Qualitative Spatial Reasoning with Super-Intuitionistic Logics

by

Paolo Torrini

Submitted in accordance with the requirements
for the degree of Doctor of Philosophy.

The University of Leeds
School of Computing

September 2003

Abstract

Topology is used in many applications that may benefit from the automation of spatial reasoning, notably in geographic information systems and in graphics. Reasoning about topology is known to be intrinsically complex, and difficult to be dealt with by a machine. Qualitative formalisms for spatial reasoning, region-based approaches based on mereotopology, encodings based on non-classical logics are some of the possible answers that have emerged in connection with this problem.

The present analysis is based on the well-known topological semantics of intuitionistic logic. That semantics is considered here from the point of view of the representation of spatial knowledge, and accordingly extended, in order to allow more naturally the expression of simple topological descriptions. Special attention is given to the formal modelling of digital representation, to the logical encoding of connectivity relations, to the concepts of granularity and dimension.

The formalisations that are investigated are based on some extensions of intuitionistic propositional logic. These can be obtained by adding to the basic logic propositional quantifiers, intuitionistic modalities and intermediate axioms. A proof-checking tool for some of these logics has been developed, by formalising them in Isabelle-HOL, an interactive theorem-prover based on classical higher-order logic. A partial decidability result is given for an extension of intuitionistic second-order propositional logics, together with an account of its mechanisation.

I would like to thank my advisors, John Stell and Brandon Bennett at the University of Leeds, and Jacques Fleuriot at the University of Edinburgh, without whom this work would have not been possible. I wish to express my gratitude to Anthony Cohn for his advice and for the constant support that he gave throughout my permanence in Leeds. I would like to thank Ewen Denney for plenty of discussion, Alan Smaill and Ian Pratt for oral and written comments, Mike Smyth, Alan Bundy and Roy Dyckhoff for workshop feedback. I would like to thank Fairouz Kamareddine for a stimulating summer school and for the encouragement that she gave on that occasion. Beyond those mentioned, I would like to include in my thanks the people of the Mathematical Reasoning Group at the University of Edinburgh, for their hospitality during an extended visit, the members of the Formal Methods Group at the University of Bremen, where I could finish writing this thesis, the Postgraduate Tutor and the computing staff of the School of Computing at Leeds. Finally, I wish to thank my mother and my father.

This PhD project has been funded by the ESPRC grant GR/M56807 on "Managing Vagueness, Uncertainty and Granularity in Spatial Information Systems".

Contents

List of Figures

Chapter 1

Introduction

The modelling of spatial information, and especially of the geographical one, typically involves relationships with the actual data, with an abstract geometry, as well as with the digital representation of both on a computer. Within a certain system, spatial information can be associated to a set of graphical or abstract data about some spatial entities. The "chunks" of space — or *regions* — corresponding, up to some indeterminacy, to the locations of physical objects, are often among the most significant of those entities. The regions may be either those described, with possible vagueness, by common sense expressions such as "West Yorkshire", "the North of England", "the safest region to build a bridge". Or else, given appropriate forms of measurement, they may be defined instrumentally, by associating them to sensor inputs.

From an abstract, geometrical point of view, the continuous space — either in two or in three dimensions — can be represented as a vector space, i.e. as a product of real numbers with its associated metric topology [RHB02, Kel55]. Regions can be associated to topological sets of some sort.

From the computational point of view, regions are objects that either can be stored explicitly, or else can be inferred from the stored data. Models that take regions into account, may generally be one of two main kinds [LT92]:

1. In a *raster model*, the domain is associated to a system of coordinates, and it is divided into a set of discrete units (or atomic regions) individuated by their position in the system. Graphically, those units may be pixels. Regions are just clusters of such units, characterised by some common attribute. These models are often associated to the representation of sensor input.

2. In a *vector model*, regions can be stored explicitly, with their geometry and

their properties as attributes. In order to obtain a graphical representation, the model must be associated to a discretisation of the continuous space, i.e. to a mesh, based on a decomposition into units that in two dimensions may be triangles, squares, hexagons, etc..

All the computer representations are ultimately digital, either in an immediate sense (as in the case of raster models) or indirectly (as in the other one). Rasters as well as discretisations are essentially meshes (i.e. partitions of the space), and so they can be usually associated to some notion of granularity (or level of detail), since in fact, in every mesh, all the points that fall inside the same unit can be identified.

1.1 Spatial reasoning and topology

From the point of view of spatial reasoning, the common AI idea of drawing a distinction between an abstract, qualitative level and a numerical one, fits in quite well with the distinction between geometry and topology. It is sometimes possible to deal with non-numerical information more efficiently, by storing it separately and by processing it independently [Wor95]. In general, a topological account of the spatial information which is available can capture many of the geometrical properties that do not involve distance, including an abstract notion of dimension (i.e. topological dimension). Moreover, in every digital representation, once the geometry of the atomic elements is fixed, a complete knowledge of the topology gives a complete knowledge of the geometry. For these reasons, topology appears to define a natural level of description, at which it is comparatively feasible to check inferences and detect inconsistencies, whenever we need to examine the information stored into a data-base, or the high-level design of a certain spatial system.

At an abstract level, topology introduces us to the mathematical concept of space. The definition of topological space is based on the notion of *open* set (or dually, on that of *closed* set). This concept can be introduced in different, equivalent ways, either relying on a set-theoretical, point-based definition, or on an algebraic, point-free notion of *interior* (dually, on one of *closure*) (see Chapter 2).

Topology can be used in order to express qualitative information related to regions in a map, and in particular, information about "connectivity" — this includes properties of regions as well as relations between them — for example, the knowledge whether two regions are interconnected (i.e. connected with each other), whether they are overlapping, whether one of them is part of the other, how many connected parts a region is made of, etc.. A significant example for a topological taxonomy is given by the so-called $RCC8$ relations (introduced in [RCC92]; treated in Section 4.2).

Although topological information seems to be easier to handle, at least in principle, than the geometrical, numerical one, topological reasoning can be still quite hard. Point-set topology is inherently second-order, at the very least, as it involves properties of subsets. This can make the task of mechanising inference quite difficult — for example, already the problem of second-order instantiation is NP-hard, whereas first-order unification has polynomial complexity [GJ79]. Point-free alternatives such as those in [Sam89, FG82] have been introduced in order to dispense with the second-order character of point-set topology. More generally, efficient representations that may be appropriate for specific aspects and problems have been pursued, using different logical approaches [CDF95, CBGG97, PH02, VDDB02]. Some of them are based on non-classical logics — examples can be found in [Ben96, LP96, AvB02, She99].

For sure, there are non-topological notions that are qualitatively significant — a notable example is convexity — and there are qualitative languages, as well as spatial logics, that include non-topological notions [BGM96, BCTH00b, CBGG97, LP96, Aie02, BDCTV97, Ven99, KSS+03]. On the other hand, [PS98] shows that, for any system that has a complete semantics, an axiomatisation of connection and one of convexity together are enough to give affine geometry. This leads to a level of expressiveness and of complexity that can be critical from the point of view of an application. Hence in this thesis, I will restrict to qualitative notions that can be expressed by topology.

1.2 Regions

Treating regions point-wise can be costly, especially in presence of incomplete information. A possible alternative is to take regions as primitives. This leads to an interest in the development of region-based qualitative languages [CH01].

From a topological point of view, the intuitive notion of region seems to be captured as that of a set with a non-empty interior (in contrast with "extensionless" points) and with no lower-dimensional features. In an n-dimensional space, a region can be an n-dimensional subspace, regardless of any lower-dimensional feature (such as, in the two-dimensional case, are cracks and dangling lines). A simple way to enforce this requirement is to take regions to be non-empty, regular open sets [RCC92] (see the discussion in Chapter 5).

From an abstract point of view, the fact that there can be undenumerably many regular open sets in a space makes it possible to argue that regions may not be generally definable in an effective way. However, it can be interesting to consider regions in a computational perspective, as objects that arise out of some constructions. In this sense, some form of effectiveness is required — regions should be defined without stretching the bounds of what is computationally feasible.

From the linguistic point of view, effectiveness can be interpreted as definability. In this sense, it should be required that each region can be defined by a finite expression in a language made of denumerable symbols. So, keeping into account logical equivalence, each region should be associated to an equivalence class over a denumerable set of expressions. Since every partition over a denumerable set is denumerable, regions turns out to be denumerable as well.

From a graphical point of view, expressiveness can be interpreted as the possibility to associate each configuration to a simple sketch. Given a space of finite dimension, each of the configurations induced by a finite number of regions, should be exemplifiable without shifting to an infinitesimally detailed picture.

Neither of these two forms of effectiveness are generally satisfied by the definition of regions as regular open sets (see the discussion in Section 4.1.2 and in Section 5.3.2).

A significant point on which abstract, continuous representations of regions and digital ones diverge with each other, is whether there should be atomic regions or not, i.e. whether regions with no smaller non-empty parts should be admitted in the spatial ontology, or, on the contrary, whether every region should be indefinitely sub-dividable. Some of the systems presented in [MV99, RS02] are compatible with atomic regions, whereas the systems in [RCC92, PS98] are not.

