \rightharpoonup \mathbb{O}$ *is recursively defined as follows:*

1. $$\circledbox_{\mathcal{M}}(\langle\langle \mathcal{V}(\alpha_{1,1}), ..., \mathcal{V}(\alpha_{1,m})\rangle, ..., \langle \mathcal{V}(\alpha_{n,1}), ..., \mathcal{V}(\alpha_{n,o})\rangle\rangle) = \langle \mathcal{V}(\bigwedge_{i=1}^{m} \alpha_{1,i}), ..., \mathcal{V}(\bigwedge_{i=1}^{o} \alpha_{n,i})\rangle$$

   for $n \geq 0$ *and* $m \geq 0$ *and* $o \geq 0$ *iff for any world set* W *such that* $\circledblacksquare W$ *corresponds to*

   $$(\langle\langle \mathcal{V}(\alpha_{1,1}), ..., \mathcal{V}(\alpha_{1,m})\rangle, ..., \langle \mathcal{V}(\alpha_{n,1}), ..., \mathcal{V}(\alpha_{n,o})\rangle\rangle)$$

   we have that W *corresponds to*

   $$\langle \mathcal{V}(\bigwedge_{i=1}^{m} \alpha_{1,i}), ..., \mathcal{V}(\bigwedge_{i=1}^{o} \alpha_{n,i})\rangle$$

   .

2. $\circledbox_{\mathcal{M}}(\langle \mathcal{O}_1, ..., \mathcal{O}_n\rangle) = \langle (\circledbox_{\mathcal{M}})\mathcal{O}_1, ..., \circledbox_{\mathcal{M}}(\mathcal{O}_n)\rangle$
   for $n \geq 0$ *iff for any world set* W *such that* $\circledblacksquare W$ *corresponds to* $\langle \mathcal{O}_1, ..., \mathcal{O}_n\rangle$ *we have that* W *corresponds to* $\langle \circledbox_{\mathcal{M}}(\mathcal{O}_1), ..., \circledbox_{\mathcal{M}}(\mathcal{O}_n)\rangle$

We may abbreviate $\circledbox_{\mathcal{M}}(\mathcal{O})$ by $\circledbox\mathcal{O}$ if the model is obvious.

Note that $\owedge$ and $\circledbox_{\mathcal{M}}$ are partial functions. It is not the case that arbitrary output sets can be used on these functions. However, if the input sets of a modal circuit are made by using the steps described in section 2, then these partial functions can always be used. This will become clear in part III section 5. Further note that the restrictions in 14.1 and 14.2 ensure that this is not a multi valued function.

Example 6. *Consider* $\circledbox_{\mathcal{M}}(\langle\langle\rangle\rangle)$. *Without the restrictions in definition 14 this function has two possibilities. Either* $\circledbox_{\mathcal{M}}(\langle\langle\rangle\rangle) = \langle True\rangle$ *or* $\circledbox_{\mathcal{M}}(\langle\langle\rangle\rangle) = \langle\langle\rangle\rangle$. *Since any world set cannot correspond to both*

$$\langle \mathcal{V}(\bigwedge_{i=1}^{m} \alpha_{1,i}), ..., \mathcal{V}(\bigwedge_{i=1}^{o} \alpha_{n,i})\rangle \text{ and } \langle \circledbox_{\mathcal{M}}(\mathcal{O}_1), ..., \circledbox_{\mathcal{M}}(\mathcal{O}_n)\rangle$$

at the same time, the restriction in the definition prevents $\circledbox_{\mathcal{M}}$ *from being a multi valued function.*

[14]In this paper, the $\rightharpoonup$ will denote a partial function

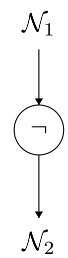
3.2 Steps for calculating

Given the input set $\mathcal{I}_{\mathcal{N}_i}$ for every input node $\mathcal{N}_i$, we now associate, for every node $\mathcal{N}$, an output set $\mathcal{O}_{\mathcal{M},\mathcal{N}} \in \mathbb{O}$ corresponding to model $\mathcal{M}$ in node $\mathcal{N}$. If the model is obvious from the context we will write $\mathcal{O}_{\mathcal{N}}$ instead of $\mathcal{O}_{\mathcal{M},\mathcal{N}}$. Define $\mathcal{O}_{\mathcal{N}_2}$, the output set at $\mathcal{N}_2$, by these rules:

1. If the circuit contains:

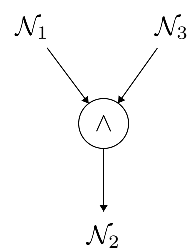
   and $\mathcal{N}_1$ is an input node, then $\mathcal{O}_{\mathcal{N}_2} = \mathcal{I}_{\mathcal{N}_1}$.

2. If the circuit contains:



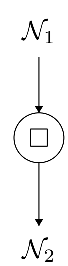
   then $\mathcal{O}_{\mathcal{N}_2} = \circleddash \mathcal{O}_{\mathcal{N}_1}$.

