



**HAL**  
open science

# Internal Proof Calculi for Modal Logics with Separating Conjunction

Stéphane Demri, Raul Fervari, Alessio Mansutti

► **To cite this version:**

Stéphane Demri, Raul Fervari, Alessio Mansutti. Internal Proof Calculi for Modal Logics with Separating Conjunction. *Journal of Logic and Computation*, 2021, 31 (3), pp.832-891. 10.1093/log-com/exab016 . hal-03185457

**HAL Id: hal-03185457**

**<https://hal.science/hal-03185457>**

Submitted on 30 Mar 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Internal Proof Calculi for Modal Logics with Separating Conjunction

Stéphane Demri\*      Raul Fervari†      Alessio Mansutti\*

\*LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay, France  
{demri,alessio.mansutti}@lsv.fr

†CONICET and Universidad Nacional de Córdoba, Argentina  
rfervari@unc.edu.ar

## Abstract

Modal separation logics are formalisms that combine modal operators to reason locally, with separating connectives that allow to perform global updates on the models. In this work, we design Hilbert-style proof systems for the modal separation logics  $MSL(*, \langle \neq \rangle)$  and  $MSL(*, \diamond)$ , where  $*$  is the separating conjunction,  $\diamond$  is the standard modal operator and  $\langle \neq \rangle$  is the difference modality. The calculi only use the logical languages at hand (no external features such as labels) and can be divided in two main parts. First, normal forms for formulae are designed and the calculi allow to transform every formula into a formula in normal form. Second, another part of the calculi is dedicated to the axiomatisation for formulae in normal form, which may still require non-trivial developments but is more manageable.

## 1 Introduction

**Separation logics with epistemic flavour.** Modal logic [8, 9] is a family of languages extending propositional logic with operators to describe and reason about different modes of truth. Such operators are usually called modalities. For instance, this family includes alethic (describing necessity and possibility), deontic (for permissions and obligations), epistemic (to reason about knowledge) and temporal modalities. On the other hand, separation logic [48, 45] is a family of assertion languages originally conceived to perform Hoare-style verification [39] of programs with mutable data structures. The key components of separation logic are its non-classical connectives, that allow us to reason about updates of the models. For example, the formula  $\phi * \psi$  uses the *separating conjunction*  $*$ , which requires to split a model into two disjoint pieces, one satisfying  $\phi$  and the other one satisfying  $\psi$ . Nowadays, there exists a wide variety of such languages, including propositional separation logic, first-order separation logic, and other variants with reachability predicates, just to name a few. Over the past years, several approaches combining modal and separation logics have appeared. In most cases, the modal and the separation dimensions are orthogonal (see e.g. [14, 18, 10, 17]), allowing us to design decision procedures by combinations of procedures from each dimension. However, recently, combinations of such operators interpreted over the same structures have been considered, such as the Modal Logics of Heaps (MLH) from [23], and the Modal Separation Logics (MSL) from [24]. In this way, the underlying modal relational model can be also seen as a memory state from separation logic: states can be seen as memory locations, and edges can be seen as links between these locations.

These efforts on combining separation and modal logics witness the numerous attempts to use separation logic in different contexts. When interpreted on sets, separation logic can be used to model some particular phenomena in belief revision [38]. A separation logic combined with modalities is introduced in [17] to capture how resources evolve not only in one particular state, but also in different states. In epistemic separation logic [19], models have equivalence relations representing possible worlds, which are resources that can be separated. This logic is extended in [20] with *public announcements*. These announcements are logical formulae that

restrict the model to those states satisfying such formulae. Lastly, in [41] operators from temporal and separation logics are combined, allowing to express both temporal and spatial conditions in search control knowledge for AI planning (see also [11]). All these examples illustrate the wealth of combinations of modal and separating connectives. Our present work contributes to this line of research, but is theoretical in nature and is rather focused on the design of internal proof systems.

From a logical perspective, modal operators to perform updates on a relational model can be seen as weaker versions or variants of separating connectives, since they all have similar effects: updating the model (by adding, removing or changing some feature of the model) while evaluating a formula. For example, consider the sabotage modal logic SML introduced in [53] (see [37] for application in formal learning theory). SML is an extension of the basic modal language with a so-called sabotage operator which (in one of its variants) deletes one arrow of the model when it is evaluated. This operator can be seen as a weak version of the separating conjunction that separates only one edge from the rest of the model (see [24] for details). Other examples of dynamic logics that perform changes on the accessibility relation of a model are investigated in [3, 4], whereas examples of logics used to describe graph evolution in games can be found in [21, 51].

**Proof systems and model updates.** Due to their ability to perform updates on a relational model, designing proof methods for separation logics and for its aforementioned relatives is known to be a non-trivial task. As a matter of fact, no proof system without features external from the logical language was known for the above-mentioned logics until the recent works [28, 27]. For instance, there exist tableaux-based procedures to check satisfiability of sabotage logics [5] and for other modal logics with update operators [3], but model updates are handled with labels. Similarly, there exist labeled tableaux calculi for the epistemic separation logics from [19, 20, 17]. On the other hand, there are no Hilbert-style calculi apart from [28, 27], as it is extremely challenging to axiomatise these logics that do not satisfy the uniform substitution rule (see e.g. [4]), since most proof-theoretical techniques rely on closure under this rule.

It is also worth noting that Boolean BI [43, 35, 12] and its variants such as the logic of bunched implications BI, are known as being the logical kernel of separation logics. The idea of adding modalities to Boolean BI, to its variants or, to related logical formalisms taking advantage of the computational interpretation of BI already appeared in [44, 46] (see also [43, Chapter 9]). It has been further developed in several directions, for instance by providing a modal extension to BI to reason about dynamic resources [16], see also related extensions in [15, 18, 1]. All these foundational works about BI, its variants and its extensions with modalities (including the design of proof systems and the quest for finding adequate semantical structures [36]) could be reused to study modal separation logics. At least, these works could inspire the developments of proof-theoretical tools for logical formalisms that mix modalities and composition/separation operators.

Herein, we pursue a research program about modal separation logics. We aim to better understand the computational complexity of their decision problems and to design proof systems, typically sequent-style calculi or Hilbert-style calculi. These calculi clearly have an historical value but also provide essential means to grasp what are the core validities and rules of the logical formalisms, see a recent illustration in [2]. It should be noted that not all modal separation logics admit finite axiomatisation, see e.g. [24], and sometimes, the axiomatisation of abstract separation logics requires the need for external features such as nominals or labels, see e.g. [13, 40]. In this work, we adopt a puristic approach to design internal Hilbert-style proof systems for the very logical language without any external help. In the context of modal separation logics, this is a requirement that happens to be rewarding for understanding their expressive power, considering that such logics freely mix modal operators and separating connectives having global effects on the models. However, in this work we use the assertion language component of separation logics without considering the components related to the extension of Hoare logic.

**Our contribution.** We design sound and complete Hilbert-style proof systems for the modal separation logics  $\text{MSL}(*, \diamond)$  and  $\text{MSL}(*, \langle \neq \rangle)$  [24], where  $*$  is the separating conjunction,  $\diamond$  is the standard modal operator and  $\langle \neq \rangle$  is the difference modality. In addition, the two logics contain

the emptiness constant  $\mathbf{emp}$ . So, in this paper, we rather focus on the design of adequate internal proof systems without addressing the question of efficient mechanisation. For both logics, we provide a syntactical treatment to the semantical abstractions used to decide the satisfiability problem of such logics in [24], leading to NP-completeness. Each formula is shown equivalent to a Boolean combination of *core formulae* (also called *test formulae*): simple formulae of the logic expressing elementary properties about the models. More precisely, each elementary property consists of a “*modal part*” (describing partially the structure of the model), and a “*size part*” (related to the number of edges). Thus, we show how to introduce axioms to transform every formula into a Boolean combination of core formulae, together with axioms to deal with these simple formulae. This result borrows some ideas from the Gaifman’s Theorem in first-order logic [31], which states that every first-order sentence is logically equivalent to a Boolean combination of so-called local formulae. A similar strategy is rather standard for axiomatising dynamic epistemic logics [55, 54, 56, 33] with the introduction of *reduction axioms*. In this technique, it is essential to translate each formula containing a dynamic operator into a formula without it, by using provably equivalent formulae. Then, completeness follows from the completeness of the system for the ‘basic’ language (see also a similar approach for the linear  $\mu$ -calculus in [30]). In our case, another difficulty arises as we also have to design an axiomatisation for such Boolean combinations. The proof system for  $\text{MSL}(*, \diamond)$  (Sec. 3) uses only partially the standard machinery for modal logic, for example the modal part differs from the Hilbert-style axiomatisation for the modal logic  $\text{Alt}_1$ , i.e., the modal logic over deterministic frames, characterised by the axiom  $\diamond p \Rightarrow \Box p$  (see e.g. [6]). For  $\text{MSL}(*, \langle \neq \rangle)$  (Sec. 4), the modal part extends results from [50] to infinite models (a peculiarity of modal separation logics as the set of locations is infinite). These constructions give us an exact characterisation of the properties that can be expressed on each logic. Moreover, it is also remarkable to have axiomatisations for these two NP-complete logics, since the full logic  $\text{MSL}$  (including the separating implication) is not (finitely) axiomatisable [24].

This paper is an extended version of [25] with more explanations, more examples and with all the derivations and proofs.

## 2 Preliminaries about modal separation logics

We briefly recall the definition of the modal separation logic  $\text{MSL}(*, \diamond, \langle \neq \rangle)$  introduced in [24]. The full version  $\text{MSL}$  [24] with the separating implication  $\rightarrow$  is omitted as it is not part of our investigation, apart from the fact that it is known not to admit a finite axiomatisation [24].

Let  $\text{PROP} = \{p, q, \dots\}$  be a countably infinite set of propositional symbols. Formulae of the language  $\text{MSL}(*, \diamond, \langle \neq \rangle)$  are defined by the grammar:

$$\phi ::= p \mid \mathbf{emp} \mid \neg\phi \mid \phi \wedge \phi \mid \diamond\phi \mid \langle \neq \rangle\phi \mid \phi * \phi,$$

where  $p \in \text{PROP}$ . Other connectives are defined as usual, in particular:

$$\begin{array}{llll} \perp \stackrel{\text{def}}{=} \mathbf{emp} \wedge \neg\mathbf{emp}; & \top \stackrel{\text{def}}{=} \neg \perp; & \phi \vee \psi \stackrel{\text{def}}{=} \neg(\neg\phi \wedge \neg\psi); & \phi \Rightarrow \psi \stackrel{\text{def}}{=} \neg\phi \vee \psi; \\ \Box\phi \stackrel{\text{def}}{=} \neg\diamond\neg\phi; & [\neq]\phi \stackrel{\text{def}}{=} \neg\langle \neq \rangle\neg\phi; & \langle U \rangle\phi \stackrel{\text{def}}{=} \phi \vee \langle \neq \rangle\phi; & [U]\phi \stackrel{\text{def}}{=} \neg\langle U \rangle\neg\phi. \end{array}$$

A *model* is a tuple  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  such that

- the set of *locations* is the set of natural numbers  $\mathbb{N}$ ,
- $\mathfrak{R} \subseteq \mathbb{N} \times \mathbb{N}$  is finite and weakly functional (i.e.  $(l, l') \in \mathfrak{R}$  and  $(l, l'') \in \mathfrak{R}$  imply  $l' = l''$ ) and,
- $\mathfrak{V} : \text{PROP} \rightarrow \mathcal{P}(\mathbb{N})$  is a valuation.

In the rest of the document, by ‘functional’, we mean ‘weakly functional’. Since separation logics are interpreted on structures representing heaps [7], this explains why in the models, the domain is  $\mathbb{N}$  (an infinite set of *locations*), and the accessibility relation is finite and functional (formal relationships with separation logics can be found in [24, Sec. 2.2]). The models  $\mathfrak{M}_1 = \langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle$  and  $\mathfrak{M}_2 = \langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle$  are *disjoint* if  $\mathfrak{R}_1 \cap \mathfrak{R}_2 = \emptyset$ ; when this holds,  $\mathfrak{M}_1 \uplus \mathfrak{M}_2$  denotes the model


corresponding to the disjoint union of  $\mathfrak{M}_1$  and  $\mathfrak{M}_2$ , i.e.,  $\mathfrak{M}_1 \uplus \mathfrak{M}_2 = \langle \mathbb{N}, \mathfrak{R}_1 \uplus \mathfrak{R}_2, \mathfrak{V} \rangle$ . We say  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  is a partition of  $\mathfrak{R}$ , if  $\mathfrak{R}_1 \cap \mathfrak{R}_2 = \emptyset$  and  $\mathfrak{R} = \mathfrak{R}_1 \cup \mathfrak{R}_2$ . Given  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  and  $l \in \mathbb{N}$ , the satisfaction relation  $\models$  is defined below:

$$\begin{array}{ll}
\mathfrak{M}, l \models p & \stackrel{\text{def}}{\iff} l \in \mathfrak{V}(p) \\
\mathfrak{M}, l \models \text{emp} & \stackrel{\text{def}}{\iff} \mathfrak{R} = \emptyset \\
\mathfrak{M}, l \models \neg\phi & \stackrel{\text{def}}{\iff} \mathfrak{M}, l \not\models \phi \\
\mathfrak{M}, l \models \phi \wedge \psi & \stackrel{\text{def}}{\iff} \mathfrak{M}, l \models \phi \text{ and } \mathfrak{M}, l \models \psi \\
\mathfrak{M}, l \models \diamond\phi & \stackrel{\text{def}}{\iff} \mathfrak{M}, l' \models \phi, \text{ for some } l' \in \mathbb{N} \text{ such that } (l, l') \in \mathfrak{R} \\
\mathfrak{M}, l \models \langle \neq \rangle \phi & \stackrel{\text{def}}{\iff} \mathfrak{M}, l' \models \phi, \text{ for some } l' \in \mathbb{N} \text{ such that } l' \neq l \\
\mathfrak{M}, l \models \phi_1 * \phi_2 & \stackrel{\text{def}}{\iff} \langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models \phi_1 \text{ and } \langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \phi_2, \\
& \text{for some partition } \{\mathfrak{R}_1, \mathfrak{R}_2\} \text{ of } \mathfrak{R}.
\end{array}$$

The semantics for the modal operators and the separating connectives is the standard one, see e.g. [8, 48]. We always consider the Boolean part and the emptiness constant  $\text{emp}$ , and we put between parentheses the rest of (separating or modal) connectives we are considering. The main two logics we consider are  $\text{MSL}(*, \diamond)$  and  $\text{MSL}(*, \langle \neq \rangle)$ . Notice that even though  $\text{emp}$  can be taken as a shortcut for  $[\text{U}]\square\perp$ , it is not expressible in any of the mentioned fragments, since it uses modalities from both logics. Therefore, we need to include it as a primitive in the language. The computational complexity of the satisfiability problems for the logics considered here has been characterised. Recall that the class TOWER mentioned in Prop. 1, is the class of problems of time complexity bounded by a tower of exponentials, whose height is an elementary function of the input (see [49] for details).

**Proposition 1** ([24]). *The satisfiability problems for  $\text{MSL}(*, \diamond)$  and  $\text{MSL}(*, \langle \neq \rangle)$  are NP-complete, whereas the problem for  $\text{MSL}(*, \diamond, \langle \neq \rangle)$  is TOWER-complete.*

Refinements about TOWER-hardness can be found in [42, Section 4.3]. To illustrate the expressive power of  $\text{MSL}(*, \diamond)$ , let us define  $\text{loop}_1$ , which states that the model consists of a single reflexive edge at the evaluation point  $l$ :

$$\neg\text{emp} \wedge \neg(\neg\text{emp} * \neg\text{emp}) \wedge \diamond\diamond\top$$


By way of example, let us show that for all models  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  and  $l \in \mathbb{N}$ , we have  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \text{loop}_1$  iff  $\mathfrak{R} = \{(l, l)\}$ . First note that  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \neg\text{emp}$  iff  $\mathfrak{R} \neq \emptyset$ . Similarly, one can show that  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \neg(\neg\text{emp} * \neg\text{emp})$  iff  $\text{card}(\mathfrak{R}) \leq 1$ . Consequently,  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \neg\text{emp} \wedge \neg(\neg\text{emp} * \neg\text{emp})$  iff  $\text{card}(\mathfrak{R}) = 1$ . Now, suppose that  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \text{loop}_1$ . Consequently,  $\text{card}(\mathfrak{R}) = 1$ . Because  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \diamond\diamond\top$ , there are  $l_1$  and  $l_2$  such that  $(l, l_1) \in \mathfrak{R}$  and  $(l_1, l_2) \in \mathfrak{R}$ . As  $\mathfrak{R}$  contains a unique element, we get  $l = l_1$  and  $l_1 = l_2$ , whence  $\mathfrak{R} = \{(l, l)\}$ . Conversely, let  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  and  $l \in \mathbb{N}$  be such that  $\mathfrak{R} = \{(l, l)\}$ . Obviously,  $\text{card}(\mathfrak{R}) = 1$  and therefore  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \neg\text{emp} \wedge \neg(\neg\text{emp} * \neg\text{emp})$ . Moreover, we have  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \diamond\diamond\top$  as  $(l, l) \in \mathfrak{R}$  and  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \diamond\top$ . Consequently,  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle, l \models \text{loop}_1$ .

Moreover, it is possible to define the formula  $\text{loop}_2$  whose satisfaction on a location  $l$  means that the model contains exactly a loop of length 2 visiting  $l$ :

$$(\neg\text{emp} * \neg\text{emp}) \wedge \neg(\neg\text{emp} * \neg\text{emp} * \neg\text{emp}) \wedge \diamond\diamond\diamond\top \wedge \neg(\neg\text{emp} * \diamond\diamond\diamond\top) \wedge \neg\diamond(\neg\text{emp} * \diamond\diamond\diamond\top)$$



Notice that  $*$  is associative. Obviously, these properties cannot be expressed in the modal logic  $\text{Alt}_1$  (for instance, we cannot express global properties in  $\text{Alt}_1$ ).

So, in this paper, we aim at providing Hilbert-style axiomatisations for the logics  $\text{MSL}(*, \diamond)$  and  $\text{MSL}(*, \langle \neq \rangle)$ , which amounts to characterise syntactically the set of valid formulae by means of a proof system. By contrast, the complexity results from [24] are obtained semantically, without any proof-theoretical analysis.

### 3 Axiomatising $\text{MSL}(*, \diamond)$ with core formulae

In this section, we define  $\mathcal{H}\text{MSL}(*, \diamond)$ , an axiomatic proof system for  $\text{MSL}(*, \diamond)$ , i.e. the modal separation logic restricted to the separating conjunction  $*$  and to the modal diamond  $\diamond$ .

To do so, we introduce a set of *core formulae* that are simple  $\text{MSL}(*, \diamond)$  formulae capturing essential properties of the models. As shown later on, every  $\text{MSL}(*, \diamond)$  formula is logically equivalent to a Boolean combination of core formulae. However, as every core formula is shown to be an  $\text{MSL}(*, \diamond)$  formula, (and therefore we remain in the original object language), we can derive an axiomatisation of  $\text{MSL}(*, \diamond)$  by axiomatising Boolean combinations of core formulae. This idea is similar, for instance, to the strategy followed in dynamic epistemic logics with the introduction of reduction axioms [55, 54, 56]: each formula containing a dynamic modality is equivalent to a formula without it, so completeness follows from the completeness of the system for the language without dynamic modalities. In our case, we will provide a complete system for core formulae. So, we define three sets of axioms and inference rules:

1. those dedicated to the propositional logic of core formulae,
2. those that, given a Boolean combination of core formulae  $\phi$ , allow to derive a Boolean combination of core formulae that is equivalent to  $\diamond\phi$  (a property called herein  $\diamond$ -elimination, see Lemma 8), and
3. those that, given two Boolean combinations of core formulae  $\phi_1, \phi_2$ , allow to derive a Boolean combination of core formulae that is equivalent to  $\phi_1 * \phi_2$  (a property called herein  $*$ -elimination, see Lemma 12).

#### 3.1 Core formulae for $\text{MSL}(*, \diamond)$

Core formulae are divided into two families: a set of *size formulae* that express properties about the size of the model (i.e. the number of edges) and a set of *graph formulae* describing the shape of the model that is observable from the current location (typically linked lists, see e.g. [29, 47, 57, 52]). As the relation  $\mathfrak{R}$  in models is functional, the number of distinct shapes is limited, ranging from lasso shapes to segments with dead-end.

Let us introduce expressions of the form  $\mathbf{size} \geq \beta$  that hold true whenever the accessibility relation  $\mathfrak{R}$  has at least  $\beta$  elements (the symbol  $\beta$  always refers to a natural number throughout the paper). A *size literal* is a formula of the form  $\mathbf{size} \geq \beta$  or  $\neg\mathbf{size} \geq \beta$ . Every Boolean combination of size literals is a *size formula*. We also use  $\mathbf{size} = \beta$  as an abbreviation for  $\mathbf{size} \geq \beta \wedge \neg\mathbf{size} \geq \beta + 1$ . At this stage, it is worth noting that  $\mathbf{size} \geq \beta$  should be understood as a built-in atomic formula enriching the logical language for  $\text{MSL}(*, \diamond)$ . However, as it will quickly appear below,  $\mathbf{size} \geq \beta$  can be characterised with a formula of  $\text{MSL}(*, \diamond)$  and later on in the document, such occurrences of  $\mathbf{size} \geq \beta$  should be understood as mere abbreviations. The same distinction applies to the graph formulae defined below.

*Graph formulae* describe the shape of a portion of the model, partly inspired from the semantical notion of abstract frame from [24] but with constraints on propositional variables. Formally, every graph formula is an expression derived from the non-terminal  $\mathcal{G}$  of the grammar below:

$$\ell := \top \mid \perp \mid p \mid \neg p \quad Q := \ell \mid Q \wedge Q \quad \mathcal{G} := |Q, \dots, Q| \mid |Q, \dots, Q| \mid |Q, \dots, \overline{Q}, \dots, \overline{Q}|,$$

where  $p \in \text{PROP}$ , and  $\mathcal{G}$  must contain at least one conjunction  $Q$ . By slightly abusing the standard terminology, expressions of the form  $\ell$  are called *literals*. A conjunction  $Q$  is *contradictory* whenever  $\perp$  occurs in  $Q$  or there is some  $p$  such that both  $p$  and  $\neg p$  occur in  $Q$ . Note that  $Q$  is contradictory iff  $Q$  is unsatisfiable. By convention, contradictory conjunctions are denoted by  $Q^\perp$ . A graph formula is *contradictory* if at least one of its conjunctions is contradictory. Note also that the semantics for graph formulae shall guarantee that a graph formula is contradictory iff it is unsatisfiable.

Since we are working on weakly functional and finite relations, graph formulae represent paths satisfying a conjunction of literals  $Q$  at each position. A formula of the form  $|Q_1, \dots, Q_n\rangle$  expresses that there exists a path of length  $n$  in which all the locations are distinct of each other, and we do

not know whether it continues after. The formula  $|Q_1, \dots, Q_n|$  states that there is a path of length  $n - 1$ , all the locations are distinct, and the last location has no successor. Finally, the formula of the form  $|Q_1, \dots, \overleftarrow{Q_i, \dots, Q_n}|$  expresses that there is a path of size  $n - 1$  with all distinct locations, and there is an edge from the location in position  $n$  and the one in the position  $i$  (lasso shape). The figure below illustrates which models are related to the graph formulae defined above.

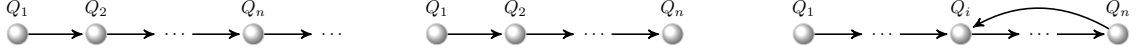


Figure 1: Models for the graph formulae  $|Q_1, \dots, Q_n|$ ,  $|Q_1, \dots, Q_n|$  and  $|Q_1, \dots, \overleftarrow{Q_i, \dots, Q_n}|$ , respectively.

We write  $|Q_1, \dots, Q_n?|$  to refer to graph formulae of any kind. Moreover, we write  $|Q, \dots, Q'?(n)|$  to express that the last argument  $Q'$  of the corresponding graph formula is at position  $n$ . For example,  $|\top, \dots, \top|_{(4)}$  stands for  $|\top, \top, \top, \top|$ . Lastly, we define the *graph size*  $\#(|Q_1, \dots, Q_n?|)$  of  $|Q_1, \dots, Q_n?|$  as follows:

$$\#(|Q_1, \dots, Q_n|) \stackrel{\text{def}}{=} n \quad \#(|Q_1, \dots, Q_n|) \stackrel{\text{def}}{=} n-1 \quad \#(|Q_1, \dots, \overleftarrow{Q_i, \dots, Q_n}|) \stackrel{\text{def}}{=} n.$$

Given a model  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  and  $l \in \mathbb{N}$ , the satisfaction relation  $\models$  is extended to core formulae:

$$\begin{aligned} \mathfrak{M}, l \models \text{size} \geq \beta & \stackrel{\text{def}}{\iff} \text{card}(\mathfrak{R}) \geq \beta \\ \mathfrak{M}, l \models |Q_1, \dots, Q_n| & \stackrel{\text{def}}{\iff} \text{there are distinct } l_1, \dots, l_{n+1} \text{ such that } l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_n \mathfrak{R} l_{n+1}, \\ & \text{and for all } j \in [1, n], \mathfrak{M}, l_j \models Q_j \\ \mathfrak{M}, l \models |Q_1, \dots, Q_n| & \stackrel{\text{def}}{\iff} \text{there are distinct } l_1, \dots, l_n \text{ such that } l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_{n-1} \mathfrak{R} l_n, \\ & \mathfrak{R}(l_n) = \emptyset \text{ and for all } j \in [1, n], \mathfrak{M}, l_j \models Q_j \\ \mathfrak{M}, l \models |Q_1, \dots, \overleftarrow{Q_i, \dots, Q_n}| & \stackrel{\text{def}}{\iff} \text{there are distinct } l_1, \dots, l_n \text{ such that } l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_n \mathfrak{R} l_i, \\ & \text{and for all } j \in [1, n], \mathfrak{M}, l_j \models Q_j. \end{aligned}$$

Below, we establish that every core formula has a logically equivalent counterpart in  $\text{MSL}(*, \diamond)$  (Lemma 2). This is an essential property as these formulae are the building blocks of the axiomatisation of  $\text{MSL}(*, \diamond)$ . Consequently, we obtain that our axioms are only made of  $\text{MSL}(*, \diamond)$  formulae, with no need of external properties or extra machinery such as nominals or labels.

For every core formula  $\psi$ , we define its *extension*  $\text{ext}(\psi)$  in  $\text{MSL}(*, \diamond)$ .

- $\text{ext}(\text{size} \geq 0) \stackrel{\text{def}}{=} \top$  and  $\text{ext}(\text{size} \geq \beta) \stackrel{\text{def}}{=} \overbrace{\neg \text{emp} * \dots * \neg \text{emp}}^{\beta \text{ times}}$  for  $\beta > 0$ .
- $\text{ext}(|Q|) \stackrel{\text{def}}{=} Q \wedge \neg \diamond \top$ . For  $n \geq 2$ ,  $\text{ext}(|Q_1, Q_2, \dots, Q_n|) \stackrel{\text{def}}{=} Q_1 \wedge \diamond \text{ext}(|Q_2, \dots, Q_n|)$ .
- $\text{ext}(|Q_1, \dots, Q_n|) \stackrel{\text{def}}{=} \text{ext}(|Q_1, \dots, Q_n, \top|) * \top$ . So,  $\text{ext}(|Q_1, \dots, Q_n|)$  is equal to the formula below:

$$(\diamond(Q_1 \wedge \diamond(Q_2 \wedge \dots \diamond(Q_n \wedge \diamond(\top \wedge \neg \diamond \top)))))) * \top.$$

- $\text{ext}(|\overleftarrow{Q_i, \dots, Q_n}|)$  is defined as the formula

$$\top * (\text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \wedge \neg \diamond(\text{ext}(\text{size} = 1) * \diamond^n \top))$$

where  $\diamond^0 \phi \stackrel{\text{def}}{=} \phi$  and  $\diamond^{i+1} \phi \stackrel{\text{def}}{=} \diamond \diamond^i \phi$ .

- For  $i > 1$ ,  $\text{ext}(|Q_1, \dots, \overleftarrow{Q_i, \dots, Q_n}|)$  is defined as the formula

$$\begin{aligned} \top * (\text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \\ \wedge \diamond^{i-1} (\text{ext}(\text{size} = i-1) * \text{ext}(|\overleftarrow{\top, \dots, \top}|_{(n-i+1)}))) \end{aligned}$$

**Lemma 2.** *Every core formula  $\psi$  is logically equivalent to  $\text{ext}(\psi)$ .*

*Proof.* Let us start with the case  $\psi = \text{size} \geq \beta$ , which is completely standard. For the base case  $\beta = 0$ , obviously  $\mathfrak{M}, l \models \text{size} \geq 0$  always holds, as well as  $\mathfrak{M}, l \models \text{ext}(\text{size} \geq 0) = \top$ . Similarly,

note that  $\mathfrak{M}, l \models \text{size} \geq 1$  iff  $\text{card}(\mathfrak{R}) \geq 1$  (by definition of  $\models$  for  $\text{size} \geq \beta$ ) iff  $\mathfrak{M}, l \models \neg \text{emp}$  (by definition of  $\models$  for  $\text{emp}$ ) iff  $\mathfrak{M}, l \models \text{ext}(\text{size} \geq 1)$  (by definition of  $\text{ext}(\cdot)$ ). Suppose that the property holds for  $\text{size} \geq \beta$ , and let us show that  $\mathfrak{M}, l \models \text{size} \geq \beta + 1$  iff  $\mathfrak{M}, l \models \text{ext}(\text{size} \geq \beta + 1)$ . Let  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  be a model, and  $l \in \mathbb{N}$  be a location. The statements below are equivalent:

- i.  $\mathfrak{M}, l \models \text{size} \geq \beta + 1$ ,
- ii.  $\text{card}(\mathfrak{R}) \geq \beta + 1$  (by definition of  $\models$  on core formulae),
- iii. there is a partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$  such that  $\text{card}(\mathfrak{R}_1) \geq 1$  and  $\text{card}(\mathfrak{R}_2) \geq \beta$ ,
- iv. there is a partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$  such that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models \neg \text{emp}$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \text{size} \geq \beta$  (by definition of  $\models$  on core formulae),
- v. there is a partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$  such that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models \neg \text{emp}$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \text{ext}(\text{size} \geq \beta)$  (by the induction hypothesis),
- vi.  $\mathfrak{M}, l \models \neg \text{emp} * \text{ext}(\text{size} \geq \beta)$  (by definition of  $\models$  for the separating conjunction),
- vii.  $\mathfrak{M}, l \models \text{ext}(\text{size} \geq \beta + 1)$  (by definition of  $\text{ext}(\cdot)$ ).

Let us consider the case  $\psi = |Q_1, Q_2, \dots, Q_n|$ . The proof is by induction on  $n$  with the base case  $n = 1$ . Let  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  be a model, and  $l \in \mathbb{N}$  be a location. The statements below are equivalent:

- i.  $\mathfrak{M}, l \models |Q|$ ,
- ii.  $\mathfrak{M}, l \models Q$  and there is no  $l'$  such that  $\mathfrak{R}l'$  (by definition of  $\models$  on core formulae),
- iii.  $\mathfrak{M}, l \models Q \wedge \neg \diamond \top$  (by definition of  $\models$ ),
- iv.  $\mathfrak{M}, l \models \text{ext}(|Q|)$  (by definition of  $\text{ext}(\cdot)$ ).

Now, suppose that the property holds for graph formulae of graph size  $n - 2$ , and let us show that  $\mathfrak{M}, l \models |Q_1, Q_2, \dots, Q_n|$  iff  $\mathfrak{M}, l \models \text{ext}(|Q_1, Q_2, \dots, Q_n|)$  (remember that  $|Q_1, Q_2, \dots, Q_n|$  is of graph size  $n - 1$ ). The statements below are equivalent:

- i.  $\mathfrak{M}, l \models |Q_1, Q_2, \dots, Q_n|$ ,
- ii. there are distinct  $l_1, l_2, \dots, l_n$  such that  $l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_{n-1} \mathfrak{R} l_n$ , there is no  $l'$  such that  $l_n \mathfrak{R} l'$  and for each  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$  (by definition of  $\models$  on core formulae),
- iii.  $\mathfrak{M}, l \models Q_1$  and there are distinct  $l_2, \dots, l_n$  such that  $l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_{n-1} \mathfrak{R} l_n$ , there is no  $l'$  such that  $l_n \mathfrak{R} l'$ , and for each  $j \in [2, n]$ ,  $\mathfrak{M}, l_j \models Q_j$ , by definition and noticing that “there is no  $l'$  such that  $l_n \mathfrak{R} l'$ ” implies that  $l_1$  is different from any  $l_j$ ,  $j \in [2, n]$ ;
- iv.  $\mathfrak{M}, l \models Q_1$  and  $\mathfrak{M}, l \models \diamond |Q_2, \dots, Q_n|$  (by definition of  $\models$  on core formulae),
- v.  $\mathfrak{M}, l \models Q_1$  and  $\mathfrak{M}, l \models \diamond \text{ext}(|Q_2, \dots, Q_n|)$  (by the induction hypothesis),
- vi.  $\mathfrak{M}, l \models Q_1 \wedge \diamond \text{ext}(|Q_2, \dots, Q_n|)$ ,
- vii.  $\mathfrak{M}, l \models \text{ext}(|Q_1, Q_2, \dots, Q_n|)$  (by definition of  $\text{ext}(\cdot)$ ).

Let us consider the case  $\psi = |Q_1, \dots, Q_n|$ . We have the following equivalences:

- i.  $\mathfrak{M}, l \models |Q_1, \dots, Q_n|$ ,
- ii. there are distinct  $l_1, \dots, l_{n+1}$  such that  $l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_n \mathfrak{R} l_{n+1}$ , and for all  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$  (by definition of  $\models$  on core formulae),



- iii. there are distinct  $l_1, \dots, l_{n+1}$  and there exists a partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$  such that  $\mathfrak{R}_1 = \{(l, l_2), \dots, (l_n, l_{n+1})\}$  (and therefore there is no  $l'$  such that  $l_{n+1} \mathfrak{R}_1 l'$ ) and for all  $j \in [1, n]$ ,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l_j \models Q_j$ ,
- iv. there is a partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$  such that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models |Q_1, \dots, Q_n, \top|$  (by definition of  $\models$  on core formulae),
- v. there is a partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$  such that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(|Q_1, \dots, Q_n, \top|)$  (by the proof of the previous case),
- vi.  $\mathfrak{M}, l \models \text{ext}(|Q_1, \dots, Q_n, \top|) * \top$  (by definition on  $\models$  for the separating conjunction),
- vii.  $\mathfrak{M}, l \models \text{ext}(|Q_1, \dots, Q_n|)$  (by definition of  $\text{ext}(\cdot)$ ).

Now let us treat the case  $\psi = |\overline{Q_1, \dots, Q_n}|$ . Again, let  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{W} \rangle$  be a model, and  $l \in \mathbb{N}$  be a location, suppose  $\mathfrak{M}, l \models |\overline{Q_1, \dots, Q_n}|$ .