Here I would like to consider regions including the aspect of their digital realisation. Hence, I will concentrate on models that are either compatible with atoms, or indeed based on atoms — the latter ones may also be called *atomic* models.

1.3 Region-based formalisms based on predicate calculus

A fragment of topology that is relevant from the qualitative point of view can be presented as an ontology — i.e. as a domain of objects, equipped with operators and relations over them. The objects here can be identified with the spatial regions. The operators can be either topological ones (such as interior, closure and regularisation) or plainly set-theoretical ones (such as union, intersection and complement). The relations and the properties must be topological ones (such as overlapping, interconnection and connectedness). Such an ontology can be described logically as a first-order theory. The general characteristics of such a theory may then be summed up as follows:

- Regions are represented by individual variables and terms.
- Topological operators (such as $\sqcap, \sqcup, -$) are represented by functions.
- Topological relations are represented by predicates.
- Logical operators (such as $\wedge, \vee, \sim$) are those of classical first-order logic.

Mereology is a theory of the relation between an object — as a whole — and its parts (i.e. of the *part* relation), as opposed to the set-theoretic notion of membership [Leś31, CV98]. Mereology fits quite naturally in the foundations of the region-based approach, as it requires no shift in abstraction between a whole and its parts. The spatial theories built on mereology are also called *mereotopologies*. They are usually based on classical logic, and they can be intererpreted in terms of point-set topology, where the part relation is associated to set-theoretical inclusion. Extensions of mereotopology, usually higher-order ones, can lead to region-bassed geometry — [Ger95] gives a survey. Also the theory presented in [BCTH00b] and developed in [BCTH00a] moves in this direction.

A differently motivated, although potentially related branch of point-free reasoning, is that originating from the formal approaches to topology based on algebra and logic [Joh82, FG82, Vic89, Sam89], where the notion of open set (or simply of *open*) is taken as primitive. These are often based on constructive logics — usually intuitionistic logic, although [Vic89] introduces also a more specific *geometric* logic.

In the classical mereotopological theory presented in [Cla81], regions can be interpreted as non-empty regular open sets. Relations over the regions are introduced axiomatically. The part relation is axiomatised by a binary predicate as a reflexive, transitive relation. The connection relation (i.e. interconnection) is axiomatised by a binary predicate as a reflexive, symmetric relation that also holds, for each region, between it and its complement. The topological notion of closure can be defined.

The system in [PS98] presents a complete axiomatisation for mereotopogy, where connectedness is taken as the primitive notion. The regions are still interpreted as regular open sets — but there are additional restrictions related to dimension and to a form of graphical effectiveness (see the discussion in Section 5.3.2). This system, resting on standard finitary rules as well as on an infinitary one, is proved to be complete with respect to its topological semantics.

The system presented in [RCC92] (the *region connection calculus RCC*) is a simplified version of standard mereotopology. No distinction between open and closed sets is admitted in the models, in explicit contrast with [Cla81], hence forbidding a duplication of the spatial entities that may lead to counter-intuitive consequences and that may unnecessarily complicate the ontology. The connection relation is the only primitive — the part relation can be defined, relying on quantification over the regions. The axiomatisation of interconnection is quite similar to that given in [Cla81] — however, in *RCC* it is also necessary to assume that, for each region, there is another one which is not connected with it. This leads to the inadmissibility of atomic regions. *RCC* has models based on connected normal spaces where individual variables are interpreted as regular open sets (i.e. the regions). Since atoms are not admissable, *RCC* does not allow digital models [Ren98].

A considerable amount of work has evolved around *RCC*. In particular, [Ste00a] has highlighted the relationship between mereotopological systems close to *RCC* and point-free topology. [RS02] has introduced alternatives to *RCC* that are compatible with digital spaces. [Ben98, Ben96] have considered the relationship between the quantifier-free fragment of *RCC* based on the *RCC*8 relations and non-classical logics. [WZ00, WZ02, RN99, RN98, Ben98] have investigated computational aspects. [CBGG97, CG96] have investigated the application of *RCC* to GIS, extending the system in order to handle spatial objects with indeterminate boundaries either.

1.4 Non-classical logics

Non-classical logics include logics that are weaker than the classical one, as well as logics that can be obtained by extending the classical language with new operators. In both cases, a gain in expressiveness is obtained, by allowing for larger collections of non-equivalent propositions.

In classical logic, the structure of propositions can be associated to Boolean algebras, and hence ultimately to two truth-values. This makes classical logic particularly simple and versatile, especially for first-order and higher order reasoning. However, by resorting to logics that have a richer propositional structure, it is sometimes possible to encode domain-specific knowledge (temporal, spatial, epistemic, etc.) at the propositional level. There are cases in which this turns out to be useful from the point of view of knowledge representation, by making it possible to model specific notions, in comparatively simple ways [GKWZ03, BCWZ02].

Intuitionistic logic is weaker than the classical one, and in fact it distinguishes between formulæ that are classically equivalent. The propositional structure can be associated to Heyting algebras — a generalisation of Boolean algebras that do not generally admit any reduction to a finite number of values [RS63].

Intuitionistic logic has been widely investigated, at different levels (propositional, first-order, higher-order) given its interest as a logic of provability for constructive mathematics, as well as its relationship with type theory [Fit69, Bar92].

An intuitionistic second-order propositional logics (ISPL) is a logic that can be obtained by extending intuitionistic propositional logic (*IPL*) with quantification that ranges over formulæ. In contrast with *IPL*, ISPLs are generally undecidable. An ISPL can be associated to the basic system of polymorphic types (one in which type variables are allowed [Bar92]).

Modal and multi-modal logics, mostly treated at the propositional level, are usually based on classical logic, i.e. they are obtained by adding modal operators — "boxes" ($\Box$) and "diamonds" ($\Diamond$) — to a classical language [Che80]. Intuitionistic modal and multi-modal logics, on the other hand, can be obtained by extending with modal operators an intuitionistic language [WZ99].

Non-classical logics can be associated to formal, model-theoretic semantics. These semantics can be sometimes associated to the modelling of specific domains of knowledge. Formal semantics can also be useful from the point of view of theorem proving, insofar as they can give a better understanding of the reasoning techniques that can be applied to a logic.

Kripke semantics is an intuitive and versatile formal approach to model theory for non-classical logics. A Kripke model is given by a *frame* — a set of points with some binary relations called *accessibility* relations — together with a notion of *truth* (or *forcing*) of a formula at a point, and an *interpretation* for the logical symbols. Most of the logics, and certainly all of those that are considered here, can be associated to Kripke semantics. Classically, each accessibility relation corresponds to a box-diamond pair of operators. The truth of $\Box\alpha$ at a point $\mathtt{p}$ represents the truth of the formula α at all the points that are accessible from $\mathtt{p}$. Dually, the truth of $\Diamond\alpha$ at a point $\mathtt{p}$ represents the truth of the formula α at some of the points that are accessible from $\mathtt{p}$. The modal logic *S4* can be associated to the frames where the accessibility relation is a partial order (or also, more generally, a preorder). The modal logic *S5* can be associated to frames where accessibility is an equivalence relation. The interpretation of *S5* is said to be *strong*, whenever each model is just a single equivalence class — it is said to be *weak* otherwise. The frames for intuitionistic logic and its extensions are quite similar to those for *S4* — the only significant difference being in the fact that in the intuitionistic case it is possible, and usually preferred, to restrict to the orders that have a minimum. Moreover, unlike *S4*-models, intuitionistic ones satisfy the *hereditary condition* — i.e. for each point, the truth of a formula at that point is preserved at every point above it.

The relationship between intuitionistic logic and S4 is a close one, and so is the relationship that they both have with topology. *IPL* can be embedded in *S4*, and so, *S4* can be regarded as a conservative extension of *IPL* [Gab81]. Both intuitionistic logic and *S4* have a well-known topological semantics that was introduced in [Tar56, MT48] and extended to the first-order case in [RS63]. A model is given by a topological space together with an interpretation of the formulæ as subspaces. Each logical symbol becomes associated to a topological operator. In particular, the *S4* box operator can be associated to the topological interior, whereas the *S4* diamond operator can be associated to the topological closure. In the case of intuitionistic logic, all the formulæ are interpreted as open sets — this corresponds to the hereditary condition, as well as to the fact that, when *IPL* is embedded into *S4*, every intuitionistic formula α is mapped to a modal formula $\Box\alpha$.

Whenever a modal logic is complete with respect to a class of Kripke frames that can be defined in terms of first-order expressions, this also gives a way of embedding that logic into first-order predicate calculus.

Most of the existing spatial logics are modal logics in which the modal operators are given a spatial interpretation — either in a geometrical sense or in a purely topological one [JAN02, GKWZ03, LP96, AvB02]. The spatial content of some of these logics is based on a spatial characterisation of the accessibility relations in their Kripke semantics. Different accessibility relations can then be used to represent different spatial relations — for example, nearness and connection in [LP96], incidence in [BDCTV97]. The systems presented in [Ben96, AvB02], on the other hand, are based on topological semantics. The basic logic in [AvB02] takes advantage of the expressiveness allowed by *S4*, whereas [Ben96] rests closer to *RCC* in banning the open-closed distinction.