3. If the circuit contains:



   then $\mathcal{O}_{\mathcal{N}_2} = \owedge(\mathcal{O}_{\mathcal{N}_1}, \mathcal{O}_{\mathcal{N}_3})$

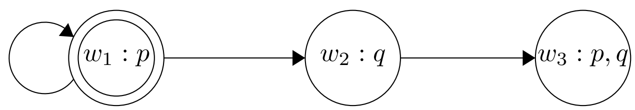
4. If the circuit contains:



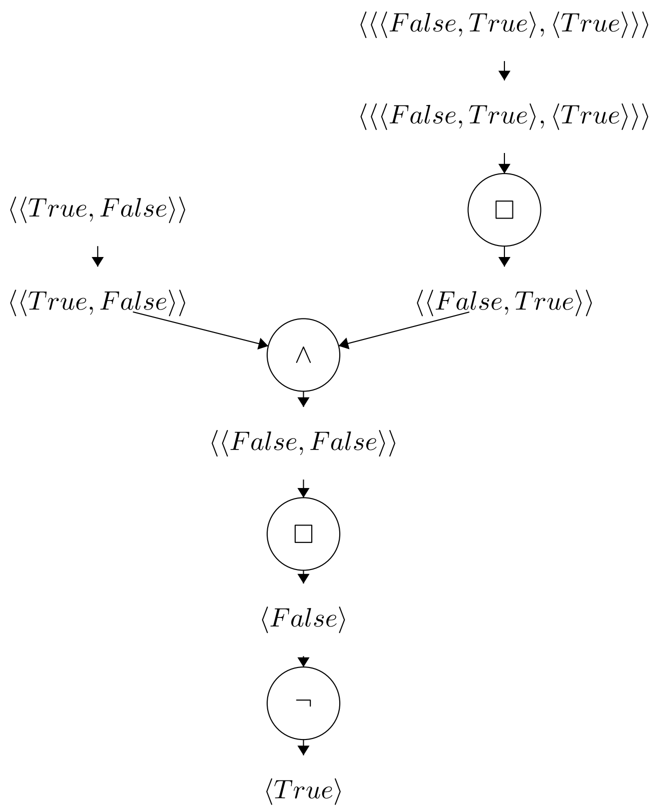
   then $\mathcal{O}_{\mathcal{N}_2} = \circledbox \mathcal{O}_{\mathcal{N}_1}$

We may abbreviate $\mathcal{O}_{\mathcal{N}_\phi}$ by $\mathcal{O}_\phi$.

Running example 3. *Let $\neg\Box(p \wedge \Box q)$ be a modal formula and let the Kripke model $\mathcal{M}$ be:*



If we want to know whether $\mathcal{M}, \tau \models \neg\Box(p \wedge \Box q)$, and we know what the input sets are, then we calculate the output set of the root starting at the leaves like this:



Since the output set at the final output node contains True, we know that $\mathcal{M}, \tau \models \neg\Box(p \wedge \Box q)$.

Lemma 1. *Let ϕ be a modal formula. Let $\mathcal{N}$ be a node in $\mathcal{C}_\phi$. Let α be a propositional formula. Suppose $\textcircled{\blacksquare}W \in \mathbb{W}$ corresponds to $\mathcal{O} \in \mathbb{O}$. Then W corresponds to $\textcircled{\square}\mathcal{O}$.*

Proof: We give a proof by induction over the structure of W.

Base case: Let W be $\langle w_1, ..., w_n \rangle \in \mathbb{W}$ for $n \geq 0$. Then by the definition of $\textcircled{\blacksquare}$ we can calculate that $\textcircled{\blacksquare}W = \textcircled{\blacksquare}(\langle w_1, ..., w_n \rangle) = \langle \langle w_i | (w_1, w_i) \in \mathcal{R} \rangle, ..., \langle w_i | (w_n, w_i) \in \mathcal{R} \rangle \rangle$. The output set $\mathcal{O}$ that corresponds to $\textcircled{\blacksquare}W$ is $\mathcal{O} = \langle \langle \mathcal{V}(\alpha_{w_i}) | (w_1, w_i) \in \mathcal{R} \rangle, ..., \langle \mathcal{V}(\alpha_{w_i}) | (w_n, w_i) \in \mathcal{R} \rangle \rangle$ where every valuation $\mathcal{V}(\alpha_{w_i})$ corresponds to world w_i in W. We can calculate by the function $\textcircled{\square}$ that

$$\textcircled{\square}\mathcal{O} = \textcircled{\square}\langle \langle \mathcal{V}(\alpha_{w_i}) | (w_1, w_i) \in \mathcal{R} \rangle, ..., \langle \mathcal{V}(\alpha_{w_i}) | (w_n, w_i) \in \mathcal{R} \rangle \rangle =$$

$$\langle \mathcal{V}(\bigwedge_{(w_1, w_i) \in \mathcal{R}} \alpha_{w_i}), ..., \mathcal{V}(\bigwedge_{(w_n, w_i) \in \mathcal{R}} \alpha_{w_i}) \rangle.$$

Now we have to prove that

$$\langle \mathcal{V}(\bigwedge_{(w_1, w_i) \in \mathcal{R}} \alpha_{w_i}), ..., \mathcal{V}(\bigwedge_{(w_n, w_i) \in \mathcal{R}} \alpha_{w_i}) \rangle \text{ corresponds to } \langle w_1, ..., w_n \rangle.$$

We must prove that for every element w_j in W it holds that

$$\mathcal{V}(\bigwedge_{(w_j, w_i) \in \mathcal{R}} \alpha_{w_i}) \text{ is True iff } \mathcal{M}, w_j \models \Box\phi_\alpha.$$