- i. By definition of  $\models$ , there are distinct  $l_1, \dots, l_n$  such that  $l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_n \mathfrak{R} l_1$  and for all  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$ . We partition  $\mathfrak{R}$  into  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$  such that  $\mathfrak{R}_1 = \{(l, l_2), \dots, (l_{n-1}, l_n), (l_n, l)\}$ .
- ii. By definition of  $\mathfrak{R}_1$ , it trivially holds that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{size} = n$  and  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond^{n+1} \top$ . By the previous cases, we also have  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(\text{size} = n)$ .
- iii.  $\mathfrak{R}_1$  can be partitioned into  $\mathfrak{R}'_1$  and  $\mathfrak{R}''_1$  such that  $\mathfrak{R}'_1 = \{(l, l_2), \dots, (l_{n-1}, l_n)\}$ . By (i), we conclude  $\langle \mathbb{N}, \mathfrak{R}'_1, \mathfrak{W} \rangle, l \models |Q_1, \dots, Q_n|$ , then  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models |Q_1, \dots, Q_n| * \top$ . By the previous cases, we also get  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(|Q_1, \dots, Q_n|) * \top$ .
- iv. Lastly, ad absurdum, suppose  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond(\text{ext}(\text{size} = 1) * \diamond^n \top)$ . Then, as  $l \mathfrak{R}_1 l_2$ , it holds that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l_2 \models (\text{ext}(\text{size} = 1) * \diamond^n \top)$ . However, this is contradictory, as by splitting  $\mathfrak{R}_1 = \{(l, l_2), \dots, (l_{n-1}, l_n), (l_n, l)\}$  into two non-empty relations, it is not possible to have a path of length at least  $n$ , starting from  $l_2$ . Then,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \neg \diamond(\text{ext}(\text{size} = 1) * \diamond^n \top)$ .
- v. Since  $\mathfrak{R}_1 \subseteq \mathfrak{R}$ , from (ii), (iii) and (iv) we conclude that  $\mathfrak{M}, l$  satisfies  $\top * (\text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \wedge \neg \diamond(\text{ext}(\text{size} = 1) * \diamond^n \top))$ , which is precisely equal to  $\text{ext}(|\overline{Q_1, \dots, Q_n}|)$  by definition.

Conversely, suppose now that  $\mathfrak{M}, l$  satisfies

$$\top * (\text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \wedge \neg \diamond(\text{ext}(\text{size} = 1) * \diamond^n \top)).$$

Then,

- i. there is a relation  $\mathfrak{R}_1 \subseteq \mathfrak{R}$  such that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \wedge \neg \diamond(\text{ext}(\text{size} = 1) * \diamond^n \top)$ .
- ii. As  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models (\text{ext}(|Q_1, \dots, Q_n|) * \top)$ , by the previous cases and by definition, there are distinct  $l_1, \dots, l_n$  such that  $l = l_1 \mathfrak{R}_1 l_2 \mathfrak{R}_1 \dots \mathfrak{R}_1 l_n$  and for each  $j \in [1, n]$ , we have  $\mathfrak{M}, l_j \models Q_j$ .
- iii. From (ii) and since  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top$ , we conclude that  $\mathfrak{R}_1$  must be of the form  $\mathfrak{R}_1 = \{(l, l_2), \dots, (l_{n-1}, l_n), (l_n, \bar{l})\}$ . As  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond^{n+1} \top$ , necessarily  $\bar{l}$  is an element among  $l, l_2, \dots, l_n$ . Therefore, it holds that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models |Q_1, \dots, \overline{Q_i, \dots, Q_n}|$  for some  $i$ . It remains to prove that  $i = 1$ .
- iv. Suppose  $i \neq 1$ . Then consider the partition  $\{\mathfrak{R}'_1, \mathfrak{R}''_1\}$  of  $\mathfrak{R}_1$  such that

$$\mathfrak{R}'_1 = \{(l, l_2)\} \quad \mathfrak{R}''_1 = \{(l_2, l_3), \dots, (l_i, l_{i+1}), \dots, (l_{n-1}, l_n), (l_n, l_i)\}.$$

Then, trivially  $\langle \mathbb{N}, \mathfrak{R}'_1, \mathfrak{W} \rangle, l_2 \models \text{ext}(\text{size} = 1)$  and  $\langle \mathbb{N}, \mathfrak{R}''_1, \mathfrak{W} \rangle, l_2 \models \diamond^n \top$ , as in  $\mathfrak{R}''_1$  there is a loop involving  $l_i, \dots, l_n$ . Then  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l_2 \models \text{ext}(\text{size} = 1) * \diamond^n \top$  as  $\mathfrak{R}'_1 \uplus \mathfrak{R}''_1 = \mathfrak{R}_1$ . Lastly, since  $l \mathfrak{R}_1 l_2$  by definition, it holds that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond(\text{ext}(\text{size} = 1) * \diamond^n \top)$ ; a contradiction. Then, it must be that  $i = 1$  and  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models |\overline{Q_1, \dots, Q_n}|$ .

- v. From (iv) and since  $\mathfrak{R}_1 \subseteq \mathfrak{R}$ , by definition of  $\overline{|Q_1, \dots, Q_n|}$  we conclude that  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{W} \rangle, l \models \overline{|Q_1, \dots, Q_n|}$ .

Lastly, let us treat the case  $\psi = |Q_1, \dots, \overline{|Q_i, \dots, Q_n|}$  with  $n \geq i \geq 2$ . Suppose  $\mathfrak{M}, l \models |Q_1, \dots, \overline{|Q_i, \dots, Q_n|}$ .

- i. By definition of  $\models$ , there are distinct  $l_1, \dots, l_n$  such that  $l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots \mathfrak{R} l_n \mathfrak{R} l_i$  and for all  $j \in [1, n]$   $\mathfrak{M}, l_j \models Q_j$ . Then, we partition  $\mathfrak{R}$  into  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$  such that  $\mathfrak{R}_1 = \{(l, l_2), \dots, (l_i, l_{i+1}), \dots, (l_{n-1}, l_n), (l_n, l_i)\}$ .
- ii. From the previous cases and by definition, we have  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(\text{size} = n)$  and  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond^{n+1} \top$ .
- iii.  $\mathfrak{R}_1$  can be partitioned into  $\mathfrak{R}'_1$  and  $\mathfrak{R}''_1$  such that  $\mathfrak{R}'_1 = \{(l, l_2), \dots, (l_{n-1}, l_n)\}$ . By (i), we conclude  $\langle \mathbb{N}, \mathfrak{R}'_1, \mathfrak{W} \rangle, l \models |Q_1, \dots, Q_n|$ , then  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models |Q_1, \dots, Q_n| * \top$ . By the previous cases, this also leads to  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(|Q_1, \dots, Q_n|) * \top$ .
- iv. We partition  $\mathfrak{R}_1$  into  $\mathfrak{R}'_1$  and  $\mathfrak{R}''_1$  such that

$$\mathfrak{R}'_1 = \{(l, l_2), \dots, (l_{i-1}, l_i)\} \quad \mathfrak{R}''_1 = \{(l_i, l_{i+1}), \dots, (l_{n-1}, l_n), (l_n, l_i)\}$$

We have  $\langle \mathbb{N}, \mathfrak{R}'_1, \mathfrak{W} \rangle, l_i \models \text{ext}(\text{size} = i-1)$ . Moreover, it holds that  $\langle \mathbb{N}, \mathfrak{R}''_1, \mathfrak{W} \rangle, l_i \models \overline{|\top, \dots, \top|}_{(n-i+1)}$ . Then,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l_i \models \text{ext}(\text{size} = i-1) * \overline{|\top, \dots, \top|}_{(n-i+1)}$  as  $\mathfrak{R}'_1 \uplus \mathfrak{R}''_1 = \mathfrak{R}_1$ . Lastly, since  $\mathfrak{M}, l_i \models Q_i$  by definition,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond^{i-1}(\text{ext}(\text{size} = i-1) * \overline{|\top, \dots, \top|}_{(n-i+1)})$ . By the previous cases, we get  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond^{i-1}(\text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)}))$ .

- v. From (ii), (iii), (iv) and since  $\mathfrak{R}_1 \subseteq \mathfrak{R}$ , we conclude that  $(\mathfrak{M}, l)$  satisfies

$$\begin{aligned} & \top * (\text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \wedge \\ & \diamond^{i-1}(\text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)}))) \end{aligned}$$

Conversely, suppose now that  $\mathfrak{M}, l$  satisfies

$$\top * (\text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \wedge \diamond^{i-1}(\text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)}))).$$

- i. There is a relation  $\mathfrak{R}_1 \subseteq \mathfrak{R}$  such that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l$  satisfies

$$\text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top \wedge (\text{ext}(|Q_1, \dots, Q_n|) * \top) \wedge \diamond^{i-1}(\text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)})).$$

- ii. As  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(|Q_1, \dots, Q_n|) * \top$ , by definition and by the previous cases, there are distinct  $l_1, \dots, l_n$  such that  $l = l_1 \mathfrak{R}_1 l_2 \mathfrak{R}_1 \dots \mathfrak{R}_1 l_n$  and for each  $j \in [1, n]$ , we have  $\mathfrak{M}, l_j \models Q_j$ .
- iii. From (ii) and since  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \text{ext}(\text{size} = n) \wedge \diamond^{n+1} \top$  we conclude that  $\mathfrak{R}_1$  must be of the form  $\mathfrak{R}_1 = \{(l, l_2), \dots, (l_{n-1}, l_n), (l_n, \bar{l})\}$ , where  $\bar{l}$  is an element among  $l, l_2, \dots, l_n$ . Therefore, it holds that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle$  satisfies  $|Q_1, \dots, \overline{|Q_j, \dots, Q_n|}$  for some  $j \in [1, n]$ . It remains to prove that  $\bar{l}$  corresponds to  $l_i$ .
- iv. First, suppose  $\bar{l} = l_j$  for some  $j < i$ . Let  $\{\mathfrak{R}'_1, \mathfrak{R}''_1\}$  be a partition of  $\mathfrak{R}_1$  such that  $\langle \mathbb{N}, \mathfrak{R}'_1, \mathfrak{W} \rangle, l_i \models \text{ext}(\text{size} = i-1)$ . Since  $j < i$  there are only  $j-1$  locations (i.e.  $l, l_2, \dots, l_{j-1}$ ) that are not part of the loop involving  $l_j, \dots, l_n$ . Then, since  $i-1 > j-1$ , it cannot be that  $\mathfrak{R}''_1$  contains a loop and therefore  $\langle \mathbb{N}, \mathfrak{R}'_1, \mathfrak{W} \rangle, l_i \not\models \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)})$ . This leads to a contradiction as it holds that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \diamond^{i-1}(\text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)}))$  and therefore  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l_i \models \text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)})$ . Then,  $j \geq i$ .

- v. Suppose now that  $\bar{l} = l_j$  for  $j > i$ . Then for any relation  $\mathfrak{R}'_1 \subseteq \mathfrak{R}_1$  it cannot hold that  $\langle \mathbb{N}, \mathfrak{R}'_1, \mathfrak{B} \rangle, l_i \models \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)})$ . Again, this leads to a contradiction as it holds that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{B} \rangle, l \models \diamond^{i-1}(\text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)}))$  and therefore  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{B} \rangle, l_i \models \text{ext}(\text{size} = i-1) * \text{ext}(\overline{|\top, \dots, \top|}_{(n-i+1)})$ . Then,  $j \leq i$ .
- vi. From (iii), (iv) and (v), it follows that  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{B} \rangle, l \models |Q_1, \dots, \overline{Q_i, \dots, Q_n}|$ . Since  $\mathfrak{R}_1 \subseteq \mathfrak{R}$ , by definition of  $|Q_1, \dots, \overline{Q_i, \dots, Q_n}|$  we conclude that  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{B} \rangle, l \models |Q_1, \dots, \overline{Q_i, \dots, Q_n}|$ .

Hence, every core formula can be expressed in  $\text{MSL}(*, \diamond)$ .  $\square$

From now on, for any occurrence of a core formula  $\psi$ , including occurrences in the axioms or inference rules, we mean the  $\text{MSL}(*, \diamond)$  formula  $\text{ext}(\psi)$  so that their provisory status of built-in atomic formula is upgraded to a permanent abbreviation.

### 3.2 Preliminaries about Hilbert-style proof systems

In forthcoming Sec. 3.3, we design the Hilbert-style proof system  $\mathcal{HMSL}(*, \diamond)$  for the logic  $\text{MSL}(*, \diamond)$  (see also other calculi in Sec. 4). In this current short section, we present the main conventions we adopt along the paper, in order to present such Hilbert-style proof systems. Most probably, for the readers familiar with such proof systems, this part can be skipped. A Hilbert-style proof system  $\mathcal{HL}$  for a logic  $\mathcal{L}$  consists of a set of *axiom schemas* **Axioms** and a set of inference rules **Rules**. In this paper, both sets are always finite.

An axiom schema (simply called an axiom) is an expression that can be instantiated by formulae from  $\mathcal{L}$ , for example by replacing metavariables by formulae. In the sequel, the metavariables that can substituted by any  $\mathcal{L}$  formula are denoted by  $\phi$ ,  $\psi$  or  $\gamma$ . The axiom schemas can be also more specific by adding side-conditions or by enforcing syntactically the constraints. For instance,  $|Q_1, \dots, Q_n?$  refers to any graph formula, whereas  $Q$  (resp.  $Q^\perp$ ) refers to a non-empty (resp. contradictory) conjunction of literals as defined in Sec. 3.1. Other conventions shall be used for the axiom schemas but the associated set of instantiations should be clear from the context. Note that an axiom schema in  $\mathcal{HL}'$  where the set of  $\mathcal{L}'$  formulae extends the set of  $\mathcal{L}$  formulae possibly leads to more instantiations than for the same axiom schema in some proof system  $\mathcal{HL}$ .

An inference rule is an expression of the form  $\frac{\phi_1, \dots, \phi_n}{\phi_{n+1}}$  where  $\phi_1, \dots, \phi_{n+1}$  are axiom schemas and  $n \geq 1$ . A *proof* of a formula  $\phi$  in  $\mathcal{HL}$  is a finite sequence  $(\psi_1, \dots, \psi_N)$  such that  $\psi_N = \phi$  and for every  $i \in [1, N]$ :

- either  $\psi_i$  is an instantiation of an axiom schema from **Axioms**,
- or  $\frac{\gamma_1, \dots, \gamma_n}{\psi_i}$  is an instantiation of some inference rule  $\frac{\phi_1, \dots, \phi_n}{\phi_{n+1}}$  in **Rules**, for some subset  $\{\gamma_1, \dots, \gamma_n\} \subseteq \{\psi_1, \dots, \psi_{i-1}\}$ .

In that case, we write  $\vdash_{\mathcal{HL}} \phi$  (the subscript is omitted when the context is clear). An axiom schema is valid for  $\mathcal{L}$  whenever all its instantiations are valid for  $\mathcal{L}$ . An inference rule  $\frac{\phi_1, \dots, \phi_n}{\phi_{n+1}}$  is valid for  $\mathcal{L}$  whenever, for all its instantiations  $\frac{\gamma_1, \dots, \gamma_n}{\gamma_{n+1}}$ , if  $\gamma_1, \dots, \gamma_n$  are  $\mathcal{L}$  valid, then  $\gamma_{n+1}$  is  $\mathcal{L}$  valid.

We will introduce axiomatic systems that are weakly complete. We say that a system  $\mathcal{HL}$  is *weakly complete* if for all  $\mathcal{L}$  formulae  $\phi$ ,  $\phi$  is valid implies  $\vdash_{\mathcal{HL}} \phi$ . However, our systems are not *strongly complete*, as they will not allow us to prove that a formula  $\phi$  is derived from a set of formulae  $\Phi$ , i.e., that  $\Phi \vdash_{\mathcal{HL}} \phi$ . In the rest of the paper, we will use the term 'complete' instead of 'weakly complete'.

### 3.3 Hilbert-style proof system for $\text{MSL}(*, \diamond)$

To obtain an axiomatisation of  $\text{MSL}(*, \diamond)$ , we start by introducing the proof system  $\mathcal{H}_c$  dedicated to Boolean combinations of core formulae. As  $\text{MSL}(*, \diamond)$  includes the propositional logic,  $\mathcal{H}_c$  and

all the subsequent Hilbert-style proof systems *contain the axiom schemas and modus ponens for the propositional calculus* (the details are omitted here). The axioms whose name is of the form  $\mathbf{G}_i^?$  handle graph formulae, whereas those with names of the form  $\mathbf{S}_i^?$  handle size formulae. We start with the axioms for  $\mathbf{size} \geq \beta$ , its interactions with graph formulae and one axiom schema for inconsistent graph formulae.

Axioms for size formulae and for inconsistent graph formulae	
$(\mathbf{S}_1^c)$ $\mathbf{size} \geq 0$	$(\mathbf{G}_1^c)$ $ Q_1, \dots, Q_n? \Rightarrow \mathbf{size} \geq \#( Q_1, \dots, Q_n?)$
$(\mathbf{S}_2^c)$ $\mathbf{size} \geq \beta+1 \Rightarrow \mathbf{size} \geq \beta$	$(\mathbf{G}_2^c)$ $\neg \dots, Q^\perp, \dots?$

The semantical meaning of these axioms is straightforward. The axiom  $(\mathbf{S}_1^c)$  states that the accessibility relation of every model has always at least 0 elements. The axiom  $(\mathbf{S}_2^c)$  states that if the accessibility relation of a model has at least  $\beta+1$  elements, then it has at least  $\beta$  elements. The axiom  $(\mathbf{G}_1^c)$  is the first one handling graph formulae, and it states that if a model satisfies a graph formula  $\mathcal{G}$ , then its accessibility relation cannot have less elements than its graph size. The axiom  $(\mathbf{G}_2^c)$  states that a contradiction in a conjunction of literals, leads to a contradiction for the whole formula. We complete the definition of  $\mathcal{H}_c$  for core formulae with two families of axioms, involving graph formulae. The first family (with the axioms from  $(\mathbf{G}_3^c)$  to  $(\mathbf{G}_{13}^c)$ ) concerns conjunctions of graph formulae. In particular, given two graph formulae, these axioms allow us to derive an equivalent graph formula. Similarly, the second family (with the axioms from  $(\mathbf{G}_{14}^c)$  to  $(\mathbf{G}_{16}^c)$ ) concerns the negation of a graph formula. With these axioms, every negation of a graph formula is shown equivalent to a disjunction of graph formulae. Let us begin with the first family.

Axioms for conjunction of graph formulae	
$(\mathbf{G}_3^c)$ $\neg( \dots _{(n)} \wedge  \overline{\dots} _{(m)})$	$(\mathbf{G}_5^c)$ $\neg( \dots _{(n)} \wedge  \overline{\dots} _{(m)})$ with $n \geq m$
$(\mathbf{G}_4^c)$ $\neg( \dots _{(n)} \wedge  \dots _{(m)})$ with $n \geq m$	$(\mathbf{G}_6^c)$ $\neg( \dots _{(n)} \wedge  \dots _{(m)})$ with $n \neq m$
$(\mathbf{G}_7^c)$ $ Q_1, \dots, Q_n \rangle \wedge  Q'_1, \dots, Q'_m \rangle \Leftrightarrow  Q_1 \wedge Q'_1, \dots, Q_n \wedge Q'_n, Q'_{n+1}, \dots, Q'_m \rangle$ with $n \leq m$ ,	
$(\mathbf{G}_8^c)$ $ Q_1, \dots, Q_n \rangle \wedge  Q'_1, \dots, Q'_m \rangle \Leftrightarrow  Q_1 \wedge Q'_1, \dots, Q_n \wedge Q'_n, Q'_{n+1}, \dots, Q'_m \rangle$ with $n < m$ ,	
$(\mathbf{G}_9^c)$ $ Q_1, \dots, Q_n \rangle \wedge  Q'_1, \dots, Q'_n \rangle \Leftrightarrow  Q_1 \wedge Q'_1, \dots, Q_n \wedge Q'_n \rangle$	
$(\mathbf{G}_{10}^c)$ $\neg( Q_1, \dots, \overline{Q_i}, \dots, Q_n \rangle \wedge  Q'_1, \dots, \overline{Q'_j}, \dots, Q'_m \rangle)$ with $n \neq m$ or $i \neq j$	
$(\mathbf{G}_{11}^c)$ $ Q_1, \dots, \overline{Q_i}, \dots, Q_n \rangle \wedge  Q'_1, \dots, \overline{Q'_i}, \dots, Q'_n \rangle \Leftrightarrow  Q_1 \wedge Q'_1, \dots, \overline{Q_i} \wedge \overline{Q'_i}, \dots, Q_n \wedge Q'_n \rangle$	
$(\mathbf{G}_{12}^c)$ if $n < i \leq m$ ,	$ Q_1, \dots, Q_n \rangle \wedge  Q'_1, \dots, \overline{Q'_i}, \dots, Q'_m \rangle \Leftrightarrow  Q_1 \wedge Q'_1, \dots, Q_n \wedge Q'_n, Q'_{n+1}, \dots, \overline{Q'_i}, \dots, Q'_m \rangle$
$(\mathbf{G}_{13}^c)$ if $i \leq n < m$ ,	$ Q_1, \dots, Q_n \rangle \wedge  Q'_1, \dots, \overline{Q'_i}, \dots, Q'_m \rangle \Leftrightarrow  Q_1 \wedge Q'_1, \dots, \overline{Q_i} \wedge \overline{Q'_i}, \dots, Q_n \wedge Q'_n, Q'_{n+1}, \dots, Q'_m \rangle$

Thanks to these axioms, any conjunction of two graph formulae is valid only if it expresses properties that can be found together in a single model. For instance,  $|\dots|_{(n)} \wedge |\overline{\dots}|_{(m)}$  is clearly contradictory (see the axiom  $(\mathbf{G}_3^c)$ ), as the existence of a loop contradicts the fact that there is a dead-end (i.e. a location without successors). To ease the readability of the axioms for negation, we first define some auxiliary formulae.

$$\rho_n \stackrel{\text{def}}{=} |\top, \dots, \top \rangle_{(n)} \quad \tau_n \stackrel{\text{def}}{=} \bigvee_{i \in [1, n]} |\top, \dots, \top \rangle_{(i)} \quad \lambda_n \stackrel{\text{def}}{=} \bigvee_{\substack{i \in [1, n] \\ j \in [1, i]}} |\top, \dots, \overline{\top}_j, \dots, \top \rangle_{(i)}$$

In  $\lambda_n$ , the index  $j$  below  $\top$  indicates that the loop begins at the  $j$ -th position. We introduce the involution  $\overline{(\cdot)}$  on literals so that for every  $p \in \text{PROP}$ ,  $\overline{\overline{p}} \stackrel{\text{def}}{=} p$ ,  $\overline{\top} \stackrel{\text{def}}{=} \perp$  and  $\overline{\perp} \stackrel{\text{def}}{=} \top$ . This development is needed since graph formulae do not admit doubly negated literals. We write  $\ell \in Q$  to denote that  $\ell$  is a literal occurring in  $Q$  with the same polarity. So,  $\neg p$  appearing in  $Q$  does not imply  $p \in Q$ . The axioms for dealing with negation are defined as follows.

Axioms for negation of graph formulae

$$\begin{aligned}
(\mathbf{G}_{14}^c) \quad \neg |Q_1, \dots, Q_n\rangle &\Leftrightarrow \lambda_n \vee \tau_n \vee \bigvee_{\ell \in Q_i} \bigvee_{i \in [1, n]} |\top, \dots, \bar{\ell}_i, \dots, \top\rangle_{(n)} \\
(\mathbf{G}_{15}^c) \quad \neg |Q_1, \dots, Q_n\rangle &\Leftrightarrow \rho_n \vee \tau_{n-1} \vee \lambda_n \vee \bigvee_{\ell \in Q_i} \bigvee_{i \in [1, n]} |\top, \dots, \bar{\ell}_i, \dots, \top\rangle_{(n)} \\
(\mathbf{G}_{16}^c) \quad \neg |Q_1, \dots, \overleftarrow{Q_i}, \dots, Q_n\rangle &\Leftrightarrow \rho_n \vee \tau_n \vee \lambda_{n-1} \vee \bigvee_{\ell \in Q_i} \bigvee_{i \in [1, n-1]} |\top, \dots, \bar{\ell}_i, \dots, \top\rangle_{(n-1)} \\
&\vee \bigvee_{k \in [1, n] \setminus \{i\}} |\top, \dots, \overleftarrow{\top}_k, \dots, \top\rangle_{(n)} \vee \bigvee_{\ell \in Q_n} |\top, \dots, \overleftarrow{\ell}_i, \dots, \top\rangle_{(n)}
\end{aligned}$$

These axioms characterise the shape of the accessibility relation when one particular shape is excluded. The general principle of the axioms  $(\mathbf{G}_{14}^c)$ - $(\mathbf{G}_{16}^c)$  is rather simple: the negation of a graph formula holds if the shape is not respected or if a literal at a given position of the shape does not hold. A case analysis for the different shapes is performed (using a disjunction). For example, if  $\mathfrak{M}, \mathfrak{l} \models \neg |\top, \top, \top\rangle$ , then the path can be of any length but the only possible path from  $\mathfrak{l}$  of length 2 is then a lasso. These cases are captured by the axiom  $(\mathbf{G}_{15}^c)$ .

**Lemma 3.** *Every axiom in  $\mathcal{H}_c$  is valid for  $MSL(*, \diamond)$ .*

*Proof.* Let us start with the axioms for size formulae. The validity of the axioms  $(\mathbf{S}_1^c)$ - $(\mathbf{S}_2^c)$  is straightforward from the definition of the semantics for  $\mathbf{size} \geq \beta$ . For the axiom  $(\mathbf{G}_1^c)$ , suppose  $\mathfrak{M}, \mathfrak{l} \models |Q_1, \dots, Q_n\rangle$ . From the definition of the semantics of graph formulae, for  $|Q_1, \dots, Q_n\rangle = |Q_1, \dots, Q_n\rangle$  or  $|Q_1, \dots, Q_n\rangle = |Q_1, \dots, \overleftarrow{Q_i}, \dots, Q_n\rangle$  we conclude that  $\text{card}(\mathfrak{R}) \geq n = \#(|Q_1, \dots, Q_n\rangle)$ . Similarly, when  $|Q_1, \dots, Q_n\rangle$  is actually equal to  $|Q_1, \dots, Q_n\rangle$  we can conclude that  $\text{card}(\mathfrak{R}) \geq n-1 = \#(|Q_1, \dots, Q_n\rangle)$ . Then  $\mathfrak{M}, \mathfrak{l} \models \mathbf{size} \geq \#(|Q_1, \dots, Q_n\rangle)$ .

For proving the validity of the axiom  $(\mathbf{G}_2^c)$ , we know that a conjunction  $Q$  is contradictory (i.e. it contains a contradictory formula) iff it is unsatisfiable, and this can be extended to graph formulae, namely, a graph formula  $\phi$  is contradictory iff it is unsatisfiable. So, obviously, the axiom  $(\mathbf{G}_2^c)$  is valid. We proceed now with the axioms for conjunction. The axiom  $(\mathbf{G}_3^c)$  is valid since the existence of a loop contradicts the fact that there is a dead-end (i.e., a location without successors), and the axiom  $(\mathbf{G}_4^c)$  is valid since by  $n \geq m$ , the existence of a dead-end at position  $m$  contradicts the fact that there exists a path on length  $n$ , and also for the loop case from the axiom  $(\mathbf{G}_5^c)$ . The validity of the axioms  $(\mathbf{G}_6^c)$ - $(\mathbf{G}_9^c)$  is direct from the semantics of graph formulae.

For proving the validity of the axiom  $(\mathbf{G}_{10}^c)$ , we reason *ad absurdum*. Suppose  $\mathfrak{M}, \mathfrak{l} \models |Q_1, \dots, \overleftarrow{Q_i}, \dots, Q_n\rangle \wedge |Q'_1, \dots, \overleftarrow{Q'_j}, \dots, Q'_m\rangle$  with  $i \neq j$  or  $n \neq m$ . By definition of the satisfaction relation  $\models$ , there exist distinct locations  $\mathfrak{l} = \mathfrak{l}_1, \dots, \mathfrak{l}_n$  and distinct locations  $\mathfrak{l} = \mathfrak{l}'_1, \dots, \mathfrak{l}'_m$ , such that  $\mathfrak{l}_1 \mathfrak{R} \mathfrak{l}_2 \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}_i \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}_n$  and  $\mathfrak{l}'_1 \mathfrak{R} \mathfrak{l}'_2 \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}'_m \mathfrak{R} \mathfrak{l}'_j$ .

- If  $n \neq m$ , then w.l.o.g. we can assume  $n < m$ . Then for all  $k \in [1, n]$ , we have  $\mathfrak{l}_k = \mathfrak{l}'_k$  as  $\mathfrak{R}$  is weakly functional. Moreover,  $\mathfrak{l}'_{n+1} = \mathfrak{l}_i$  by (weak) functionality of  $\mathfrak{R}$ , which contradicts the fact that  $\mathfrak{l}'_1, \dots, \mathfrak{l}'_m$  must be all distinct.
- Otherwise,  $n = m$  and  $i \neq j$ . Then  $\mathfrak{l}_n = \mathfrak{l}'_m$ , so  $\mathfrak{l}_n \mathfrak{R} \mathfrak{l}_i$  and  $\mathfrak{l}_n \mathfrak{R} \mathfrak{l}'_j$ , which by (weak) functionality of  $\mathfrak{R}$  implies  $\mathfrak{l}_i = \mathfrak{l}'_j$ , a contradiction.

Therefore,  $\mathfrak{M}, \mathfrak{l} \models \neg(|Q_1, \dots, \overleftarrow{Q_i}, \dots, Q_n\rangle \wedge |Q'_1, \dots, \overleftarrow{Q'_j}, \dots, Q'_m\rangle)$ .

For the axiom  $(\mathbf{G}_{11}^c)$  suppose  $\mathfrak{M}, \mathfrak{l} \models |Q_1, \dots, \overleftarrow{Q_i}, \dots, Q_n\rangle \wedge |Q'_1, \dots, \overleftarrow{Q'_i}, \dots, Q'_n\rangle$ . Then, there exist distinct locations  $\mathfrak{l} = \mathfrak{l}_1, \dots, \mathfrak{l}_n$  such that  $\mathfrak{l}_1 \mathfrak{R} \mathfrak{l}_2 \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}_i \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}_n$ , and for every  $j \in [1, n]$ ,  $\mathfrak{M}, \mathfrak{l}_j \models Q_j \wedge Q'_j$ . Hence,  $\mathfrak{M}, \mathfrak{l} \models |Q_1 \wedge Q'_1, \dots, \overleftarrow{Q_i} \wedge Q'_i, \dots, Q_n \wedge Q'_n\rangle$ . The proof for the other direction is similar.

For the axiom  $(\mathbf{G}_{12}^c)$ , notice that we simply take the conjunction at every position  $n < i \leq m$ , and after  $i$ , we keep the path from the loop formula. The validity of the axiom  $(\mathbf{G}_{13}^c)$  is proved in a similar way but considering also the overlap between the loop part and the other path.

As far as negation is concerned, let us start by proving the validity of the axiom  $(\mathbf{G}_{14}^c)$ , i.e., we need to show that the disjunction on the right is logically equivalent to the negation on the

left. First, notice that  $\mathfrak{M}, \mathfrak{l} \not\models |Q_{1,\dots}, Q_n\rangle$  iff there are no  $l_1, \dots, l_{n+1}$  such that the following three conditions hold:

- i.  $l = l_1, \dots, l_{n+1}$  are all distinct;
- ii.  $l_1 \mathfrak{R} l_2 \dots l_n \mathfrak{R} l_{n+1}$ ; and
- iii. for all  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$ .

On the other hand, notice that:

- iv.  $\mathfrak{M}, \mathfrak{l} \models \lambda_n$  iff there is  $i \in [1, n]$  and  $j \in [1, i]$  such that there are distinct locations  $l_1, \dots, l_i$  with  $l_1 \mathfrak{R} l_2 \dots \mathfrak{R} l_i$  and  $l_j \mathfrak{R} l_j$ . This condition contradicts the condition (i) above.
- v.  $\mathfrak{M}, \mathfrak{l} \models \tau_n$  iff there is some  $j \in [1, n]$  such that  $\mathfrak{R}^j(\mathfrak{l}) = \emptyset$ , which contradicts the condition (ii).
- vi.  $\mathfrak{M}, \mathfrak{l} \models \bigvee_{\substack{i \in [1, n] \\ \ell \in Q_i}} |\top, \dots, \bar{\ell}, \dots, \top\rangle_{(n)}$ , iff there is  $j \in [1, n]$  such that  $\{l_j\} = \mathfrak{R}^j(\mathfrak{l})$  and  $\mathfrak{M}, l_j \not\models Q_j$ , which contradicts the condition (iii).

Therefore, as all the cases are treated, the axiom is valid.

For the axiom ( $\mathbf{G}_{15}^c$ ), first notice that  $\mathfrak{M}, \mathfrak{l} \not\models |Q_{1,\dots}, Q_n]$  iff there are no  $l_1, \dots, l_n$  such that the following conditions hold:

- i.  $l = l_1, \dots, l_n$  are all distinct;
- ii.  $l_1 \mathfrak{R} l_2 \dots l_{n-1} \mathfrak{R} l_n$ ;
- iii. there is no  $l'$  such that  $l_n \mathfrak{R} l'$ ; and
- iv. for all  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$ .

On the other hand, notice that:

- v.  $\mathfrak{M}, \mathfrak{l} \models \lambda_n \vee \tau_{n-1}$  contradicts the conditions (i)-(ii) above.
- vi.  $\mathfrak{M}, \mathfrak{l} \models \rho_n$  obviously contradicts condition (iii).
- vii. Finally, if  $\mathfrak{M}, \mathfrak{l} \models \bigvee_{\substack{i \in [1, n] \\ \ell \in Q_i}} |\top, \dots, \bar{\ell}, \dots, \top\rangle_{(n)}$ , then by applying a similar reasoning as for the previous axiom, it leads to a contradiction by the condition (iv).

Therefore, as all the cases are treated, the axiom is valid.

For the axiom ( $\mathbf{G}_{16}^c$ ), first notice that  $\mathfrak{M}, \mathfrak{l} \not\models |\overline{Q_{1,\dots}, Q_n}]$  iff there are no  $l_1, \dots, l_n$  such that the following conditions hold:

- i.  $l = l_1, \dots, l_n$  are all distinct;
- ii.  $l_1 \mathfrak{R} l_2 \dots l_n \mathfrak{R} l_i$ ; and
- iii. for all  $j \in [1, n]$ , we have  $\mathfrak{M}, l_j \models Q_j$ .

On the other hand, notice that:

- iv.  $\mathfrak{M}, \mathfrak{l} \models \lambda_{n-1}$  contradicts the condition (i) above, since it establishes that there is a loop before the location  $l_n$ .
- v.  $\mathfrak{M}, \mathfrak{l} \models \rho_n \vee \tau_n \vee \bigvee_{k \in [1, n] \setminus \{i\}} |\top, \dots, \overline{\top}_k, \dots, \top\rangle_{(n)}$  contradicts the condition (ii):  $\rho_n$  says that  $i \notin [1, n]$ ;  $\tau_n$  establishes that  $\mathfrak{R}(l_k) = \emptyset$ , for some  $k \leq n$ ; and  $\bigvee_{k \in [1, n] \setminus \{i\}} |\top, \dots, \overline{\top}_k, \dots, \top\rangle_{(n)}$  indicates that  $\mathfrak{R}(l_n) \neq \{l_i\}$ .
- vi. Finally, if  $\mathfrak{M}, \mathfrak{l} \models \bigvee_{\substack{i \in [1, n-1] \\ \ell \in Q_i}} |\top, \dots, \bar{\ell}, \dots, \top\rangle_{(n-1)} \vee \bigvee_{\ell \in Q_n} |\top, \dots, \overline{\top}_i, \dots, \bar{\ell}\rangle_{(n)}$  ( $\otimes$ ), then it contradicts the condition (iii), since for some  $i \in [1, n]$  and  $\ell \in Q_j$ ,  $\mathfrak{M}, l_j \models \ell \wedge \bar{\ell}$  (notice that both disjuncts in ( $\otimes$ ) cover all the possible positions of such contradictory literal).