1.5 Spatial representation in non-classical logic

There are different senses in which it is possible to encode into a non-classical logic a constraint that describes some spatial configuration. Let C be the constraint stating that the n-ary relation R holds between the open sets $A_1, \ldots, A_n$.

It is possible to represent C, in a *weak* sense, whenever there exist some formulæ $\alpha_1, \ldots, \alpha_i, \beta_1, \ldots, \beta_j$, such that the configurations characterised by C are represented by the models in which $\alpha_1, \ldots, \alpha_i$ are satisfied and $\beta_1, \ldots, \beta_j$ are not. In this case, it can be said that C is *encoded* into the logic at the *meta-level*.

On the other hand, C can be represented in a *strong* sense, whenever there exists a formula α, such that the configurations characterised by C are represented by the models that satisfy α. In this case, it can be said that C is encoded into the logic at the *object-level*, and α can be called a representation of C.

In the theories based on classical logic, no such difference between weak and strong encoding arises, since classically, a model does not satisfy a formula if and only if it satisfies the negation of that formula.

The question whether there exists a model in which a certain formula is satisfied (or valid) is also said to be a *satisfiability* problem. The question whether, given a generic model that satisfies some formulæ, that model also satisfies some other formulæ, for the logics that are being treated here, can be regarded as an *inference* problem.

Practically, a basic question that may be asked is whether there exists a configuration in which a certain constraint holds. In case the constraint is encoded weakly, answering positively this question resolves into showing that some formula is satisfiable, and that some inference is not provable [Ben97]. Hence, a meta-level encoding can be practically useful particularly insofar as it is based on a decidable formalism. In the case of an object-level encoding, the same question reduces to a satisfiability problem — but then, also in this case proving a theorem in the logic will not be generally enough to give an answer, unless the answer is negative.

The question whether a certain constraint holds in every configuration that satifies a certain set of constraints, turns out to be hard to express when the constraints are just weakly encoded. When all of them are strongly encoded though, this question reduces to an inference problem. In this case, if the answer is positive then it can be obtained by means of theorem proving, even if the formalism is undecidable.

In contrast with the first-order theories considered in Section 1.3, the general characteristics of propositional encodings (based on intuitionisitc, modal, multi-modal logics) may be summarised as follows:

- Regions are represented by propositional variables.
- Topological operators are represented by logical operators.
- Topological relations are represented by formulæ with free variables.

The theories based on predicate logic have in general the advantage of offering perspicuous axiomatisations, with a clear distinction between the logical machinery and the spatial predicates. On the other hand, an encoding based on a non-classical logic yields for free a theory of space embedded into the logic. Hence, proving the correctness and the completeness for the logic is enough to guarantee also the consistency and the completeness for the spatial theory. Anyway, the contrast between non-classical logic and first-order theories should not be taken as something running too deep: as already remarked, many modal logics can be embedded into first-order predicate calculus.

1.6 Intuitionistic encodings

1.6.1 Previous work

The application of topological semantics to spatial reasoning that rests closer to this thesis has been introduced in [Ben97, Ben96, Ben98], where a tractable solution to a significant problem is obtained by encoding the *RCC*8 fragment of *RCC* in *IPL*. Intuitionistic logic is one of the simplest formalisms in which a qualitatively significant fragment of topology can be expressed. The notion of topological regularisation can be represented intuitionistically — as double negation — and hence it is possible, in the models, to represent regions as regular open sets. In contrast with *S4*, the fact that the distinction between open and closed sets is not represented in intuitionistic logic, matches quite naturally the *RCC* approach. Moreover, by assuming that the regions in a model are those sets that can be represented by the language, one aspect of effectiveness — i.e. denumerability — turns out to be enforced quite immediately. In contrast with *RCC*, atomic as well as finite models are admissable.

The *IPL* encoding turns out to be quite efficient, in terms of implementation, but it is not very expressive. Topological definitions involving quantification cannot be expressed in general — these include notions such as those of connected region and of atomic region, as well as other ones related to qualitative aspects of connectivity, granularity and dimension (see Chapter 5). The $RCC8$ relations can be only weakly encoded in *IPL*. This encoding can be lifted to an object-level one by using, instead, a multi-modal logic based on *S4* and strong *S5* — i.e. the logic $S4_u$ in [Ben96]. However, this shift appears to reintroduce into the logical representation a considerable amount of semantical redundancy that *RCC* wanted to avoid — that is, the open-closed duplication of spatial entities.

1.6.2 Present work

In this work, I will focus on spatial representation for theorem proving by means of encodings into extensions of *IPL* (or super-intuitionistic logics, as mentioned in the title) that are presented in Chapter 3. These encodings extend significantly Bennett's result from the point of view of expressiveness. An object level encoding of the $RCC8$ relations that is based on a modal extension of intuitionistic logic, rather than on a classical multi-modal logic, is presented in Section 5.3.4. Propositional quantification, in the second-order extensions of *IPL*, is used to express quantification over regions. A simple specification language for topological relations is introduced (Section 4.1.2), and later used (Chapter 5) in order to express notions related to the modelling of granularity (Section 4.3), connectivity, graphical effectiveness and dimension. It is also suggested how a weaker modality could be used in order to deal with an idea of multiple views over the same space.

Although expressively quite powerful, propositional quantification, in order to be axiomatised, requires some adaptation for some of the topological notions that are encoded. Moreover, propositional quantification in intuitionistic logic is critical from the point of view of decidability [Gab81], and hence from that of the satisfiability problem. On the other hand, it might be altogether difficult to have connectedness, quantification over regions, and decidability all together, considering the proximity of this case to the undecidability result in [Dor98]. In contrast, the decidable formalism for the $RCC8$ relations and connectedness presented in [PH02] does not have quantification and is based on finite models.

Anyway, a partial decidability result is established, and an effective decision procedure is given for one of the logics (Chapter 6). Some additional remarks about decidability and related computational aspects are contained in the Conclusion.

1.7 An application

1.7.1 Plan and development of the present work

The initial plan for this thesis was to introduce a new formalism, comparable to *RCC* from the point of view of the underlying ontology, more expressive than the encoding of *RCC*8 presented in [Ben96], and capable of representing granular information. With particular respect to granularity, it seemed very important to obtain a formalism that would be compatible with digital models, something that *RCC* is missing (as remarked in Section 1.3). After observing that *IPL* extended with propositional quantification and modalities could be a candidate as a framework for such a formalism, the investigation turned toward the topological expressiveness allowed by some of those extensions, focusing on models that seemed particularly fit to represent granular information. This investigation resulted in the introduction of new logics and of new encodings that are quite satisfactory from the point of view of expressiveness (see the references in Section 1.6.2). However, neither the useful computational properties of the encoding in [Ben96] could be recovered, nor a general decidability result for any of the logics could be reached. On the other hand, the fact that the new formalisms could be useful in order to prove topological properties of computer spatial models, has lead me to consider theorem-proving in ISPLs as a significant application topic.

1.7.2 Mechanisation and theorem proving

Some of the ISPLs that are presented in Chapter 3 have been mechanised (Chapter 7). Lacking a general decision procedure, automated theorem-proving seemed unhelpful. I relied instead on Isabelle, a state-of-the-art interactive theorem prover, widely used in formal methods [Pau96], capable of supporting forward proofs as well as backward, tactic-based ones. In particular, Isabelle-HOL is the Isabelle implementation of classical higher-order logic (*HOL*, [Lei94]), an expressive formalism that has already been used as a logical framework (a significant example is [DG02]). Isabelle-HOL allows considerable freedom in the representation of object logics, as well as a significant degree of semi-automation.

The mechanisation presented in Chapter 7 makes it possible to prove interactively theorems in the basic logics and in their spatial extensions, at the object-level as well as at the meta-level. Via the semantical completeness results, this application may also be regarded, albeit in a limited way, as a proof-tool for a fragment of topology.

Although theorem proving in geometry and topology, as well as their relationship with formal methods, are issues far too wide to be addressed here [Fle01, SVV96], the ultimate rationale behind the present mechanisation is to provide a support to check the validity of topological inferences that can be drawn within a spatial system. Relevant examples of systems could be found in robotics applications that rely on internal spatial representation, such as the one presented in [MRL+00].

The present formalisation of ISPL is based on sequent calculus rules, and takes advantage of the expressiveness of *HOL* with respect to meta-level reasoning. Section 7.4 contains some case-studies in proof-checking. In particular, it has been possible to verify the main step of the decision procedure that is presented in Chapter 6, and, as an example of application to spatial problems, a semantical result discussed in Section 5.2.2.

Chapter 2

Topology

Topology deals with geometric properties that are invariant under continuous transformations, i.e. with notions that do not involve distance — for this reason, it has also been dubbed “rubber-sheet geometry”. For example, the question, whether in a region there is a continuous path between two points, is a topological one, in contrast with the question whether the shortest path between two points lies within a region — hence, connectedness is a topological property whereas convexity is not.