We know that

$$\mathcal{V}(\bigwedge_{(w_j, w_i) \in \mathcal{R}} \alpha_{w_i})$$

is True iff for every world v where $(w_j, v) \in \mathcal{R}$ it holds that $\mathcal{M}, v \models \phi_\alpha$. We also know by the definition of $\Box$ that $\mathcal{M}, w_j \models \Box\phi_\alpha$ holds iff for every world v where $(w_j, v) \in \mathcal{R}$ it holds that $\mathcal{M}, v \models \phi_\alpha$. Therefore, we know that

$$\mathcal{V}(\bigwedge_{(w_j, w_i) \in \mathcal{R}} \alpha_{w_i})$$

is True iff $\mathcal{M}, w_j \models \Box\phi_\alpha$

Inductive hypothesis. *Suppose for world sets $W_1, ..., W_n$, we have that for $0 \leq i \leq n$, if $\textcircled{\blacksquare}W_i$ corresponds to $\mathcal{O}_i$, then W_i corresponds to $\textcircled{\square}\mathcal{O}_i$.*

Inductive step: Let W be $\langle W_1, ..., W_n \rangle$. Then by the definition of $\textcircled{\blacksquare}$ we calculate that $\textcircled{\blacksquare}W = \textcircled{\blacksquare}\langle W_1, ..., W_n \rangle = \langle \textcircled{\blacksquare}W_1, ..., \textcircled{\blacksquare}W_n \rangle$. Now we know that the output set $\mathcal{O}$ that corresponds to $\textcircled{\blacksquare}W$ is $\mathcal{O} = \langle \mathcal{O}_1, ..., \mathcal{O}_n \rangle$. Then we calculate by the function $\textcircled{\square}$ that $\textcircled{\square}\mathcal{O} = \textcircled{\square}\langle \mathcal{O}_1, ..., \mathcal{O}_n \rangle = \langle \textcircled{\square}\mathcal{O}_1, ..., \textcircled{\square}\mathcal{O} \rangle$. Now we have to prove that $W = \langle W_1, ..., W_n \rangle$ corresponds to $\textcircled{\square}\mathcal{O} = \langle \textcircled{\square}\mathcal{O}_1, ..., \textcircled{\square}\mathcal{O} \rangle$. Therefore, by definition of correspondence, we have to prove that every W_i in W corresponds to $\textcircled{\square}\mathcal{O}_i$ in $\textcircled{\square}\mathcal{O}$. This is true by the inductive hypothesis.

$\Box$

Part III

Satisfiability of modal circuits

4 How is a modal circuit satisfiable

There are several ways to define satisfiability for modal circuits. In this paper we will consider only the definition below. Some other definitions of satisfiability will be given in the conclusion of the paper to consider for future research.

Definition 15. *An output node in a modal circuit* ***can be calculated*** *iff the output set of that output node can be calculated from the input sets by using the functions and steps defined in sections 3.1 and 3.2.*

Definition 16. *A modal circuit* ***is satisfiable*** *iff there is a configuration of input sets such that the value of every output node can be calculated and such that the calculated value of the final output node is a singleton containing True and there is a Kripke model such that if the world set at the final output node is $\langle \tau \rangle$, then the input sets can be calculated using the algorithm described in section 2 of part II.*

Running example 4. *In running example 2 we saw that there is a Kripke model such that if the world set at the final output node is $\langle \tau \rangle$, then the input sets can be calculated using the algorithm described in section 2 of part II, because we calculated the input sets using the algorithm. In running example 3 we saw that there is a configuration of input sets such that the value of every output node can be calculated and such that the calculated value of the final output node is a singleton containing True. Now we know that our circuit is satisfiable.*

Modal circuit satisfiability, from now on MCSAT, is defined as follows:

$$MCSAT = \{< \mathcal{C} > \mid \mathcal{C} \text{ is a satisfiable modal circuit}\}$$

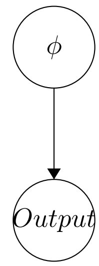
5 Polynomial-time reduction from $MSAT$ to $MCSAT$

In this section we will prove two theorems. The first theorem states that modal circuits produce the same truth values as modal formulas, generalizing the well known result that Boolean formulas and the corresponding Boolean circuits produce the same truth values. The second theorem will use the first theorem to prove that $MSAT$ is polynomial-time reducible to $MCSAT$.

Theorem 1. *Given model $\mathcal{M}$ and a modal circuit $\mathcal{C}_\phi$. For every valuation $\mathcal{V}(\alpha)$ in the output set $\mathcal{O}_\phi$ of the final output node it holds that $\mathcal{V}(\alpha)$ is True iff for that world w corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w \models \phi$.*

Proof: Let W_ϕ be the world set of the final output node of the modal circuit $\mathcal{C}_\phi$ corresponding to the modal formula ϕ. We give a proof by induction:

Main base case: Let ϕ be an atomic proposition. Then the corresponding circuit is:



The world set of *Output* is by assumption W_ϕ. We can calculate the input set by using the algorithm described in section 2. By using this algorithm, we calculate that $\mathcal{I}_i = \mathcal{SET}(W_\phi, \phi)$. By the definition of the modal circuit in section 3, the calculated output set in *Output* is $\mathcal{SET}(W_\phi, \phi)$. We now have to prove that for every valuation $\mathcal{V}(\alpha)$ in $\mathcal{SET}(W_\phi, \phi)$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w \models \phi$. We can prove this by induction on the structure of world sets:

Base case: Let W_i be a set of worlds $\langle w_1, ..., w_n \rangle$ for $n \geq 0$. Then we have to prove that for every valuation $\mathcal{V}(\alpha)$ in $\mathcal{SET}(\langle w_1, ..., w_n \rangle, \phi)$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w_i \models \phi$. By the definition of $\mathcal{SET}$ we calculate that $\mathcal{SET}(\langle w_1, ..., w_n \rangle, \phi) = \langle \mathcal{V}(\phi_{w_1}), ..., \mathcal{V}(\phi_{w_n}) \rangle$ where ϕ_{w_i} is True iff $\mathcal{M}, w_i \models \phi$.