Therefore, as all the cases are treated, the axiom is valid.  $\square$

To show the completeness of  $\mathcal{H}_c$ , we exploit its ability to eliminate negations and conjunctions of graph formulae. Together with propositional calculus, this is enough to show that every Boolean combination of core formulae is equivalent to a disjunction of formulae of the form either  $\mathcal{G} \wedge \mathbf{size} \geq \beta$  or  $\mathcal{G} \wedge \mathbf{size} \geq \beta \wedge \neg \mathbf{size} \geq \beta'$ , where  $\mathcal{G}$  is a graph formula. Such formulae are called *elementary shapes*.

**Lemma 4.** *Let  $\phi$  be a Boolean combination of core formulae. There is a disjunction of elementary shapes  $\psi$  such that  $\vdash_{\mathcal{H}_c} \phi \Leftrightarrow \psi$ .*

By Lemma 3,  $\vdash_{\mathcal{H}_c}$  is sound and therefore  $\vdash_{\mathcal{H}_c} \phi \Leftrightarrow \psi$  implies that the formulae  $\phi$  and  $\psi$  are logically equivalent.

*Proof.* By propositional reasoning, there exists a formula  $\phi' = \bigvee_i \psi_i$  in disjunctive normal form (DNF) such that  $\vdash_{\mathcal{H}_c} \phi \Leftrightarrow \phi'$ . Each  $\psi_i$  is of the form

$$\psi_i = \bigwedge_{j \in [1, n]} \mathcal{G}_j \wedge \bigwedge_{j \in [1, m]} \neg \mathcal{G}'_j \wedge \bigwedge_{j \in [1, k]} \mathbf{size} \geq \beta_j \wedge \bigwedge_{j \in [1, l]} \neg \mathbf{size} \geq \beta'_j$$

where the  $\mathcal{G}_j$ 's and  $\mathcal{G}'_j$ 's are graph formulae. Some additional work is required in the case  $n = 0$  or  $k = 0$  but the axioms from  $\mathcal{H}_c$  can help a lot.

- By the axiom (**S<sub>1</sub><sup>c</sup>**),  $\vdash_{\mathcal{H}_c} \psi_i \Leftrightarrow (\psi_i \wedge \mathbf{size} \geq 0)$  and therefore, without loss of generality, we can assume that  $k \geq 1$ .
- By the axiom (**G<sub>14</sub><sup>c</sup>**),  $\vdash_{\mathcal{H}_c} \neg |\top| \Leftrightarrow (|\top| \vee |\overline{\top}| \vee |\perp|)$  and therefore by propositional reasoning  $\vdash_{\mathcal{H}_c} |\top| \vee |\overline{\top}| \vee |\perp| \vee |\top|$  and therefore  $\vdash_{\mathcal{H}_c} |\top| \vee |\overline{\top}| \vee |\top|$  by taking advantage of the axiom (**G<sub>2</sub><sup>c</sup>**). Without loss of generality, we can assume that  $n \geq 1$ , as

$$\begin{aligned} \vdash_{\mathcal{H}_c} ((|\top| \vee |\overline{\top}| \vee |\top|) \wedge \bigwedge_{j \in [1, m]} \neg \mathcal{G}'_j \wedge \bigwedge_{j \in [1, k]} \mathbf{size} \geq \beta_j \wedge \bigwedge_{j \in [1, l]} \neg \mathbf{size} \geq \beta'_j) \Leftrightarrow \\ \bigwedge_{j \in [1, m]} \neg \mathcal{G}'_j \wedge \bigwedge_{j \in [1, k]} \mathbf{size} \geq \beta_j \wedge \bigwedge_{j \in [1, l]} \neg \mathbf{size} \geq \beta'_j \end{aligned}$$

Indeed, by distributing the elements of  $(|\top| \vee |\overline{\top}| \vee |\top|)$ , we can obtain conjunctions with at least one positive occurrence of a graph formula.

Let  $\beta_L \stackrel{\text{def}}{=} \max\{\beta_j \mid j \in [1, k]\}$ . If  $l \geq 1$ , then let  $\beta_U \stackrel{\text{def}}{=} \min\{\beta'_j \mid j \in [1, l]\}$ . If  $\psi_i$  has no negative occurrences of  $\mathbf{size} \geq \beta$ , let  $\gamma = \top$ , otherwise let  $\gamma = \neg \mathbf{size} \geq \beta_U$ . By the axiom (**S<sub>2</sub><sup>c</sup>**), we easily obtain the equivalence

$$\vdash_{\mathcal{H}_c} \psi_i \Leftrightarrow \bigwedge_{j \in [1, n]} \mathcal{G}_j \wedge \bigwedge_{j \in [1, m]} \neg \mathcal{G}'_j \wedge \mathbf{size} \geq \beta_L \wedge \gamma.$$

Now, let us manipulate the graph formulae. By the axioms (**G<sub>14</sub><sup>c</sup>**)-(**G<sub>16</sub><sup>c</sup>**), each negative occurrence of a graph formula  $\neg \mathcal{G}'_j$  can be rewritten as a disjunction of positive occurrences of graph formulae  $\bigvee_{k \in [1, b_j]} \mathcal{G}_k^j$ , leading to the equivalence

$$\vdash_{\mathcal{H}_c} \psi_i \Leftrightarrow \bigwedge_{j \in [1, n]} \mathcal{G}_j \wedge \bigwedge_{j \in [1, m]} (\bigvee_{k \in [1, b_j]} \mathcal{G}_k^j) \wedge \mathbf{size} \geq \beta_L \wedge \gamma$$

which by distribution of conjunctions over disjunctions leads to

$$\vdash_{\mathcal{H}_c} \psi_i \Leftrightarrow \bigvee_{j_1 \in [1, b_1], \dots, j_m \in [1, b_m]} \bigwedge_{j \in [1, n]} \mathcal{G}_j \wedge \bigwedge_{j \in [1, m]} \mathcal{G}_{j_1}^j \wedge \mathbf{size} \geq \beta_L \wedge \gamma.$$

Lastly, by the axioms (**G<sub>7</sub><sup>c</sup>**)-(**G<sub>11</sub><sup>c</sup>**), each  $\mathcal{G} \wedge \mathcal{G}'$  is equivalent to  $\perp$  or to a graph formula  $\mathcal{G}^*$ . Then, the conjunction  $\bigwedge_{j \in [1, n]} \mathcal{G}_j \wedge \bigwedge_{j \in [1, m]} \mathcal{G}_{j_1}^j$  of  $\psi_i$  is equivalent to  $\perp$ , or equivalent to a graph formula  $\mathcal{G}$ . In both cases we obtain a disjunct of the form  $\mathcal{G} \wedge \mathbf{size} \geq \beta_L \wedge \gamma$ . We conclude that  $\vdash_{\mathcal{H}_c} \phi \Leftrightarrow \psi$ , for some formula  $\psi$  equal to a disjunction of elementary shapes of the form either  $\mathcal{G} \wedge \mathbf{size} \geq \beta$  or  $\mathcal{G} \wedge \mathbf{size} \geq \beta \wedge \neg \mathbf{size} \geq \beta'$ .  $\square$

We prove that  $\mathcal{H}_c$  is complete for the restricted case of elementary shapes.

**Lemma 5.** *Let  $\phi$  be an elementary shape.  $\phi$  is satisfiable iff  $\not\vdash_{\mathcal{H}_c} \neg\phi$ .*

*Proof.* Let  $\phi$  be an elementary shape  $\mathcal{G} \wedge \mathbf{size} \geq \beta \wedge \gamma$  where either  $\gamma = \top$  or  $\gamma = \neg\mathbf{size} \geq \beta'$ . The proof from left to right follows from the correctness of  $\mathcal{H}_c$  (Lemma 3). In order to prove the direction from right to left, let us suppose that  $\not\vdash_{\mathcal{H}_c} \neg\phi$ . Let us build a model satisfying  $\phi$  by an iterative process starting from the empty model  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R} = \emptyset, \mathfrak{V} = \emptyset \rangle$  and by considering  $\mathfrak{l} \in \mathbb{N}$  as the location where  $\phi$  is evaluated. Any element of  $\mathbb{N}$  that does not occur yet in  $\mathfrak{R}$  is understood as a *fresh location*. Let us analyse the elementary shape  $\phi$ .

1. If  $\mathcal{G} = |Q_1, \dots, Q_n\rangle$ , let  $\mathfrak{l} = \mathfrak{l}_1, \dots, \mathfrak{l}_{n+1}$  be  $n+1$  distinct fresh locations. For every  $i \in [1, n]$ , we update  $\mathfrak{R}$  by adding  $(\mathfrak{l}_i, \mathfrak{l}_{i+1})$  to it. For every propositional variable  $p$  appearing positively in  $Q_i$ , we update  $\mathfrak{V}$  by adding  $\mathfrak{l}_i$  to  $\mathfrak{V}(p)$ . Nothing is done for negative literals of the form  $\neg q$ .
2. If  $\mathcal{G} = |Q_1, \dots, Q_n]$ , let  $\mathfrak{l} = \mathfrak{l}_1, \dots, \mathfrak{l}_n$  be  $n$  distinct fresh locations. We update  $\mathfrak{R}$  by adding  $(\mathfrak{l}_i, \mathfrak{l}_{i+1})$  to it, for every  $i \in [1, n-1]$ . Then, for every  $i \in [1, n]$  and every propositional symbol  $p$  appearing positively in  $Q_i$ , we update  $\mathfrak{V}$  by adding  $\mathfrak{l}_i$  to  $\mathfrak{V}(p)$ .
3. Lastly, if  $\mathcal{G} = |Q_1, \dots, \overline{Q_i, \dots, Q_n}]$ , let  $\mathfrak{l} = \mathfrak{l}_1, \dots, \mathfrak{l}_n$  be  $n$  distinct fresh locations. We update  $\mathfrak{R}$  by adding  $(\mathfrak{l}_n, \mathfrak{l}_i)$  and  $(\mathfrak{l}_j, \mathfrak{l}_{j+1})$ , for every  $j \in [1, n-1]$ , to it. Then, for every  $j \in [1, n]$  and every propositional symbol  $p$  appearing positively in  $Q_j$ , we update  $\mathfrak{V}$  by adding  $\mathfrak{l}_j$  to  $\mathfrak{V}(p)$ .

We conclude the construction by considering the formula  $\mathbf{size} \geq \beta$ .

- If  $\beta \leq \text{card}(\mathfrak{R})$  (i.e.  $\sharp(\mathcal{G}) \geq \beta$ ), the construction of  $\mathfrak{M}$  is complete.
- If  $\beta > \text{card}(\mathfrak{R})$ , let  $\mathfrak{l}'_1, \dots, \mathfrak{l}'_{\beta - \text{card}(\mathfrak{R})}$  be  $(\beta - \text{card}(\mathfrak{R}))$  distinct fresh locations different from  $\mathfrak{l}$ . For every  $i \in [1, \beta - \text{card}(\mathfrak{R})]$ , we update  $\mathfrak{R}$  by adding  $(\mathfrak{l}'_i, \mathfrak{l}'_i)$  to it. In this step, the following property holds:
  - ( $\star$ ) As every newly introduced location is fresh and different from the evaluation point  $\mathfrak{l}$ , it does not reach nor is reached by  $\mathfrak{l}$ .

Now, we show that  $\mathfrak{M}, \mathfrak{l}_1 \models \phi$ . By hypothesis,  $\not\vdash_{\mathcal{H}_c} \neg\phi$ . We start by considering the graph formula  $\mathcal{G}$  of the elementary shape  $\phi$  and we distinguish three cases, as above (all cases are handled similarly). First, note that  $\not\vdash_{\mathcal{H}_c} \neg\phi$  implies  $\not\vdash_{\mathcal{H}_c} \neg\mathcal{G}$  by propositional reasoning and by the axiom (**G<sub>2</sub>**), all the conjunctions  $Q_i$  occurring in  $\mathcal{G}$  are not contradictory (and therefore are satisfiable). Moreover, given a non-contradictory conjunction  $Q$ , a valuation  $v : \text{PROP} \rightarrow \{\perp, \top\}$  satisfying  $Q$  can be defined so that  $v(p) \stackrel{\text{def}}{=} \top$  iff  $p$  occurs in  $Q$ . This is precisely the principle used to define  $\mathfrak{V}$  in  $\mathfrak{M}$ .

- If  $\mathcal{G} = |Q_1, \dots, Q_n\rangle$ , then by definition  $\mathfrak{M}, \mathfrak{l} \models \mathcal{G}$  iff there are distinct  $\mathfrak{l}_1, \dots, \mathfrak{l}_{n+1}$  such that  $\mathfrak{l} = \mathfrak{l}_1 \mathfrak{R} \mathfrak{l}_2 \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}_{n+1}$  and for all  $j \in [1, n]$ , we have  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$ . By the point (1) of the construction, the constraints on  $\mathfrak{R}$  are trivially satisfied. Note that for every  $j \in [1, n]$ ,  $\mathfrak{V}$  restricted to the propositional variables occurring in  $Q_j$  and to  $\mathfrak{l}_j$  satisfies the conditions of the valuations  $v$  above. Hence,  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$ .
- If  $\mathcal{G} = |Q_1, \dots, Q_n]$ , then by definition  $\mathfrak{M}, \mathfrak{l} \models \mathcal{G}$  iff there are distinct  $\mathfrak{l}_1, \dots, \mathfrak{l}_n$  such that  $\mathfrak{l} = \mathfrak{l}_1 \mathfrak{R} \mathfrak{l}_2 \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}_n$ , there is no  $\mathfrak{l}'$  such that  $\mathfrak{l}_n \mathfrak{R} \mathfrak{l}'$  and for each  $j \in [1, n]$ , we have  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$ . By the point (2) of the construction, together with ( $\star$ ), the constraints on  $\mathfrak{R}$  are trivially satisfied. As in the previous case, one can show that for every  $j \in [1, n]$ ,  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$ .
- Lastly, if  $\mathcal{G} = |Q_1, \dots, \overline{Q_i, \dots, Q_n}]$  then by definition  $\mathfrak{M}, \mathfrak{l} \models \mathcal{G}$  iff there are distinct  $\mathfrak{l}_1, \dots, \mathfrak{l}_n$  such that  $\mathfrak{l} = \mathfrak{l}_1 \mathfrak{R} \mathfrak{l}_2 \mathfrak{R} \dots \mathfrak{R} \mathfrak{l}_n \mathfrak{R} \mathfrak{l}_i$  and for all  $j \in [1, n]$ ,  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$ . Again, by the point (3) of the construction, together with ( $\star$ ), the constraints on  $\mathfrak{R}$  are trivially satisfied whereas the proof that for every  $j \in [1, n]$  it holds that  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$  is performed as above.

For  $\mathbf{size} \geq \beta$  formulae, from the last step of the construction, it trivially holds that  $\mathfrak{M}, \mathfrak{l} \models \mathbf{size} \geq \beta$ . If  $\gamma = \top$ , the proof is completed. Otherwise  $\gamma = \neg\mathbf{size} \geq \beta'$  and it remains to show that  $\mathfrak{M}, \mathfrak{l} \models \neg\mathbf{size} \geq \beta'$ . Let us recall the semantics:  $\mathfrak{M}, \mathfrak{l} \models \neg\mathbf{size} \geq \beta'$  if and only if  $\text{card}(\mathfrak{R}) < \beta'$ .



Let us distinguish different cases. If  $\beta' \leq \beta$ , then by propositional reasoning and by using the axiom  $(\mathbf{S}_2^\diamond)$   $(\beta - \beta')$  times, we can conclude that  $\vdash_{\mathcal{H}_c} \text{size} \geq \beta \Rightarrow \text{size} \geq \beta'$  and therefore  $\vdash_{\mathcal{H}_c} \neg(\text{size} \geq \beta \wedge \neg \text{size} \geq \beta')$ . Consequently,  $\vdash_{\mathcal{H}_c} \neg\phi$  by propositional reasoning, which leads to a contradiction. Otherwise  $\beta' > \beta$  and again we distinguish two cases. If  $\text{card}(\mathfrak{A}) = \beta$ , then obviously,  $\mathfrak{M}, l \models \neg \text{size} \geq \beta'$ . Otherwise (i.e.  $\text{card}(\mathfrak{A}) > \beta$  and  $\beta' > \beta$ ), we are in the case  $\sharp(\mathcal{G}) = \text{card}(\mathfrak{A})$ . *Ad absurdum*, let us suppose that  $\text{card}(\mathfrak{A}) \geq \beta'$ , i.e.  $\sharp(\mathcal{G}) \geq \beta'$ . By the axiom  $(\mathbf{G}_1^\diamond)$ , we obtain  $\vdash_{\mathcal{H}_c} \mathcal{G} \Rightarrow \text{size} \geq \sharp(\mathcal{G})$ . By propositional reasoning and by using the axiom  $(\mathbf{S}_2^\diamond)$   $(\sharp(\mathcal{G}) - \beta')$  times, we can conclude that  $\vdash_{\mathcal{H}_c} \text{size} \geq \sharp(\mathcal{G}) \Rightarrow \text{size} \geq \beta'$  and therefore  $\vdash_{\mathcal{H}_c} \mathcal{G} \Rightarrow \text{size} \geq \beta'$ . Again by propositional reasoning, we get  $\vdash_{\mathcal{H}_c} \neg(\mathcal{G} \wedge \neg \text{size} \geq \beta')$ . Consequently,  $\vdash_{\mathcal{H}_c} \neg\phi$  by propositional reasoning, which leads to a contradiction.  $\square$

From this result, we can establish the completeness of  $\mathcal{H}_c$  with respect to Boolean combinations of core formulae. This is an essential step to get a complete proof system for  $\text{MSL}(*, \diamond)$  (its definition is to be completed in the rest of Sec. 3).

**Theorem 6.** *A Boolean combination of core formulae  $\phi$  is valid iff  $\vdash_{\mathcal{H}_c} \phi$ .*

*Proof.* Let  $\phi$  be a Boolean combination of core formulae. By Lemma 3,  $\vdash_{\mathcal{H}_c} \phi$  implies that  $\phi$  is valid. Conversely, let us assume that  $\phi$  is valid and *ad absurdum*, let us suppose that  $\not\vdash_{\mathcal{H}_c} \phi$ . By propositional calculus, there exists a formula  $\phi'$  in conjunctive normal form (CNF) such that the “literals” are core formulae or their negations, and  $\vdash_{\mathcal{H}_c} \phi \Leftrightarrow \phi'$ . As  $\not\vdash_{\mathcal{H}_c} \phi$ , there is a conjunct of  $\phi'$ , say  $\psi$ , such that  $\not\vdash_{\mathcal{H}_c} \psi$ . As  $\phi'$  is valid, this implies that  $\psi$  is valid too. By Lemma 4,  $\vdash_{\mathcal{H}_c} \neg\psi \Leftrightarrow (\gamma_1 \vee \dots \vee \gamma_n)$  where  $\gamma_1 \vee \dots \vee \gamma_n$  is a disjunction of elementary shapes and therefore  $(\gamma_1 \vee \dots \vee \gamma_n)$  is unsatisfiable. Consequently, for all  $i \in [1, n]$ , the formula  $\gamma_i$  is unsatisfiable and by Lemma 5, we get that  $\vdash_{\mathcal{H}_c} \neg\gamma_i$ . By propositional reasoning, we get  $\vdash_{\mathcal{H}_c} \neg\gamma_1 \wedge \dots \wedge \neg\gamma_n$  and again by propositional reasoning using  $\vdash_{\mathcal{H}_c} \neg\psi \Leftrightarrow (\gamma_1 \vee \dots \vee \gamma_n)$ , we obtain  $\vdash_{\mathcal{H}_c} \psi$ , which leads to a contradiction.  $\square$

### 3.3.1 $\diamond$ -elimination.

We enrich the proof system  $\mathcal{H}_c$  by adding axioms and one inference rule that handle the modality  $\diamond$ . This leads to the extended proof system  $\mathcal{H}_c(\diamond)$  dedicated to the set of formulae obtained by closing core formulae under Boolean connectives and  $\diamond$ .

Axioms and inference rule for $\mathcal{H}_c(\diamond)$	
$(\diamond\text{DISTR})$ $\diamond(\phi \vee \psi) \Leftrightarrow \diamond(\phi) \vee \diamond(\psi)$	$(\mathbf{G}_{17}^\diamond)$ $\diamond( Q_1, \dots, Q_n ) \Leftrightarrow  \top, Q_1, \dots, Q_n $
$(\mathbf{S}_3^\diamond)$ $\diamond(\phi \wedge \mathcal{S}) \Leftrightarrow \diamond(\phi) \wedge \mathcal{S}$ where $\mathcal{S}$ is a size formula,	
$(\mathbf{G}_{18}^\diamond)$ $\diamond( Q_1, \dots, Q_n ) \Leftrightarrow  \overline{\top, Q_1, \dots, Q_n}  \vee  \top, Q_1, \dots, Q_n $	
$(\mathbf{G}_{19}^\diamond)$ $\diamond( Q_1, \dots, \overline{Q_i}, \dots, Q_n ) \Leftrightarrow  \top, Q_1, \dots, \overline{Q_i}, \dots, Q_n $ with $i \geq 2$ ,	
$(\mathbf{G}_{20}^\diamond)$ $\diamond( \overline{Q_1}, \dots, Q_{n-1}, Q_n ) \Leftrightarrow  \overline{Q_n}, Q_1, \dots, Q_{n-1}  \vee  \top, \overline{Q_1}, \dots, Q_{n-1}, Q_n $	
Regularity rule: $\frac{\phi \Rightarrow \psi}{\diamond\phi \Rightarrow \diamond\psi}$	

**Lemma 7.** *The axioms and rules in  $\mathcal{H}_c(\diamond)$  are valid for  $\text{MSL}(*, \diamond)$ .*

*Proof.* Let  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  be a model and  $l \in \mathbb{N}$ . The axiom  $(\diamond\text{DISTR})$  is valid since  $\mathfrak{M}, l \models \diamond(\phi \vee \psi) \Leftrightarrow \diamond\phi \vee \diamond\psi$  for any Kripke-style structure ( $\diamond(\phi \vee \psi) \Leftrightarrow \diamond\phi \vee \diamond\psi$  is valid for the modal logic K). As far as the axiom  $(\mathbf{G}_{17}^\diamond)$  is concerned,  $\mathfrak{M}, l \models \diamond(|Q_1, \dots, Q_n|)$ , iff there exists  $l'$  such that  $\mathfrak{M}, l' \models |Q_1, \dots, Q_n|$ . This is the case if and only if, there are distinct  $l_1, \dots, l_n$  such that  $l' = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots \mathfrak{R} l_n$ , there is no  $l'$  such that  $l_n \mathfrak{R} l'$  and for each  $i \in [1, n]$ , we have  $\mathfrak{M}, l_i \models Q_i$ . Moreover, for all  $i \in [1, n]$ , we have  $l_i \neq l$ .

But we know that  $\mathfrak{M}, l' \models \top$  and also trivially  $\mathfrak{M}, l \models \top$ , so by definition of the satisfaction relation  $\models$  on graph formulae again,  $\mathfrak{M}, l \models |\top, Q_1, \dots, Q_n|$  (notice that each step is in both directions).

Let us deal with the axiom  $(\mathbf{S}_3^\diamond)$ . Suppose  $\mathfrak{M}, l \models \diamond(\phi \wedge \mathcal{S})$ . There is  $l'$  such that  $\mathfrak{R}l'$  and  $\mathfrak{M}, l' \models \phi \wedge \mathcal{S}$ . As  $\mathcal{S}$  is a size formula, the evaluation of  $\mathcal{S}$  on  $\mathfrak{M}, l'$  does not require the use of  $l'$  (and  $\mathfrak{R}$ ) and therefore  $\mathfrak{M}, l \models \mathcal{S}$  too. Consequently,  $\mathfrak{M}, l \models (\diamond\phi) \wedge \mathcal{S}$ . Conversely, suppose that  $\mathfrak{M}, l \models (\diamond\phi) \wedge \mathcal{S}$ . There is  $l'$  such that  $\mathfrak{R}l'$  and  $\mathfrak{M}, l' \models \phi$ . As  $\mathcal{S}$  is a size formula, the evaluation of  $\mathcal{S}$  on  $\mathfrak{M}, l$  does not require the use of  $l$  and therefore  $\mathfrak{M}, l' \models \mathcal{S}$  too. Consequently,  $\mathfrak{M}, l \models \diamond(\phi \wedge \mathcal{S})$ .

For the axiom  $(\mathbf{G}_{18}^\diamond)$ ,  $\mathfrak{M}, l \models \diamond(|Q_1, \dots, Q_n\rangle)$ , iff there exists  $l'$  such that  $\mathfrak{R}l'$  and  $\mathfrak{M}, l' \models |Q_1, \dots, Q_n\rangle$ . This is the case iff there are distinct  $l_1, \dots, l_{n+1}$  such that  $l' = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots \mathfrak{R} l_{n+1}$  and for all  $i \in [1, n]$ , we have  $\mathfrak{M}, l_i \models Q_i$ . Notice that since  $\mathfrak{R}$  is (weakly) functional, and the fact that  $l' = l_1 \neq l_2$  and  $l_1 \mathfrak{R} l_2$ , necessarily  $l \neq l'$ . Then we have two cases to consider. If  $l \neq l_{n+1}$ , then we have  $\mathfrak{M}, l \models |\top, Q_1, \dots, Q_n\rangle$ . Otherwise, since  $l = l_{n+1}$ , then we have that  $l_n \mathfrak{R} l$ , so  $\mathfrak{M}, l \models |\overline{\top}, Q_1, \dots, Q_n\rangle$ . The other direction can be proved in the same way.

Let us prove the validity of the axiom  $(\mathbf{G}_{19}^\diamond)$ , so for the left to the right direction suppose  $\mathfrak{M}, l \models \diamond(|Q_1, \dots, \overline{Q_i}, \dots, Q_n\rangle)$ , for some  $i \geq 2$ . Then there exists  $l'$  such that  $\mathfrak{R}l'$  and  $\mathfrak{M}, l' \models |Q_1, \dots, \overline{Q_i}, \dots, Q_n\rangle$ . By the semantics for graph formulae, there are distinct  $l_1, \dots, l_n$  such that  $l' = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots \mathfrak{R} l_n \mathfrak{R} l_i$  and for all  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$ . But  $l \neq l'$ , otherwise  $l' = l_1 = l_2$ , which we know is false by hypothesis and the fact that  $i \geq 2$ . So, there are distinct  $l, l_1, \dots, l_n$  such that  $\mathfrak{R}l_1 \mathfrak{R} l_2 \mathfrak{R} \dots \mathfrak{R} l_n \mathfrak{R} l_i$ , and for all  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$ . Therefore,  $\mathfrak{M}, l \models |\top, Q_1, \dots, \overline{Q_i}, \dots, Q_n\rangle$ . The proof in the other direction is done similarly (and even simpler).

Now, let us prove the validity of the axiom  $(\mathbf{G}_{20}^\diamond)$ . For the left to the right direction suppose  $\mathfrak{M}, l \models \diamond(|\overline{Q_1}, \dots, Q_{n-1}, Q_n\rangle)$ , and so there exists  $l'$  such that  $\mathfrak{R}l'$  and  $\mathfrak{M}, l' \models |\overline{Q_1}, \dots, Q_{n-1}, Q_n\rangle$ . By the semantics for graph formulas, there are distinct  $l_1, \dots, l_n$  such that  $l' = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots \mathfrak{R} l_n \mathfrak{R} l_i$  and for all  $j \in [1, n]$ ,  $\mathfrak{M}, l_j \models Q_j$ . Again, notice  $l \neq l'$ , so we have to consider two cases. If  $l = l_n$ , then there exist  $l_n, l_1, \dots, l_{n-1}$  all distinct, and  $l_n \mathfrak{R} l_1 \dots \mathfrak{R} l_{n-1}$ , then  $\mathfrak{M}, l \models |\overline{Q_n}, Q_1, \dots, Q_{n-1}\rangle$ . Otherwise, we have  $l, l_1, \dots, l_n$  all distinct and  $\mathfrak{R}l_1 \dots \mathfrak{R} l_n \mathfrak{R} l_1$ , then  $\mathfrak{M}, l \models |\top, \overline{Q_1}, \dots, Q_{n-1}, Q_n\rangle$ . The other direction uses similar steps.

Finally, we will show that the **Regularity rule** is valid. Suppose that  $\phi \Rightarrow \psi$  is valid and  $\mathfrak{M}, l \models \diamond\phi$ . Then, there exists  $l'$  such that  $\mathfrak{R}l'$  and  $\mathfrak{M}, l' \models \phi$ . As  $\phi \Rightarrow \psi$  is valid, we also get  $\mathfrak{M}, l' \models \psi$  and therefore  $\mathfrak{M}, l \models \diamond\psi$ .  $\square$

These axioms give us some insight about the interplay between separating and modal connectives. In the case of size formulae there is no interplay at all (see the axiom  $(\mathbf{S}_3^\diamond)$ ). Indeed, every condition in a formula  $\psi$  about the size of the accessibility relation  $\mathfrak{R}$  carries on independently of the structure of  $\mathfrak{R}$  described by  $\psi$  through modalities. However, there are interplays with respect to loops (see e.g. the axiom  $(\mathbf{G}_{18}^\diamond)$  and recall that  $\text{ext}(|Q_1, \dots, \overline{Q_i}, \dots, Q_n\rangle)$  uses the separating conjunction  $*$ ). Note also that no axiom of the form  $\diamond\phi \Rightarrow \Box\phi$  is explicitly present to encode weak functionality but it is derivable by completeness. Indeed, functionality is taken care with the axioms dedicated to the Boolean combinations of core formulae as well as with those dedicated to the interaction between core formulae and  $\diamond$ . A similar situation happens with the distribution axiom  $\Box(\phi \Rightarrow \psi) \Rightarrow (\Box\phi \Rightarrow \Box\psi)$  that is not present in our axiomatisation. In a way, thanks to the core formulae (and more specifically to the graph formulae), the axiomatisation “manipulates modal frames” and this is done exhaustively thanks to the completeness for Boolean combinations of core formulae.

**Lemma 8.** *Let  $\phi$  be a Boolean combination of core formulae. There is a Boolean combination of core formulae  $\psi$  such that  $\vdash_{\mathcal{H}_c(\diamond)} \diamond\phi \Leftrightarrow \psi$ .*

Observe that the formula  $\psi$  in Lemma 8 is a combination of core formulae and therefore  $\diamond$  does not occur in it. By Lemma 7 (soundness of  $\vdash_{\mathcal{H}_c(\diamond)}$ ), the formulae  $\diamond\phi$  and  $\psi$  in Lemma 8 are logically equivalent

*Proof.* Before providing the proof, let us state a property used in several places.

( $\dagger\dagger$ ) Let  $\phi, \phi'$  and  $\psi$  be formulae built from core formulae, the Boolean connectives and the modality  $\diamond$  such that  $\vdash_{\mathcal{H}_c(\diamond)} \phi \Leftrightarrow \phi'$ . Then  $\vdash_{\mathcal{H}_c(\diamond)} \psi[\phi]_\rho \Leftrightarrow \psi[\phi']_\rho$  where  $\psi[\phi]_\rho$  stands for the formula obtained from  $\psi$  by replacing the formula at the occurrence  $\rho$  by the formula  $\phi$ .

The proof of ( $\dagger\dagger$ ) is performed along the lines of the proof of Lemma 21 and is therefore omitted herein (the regularity rule needs to be used).

Suppose  $\phi$  is a Boolean combination of core formulae. By Lemma 4, there is a disjunction of elementary shapes  $\bigvee_i \psi_i$  such that  $\vdash_{\mathcal{H}_c(\diamond)} \phi \Leftrightarrow \bigvee_i \psi_i$ , as  $\mathcal{H}_c(\diamond)$  is an extension of  $\mathcal{H}_c$ . By ( $\dagger\dagger$ ), and by using the axiom ( **$\diamond$ DISTR**), we can conclude that  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(\phi) \Leftrightarrow \bigvee_i \diamond(\psi_i)$ . In order to prove the result, it is then sufficient to show that for every elementary shape  $\psi$ , there is a Boolean combination of core formulae  $\psi'$  such that  $\vdash_{\mathcal{H}_c(\diamond)} \diamond\psi \Leftrightarrow \psi'$ . Let  $\gamma_S$  be a size formula of the form either  $\text{size} \geq \beta \wedge \neg \text{size} \geq \beta'$  or  $\text{size} \geq \beta$ . Indeed, in  $\mathcal{H}_c(\diamond)$  we can derive the following formulae:

- $\diamond(|Q_1, \dots, Q_n| \wedge \gamma_S) \Leftrightarrow |\top, Q_1, \dots, Q_n| \wedge \gamma_S$ :
  - i.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, Q_n| \wedge \gamma_S) \Leftrightarrow \diamond(|Q_1, \dots, Q_n|) \wedge \gamma_S$  by the axiom ( **$S_3^\diamond$** );
  - ii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, Q_n|) \wedge \gamma_S \Leftrightarrow |\top, Q_1, \dots, Q_n| \wedge \gamma_S$  by the axiom ( **$G_{17}^\diamond$** );
  - iii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, Q_n| \wedge \gamma_S) \Leftrightarrow |\top, Q_1, \dots, Q_n| \wedge \gamma_S$  by (i) and (ii).
- $\diamond(|Q_1, \dots, Q_n| \wedge \gamma_S) \Leftrightarrow (|\overline{\top, Q_1, \dots, Q_n}| \vee |\top, Q_1, \dots, Q_n|) \wedge \gamma_S$ 
  - i.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, Q_n| \wedge \gamma_S) \Leftrightarrow \diamond(|Q_1, \dots, Q_n|) \wedge \gamma_S$  by the axiom ( **$S_3^\diamond$** );
  - ii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, Q_n|) \wedge \gamma_S \Leftrightarrow (|\overline{\top, Q_1, \dots, Q_n}| \vee |\top, Q_1, \dots, Q_n|) \wedge \gamma_S$  by the axiom ( **$G_{18}^\diamond$** );
  - iii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, Q_n| \wedge \gamma_S) \Leftrightarrow (|\overline{\top, Q_1, \dots, Q_n}| \vee |\top, Q_1, \dots, Q_n|) \wedge \gamma_S$  by (i), (ii).
- for each  $i \geq 2$ ,  $\diamond(|Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \gamma_S) \Leftrightarrow |\top, Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \gamma_S$ 
  - i.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \gamma_S) \Leftrightarrow \diamond(|Q_1, \dots, \overline{Q_i, \dots, Q_n}|) \wedge \gamma_S$  by the axiom ( **$S_3^\diamond$** );
  - ii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, \overline{Q_i, \dots, Q_n}|) \wedge \gamma_S \Leftrightarrow |\top, Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \gamma_S$  by the axiom ( **$G_{19}^\diamond$** );
  - iii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \gamma_S) \Leftrightarrow |\top, Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \gamma_S$  by (i), (ii).
- $\diamond(|\overline{Q_1, \dots, Q_{n-1}, Q_n}| \wedge \gamma_S) \Leftrightarrow (|\overline{Q_n, Q_1, \dots, Q_{n-1}}| \vee |\top, \overline{Q_1, \dots, Q_{n-1}, Q_n}|) \wedge \gamma_S$ 
  - i.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|\overline{Q_1, \dots, Q_{n-1}, Q_n}| \wedge \gamma_S) \Leftrightarrow \diamond(|\overline{Q_1, \dots, Q_{n-1}, Q_n}|) \wedge \gamma_S$  by the axiom ( **$S_3^\diamond$** );
  - ii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|\overline{Q_1, \dots, Q_{n-1}, Q_n}|) \wedge \gamma_S \Leftrightarrow (|\overline{Q_n, Q_1, \dots, Q_{n-1}}| \vee |\top, \overline{Q_1, \dots, Q_{n-1}, Q_n}|) \wedge \gamma_S$  by ( **$G_{20}^\diamond$** );
  - iii.  $\vdash_{\mathcal{H}_c(\diamond)} \diamond(|\overline{Q_1, \dots, Q_{n-1}, Q_n}| \wedge \gamma_S) \Leftrightarrow (|\overline{Q_n, Q_1, \dots, Q_{n-1}}| \vee |\top, \overline{Q_1, \dots, Q_{n-1}, Q_n}|) \wedge \gamma_S$  by (i), (ii).