Most of the topological and algebraic notions that are introduced in the following are standard ones (see [RS63, Kel55, Smy92]). As far as the notation is concerned, I refer to Appendix A. I will use $\mathsf{a}, \mathsf{b}, \ldots$ for points, $A, B \ldots$ for sets and for algebraic elements, and $\mathcal{A}, \mathcal{B}, \ldots$ for families of sets and for structures. I will use $\sqcap, \sqcup, \bigwedge, \bigvee, \sqsubseteq$ etc. for the topological notions, also when topological spaces are treated from a set-theoretical point of view, keeping the standard set-theoretical symbols ($\cap, \cup, \bigcap, \bigcup, \subseteq$ etc.) for a more general use.

2.1 Basic notions

A topological space is a pair $\mathcal{S} = (S, \mathcal{O})$, where S is a set, and $\mathcal{O} \subseteq \wp(S)$ is a collection of subsets, called the *open sets* (or simply the *opens*), satisfying the following conditions:

1. $\varnothing, S \in \mathcal{O}$.

2. If $A, B \in \mathcal{O}$ then $A \sqcap B \in \mathcal{O}$.

3. If $\mathcal{Q} \subseteq \mathcal{O}$ then $\bigvee\{X | X \in \mathcal{Q}\} \in \mathcal{O}$.

The set-theoretical complements of the opens are also called the *closed sets* of $\mathcal{S}$, and their class will be normally denoted by $\mathcal{C}$.

A subset in a space is said to be *clopen* whenever it is open and closed. It follows from the definitions that, for any space, S and $\varnothing$ are clopen. The space $\mathcal{S}$ is said to be *discrete* whenever every open set is clopen. It is said to be *connected* whenever the only clopen sets are S and $\varnothing$.

For any $A \in \mathcal{O}$, the pair $\mathcal{S}^A = (A, \mathcal{O}^A)$, with $\mathcal{O}^A = \{X \sqcap A | X \in \mathcal{O}\})$ is called the *restriction* to A of $\mathcal{S}$. It is a routine matter to show that $\mathcal{S}^A$ is a topological subspace of $\mathcal{S}$ [RS63].

The collection $\mathcal{B} \subseteq \mathcal{O}$ is said to be a *basis* for $\mathcal{S}$ iff every $A \in \mathcal{O}$ can be represented as a union of elements of $\mathcal{B}$.

The collection $\mathcal{B} \subseteq \mathcal{O}$ is said to be a *sub-basis* for $\mathcal{S}$ iff there is a basis $\mathcal{B}'$ for $\mathcal{S}$ such that each element of $\mathcal{B}'$ can be represented as an intersection of elements of $\mathcal{B}$.

The elements of a basis (or of a sub-basis) can be regarded, intuitively, as the primitive elements of the topology. A space is said to be *second-countable* whenever it has a denumerable basis,

It may be useful to observe that, even in a second-countable space, the collection of the open sets can be undenumerable, as an effect of the closure w.r.t. arbitrary union. In fact, if the space include infinitely many disjoint, non-empty opens, arbitrary unions of opens can be used to mimic infinite sequences of natural numbers.

2.2 Separation properties

The spaces that are relevant here can be classified in terms of the following *separation properties* [Kel55]. Let $\mathcal{S} = (S, \mathcal{O})$ be a topological space. Then:

1. $\mathcal{S}$ is said to be *regular* iff, whenever $\mathtt{x} \in S$, $A \in \mathcal{C}$ and $\mathtt{x} \notin A$, there exist $X, Y \in \mathcal{O}$ such that $\mathtt{x} \in X$, $A \sqsubseteq Y$ and $X \sqcap Y = \varnothing$.

2. $\mathcal{S}$ is said to be a T_0 space iff for every two points $\mathtt{x}, \mathtt{y} \in S$, $\mathtt{x} \neq y$, there exists $X \in \mathcal{O}$ such that one and only one of the two points is a member of X.

3. $\mathcal{S}$ is said to be a T_1 space iff for every two points $\mathtt{x}, \mathtt{y} \in S$, $\mathtt{x} \neq \mathtt{y}$, there exist $X, Y \in \mathcal{O}$ such that $\mathtt{x} \in X$, $\mathtt{y} \in Y$, $\mathtt{x} \notin Y$ and $\mathtt{y} \notin X$.

4. $\mathcal{S}$ is said to be a T_2 (or *Hausdorff*) space iff it is T_1 and regular.

5. $\mathcal{S}$ is said to be a T_3 (or *normal*) space iff for every disjoint $A, B \sqsubseteq S$, there are disjoint $C, D \in \mathcal{O}$ s.t. $A \sqsubseteq C, B \sqsubseteq D$.

6. $\mathcal{S}$ is said to be *metric* iff it is possible to define a function $d : S * S \mapsto \Re$ (i.e. from pairs of points to the reals), such that $d(\mathtt{a},\mathtt{a}) = 0$, $d(\mathtt{a},\mathtt{b}) = d(\mathtt{b},\mathtt{a})$ and $d(\mathtt{a},\mathtt{b}) \leq d(\mathtt{a},\mathtt{c}) + d(\mathtt{c},\mathtt{b})$, for every $\mathtt{a},\mathtt{b},\mathtt{c} \in S$.

The T_0 property is the most important from the point of view of the spatial representations that are going to be considered in the next chapters. From the point of view of standard geometry, where the space is always meant to be normal — and hence metric — the T_0 separation property is a very weak one. On the other hand, T_0 spaces play a significant role in computer science, as they are compatible with an idea of approximation in information [Vic89]. In the following chapters, a similar idea will play a certain role with respect to the notion of granularity.

2.3 Covering and primeness

Let $\mathcal{S} = (S, \mathcal{O})$ be a topological space.

Definition 1 A family $\mathcal{A}$ of opens in $\mathcal{S}$ is said to *cover* T, where $T \sqsubseteq S$ (or also, to be an *open cover* of T) iff $T \sqsubseteq \bigvee \mathcal{A}$.

A subset $T \sqsubseteq S$ is said to be *compact* in $\mathcal{S}$ iff for every open cover $\mathcal{D}$ of T, there exists a finite subset of $\mathcal{D}$ that covers T. Compactness is essentially a notion that applies when infinite collections are not essential. The following gives a stronger notion, that is going to play a significant role here:

Definition 2 $A \in \mathcal{O}$ is said to be a prime subspace (or simply a *prime*) in $\mathcal{S}$ iff for every open cover $\mathcal{D}$ of A, there exists an open $B \in \mathcal{D}$ such that $A \sqsubseteq B$.

The family $\mathcal{P}$ of the primes in $\mathcal{S}$, elsewhere called *strongly compact open sets* [RS63] and *point-like sets* [FS79], is a subclass of every basis of $\mathcal{S}$ — since essentially, primes are opens that cannot be represented in terms of other elements. A prime space can also be characterised as follows:

Proposition 1 The space $\mathcal{S}$ is prime iff for any indexed family X_I of non-empty opens, $\bigwedge_{i \in I} \mathsf{C}(X_i) \neq \varnothing$.

pf: Since $\bigwedge_{i \in I} \mathsf{C}(X_i) \neq \varnothing$ iff $\bigvee_{i \in I}(-\mathsf{C}(X_i)) \neq S$.

Given a generic space, a simple way to get a prime space is to add an extra point. More precisely ([RS63] chapter 4, par. 5):

Proposition 2 For each space $\mathcal{S} = (S, \mathcal{O})$, $\mathcal{S}$ is an open subspace of a prime space $\mathcal{S}' = (S', \mathcal{O} \cup \{S'\})$, where $S' = S \cup \{\mathtt{p}\}$, with $\mathtt{p} \notin S$.

The space $\mathcal{S}'$ may also be called the *one-point compactification* of $\mathcal{S}$.

2.4 Alexandroff spaces

The relationship between orders and topologies can be a quite close one [Smy92, FS79, Goe71, Gab81, Kop92, TSB02, Tor01]. Let $\mathcal{S} = (S, \mathcal{O})$ be a topological space.

Proposition 3 In $\mathcal{S}$, the following always defines a pre-order on S:
$\mathtt{p} \prec \mathtt{q}$ iff, for any $A \in \mathcal{O}$, if $\mathtt{p} \in A$ then $\mathtt{q} \in A$.
$\prec$ is said to be the *specialisation order* of $\mathcal{S}$ [FS79].

The relations $\prec$ is a partial order whenever $\mathcal{S}$ is a T_0-space, whereas it trivialises to an identity whenever $\mathcal{S}$ is a T_1-space.

The specialisation order has a natural interpretation from the point of view of computer science. If the open sets represent pieces of information, $\prec$ is an order on the information that is available at different points — hence an order on their level of detail.

On the other hand, every order can be associated to a topology. Given a pre-order $(S, <)$, let $\mathcal{U}_<$ be the class of the *upper-closed subsets* of S w.r.t. $<$ — i.e. $X \in \mathcal{U}_<$ iff $X \sqsubseteq S$ and, for every $\mathtt{p} \in S$, if $\mathtt{p} \in X$ and $\mathtt{p} < \mathtt{q}$, then $\mathtt{q} \in X$).

Proposition 4 The structure $\mathcal{T} = (S, \mathcal{U}_<)$ is a topological space, called the *order topology* determined by $<$ on S [FS79].