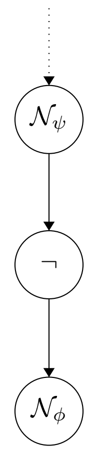
Inductive hypothesis. *Suppose for world sets $W_1, ..., W_n$, we have that for every valuation $\mathcal{V}(\alpha)$ in $\mathcal{SET}(W_i, \phi)$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w_i \models \phi$.*

Inductive step: Let W_m be $\langle W_1, ..., W_n \rangle$ for $n \geq 0$. Then we have to prove that for every valuation $\mathcal{V}(\alpha)$ in $\mathcal{SET}(W_m, \phi)$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w_i \models \phi$. By using the definition of $\mathcal{SET}$ we can calculate that $\mathcal{SET}(\langle W_1, ..., W_n \rangle, \phi) = \langle \mathcal{SET}(W_1, \phi), ..., \mathcal{SET}(W_n, \phi) \rangle$. By the inductive hypothesis, we know that for every valuation $\mathcal{V}(\alpha)$ in $\mathcal{SET}(W_1, \phi), ..., \mathcal{SET}(W_n, \phi)$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w_i \models \phi$.

This is the conclusion of the base case.

Main inductive hypothesis. *Suppose for any world set for the final output node of the modal circuit $\mathcal{C}_\psi$ corresponding to modal formula ψ, we have that for every valuation $\mathcal{V}(\alpha)$ in the calculated output set $\mathcal{O}_\psi$ of the final output node it holds that $\mathcal{V}(\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w \models \psi$. Suppose this is the same for χ.*

Main inductive step - negation(¬): suppose ϕ is $\neg\psi$. The corresponding (partial) circuit is then:



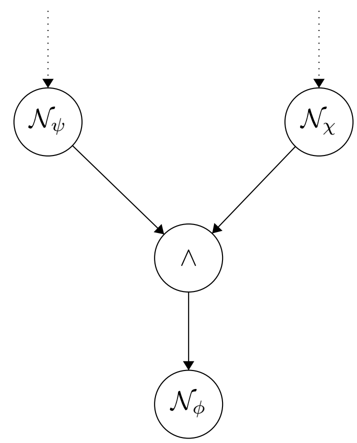
The world set of $\mathcal{N}_\phi$ is by assumption W_ϕ. By using the algorithm of section 2 we can calculate that $W_\phi = W_\psi$. By the inductive hypothesis, we know that for every valuation $\mathcal{V}(\alpha)$ in the calculated output set $\mathcal{O}_\psi$ of $\mathcal{N}_\psi$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w \models \psi$. Now we have to prove that for every valuation $\mathcal{V}(\gamma)$ in the calculated output set $\ominus\mathcal{O}_\psi$ of $\mathcal{N}_\phi$ it holds that $\mathcal{V}(\gamma)$ is True iff for the world v corresponding to $\mathcal{V}(\gamma)$ it holds that $\mathcal{M}, v \models \neg\psi$. We can prove this by induction on the structure of world sets:

Base case: Let W_ϕ be a set of worlds $\langle w_1, ..., w_n\rangle$ for $n \geq 0$. Therefore, we know that $W_\psi = \langle w_1, ..., w_n\rangle$. Therefore, we know that $\mathcal{O}_\psi = \langle \mathcal{V}(\alpha_{w_1}), ..., \mathcal{V}(\alpha_{w_n})\rangle$ where every valuation $\mathcal{V}(\alpha_{w_i})$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha_{w_i})$ it holds that $\mathcal{M}, w_i \models \psi$. Now, following the definition of $\ominus$, we know that $\ominus\mathcal{O}_\psi = \ominus\langle \mathcal{V}(\alpha_{w_1}), ..., \mathcal{V}(\alpha_{w_n})\rangle = \langle \mathcal{V}(\neg\alpha_{w_1}), ..., \mathcal{V}(\neg\alpha_{w_n})\rangle$. Since we know that for every valuation $\mathcal{V}(\alpha_{w_i})$ in $\langle \mathcal{V}(\alpha_{w_1}), ..., \mathcal{V}(\alpha_{w_n})\rangle$ of $\mathcal{N}_\psi$ it holds that $\mathcal{V}(\alpha_{w_i})$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha_{w_i})$ it holds that $\mathcal{M}, w_i \models \psi$, we know by the definition function of negation that every valuation $\mathcal{V}(\neg\alpha_{w_i})$ in $\langle \mathcal{V}(\neg\alpha_{w_1}), ..., \mathcal{V}(\neg\alpha_{w_n})\rangle$ of $\mathcal{N}_\phi$ is True iff for the world w_i corresponding to $\mathcal{V}(\neg\alpha_{w_i})$ it holds that $\mathcal{M}, w_i \models \neg\psi$.