This concludes the proof.  $\square$

### 3.3.2 \*-elimination.

Finally, we enrich the proof system  $\mathcal{H}_c$  by adding axioms and one inference rule for the separating conjunction. We denote the resulting proof system by  $\mathcal{H}_c(*)$ .

Axioms and inference rule for $\mathcal{H}_c(*)$	
<b>(COM)</b> $(\phi * \psi) \Leftrightarrow (\psi * \phi)$	<b>(*DISTR)</b> $(\phi_1 \vee \phi_2) * \psi \Leftrightarrow (\phi_1 * \psi) \vee (\phi_2 * \psi)$
<b>(ASSOC)</b> $(\phi * \psi) * \gamma \Leftrightarrow \phi * (\psi * \gamma)$	<b>(<math>G_{22}^*</math>)</b> $\neg(\mathcal{G}_1 * \mathcal{G}_2)$ with $\sharp(\mathcal{G}_1) \times \sharp(\mathcal{G}_2) \geq 1$
<b>(<math>\perp</math>)</b> $\neg(\perp * \phi)$	<b>(<math>G_{23}^*</math>)</b> $ Q_1, \dots, Q_n  * \phi \Rightarrow  Q_1, \dots, Q_n $
<b>(<math>S_4^*</math>)</b> $\phi \Leftrightarrow (\phi * \text{size} \geq 1)$	<b>(<math>G_{24}^*</math>)</b> $ Q_1, \dots, \overline{Q_i, \dots, Q_n}  * \phi \Rightarrow  Q_1, \dots, \overline{Q_i, \dots, Q_n} $
<b>(<math>S_5^*</math>)</b> $\text{size} \geq \beta_1 + \beta_2 \Rightarrow \text{size} = \beta_1 * \text{size} \geq \beta_2$	
<b>(<math>S_6^*</math>)</b> $\neg \text{size} \geq \beta_1 * \neg \text{size} \geq \beta_2 \Rightarrow \neg \text{size} \geq (\beta_1 + \beta_2) - 1$	$(\alpha_1 \dot{-} \alpha_2 \stackrel{\text{def}}{=} \max(0, \alpha_1 - \alpha_2))$
<b>(<math>G_{25}^*</math>)</b> $ Q_1, \dots, Q_n  * \text{size} \geq 1 \Rightarrow  Q_1, \dots, Q_n  \vee  Q_1, \dots, Q_n  \vee \bigvee_{i \in [1, n]}  Q_1, \dots, \overline{Q_i, \dots, Q_n} $	
<b>(<math>G_{26}^*</math>)</b> $( Q_1 \wedge Q_2, \dots, Q_n  * \phi) * \psi \Leftrightarrow ( Q_1, \dots, Q_n  * \phi) * ( Q  \wedge \psi)$	
<b>(<math>G_{27}^*</math>)</b> $ Q_1, \dots, Q_n  * \text{size} \geq \beta \Rightarrow ( Q_1, \dots, Q_n  * \text{size} = \beta) * \top$ with $\beta \geq \sharp( Q_1, \dots, Q_n )$	
<b>(<math>G_{28}^*</math>)</b> $ Q_1, \dots, Q_n  \wedge \text{size} \geq \beta + n \Rightarrow ( Q_1, \dots, Q_n  \wedge \text{size} \geq (\beta + n) - 1) * \text{size} = 1$	

( $\mathbf{G}_{29}^*$ )  $|Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \text{size} \geq \beta + n \Rightarrow (|Q_1, \dots, Q_n| \wedge \text{size} \geq (\beta + n) - 1) * \text{size} = 1$

\*-introduction rule:  $\frac{\phi \Rightarrow \gamma}{\phi * \psi \Rightarrow \gamma * \psi}$

The first property to check is the soundness of  $\mathcal{H}_c(*)$ .

**Lemma 9.** *The axioms and rules in  $\mathcal{H}_c(*)$  are valid for  $MSL(*, \diamond)$ .*

*Proof.* First, notice that the axioms (**COM**), (**ASSOC**), (**\*DISTR**), ( **$\perp$** ), ( **$\mathbf{S}_4^*$** ) and the **\*-introduction rule** are the classical axioms and inference rule for  $*$  in separation logic (see e.g. [48]), therefore their validity is straightforward.

Let  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  be an MSL model, and let  $l \in \mathbb{N}$ .

For the validity of the axiom ( **$\mathbf{G}_{22}^*$** ), suppose  $\mathcal{G}_1$  and  $\mathcal{G}_2$  are graph formulae such that  $\sharp(\mathcal{G}_1) \times \sharp(\mathcal{G}_2) \geq 1$ . Observe that  $\mathfrak{M}, l \models \mathcal{G}_1 * \mathcal{G}_2$  iff there are  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$  such that  $\mathfrak{R} = \mathfrak{R}_1 \uplus \mathfrak{R}_2$ ,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models \mathcal{G}_1$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \mathcal{G}_2$ . As  $\sharp(\mathcal{G}_1) \geq 1$  and  $\sharp(\mathcal{G}_2) \geq 1$ , there are  $l_1, l_2$  such that  $(l, l_1) \in \mathfrak{R}_1$  and  $(l, l_2) \in \mathfrak{R}_2$ . As  $\mathfrak{R} = \mathfrak{R}_1 \uplus \mathfrak{R}_2$ ,  $l_1 \neq l_2$ , which is in contradiction with the fact that  $\mathfrak{R}$  is weakly functional. Consequently,  $\mathfrak{M}, l \models \neg(\mathcal{G}_1 * \mathcal{G}_2)$ .

For the validity of the axiom ( **$\mathbf{G}_{23}^*$** ), suppose  $\mathfrak{M}, l \models |Q_1, \dots, Q_n| * \phi$ , iff  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models |Q_1, \dots, Q_n|$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \phi$ , for some partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$ . Then, there exist distinct locations  $l = l_1, \dots, l_{n+1}$  such that  $l_1 \mathfrak{R}_1 l_2 \mathfrak{R}_1 \dots l_n \mathfrak{R}_1 l_{n+1}$ , and for all  $i \in [1, n]$ ,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l_i \models Q_i$ . Since  $\mathfrak{R}_1 \subseteq \mathfrak{R}$ , there exist distinct locations  $l = l_1, \dots, l_{n+1}$  such that  $l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_n \mathfrak{R} l_{n+1}$ , and since each  $Q_i$  is purely propositional,  $\mathfrak{M}, l_i \models Q_i$ , therefore  $\mathfrak{M}, l \models |Q_1, \dots, Q_n|$ .

For the validity of the axiom ( **$\mathbf{G}_{24}^*$** ), suppose  $\mathfrak{M}, l \models |Q_1, \dots, \overline{Q_i, \dots, Q_n}| * \phi$ , iff (by definition of  $\models$ ),  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models |Q_1, \dots, \overline{Q_i, \dots, Q_n}|$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \phi$ , for some partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$ . So, there exist distinct locations  $l = l_1, \dots, l_n$  and  $i \in [1, n]$  such that  $l_1 \mathfrak{R}_1 l_2 \mathfrak{R}_1 \dots l_n \mathfrak{R}_1 l_i$ , and for all  $j \in [1, n]$ ,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l_j \models Q_j$ . Since  $\mathfrak{R}_1 \subseteq \mathfrak{R}$ , there exist distinct locations  $l = l_1, \dots, l_n$  and  $i \in [1, n]$  such that  $l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_n \mathfrak{R} l_i$ , and since each  $Q_j$  is purely propositional,  $\mathfrak{M}, l_j \models Q_j$ , therefore  $\mathfrak{M}, l \models |Q_1, \dots, \overline{Q_i, \dots, Q_n}|$ .

Let us prove now the validity of the axiom ( **$\mathbf{G}_{25}^*$** ). Suppose  $\mathfrak{M}, l \models |Q_1, \dots, Q_n| * \text{size} \geq 1$ , iff  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models |Q_1, \dots, Q_n|$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \text{size} \geq 1$ , for some partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$ . Since  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models |Q_1, \dots, Q_n|$ , there are distinct  $l_1, \dots, l_n$  such that  $l = l_1 \mathfrak{R}_1 l_2 \mathfrak{R}_1 \dots l_n$ , there is no  $l'$  such that  $l_n \mathfrak{R}_1 l'$  and for each  $i \in [1, n]$ ,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l_i \models Q_i$ . On the other hand, we have  $\text{card}(\mathfrak{R}_2) \geq 1$ . We have three cases to consider:

- if  $\mathfrak{R}_2(l_n) = \emptyset$ , since  $\mathfrak{R}_1(l_n) = \emptyset$  then  $\mathfrak{R}(l_n) = \emptyset$ . As a consequence,  $\mathfrak{M}, l \models |Q_1, \dots, Q_n|$ .
- if  $l_n \mathfrak{R}_2 l'$ , for some  $l'$ , and  $l' \neq l_i$  for all  $i \in [1, n]$ , then  $l = l_1 \mathfrak{R} l_2 \mathfrak{R} \dots l_n$  by  $\mathfrak{R}_1$ , and  $l_n \mathfrak{R} l'$  by  $\mathfrak{R}_2$ . Therefore,  $\mathfrak{M}, l \models |Q_1, \dots, Q_n|$ .
- Otherwise,  $l_n \mathfrak{R}_2 l'$ , for some  $l'$  such that  $l' = l_i$  for some  $i \in [1, n]$ . Then we get  $\mathfrak{M}, l \models \bigvee_{i \in [1, n]} |Q_1, \dots, \overline{Q_i, \dots, Q_n}|$ .

For the validity of the axiom ( **$\mathbf{G}_{26}^*$** ), suppose  $\mathfrak{M}, l \models (|Q_1 \wedge Q, \dots, Q_n? \wedge \phi) * \psi$ , iff  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models |Q_1 \wedge Q, \dots, Q_n? \wedge \phi$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models \psi$ , for some partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$ . There exists a sequence of distinct locations  $l = l_1, \dots, l_m$ , with  $l_1 \mathfrak{R}_1 \dots \mathfrak{R} l_m$  (with  $m = n + 1$  if  $|Q_1, \dots, Q_n?$  is equal  $|Q_1, \dots, Q_n|$ ) or  $|Q_1, \dots, Q_n?$  is equal to  $|Q_1, \dots, \overline{Q_i, \dots, Q_n}|$ , otherwise  $m = n$ ), while in the latter case, we have  $\mathfrak{R}_2(l) = \emptyset$ . Moreover, since  $Q$  and  $Q_1$  are purely propositional and  $\mathfrak{M}, l \models Q_1 \wedge Q$ , we have  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models Q_1$ , and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models Q$ . Then,  $\mathfrak{M}, l \models (|Q_1, \dots, Q_n? \wedge \phi) * (|Q| \wedge \psi)$ . For the other direction suppose  $\mathfrak{M}, l \models (|Q_1, \dots, Q_n? \wedge \phi) * (|Q| \wedge \psi)$ , iff  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, l \models |Q_1, \dots, Q_n? \wedge \phi$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, l \models |Q| \wedge \psi$ , for some partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$ . Since  $Q$  is purely propositional, and moreover  $\mathfrak{R}_2(l) = \emptyset$ , it is obvious that  $\mathfrak{M}, l \models (|Q_1 \wedge Q, \dots, Q_n? \wedge \phi) * \psi$ .

Let us prove the validity of the axiom ( **$\mathbf{G}_{27}^*$** ). Suppose  $\mathfrak{M}, l \models |Q_1, \dots, Q_n? \wedge \text{size} \geq \beta$ , with  $\beta \geq \sharp(|Q_1, \dots, Q_n?|)$ . Then  $\beta \geq m$  with  $m = n - 1$  if  $|Q_1, \dots, Q_n?$  is  $|Q_1, \dots, Q_n|$ , or  $m = n$  otherwise. Since  $\mathfrak{M}, l \models |Q_1, \dots, Q_n?$ ,  $\mathfrak{R}$  contains at least  $m$  elements, so let us define  $\mathfrak{R}_1 = \{(l_1, l_2), \dots, (l_m, l_{m+1})\} \cup \mathfrak{R}'$ ,

where  $\mathfrak{R}'$  is an arbitrary set of  $\beta - m$  edges from  $\mathfrak{R}$ . Take the partition  $\{\mathfrak{R}_1, \mathfrak{R} \setminus \mathfrak{R}_1\}$ . Notice that  $\text{card}(\mathfrak{R}_1) = \beta$  and  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, \mathfrak{l} \models |Q_1, \dots, Q_n|$  (considering the adequate  $m$  for each case). Moreover,  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{W} \rangle, \mathfrak{l} \models \top$ . Then  $\mathfrak{M}, \mathfrak{l} \models (|Q_1, \dots, Q_n| \wedge \text{size} = \beta) * \top$ .

For the validity of the axiom **(G<sub>28</sub><sup>\*</sup>)**, suppose  $\mathfrak{M}, \mathfrak{l} \models |Q_1, \dots, Q_n| \wedge \text{size} \geq \beta + n$ , iff there exists a sequence of distinct locations  $\mathfrak{l} = \mathfrak{l}_1, \dots, \mathfrak{l}_{n+1}$ , with  $\mathfrak{l}_1 \mathfrak{R} \dots \mathfrak{l}_n \mathfrak{R} \mathfrak{l}_{n+1}$ , and for all  $j \in [1, n]$ , we have  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$ , and  $\text{card}(\mathfrak{R}) \geq \beta + n$ . Take the partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$ , where  $\mathfrak{R}_2 = \{(\mathfrak{l}_n, \mathfrak{l}_{n+1})\}$ , and  $\mathfrak{R}_1 = \mathfrak{R} \setminus \mathfrak{R}_2$ . Since  $\mathfrak{R}_1(\mathfrak{l}_n) = \emptyset$  (by definition of  $\mathfrak{R}_1$  and by weak functionality of  $\mathfrak{R}$ ), and also  $\text{card}(\mathfrak{R}_1) \geq \beta + n - 1$ , then  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, \mathfrak{l} \models |Q_1, \dots, Q_n| \wedge \text{size} \geq \beta + n - 1$ . On the other hand,  $\text{card}(\mathfrak{R}_2) = 1$ , therefore  $\mathfrak{M}, \mathfrak{l} \models (|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta + n - 1) * \text{size} = 1$ .

Finally, for the validity of the axiom **(G<sub>29</sub><sup>\*</sup>)**, suppose  $\mathfrak{M}, \mathfrak{l} \models |Q_1, \dots, \overline{Q_i, \dots, Q_n}| \wedge \text{size} \geq \beta + n$ , iff there exists a sequence of distinct locations  $\mathfrak{l} = \mathfrak{l}_1, \dots, \mathfrak{l}_n$ , and  $i \in [1, n]$  such that  $\mathfrak{l}_1 \mathfrak{R} \dots \mathfrak{l}_n \mathfrak{R} \mathfrak{l}_i$ , and for all  $j \in [1, n]$ ,  $\mathfrak{M}, \mathfrak{l}_j \models Q_j$ , and  $\text{card}(\mathfrak{R}) \geq \beta + n$ . Take the partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$ , where  $\mathfrak{R}_2 = \{(\mathfrak{l}_n, \mathfrak{l}_i)\}$ , and  $\mathfrak{R}_1 = \mathfrak{R} \setminus \mathfrak{R}_2$ . Since  $\mathfrak{R}_1(\mathfrak{l}_n) = \emptyset$  (by definition of  $\mathfrak{R}_1$  and by weak functionality of  $\mathfrak{R}$ ), and also  $\text{card}(\mathfrak{R}_1) \geq \beta + n - 1$ , then  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, \mathfrak{l} \models |Q_1, \dots, Q_n| \wedge \text{size} \geq \beta + n - 1$ . On the other hand,  $\text{card}(\mathfrak{R}_2) = 1$ , therefore  $\mathfrak{M}, \mathfrak{l} \models (|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta + n - 1) * \text{size} = 1$ .

Let us establish the validity of the axiom **(S<sub>5</sub><sup>\*</sup>)**, suppose  $\mathfrak{M}, \mathfrak{l} \models \text{size} \geq \beta_1 + \beta_2$ , iff  $\text{card}(\mathfrak{R}) \geq \beta_1 + \beta_2$ . So, we can find a partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$  such that  $\text{card}(\mathfrak{R}_1) = \beta_1$  and  $\text{card}(\mathfrak{R}_2) \geq \beta_2$ , then  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, \mathfrak{l} \models \text{size} = \beta_1$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{W} \rangle, \mathfrak{l} \models \text{size} \geq \beta_2$ . Therefore,  $\mathfrak{M}, \mathfrak{l} \models \text{size} = \beta_1 * \text{size} \geq \beta_2$ .

For the validity of the axiom **(S<sub>6</sub><sup>\*</sup>)**. Suppose that  $\mathfrak{M}, \mathfrak{l} \models (\neg \text{size} \geq \beta_1) * (\neg \text{size} \geq \beta_2)$ , iff  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, \mathfrak{l} \models \neg \text{size} \geq \beta_1$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{W} \rangle, \mathfrak{l} \models \neg \text{size} \geq \beta_2$ , for some partition  $\{\mathfrak{R}_1, \mathfrak{R}_2\}$  of  $\mathfrak{R}$ . Then, we have  $\text{card}(\mathfrak{R}_1) < \beta_1$  and  $\text{card}(\mathfrak{R}_2) < \beta_2$ , which gives us  $\text{card}(\mathfrak{R}) < \beta_1 + \beta_2$ , or equivalently,  $\text{card}(\mathfrak{R}) \leq (\beta_1 + \beta_2) - 1 \leq (\beta_1 + \beta_2) \div 1$ . So, we get  $\mathfrak{M}, \mathfrak{l} \models \neg \text{size} \geq (\beta_1 + \beta_2) \div 1$ .

Hence, all the axioms are valid.  $\square$

Forthcoming Lemma 12 states that the separating conjunction  $\phi * \psi$  of two Boolean combinations of core formulae is equivalent in  $\mathcal{H}_c(*)$  to some Boolean combination of core formulae  $\gamma$ , and therefore by Lemma 9,  $\phi * \psi$  is also logically equivalent to  $\gamma$ . Thanks to the axioms **(COM)** and **(\*DISTR)**, the **\*-introduction rule** and propositional reasoning, the satisfaction of such a property amounts to check it in the restricted case of elementary shapes (see Lemma 11).

Let us establish a preliminary lemma that is useful to prove Lemma 11.

**Lemma 10.** *The following formulae are derivable in  $\mathcal{H}_c(*)$ .*

**R0** *Let  $\phi, \phi'$  and  $\psi$  be formulae built from core formulae, and using Boolean connectives and the separating conjunction  $*$  such that  $\vdash_{\mathcal{H}_c(*)} \phi \Leftrightarrow \phi'$ . Then,  $\vdash_{\mathcal{H}_c(*)} \psi[\phi]_\rho \Leftrightarrow \psi[\phi']_\rho$ .*

**L0**  $(\phi \wedge \phi') * (\psi \wedge \psi') \Rightarrow \phi * \psi$ .

**L1**  $\text{size} \geq \beta_1 * \text{size} \geq \beta_2 \Leftrightarrow \text{size} \geq \beta_1 + \beta_2$ .

**L2**  $((\phi \wedge \text{size} \geq \beta) * \psi) \wedge \neg \text{size} \geq \beta' \Rightarrow (\phi \wedge \text{size} \geq \beta) * (\psi \wedge \neg \text{size} \geq \beta' - \beta)$ .

**L3**  $((\phi \wedge \neg \text{size} \geq \beta + 1) * \psi) \wedge \text{size} \geq \beta' \Rightarrow (\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \text{size} \geq \beta' - \beta)$ .

**L4** *for any  $\beta_1 < \beta'_1$  and  $\beta_2 < \beta'_2$ ,*

$$\text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \Leftrightarrow (\text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2).$$

The formula  $\psi[\phi]_\rho$  in **R0** stands for the formula obtained from  $\psi$  by replacing the formula at the occurrence  $\rho$  by the formula  $\phi$ . The proof of Lemma 10 can be found in the appendix.

The validity of the axiom **(G<sub>22</sub><sup>\*</sup>)** rests on the fact that the separating conjunction of two graph formulae, each having a graph size at least one is unsatisfiable. This property can be lifted to elementary shapes. However, what remains to be established is how to eliminate the separating conjunction of two elementary shapes such that at least one of them has graph size equal to zero. The following lemma is dedicated to this special type of **\*-elimination**, which is then used for the general result on arbitrary formulae (Lemma 12).

**Lemma 11.** *The formulae listed in the table below are derivable in  $\mathcal{H}_c(*)$ .*

Derivable formulae about separating conjunctions of elementary shapes

**Notation:** The formula  $|Q_1, \dots, Q_n \overline{\phantom{x}}|$  denotes either a formula of the form  $|Q_1, \dots, Q_n \rangle$ , or a formula of the form  $|Q_1, \dots, \overline{Q_i}, \dots, Q_n|$  (this excludes graph formulae of the form  $|Q_1, \dots, Q_n|$ ). Below, the occurrences of  $|Q_1, \dots, Q_n \overline{\phantom{x}}|$  on the left and on the right of every equivalence are for the same form, i.e. either both  $|Q_1, \dots, Q_n \rangle$  or both  $|Q_1, \dots, \overline{Q_i}, \dots, Q_n|$  (where the position  $i$  is the same).

**Assumption:** below, in every elementary shape  $\psi$  of the form  $\mathcal{G} \wedge \text{size} \geq \beta$  or  $\mathcal{G} \wedge \text{size} \geq \beta \wedge \neg \text{size} \geq \beta'$ , we have  $\sharp(\mathcal{G}) \leq \beta$  and  $\forall \mathcal{H}_c \neg \psi$  (hence e.g.  $\beta < \beta'$ ).

- $(|Q_1, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1) * (|Q| \wedge \text{size} \geq \beta_2) \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1 + \beta_2$
- $(|Q_1, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2) \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1 + \beta_2$
- $(|Q_1, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1 + \beta_2$
- $(|Q_1, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2)$   
 $\Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{x}}| \wedge \text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1$
- $(|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta_1) * (|Q| \wedge \neg \text{size} \geq 1) \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n| \wedge \text{size} \geq \beta_1$
- $(|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta_2) * (|Q| \wedge \neg \text{size} \geq 1) \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta_2$

Let  $\gamma_n \stackrel{\text{def}}{=} (|Q_1 \wedge Q, \dots, Q_n| \vee |Q_1 \wedge Q, \dots, Q_n \rangle \vee \bigvee_{i \in [1, n]} |Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n|) \wedge \text{size} \geq \beta_1 + \beta_2 + 1$ .

- $(|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta_1) * (|Q| \wedge \text{size} \geq \beta_2 + 1) \Leftrightarrow \gamma_n$
- $(|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 + 1) \Leftrightarrow \gamma_n$
- $(|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta_1) * (|Q| \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Leftrightarrow \gamma_n$
- $(|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Leftrightarrow \gamma_n \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \div 1$

The long syntactic proof of Lemma 11 can be found in the appendix. It should be noted that we could directly add these formulae to the proof system: it would avoid the lengthy proof of Lemma 11 in favor of a simpler semantical proof. However, the resulting calculus would certainly be redundant. From Lemmata 9 and 11, we get the main result about  $*$ -elimination.

**Lemma 12.** *Let  $\phi, \psi$  be Boolean combinations of core formulae. There is a Boolean combination of core formulae  $\gamma$  such that  $\vdash_{\mathcal{H}_c(*)} (\phi * \psi) \Leftrightarrow \gamma$ .*

Observe that  $\gamma$  is a Boolean combination of core formulae and  $*$  does not occur in it. In the proof of Lemma 12, if  $\vdash_{\mathcal{H}_c(*)} \neg \phi$  or  $\vdash_{\mathcal{H}_c(*)} \neg \psi$ , then the axiom ( $\perp$ ) is used. Otherwise, the proof amounts to prove the statement for elementary shapes only, which corresponds to Lemma 11.

*Proof.* Before providing the proof, let us state a property used in several places.

( $\dagger\dagger$ ) Let  $\phi, \phi'$  and  $\psi$  be formulae built from core formulae, the Boolean connectives and the separating conjunction  $*$  such that  $\vdash_{\mathcal{H}_c(*)} \phi \Leftrightarrow \phi'$ . Then  $\vdash_{\mathcal{H}_c(*)} \psi[\phi]_\rho \Leftrightarrow \psi[\phi']_\rho$  where  $\psi[\phi]_\rho$  stands for the formula obtained from  $\psi$  by replacing the formula at the occurrence  $\rho$  by the formula  $\phi$ .

( $\dagger\dagger$ ) is proved along the lines of the proof of Lemma 21 and is therefore omitted herein. It corresponds also to **R0** from Lemma 10.

Let  $\phi$  and  $\psi$  be Boolean combinations of core formulae. By Lemma 4, there are disjunctions of elementary shapes  $\bigvee_i \phi_i$  and  $\bigvee_j \psi_j$  such that  $\vdash_{\mathcal{H}_c(*)} \phi \Leftrightarrow \bigvee_i \phi_i$  and  $\vdash_{\mathcal{H}_c(*)} \psi \Leftrightarrow \bigvee_j \psi_j$ . By ( $\dagger\dagger$ ), and by using the axiom (**\*DISTR**), we can conclude that  $\vdash_{\mathcal{H}_c(*)} \phi * \psi \Leftrightarrow \bigvee_i \bigvee_j \phi_i * \psi_j$ . In order to prove the result, it is then sufficient to show that for all the elementary shapes  $\psi', \psi''$ , there is a Boolean combination of core formulae  $\gamma'$  such that  $\vdash_{\mathcal{H}_c(\diamond)} \psi' * \psi'' \Leftrightarrow \gamma'$ .

- In the case  $\vdash_{\mathcal{H}_c(\diamond)} \neg \psi'$  (which amounts to unsatisfiability of  $\psi'$  by Lemma 5), by propositional reasoning  $\vdash_{\mathcal{H}_c(\diamond)} \psi' \Rightarrow \perp$  and by the **\*-introduction rule**, we get  $\vdash_{\mathcal{H}_c(\diamond)} \psi' * \psi'' \Rightarrow \perp * \psi''$ . By

the axiom  $(\perp)$ ,  $\vdash_{\mathcal{H}_c(\diamond)} \neg(\perp * \psi'')$ , which by propositional reasoning leads to  $\vdash_{\mathcal{H}_c(\diamond)} \neg(\psi' * \psi'')$ . Finally, by propositional reasoning, we get  $\vdash_{\mathcal{H}_c(\diamond)} \psi' * \psi'' \Leftrightarrow \perp$ . A similar reasoning applies when  $\vdash_{\mathcal{H}_c(\diamond)} \neg\psi''$ , but this time the axiom  $(\text{COM})$  needs to be evoked.

- In the case,  $\psi' = \mathcal{G} \wedge \dots$  and  $\psi'' = \mathcal{G}' \wedge \dots$  with  $\sharp(\mathcal{G}) \times \sharp(\mathcal{G}') \geq 1$ , we get  $\vdash_{\mathcal{H}_c(\diamond)} \neg(\mathcal{G} * \mathcal{G}')$  by the axiom  $(\mathbf{G}_{22}^*)$ . By **L0**,  $\vdash_{\mathcal{H}_c(\diamond)} \psi' * \psi'' \Rightarrow \mathcal{G} * \mathcal{G}'$  and therefore by propositional reasoning, we get  $\vdash_{\mathcal{H}_c(\diamond)} \neg(\psi' * \psi'')$ , which leads again to  $\vdash_{\mathcal{H}_c(\diamond)} \psi' * \psi'' \Leftrightarrow \perp$ .

It remains to consider the cases when if  $\psi'$  or  $\psi''$  is an elementary shape of the form either  $\mathcal{G} \wedge \text{size} \geq \beta$  or  $\mathcal{G} \wedge \text{size} \geq \beta \wedge \neg \text{size} \geq \beta'$ , then  $\sharp(\mathcal{G}) \leq \beta$ ,  $\beta < \beta'$  and more generally not  $\vdash_{\mathcal{H}_c(\diamond)} \neg\psi'$  and not  $\vdash_{\mathcal{H}_c(\diamond)} \neg\psi''$ . Similarly, we assume that  $\sharp(\mathcal{G}) \times \sharp(\mathcal{G}') = 0$  where  $\mathcal{G}$  (resp.  $\mathcal{G}'$ ) is the graph formula of  $\psi'$  (resp.  $\psi''$ ). These are exactly the conditions from Lemma 11 and therefore we are done.  $\square$

### 3.3.3 Putting all together: axiomatising $\text{MSL}(*, \diamond)$

Let  $\mathcal{HMSL}(*, \diamond)$  be the Hilbert-style proof system defined as the union of the axioms and inference rules from  $\mathcal{H}_c(\diamond)$  and  $\mathcal{H}_c(*)$  (with the intersection  $\mathcal{H}_c$ ) augmented with the axiom below, dealing with standalone occurrences of propositional variables (i.e., occurrences that are not part of some graph formula):

$$(\mathbf{G}_{30}) \quad p \Leftrightarrow (|p\rangle \vee |p\rangle \vee |\overline{p}\rangle) \text{ with } p \in \text{PROP.}$$

**Theorem 13** (Adequacy of  $\mathcal{HMSL}(*, \diamond)$ ). *The axiom system  $\mathcal{HMSL}(*, \diamond)$  is sound and complete for  $\text{MSL}(*, \diamond)$ .*

*Proof.* The proof can be divided in three parts, with increasing difficulty.

1. To show that the axiom  $(\mathbf{G}_{30})$  is valid for  $\text{MSL}(*, \diamond)$  (direct).
2. To show that all the axioms and inference rules of  $\mathcal{HMSL}(*, \diamond)$  are valid for  $\text{MSL}(*, \diamond)$ .
3. To show that for every valid formula  $\phi$ , we have  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi$ .

The proof of (2.) is a consequence of (1.), Lemma 7 and Lemma 9. However, one needs to notice that the validity of the axiom schemas and inference rules can be deduced from the proofs of Lemma 7 and Lemma 9, even though in  $\mathcal{HMSL}(*, \diamond)$ , the metavariables  $\phi$ ,  $\psi$  and  $\gamma$  used in the axioms and inference rules from  $\mathcal{H}_c(\diamond)$  and  $\mathcal{H}_c(*)$ , can be safely instantiated by any formula in  $\text{MSL}(*, \diamond)$ .

The proof of (3.) consists in showing that there is a Boolean combination of core formulae  $\psi$  such that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi \Leftrightarrow \psi$  (and therefore  $\phi$  and  $\psi$  are logically equivalent by (2.)). For instance,  $\text{loop}_2$  from Section 2 is logically equivalent to  $|\overline{\top}, \top\rangle \wedge \text{size} \geq 2 \wedge \neg \text{size} \geq 3$  and this can be derived in  $\mathcal{HMSL}(*, \diamond)$ . So,  $\psi$  is a valid combination of core formulae and by Theorem 6, we get  $\vdash_{\mathcal{H}_c} \psi$  and therefore  $\vdash_{\mathcal{HMSL}(*, \diamond)} \psi$  as  $\mathcal{HMSL}(*, \diamond)$  obviously extends  $\mathcal{H}_c$ . By propositional reasoning, we can conclude that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi$ . It remains to prove that  $\psi$  exists. The proof can be done by induction on the structure of  $\phi$ .

**Base case**  $\phi = p$ . By the axiom  $(\mathbf{G}_{30})$ , we have  $\vdash_{\mathcal{HMSL}(*, \diamond)} p \Leftrightarrow (|p\rangle \vee |p\rangle \vee |\overline{p}\rangle)$ .

**Case**  $\phi = \neg\phi_1$ . By the induction hypothesis, there is a Boolean combination of core formulae  $\psi_1$  such that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi_1 \Leftrightarrow \psi_1$ . By propositional reasoning, we conclude that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \neg\phi_1 \Leftrightarrow \neg\psi_1$ .

**Case**  $\phi = \phi_1 \wedge \phi_2$ . Similar to the previous case.

**Case**  $\phi = \diamond\phi_1$ . By the induction hypothesis, there is a Boolean combination of core formulae  $\psi_1$  such that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi_1 \Leftrightarrow \psi_1$ . By propositional reasoning and using the [Regularity rule](#) (twice), we conclude  $\vdash_{\mathcal{HMSL}(*, \diamond)} \diamond\phi_1 \Leftrightarrow \diamond\psi_1$ . By [Lemma 8](#), there is a Boolean combination of core formula  $\psi'_1$  such that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \diamond\psi_1 \Leftrightarrow \psi'_1$ . By propositional reasoning, we get that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \diamond\phi_1 \Leftrightarrow \psi'_1$ .

**Case**  $\phi = \phi_1 * \phi_2$ . By the induction hypothesis, there are Boolean combinations of core formulae  $\psi_1$  and  $\psi_2$  such that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi_1 \Leftrightarrow \psi_1$  and  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi_2 \Leftrightarrow \psi_2$ . By propositional reasoning, and by using the [\\*-introduction rule](#) (4 times) and the axiom [\(COM\)](#), we conclude  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi_1 * \phi_2 \Leftrightarrow \psi_1 * \psi_2$ . By [Lemma 12](#), there is a Boolean combination of core formula  $\psi'_1$  such that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \psi_1 * \psi_2 \Leftrightarrow \psi'_1$ . By propositional reasoning, we get that  $\vdash_{\mathcal{HMSL}(*, \diamond)} \phi_1 * \phi_2 \Leftrightarrow \psi'_1$ .  $\square$

We conclude this section by showing that the logic  $\text{MSL}(*, \diamond)$  is not compact. As a consequence, the proof system  $\mathcal{HMSL}(*, \diamond)$  (and actually, any finite axiom system) is not strongly complete. This means that every theorem in  $\text{MSL}(*, \diamond)$  can be derived in the system, but it is not always possible to prove that a formula  $\varphi$  is derived from a set of formulae  $\Phi$ , i.e., to prove  $\Phi \vdash_{\mathcal{HMSL}(*, \diamond)} \varphi$ .