It is straightforward to observe that the specialisation order of $\mathcal{T}$ is isomorphic to the order relation $<$.

Definition 3 In $(S, <)$, for any $\mathtt{a} \in S$, the smallest upper-closed set that contains $\mathtt{a}$ is said to be the upper-closed *generated* by $\mathtt{a}$, or the *pointed set* of $\mathtt{a}$, and can be denoted by $\mathtt{a}\uparrow$.

Clearly, each point $\mathtt{a}$ can be obtained as the intersection of all the upper-closed sets generated by $\mathtt{a}$, and the specialisation order defined over $\mathcal{T}$ can be expressed in terms of inclusion between pointed sets, since $\mathtt{p} \prec \mathtt{q}$ iff $\mathtt{q}\uparrow \sqsubseteq \mathtt{p}\uparrow$.
Hence, pointed sets can be used to represent the level of detail associated to the corresponding points. Moreover, whenever $<$ is a partial order, the correspondence between the pointed sets and the points is one-to-one, and so the pointed sets turn out to represent exactly the points.

Proposition 5 Let $\mathcal{P}$ be the class of the pointed sets in $(S, <)$. Then:
(a) $\mathcal{P}$ is the class of the primes in $\mathcal{U}_<$.
(b) $\mathcal{P}$ is a basis for the order topology.
(c) The order topology is closed w.r.t. $\bigwedge$.

pf: (a) A pointed set generated by $\mathtt{p}$ cannot be obtained as a join over its proper subsets — otherwise $\mathtt{p}$ would be member of one of them. Vice-versa, only the pointed sets are primes, since every other non-empty upper-closed set can be obtained as the union of its pointed proper subsets, i.e. for every $X \in \mathcal{U}_<$, $X = \bigvee_{\mathtt{a} \in X} (\mathtt{a}\uparrow)$. This also suffices in order to prove b.
(c) Follows from b.

Indeed, the above mentioned properties induce different characterisations for order topologies.

Proposition 6 If $\mathcal{S}$ is an order topology, then it is isomorphic to the order topology determined on S by $\prec$ (i.e. by the specialisation order on $\mathcal{S}$).

pf: Every open set $X \in \mathcal{O}$ can be mapped into the union of the pointed sets of the elements of X (relative to $\prec$). This mapping turns out to be an isomorphism.

A closely related notion is the following one:

Definition 4 The space $\mathcal{S}$ is said to be *Alexandroff* (also $\bigwedge$-closed) iff $\mathcal{O}$ is closed with regards to $\bigwedge$, i.e. iff every arbitrary intersections of open sets is an open set [Kop92].

Open sets in a $\bigwedge$-closed space behave exactly like the closed ones. Alexandroff spaces are just another way to look at order topologies, as shown by the following:

Proposition 7 The space $\mathcal{S}$ is Alexandroff iff it is an order topology.

pf: If a space is isomorphic to an order topology, then it is $\bigwedge$-closed (Proposition 5). On the other hand, if $\mathcal{S}$ is Alexandroff, for any point S, there always exists the smallest open set containing that point (obtained as an arbitrary intersection of opens). Hence it is possible to use the argument of Proposition 6, showing that $\mathcal{S}$ is isomorphic to the order topology determined by $\prec$ on S.

Proposition 8 The space $\mathcal{S}$ is Alexandroff iff the class of its primes $\mathcal{P}$ is a basis.

pf: An Alexandroff space is isomorphic to an order topology, so $\mathcal{P}$ is a basis. On the other hand, if every open set is given as a union of primes, the topology is $\bigwedge$-closed.

It is possible to conclude, then, by saying that order topologies, Alexandroff spaces, topologies that have primes as a basis — are nothing but equivalent notions. From the point of view of the spatial semantics that is going to be developed, the fact that an Alexandroff space can be intuitively associated to a canonical basis, formed by elements which cannot be reduced any further, offers a simple way to model different levels of granularity, i.e. different levels of discretisation of an underlying metric space [Kop92].

2.5 Atomicity

A directed, acyclic graph is said to be *atomic* (or *terminable*) whenever, for each node, either that is a terminal node or there is a finite branch departing from it. The graph can be said to have a *finite depth* whenever all of its branches have finite length. Corresponding notions can be introduced for spaces [Gab81, SW97, TSB02, Tor01]. Let $\mathcal{S} = (S, \mathcal{O})$ be a topological space.

Definition 5 $A \in \mathcal{O}$ is said to be an *atom* in $\mathcal{S}$ iff, for every non-empty $X \in \mathcal{O}$, if $X \sqsubseteq A$ then $X = A$.

Definition 6

1. The space $\mathcal{S}$ is said to have *finite depth* iff, for every chain of opens X_I s.t., for every $i \in I$, $X_i \sqsubset X_{i+1}$, X_I is finite.
2. The space $\mathcal{S}$ is said to be *atomic* (or *terminable* [TSB02]) iff, for every non-empty $A \in \mathcal{O}$, there exists an atom $B \in \mathcal{O}$ such that $B \sqsubseteq A$.

3. The space $\mathcal{S}$ is said to be *anti-atomic* (or *inexhaustible* [SW97]) iff it has no atoms.

Clearly, all atoms are primes. They correspond to the maximal point with respect to the specialisation order, i.e. to those points that can be intuitively associated to the highest level of detail. Moreover, since atoms have no proper parts, although they are not generally clopen, they essentially behave like discrete elements. This suggests the possibility of relying on atomic spaces in order to give an explicit account of the lowest level of a spatial representation (see Section 4.3).

2.6 Topological algebras

An open topology can be introduced algebraically, without relying on sets of points, by adding to a Boolean algebra $(\mathcal{A}, \sqcap, \sqcup, \top, \bot)$ an *interior operator* characterised by the following axioms [RS63, Vic89]:

1. $\mathsf{I}(A \sqcap B) = \mathsf{I}(A) \sqcap \mathsf{I}(B)$
2. $\mathsf{I}(A) \sqsubseteq A$
3. $\mathsf{I}(\mathsf{I}A) = \mathsf{I}(A)$
4. $\mathsf{I}(\top) = \top$

The structure $(\mathcal{A}, \sqcap, \sqcup, \top, \bot, \mathsf{I})$ is then called a *topological Boolean algebra.* A closure operator C can be defined as the dual of I.

For each topological Boolean algebra $\mathcal{A}$, and for each countable collection E of arbitrary meets and joins in $\mathcal{A}$, there is a space $\mathcal{S} = (S, \mathcal{O})$ and an isomorphism between $\mathcal{A}$ and $\mathcal{S}$ that preserves all the elements of E (see [RS63] chapter 4, 4.3).

On the other hand, whenever $(S, \mathcal{O})$ is a topological space (according to the point-based definition), the complete topological Boolean algebra $(\mathcal{O}, \sqcap, \sqcup, \bigwedge, \bigvee, S, \varnothing, \mathsf{I})$ can be obtained, relying on the following definitions:

1. $\mathsf{I}(A) = \bigvee\{X \in \mathcal{O} | X \sqsubseteq A\}$
2. $\mathsf{C}(A) = \bigwedge\{-X | X \in \mathcal{O}, X \sqcap A = \varnothing\}$

So, the topological operators I, C can be used to define new operators, regardless of whether the space has been introduced using points or not. On the other hand, whenever it is not necessary to rely on points, the set-theoretical operations of union and intersection can be regarded, without any loss, as joins and meets over algebraic elements.

A presentation of topology that does not rely on points highlights the relationship with algebra, as well as with modal logic — indeed, there is a close relationship between interior and closure, and the modal operators of the logic *S4* [RS63].

2.7 Topological operators

Let $\mathcal{S} = (S, \mathcal{O})$ be a topological space, and let $A, B \in \mathcal{O}$. The following are some useful topological operators [RS63, Tar56]:

1. $A \Rightarrow B = \bigvee\{X \in \mathcal{O} | X \sqcap A \sqsubseteq B\}$.
   It also holds, in general: $A \Rightarrow B = \mathsf{I}(-A \sqcup B)$.
   Set-theoretically, $A \Rightarrow B$ gives the largest open subspace of $\mathcal{S}$ in which A is included in B.

2. $A^* = A \Rightarrow \varnothing$.
   A^* gives the largest open included in the set-theoretic complement of A.
   The equality $A^* = \mathsf{I}(-A)$ holds in general.

3. $\mathsf{I}(\mathsf{C}(A))$, which is called the *regularisation* (or, more precisely, the *open regularisation*) of A.
   It holds, in general: $\mathsf{I}(\mathsf{C}(A)) = A^{**}$.

4. $A + B = (A \sqcup B)^{**}$, which is called the *regularised union* (or the *sum*) of A and B.

There is a very close relationship between $\Rightarrow, *$ and the algebraic operators that are introduced in the next section (i.e. relative pseudo-complement and pseudo-complement — indeed, I will use the same symbols to denote them).

The following properties, related to regularisation, can be defined:

1. If $A^{**} = A$, we say that A is *regular open*.

2. If $A^{**} = B$, we say that A is *dense* in B.

As noted in the Introduction, regular opens play an important role in the representation of regions.