Inductive hypothesis. *Suppose for world sets $W_1, ..., W_n$, we have that for every valuation $\mathcal{V}(\neg\alpha)$ in $\ominus\mathcal{O}_\psi$ it holds that $\mathcal{V}(\neg\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\neg\alpha)$ it holds that $\mathcal{M}, w \models \neg\psi$.*

Inductive step: Let W_ϕ be $\langle W_1, ..., W_n\rangle$ for $n \geq 0$. Therefore, we know that the world set for $\mathcal{N}_\psi$, W_ψ is $\langle W_1, ..., W_n\rangle$. Therefore, we know that the output set $\mathcal{O}_\psi$ for $\mathcal{N}_\psi$ is $\langle \mathcal{O}_1, ..., \mathcal{O}_n\rangle$ where $\mathcal{O}_i$ corresponds to W_i. By the main inductive hypothesis, we know that for every valuation $\mathcal{V}(\alpha)$ in the calculated output set $\mathcal{O}_\psi$ of the final output node of $\mathcal{C}_\psi$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w \models \psi$. Now, following the definition of $\ominus$ we can calculate that $\ominus\mathcal{O}_\psi = \ominus\langle \mathcal{O}_1, ..., \mathcal{O}_n\rangle = \langle \ominus\mathcal{O}_1, ..., \ominus\mathcal{O}_n\rangle$. By the inductive hypothesis we know that for every valuation $\mathcal{V}(\neg\alpha)$ in $\ominus\mathcal{O}_1, ..., \ominus\mathcal{O}_n$ it holds that $\mathcal{V}(\neg\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\neg\alpha)$ it holds that $\mathcal{M}, w \models \neg\psi$.

Main inductive step - conjunction(∧): Suppose ϕ is $\psi \wedge \chi$. The corresponding (partial) circuit is then:



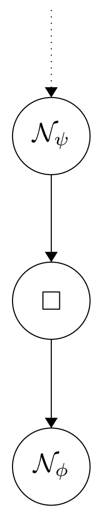
The world set of $\mathcal{N}_\phi$ is by assumption W_ϕ. By using the algorithm of section 2 we can calculate that $W_\phi = W_\psi = W_\chi$. By the inductive hypothesis, we know that for every valuation $\mathcal{V}(\alpha)$ and $\mathcal{V}(\beta)$ in the calculated output sets $\mathcal{O}_\psi$ and $\mathcal{O}_\chi$ of $\mathcal{N}_\psi$ and $\mathcal{N}_\chi$ it holds that $\mathcal{V}(\alpha)$ and $\mathcal{V}(\beta)$ are True iff for the world w corresponding to $\mathcal{V}(\alpha)$ and $\mathcal{V}(\beta)$ it holds that $\mathcal{M}, w \models \psi$ and $\mathcal{M}, w \models \chi$. Now we have to prove that for every valuation $\mathcal{V}(\gamma)$ in the calculated output set $\owedge(\mathcal{O}_\psi, \mathcal{O}_\chi)$ of $\mathcal{N}_\phi$ it holds that $\mathcal{V}(\gamma)$ is True iff for the world v corresponding to $\mathcal{V}(\gamma)$ it holds that $\mathcal{M}, v \models \psi \wedge \chi$. We can prove this by induction on the structure of world sets:

Base case: Let W_ϕ be a set of worlds $\langle w_1, ..., w_n\rangle$ for $n \geq 0$. Therefore, we know that $W_\psi = W_\chi = \langle w_1, ..., w_n\rangle$. Therefore, we know that $\mathcal{O}_\psi = \langle \mathcal{V}(\alpha_{w_1}), ..., \mathcal{V}(\alpha_{w_n})\rangle$ where for every valuation $\mathcal{V}(\alpha_{w_i})$ it holds that $\mathcal{V}(\alpha_{w_i})$ is True iff $\mathcal{M}, w_i \models \psi$ and $\mathcal{O}_\chi = \langle \mathcal{V}(\beta_{w_1}), ..., \mathcal{V}(\beta_{w_n})\rangle$ where for every valuation $\mathcal{V}(\beta_{w_i})$ it holds that $\mathcal{V}(\beta_{w_i})$ is True iff $\mathcal{M}, w_i \models \chi$. Now, following the definition of $\owedge$, we know that $\owedge(\mathcal{O}_\psi, \mathcal{O}_\chi) = \owedge(\langle \mathcal{V}(\alpha_{w_1}), ..., \mathcal{V}(\alpha_{w_n})\rangle, \langle \mathcal{V}(\beta_{w_1}), ..., \mathcal{V}(\beta_{w_n})\rangle) = \langle \mathcal{V}(\alpha_{w_1} \wedge \beta_{w_1}), ..., \mathcal{V}(\alpha_{w_n} \wedge \beta_{w_n})\rangle$. Since the main inductive hypothesis gives that for every valuation $\mathcal{V}(\alpha_{w_i})$ and $\mathcal{V}(\beta_{w_i})$ in $\langle \mathcal{V}(\alpha_{w_1}), ..., \mathcal{V}(\alpha_{w_n})\rangle$ and $\langle \mathcal{V}(\beta_{w_1}), ..., \mathcal{V}(\beta_{w_n})\rangle$ of $\mathcal{N}_\psi$ and $\mathcal{N}_\chi$ respectively it holds that $\mathcal{V}(\alpha_{w_i})$ and $\mathcal{V}(\beta_{w_i})$ are True iff for the world w_i corresponding to $\mathcal{V}(\alpha_{w_i})$ and $\mathcal{V}(\beta_{w_i})$ it holds that $\mathcal{M}, w_i \models \psi$ and $\mathcal{M}, w_i \models \chi$ respectively, we know by the definition of the valuation function of conjunction that for every valuation $\mathcal{V}(\alpha_{w_i} \wedge \beta_{w_i})$ in $\langle \mathcal{V}(\alpha_{w_1} \wedge \beta_{w_1}), ..., \mathcal{V}(\alpha_{w_n} \wedge \beta_{w_n})\rangle$ of $\mathcal{N}_\phi$ it holds that $\mathcal{V}(\alpha_{w_i} \wedge \beta_{w_i})$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha_{w_i} \wedge \beta_{w_i})$ it holds that $\mathcal{M}, w_i \models \psi \wedge \chi$.