**Theorem 14.**  *$\text{MSL}(*, \diamond)$  is not compact; therefore,  $\mathcal{HMSL}(*, \diamond)$  is not strongly complete for  $\text{MSL}(*, \diamond)$ .*

*Proof.* Let  $X_\infty = \{\text{size} \geq \beta \mid \beta \in \mathbb{N}\}$ . Notice that  $X_\infty$  is unsatisfiable, since  $\text{MSL}$  models have finite accessibility relations. Strong completeness would imply that  $\perp$  could be derived from  $X_\infty$ . As all rules are finitary, then there is a finite subset  $X \subseteq X_\infty$  such that  $X \vdash_{\mathcal{HMSL}(*, \diamond)} \perp$ , or equivalently  $\vdash_{\mathcal{HMSL}(*, \diamond)} \bigvee_{\psi \in X} \neg\psi$ . This leads to a contradiction by the correctness of  $\mathcal{HMSL}(*, \diamond)$ . The same argument can be used for other finitary proof systems, with the same set  $X_\infty$ .  $\square$

## 4 Hilbert-style proof system for $\text{MSL}(*, \langle \neq \rangle)$

In this section, we present a proof system for the modal separation logic  $\text{MSL}(*, \langle \neq \rangle)$ . In order to do that, we will use previous developments from [Sec. 3](#), as well as adapting to infinite models the proof method in [\[50\]](#) for axiomatising the logic of elsewhere  $\text{ML}(\langle \neq \rangle)$ . The NP upper bound proof for  $\text{MSL}(*, \langle \neq \rangle)$  satisfiability in [\[24\]](#) takes advantage of an abstraction that considers the number of edges in the model (up to a value depending linearly on the size of the input formula) and whether given a propositional valuation (restricted to the propositional variables occurring in the input formula), there are none, one or two locations satisfying it. The developments below propose a syntactic characterisation for  $\text{MSL}(*, \langle \neq \rangle)$  validity. Such a characterisation also witnesses that the interplay between the number of edges and the constraints on the propositional valuations is very weak (see the axioms [\( \$\langle \neq \rangle\$ SEP\)](#) and [\(\\*SEP\)](#) below). It is worth noting that the logic  $\text{MSL}(*, \langle \neq \rangle)$  might appear a bit more esoteric than  $\text{MSL}(*, \diamond)$  and we are not aware of a killer application of the logic. However, the treatments below illustrate how our method can be further developed (see also [\[27\]](#)), though we need to take advantage of a few specific features of  $\text{MSL}(*, \langle \neq \rangle)$ .

Below, we introduce two families of formulae that will be used in the sequel. First, we introduce the set of *pure separation formulae*  $\text{MSL}(*)$ , given by the following grammar:

$$\phi ::= \text{emp} \mid \phi \wedge \phi \mid \neg\phi \mid \phi * \phi.$$

The set of *pure modal formulae*  $\text{MSL}(\langle \neq \rangle)$  is given by:

$$\phi ::= p \mid \phi \wedge \phi \mid \neg\phi \mid \langle \neq \rangle\phi \mid [\neq]\phi,$$

with  $p \in \text{PROP}$ .

We design the Hilbert-style proof system  $\mathcal{HMSL}(*, \langle \neq \rangle)$  for  $\text{MSL}(*, \langle \neq \rangle)$  as the union of the proof system  $\mathcal{HMSL}(\langle \neq \rangle)$  for  $\text{MSL}(\langle \neq \rangle)$ , the proof system  $\mathcal{HMSL}(*)$  for  $\text{MSL}(*)$  (no propositional variables and modalities), and new axioms [\( \$\langle \neq \rangle\$ SEP\)](#) and [\(\\*SEP\)](#). Hence, we propose below a modular approach to design  $\mathcal{HMSL}(*, \langle \neq \rangle)$  that takes advantage of more elementary building blocks.



## 4.1 Axiomatising $ML(\langle \neq \rangle)$ on MSL models

We introduce the proof system  $\mathcal{HMSL}(\langle \neq \rangle)$  for axiomatising the logic  $MSL(\langle \neq \rangle)$ , that is designed by augmenting the Hilbert-style system for the logic of elsewhere  $ML(\langle \neq \rangle)$  from [50] by an axiom expressing that  $MSL(\langle \neq \rangle)$  models have an infinite number of locations (namely **(INF)**). For instance, the formula  $\langle U \rangle(p \wedge [\neq] \neg p) \wedge \langle U \rangle(\neg p \wedge [\neq] p)$  is satisfiable in some  $ML(\langle \neq \rangle)$  model with two locations exactly whereas it is unsatisfiable for  $MSL(\langle \neq \rangle)$ . As usual, the axiom schemas and modus ponens for propositional calculus are part of  $\mathcal{HMSL}(\langle \neq \rangle)$ .

Axioms and inference rule for  $\mathcal{HMSL}(\langle \neq \rangle)$

<b>(K)</b> $[\neq](\phi \Rightarrow \psi) \Rightarrow ([\neq]\phi \Rightarrow [\neq]\psi)$	Necessitation rule: $\frac{\phi}{[\neq]\phi}$
<b>(B)</b> $\phi \Rightarrow [\neq]\langle \neq \rangle \phi$	
<b>(ALIO)</b> $\phi \Rightarrow ([\neq]\phi \Rightarrow [\neq][\neq]\phi)$	
<b>(INF)</b> $\bigvee_{X \subseteq P} \langle U \rangle(\psi_X \wedge \langle \neq \rangle \psi_X)$ for every $P \subseteq_{\text{fin}} \text{PROP}$ , where $\psi_X$ stands for $(\bigwedge_{p \in X} p) \wedge (\bigwedge_{p \in (P \setminus X)} \neg p)$ .	

In  $\mathcal{HMSL}(\langle \neq \rangle)$ , the axiom **(K)** and the necessitation rule are standard for normal modal logics, whereas the axiom **(B)** (resp. **(ALIO)**) takes care of the symmetry (resp. the aliotransitivity) of the difference relation (see [50]). As the  $MSL(\langle \neq \rangle)$  models are necessarily infinite (by contrast to the models for the logic of elsewhere), we add the axiom **(INF)**. It states that for any finite set  $X$  of propositional variables, there exist two distinct locations with the same valuation over  $X$ .

**Lemma 15.** *The axioms and rules in  $\mathcal{HMSL}(\langle \neq \rangle)$  are valid for  $MSL(\langle \neq \rangle)$ .*

An  $MSL(\langle \neq \rangle)$  model  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$  can be understood as the  $ML(\langle \neq \rangle)$  model  $\langle \mathbb{N}, \neq, \mathfrak{V} \rangle$  since the language  $MSL(\langle \neq \rangle)$  does not require to use of the relation  $\mathfrak{R}$  to evaluate formulae. So, in the sequel, we assume that the models for  $ML(\langle \neq \rangle)$  are of the form  $\langle \mathfrak{W}, \neq, \mathfrak{V} \rangle$ , whereas those for  $MSL(\langle \neq \rangle)$  are the restrictions with  $\mathfrak{W} = \mathbb{N}$ .

*Proof.* All the axioms and rules in  $\mathcal{HMSL}(\langle \neq \rangle)$  except **(INF)** are valid for the modal logic  $ML(\langle \neq \rangle)$  [50]. As all the  $MSL(\langle \neq \rangle)$  models are  $ML(\langle \neq \rangle)$  models, we get also validity with respect to  $MSL(\langle \neq \rangle)$ . It remains to show that **(INF)** is valid for  $MSL(\langle \neq \rangle)$ . Let  $\mathfrak{M} = \langle \mathbb{N}, \neq, \mathfrak{V} \rangle$  be a model for  $MSL(\langle \neq \rangle)$  and  $l \in \mathbb{N}$ . Given a finite set  $\{p_1, \dots, p_n\}$ ,  $n \geq 0$ , for each  $X \subseteq \{p_1, \dots, p_n\}$ , we write  $Y_X \subseteq \mathbb{N}$  to denote the set below:

$$Y_X \stackrel{\text{def}}{=} \{l \in \mathbb{N} \mid \mathfrak{M}, l \models (\bigwedge_{p \in X} p) \wedge (\bigwedge_{p \in (\{p_1, \dots, p_n\} \setminus X)} \neg p)\}.$$

Obviously, the set  $\{Y_X \mid X \in \mathcal{P}(\{p_1, \dots, p_n\})\}$  defines a finite partition of  $\mathbb{N}$  (with at most  $2^n$  elements) and therefore there is  $X_0$  such that  $Y_{X_0}$  is infinite. So, there are  $l_1 \neq l_2$  such that  $l_1, l_2 \in Y_{X_0}$ . Consequently,

$$\mathfrak{M}, l \models \langle U \rangle(\psi_{X_0} \wedge \langle \neq \rangle \psi_{X_0}),$$

and therefore  $\mathfrak{M}, l \models \bigvee_{X \subseteq \{p_1, \dots, p_n\}} \langle U \rangle(\psi_X \wedge \langle \neq \rangle \psi_X)$ .  $\square$

**Lemma 16.**  *$\mathcal{HMSL}(\langle \neq \rangle)$  is sound and complete for  $MSL(\langle \neq \rangle)$ .*

The completeness of  $\mathcal{HMSL}(\langle \neq \rangle)$  is shown by adapting the completeness proof from [50] and by taking advantage of the infinity axiom **(INF)**.

*Proof.* Let  $\mathfrak{M}_C = \langle \mathfrak{W}_C, \mathfrak{R}_C, \mathfrak{V}_C \rangle$  be the canonical model for  $\mathcal{HMSL}(\langle \neq \rangle)$ , see details of the construction in [8]. We recall that  $\mathfrak{W}_C$  is the set of maximally consistent sets of formulae (based on  $\mathcal{HMSL}(\langle \neq \rangle)$ ). By Lemma 15,  $\emptyset$  is consistent and by Lindenbaum's Lemma, there is at least one maximally consistent set, whence  $\mathfrak{W}_C$  is non-empty. For all  $w, w' \in \mathfrak{W}_C$ , we have  $w \mathfrak{R}_C w'$  iff for all  $[\neq]\phi \in w$ , we have  $\phi \in w'$ . Furthermore, by definition,  $w \in \mathfrak{V}(p)$  iff  $p \in w$ , for all  $w \in \mathfrak{W}_C$  and propositional variables  $p$ . As shown in [50],  $\mathfrak{R}_C$  is symmetric and aliotransitive, but not necessarily equal to the difference relation on  $\mathfrak{W}_C$ .

Let  $\phi$  be a valid formula and *ad absurdum*, suppose that  $\text{not } \vdash_{\mathcal{HMSL}(\langle \neq \rangle)} \phi$ . Without loss of generality, we can assume that  $\phi$  contains at least one propositional variable, as  $\phi$  is valid iff  $\phi \wedge p \Leftrightarrow p$  is valid, and  $\vdash_{\mathcal{HMSL}(\langle \neq \rangle)} \phi$  iff  $\vdash_{\mathcal{HMSL}(\langle \neq \rangle)} \phi \wedge p \Leftrightarrow p$  (by propositional reasoning). Consequently,  $\{\neg\phi\}$  is consistent and therefore there is  $w^\dagger \in \mathfrak{W}_C$  such that  $\neg\phi \in w^\dagger$ . By the Truth Lemma,  $\mathfrak{M}_C, w^\dagger \models \neg\phi$  but  $\mathfrak{M}_C$  is not an  $\text{ML}(\langle \neq \rangle)$  model, and a fortiori,  $\mathfrak{M}_C$  is not an  $\text{MSL}(\langle \neq \rangle)$  model. Therefore, some more work is needed to lead to a contradiction.

Furthermore, as shown in [50], let us consider  $\mathfrak{M} = \langle \mathfrak{W}, \mathfrak{R}, \mathfrak{V} \rangle$  such that  $\mathfrak{W} = \{w' \in \mathfrak{W}_C \mid (w^\dagger, w') \in \mathfrak{R}_C^*\}$  and,  $\mathfrak{R}$  and  $\mathfrak{V}$  are the restriction of  $\mathfrak{R}_C$  and  $\mathfrak{V}_C$  to  $\mathfrak{W}$  respectively ( $\mathfrak{R}_C^*$  is the reflexive and transitive closure of  $\mathfrak{R}_C$ ). Consequently,  $\mathfrak{M}, w^\dagger \models \neg\phi$  as  $\mathfrak{M}$  is the generated submodel from  $w^\dagger$ .

Let  $\mathfrak{M}^\dagger = \langle \mathfrak{W}^\dagger, \mathfrak{R}^\dagger, \mathfrak{V}^\dagger \rangle$  be the model such that

- $\mathfrak{W}^\dagger \stackrel{\text{def}}{=} \{(w, 0) \mid (w, w) \notin \mathfrak{R}, w \in \mathfrak{W}\} \cup \{(w, 1), (w, 2) \mid (w, w) \in \mathfrak{R}, w \in \mathfrak{W}\}$ .
- $(w, i)\mathfrak{R}^\dagger(w', j) \stackrel{\text{def}}{\Leftrightarrow}$  either  $w \neq w'$  and  $w\mathfrak{R}w'$ , or  $w = w'$  and  $i \neq j$ .
- $(w, i) \in \mathfrak{V}^\dagger(p)$  iff  $w \in \mathfrak{V}(p)$ .

It is shown in [50] that  $\mathfrak{R}^\dagger$  is the difference relation on  $\mathfrak{W}^\dagger$  and there is a p-morphism from  $\mathfrak{M}^\dagger = \langle \mathfrak{W}^\dagger, \mathfrak{R}^\dagger, \mathfrak{V}^\dagger \rangle$  to  $\mathfrak{M} = \langle \mathfrak{W}, \mathfrak{R}, \mathfrak{V} \rangle$ . Hence,  $\mathfrak{M}^\dagger, (w^\dagger, i^\dagger) \models \neg\phi$  for some  $i^\dagger \in \{0, 1, 2\}$  as p-morphic images preserve the satisfaction of formulae. We shall use this property even further. Let  $\{p_1, \dots, p_n\}$  ( $n \geq 1$ ) be the set of propositional variables occurring in  $\phi$ . By the axiom **(INF)**, we get  $\vdash_{\mathcal{HMSL}(\langle \neq \rangle)} \bigvee_{X \subseteq \{p_1, \dots, p_n\}} \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X)$  and as  $w^\dagger$  is a maximally consistent set, we have  $\bigvee_{X \subseteq \{p_1, \dots, p_n\}} \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X) \in w^\dagger$ . Again, as  $w^\dagger$  is maximally consistent, there is  $X \subseteq \{p_1, \dots, p_n\}$  such that  $\langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X) \in w^\dagger$ . Indeed, every maximally consistent set contains all the theorems of  $\mathcal{HMSL}(\langle \neq \rangle)$  and a disjunction belongs to such a set iff one of its disjuncts belongs to it. By the Truth Lemma, we get  $\mathfrak{M}_C, w^\dagger \models \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X)$ , and therefore  $\mathfrak{M}, w^\dagger \models \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X)$  and  $\mathfrak{M}^\dagger, (w^\dagger, i^\dagger) \models \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X)$ . In conclusion,  $\mathfrak{M}^\dagger, (w^\dagger, i^\dagger) \models \psi$  with  $\psi \stackrel{\text{def}}{=} \neg\phi \wedge \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X)$ . So,  $\neg\phi \wedge \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X)$  is  $\text{ML}(\langle \neq \rangle)$  satisfiable and by [22, Proposition 2], there is  $\alpha \leq 2|\psi|+1$  such that  $\mathfrak{M}' = \langle [0, \alpha], \neq, \mathfrak{V}' \rangle$  and  $\mathfrak{M}', 0 \models \neg\phi \wedge \langle \text{U} \rangle (\psi_X \wedge \langle \neq \rangle \psi_X)$ . There are  $i \neq j \in [0, \alpha]$  such that  $\mathfrak{M}', i \models \psi_X$  and  $\mathfrak{M}', j \models \psi_X$ .

Let  $\mathfrak{M}'' = \langle \mathbb{N}, \neq, \mathfrak{V}'' \rangle$  be the  $\text{MSL}(\langle \neq \rangle)$  model, such that

- The restriction of  $\mathfrak{V}''$  to  $[0, \alpha]$  is equal to  $\mathfrak{V}'$ .
- For all  $\beta > \alpha$  and  $p_I$  with  $I \in [1, n]$ , we have  $\beta \in \mathfrak{V}''(p_I)$  iff  $p_I \in X$ .

One can show that  $\mathfrak{M}'', 0 \models \neg\phi$  and therefore this leads to a contradiction by the validity of  $\phi$ . In order to get  $\mathfrak{M}'', 0 \models \neg\phi$ , it is sufficient to show by structural induction, that for all subformulae  $\psi$  of  $\neg\phi$ , for all  $\beta \in [0, \alpha]$ , we have  $\mathfrak{M}', \beta \models \psi$  iff  $\mathfrak{M}'', \beta \models \psi$ .

First, let us show that  $(\dagger)$  for all distinct  $l, l'$  that agree on their valuation on  $\{p_1, \dots, p_n\}$  in  $\mathfrak{M}''$ , we have for all formulae  $\psi$  built over  $\{p_1, \dots, p_n\}$ ,  $\mathfrak{M}'', l \models \psi$  iff  $\mathfrak{M}'', l' \models \psi$ . The base case with  $\psi \in \{p_1, \dots, p_n\}$  or the cases in the induction step for  $\wedge$  and  $\neg$  are by an easy verification. Now suppose that  $\mathfrak{M}'', l \models \langle \neq \rangle \psi$ . There is  $l'' \neq l$  such that  $\mathfrak{M}'', l'' \models \psi$ . If  $l'' \neq l'$  too, then obviously there is also  $l'' \neq l'$  such that  $\mathfrak{M}'', l'' \models \psi$  and therefore  $\mathfrak{M}'', l' \models \langle \neq \rangle \psi$ . Otherwise (i.e.  $l'' = l'$ ), by the induction hypothesis, we also have  $\mathfrak{M}'', l \models \psi$  and therefore there is  $l'' \neq l'$  such that  $\mathfrak{M}'', l'' \models \psi$ , namely  $l'' = l$ , whence  $\mathfrak{M}'', l' \models \langle \neq \rangle \psi$ .

Now, let us establish that for all subformulae  $\psi$  of  $\neg\phi$ , for all  $\beta \in [0, \alpha]$ , we have  $\mathfrak{M}', \beta \models \psi$  iff  $\mathfrak{M}'', \beta \models \psi$ . The base case with  $\psi \in \{p_1, \dots, p_n\}$  or the cases in the induction step for  $\wedge$  and  $\neg$  are again by an easy verification.

First, let us suppose that  $\mathfrak{M}', \beta \models \langle \neq \rangle \psi$ . There is  $\beta' \neq \beta$  such that  $\mathfrak{M}', \beta' \models \psi$ . By the induction hypothesis, we have  $\mathfrak{M}'', \beta' \models \psi$  and therefore  $\mathfrak{M}'', \beta \models \langle \neq \rangle \psi$ . Conversely, suppose that  $\mathfrak{M}'', \beta \models \langle \neq \rangle \psi$ . There is  $\beta' \neq \beta$  such that  $\mathfrak{M}'', \beta' \models \psi$ . If  $\beta' \in [0, \alpha]$ , then by the induction hypothesis we have  $\mathfrak{M}', \beta' \models \psi$  and therefore  $\mathfrak{M}', \beta \models \langle \neq \rangle \psi$ . Otherwise (i.e.  $\beta' > \alpha$ ), in  $\mathfrak{M}'', \beta', i$ , and  $j$  agree on the propositional variables in  $\{p_1, \dots, p_n\}$ . Moreover, either  $\beta \neq i$  or  $\beta \neq j$ . Without lack of generality, suppose that  $\beta \neq i$ . Consequently, by  $(\dagger)$ , we have  $\mathfrak{M}'', i \models \psi$ . By the induction hypothesis, we have  $\mathfrak{M}', i \models \psi$  and therefore  $\mathfrak{M}', \beta \models \langle \neq \rangle \psi$ .  $\square$

## 4.2 Axiomatising $\text{MSL}(\ast)$

Now we present the Hilbert-style system  $\mathcal{HMSL}(\ast)$  for the logic  $\text{MSL}(\ast)$ . It is designed as a fragment of the Hilbert-style system  $\mathcal{HMSL}(\ast, \diamond)$  from Sec. 3 by simplifying the axioms and by keeping only what is needed for  $\text{MSL}(\ast)$ .

Axioms and inference rules for $\mathcal{HMSL}(\ast)$	
( $\perp$ )	$\neg(\perp \ast \phi)$
(COM)	$(\phi \ast \psi) \Leftrightarrow (\psi \ast \phi)$
( $\ast$ DISTR)	$(\phi_1 \vee \phi_2) \ast \psi \Leftrightarrow (\phi_1 \ast \psi) \vee (\phi_2 \ast \psi)$
(ASSOC)	$(\phi \ast \psi) \ast \gamma \Leftrightarrow \phi \ast (\psi \ast \gamma)$
( $\mathbf{S}_4^*$ )	$\phi \Leftrightarrow (\phi \ast \neg \text{size} \geq 1)$
( $\mathbf{S}_5^*$ )	$\text{size} \geq \beta_1 + \beta_2 \Rightarrow \text{size} = \beta_1 \ast \text{size} \geq \beta_2$
( $\mathbf{S}_6^*$ )	$\neg \text{size} \geq \beta_1 \ast \neg \text{size} \geq \beta_2 \Rightarrow \neg \text{size} \geq (\beta_1 + \beta_2) \dot{-} 1$
( $\mathbf{S}_1^c$ )	$\text{size} \geq 0$
( $\mathbf{S}_2^c$ )	$\text{size} \geq \beta + 1 \Rightarrow \text{size} \geq \beta$
	$\ast$ -introduction rule: $\frac{\phi \Rightarrow \gamma}{\phi \ast \psi \Rightarrow \gamma \ast \psi}$
	$(\alpha_1 \dot{-} \alpha_2 \stackrel{\text{def}}{=} \max(0, \alpha_1 - \alpha_2))$

As  $\text{MSL}(\ast)$  is a fragment of both  $\text{MSL}(\ast, \diamond)$  and  $\text{MSL}(\ast, \langle \neq \rangle)$ , it should not come as a surprise that all the axioms above were already introduced in Sec. 3.3. Before proving completeness, we establish a few results about  $\mathcal{HMSL}(\ast)$  that can be shown along the lines of Sec. 3.3 but drastic simplifications apply.

**Lemma 17** (Correctness of  $\text{MSL}(\ast)$ ). *The axioms and rules in  $\mathcal{HMSL}(\ast)$  are valid for  $\text{MSL}(\ast)$ .*

This is a consequence of the correctness for  $\mathcal{HMSL}(\ast, \diamond)$  (see Sec. 3), as derivability in  $\mathcal{HMSL}(\ast)$  implies derivability in  $\mathcal{HMSL}(\ast, \diamond)$ .

**Lemma 18.** *Let  $\phi$  be a size formula.*

- (I) *There is a size formula  $\phi'$  in conjunctive normal form (CNF) where the literals are size literals, such that  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$  and each conjunct of  $\phi'$  contains at most two size literals, and they are of distinct polarity.*
- (II) *There is a size formula  $\phi'$  in disjunctive normal form (DNF) where the literals are size literals, such that  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$  and each disjunct of  $\phi'$  contains at most two size literals, and they are of distinct polarity.*

*Proof.* Let  $\phi$  be a size formula. We prove (I), the proof for (II) being analogous. By propositional reasoning in  $\mathcal{HMSL}(\ast)$ , there is  $\phi'$  in conjunctive normal form (CNF) such that  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$  and  $\phi'$  is a conjunction of disjunctions of size literals. Suppose that a conjunct of  $\phi'$  does not satisfy the constraint on the number of size literals or on the polarity.

- Suppose there is a finite set  $I \subseteq \mathbb{N}$  such that  $\text{card}(I) \geq 2$  and  $\bigvee_{\beta \in I} (\text{size} \geq \beta)$  is a conjunct of  $\phi'$ . Let  $\beta_{\min} = \min(I)$ . The case when some literal  $\text{size} \geq \beta$  occurs more than twice can be treated by removing the additional occurrences by using propositional reasoning. By using the axiom ( $\mathbf{S}_2^c$ ) and propositional reasoning, one can show that  $\vdash_{\mathcal{HMSL}(\ast)} \bigvee_{\beta \in I} (\text{size} \geq \beta) \Leftrightarrow \text{size} \geq \beta_{\min}$  and therefore,  $\bigvee_{\beta \in I} (\text{size} \geq \beta)$  can be replaced by  $\text{size} \geq \beta_{\min}$  in  $\phi'$  while preserving  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$ .
- Suppose there is a finite set  $I \subseteq \mathbb{N}$  such that  $\text{card}(I) \geq 2$  and  $\bigvee_{\beta \in I} \neg(\text{size} \geq \beta)$  is a conjunct of  $\phi'$ . Let  $\beta_{\max} = \max(I)$ . By using the axiom ( $\mathbf{S}_5^*$ ) and propositional reasoning, one can show that  $\vdash_{\mathcal{HMSL}(\ast)} \bigvee_{\beta \in I} \neg(\text{size} \geq \beta) \Leftrightarrow \neg(\text{size} \geq \beta_{\max})$  and therefore,  $\bigvee_{\beta \in I} \neg(\text{size} \geq \beta)$  can be replaced by  $\neg(\text{size} \geq \beta_{\max})$  in  $\phi'$  while preserving  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$ .
- Finally, suppose there are finite sets  $I, I' \subseteq \mathbb{N}$  such that  $\text{card}(I) \times \text{card}(I') > 1$ ,  $\psi = \bigvee_{\beta \in I} (\text{size} \geq \beta) \vee \bigvee_{\beta \in I'} \neg(\text{size} \geq \beta)$  is a conjunct of  $\phi'$ . Let  $\beta_{\min} = \min(I)$  and  $\beta_{\max} = \max(I')$ . By using the axiom ( $\mathbf{S}_2^c$ ) and propositional reasoning, one can show that

$$\vdash_{\mathcal{HMSL}(\ast)} \psi \Leftrightarrow \text{size} \geq \beta_{\min} \vee \neg(\text{size} \geq \beta_{\max}),$$

and therefore,  $\psi$  can be replaced by  $\text{size} \geq \beta_{\min} \vee \neg(\text{size} \geq \beta_{\max})$ .

Consequently, there is a size formula  $\phi'$  in CNF when the literals are size literals, such that  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$  and each conjunct of  $\phi'$  contains at most two size literals, and there are of distinct polarity.  $\square$

**Lemma 19.** *Given  $\phi$  in  $MSL(\ast)$ ,  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \psi$  for some size formula  $\psi$ .*

*Proof.* The essential ingredient of the proof is to show that given two size formulae  $\phi_0, \phi_1$ , there is a size formula  $\psi$  such that  $\vdash_{\mathcal{HMSL}(\ast)} (\phi_0 \ast \phi_1) \Leftrightarrow \psi$ . Then, using Lemma 21 for  $\mathcal{HMSL}(\ast)$  (by using the  $\ast$ -introduction rule) and applying recursively this transformation leads to the desired property. For the base cases, we take advantage of the fact that  $\vdash_{\mathcal{HMSL}(\ast)} \text{emp} \Leftrightarrow \neg(\text{size} \geq 1)$  and  $\vdash_{\mathcal{HMSL}(\ast)} \top \Leftrightarrow \text{size} \geq 0$  (actually  $\text{size} \geq 0$  is equal to  $\top$  by definition).

By Lemma 18(II), there are size formulae  $\phi'_0$  and  $\phi'_1$  in DNF when the literals are size literals, such that for each  $i \in \{0, 1\}$ ,  $\vdash_{\mathcal{HMSL}(\ast)} \phi_i \Leftrightarrow \phi'_i$  and each disjunct of  $\phi'_i$  contains at most two size literals, and they are of distinct polarity. Say,  $\phi'_0 = \psi_0^1 \vee \dots \vee \psi_0^{N_0}$  and  $\phi'_1 = \psi_1^1 \vee \dots \vee \psi_1^{N_1}$ . By propositional reasoning and by using the axiom (**\*DISTR**), we can show that

$$\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \bigvee_{i \in [1, N_0], j \in [1, N_1]} \psi_0^i \ast \psi_1^j.$$

In the case  $\psi_0^i = \text{size} \geq \beta \wedge \neg(\text{size} \geq \beta')$  with  $\beta' \leq \beta$ , then  $\vdash_{\mathcal{HMSL}(\ast)} \neg(\psi_0^i \ast \psi_1^j)$  by the axiom ( **$\perp$** ). Indeed,  $\vdash_{\mathcal{H}_c} \neg\psi_0^i$  by completeness of  $\mathcal{H}_c$  and therefore  $\vdash_{\mathcal{HMSL}(\ast)} \psi_0^i \Leftrightarrow \perp$ . Similarly, if  $\psi_0^i = \neg(\text{size} \geq 1)$ , then  $\vdash_{\mathcal{HMSL}(\ast)} (\psi_0^i \ast \psi_1^j) \Leftrightarrow \psi_1^j$  by using the axiom (**S<sub>4</sub><sup>\*</sup>**). As  $\text{size} \geq 0 = \top$ , without loss of generality, we can assume that the  $\psi_0^i$ 's and the  $\psi_1^j$ 's always contain a positive size literal (see the axiom (**S<sub>1</sub><sup>\*</sup>**) and the adequate variant of Lemma 21). Consequently, by using the axiom (**S<sub>5</sub><sup>\*</sup>**), **L1** and **L4** (see Lemma 10),  $\vdash_{\mathcal{HMSL}(\ast)} \psi_0^i \ast \psi_1^j \Leftrightarrow \psi_{i,j}$  for some size formula  $\psi_{i,j}$ . Notice that, indeed, **L1** and **L4** are provable in  $\mathcal{HMSL}(\ast)$  (see the proof of Lemma 10, where only the axioms from this system are used for their proofs). The use of these axioms and lemmata may require first the use of the axiom (**COM**). Hence, there is a size formula  $\psi$  such that  $\vdash_{\mathcal{HMSL}(\ast)} (\phi_0 \ast \phi_1) \Leftrightarrow \psi$ .  $\square$

Proving completeness is now by an easy verification.

**Lemma 20.**  *$\mathcal{HMSL}(\ast)$  is sound and complete for  $MSL(\ast)$ .*

*Proof.* (sketch) Soundness is from Lemma 17. It remains to establish completeness. Let  $\phi$  be a formula that is valid for  $MSL(\ast)$ . First, notice that the following property holds: if  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$ , then  $\vdash_{\mathcal{HMSL}(\ast)} \psi[\phi]_\rho \Leftrightarrow \psi[\phi']_\rho$ , where the formula  $\psi[\phi]_\rho$  stands for the formula obtained from  $\psi$  by replacing the formula at the occurrence  $\rho$  by the formula  $\phi$ .

By Lemma 19, it is easy to show that there is a size formula  $\phi'$  in CNF such that  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$  in  $\mathcal{HMSL}(\ast)$  and each conjunct of  $\phi'$  contains at most 2 size literals, and they are of distinct polarity. By the validity of the axioms and inference rules (Lemma 17),  $\phi'$  is also  $MSL(\ast)$  valid and therefore each conjunct is valid. If a conjunct is of the form  $\text{size} \geq \beta$ , then  $\beta = 0$  as  $\text{size} \geq \beta$  should be valid. As  $\text{size} \geq 0 = \top$ , we have  $\vdash_{\mathcal{HMSL}(\ast)} \text{size} \geq 0$ . No conjunct can be of the form  $\neg(\text{size} \geq \beta)$  as no formula of the form  $\neg(\text{size} \geq \beta)$  is valid. If a conjunct is of the form  $\text{size} \geq \beta \vee \neg(\text{size} \geq \beta')$ , then  $\beta' \geq \beta$  as  $\text{size} \geq \beta \vee \neg(\text{size} \geq \beta')$  is required to be valid. By propositional reasoning and by using  $(\beta' - \beta)$  times the axiom (**S<sub>2</sub><sup>\*</sup>**), we can conclude that  $\vdash_{\mathcal{HMSL}(\ast)} (\text{size} \geq \beta') \Rightarrow (\text{size} \geq \beta)$  and therefore  $\vdash_{\mathcal{HMSL}(\ast)} \text{size} \geq \beta \vee \neg(\text{size} \geq \beta')$  by propositional reasoning. Hence,  $\vdash_{\mathcal{HMSL}(\ast)} \phi'$ , and since  $\vdash_{\mathcal{HMSL}(\ast)} \phi \Leftrightarrow \phi'$ , by propositional reasoning, we also get  $\vdash_{\mathcal{HMSL}(\ast)} \phi$ .  $\square$

### 4.3 Putting all together: axiomatising $MSL(\ast, \langle \neq \rangle)$

It is now time to define the Hilbert-style proof system  $\mathcal{HMSL}(\ast, \langle \neq \rangle)$  obtained from the calculus containing the axioms and rules from  $\mathcal{HMSL}(\ast)$  and  $\mathcal{HMSL}(\langle \neq \rangle)$ . However, we need to introduce two more axioms, stating that pure separation formulae can be separated from pure modal formulae. Notice that this property has some similarities with the separation theorem for Past LTL from [34].

Separation axioms

**( $\langle \neq \rangle$ SEP)**  $\langle \neq \rangle(\phi \wedge \psi) \Leftrightarrow (\langle \neq \rangle\phi) \wedge \psi$  where  $\psi$  is a pure separation formula

**(\*SEP)**  $\phi * (\phi' \wedge \psi) \Leftrightarrow (\phi * \phi') \wedge \psi$  where  $\psi$  is a pure modal formula

First, we establish a preliminary result useful in the forthcoming proofs but of rather standard nature. The formula  $\psi[\phi]_\rho$  below stands for the formula obtained from  $\psi$  by replacing the formula at the occurrence  $\rho$  by the formula  $\phi$ .

**Lemma 21** (Replacement of equivalent formulae). *Let  $\phi, \phi', \psi$  be formulae in  $MSL(*, \langle \neq \rangle)$  such that  $\vdash_{\mathcal{HMSL}(*, \langle \neq \rangle)} \phi \Leftrightarrow \phi'$ . Then  $\vdash_{\mathcal{HMSL}(*, \langle \neq \rangle)} \psi[\phi]_\rho \Leftrightarrow \psi[\phi']_\rho$ .*

*Proof.* The following rules can be shown admissible in  $\mathcal{HMSL}(*, \langle \neq \rangle)$ :

$$\frac{\phi \Leftrightarrow \phi'}{\neg\phi \Leftrightarrow \neg\phi'} \quad \frac{\phi \Leftrightarrow \phi'}{\phi \vee \psi \Leftrightarrow \phi' \vee \psi} \quad \frac{\phi \Leftrightarrow \phi'}{\phi \wedge \psi \Leftrightarrow \phi' \wedge \psi}$$

Admissibility of such rules is the direct consequence of the axioms and the modus ponens rule for the propositional calculus. Thanks to **\*-introduction rule**, the rule below is also admissible:

$$\frac{\phi \Leftrightarrow \phi'}{\phi * \psi \Leftrightarrow \phi' * \psi}$$

Finally, the rule below is admissible by using the axiom **(K)** and the necessitation rule:

$$\frac{\phi \Leftrightarrow \phi'}{[\neq]\phi \Leftrightarrow [\neq]\phi'}$$

Consequently, by structural induction on  $\psi$ , one can conclude that  $\vdash_{\mathcal{HMSL}(*, \langle \neq \rangle)} \phi \Leftrightarrow \phi'$  implies  $\vdash_{\mathcal{HMSL}(*, \langle \neq \rangle)} \psi[\phi]_\rho \Leftrightarrow \psi[\phi']_\rho$ .  $\square$

**Lemma 22.** *The axioms and rules in  $\mathcal{HMSL}(*, \langle \neq \rangle)$  are valid for  $MSL(*, \langle \neq \rangle)$ .*

*Proof.* Correctness of the axioms and rules from  $\mathcal{HMSL}(*)$  and  $\mathcal{HMSL}(\langle \neq \rangle)$  can be established along the lines of the proofs for Lemma 15 and Lemma 20. It remains to show the validity of the axioms **( $\langle \neq \rangle$ SEP)** and **(\*SEP)**.