2.8 Heyting algebras

It is possible to use different algebraic structures in order to represent either topology, or some of its fragments. Here a few classical results are reviewed, before introducing a new one (Proposition 10).

Definition 7

1. The *Heyting algebra* $(\mathcal{A}, \sqcap, \sqcup, \perp, \top, \Rightarrow)$ is the lattice $(\mathcal{A}, \sqcap, \sqcup)$, equipped with the minimum $\perp$, the maximum $\top$ and with the *relative pseudo-complement* $\Rightarrow$ (also called *relative Heyting complement*). This is defined, for every $A, B \in \mathcal{A}$, as
$A \Rightarrow B = \bigvee\{X \,|\, A \sqcap X \sqsubseteq B\}$
(to be read as the *pseudo-complement* of A *relative* to B).
2. The *complete Heyting algebra* $(\mathcal{A}, \sqcap, \sqcup, \bigwedge, \bigvee, \perp, \top, \Rightarrow)$ is a complete lattice equipped with $\Rightarrow$, where the following distributive property holds for all the elements A, B:
$A \sqcap \bigvee_{i\in I} B_i \sqsubseteq \bigvee_{i\in I}(A \sqcap B_i)$
3. A (complete) Heyting algebra is said to be *meet-distributive* iff the following distributive property holds:
$\bigwedge_{i\in I}(A \sqcup B_i) \sqsubseteq A \sqcup \bigwedge_{i\in I} B_i$
4. A (complete) Heyting algebra is said to satisfy the *atomicity condition* iff the following property holds:
$\bigwedge_{i\in I} A_i^{**} \sqsubseteq (\bigwedge_{i\in I} A_i)^{**}$
where $A^* = A \Rightarrow \perp$, is called the *pseudo-complement* (or *Heyting complement*) of A.

The following results are well-known ones — they can be worded in different ways, here I refer mainly to [RS63, Goe71]:

Proposition 9

1. For every space $\mathcal{S} = (S, \mathcal{O})$, the structure $(\mathcal{O}, \sqcap, \sqcup, \bigwedge', \bigvee, \varnothing, S, \Rightarrow)$ where $\bigwedge' \mathcal{F} = \mathsf{I}(\bigwedge \mathcal{F})$, is a complete Heyting algebra (see [RS63] chapter 4, theorem 1.4).

2. For every countable Heyting algebra $\mathcal{A}$ and for every countable collection E of arbitrary joins and arbitrary meets in $\mathcal{A}$, there is a space $\mathcal{S} = (S, \mathcal{O})$ and an embedding (i.e. a monomorphism) of $\mathcal{A}$ into $\mathcal{S}$ that preserves all the elements of E (see [RS63] chapter 4, theorem 9.2, extending a result in [Tar56]).
3. For every Alexandroff space $\mathcal{S} = (S, \mathcal{O})$, the structure $(\mathcal{O}, \sqcap, \sqcup, \bigwedge, \bigvee, \varnothing, S, \Rightarrow)$ is a complete meet-distributive Heyting algebra (see [Goe71] 5.1).
4. For every countable Heyting algebra $\mathcal{A}$ and for every countable collection E of arbitrary joins and arbitrary meets in $\mathcal{A}$, there is an Alexandroff space $\mathcal{S} = (S, \mathcal{O})$ and an embedding of $\mathcal{A}$ into $\mathcal{S}$ that preserves all the elements of E (see [Goe71] 7.8).

The following introduces a characterisation for atomic Alexandroff spaces:

Proposition 10 An Alexandroff space $\mathcal{S} = (S, \mathcal{O})$ is atomic iff, for any indexed family $A_I \subseteq \mathcal{O}$, $\bigwedge_{i \in I} A_i^{**} \sqsubseteq (\bigwedge_{i \in I} A_i)^{**}$ (atomicity condition).

pf: *Left to right.* Take $X = \bigwedge_{i \in I} A_i^{**}$ and $Y = \bigwedge_{i \in I} A_i$. First note that $X^{**} \sqsubseteq A_i^{**}$, for every $i \in I$, and so $X = X^{**}$. It follows that both X and Y are regular opens. So, assuming $X \not\sqsubseteq Y^{**}$, there exists a non-empty $Z \in \mathcal{O}$ such that $Z \sqsubseteq X$ and $Z \sqsubseteq Y^{*}$. But if $\mathcal{S}$ is atomic, Z can be taken to be an atom. Then, whenever $Z \sqsubseteq A_i^{**}$ also $Z \sqsubseteq A_i$ holds (otherwise $Z \sqcap A_i$ would be a proper part of Z), and so $Z \sqsubseteq Y$ follows from $Z \sqsubseteq X$, giving a contradiction. Hence $\mathcal{S}$ cannot be atomic.

Right to left. Assume that $\mathcal{S}$ is not atomic. Then, for some non-empty subset $T \in \mathcal{O}$, it must hold that there are no atoms in T. However, since the space is Alexandroff, by the closure of $\mathcal{O}$ w.r.t. $\bigwedge$, for each point $\mathtt{p} \in T$, there exists a smallest $B \in \mathcal{O}$ such that $\mathtt{p} \in B$. Since $B \sqsubseteq T$, B cannot be an atom — hence there must be a smaller non-empty open set. But for any such $C \in \mathcal{O}$, $\mathtt{p}$ can only belong to the boundary of C — otherwise B would not be the smallest open containing $\mathtt{p}$. Now let $K = \bigwedge_{X \in \mathcal{O}} (X \sqcup X^{*})$. Since every point in T turns out to be on the boundary of some open, we then have $K \sqcap T = \varnothing$. Then, since T is a non-empty open, it should be $K^{**} \neq S$. However, $\bigwedge_{X \in \mathcal{O}} (X \sqcup X^{*})^{**} = S$ and hence, using the condition in the hypothesis, $K^{**} = S$ — a contradiction. Therefore $\mathcal{S}$ must be atomic.

It is now possible to see how atomic Alexandroff spaces can be represented topologically.

Proposition 11

1. For every Alexandroff space $\mathcal{S} = (S, \mathcal{O})$, the structure $(\mathcal{O}, \sqcap, \ \sqcup, \bigwedge, \bigvee, \varnothing, S, \Rightarrow)$ is a complete meet-distributive Heyting algebra that satisfies the atomicity condition.
2. For each countable Heyting algebra $\mathcal{A}$ that satisfies the atomicity condition, and for every countable collection E of arbitrary joins and arbitrary meets in $\mathcal{A}$, there is an atomic Alexandroff space $\mathcal{S} = (S, \mathcal{O})$ and an embedding of $\mathcal{A}$ into $\mathcal{S}$ that preserves all the elements of E.

pf:

1. Consequence of Proposition 10.
2. This can be proved, using Proposition 10, as [Goe71] 7.8.

The results in Propositions 9 (1–2, 3–4) and 11 (1–2) can be regarded as a basis for the algebraic completeness of the logics *I2*, *C2* and *D2*, respectively, that are going to be introduced in the next chapter. Completeness could be proved relying on the approach used in [RS63, Goe71] — with some adjustment due in order to keep into account that here quantification ranges over the formulæ. However, in the next chapter, I will introduce Kripke models in order to make the semantics more intuitive.

Chapter 3

The logics

An intuitionistic 2nd-order propositional logic (ISPL) can be obtained by adding to intuitionistic propositional logic (*IPL*) quantification over the propositional variables. However, there are two different senses in which it is possible to understand propositional quantification — either relying primarily on the semantics or on the syntax.

In a model-theoretic sense, propositional quantification ranges over all the possible denotations of the propositional formulæ — the "semantical propositions". Those, in the case of a topological semantics, are the open sets [Kre97, Skv97].

In a proof-theoretic sense, propositional quantification ranges over all the possible syntactical substitutions of the propositional variables [Gab74, Gab81, Loe76]. Such a notion of quantification can also be called *substitutional*.

Unless it is assumed that, for each possible semantical denotation, the language includes a variable referencing it, the range of substitutional quantification may be just a proper subset of the semantical propositions. The models that satisfy this condition (also called *second order completeness*), are said to be the *principal* ones. In general, semantical propositions are not recursively denumerable — just as the opens in a topological space are not. Second order completeness turns out to be a very strong requirement, that cannot be expressed in the language of the logic [Skv97].

The gap between the semantical notion and the syntactical one is indeed quite deep: *IPL* extended with semantical quantification is not recursively axiomatisable [Kre97, Skv97]. On the other hand, logics with substitutional quantification can be axiomatised in a way quite similar to intuitionistic first-order predicate calculus (*IPC*) [Gab81]. Only substitutional quantification and axiomatisable logics will be considered in the following.

3.1 ISPL

An ISPL — in the axiomatisable sense that is considered here — is given by extending *IPL* with an axiomatisation of quantification over formulæ. Different formalisations are available. Examples of Hilbert axiomatisations are given in [Gab74,Gab81]. The system in [Loe76] is based on sequent calculus. In [Bar92] the logic associated to polymorphic type systems is presented in terms of natural deduction.