Inductive hypothesis. *Suppose for world sets $W_1, ..., W_n$, we have that for every valuation $\mathcal{V}(\alpha \wedge \beta)$ in $\owedge(\mathcal{O}_\psi, \mathcal{O}_\chi)$ it holds that $\mathcal{V}(\alpha \wedge \beta)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha \wedge \beta)$ it holds that $\mathcal{M}, w \models \psi \wedge \chi$.*

Inductive step: Let W_ϕ be $\langle W_1, ..., W_n\rangle$ for $n \geq 0$. Therefore, we know that $W_\psi = W_\chi = \langle W_1, ..., W_n\rangle$. Therefore, we know that $\mathcal{O}_\psi = \langle \mathcal{O}_{\psi_1}, ..., \mathcal{O}_{\psi_n}\rangle$ and $\mathcal{O}_\chi = \langle \mathcal{O}_{\chi_1}, ..., \mathcal{O}_{\chi_n}\rangle$ where $\mathcal{O}_{j_i}$ corresponds to W_i in $\mathcal{N}_j$. By the main inductive hypothesis, we know that for every valuation $\mathcal{V}(\alpha)$ and $\mathcal{V}(\beta)$ in the calculated output set $\mathcal{O}_\psi$ and $\mathcal{O}_\chi$ it holds that $\mathcal{V}(\alpha)$ and $\mathcal{V}(\beta)$ are True iff for the world w corresponding to $\mathcal{V}(\alpha)$ and $\mathcal{V}(\beta)$ it holds that $\mathcal{M}, w \models \psi$ and $\mathcal{M}, w \models \chi$ respectively. Now, following the definition of $\owedge$ we can calculate that $\owedge(\mathcal{O}_\psi, \mathcal{O}_\chi) = \owedge(\langle \mathcal{O}_{\psi_1}, ..., \mathcal{O}_{\psi_n}\rangle, \langle \mathcal{O}_{\chi_1}, ..., \mathcal{O}_{\chi_n}\rangle) = \langle \owedge(\mathcal{O}_{\psi_1}, \mathcal{O}_{\chi_1}), ..., \owedge(\mathcal{O}_{\psi_n}, \mathcal{O}_{\chi_n})\rangle$. By the inductive hypothesis we know that for every valuation $\mathcal{V}(\alpha \wedge \beta)$ in $\owedge(\mathcal{O}_{\psi_1}, \mathcal{O}_{\chi_1}), ..., \owedge(\mathcal{O}_{\psi_n}, \mathcal{O}_{\chi_n})$ it holds that $\mathcal{V}(\alpha \wedge \beta)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha \wedge \beta)$ it holds that $\mathcal{M}, w \models \psi \wedge \chi$.

Main inductive step - box($\Box$): Suppose ϕ is $\Box\psi$. The corresponding (partial) modal circuit is then:



The world set of $\mathcal{N}_\phi$ is by assumption W_ϕ. By using the algorithm of section 2 we can calculate that $W_\psi = \textcircled{\blacksquare} W_\phi$. By the inductive hypothesis, we know that for every valuation $\mathcal{V}(\alpha)$ in the calculated output set $\mathcal{O}_\psi$ of $\mathcal{N}_\psi$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w \models \psi$. Now we have to prove that for every valuation $\mathcal{V}(\gamma)$ in the calculated output set $\textcircled{\Box}\mathcal{O}_\psi$ of $\mathcal{N}_\phi$ it holds that $\mathcal{V}(\gamma)$ is True iff for the world v corresponding to $\mathcal{V}(\gamma)$ it holds that $\mathcal{M}, v \models \Box\psi$. We can prove this by induction on the structure of world sets:

Base case: Let W_ϕ be a set of worlds $\langle w_1, ..., w_n \rangle$ for $n \geq 0$. Therefore, we know that $W_\psi = \textcircled{$\blacksquare$}\langle w_1, ..., w_n \rangle = \langle \langle w_i | (w_1, w_i) \in \mathcal{R} \rangle, ..., \langle w_i | (w_n, w_i) \in \mathcal{R} \rangle \rangle$. Therefore, we know that $\mathcal{O}_\psi = \langle \langle \mathcal{V}(\alpha_{w_i}) | (w_1, w_i) \in \mathcal{R} \rangle, ..., \langle \mathcal{V}(\alpha_{w_i}) | (w_n, w_i) \in \mathcal{R} \rangle \rangle$ where for every valuation $\mathcal{V}(\alpha_{w_i})$ it holds that $\mathcal{V}(\alpha_{w_i})$ is True iff $\mathcal{M}, w_i \models \psi$.
Now, following the definition of $\textcircled{$\square$}$, we know that