**( $\langle \neq \rangle$ SEP)** Let  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{W} \rangle$  and  $l \in \mathbb{N}$  be such that  $\mathfrak{M}, l \models \langle \neq \rangle(\phi \wedge \psi)$ . There is  $l' \neq l$  such that  $\mathfrak{M}, l' \models \phi \wedge \psi$ . As  $\psi$  is a pure separation formula, the evaluation of  $\psi$  on  $\mathfrak{M}, l'$  does not require the use of  $l'$  (and  $\mathfrak{W}$ ) and therefore  $\mathfrak{M}, l \models \psi$  too. Consequently,  $\mathfrak{M}, l \models (\langle \neq \rangle\phi) \wedge \psi$ . Conversely, suppose that  $\mathfrak{M}, l \models (\langle \neq \rangle\phi) \wedge \psi$ . There is  $l' \neq l$  such that  $\mathfrak{M}, l' \models \phi$ . As  $\psi$  is a pure separation formula, the evaluation of  $\psi$  on  $\mathfrak{M}, l$  does not require the use of  $l$  and therefore  $\mathfrak{M}, l' \models \psi$  too. Consequently,  $\mathfrak{M}, l \models \langle \neq \rangle(\phi \wedge \psi)$ .

**(\*SEP)** Let  $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{W} \rangle$  and  $l \in \mathbb{N}$  be such that  $\mathfrak{M}, l \models \phi * (\phi' \wedge \psi)$ . There are  $\mathfrak{R}_1, \mathfrak{R}_2$  such that  $\mathfrak{R} = \mathfrak{R}_1 \uplus \mathfrak{R}_2$ ,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \phi$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{W} \rangle, l \models \phi' \wedge \psi$ . As  $\psi$  is a pure modal formula (with unique modality  $\langle \neq \rangle$ ), the evaluation of  $\psi$  on  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{W} \rangle, l$  does not require the use of  $\mathfrak{R}_2$  and therefore  $\mathfrak{M}, l \models \psi$ . Consequently,  $\mathfrak{M}, l \models (\phi * \phi') \wedge \psi$ . Conversely, suppose that  $\mathfrak{M}, l \models (\phi * \phi') \wedge \psi$ . There are  $\mathfrak{R}_1, \mathfrak{R}_2$  such that  $\mathfrak{R} = \mathfrak{R}_1 \uplus \mathfrak{R}_2$ ,  $\langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{W} \rangle, l \models \phi$  and  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{W} \rangle, l \models \phi'$ . As  $\psi$  is a pure modal formula, the evaluation of  $\psi$  on  $\langle \mathbb{N}, \mathfrak{R}, \mathfrak{W} \rangle, l$  does not require the use of  $\mathfrak{R}$  and therefore  $\langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{W} \rangle, l \models \psi$ . Consequently,  $\mathfrak{M}, l \models \phi * (\phi' \wedge \psi)$ .  $\square$

Completeness of  $\mathcal{HMSL}(*, \langle \neq \rangle)$  takes advantage of the respective completeness of  $\mathcal{HMSL}(\langle \neq \rangle)$  and  $\mathcal{HMSL}(*)$ , and the fact that for all pure modal (resp. separation) formulae  $\phi_M$  (resp.  $\phi_S$ ),  $\phi_M \vee \phi_S$  is valid iff  $\phi_M$  is valid or  $\phi_S$  is valid.

**Theorem 23** (Adequacy of  $\mathcal{HMSL}(*, \langle \neq \rangle)$ ). *The axiom system  $\mathcal{HMSL}(*, \langle \neq \rangle)$  is sound and complete for  $MSL(*, \langle \neq \rangle)$ .*

*Proof.* Soundness is from Lemma 22. It remains to establish completeness. Let  $\phi$  be a formula that is valid for  $MSL(*, \langle \neq \rangle)$ .

By using the axioms **( $\langle \neq \rangle$ SEP)** and **(\*SEP)**, there is a formula  $\phi'$  such that  $\vdash_{\mathcal{HMSL}(*, \langle \neq \rangle)} \phi \Leftrightarrow \phi'$  and  $\phi'$  belongs to  $\text{Bool}(MSL(*)) \cup MSL(\langle \neq \rangle)$ , the set of Boolean combinations of formulae from

$\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle)$ . Here, we use intensively Lemma 21 and the fact that each “application” of  $(\langle \neq \rangle\text{SEP})$  or  $(*\text{SEP})$  strictly decreases the number of alternations between the modal language and the separation language. The core argument relies on the two following simpler properties.

1. For every formula  $\psi \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ , there is a formula  $\psi' \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$  such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \langle \neq \rangle \psi \Leftrightarrow \psi'$ .
2. For all formulae  $\psi_0, \psi_1 \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ , there is a formula  $\psi' \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$  such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} (\psi_0 * \psi_1) \Leftrightarrow \psi'$ .

Let us start by showing (1.). By propositional reasoning in  $\mathcal{H}\text{MSL}(*, \langle \neq \rangle)$ , there is  $\gamma$  in disjunctive normal form (DNF) such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \psi \Leftrightarrow \gamma$  and  $\gamma$  is a disjunction of conjunctions of the form  $\phi_M \wedge \phi_S$  where  $\phi_M$  is a pure modal formula and  $\phi_S$  is a pure separation formula. By Lemma 21, we have  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \langle \neq \rangle \psi \Leftrightarrow \langle \neq \rangle \gamma$ . As the disjunction distributes over  $\langle \neq \rangle$  ( $\mathcal{H}\text{MSL}(*, \langle \neq \rangle)$  inherits this property from  $\mathcal{H}\text{MSL}(\langle \neq \rangle)$ ), we get that

$$\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \langle \neq \rangle \psi \Leftrightarrow \bigvee_{\phi_M \wedge \phi_S} \langle \neq \rangle (\phi_M \wedge \phi_S).$$

By application of  $(\langle \neq \rangle\text{SEP})$  and by Lemma 21, we get that

$$\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \langle \neq \rangle \psi \Leftrightarrow \bigvee_{\phi_M \wedge \phi_S} (\langle \neq \rangle \phi_M) \wedge \phi_S,$$

and therefore there is  $\psi' \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$  such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \langle \neq \rangle \psi \Leftrightarrow \psi'$ . Now let us show (2.). By propositional reasoning in  $\mathcal{H}\text{MSL}(*, \langle \neq \rangle)$ , for each  $i \in \{0, 1\}$ , there is  $\gamma_i$  in disjunctive normal form (DNF) such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \psi_i \Leftrightarrow \gamma_i$  and  $\gamma_i$  is a disjunction of conjunctions of the form  $\phi_M \wedge \phi_S$  where  $\phi_M$  is a pure modal formula and  $\phi_S$  is a pure separation formula. By Lemma 21, we have  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \psi_0 * \psi_1 \Leftrightarrow \gamma_0 * \gamma_1$ . As the disjunction distributes over  $*$  ( $\mathcal{H}\text{MSL}(*, \langle \neq \rangle)$  inherits this property from  $\mathcal{H}\text{MSL}(*)$ ), we get that

$$\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \psi_0 * \psi_1 \Leftrightarrow \bigvee_{\phi_M \wedge \phi_S, \phi'_M \wedge \phi'_S} (\phi_M \wedge \phi_S) * (\phi'_M \wedge \phi'_S).$$

By two applications of  $(*\text{SEP})$  per disjunct and by Lemma 21, we get that

$$\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \langle \neq \rangle \psi \Leftrightarrow \bigvee_{\phi_M \wedge \phi_S, \phi'_M \wedge \phi'_S} (\phi_S * \phi'_S) \wedge \phi_M \wedge \phi'_M,$$

and therefore there is  $\psi' \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$  such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} (\psi_0 * \psi_1) \Leftrightarrow \psi'$ .

So, (1.) and (2.) hold true and now let us briefly explain why for every  $\text{MSL}(*, \langle \neq \rangle)$  formula  $\phi$ , there is a formula  $\phi'$  such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \phi \Leftrightarrow \phi'$  and  $\phi'$  belongs to  $\text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ . Given  $\psi$  in  $\text{MSL}(*, \langle \neq \rangle)$ , let  $\mathbf{c}(\psi)$  be the number of subformulae of  $\psi$  that do not belong to  $\text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ . Note that when  $\psi$  is in  $\text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ , we have  $\mathbf{c}(\psi) = 0$ . Suppose that  $\phi$  does not belong to  $\text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ . So, there is a subformula  $\langle \neq \rangle \psi$  of  $\phi$  with  $\psi \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$  or there is a subformula  $\psi_0 * \psi_1$  with  $\psi_0, \psi_1 \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ . Let us treat the first case (the second one being similar). By (1.), there is a formula  $\psi' \in \text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$  such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \langle \neq \rangle \psi \Leftrightarrow \psi'$ . Consequently, by Lemma 21,  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \phi \Leftrightarrow \phi[\langle \neq \rangle \psi \leftarrow \psi']$  where  $\phi[\langle \neq \rangle \psi \leftarrow \psi']$  is equal to  $\phi$  in which *all* the occurrences of  $\langle \neq \rangle \psi$  are replaced by  $\psi'$ . Note that  $\mathbf{c}(\phi) > \mathbf{c}(\phi[\langle \neq \rangle \psi \leftarrow \psi'])$ . It is here important to replace all the occurrences of  $\langle \neq \rangle \psi$  to have a strict decrease of  $\mathbf{c}$ . By repeating this process a finite amount of times, there is a formula  $\phi'$  such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \phi \Leftrightarrow \phi'$  and  $\phi'$  belongs to  $\text{Bool}(\text{MSL}(*) \cup \text{MSL}(\langle \neq \rangle))$ .

By the validity of the axioms and inference rules (Lemma 22), we have that  $\phi'$  is  $\text{MSL}(*, \langle \neq \rangle)$  valid too. By propositional reasoning in  $\mathcal{H}\text{MSL}(*, \langle \neq \rangle)$ , there is  $\phi''$  in conjunctive normal form (CNF) such that  $\vdash_{\mathcal{H}\text{MSL}(*, \langle \neq \rangle)} \phi' \Leftrightarrow \phi''$  and  $\phi''$  is a conjunction of disjunctions of the form  $\phi_M \vee \phi_S$  where  $\phi_M$  is a pure modal formula and  $\phi_S$  is a pure separation formula. Again, by the validity of the axioms and inference rules, each disjunction  $\phi_M \vee \phi_S$  is valid in  $\text{MSL}(*, \langle \neq \rangle)$ .

One can easily show that  $\phi_M \vee \phi_S$  is valid if and only if either  $\phi_M$  is valid for  $\text{MSL}(\langle \neq \rangle)$  or  $\phi_S$  is valid for  $\text{MSL}(*)$ . The right-to-left direction is obvious. For the other direction, suppose that neither  $\phi_M$  nor  $\phi_S$  is valid.

- There exist a model  $\mathfrak{M}_M = \langle \mathbb{N}, \mathfrak{R}_M, \mathfrak{V}_M \rangle$  and  $l_M \in \mathbb{N}$  such that  $\mathfrak{M}_M, l_M \not\models \phi_M$ . As the evaluation of  $\phi_M$  on  $\mathfrak{M}$ , does not require the use of  $\mathfrak{R}_M$ , for all finite and (weakly) functional  $\mathfrak{R}'$ , we have  $\langle \mathbb{N}, \mathfrak{R}', \mathfrak{V}_M \rangle, l_M \not\models \phi_M$ .
- There exist a model  $\mathfrak{M}_S = \langle \mathbb{N}, \mathfrak{R}_S, \mathfrak{V}_S \rangle$  and  $l_S \in \mathbb{N}$  such that  $\mathfrak{M}_S, l_S \not\models \phi_S$ . As the evaluation of  $\phi_S$  on  $\mathfrak{M}_S$ , does not require the use of  $\mathfrak{V}_S$  and  $l_S$ , for all valuations  $\mathfrak{V}_S$  and locations  $l'$ , we have  $\langle \mathbb{N}, \mathfrak{R}_S, \mathfrak{V}' \rangle, l' \not\models \phi_S$ .

Consequently,  $\langle \mathbb{N}, \mathfrak{R}_S, \mathfrak{V}_M \rangle, l_M \models \neg\phi_M \wedge \neg\phi_S$  and therefore  $\phi_M \vee \phi_S$  is not valid. So  $\phi_M \vee \phi_S$  is valid implies  $\phi_M$  is valid or  $\phi_S$  is valid.

By completeness of  $\mathcal{HMSL}(\langle \neq \rangle)$  and  $\mathcal{HMSL}(\ast)$ , we get that  $\phi_M \vee \phi_S$  is valid in  $\text{MSL}(\ast, \langle \neq \rangle)$  iff either  $\vdash_{\mathcal{HMSL}(\langle \neq \rangle)} \phi_M$  or  $\vdash_{\mathcal{HMSL}(\ast)} \phi_S$ . As the rule

$$\frac{\gamma}{\gamma \vee \gamma'}$$

is admissible thanks to the axiom schemas from propositional calculus and to the modus ponens rule, we get that  $\vdash_{\mathcal{HMSL}(\langle \neq \rangle)} \phi_M$  implies  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi_M \vee \phi_S$  and  $\vdash_{\mathcal{HMSL}(\ast)} \phi_S$  implies  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi_M \vee \phi_S$ . As  $\phi_M \vee \phi_S$  is valid, we conclude that  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi_M \vee \phi_S$ . Consequently, for each disjunct  $\phi_M \vee \phi_S$  of  $\phi''$ , we have  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi_M \vee \phi_S$  and therefore by propositional reasoning, we get that  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi''$  in  $\mathcal{HMSL}(\ast, \langle \neq \rangle)$ . As  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi \Leftrightarrow \phi'$  and  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi' \Leftrightarrow \phi''$ , by propositional reasoning, we get that  $\vdash_{\mathcal{HMSL}(\ast, \langle \neq \rangle)} \phi$  and therefore  $\mathcal{HMSL}(\ast, \langle \neq \rangle)$  is complete.  $\square$

By using the same argument as in Thm. 14 we can show the following.

**Corollary 24.**  *$\text{MSL}(\ast, \langle \neq \rangle)$  is not compact; therefore,  $\mathcal{HMSL}(\ast, \langle \neq \rangle)$  is not strongly complete.*

## 5 Concluding remarks

We provided a Hilbert-style axiomatisation for the modal separation logics  $\text{MSL}(\ast, \diamond)$  and  $\text{MSL}(\ast, \langle \neq \rangle)$ , despite the well-known difficulties to axiomatise logics equipped with operators that update the models in the evaluation process. Such operators are ubiquitous in theoretical computer science and in knowledge representation areas, and we hope that our calculi shed some new light on their expressive power. For the axiomatisation of  $\text{MSL}(\ast, \diamond)$ , we had to identify the core properties that can be expressed in the logic, partially following the semantical analysis from [24]. We also had to express them in the language with the so-called core formulae. Implicitly, the axiomatisation is divided into two parts: axioms and rules to transform any formula of  $\text{MSL}(\ast, \diamond)$  into a Boolean combination of core formulae and the axiomatisation of these Boolean combinations. For the axiomatisation of  $\text{MSL}(\ast, \langle \neq \rangle)$ , we use a similar approach, except that we had to adapt the axiomatisation of the logic of elsewhere from [50] to infinite models and to implement syntactically a separation principle satisfied by the logic  $\text{MSL}(\ast, \langle \neq \rangle)$ . It is worth noting that the completeness of  $\mathcal{HMSL}(\ast, \diamond)$  and  $\mathcal{HMSL}(\ast, \langle \neq \rangle)$  does not imply their strong completeness, as  $\text{MSL}(\ast)$  is not compact. Moreover, the same argument can be used for other finitary proof systems.

As part of future work, we aim at Hilbert-style axiomatisations for separation logics having a notion of core formulae (see e.g. [32, 26]), or for very expressive modal separation logics such as  $\text{MSL}(\ast, \langle \neq \rangle, \diamond)$ , or  $\text{MSL}(\ast, \diamond)$  over different class of Kripke models such as tree-models.

Additionally, the expressivity characterisation provided by core formulae appears to be handy not only as the basic ingredient for the axiomatisations, but also for studying other problems, such as the implementation of proof methods, or the analysis of meta-theoretical properties of the logics. Finally, the design of proof systems better suited to automated reasoning remains open as well as the design of real-life applications taking advantage of  $\text{MSL}(\ast, \diamond)$  or  $\text{MSL}(\ast, \langle \neq \rangle)$ . Similarly, it would be interesting to investigate how to use the insights provided by the Hilbert-style axiomatisations introduced in this paper to design sequent-style proof systems, aiming for good computational properties.

**Acknowledgements.** First, we would like to thank the anonymous referees for their suggestions and comments that helped us to improve the quality of the document. This work was partially supported by ANPCyT-PICTs-2017-1130 and 2016-0215, MinCyT Córdoba, SeCyT-UNC, the Laboratoire International Associé SINFIN and the Centre National de la Recherche Scientifique (CNRS).

## References

- [1] G. Anderson and D. Pym. A Substructural Modal Logic of Utility. *Journal of Logic and Computation*, 27(5):1421–1464, 2017.
- [2] C. Areces and R. Fervari. Hilbert-style axiomatization for hybrid XPath with data. In *JELIA'16*, volume 10021 of *LNCS*, pages 34–48. Springer, 2016.
- [3] C. Areces, R. Fervari, and G. Hoffmann. Tableaux for relation-changing modal logics. In *FroCos'13*, volume 8152 of *LNCS*, pages 263–278, 2013.
- [4] C. Areces, R. Fervari, and G. Hoffmann. Relation-changing modal operators. *Logic Journal of the IGPL*, 23(4):601–627, 2015.
- [5] G. Aucher, J. van Benthem, and D. Grossi. Modal logics of sabotage revisited. *Journal of Logic and Computation*, 28(2):269–303, 2018.
- [6] Ph. Balbiani and T. Tinchev. Unification in modal logic  $\text{Alt}_1$ . In *AiML'16*, pages 117–134. College Publications, 2016.
- [7] J. Berdine, C. Calcagno, and P. O’Hearn. A decidable fragment of separation logic. In *FST&TCS'04*, volume 3328 of *LNCS*, pages 97–109. Springer, 2004.
- [8] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. Cambridge University Press, 2001.
- [9] P. Blackburn, J. van Benthem, and F. Wolter, editors. *Handbook of Modal Logic*. Elsevier, 2006.
- [10] J. Boudou. Decidable logics with associative binary modalities. In *CSL'17*, volume 82 of *LIPICs*, pages 1–15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.
- [11] R. Brochenin, S. Demri, and E. Lozes. Reasoning about sequences of memory states. *Annals of Pure and Applied Logic*, 161(3):305–323, 2009.
- [12] J. Brotherston and M. Kanovich. Undecidability of propositional separation logic and its neighbours. In *LiCS'10*, pages 130–139. IEEE, 2010.
- [13] J. Brotherston and J. Villard. Parametric completeness for separation theories. In *POPL'14*, pages 453–464. ACM, 2014.
- [14] D. Calvanese, T. Kotek, M. Simkus, H. Veith, and F. Zuleger. Shape and content - A database-theoretic perspective on the analysis of data structures. In *IFM'14*, volume 8739 of *LNCS*, pages 3–17. Springer, 2014.
- [15] J.-R. Courtault. *Logiques de ressources dynamiques: modèles, propriétés et preuves*. PhD thesis, Université de Lorraine, 2015.
- [16] J.-R. Courtault and D. Galmiche. A modal BI logic for dynamic resource properties. In *LFCS'13*, volume 7734 of *LNCS*, pages 134–148. Springer, 2013.
- [17] J.-R. Courtault and D. Galmiche. A modal separation logic for resource dynamics. *Journal of Logic and Computation*, 28(4):733–778, 2018.
- [18] J.-R. Courtault, D. Galmiche, and D. J. Pym. A logic of separating modalities. *Theoretical Computer Science*, 637:30–58, 2016.



- [19] J.-R. Courtault, H. van Ditmarsch, and D. Galmiche. An epistemic separation logic. In *WoLLIC'15*, volume 9160 of *LNCS*, pages 156–173. Springer, 2015.
- [20] J.-R. Courtault, H. van Ditmarsch, and D. Galmiche. A public announcement separation logic. *Mathematical Structures in Computer Science*, 29(6):828–871, 2019.
- [21] A. Dawar, Ph. Gardner, and G. Ghelli. Expressiveness and complexity of graph logic. *Information and Computation*, 205(3):263–310, 2007.
- [22] S. Demri. A simple tableau system for the logic of elsewhere. In *TABLEAUX'96*, volume 1071 of *LNAI*, pages 177–192. Springer, 1996.
- [23] S. Demri and M. Deters. Two-variable separation logic and its inner circle. *ACM Transactions on Computational Logic*, 2(16), 2015.
- [24] S. Demri and R. Fervari. The power of modal separation logics. *Journal of Logic and Computation*, 29(8):1139–1184, 2019.
- [25] S. Demri, R. Fervari, and A. Mansutti. Axiomatising logics with separating conjunctions and modalities. In *JELIA'19*, volume 11468 of *LNAI*, pages 692–708. Springer, 2019.
- [26] S. Demri, É. Lozes, and A. Mansutti. The effects of adding reachability predicates in propositional separation logic. In *FoSSaCS*, volume 10803 of *LNCS*, pages 476–493. Springer, 2018.
- [27] S. Demri, É. Lozes, and A. Mansutti. A complete axiomatisation for quantifier-free separation logic. *CoRR*, abs/2006.05156, 2020.
- [28] S. Demri, É. Lozes, and A. Mansutti. Internal calculi for separation logics. In *CSL'20*, Leibniz International Proceedings in Informatics, pages 19:1–19:18. Leibniz-Zentrum für Informatik, 2020.
- [29] D. Distefano, J.-P. Katoen, and A. Rensink. Who is pointing when to whom? On the automated verification of linked list structures. In *FST&TCS'04*, volume 3328 of *LNCS*, pages 250–262. Springer, 2004.
- [30] A. Doumane. Constructive completeness for the linear-time  $\mu$ -calculus. In *LiCS'17*, pages 1–12. IEEE Computer Society, 2017.
- [31] H.D. Ebbinghaus and J. Flum. *Finite Model Theory*. Perspectives in Mathematical Logic. Springer Berlin Heidelberg, 1999.
- [32] M. Echenim, R. Iosif, and N. Peltier. The Bernays-Schönfinkel-Ramsey class of separation logic on arbitrary domains. In *FoSSaCS'19*, volume 11425 of *LNCS*, pages 242–259. Springer, 2019.
- [33] R. Fervari and F. R. Velázquez-Quesada. Introspection as an action in relational models. *Journal of Logical and Algebraic Methods in Programming*, 108:1–23, 2019.
- [34] D. Gabbay. The declarative past and imperative future. In *Temporal Logic in Specification*, *Altrincham, UK*, volume 398 of *LNCS*, pages 409–448. Springer, 1987.
- [35] D. Galmiche and D. Larchey-Wending. Expressivity properties of boolean BI through relational models. In *FST&TCS'06*, volume 4337 of *LNCS*, pages 358–369. Springer, 2006.
- [36] D. Galmiche, D. Méry, and D. Pym. The semantics of BI and resource tableaux. *Mathematical Structures in Computer Science*, 15(6):1033–1088, 2005.
- [37] N. Gierasimczuk, L. Kurzen, and F.R. Velázquez-Quesada. Learning and teaching as a game: A sabotage approach. In *LORI'09*, volume 5834 of *LNCS*, pages 119–132. Springer, 2009.

- [38] A. Herzig. A simple separation logic. In *WoLLIC'13*, volume 8071 of *LNCS*, pages 168–178. Springer, 2013.
- [39] C.A.R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, 1969.
- [40] Z. Hou, R. Clouston, R. Goré, and A. Tiu. Modular labelled sequent calculi for abstract separation logics. *ACM Transactions on Computational Logic*, 19(2):13:1–13:35, 2018.
- [41] X. Lu, C. Tian, and Z. Duan. Temporalising separation logic for planning with search control knowledge. In *IJCAI'17*, pages 1167–1173, 2017.
- [42] A. Mansutti. An Auxiliary Logic on Trees: on the Tower-Hardness of Logics Featuring Reachability and Submodel Reasoning. In *FoSSaCS'20*, volume 12077 of *LNCS*, pages 462–481. Springer, 2020.
- [43] D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic*. Kluwer Academic Publishers, 2002.
- [44] D. Pym, P. O’Hearn, and H. Yang. Possible worlds and resources: the semantics of BI. *Theoretical Computer Science*, 315(1):257–305, 2004.
- [45] D. Pym, J. Spring, and P.W. O’Hearn. Why separation logic works. *Philosophy & Technology*, pages 1–34, 2018.
- [46] D. Pym and Ch. Tofts. A calculus and logic of resources and processes. *Formal Aspects of Computing*, 18(4):495–517, 2006.
- [47] S. Ranise and C. Zarba. A theory of singly-linked lists and its extensible decision procedure. In *SEFM'06*, pages 206–215. IEEE, 2006.
- [48] J.C. Reynolds. Separation logic: a logic for shared mutable data structures. In *LiCS'02*, pages 55–74. IEEE, 2002.
- [49] S. Schmitz. Complexity hierarchies beyond Elementary. *ACM Transactions on Computation Theory*, 8(1):3:1–3:36, 2016.
- [50] K. Segerberg. A note on the logic of elsewhere. *Theoria*, 47:183–187, 1981.
- [51] Y. Shoham and K. Leyton-Brown. *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*. Cambridge University Press, New York, NY, USA, 2008.
- [52] A. Thakur, J. Breck, and T. Reps. Satisfiability modulo abstraction for separation logic with linked lists. In *SPIN'14*, pages 58–67. ACM, 2014.
- [53] J. van Benthem. An essay on sabotage and obstruction. In *Mechanizing Mathematical Reasoning, Essays in Honor of Jörg Siekmann on the Occasion of his 69th Birthday*, pages 268–276. Springer Verlag, 2005.
- [54] J. van Benthem. *Logical Dynamics of Information and Interaction*. Cambridge University Press, 2011.
- [55] H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*, volume 337 of *Synthese Library Series*. Springer, Dordrecht, 2008.
- [56] Y. Wang and Q. Cao. On axiomatizations of public announcement logic. *Synthese*, 190(Supplement-1):103–134, 2013.
- [57] G. Yorsh, A. Rabinovich, M. Sagiv, A. Meyer, and A. Bouajjani. A logic of reachable patterns in linked data-structures. In *FoSSaCS'06*, volume 3921 of *LNCS*, pages 94–110. Springer, 2006.

## Appendix: Two proofs with a strong syntactic flavour

In this appendix we show the derivations in  $\mathcal{H}_c(*)$  of the formulae appearing in Lemmata 10 and 11. In order to help the readability of these lengthy derivations, we introduce the following notation. A line “ $j \mid \gamma \text{ A}, i_1, \dots, i_k$ ” states that  $\gamma$  is a theorem of  $\mathcal{H}_c(*)$  denoted by the index  $j$  and derivable by the axiom or the rule **A**. If **A** is a rule, the indices  $i_1, \dots, i_k < j$  denote the theorems used as premises in order to derive  $\gamma$ . Some easy steps are omitted to shorten the presentation, as for example proofs of the following well-known tautologies and rules of propositional calculus:

$$\begin{array}{lll}
 (\wedge\mathbf{E}) \quad \phi \wedge \psi \Rightarrow \phi & (\wedge\mathbf{V}) \quad \phi \wedge (\psi \vee \gamma) \Rightarrow & (\Rightarrow\mathbf{T}) \quad \frac{\phi \Rightarrow \psi \quad \psi \Rightarrow \gamma}{\phi \Rightarrow \gamma} \\
 (\wedge\mathbf{D}) \quad \phi \Rightarrow \phi \wedge \phi & (\phi \wedge \psi) \vee (\phi \wedge \gamma) & \\
 (\top\mathbf{I}) \quad \phi \Leftrightarrow \phi \wedge \top & (\neg\mathbf{I}) \quad \frac{\phi \Leftrightarrow \phi'}{\neg\phi \Leftrightarrow \neg\phi'} & (\Leftrightarrow\mathbf{T}) \quad \frac{\phi \Leftrightarrow \psi \quad \psi \Leftrightarrow \gamma}{\phi \Leftrightarrow \gamma} \\
 (\top\mathbf{S}) \quad \top \Leftrightarrow \phi \vee \neg\phi & (\wedge\mathbf{I}) \quad \frac{\psi \Rightarrow \gamma}{\phi \wedge \psi \Rightarrow \phi \wedge \gamma} & (\vee\mathbf{L}) \quad \frac{\phi \Rightarrow \gamma \quad \psi \Rightarrow \gamma}{\phi \vee \psi \Rightarrow \gamma} \\
 (\perp\mathbf{I}) \quad \perp \Rightarrow \phi & (\wedge\mathbf{I}_2) \quad \frac{\psi \Leftrightarrow \gamma}{\phi \wedge \psi \Leftrightarrow \phi \wedge \gamma} & (\wedge\mathbf{R}) \quad \frac{\phi \Rightarrow \psi \quad \phi \Rightarrow \gamma}{\phi \Rightarrow \psi \wedge \gamma} \\
 (\wedge\mathbf{C}) \quad \phi \wedge \psi \Rightarrow \psi \wedge \phi & & 
 \end{array}$$

### Proof of Lemma 10

**Proof of R0.** As a consequence of the *\*-introduction rule*, the rule below is also admissible:

$$(\Leftrightarrow*\mathbf{Intro}) \quad \frac{\phi \Leftrightarrow \gamma}{\phi * \psi \Leftrightarrow \gamma * \psi}$$

With this rule, together with **( $\neg\mathbf{I}$ )**, **( $\wedge\mathbf{I}_2$ )** and **(COM)**, one can conclude that  $\vdash_{\mathcal{H}_c(*)} \phi \Leftrightarrow \phi'$  implies  $\vdash_{\mathcal{H}_c(*)} \psi[\phi]_p \Leftrightarrow \psi[\phi']_p$  by structural induction on  $\psi$ .

### Proof of L0.

$$\begin{array}{ll}
 1 & \phi \wedge \phi' \Rightarrow \phi \quad (\wedge\mathbf{E}) \\
 2 & (\phi \wedge \phi') * (\psi \wedge \psi') \Rightarrow \phi * (\psi \wedge \psi') \quad \text{*-introduction rule, 1} \\
 3 & \phi * (\psi \wedge \psi') \Rightarrow (\psi \wedge \psi') * \phi \quad (\mathbf{COM}) \\
 4 & (\phi \wedge \phi') * (\psi \wedge \psi') \Rightarrow (\psi \wedge \psi') * \phi \quad (\Rightarrow\mathbf{T}), 2, 3 \\
 5 & \psi \wedge \psi' \Rightarrow \psi \quad (\wedge\mathbf{E}) \\
 6 & (\psi \wedge \psi') * \phi \Rightarrow \psi * \phi \quad \text{*-introduction rule, 5} \\
 7 & (\phi \wedge \phi') * (\psi \wedge \psi') \Rightarrow \psi * \phi \quad (\Rightarrow\mathbf{T}), 4, 6 \\
 8 & \psi * \phi \Rightarrow \phi * \psi \quad (\mathbf{COM}) \\
 9 & (\phi \wedge \phi') * (\psi \wedge \psi') \Rightarrow \phi * \psi \quad (\Rightarrow\mathbf{T}), 7, 8
 \end{array}$$

**Proof of L1.** If both  $\beta_1$  and  $\beta_2$  are at least 1, then **L1** is trivially proved by definition of  $\mathbf{size} \geq \beta$  together with the axiom **(ASSOC)**. Recall that  $\mathbf{size} \geq 0 = \top$ ,  $\mathbf{size} \geq 1 = \neg\mathbf{emp}$  and  $\mathbf{size} \geq \beta + 1 \stackrel{\text{def}}{=} \neg\mathbf{emp} * \mathbf{size} \geq \beta$  for  $\beta \geq 1$ . Then, whenever  $\beta_1, \beta_2 \geq 1$ , the formula  $\mathbf{size} \geq \beta_1 * \mathbf{size} \geq \beta_2$  is provably equivalent to

$$\underbrace{(\neg\mathbf{emp} * \dots * (\neg\mathbf{emp} * \neg\mathbf{emp}))}_{\beta_1 \text{ occurrences of } \neg\mathbf{emp}} * \underbrace{(\neg\mathbf{emp} * \dots * (\neg\mathbf{emp} * \neg\mathbf{emp}))}_{\beta_2 \text{ occurrences of } \neg\mathbf{emp}}$$

which by the axioms **(ASSOC)** and **(COM)**, is provably equivalent to

$$\underbrace{\neg\mathbf{emp} * \dots * (\neg\mathbf{emp} * \neg\mathbf{emp})}_{\beta_1 + \beta_2 \text{ occurrences of } \neg\mathbf{emp}}$$

which is the definition of  $\mathbf{size} \geq \beta_1 + \beta_2$ .

Suppose now  $\beta_1$  or  $\beta_2$  to be 0. We divide the proof in three cases.

1.  $\beta_1 = 0, \beta_2 \geq 1$ . We first show that  $\mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq \beta_2$ .

1	$\mathbf{size} \geq 0 \Leftrightarrow (\mathbf{size} \geq 1 \vee \neg \mathbf{size} \geq 1)$	(TS)
2	$\mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2 \Leftrightarrow$ $(\mathbf{size} \geq 1 \vee \neg \mathbf{size} \geq 1) * \mathbf{size} \geq \beta_2$	( $\Leftrightarrow$ *Intro), 1
3	$(\mathbf{size} \geq 1 \vee \neg \mathbf{size} \geq 1) * \mathbf{size} \geq \beta_2 \Leftrightarrow$ $(\mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2) \vee (\neg \mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2)$	(*DISTR)
4	$\mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2 \Rightarrow$ $(\mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2) \vee (\neg \mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2)$	( $\Rightarrow$ T), 2, 3
5	$\mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq \beta_2 + 1$	L1, case $\beta_1, \beta_2 \geq 1$
6	$\mathbf{size} \geq \beta_2 + 1 \Rightarrow \mathbf{size} \geq \beta_2$	(S <sub>2</sub> <sup>*</sup> )
7	$\mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq \beta_2$	( $\Rightarrow$ T), 5, 6
8	$\neg \mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2 \Leftrightarrow \mathbf{size} \geq \beta_2 * \neg \mathbf{size} \geq 1$	(COM)
9	$\mathbf{size} \geq \beta_2 * \neg \mathbf{size} \geq 1 \Leftrightarrow \mathbf{size} \geq \beta_2$	(S <sub>4</sub> <sup>*</sup> )
10	$\neg \mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq \beta_2$	( $\Rightarrow$ T), 8, 9
11	$(\mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2) \vee (\neg \mathbf{size} \geq 1 * \mathbf{size} \geq \beta_2) \Rightarrow \mathbf{size} \geq \beta_2$	( $\vee$ L), 7, 10
12	$\mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq \beta_2$	( $\Rightarrow$ T), 4, 11

We now show the converse:  $\vdash_{\mathcal{H}_c(*)} \mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2$ . Then,  $\vdash_{\mathcal{H}_c(*)} \mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2 \Leftrightarrow \mathbf{size} \geq \beta_2$  trivially follows from propositional reasoning.