The range of substitutional quantification depends on the way substitution is defined. One possibility is to allow the substitution of an arbitrarily complex formula for a variable — this notion can be called *impredicative substitution* (since it explicitly forces the definition of formula to be impredicative). Another possibility is to allow only the substitution of a variable for another variable — this may be called *predicative substitution* (since, by itself, it still allows for formulæ to be defined inductively).

With impredicative substitution, quantification must range over all the semantical propositions that are syntactically definable — in the topological semantics, these will be the definable opens (as it will be seen further on) — hence quantification can be said to satisfy the *comprehension principle* (or *full comprehension*), so called in analogy with the set-theoretical principle, stating that every definable collection is a set [Gab74].

With predicative substitution however, quantification might also range on a proper subset of the formulæ. In order to rule out this possibility, it must be explicitly required that the comprehension principle is satisfied, by introducing an additional axiom schema. For technical reasons, in Hilbert axiomatisations predicative substitution with explicit comprehension is preferred, whereas impredicative substitution is usually favoured in the rule systems.

The fact that it is not possible to define the class of the formulæ without referring to the class itself (either through impredicative substitution, or through the comprehension axiom) gives, in any case, the impredicative character of ISPL.

In the following, three different second-order logics based on *IPL* are going to be introduced — *I2*, *C2* and *D2* — using Hilbert axiomatisations. *I2* is the weakest, and it may be regarded as an axiomatisation of standard ISPL — corresponding to the logic of the natural deduction system in [Bar92]. *I2* is important for its proof-theory, but it is semantically too general from the point of view of the present analysis. *C2*, corresponding semantically to order topologies, is equivalent to the system introduced as *C2h* in [Gab74] and as *C2I* in [Gab81]. *D2* is the strongest of the three, and it has been introduced in [TSB02] (there called *2tA*). It is particularly significant from the point of view of digital representation, since it corresponds to atomic Alexandroff spaces.

3.2 Modality

Intuitionistic modal logics (IMLs) are obtained by adding modalities to an intuitionistic logic. Since *IPL* can be embedded into *S4*, IMLs can also be regarded as fragments of classical multi-modal logics, where one of the modalities is an *S4* operator [WZ99, ZWC02].

In the case of IMLs, Kripke semantics are generally based on frames with more than one accessibility relation. The interpretation of the standard intuitionistic connectives is associated to a partial order (denoted by $\leq$ in the following), whereas the interpretation of the modalities can be associated to additional relations [WZ99].

Here the case is different. Modal operators are needed in order to express topological notions for which the intuitionistic operators will not suffice. The aim is to gain expressiveness over the topology which is determined by $\leq$. Hence, the interpretation of the new operators, in order to be useful, must refer to $\leq$, too.

In the following, two different kinds of modalities are going to be considered, as possible ways to extend an ISPL. Both of them are based on a primitive box operator ($\Box$). The diamond operator ($\Diamond$) can be defined in terms of box and negation. I will refer to the first kind as to the *N-modalities*, giving the N-modal logics as extensions of *C2* and *D2*. The N-box bears some relationship to the strong *S5* necessity operator. Models can be associated to the same frames as those of the underlying non-modal logic. The meaning of the N-box formula $\Box\alpha$ is that α is true everywhere in the model.

The second kind of modalities — here I will call them *V-modalities*, giving rise to the *V-modal* logics — may be considered separately from the first ones. The V-box is comparable to a weak *S5* modality. Semantically, the models can be associated to frames for the underlying non-modal logic extended with a family of selected subframes. The meaning of the V-box formula $\Box\alpha$ is that α is true everywhere in the sub-model determined by the local subframe.

Differently from the case of classical *S5*, here the difference between strong (N) and weak (V) interpretation of the box operator is reflected in the axiomatisation. N-box formulæ are two-valued — hence, the N-modal logics have some disjunctions as theorems. In contrast, the V-modalities preserve the constructive character of intuitionistic logic (no disjunctions or existentials are forced as theorems).

The N-modal logics are going to be discussed in detail, from the point of view of spatial representation, in the next chapters. In contrast, a spatial interpretation for the V-modal logics will be only sketched in the last section of Chapter 5.

3.3 Language

The set of the formulæ of a language $\mathcal{L}_i$ for ISPL is the smallest one that contains an enumerable set of variables $Var = x, y, \ldots$, an enumerable set of propositional constants $Const = a, b, \ldots$, and is closed w.r.t. the constructs $\alpha \to \beta$ (where $\to$ is intuitionistic implication) and $\forall x.\alpha$ (where $\forall$ is the universal quantifier). Propositions are formulæ without free variables.

Lower-case Greek letters $\alpha, \beta, \ldots$ are going to be used, by default, as meta-variables for formulæ. As usual, $\alpha(x)$ means that x may be free in α, whenever x is a variable that is bound elsewhere in the formula. On the other hand, it may be useful to remark that if $\beta(x)$ was taken to be syntactic sugar for $\lambda x.\beta$, propositions could be defined as $\alpha = a \mid \beta \to \gamma \mid \forall x.\beta(x)$ — although this fact will turn out to be significant only when we consider the point of view of mechanisation.

The expression $\alpha(y/x)$ (predicative substitution) means that the variable y is uniformly substituted for the variable x, i.e. every occurrence (possibly none) of x in the formula α is replaced by an occurrence of y. Any capture of free variables is avoided by renaming.

The expression $\alpha[\beta/x]$ (impredicative substitution) means that the formula β is uniformly substituted for the variable x, i.e. every occurrence (possibly none) of x in the formula α is replaced by an occurrence of β, avoiding any capture of free variables in β by renaming.

The language $\mathcal{L}_i$ is then extended by the following definitions [TS00]:

Definition 8

$$\alpha \wedge \beta = \forall x.(\alpha \to \beta \to x) \to x$$

$$\alpha \vee \beta = \forall x.(\alpha \to x) \to (\beta \to x) \to x$$

$$\exists x.\alpha(x) = \forall z.(\forall x.\alpha(x) \to z) \to z \qquad z \text{ not free in } \alpha.$$

$$\bot = \forall x.x$$

$$\sim\alpha = \alpha \to \bot$$

$$\top = \bot \to \bot$$

$\alpha \leftrightarrow \beta = (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$

$\approx\alpha = \sim\sim\alpha$

$\bigwedge_{0<i<n}\alpha_i = \alpha_1 \wedge \ldots \wedge \alpha_{n-1}$

$\bigvee_{0<i<n}\alpha_i = \alpha_1 \vee \ldots \vee \alpha_{n-1}$

The set of the formulæ in a modal language $\mathcal{L}_m$ that extends $\mathcal{L}_i$, is defined by requiring also the closure w.r.t. the construct $\Box\alpha$ (where $\Box$ is the box operator).

The modal language is then extended by the following definitions, in addition to the previous ones:

Definition 9

$\Diamond\alpha = \sim\Box\sim\alpha$

$\alpha \supset \beta = \sim\Box\alpha \vee \Box\beta$

The operators $\rightarrow, \wedge, \vee$ are taken to be right-associative, and the precedences are $\{\sim, \approx, \Box, \Diamond, \bigwedge_{1<i<n}, \bigvee_{1<i<n}\} > \{\wedge, \vee\} > \{\rightarrow, \supset\} > \leftrightarrow > \{\exists, \forall\}$.
The letters $\Delta, \Gamma, \ldots$ are used to denote sets of formulæ.

3.4 The axiomatisation of ISPL

The Hilbert axiomatisations based on predicative substitution, in a language $\mathcal{L}_i$, for three different forms of ISPL (*I2*, *C2* and *D2*) can be obtained from the following list of axiom schemas and inference rules. Uniform substitution for the free variables is assumed here.

- Basic propositional schemas:

  A1. $\alpha \rightarrow \beta \rightarrow \alpha$

  A2. $(\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow \alpha \rightarrow \gamma$

  A3. $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$

  A4. $\Gamma \vdash \alpha$ and $\Gamma \vdash \alpha \rightarrow \beta$ implies $\Gamma \vdash \beta$

- Minimal quantification schemas:

  A5. $(\forall x.\alpha(x)) \rightarrow \alpha(y/x)$

  A6. $\Gamma \vdash \alpha \rightarrow \beta(y/x)$ implies $\Gamma \vdash \alpha \rightarrow \forall x.\beta(x)$ $\quad$ x not free in Γ, α

- Other quantification schemas:

  A7. $(\forall x.\alpha \vee \beta(x)) \rightarrow \alpha \vee (\forall x.\beta(x))$ $\quad x$ not free in α.

  A8. $(\forall x.\approx\alpha(x)) \rightarrow \approx\forall x.\alpha(x)$

  A9. $\exists x.x \leftrightarrow \alpha$ $\quad \alpha$ any formula, x not free in α.

Intuitionistic implication can be axiomatised by A1, A2, A3 together with Rule A4 (*Modus Ponens*). Schema A5 and Rule A6 give the minimal notion of quantification, and they are similar to those for intuitionistic predicate calculus. A9 is the *Full Comprehension Schema* for second-order propositional logic. All these together give an axiomatisation of *I2*, equivalent to the basic intuitionistic second-order propositional logic in [Gab74].