$$\textcircled{$\square$}\mathcal{O}_\psi = \textcircled{$\square$}\langle \langle \mathcal{V}(\alpha_{w_i}) | (w_1, w_i) \in \mathcal{R} \rangle, ..., \langle \mathcal{V}(\alpha_{w_i}) | (w_n, w_i) \in \mathcal{R} \rangle \rangle =$$

$$\langle \mathcal{V}(\bigwedge_{(w_1, w_i) \in \mathcal{R}} \alpha_{w_i}), ..., \mathcal{V}(\bigwedge_{(w_n, w_i) \in \mathcal{R}} \alpha_{w_i}) \rangle$$

Since we know by the main inductive hypothesis that for every valuation $\mathcal{V}(\alpha_{w_i})$ in $\langle \langle \mathcal{V}(\alpha_{w_i}) | (w_1, w_i) \in \mathcal{R} \rangle, ..., \langle \mathcal{V}(\alpha_{w_i}) | (w_n, w_i) \in \mathcal{R} \rangle \rangle$ of $\mathcal{N}_\psi$ it holds that $\mathcal{V}(\alpha_{w_i})$ is True iff for the world w_i corresponding to $\mathcal{V}(\alpha_{w_i})$ it holds that $\mathcal{M}, w_i \models \psi$, and since $\mathcal{M}, w_j \models \Box\psi$ holds iff for all worlds $w_i \in \mathcal{W}$ where $(w_j, w_i) \in \mathcal{R}$ it holds that $\mathcal{M}, w_i \models \psi$, we know that for every valuation

$$\mathcal{V}(\bigwedge_{(w_j, w_i) \in \mathcal{R}} \alpha_{w_i}) \text{ in } \langle \mathcal{V}(\bigwedge_{(w_1, w_i) \in \mathcal{R}} \alpha_{w_i}), ..., \mathcal{V}(\bigwedge_{(w_n, w_i) \in \mathcal{R}} \alpha_{w_i}) \rangle$$

of $\mathcal{N}_\phi$ it holds that

$$\mathcal{V}(\bigwedge_{(w_j, w_i) \in \mathcal{R}} \alpha_{w_i})$$

is True iff for the world w_j corresponding to

$$\mathcal{V}(\bigwedge_{(w_j, w_i) \in \mathcal{R}} \alpha_{w_i})$$

it holds that $\mathcal{M}, w_j \models \Box\psi$.

Inductive hypothesis. *Suppose for world sets $W_1, ..., W_n$, we have that for every valuation*

$$\mathcal{V}(\bigwedge_{(w_i, w_j) \in \mathcal{R}} \alpha_{w_j})$$

in $\textcircled{$\square$}\mathcal{O}_\psi$ it holds that

$$\mathcal{V}(\bigwedge_{(w_i, w_j) \in \mathcal{R}} \alpha_{w_j})$$

is True iff for the world w_i corresponding to

$$\mathcal{V}(\bigwedge_{(w_i, w_j) \in \mathcal{R}} \alpha_{w_j})$$

it holds that $\mathcal{M}, w_i \models \Box\psi$.

Inductive step: Let W_ϕ be $\langle W_1, ..., W_n \rangle$ for $n \geq 0$. Therefore, we know that $W_\psi = \textcircled{\tiny$\blacksquare$}\langle W_1, ..., W_n \rangle = \langle \textcircled{\tiny$\blacksquare$}(W_1), ..., \textcircled{\tiny$\blacksquare$}(W_n) \rangle$. Therefore, we know that $\mathcal{O}_\psi = \langle \mathcal{O}_1, ..., \mathcal{O}_n \rangle$ where $\mathcal{O}_j$ corresponds to $\textcircled{\tiny$\blacksquare$}(W_j)$. By the main inductive hypothesis, we know that for every valuation $\mathcal{V}(\alpha)$ in the calculated output set $\mathcal{O}_\psi$ of $\mathcal{N}_\psi$ it holds that $\mathcal{V}(\alpha)$ is True iff for the world w corresponding to $\mathcal{V}(\alpha)$ it holds that $\mathcal{M}, w \models \psi$. Now, following the definition of $\textcircled{\tiny$\square$}$, we can calculate that $\textcircled{\tiny$\square$}\mathcal{O}_\psi = \textcircled{\tiny$\square$}\langle \mathcal{O}_1, ..., \mathcal{O}_n \rangle = \langle \textcircled{\tiny$\square$}\mathcal{O}_1, ..., \textcircled{\tiny$\square$}\mathcal{O}_n \rangle$. We know by lemma 1 that $W_1, ..., W_n$ correspond to $\textcircled{\tiny$\square$}\mathcal{O}_1, ..., \textcircled{\tiny$\square$}\mathcal{O}_n$. Then, by the inductive hypothesis, we know that for every valuation

$$\mathcal{V}(\bigwedge_{(w_i, w_j) \in \mathcal{R}} \alpha_{w_j})$$

in $\textcircled{\tiny$\square$}\mathcal{O}_\psi$ it holds that

$$\mathcal{V}(\bigwedge_{(w_i, w_j) \in \mathcal{R}} \alpha_{w_j})$$

is True iff for the world w_i corresponding to

$$\mathcal{V}(\bigwedge_{(w_i, w_j) \in \mathcal{R}} \alpha_{w_j})$$

it holds that $\mathcal{M}, w_i \models \Box\psi$.