1	$\mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} = 0 * \mathbf{size} \geq \beta_2$	(S <sub>5</sub> <sup>*</sup> )
2	$\mathbf{size} = 0 \Rightarrow \mathbf{size} \geq 0$	( $\wedge$ E)
3	$\mathbf{size} = 0 * \mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2$	*-introduction rule, 2
4	$\mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2$	( $\Rightarrow$ T), 1, 3

2.  $\beta_1 \geq 1$  and  $\beta_2 = 0$ . Direct from the proof of the previous case and (COM).
3.  $\beta_1 = \beta_2 = 0$ . Directly by propositional reasoning and since  $\mathbf{size} \geq 0 \stackrel{\text{by def}}{\Leftrightarrow} \top$ , we conclude that  $\mathbf{size} \geq 0 * \mathbf{size} \geq 0 \Rightarrow \mathbf{size} \geq 0$  is derivable in  $\mathcal{H}_c(*)$ . For the other direction,  $\vdash_{\mathcal{H}_c(*)} \mathbf{size} \geq 0 \Rightarrow \mathbf{size} \geq 0 * \mathbf{size} \geq 0$  follows from the proof of  $\mathbf{size} \geq \beta_2 \Rightarrow \mathbf{size} \geq 0 * \mathbf{size} \geq \beta_2$  shown above (first case). Hence, by propositional reasoning we conclude  $\vdash_{\mathcal{H}_c(*)} \mathbf{size} \geq 0 \Leftrightarrow \mathbf{size} \geq 0 * \mathbf{size} \geq 0$ , ending the proof of L1.

**Proof of L2.** In the following syntactical proof, we denote with  $\hat{\gamma}$  the formula

$$((\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge \mathbf{size} \geq \beta' \dot{-} \beta)) \vee ((\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge \neg \mathbf{size} \geq \beta' \dot{-} \beta)).$$

1	$\psi \Rightarrow \psi \wedge (\mathbf{size} \geq \beta' \dot{-} \beta \vee \neg \mathbf{size} \geq \beta' \dot{-} \beta)$	(TI) and (TS)
2	$(\phi \wedge \mathbf{size} \geq \beta) * \psi \Rightarrow$ $(\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge (\mathbf{size} \geq \beta' \dot{-} \beta \vee \neg \mathbf{size} \geq \beta' \dot{-} \beta))$	*-introduction rule and (COM), 1
3	$(\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge (\mathbf{size} \geq \beta' \dot{-} \beta \vee \neg \mathbf{size} \geq \beta' \dot{-} \beta)) \Rightarrow \hat{\gamma}$	( $\wedge$ V) and (*DISTR)
4	$(\phi \wedge \mathbf{size} \geq \beta) * \psi \Rightarrow \hat{\gamma}$	( $\Rightarrow$ T), 2, 3
5	$((\phi \wedge \mathbf{size} \geq \beta) * \psi) \wedge \neg \mathbf{size} \geq \beta' \Rightarrow \hat{\gamma} \wedge \neg \mathbf{size} \geq \beta'$	( $\wedge$ I) and ( $\wedge$ C), 4
6	$\hat{\gamma} \wedge \neg \mathbf{size} \geq \beta' \Rightarrow$ $((\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge \mathbf{size} \geq \beta' \dot{-} \beta)) \wedge \neg \mathbf{size} \geq \beta' \vee$ $((\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge \neg \mathbf{size} \geq \beta' \dot{-} \beta)) \wedge \neg \mathbf{size} \geq \beta'$	( $\wedge$ V) and ( $\wedge$ C)

In the remaining part of this proof, we denote with  $\tilde{\gamma}$  the formula

$$(((\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge \mathbf{size} \geq \beta' \dot{-} \beta)) \wedge \neg \mathbf{size} \geq \beta') \vee (((\phi \wedge \mathbf{size} \geq \beta) * (\psi \wedge \neg \mathbf{size} \geq \beta' \dot{-} \beta)) \wedge \neg \mathbf{size} \geq \beta').$$

7	$((\phi \wedge \text{size} \geq \beta) * \psi) \wedge \neg \text{size} \geq \beta' \Rightarrow \tilde{\gamma}$	$(\Rightarrow \mathbf{T})$ , 5, 6
8	$((\phi \wedge \text{size} \geq \beta) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \Rightarrow \text{size} \geq \beta * \text{size} \geq \beta' \dot{-} \beta$	<b>L0</b>
9	$\text{size} \geq \beta * \text{size} \geq \beta' \dot{-} \beta \Rightarrow \text{size} \geq \max(\beta, \beta')$	<b>L1</b>
10	$((\phi \wedge \text{size} \geq \beta) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \Rightarrow \text{size} \geq \max(\beta, \beta')$	$(\Rightarrow \mathbf{T})$ , 8, 9
11	$\text{size} \geq \max(\beta, \beta') \Rightarrow \text{size} \geq \beta'$	repeated ( <b>S<sub>2</sub><sup>c</sup></b> )
12	$((\phi \wedge \text{size} \geq \beta) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \Rightarrow \text{size} \geq \beta'$	$(\Rightarrow \mathbf{T})$ , 10, 11
13	$((\phi \wedge \text{size} \geq \beta) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \wedge \neg \text{size} \geq \beta' \Rightarrow$ $\quad \text{size} \geq \beta' \wedge \neg \text{size} \geq \beta'$	$(\wedge \mathbf{I})$ and $(\wedge \mathbf{C})$ , 12
14	$\text{size} \geq \beta' \wedge \neg \text{size} \geq \beta' \Leftrightarrow \perp$	$(\top \mathbf{S})$ and def $\top$
15	$((\phi \wedge \text{size} \geq \beta) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \wedge \neg \text{size} \geq \beta' \Leftrightarrow \perp$	$(\Rightarrow \mathbf{T})$ and $(\perp \mathbf{I})$ , 13, 14
16	$((\phi \wedge \text{size} \geq \beta) * \psi) \wedge \neg \text{size} \geq \beta' \Rightarrow$ $\quad \perp \vee ((\phi \wedge \text{size} \geq \beta) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta) \wedge \neg \text{size} \geq \beta')$	<b>R0</b> , 7, 15
17	$\perp \vee ((\phi \wedge \text{size} \geq \beta) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta) \wedge \neg \text{size} \geq \beta') \Rightarrow$ $\quad (\phi \wedge \text{size} \geq \beta) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)$	propositional reasoning
18	$((\phi \wedge \text{size} \geq \beta) * \psi) \wedge \neg \text{size} \geq \beta' \Rightarrow$ $\quad (\phi \wedge \text{size} \geq \beta) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)$	$(\Rightarrow \mathbf{T})$ , 16, 17

**Proof of L3.** The proof is similar to the previous one. Let  $\hat{\gamma}$  be the formula

$$((\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \vee ((\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)).$$

1	$\psi \Rightarrow \psi \wedge (\text{size} \geq \beta' \dot{-} \beta \vee \neg \text{size} \geq \beta' \dot{-} \beta)$	$(\top \mathbf{I})$ and $(\top \mathbf{S})$
2	$(\phi \wedge \neg \text{size} \geq \beta+1) * \psi \Rightarrow$ $\quad (\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge (\text{size} \geq \beta' \dot{-} \beta \vee \neg \text{size} \geq \beta' \dot{-} \beta))$	<b>*-introduction rule</b> and <b>(COM)</b> , 1
3	$(\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge (\text{size} \geq \beta' \dot{-} \beta \vee \neg \text{size} \geq \beta' \dot{-} \beta)) \Rightarrow \hat{\gamma}$	$(\wedge \vee)$ and <b>(*DISTR)</b>
4	$(\phi \wedge \neg \text{size} \geq \beta+1) * \psi \Rightarrow \hat{\gamma}$	$(\Rightarrow \mathbf{T})$ , 2, 3
5	$((\phi \wedge \neg \text{size} \geq \beta+1) * \psi) \wedge \text{size} \geq \beta' \Rightarrow \hat{\gamma} \wedge \text{size} \geq \beta'$	$(\wedge \mathbf{I})$ and $(\wedge \mathbf{C})$ , 4
6	$\hat{\gamma} \wedge \text{size} \geq \beta' \Rightarrow$ $\quad (((\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \wedge \text{size} \geq \beta') \vee$ $\quad (((\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)) \wedge \text{size} \geq \beta')$	$(\wedge \vee)$ and $(\wedge \mathbf{C})$

In the remaining part of this proof, we denote with  $\tilde{\gamma}$  the formula

$$(((\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)) \wedge \text{size} \geq \beta') \vee (((\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)) \wedge \text{size} \geq \beta')$$

7	$((\phi \wedge \neg \text{size} \geq \beta+1) * \psi) \wedge \text{size} \geq \beta' \Rightarrow \tilde{\gamma}$	$(\Rightarrow \mathbf{T})$ , 5, 6
8	$((\phi \wedge \neg \text{size} \geq \beta+1) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)) \Rightarrow \neg \text{size} \geq \beta+1 * \neg \text{size} \geq \beta' \dot{-} \beta$	<b>L0</b>

We now prove that  $\vdash_{\mathcal{H}_c(*)} \neg \text{size} \geq \beta+1 * \neg \text{size} \geq \beta' \dot{-} \beta \Rightarrow \neg \text{size} \geq \beta'$  by splitting the proof on whether or not  $\beta' \leq \beta$ . If  $\beta' \leq \beta$  then  $\beta' \dot{-} \beta = 0$  and therefore

9	$\neg \text{size} \geq 0 \Leftrightarrow \perp$	def. of <b>size</b> and propositional reasoning
10	$\neg \text{size} \geq \beta+1 * \neg \text{size} \geq 0 \Rightarrow \neg \text{size} \geq \beta+1 * \perp$	<b>*-introduction rule</b> and <b>(COM)</b> , 9
11	$\neg \text{size} \geq \beta+1 * \perp \Rightarrow \perp$	$(\perp)$
12	$\neg \text{size} \geq \beta+1 * \neg \text{size} \geq 0 \Rightarrow \perp$	$(\Rightarrow \mathbf{T})$ , 10, 11
13	$\perp \Rightarrow \neg \text{size} \geq \beta'$	$(\perp \mathbf{I})$
14	$\neg \text{size} \geq \beta+1 * \neg \text{size} \geq \beta' \dot{-} \beta \Rightarrow \neg \text{size} \geq \beta'$	$(\Rightarrow \mathbf{T})$ , 12, 13

If instead  $\beta' > \beta$  then  $\beta' \dot{-} \beta = \beta' - \beta$  and  $\vdash_{\mathcal{H}_c(*)} \neg \text{size} \geq \beta + 1 * \neg \text{size} \geq \beta' - \beta \Rightarrow \neg \text{size} \geq \beta'$  follows by **(S<sub>6</sub><sup>\*</sup>)**. We are now ready to conclude the proof of **L3**.

15	$\neg \text{size} \geq \beta + 1 * \neg \text{size} \geq \beta' \dot{-} \beta \Rightarrow \neg \text{size} \geq \beta'$	as shown above
16	$((\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)) \Rightarrow \neg \text{size} \geq \beta'$	<b>(<math>\Rightarrow</math>T)</b> , 8, 15
17	$((\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)) \wedge \text{size} \geq \beta' \Rightarrow \neg \text{size} \geq \beta' \wedge \text{size} \geq \beta'$	<b>(<math>\wedge</math>I)</b> and <b>(<math>\wedge</math>C)</b> , 16
18	$\neg \text{size} \geq \beta' \wedge \text{size} \geq \beta' \Leftrightarrow \perp$	<b>(<math>\top</math>S)</b> and def. $\top$
19	$((\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \neg \text{size} \geq \beta' \dot{-} \beta)) \wedge \text{size} \geq \beta' \Leftrightarrow \perp$	<b>(<math>\Rightarrow</math>T)</b> and <b>(<math>\perp</math>I)</b> , 17, 18
20	$((\phi \wedge \neg \text{size} \geq \beta + 1) * \psi) \wedge \text{size} \geq \beta' \Rightarrow$ $((\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta) \wedge \text{size} \geq \beta') \vee \perp$	<b>R0</b> , 7, 19
21	$((\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta) \wedge \text{size} \geq \beta') \vee \perp \Rightarrow$ $(\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)$	<b>(<math>\top</math>I)</b>
22	$((\phi \wedge \neg \text{size} \geq \beta + 1) * \psi) \wedge \text{size} \geq \beta' \Rightarrow$ $(\phi \wedge \neg \text{size} \geq \beta + 1) * (\psi \wedge \text{size} \geq \beta' \dot{-} \beta)$	<b>(<math>\Rightarrow</math>T)</b> , 20, 21

**Proof of L4.** Suppose  $0 \leq \beta_1 < \beta'_1$  and  $0 \leq \beta_2 < \beta'_2$ .

( $\Leftarrow$ ):

1	$(\text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \text{size} \geq \beta_1 * \text{size} \geq \beta_2$	<b>L0</b>
2	$\text{size} \geq \beta_1 * \text{size} \geq \beta_2 \Rightarrow \text{size} \geq \beta_1 + \beta_2$	<b>L1</b>
3	$(\text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \text{size} \geq \beta_1 + \beta_2$	<b>(<math>\Rightarrow</math>T)</b> , 1, 2
4	$(\text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \neg \text{size} \geq \beta'_1 * \neg \text{size} \geq \beta'_2$	<b>L0</b>
5	$\neg \text{size} \geq \beta'_1 * \neg \text{size} \geq \beta'_2 \Rightarrow \neg \text{size} \geq (\beta_1 + \beta_2) \dot{-} 1$	<b>(S<sub>6</sub><sup>*</sup>)</b>
6	$(\text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \neg \text{size} \geq (\beta_1 + \beta_2) \dot{-} 1$	<b>(<math>\Rightarrow</math>T)</b> , 4, 5
7	$(\text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $\text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta_1 + \beta_2) \dot{-} 1$	<b>(<math>\wedge</math>R)</b> , 3, 6

( $\Rightarrow$ ): We start this case by first proving that for every  $\beta, \beta' \geq 1$

$$\vdash_{\mathcal{H}_c(*)} \neg \text{size} \geq (\beta + \beta') \dot{-} 1 \Rightarrow \neg \text{size} \geq \beta * \neg \text{size} \geq \beta'.$$

1	$\neg \text{size} \geq (\beta + \beta') \dot{-} 1 \Rightarrow$ $\neg \text{size} \geq (\beta + \beta') \dot{-} 1 \wedge \bigwedge_{k \in [0, (\beta + \beta') \dot{-} 2]} (\text{size} \geq k \vee \neg \text{size} \geq k)$	repeated <b>(<math>\top</math>I)</b> and <b>(<math>\top</math>S)</b>
2	$\neg \text{size} \geq (\beta + \beta') \dot{-} 1 \wedge \bigwedge_{k \in [0, (\beta + \beta') \dot{-} 2]} (\text{size} \geq k \vee \neg \text{size} \geq k) \Rightarrow$ $\bigvee_{k \in [0, (\beta + \beta') \dot{-} 2]} \text{size} = k$	repeated <b>(<math>\wedge</math>V)</b> + reasoning on <b>size</b>
3	$\neg \text{size} \geq (\beta + \beta') \dot{-} 1 \Rightarrow \bigvee_{k \in [0, (\beta + \beta') \dot{-} 2]} \text{size} = k$	<b>(<math>\Rightarrow</math>T)</b> , 1, 2
4	$\text{size} \geq k \Rightarrow \text{size} = \min(k, \beta - 1) * \text{size} \geq k \dot{-} (\beta - 1)$	<b>(S<sub>5</sub><sup>*</sup>)</b>
5	$\text{size} = k \Rightarrow (\text{size} = \min(k, \beta - 1) * \text{size} \geq k \dot{-} (\beta - 1)) \wedge \neg \text{size} \geq k + 1$	<b>(<math>\wedge</math>I)</b> and <b>(<math>\wedge</math>C)</b> , 4
6	$(\text{size} = \min(k, \beta - 1) * \text{size} \geq k \dot{-} (\beta - 1)) \wedge \neg \text{size} \geq k + 1 \Rightarrow$ $\text{size} = \min(k, \beta - 1) * (\text{size} \geq k \dot{-} (\beta - 1) \wedge \neg \text{size} \geq (k + 1) \dot{-} \min(k, (\beta - 1)))$	<b>L2</b>
7	$\text{size} = k \Rightarrow$ $\text{size} = \min(k, \beta - 1) * (\text{size} \geq k \dot{-} (\beta - 1) \wedge \neg \text{size} \geq (k + 1) \dot{-} \min(k, (\beta - 1)))$	<b>(<math>\Rightarrow</math>T)</b> , 5, 6
8	$\text{size} = \min(k, \beta - 1) * (\text{size} \geq k \dot{-} (\beta - 1) \wedge \neg \text{size} \geq (k + 1) \dot{-} \min(k, (\beta - 1))) \Rightarrow$ $\neg \text{size} \geq \min(k + 1, \beta) * \neg \text{size} \geq (k + 1) \dot{-} \min(k, (\beta - 1))$	<b>L0</b>
9	$\text{size} = k \Rightarrow \neg \text{size} \geq \min(k + 1, \beta) * \neg \text{size} \geq (k + 1) \dot{-} \min(k, (\beta - 1))$	<b>(<math>\Rightarrow</math>T)</b> , 7, 8

We continue the proof by showing that for every  $k \in [0, (\beta + \beta') \dot{-} 2]$ ,

$$\vdash_{\mathcal{H}_c(*)} \neg \text{size} \geq \min(k+1, \beta) * \neg \text{size} \geq (k+1) \dot{-} \min(k, (\beta-1)) \Rightarrow \neg \text{size} \geq \beta * \neg \text{size} \geq \beta'.$$

Indeed, for  $k < \beta$  the antecedent of this implication, i.e.  $\neg \text{size} \geq \min(k+1, \beta) * \neg \text{size} \geq (k+1) \dot{-} \min(k, (\beta-1))$ , simplifies to  $\neg \text{size} \geq k * \neg \text{size} \geq 1$ . Then, recalling that  $1 \leq \beta'$ , by iterating the axiom **(S<sub>5</sub><sup>c</sup>)** together with **\*-introduction rule**, we can conclude  $\vdash_{\mathcal{H}_c(*)} \neg \text{size} \geq k * \neg \text{size} \geq 1 \Rightarrow \neg \text{size} \geq \beta * \neg \text{size} \geq \beta'$ . If instead  $k \geq \beta$ , then the antecedent becomes  $\neg \text{size} \geq \beta * \neg \text{size} \geq (k+1) \dot{-} (\beta-1)$ . Since  $k \in [0, (\beta + \beta') \dot{-} 2]$  and  $\beta, \beta' \geq 1$ , we have  $(k+1) \dot{-} (\beta-1) \leq (((\beta + \beta') \dot{-} 2) + 1) \dot{-} (\beta-1) \leq \beta'$ . Hence,  $\neg \text{size} \geq \beta * \neg \text{size} \geq (k+1) \dot{-} (\beta-1)$  simplifies to  $\neg \text{size} \geq \beta * \neg \text{size} \geq j$  for some  $j \leq \beta'$ . Then,  $\vdash_{\mathcal{H}_c(*)} \neg \text{size} \geq \beta * \neg \text{size} \geq j \Rightarrow \neg \text{size} \geq \beta * \neg \text{size} \geq \beta'$  again by iterating the axiom **(S<sub>5</sub><sup>c</sup>)** together with **\*-introduction rule**. We can now conclude the proof of  $\vdash_{\mathcal{H}_c(*)} \neg \text{size} \geq (\beta + \beta') \dot{-} 1 \Rightarrow \neg \text{size} \geq \beta * \neg \text{size} \geq \beta'$ .

10	$\neg \text{size} \geq \min(k+1, \beta) * \neg \text{size} \geq (k+1) \dot{-} \min(k, (\beta-1)) \Rightarrow$	
	$\neg \text{size} \geq \beta * \neg \text{size} \geq \beta'$	$\forall k \in [0, (\beta + \beta') \dot{-} 2]$ – just shown
11	$\text{size} = k \Rightarrow \neg \text{size} \geq \beta * \neg \text{size} \geq \beta'$	$\forall k \in [0, (\beta + \beta') \dot{-} 2]$ – <b>(<math>\Rightarrow</math>T)</b> , 9, 10
12	$\neg \text{size} \geq (\beta + \beta') \dot{-} 1 \Rightarrow \neg \text{size} \geq \beta * \neg \text{size} \geq \beta'$	propositional reasoning, 3, 11

We now tackle the left-to-right direction of **L4**. Recall that  $0 \leq \beta_1 < \beta'_1$  and  $0 \leq \beta_2 < \beta'_2$ .

1	$\text{size} \geq \beta_1 + \beta_2 \Rightarrow \text{size} = \beta_1 * \text{size} \geq \beta_2$	<b>(S<sub>5</sub><sup>c</sup>)</b>
2	$\text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1 \Rightarrow$	
	$(\text{size} = \beta_1 * \text{size} \geq \beta_2) \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1$	<b>(<math>\wedge</math>I)</b> and <b>(<math>\wedge</math>C)</b> , 1
3	$(\text{size} = \beta_1 * \text{size} \geq \beta_2) \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\text{size} = \beta_1 * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1)$	<b>L2</b> and $\beta_1 < \beta'_1$
4	$\text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\text{size} = \beta_1 * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1)$	<b>(<math>\Rightarrow</math>T)</b> , 2, 3
5	$\text{size} \geq \beta_2 \Rightarrow \text{size} = \beta_2 * \text{size} \geq 0$	<b>(S<sub>5</sub><sup>c</sup>)</b>
6	$\text{size} \geq \beta_2 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1 \Rightarrow$	
	$(\text{size} = \beta_2 * \text{size} \geq 0) \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1$	<b>(<math>\wedge</math>I)</b> and <b>(<math>\wedge</math>C)</b> , 5
7	$(\text{size} = \beta_2 * \text{size} \geq 0) \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\text{size} = \beta_2 * (\text{size} \geq 0 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1)$	<b>L2</b> and $\beta_1 < \beta'_1$
8	$\text{size} \geq \beta_2 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\text{size} = \beta_2 * (\text{size} \geq 0 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1)$	<b>(<math>\Rightarrow</math>T)</b> , 6, 7
9	$\text{size} \geq 0 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1 \Rightarrow$	
	$\neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1$	<b>(<math>\wedge</math>E)</b>
10	$\text{size} = \beta_2 * (\text{size} \geq 0 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1) \Rightarrow$	
	$\text{size} = \beta_2 * \neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1$	<b>*-introduction rule</b> and <b>(COM)</b> , 9
11	$\text{size} \geq \beta_2 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\text{size} = \beta_2 * \neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1$	<b>(<math>\Rightarrow</math>T)</b> , 8, 10
12	$\neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1 \Rightarrow$	
	$\neg \text{size} \geq \beta'_1 - \beta_1 * \neg \text{size} \geq \beta'_2 - \beta_2$	previous result, as $\beta_1 < \beta'_1$ and $\beta_2 < \beta'_2$
13	$\text{size} = \beta_2 * \neg \text{size} \geq ((\beta'_1 - \beta_1) + (\beta'_2 - \beta_2)) \dot{-} 1 \Rightarrow$	
	$\text{size} = \beta_2 * (\neg \text{size} \geq \beta'_1 - \beta_1 * \neg \text{size} \geq \beta'_2 - \beta_2)$	<b>*-introduction rule</b> and <b>(COM)</b> , 12
14	$\text{size} \geq \beta_2 \wedge \neg \text{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\text{size} = \beta_2 * (\neg \text{size} \geq \beta'_1 - \beta_1 * \neg \text{size} \geq \beta'_2 - \beta_2)$	<b>(<math>\Rightarrow</math>T)</b> , 12, 13

15	$\mathbf{size} = \beta_2 * (\neg \mathbf{size} \geq \beta'_1 - \beta_1 * \neg \mathbf{size} \geq \beta'_2 - \beta_2) \Rightarrow$	
	$\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2)$	(COM) and (ASSOC)
16	$\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2)$	( $\Rightarrow$ T), 14, 15
17	$\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2 \Rightarrow \mathbf{size} \geq \beta_2 * \mathbf{size} \geq 0$	( $S_1^c$ ) and L0
18	$\mathbf{size} \geq \beta_2 * \mathbf{size} \geq 0 \Rightarrow \mathbf{size} \geq \beta_2$	L1
19	$\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2 \Rightarrow \mathbf{size} \geq \beta_2$	( $\Rightarrow$ T), 17, 18
20	$\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2 \Rightarrow \neg \mathbf{size} \geq \beta_2 + 1 * \neg \mathbf{size} \geq \beta'_2 - \beta_2$	L0
21	$\neg \mathbf{size} \geq \beta_2 + 1 * \neg \mathbf{size} \geq \beta'_2 - \beta_2 \Rightarrow \neg \mathbf{size} \geq \beta'_2$	( $S_6^*$ )
22	$\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2 \Rightarrow \neg \mathbf{size} \geq \beta'_2$	( $\Rightarrow$ T), 20, 21
23	$\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2 \Rightarrow \mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2$	( $\wedge$ R), 19, 22
24	$\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} = \beta_2 * \neg \mathbf{size} \geq \beta'_2 - \beta_2) \Rightarrow$	
	$\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2)$	*-introduction rule and (COM), 23
25	$\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2)$	( $\Rightarrow$ T), 16, 24
26	$\mathbf{size} = \beta_1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq ((\beta'_1 - \beta_1) + \beta'_2) \dot{-} 1)$	
	$\mathbf{size} = \beta_1 * (\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2))$	*-introduction rule and (COM), 25
27	$\mathbf{size} \geq \beta_1 + \beta_2 \wedge \neg \mathbf{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1 \Rightarrow$	
	$\mathbf{size} = \beta_1 * (\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2))$	( $\Rightarrow$ T), 4, 26
28	$\mathbf{size} = \beta_1 * (\neg \mathbf{size} \geq \beta'_1 - \beta_1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2)) \Rightarrow$	
	$(\mathbf{size} = \beta_1 * \neg \mathbf{size} \geq \beta'_1 - \beta_1) * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2)$	(ASSOC)
29	$\mathbf{size} \geq \beta_1 + \beta_2 \wedge \neg \mathbf{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1 \Rightarrow$	
	$(\mathbf{size} = \beta_1 * \neg \mathbf{size} \geq \beta'_1 - \beta_1) * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2)$	( $\Rightarrow$ T), 27, 28
30	$\mathbf{size} = \beta_1 * \neg \mathbf{size} \geq \beta'_1 - \beta_1 \Rightarrow \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1$	analogous to 23
31	$(\mathbf{size} = \beta_1 * \neg \mathbf{size} \geq \beta'_1 - \beta_1) * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2) \Rightarrow$	
	$(\mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2)$	*-introduction rule, 30
32	$\mathbf{size} \geq \beta_1 + \beta_2 \wedge \neg \mathbf{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1 \Rightarrow$	
	$(\mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2)$	( $\Rightarrow$ T), 29, 31

## Proof of Lemma 11

We start by handling the cases for graph formulae of the form  $|Q_1, \dots, Q_n\rangle$  and  $|Q_1, \dots, \overline{Q_i, \dots, Q_n}\rangle$ . Recall that  $|Q_1, \dots, Q_n \overline{\phantom{Q}}\rangle$  denotes only formulae of these two kinds (hence excluding  $|Q_1, \dots, Q_n\rangle$  formulae, that we treat separately). Moreover, recall that we are working under the hypothesis that for any elementary shape  $\psi$  of the form either  $\mathcal{G} \wedge \mathbf{size} \geq \beta$  or  $\mathcal{G} \wedge \mathbf{size} \geq \beta \wedge \neg \mathbf{size} \geq \beta'$ , we have  $\sharp(\mathcal{G}) \leq \beta$ ,  $\not\vdash_{\mathcal{H}_c} \neg \psi$  (which implies  $\beta < \beta'$ ). Below, this assumption is denoted by  $(\mathcal{G}_{Hyp})$ .

■  $(|Q_1, \dots, Q_n \overline{\phantom{Q}}\rangle \wedge \mathbf{size} \geq \beta_1) * (|Q\rangle \wedge \mathbf{size} \geq \beta_2) \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}\rangle \wedge \mathbf{size} \geq \beta_1 + \beta_2$

( $\Rightarrow$ ):

1	$( Q_1, \dots, Q_n \overline{\phantom{Q}}\rangle \wedge \mathbf{size} \geq \beta_1) * ( Q\rangle \wedge \mathbf{size} \geq \beta_2) \Leftrightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}\rangle \wedge \mathbf{size} \geq \beta_1) * \mathbf{size} \geq \beta_2$	( $G_{26}^*$ )
2	$( Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}\rangle \wedge \mathbf{size} \geq \beta_1) * \mathbf{size} \geq \beta_2 \Rightarrow  Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}\rangle$	( $G_{23}^*$ )/( $G_{24}^*$ ) and L0
3	$( Q_1, \dots, Q_n \overline{\phantom{Q}}\rangle \wedge \mathbf{size} \geq \beta_1) * ( Q\rangle \wedge \mathbf{size} \geq \beta_2) \Rightarrow  Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}\rangle$	( $\Rightarrow$ T), 1, 2
4	$( Q_1, \dots, Q_n \overline{\phantom{Q}}\rangle \wedge \mathbf{size} \geq \beta_1) * ( Q\rangle \wedge \mathbf{size} \geq \beta_2) \Rightarrow \mathbf{size} \geq \beta_1 * \mathbf{size} \geq \beta_2$	L0



5	$\text{size} \geq \beta_1 * \text{size} \geq \beta_2 \Rightarrow \text{size} \geq \beta_1 + \beta_2$	<b>L1</b>
6	$( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2) \Rightarrow \text{size} \geq \beta_1 + \beta_2$	<b>(<math>\Rightarrow</math>T)</b> , 4, 5
7	$( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2) \Rightarrow$ $ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2$	<b>(<math>\wedge</math>R)</b> , 3, 6

( $\Leftarrow$ ):

1	$\text{size} \geq \beta_1 + \beta_2 \Rightarrow \text{size} \geq \beta_1$	repeated ( <b>S<sub>2</sub></b> )
2	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow  Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1$	<b>(<math>\wedge</math>I)</b> , 1
3	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \top$	<b>(G<sub>27</sub><sup>*</sup>)</b> and ( <b>G<sub>Hyp</sub></b> )
4	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \top) \wedge \text{size} \geq \beta_1 + \beta_2$	<b>(<math>\Rightarrow</math>T)</b> and ( <b>(<math>\wedge</math>D)</b> ), 2, 3
5	$(( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \top) \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2$	<b>L3</b>
6	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2$	<b>(<math>\Rightarrow</math>T)</b> , 4, 5
7	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1 \Rightarrow  Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1$	<b>(<math>\wedge</math>E)</b>
8	$( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2$	<b>*-introduction rule</b> , 7
9	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2$	<b>(<math>\Rightarrow</math>T)</b> , 6, 8
10	$( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2 \Rightarrow ( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>(G<sub>26</sub><sup>*</sup>)</b>
11	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow ( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>(<math>\Rightarrow</math>T)</b> , 9, 10

$$\blacksquare (|Q_1, \dots, Q_n \bar{\cdot}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2) \\ \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \bar{\cdot}| \wedge \text{size} \geq \beta_1 + \beta_2$$

( $\Rightarrow$ ):

1	$( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) \Rightarrow  Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1$	<b>(<math>\wedge</math>E)</b>
2	$( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q  \wedge \text{size} \geq \beta_2) \Rightarrow$ $( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>*-introduction rule</b> , 1
3	$( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2) \Rightarrow  Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2$	previously derived
4	$( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q  \wedge \text{size} \geq \beta_2) \Rightarrow$ $ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2$	<b>(<math>\Rightarrow</math>T)</b> , 2, 3

( $\Leftarrow$ ):

1	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2$	previously derived
2	$( Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 \Rightarrow$ $( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>(G<sub>26</sub><sup>*</sup>)</b>
3	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow ( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>(<math>\Rightarrow</math>T)</b> , 1, 2
4	$\neg \text{size} \geq \beta_1 + 1 \Rightarrow \neg \text{size} \geq \beta'_1$	<b>(S<sub>2</sub></b> ) and ( <b>G<sub>Hyp</sub></b> )
5	$ Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1 \Rightarrow  Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1$	<b>(<math>\wedge</math>I)</b> , 4
6	$( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} = \beta_1) * ( Q  \wedge \text{size} \geq \beta_2) \Rightarrow$ $( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>*-introduction rule</b> , 5
7	$ Q_1 \wedge Q, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $( Q_1, \dots, Q_n \bar{\cdot}  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>(<math>\Rightarrow</math>T)</b> , 3, 6

$$\blacksquare (|Q_1, \dots, Q_n \bar{\neg}| \wedge \text{size} \geq \beta_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2)$$

$$\Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \bar{\neg}| \wedge \text{size} \geq \beta_1 + \beta_2$$

( $\Rightarrow$ ):

1	$( Q  \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow  Q  \wedge \text{size} \geq \beta_2$	( $\wedge E$ )
2	$( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2)$	( <b>COM</b> ) and <i>*-introduction rule</i> , 1
3	$( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2) \Rightarrow$ $ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2$	previously derived
4	$( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2$	( $\Rightarrow T$ ), 2, 3

( $\Leftarrow$ ):

1	$ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2$	previously derived
2	$\text{size} \geq \beta_2 \Rightarrow \text{size} = \beta_2 * \text{size} \geq 0$	( $S_5^*$ )
3	$( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * (\text{size} = \beta_2 * \text{size} \geq 0)$	<i>*-introduction rule</i> , ( <b>COM</b> ), 2
4	$ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * (\text{size} = \beta_2 * \text{size} \geq 0)$	( $\Rightarrow T$ ), 1, 3
5	$( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * (\text{size} = \beta_2 * \text{size} \geq 0) \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * \text{size} \geq 0) * \text{size} = \beta_2$	( <b>ASSOC</b> ), ( <b>COM</b> ) and ( $\Rightarrow T$ )
6	$ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * \text{size} \geq 0) * \text{size} = \beta_2$	( $\Rightarrow T$ ), 4, 5
7	$( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * \text{size} \geq 0 \Rightarrow  Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1$	previously derived
8	$(( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} = \beta_1) * \text{size} \geq 0) * \text{size} = \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * \text{size} = \beta_2$	<i>*-introduction rule</i> , 7
9	$ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * \text{size} = \beta_2$	( $\Rightarrow T$ ), 6, 8
10	$\neg \text{size} \geq \beta_2 + 1 \Rightarrow \neg \text{size} \geq \beta'_2$	( $S_2^c$ ) and ( $\mathcal{G}_{Hyp}$ )
11	$\text{size} = \beta_2 \Rightarrow \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2$	( $\wedge I_2$ ), 10
12	$( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * \text{size} = \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2)$	<i>*-introduction rule</i> , ( <b>COM</b> ), 11
13	$ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2)$	( $\Rightarrow T$ ), 9, 12
14	$( Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2)$	( $G_{26}^*$ )
15	$ Q_1 \wedge Q, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2)$	( $\Rightarrow T$ ), 13, 14

$$\blacksquare (|Q_1, \dots, Q_n \bar{\neg}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2)$$

$$\Leftrightarrow |Q_1 \wedge Q, \dots, Q_n \bar{\neg}| \wedge \text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1$$

( $\Rightarrow$ ):

1	$( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q  \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $( Q_1, \dots, Q_n \bar{\neg}  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2)$	<b>L0</b>
---	--	-----------

$$\begin{array}{l}
2 \quad (|Q_1, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1) * (|Q| \wedge \text{size} \geq \beta_2) \Rightarrow |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 + \beta_2 \quad \text{previously derived} \\
3 \quad (|Q_1, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
\quad |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 + \beta_2 \quad (\Rightarrow \mathbf{T}), 1, 2 \\
4 \quad (|Q_1, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
\quad \neg \text{size} \geq \beta'_1 * \neg \text{size} \geq \beta'_2 \quad \mathbf{L0} \\
5 \quad \neg \text{size} \geq \beta'_1 * \neg \text{size} \geq \beta'_2 \Rightarrow \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \quad (\mathbf{S}_6^*) \\
6 \quad (|Q_1, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
\quad \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \quad (\Rightarrow \mathbf{T}), 4, 5 \\
7 \quad (|Q_1, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
\quad |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \quad (\wedge \mathbf{R}), 3, 6
\end{array}$$

( $\Leftarrow$ ):

$$\begin{array}{l}
1 \quad |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow \\
\quad (|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 \quad \text{previously derived} \\
2 \quad |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \Rightarrow \\
\quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2) \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \quad (\wedge \mathbf{I}), 1 \\
3 \quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2) \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \Rightarrow \\
\quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div (\beta_1 + 1))) \quad \mathbf{L2} \text{ and } (\mathcal{G}_{Hyp}) \\
4 \quad |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \Rightarrow \\
\quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div (\beta_1 + 1))) \quad (\Rightarrow \mathbf{T}), 2, 3 \\
5 \quad \text{size} \geq \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div (\beta_1 + 1) \Rightarrow \\
\quad (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 \div \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \quad \mathbf{L4} \text{ and } (\mathcal{G}_{Hyp}) \\
6 \quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div (\beta_1 + 1))) \Rightarrow \\
\quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * \\
\quad ((\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 \div \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2))) \quad * \text{-introduction rule and } (\mathbf{COM}), 5 \\
7 \quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * \\
\quad ((\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 \div \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2))) \Rightarrow \\
\quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 \div \beta_1)) * \\
\quad (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \quad (\mathbf{ASSOC}) \\
8 \quad (|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 \div \beta_1) \Rightarrow \\
\quad |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1 \quad \text{previously derived} \\
9 \quad ((|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} = \beta_1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 \div \beta_1)) * \\
\quad (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
\quad (|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \quad * \text{-introduction rule, } 8 \\
10 \quad (|Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
\quad (|Q_1, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \quad (\mathbf{G}_{26}^*) \\
11 \quad |Q_1 \wedge Q, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 + \beta_2 \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \div 1 \Rightarrow \\
\quad (|Q_1, \dots, Q_n \overline{\phantom{Q}}| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2) \quad \text{repeated } (\Rightarrow \mathbf{T}), 4, 6, 7, 9, 10
\end{array}$$

This ends the translation for the formulae of the form either  $|Q_1, \dots, Q_n \overline{\phantom{Q}}|$  or  $|Q_1, \dots, \overline{Q_i}, \dots, Q_n|$ .

In order to conclude the proof, it remains to handle the cases with graph formulae of the form  $|Q_1, \dots, Q_n|$ , that are quite similar to the previous ones, with some peculiarities resulting from the axiom  $(\mathbf{G}_{25}^*)$ . Let us start with an easy case.

■  $(|Q_1, \dots, Q_n] \wedge \phi) * (|Q] \wedge \neg \text{size} \geq 1) \Leftrightarrow |Q_1 \wedge Q, \dots, Q_n] \wedge \phi$ ,  
 where  $\phi = \text{size} \geq \beta_1$  or  $\phi = \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta_2$

1	$( Q_1, \dots, Q_n] \wedge \phi) * ( Q] \wedge \neg \text{size} \geq 1) \Leftrightarrow ( Q_1 \wedge Q, \dots, Q_n] \wedge \phi) * \neg \text{size} \geq 1$	<b>(G*<sub>26</sub>)</b>
2	$( Q_1 \wedge Q, \dots, Q_n] \wedge \phi) * \neg \text{size} \geq 1 \Leftrightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \phi$	<b>(S<sub>1</sub>*)</b>
3	$( Q_1, \dots, Q_n] \wedge \phi) * ( Q] \wedge \neg \text{size} \geq 1) \Leftrightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \phi$	<b>(<math>\Leftrightarrow</math>T), 1, 2</b>

Notice how the right argument of the subformula headed by the operator  $*$  is a formula  $(|Q] \wedge \neg \text{size} \geq 1)$  that is satisfied only by models with empty accessibility relation. Now, instead, we consider the cases of formulae that are satisfied by models with non-empty accessibility relation. Recall that we are working under the assumption  $(\mathcal{G}_{Hyp})$ , hence in what follows  $n - 1 = \#(|Q_1, \dots, Q_n]) \leq \beta_1$ ,  $\beta_1 < \beta'_1$  and  $\beta_2 + 1 < \beta'_2$ .

In the following,  $G_n$  denotes  $(|Q_1 \wedge Q, \dots, Q_n] \vee |Q_1 \wedge Q, \dots, Q_n] \vee \bigvee_{i \in [1, n]} |Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}]$  whereas  $\gamma_n$  denotes  $G_n \wedge \text{size} \geq \beta_1 + \beta_2 + 1$  (as in the body of the paper).

■  $(|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1) \Leftrightarrow \gamma_n$

( $\Rightarrow$ ):

1	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow \text{size} \geq \beta_1 * \text{size} \geq \beta_2 + 1$	<b>L0</b>
2	$\text{size} \geq \beta_1 * \text{size} \geq \beta_2 + 1 \Rightarrow \text{size} \geq \beta_1 + \beta_2 + 1$	<b>L1</b>
3	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow \text{size} \geq \beta_1 + \beta_2 + 1$	<b>(<math>\Rightarrow</math>T), 2, 3</b>
4	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow  Q_1, \dots, Q_n] * \text{size} \geq \beta_2 + 1$	<b>L0</b>
5	$\text{size} \geq \beta_2 + 1 \Rightarrow \text{size} \geq 1$	repeated <b>(S<sub>2</sub>*)</b>
6	$ Q_1, \dots, Q_n] * \text{size} \geq \beta_2 + 1 \Rightarrow  Q_1, \dots, Q_n] * \text{size} \geq 1$	<b>*-introduction rule and (COM), 5</b>
7	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow  Q_1, \dots, Q_n] * \text{size} \geq 1$	<b>(<math>\Rightarrow</math>T), 4, 6</b>
8	$ Q_1, \dots, Q_n] * \text{size} \geq 1 \Rightarrow G_n$	<b>(G*<sub>25</sub>)</b>
9	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow G_n$	<b>(<math>\Rightarrow</math>T), 7, 8</b>
10	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow \gamma_n$	<b>(<math>\wedge</math>R), 3, 9</b>

( $\Leftarrow$ ): By propositional reasoning we can distribute the conjunction over the disjunctions (i.e. the axiom  $(\wedge \vee)$ ) and treat separately each disjunct. Then, to prove the right-to-left direction it is sufficient to show that the following three formulae are derivable in  $\mathcal{H}_c(*)$ :

- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1)$
- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1)$
- For all  $i \in [1, n]$ ,  
 $|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1)$

Let us start with the first one:

1	$\text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow \text{size} \geq \beta_1$	repeated <b>(S<sub>2</sub>*)</b>
2	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1$	<b>(<math>\wedge</math>I), 1</b>
3	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \top$	<b>(G*<sub>27</sub>), <math>\#( Q_1, \dots, Q_n]) \leq \beta_1</math></b>
4	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \top$	<b>(<math>\Rightarrow</math>T), 2, 3</b>
5	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \top) \wedge \text{size} \geq \beta_1 + \beta_2 + 1$	<b>(<math>\wedge</math>D), (<math>\wedge</math>I) and (<math>\Rightarrow</math>T), 4</b>
6	$(( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \top) \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1$	<b>L3</b>
7	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1$	<b>(<math>\Rightarrow</math>T), 5, 6</b>
8	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1 \Rightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1$	<b>(<math>\wedge</math>E)</b>

9	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2 + 1$	*introduction rule, 8
10	$ Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2 + 1$	( $\Rightarrow \mathbf{T}$ ), 7, 9
11	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 + 1)$	( $\mathbf{G}_{26}^*$ )
12	$ Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow ( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 + 1)$	( $\Rightarrow \mathbf{T}$ ), 10, 11

The second and third cases can be proved in an analogous way, hence we treat them as one case. Again, we write  $|Q_1 \wedge Q, \dots, Q_n \overline{\vee}|$  for  $|Q_1 \wedge Q, \dots, Q_n|$  or  $|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n|$ , where  $i \in [1, n]$ . The proof is as follows:

1	$ Q_1 \wedge Q, \dots, Q_n \overline{\vee}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + \beta_2) * \text{size} = 1$	( $\mathbf{G}_{28}^*$ )/( $\mathbf{G}_{29}^*$ )
2	$ Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2$	previously derived, $\#( Q_1, \dots, Q_n ) \leq \beta_1$
3	$\text{size} = 1 \Rightarrow \text{size} \geq 1$	( $\wedge \mathbf{E}$ )
4	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + \beta_2) * \text{size} = 1 \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2) * \text{size} \geq 1$	*introduction rule twice, and ( $\mathbf{COM}$ ), 2, 3
5	$ Q_1 \wedge Q, \dots, Q_n \overline{\vee}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2) * \text{size} \geq 1$	( $\Rightarrow \mathbf{T}$ ), 1, 4
6	$(( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2) * \text{size} \geq 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 * \text{size} \geq 1)$	( $\mathbf{ASSOC}$ )
7	$ Q_1 \wedge Q, \dots, Q_n \overline{\vee}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 * \text{size} \geq 1)$	( $\Rightarrow \mathbf{T}$ ), 5, 6
8	$\text{size} \geq \beta_2 * \text{size} \geq 1 \Rightarrow \text{size} \geq \beta_2 + 1$	$\mathbf{L1}$
9	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 * \text{size} \geq 1) \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2 + 1$	*introduction rule and ( $\mathbf{COM}$ ), 8
10	$ Q_1 \wedge Q, \dots, Q_n \overline{\vee}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2 + 1$	( $\Rightarrow \mathbf{T}$ ), 7, 9
11	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 + 1)$	( $\mathbf{G}_{26}^*$ )
12	$ Q_1 \wedge Q, \dots, Q_n \overline{\vee}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 + 1)$	( $\Rightarrow \mathbf{T}$ ), 10, 11

■  $(|Q_1, \dots, Q_n| \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q| \wedge \text{size} \geq \beta_2 + 1) \Leftrightarrow \gamma_n$ .

( $\Rightarrow$ ):

1	$ Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1 * ( Q  \wedge \text{size} \geq \beta_2 + 1) \Rightarrow \gamma_n$	previously derived
2	$ Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1 \Rightarrow  Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1$	( $\wedge \mathbf{E}$ )
3	$( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q  \wedge \text{size} \geq \beta_2 + 1) \Rightarrow$ $( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1) * ( Q  \wedge \text{size} \geq \beta_2 + 1)$	*introduction rule, 2
4	$( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q  \wedge \text{size} \geq \beta_2 + 1) \Rightarrow \gamma_n$	( $\Rightarrow \mathbf{T}$ ), 1, 3

( $\Leftarrow$ ): As done for the right-to-left direction of the previous case, by propositional reasoning we can distribute the conjunction over the disjunctions and treat separately each disjunct. We then show that the following formulae are derivable in  $\mathcal{H}_c(*)$ .

- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1)$
- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1)$
- For all  $i \in [1, n]$ ,  $|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1$   
 $\Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1)$

As in the previous case, the second and third types of formulae can be treated analogously. Let us start with the first formula:

1	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow ( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1$	previously derived
2	$\neg \text{size} \geq \beta_1 + 1 \Rightarrow \neg \text{size} \geq \beta'_1$	repeated $(S_2^c)$ and $(G_{Hyp})$
3	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1 \Rightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1$	$(\wedge I)$ , 2
4	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * \text{size} \geq \beta_2 + 1$	$*$ -introduction rule, 3
5	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1)$	$(G_{26}^*)$
6	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1)$	$(\Rightarrow T)$ , 4, 5
7	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1)$	$(\Rightarrow T)$ , 1, 6

We now focus on the two remaining types of formulae. Let  $|Q_1 \wedge Q, \dots, Q_n \overline{]}]$  be either  $|Q_1 \wedge Q, \dots, Q_n]$  or  $|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}]$ , for some  $i \in [1, n]$ . Then:

1	$ Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2) * \text{size} = 1$	$(G_{28}^*) / (G_{29}^*)$
2	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2$	previously derived, $\#( Q_1, \dots, Q_n]) \leq \beta_1$
3	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2) * \text{size} = 1 \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2) * \text{size} = 1$	$*$ -introduction rule, 2
4	$ Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $(( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2) * \text{size} = 1$	$(\Rightarrow T)$ , 1, 3
5	$(( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2) * \text{size} = 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 * \text{size} = 1)$	$(ASSOC)$
6	$ Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 * \text{size} = 1)$	$(\Rightarrow T)$ , 4, 5
7	$\text{size} = 1 \Rightarrow \text{size} \geq 1$	$(\wedge E)$
8	$\text{size} \geq \beta_2 * \text{size} = 1 \Rightarrow \text{size} \geq \beta_2 + 1$	$*$ -introduction rule, $(COM)$ and $L1$ , 7
9	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 * \text{size} = 1) \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1$	$*$ -introduction rule and $(COM)$ , 8
10	$ Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1$	$(\Rightarrow T)$ , 6, 9
11	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1)$	previously derived
12	$ Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1)$	$(\Rightarrow T)$ , 10, 11

$$\blacksquare (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Leftrightarrow \gamma_n$$

( $\Rightarrow$ ):

1	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow \gamma_n$	previously derived
2	$ Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2 \Rightarrow  Q] \wedge \text{size} \geq \beta_2 + 1$	( $\wedge E$ )
3	$( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1)$	*-introduction rule and (COM), 2
4	$( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \gamma_n$	( $\Rightarrow T$ ), 1, 3

( $\Leftarrow$ ): Again, by propositional reasoning we can distribute the conjunction over the disjunctions and treat separately each disjunct. We then show that the formulae below are derivable in  $\mathcal{H}_c(*)$ :

- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$
- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$
- For all  $i \in [1, n]$ ,  $|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1$   
 $\Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$

Let us start with the first one:

1	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1$	previously derived
2	$\text{size} \geq \beta_2 + 1 \Rightarrow \text{size} = \beta_2 + 1 * \text{size} \geq 0$	(ASSOC)
3	$\text{size} \geq 0 \Rightarrow \text{size} \geq 1 \vee \neg \text{size} \geq 1$	(TS)
4	$\text{size} = \beta_2 + 1 * \text{size} \geq 0 \Rightarrow (\text{size} \geq 1 \vee \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1$	*-introduction rule and (COM), 3
5	$\text{size} \geq \beta_2 + 1 \Rightarrow (\text{size} \geq 1 \vee \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1$	( $\Rightarrow T$ ), 2, 4
6	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * ((\text{size} \geq 1 \vee \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1)$	*-introduction rule and (COM), 5
7	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * ((\text{size} \geq 1 \vee \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1) \Rightarrow$ $((( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1) * \text{size} = \beta_2 + 1) \vee$ $((( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1)$	(ASSOC), (COM) and (*DISTR)
8	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $((( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1) * \text{size} = \beta_2 + 1) \vee$ $((( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1)$	( $\Rightarrow T$ ), 1, 6, 7

We split the proof (cases (1) and (2) below), deriving the following two tautologies:

1.  $((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1$   
 $\Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$
2.  $|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1) * \text{size} = \beta_2 + 1$   
 $\Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$

Trivially, these two formulae allow us to conclude that

$$|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$$

is derivable in  $\mathcal{H}_c(*)$  directly from the last formula derived above, by propositional reasoning.

1.

1	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \neg \text{size} \geq 1 \Rightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1$	previously derived
2	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1 \Rightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1$	( $\wedge E$ )
3	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \neg \text{size} \geq 1 \Rightarrow  Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1$	( $\Rightarrow T$ ), 1, 2
4	$\neg \text{size} \geq \beta_2 + 2 \Rightarrow \neg \text{size} \geq \beta'_2$	( $S'_2$ ), $\beta_2 + 2 \leq \beta'_2$
5	$\text{size} = \beta_2 + 1 \Rightarrow \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2$	( $\wedge I$ ), 4

$$\begin{array}{l}
6 \quad ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1 * \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1) \Rightarrow \\
\quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \quad \text{*introduction rule and (COM), 3, 5} \\
7 \quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
\quad (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \quad (\mathbf{G}_{26}^*) \\
8 \quad ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1 * \neg \text{size} \geq 1) * \text{size} = \beta_2 + 1) \Rightarrow \\
\quad (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \quad (\Rightarrow \mathbf{T}), 6, 7
\end{array}$$

2.

$$\begin{array}{l}
1 \quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1 \Rightarrow \\
\quad (|Q_1, \dots, Q_n] \vee |Q_1, \dots, Q_n] \vee \bigvee_{i \in [1, n]} |Q_1, \dots, \overline{Q_i}, \dots, Q_n]) \wedge \text{size} \geq \beta_1 + 1 \quad \text{previously derived} \\
2 \quad ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1) * \text{size} = \beta_2 + 1 \Rightarrow \\
\quad ((|Q_1 \wedge Q, \dots, Q_n] \vee |Q_1 \wedge Q, \dots, Q_n] \vee \bigvee_{i \in [1, n]} |Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n]) \wedge \text{size} \geq \beta_1 + 1) \\
\quad * \text{size} = \beta_2 + 1 \quad \text{*introduction rule, 1} \\
3 \quad ((|Q_1 \wedge Q, \dots, Q_n] \vee |Q_1 \wedge Q, \dots, Q_n] \vee \bigvee_{i \in [1, n]} |Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n]) \wedge \text{size} \geq \beta_1 + 1) \\
\quad * \text{size} = \beta_2 + 1 \Rightarrow ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \\
\quad \vee ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \\
\quad \vee \bigvee_{i \in [1, n]} ((|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \quad (\wedge \mathbf{C}) \text{ and } (*\mathbf{DISTR}) \\
4 \quad ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1) * \text{size} = \beta_2 + 1 \Rightarrow \\
\quad ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \\
\quad \vee ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \\
\quad \vee \bigvee_{i \in [1, n]} ((|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \quad (\Rightarrow \mathbf{T}), 2, 3 \\
5 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge (((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1) * \text{size} = \beta_2 + 1) \Rightarrow \\
\quad (|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1)) \\
\quad \vee (|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1)) \\
\quad \vee \bigvee_{i \in [1, n]} (|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1)) \quad (\wedge \mathbf{I}) \text{ and } (\wedge \mathbf{V}), 4 \\
6 \quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1 \Rightarrow |Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 2 \quad \text{previously derived} \\
7 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \Rightarrow \\
\quad |Q_1 \wedge Q, \dots, Q_n] \wedge |Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 2 \quad (\wedge \mathbf{I}), 6 \\
8 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge |Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 2 \Rightarrow \perp \quad (\mathbf{G}_3^*) \text{ and } (\wedge \mathbf{E}) \\
9 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \Leftrightarrow \perp \quad (\Rightarrow \mathbf{T}) \text{ and } (\perp \mathbf{I}), 7, 8 \\
10 \quad (|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1 \Rightarrow \\
\quad |Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 2 \quad \text{previously derived} \\
11 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \Rightarrow \\
\quad |Q_1 \wedge Q, \dots, Q_n] \wedge |Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 2 \quad (\wedge \mathbf{I}), 10 \\
12 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge |Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 2 \Rightarrow \perp \quad (\mathbf{G}_3^*) \text{ and } (\wedge \mathbf{E}) \\
13 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \Leftrightarrow \perp \quad (\Rightarrow \mathbf{T}) \text{ and } (\perp \mathbf{I}), 11, 12 \\
14 \quad (|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1)) \\
\quad \vee (|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1)) \\
\quad \vee \bigvee_{i \in [1, n]} (|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1)) \Rightarrow \\
\quad (|Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1)) \vee \perp \vee \bigvee_{i \in [1, n]} \perp \quad \mathbf{R0}, 9, 13 \\
15 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge (((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq 1) * \text{size} = \beta_2 + 1) \Rightarrow \\
\quad |Q_1 \wedge Q, \dots, Q_n] \wedge ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \quad (\Rightarrow \mathbf{T}) \text{ and } (\top \mathbf{I}), 5, 14
\end{array}$$



16	$ Q_1 \wedge Q, \dots, Q_n  \wedge (( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1$	$(\wedge \mathbf{E})$ and $(\wedge \mathbf{C})$
17	$\text{size} = \beta_2 + 1 \Rightarrow \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2$	previously derived
18	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	$*$ -introduction rule and $(\mathbf{COM})$ , 17
19	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$	
	$( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * ( Q  \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	$(\mathbf{G}_{26}^*)$
20	$ Q_1 \wedge Q, \dots, Q_n  \wedge (( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * \text{size} = \beta_2 + 1) \Rightarrow$	
	$( Q_1, \dots, Q_n  \wedge \text{size} \geq \beta_1 + 1) * ( Q  \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	repeated $(\Rightarrow \mathbf{T})$ , 16, 18, 19

We now focus on the two remaining types of formulae. Let  $|Q_1 \wedge Q, \dots, Q_n \overline{\neg}|$  be either  $|Q_1 \wedge Q, \dots, Q_n|$  or  $|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}|$ , for some  $i \in [1, n]$ . Then:

1	$ Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * \text{size} \geq \beta_2$	previously derived, $\#( Q_1, \dots, Q_n ) \leq \beta_1 + 1$
2	$\text{size} \geq \beta_2 \Rightarrow \text{size} = \beta_2 * \text{size} \geq 0$	$(\mathbf{S}_5^*)$
3	$( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * \text{size} \geq \beta_2 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * (\text{size} = \beta_2 * \text{size} \geq 0)$	$*$ -introduction rule and $(\mathbf{COM})$ , 2
4	$ Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * (\text{size} = \beta_2 * \text{size} \geq 0)$	$(\Rightarrow \mathbf{T})$ , 1, 3
5	$( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * (\text{size} = \beta_2 * \text{size} \geq 0) \Rightarrow$	
	$(( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * \text{size} \geq 0) * \text{size} = \beta_2$	$(\mathbf{COM})$ and $(\mathbf{ASSOC})$
6	$ Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$	
	$(( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * \text{size} \geq 0) * \text{size} = \beta_2$	$(\Rightarrow \mathbf{T})$ , 4, 5
7	$( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * \text{size} \geq 0 \Rightarrow$	
	$ Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} \geq \beta_1 + 1$	previously derived
8	$ Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} \geq \beta_1 + 1 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} = 1$	$(\mathbf{G}_{28}^*) / (\mathbf{G}_{29}^*)$
9	$( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * \text{size} \geq 0 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} = 1$	$(\Rightarrow \mathbf{T})$ , 7, 8
10	$(( Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} = \beta_1 + 1) * \text{size} \geq 0) * \text{size} = \beta_2 \Rightarrow$	
	$(( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} = 1) * \text{size} = \beta_2$	$*$ -introduction rule, 9
11	$ Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$	
	$(( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} = 1) * \text{size} = \beta_2$	$(\Rightarrow \mathbf{T})$ , 6, 10
12	$(( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * \text{size} = 1) * \text{size} = \beta_2 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * (\text{size} = 1 * \text{size} = \beta_2)$	$(\mathbf{COM})$
13	$ Q_1 \wedge Q, \dots, Q_n \overline{\neg}  \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$	
	$( Q_1 \wedge Q, \dots, Q_n  \wedge \text{size} \geq \beta_1) * (\text{size} = 1 * \text{size} = \beta_2)$	$(\Rightarrow \mathbf{T})$ , 11, 12
14	$\text{size} = 1 * \text{size} = \beta_2 \Rightarrow \text{size} = \beta_2 + 1$	$\mathbf{L4}$
15	$\neg \text{size} \geq \beta_2 + 1 \Rightarrow \neg \text{size} \geq \beta'_2$	repeated $(\mathbf{S}_2^*)$ , $(\mathcal{G}_{Hyp})$
16	$\text{size} = \beta_2 + 1 \Rightarrow \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2$	$(\wedge \mathbf{I})$ , 15
17	$\text{size} = 1 * \text{size} = \beta_2 \Rightarrow \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2$	$(\Rightarrow \mathbf{T})$ , 14, 16

18	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (\text{size} = 1 * \text{size} = \beta_2) \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	*introduction rule and (COM), 17
19	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	( $\Rightarrow$ T), 13, 18
20	$( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	( $\mathbf{G}_{26}^*$ )
21	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	( $\Rightarrow$ T), 19, 20

$$\blacksquare (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Leftrightarrow \gamma_n \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \dot{-} 1$$

( $\Rightarrow$ ):

1	$ Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1) \Rightarrow \gamma_n$	previously derived
2	$( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1)$	<b>L0</b>
3	$( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \gamma_n$	( $\Rightarrow$ T), 1, 2
4	$( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $\neg \text{size} \geq \beta'_1 * \neg \text{size} \geq \beta'_2$	<b>L0</b>
5	$\neg \text{size} \geq \beta'_1 * \neg \text{size} \geq \beta'_2 \Rightarrow \neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1$	( $\mathbf{S}_6^*$ )
6	$( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $\neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1$	( $\Rightarrow$ T), 4, 5
7	$( Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * ( Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow$ $\gamma_n \wedge \neg \text{size} \geq (\beta'_1 + \beta'_2) \dot{-} 1$	( $\wedge$ R), 3, 6

( $\Leftarrow$ ): Again, by propositional reasoning we can distribute the conjunction over the disjunctions and treat separately each disjunct. We then show that the formulae below are derivable in  $\mathcal{H}_c(*)$ :

- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \dot{-} 1$   
 $\Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$
- $|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \dot{-} 1$   
 $\Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$
- For all  $i \in [1, n]$ ,  $|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \dot{-} 1$   
 $\Rightarrow (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$

Let us start with the first one:

1	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1$	previously derived
2	$(( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * \text{size} \geq \beta_2 + 1) \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \dot{-} 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq (\beta'_1 - \beta_1) + \beta'_2 \dot{-} 1)$	<b>L2</b> , $\beta_1 < \beta'_1$
3	$ Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \dot{-} 1 \Rightarrow$ $( Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} = \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq (\beta'_1 - \beta_1) + \beta'_2 \dot{-} 1)$	( $\wedge$ D) and ( $\wedge$ I), 2
4	$\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq (\beta'_1 - \beta_1) + \beta'_2 \dot{-} 1 \Rightarrow$ $(\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2)$	<b>L4</b>

5	$\begin{aligned} & ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} = \beta_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq (\beta'_1 - \beta_1) + \beta'_2 + 1) \Rightarrow \\ & \quad ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} = \beta_1) * \\ & \quad ((\mathbf{size} \geq 0 \wedge \neg \mathbf{size} \geq \beta'_1 - \beta_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2)) \end{aligned}$	*-intro. rule and <b>(COM)</b> , 4
6	$\begin{aligned} & ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} = \beta_1) * \\ & \quad ((\mathbf{size} \geq 0 \wedge \neg \mathbf{size} \geq \beta'_1 - \beta_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2)) \Rightarrow \\ & \quad ( ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} = \beta_1) * (\mathbf{size} \geq 0 \wedge \neg \mathbf{size} \geq \beta'_1 - \beta_1) \\ & \quad * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \end{aligned}$	<b>(ASSOC)</b>
7	$\begin{aligned} &  Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_1 + \beta'_2 + 1 \Rightarrow \\ & \quad ( ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} = \beta_1) * (\mathbf{size} \geq 0 \wedge \neg \mathbf{size} \geq \beta'_1 - \beta_1) \\ & \quad * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \end{aligned}$	repeated <b>(<math>\Rightarrow</math>T)</b> , 3, 5, 6
8	$\begin{aligned} & ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} = \beta_1) * (\mathbf{size} \geq 0 \wedge \neg \mathbf{size} \geq \beta'_1 - \beta_1) \Rightarrow \\ & \quad ( Q_1 \wedge Q, \dots, Q_n] \vee  Q_1 \wedge Q, \dots, Q_n) \vee \bigvee_{i \in [1, n]}  Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \\ & \quad \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1 \end{aligned}$	previously derived
9	$\begin{aligned} & ( ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} = \beta_1) * (\mathbf{size} \geq 0 \wedge \neg \mathbf{size} \geq \beta'_1 - \beta_1) \\ & \quad * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \Rightarrow \\ & \quad ( ( Q_1 \wedge Q, \dots, Q_n] \vee  Q_1 \wedge Q, \dots, Q_n) \vee \bigvee_{i \in [1, n]}  Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \\ & \quad \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \end{aligned}$	*-introduction rule, 8
10	$\begin{aligned} & ( ( Q_1 \wedge Q, \dots, Q_n] \vee  Q_1 \wedge Q, \dots, Q_n) \vee \bigvee_{i \in [1, n]}  Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \\ & \quad \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \Rightarrow \\ & \quad ( ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \\ & \quad \vee ( ( Q_1 \wedge Q, \dots, Q_n) \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \\ & \quad \vee \bigvee_{i \in [1, n]} ( ( Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) \\ & \quad * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) ) \end{aligned}$	<b>(<math>\wedge</math>C)</b> and <b>(<math>*</math>DISTR)</b>
11	$\begin{aligned} &  Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_1 + \beta'_2 + 1 \Rightarrow \\ & \quad ( ( Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \\ & \quad \vee ( ( Q_1 \wedge Q, \dots, Q_n) \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \\ & \quad \vee \bigvee_{i \in [1, n]} ( ( Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) \\ & \quad * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) ) \end{aligned}$	repeated <b>(<math>\Rightarrow</math>T)</b> , 7, 9, 10

Similarly to what is proved in the right-to-left direction of the previous case of this lemma, the two following formulae can be derived in  $\mathcal{H}_c(*)$ , essentially by relying on the axioms **(G<sub>3</sub><sup>c</sup>)** and **(G<sub>4</sub><sup>c</sup>)**:

- $|Q_1 \wedge Q, \dots, Q_n] \wedge ( (|Q_1 \wedge Q, \dots, Q_n) \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) ) \Rightarrow \perp$
- $|Q_1 \wedge Q, \dots, Q_n] \wedge ( (|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) ) \Rightarrow \perp$

Hence, by propositional reasoning it is possible to show a derivation in  $\mathcal{H}_c(*)$  of

$$\begin{aligned} 12 \quad & ( ( (|Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \\ & \quad \vee ( (|Q_1 \wedge Q, \dots, Q_n) \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \\ & \quad \vee \bigvee_{i \in [1, n]} ( (|Q_1 \wedge Q, \dots, \overline{Q_i}, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) \\ & \quad * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) ) ) \wedge |Q_1 \wedge Q, \dots, Q_n] \Rightarrow \\ & \quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \end{aligned}$$

which then allows us to conclude.

$$\begin{array}{l|l}
13 & |Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \div 1 \Rightarrow \\
& \left( (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \right) \\
& \vee (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \\
& \vee \bigvee_{i \in [1, n]} (|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) \quad (\wedge \mathbf{D}) \text{ and } (\wedge \mathbf{I}), 11 \\
14 & (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (\text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \Rightarrow \\
& (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \quad (\mathbf{G}_{26}^*) \\
15 & |Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \div 1 \Rightarrow \\
& (|Q_1, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * (|Q] \wedge \text{size} \geq \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_2) \quad \text{repeated } (\Rightarrow \mathbf{T}), 12, 13, 14
\end{array}$$

We now focus on the two remaining types of formulae. Let  $|Q_1 \wedge Q, \dots, Q_n \overline{]}]$  be either  $|Q_1 \wedge Q, \dots, Q_n \overline{]}]$  or  $|Q_1 \wedge Q, \dots, \overline{Q_i, \dots, Q_n}]$ , for some  $i \in [1, n]$ . Then:

$$\begin{array}{l|l}
1 & |Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \Rightarrow \\
& (|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * \text{size} \geq \beta_2 \quad \text{previously derived} \\
2 & |Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \div 1 \Rightarrow \\
& ((|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * \text{size} \geq \beta_2) \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \div 1 \quad (\wedge \mathbf{I}) \text{ and } (\wedge \mathbf{C}), 1 \\
3 & ((|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * \text{size} \geq \beta_2) \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \div 1 \Rightarrow \\
& (|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq (\beta'_1 - \beta_1) + \beta'_2 \div 2) \quad \mathbf{L2}, \beta_1 < \beta'_1 \\
4 & \text{size} \geq \beta_2 \wedge \neg \text{size} \geq (\beta'_1 - \beta_1) + \beta'_2 \div 2 \Rightarrow \\
& (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2 - 1) \quad \mathbf{L4}, \beta'_2 \geq 2 \\
5 & (|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq (\beta'_1 - \beta_1) + \beta'_2 \div 2) \Rightarrow \\
& (|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * \\
& ((\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2 - 1)) \quad \text{*introduction rule and } (\mathbf{COM}), 4 \\
6 & (|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * \\
& ((\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) * (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2 - 1)) \Rightarrow \\
& ((|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) * \\
& (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2 - 1) \quad (\mathbf{ASSOC}) \\
7 & |Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \text{size} \geq \beta'_1 + \beta'_2 \div 1 \Rightarrow \\
& ((|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) * \\
& (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2 - 1) \quad \text{repeated } (\Rightarrow \mathbf{T}), 2, 3, 5, 6 \\
8 & (|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) \Rightarrow \\
& |Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + 1 \wedge \neg \text{size} \geq \beta'_1 + 1 \quad \text{previously derived} \\
9 & |Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + 1 \Rightarrow (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * \text{size} = 1 \quad (\mathbf{G}_{28}^*) / (\mathbf{G}_{29}^*) \\
10 & |Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} \geq \beta_1 + 1 \wedge \neg \text{size} \geq \beta'_1 + 1 \Rightarrow \\
& ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * \text{size} = 1) \wedge \neg \text{size} \geq \beta'_1 + 1 \quad (\wedge \mathbf{I}) \text{ and } (\wedge \mathbf{C}), 9 \\
11 & ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1) * \text{size} = 1) \wedge \neg \text{size} \geq \beta'_1 + 1 \Rightarrow \\
& (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * \text{size} = 1 \quad \mathbf{L2} \text{ and } (\mathbf{COM}) \\
12 & (|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) \Rightarrow \\
& (|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * \text{size} = 1 \quad \text{repeated } (\Rightarrow \mathbf{T}), 8, 10, 11 \\
13 & ((|Q_1 \wedge Q, \dots, Q_n \overline{]}] \wedge \text{size} = \beta_1 + 1) * (\text{size} \geq 0 \wedge \neg \text{size} \geq \beta'_1 - \beta_1) * \\
& (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2 - 1) \Rightarrow \\
& ((|Q_1 \wedge Q, \dots, Q_n] \wedge \text{size} \geq \beta_1 \wedge \neg \text{size} \geq \beta'_1) * \text{size} = 1) * \\
& (\text{size} \geq \beta_2 \wedge \neg \text{size} \geq \beta'_2 - 1) \quad \text{*introduction rule, 12}
\end{array}$$

$$\begin{array}{l}
14 \quad ( (|Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * \mathbf{size} = 1 ) * \\
\quad (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2 - 1) \Rightarrow \\
\quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * \\
\quad (\mathbf{size} = 1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2 - 1)) \quad \text{(ASSOC)} \\
15 \quad \mathbf{size} = 1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2 - 1) \Rightarrow \mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2 \quad \text{L4} \\
16 \quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * \\
\quad (\mathbf{size} = 1 * (\mathbf{size} \geq \beta_2 \wedge \neg \mathbf{size} \geq \beta'_2 - 1)) \Rightarrow \\
\quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \quad \text{*introduction rule and (COM), 15} \\
17 \quad (|Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (\mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \Rightarrow \\
\quad (|Q_1, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (|Q] \wedge \mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \quad \text{(G}_{26}^*) \\
18 \quad |Q_1 \wedge Q, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 + \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_1 + \beta'_2 \div 1 \Rightarrow \\
\quad (|Q_1, \dots, Q_n] \wedge \mathbf{size} \geq \beta_1 \wedge \neg \mathbf{size} \geq \beta'_1) * (|Q] \wedge \mathbf{size} \geq \beta_2 + 1 \wedge \neg \mathbf{size} \geq \beta'_2) \quad \text{repeated } (\Rightarrow \mathbf{T}), 7, 13, 14, 16, 17
\end{array}$$

This completes the proof.