$\square$

We now prove that local modal satisfiability is reducible to the modal circuit satisfiability using Theorem 1.

Theorem 2. $MSAT \leq_p MCSAT$.

Proof: We must find a reduction function f such that for every $s \in \mathcal{L}$, $s \in MSAT$ iff $f(s) \in MCSAT$. We claim a function f that works would be the obvious function f such that $f(< \phi >) =< s >$ where $< s >$ is a string that encodes the modal circuit of ϕ.[15] This function is clearly polynomial-time computable for the same reason as the reduction function from propositional formulas to Boolean circuits.

Let ϕ be a modal formula. Then we have to prove that there exists an input set for $\mathcal{C}_\phi$ such that every output node can be calculated and such that the calculated value of the final output node $\mathcal{N}_\phi$ is a singleton containing True iff there exists a world $w \in \mathcal{W}$ such that $\mathcal{M}, w \models \phi$

$\Rightarrow$ Suppose ϕ is satisfiable. Then we know that there exists a model $\mathcal{M}$ and a current world τ where it holds that $\mathcal{M}, \tau \models \phi$. Then we have to prove that there exists an input set for the modal circuit $\mathcal{C}_\phi$ that satisfies the circuit. Let the world set of the final output node be $\langle \tau \rangle$. Then we know by theorem 1 that the valuation $\mathcal{V}(\alpha)$ of the output set $\langle \mathcal{V}(\alpha) \rangle$ is True iff for the world τ it holds that $\mathcal{M}, \tau \models \phi$. By assumption $\mathcal{M}, \tau \models \phi$ holds. Therefore, $\mathcal{V}(\alpha)$ is True.

$\neg \Rightarrow$ Suppose ϕ is not satisfiable. Then we know that there exists no model $\mathcal{M}$ with a current world τ where it holds that $\mathcal{M}, \tau \models \phi$. Then we have to prove that there exists no input set for the modal circuit $\mathcal{C}_\phi$ that satisfies the circuit. We know by theorem 1 that for any model $\mathcal{M} = \langle \mathcal{W}, \mathcal{R}, \mathcal{V}, \tau \rangle$, if $W_\phi = \langle \tau \rangle$, then if $\mathcal{O}_\phi = \mathcal{O}_{\mathcal{M}, \mathcal{N}_\phi} = \langle \mathcal{V}(\alpha) \rangle$, for some valuation $\mathcal{V}(\alpha)$, we have that $\mathcal{V}(\alpha)$ is True iff $\mathcal{M}, \tau \models \phi$. By assumption, $\mathcal{M}, \tau \not\models \phi$. Therefore $\mathcal{C}_\phi$ is not satisfiable.

□

[15] Note that the symbols $<$ and $>$ are different from $\langle$ and $\rangle$. $< x >$ is the string that encodes x and $\langle x \rangle$ is a singleton containing x.

Part IV
Conclusion

In this paper, we looked at modal circuits as an extension of Boolean circuits. In part II, we defined modal circuits. Then we looked at a definition for calculating input sets corresponding to models. After that, we learned how to calculate the output sets using the input sets in a circuit.

In part III we have proven that modal logic is polynomial time reducible to modal circuits. First we defined the satisfiability of modal circuits. Then we proved the reduction from modal logic to modal circuits. For proving the reduction, we first proved the more general theorem 1. Then we used that theorem to prove the actual reduction.

Proving the reduction means that the modal circuit problem $MCSAT$ is $PSPACE$-*hard*, since the modal logic problem $MSAT$ is $PSCPACE$-*complete*. For future research, $PSPACE$-*completeness* can be proven by proving that $MCSAT \leq_p MSAT$. In this paper the definition of $MCSAT$ was very specific. Other satisfiability problems can be imagined and can be proven still. For example, satisfiability can be defined like this: A modal circuit is satisfiable iff there is a configuration of input sets such that the value of every output node can be calculated and such that the calculated value of the final output node is a singleton containing True. An even simpler version could be that a modal circuit is satisfiable iff there is a configuration of input sets such that the calculated output set at the final output node is a singleton containing True.

When the reductions from and to $MSAT$ for the other satisfiability problems are proven, modal circuits may be useful for finding an answer for the $NP \stackrel{?}{=} PSPACE$ question. Since modal circuits look a lot like Boolean circuits, modal circuits can be a nice addition towards solving this problem.

References

[1] Boole, George. An Investigation of the Laws of Thought on Which Are Founded the Mathematical Theories of Logic and Probabilities. New York, NY: Dover Publications, 1958.

[2] Shannon, Claude E. "A Symbolic Analysis of Relay and Switching Circuits." Electrical Engineering 57.12 (1938): p.471 - p.495.

[3] Sipser, Michael. Introduction to the Theory of Computation. S.l.: Cengage Learning, 2013.

[4] Kripke, Saul A. "Semantical Analysis of Modal Logic I Normal Modal Propositional Calculi." Zeitschrift Für Mathematische Logik Und Grundlagen Der Mathematik 9.5-6 (1963): p.67 - p.96.

[5] Fischer, Michael J., and Richard E. Ladner. "Propositional Dynamic Logic of Regular Programs." Journal of Computer and System Sciences 18.2 (1979): p.194 - p.211.