Adding to *I2* the schema A7 (also called *Constant Domain Schema*) gives the axiomatisation of *C2*, i.e. the ISPL with constant domain (w.r.t. the Kripke semantics) that is equivalent to *C2h* in [Gab81] (or to *C2I* in [Gab74]).

The axiomatisations in [Gab81] differ from those presented here insofar as there also the logics without Full Comprehension are considered. For those logics, it is not possible to rely on the definitions of the operators given in Def. 8, and hence independent axioms for $\wedge, \vee, \exists, \perp$ are needed.

The logic *D2* (*2tA* in [TSB02]) is obtained by adding Schema A8 (also called *Atomicity Schema*, or *Terminability Schema*) to *C2*. A schema similar to A8 has been already considered in [Gab81] for an extension of intuitionistic predicate calculus (there called *MH*).

Summarising, the following definitions can be given:

Definition 10

I2: Schemas A1, A2, A3, A5, A9, Rules A4, A6.
C2: *I2* + Schema A7.
D2: *C2* + Schema A8.

3.5 Modal extensions

The Hilbert axiomatisations for the modal extensions of the logics $H \in \{C2, D2\}$ that are considered here, can be obtained from the following list of schemas in a modal intuitionistic language $\mathcal{L}_m$.

- *S4*-style modal schemas:

A10. $\Box\alpha \to \alpha$

A11. $\Box\alpha \to \Box\Box\alpha$

A12. $\Box(\alpha \to \beta) \to \Box\alpha \to \Box\beta$

A13. $\Gamma \vdash \alpha$ implies $\Gamma \vdash \Box\alpha$ all formulæ in Γ have form $\Box\beta$.

- Other modal schemas:

A14. $\Box\alpha \vee \sim\Box\alpha$

A15. $\Box(\alpha \vee \beta) \to \Box\alpha \vee \Box\beta$

- Quantified modal schemas:

A16. $(\forall x.\Box\alpha(x)) \to \Box\forall x.\alpha(x)$

A17. $(\Box\exists x.\alpha(x)) \to \exists x.\Box\alpha(x)$

The logics H extended with all the schemas and with the rule presented here, will be referred to as the N-modal logics (respectively, *NC2* and *ND2*). The logics extended with the rule and with all the schemas except A14, will be referred to as the V-modal logics (respectively, *VC2* and *VD2*).

The schemas A10–A12 and Rule A13 are those generally used to axiomatise an *S4*-style necessity operator [WZ99, Pra65]. Schema A16 is the Barcan formula. Schemas A14, A15 and A17 are more specific. From the point of view of the Kripke models discussed further on, the schemas A15 and A17 force the interpretation of $\Box\alpha$ to depend on that of α at a single point. Adding Schema 14, this point is forced to be the minimum w.r.t. the partial order $\leq$, so the interpretation of $\Box$ is forced to be the "strong" one.

Dropping both A15 and A17 one can abandon the restriction to frames that have a minimum (w.r.t. Defs. 15, 18) — correspondingly, the restriction to prime spaces. The resulting logics will not be treated here, although they are interesting (see the comment in the Conclusion).

Summarising, the following definitions can be given here:

Definition 11

VC2: *C2* + Schemas A10, A11, A12, A15, A16, A17, Rule A13.
VD2: *D2* + Schemas A10, A11, A12, A15, A16, A17, Rule A13.
NC2: *VC2* + Schema A14.
ND2: *VD2* + Schema A14.

3.6 Syntactical properties

For any logic of those that have been introduced, the notions of derivation of a formula from a set of assumptions (also called a *deduction*) and the notion of proof can be defined as follows [TS00]. Let $L \in \{I2, C2, D2, NC2, ND2, VC2, VD2\}$.

Definition 12

(a) A *derivation* (of length n) of a formula α from a set of assumptions Δ, in L, is defined inductively, as a finite sequence of formulæ $\alpha_1, \ldots, \alpha_n$ such that $\alpha = \alpha_n$, and for each $1 \leq i \leq n$, one of the following holds:

1. $\alpha_i \in \Delta$.
2. α_i is an instance of an axiom schema of L.
3. There are $j, k < i$ such that $\alpha_k = \alpha_j \to \alpha_i$.
4. $\alpha_i = \beta \to \forall x.\gamma(x)$ and $\alpha_j = \beta \to \gamma$, with $j < i$, and x is not free in β and in Δ.
5. [for L modal logic] $\alpha_i = \Box\alpha_j$, with $j < i$, and there is a subsequence of $\alpha_1, \ldots, \alpha_j$ which is a deduction of α_j from Γ, where every $\beta \in \Gamma$ has form $\Box\gamma$ (i.e. is a box formula).

(b) A derivation of α from the empty set is said to be a *proof* of α.

Definition 13

(a) In L, a formula α is said to be *derivable* from a set of assumptions Δ (written $\Delta \vdash_L \alpha$) iff there is a derivation of α from Δ.
(b) In L, α is said to be *provable* (written $\vdash_L \alpha$) iff there is a proof of α.

In contrast with the notion of object-level derivation that has been just defined, the following principles can be proved valid at the meta-level, using induction — here either on the length of the derivations or on the length of the formulæ (defined as usual, see [TS00]).

Proposition 12 [DE — Deduction Equivalence]
$\Delta, \alpha \vdash_L \beta$ iff $\Delta \vdash_L \alpha \to \beta$.

pf: *Right to left.* By $\Delta, \alpha \vdash_L \alpha$ and rule A4.
Left to right. By induction on the length of the derivation.
Base case. If β is an axiom, by A1 and rule A4. If $\beta \in \Delta$, by $\vdash_L \beta \to \beta$.

Step case. (a) For an application of Rule A4: by induction hypothesis, A2 and A4 itself.

(b) For an application of Rule A6, with $\beta = \gamma \rightarrow \forall x.\delta(x)$: from the induction hypothesis, given that $\Delta \vdash_L \alpha \rightarrow \gamma \rightarrow \delta$ is equivalent to $\Delta \vdash_L \alpha \wedge \beta \rightarrow \gamma$, and x is not free in $\alpha \wedge \beta$.

(c) [For L modal logic] For an application of Rule A13, with $\beta = \Box\gamma$: then there is a sub-deduction of γ from $\Delta' \subseteq \Delta \cup \{\alpha\}$, where all the formulæ in Δ' are box-formulæ.

(c1) If $\Delta' = \Gamma \cup \{\alpha\}$, by induction hypothesis, $\Gamma \vdash_L \alpha \rightarrow \gamma$. Then $\Gamma \vdash_L \Box(\alpha \rightarrow \gamma)$ follows by Rule A13. So, by A12, using Rule A4, we get $\Gamma \vdash_L \Box\alpha \rightarrow \beta$. Since α is a box-formula, using A11, $\Gamma \vdash_L \alpha \rightarrow \beta$ follows, and hence, by definition of deduction, also $\Delta \vdash_L \alpha \rightarrow \beta$.

(c2) If $\alpha \notin \Delta'$, from $\Gamma \vdash_L \beta$, $\Delta \vdash_L \beta$ follows by definition of deduction, and hence $\Delta \vdash_L \alpha \rightarrow \beta$ follows using A1 and Rule A4.

Proposition 13 [RE — Replacement of Equivalents]

$\Delta \vdash_L \alpha \leftrightarrow \beta$ implies $\Delta \vdash_L \gamma[\alpha/x] \leftrightarrow \gamma[\beta/x]$.

[For L modal logic] Proviso (*): if γ contains some occurrence of $\Box$, then for any $\phi \in \Delta$, $\Delta \vdash_L \Box\phi$.

pf: By induction on the length of the formulæ.

Base case. If $\gamma = x$, by assumption. If x is not free in γ, by $\vdash_L \gamma \rightarrow \gamma$.

Step case. (a) $\gamma = \eta \rightarrow \delta$. As consequences of the induction hypothesis, we have $\Delta \vdash_L \eta[\alpha/x] \leftrightarrow \eta[\beta/x]$ and $\Delta \vdash_L \delta[\alpha/x] \leftrightarrow \delta[\beta/x]$. Since

$\eta[\beta/x] \rightarrow \eta[\alpha/x], \delta[\alpha/x] \rightarrow \delta[\beta/x] \vdash_L (\eta[\alpha/x] \rightarrow \delta[\alpha/x]) \rightarrow (\eta[\beta/x] \rightarrow \delta[\beta/x])$

it follows $\Delta \vdash_L (\eta[\alpha/x] \rightarrow \delta[\alpha/x]) \rightarrow (\eta[\beta/x] \rightarrow \delta[\beta/x])$.

Similarly for $\Delta \vdash_L (\eta[\beta/x] \rightarrow \delta[\beta/x]) \rightarrow (\eta[\alpha/x] \rightarrow \delta[\alpha/x])$.

(b) $\gamma = \forall y.\delta(y)$. Then, for any z not free in Δ, as consequences of the induction hypothesis, $\Delta \vdash_L \delta(z/y)[\alpha/x] \rightarrow \delta(z/y)[\beta/x]$;

using A5 it follows $\Delta \vdash_L (\forall z.\delta(z/y)[\alpha/x]) \rightarrow \delta(z/y)[\beta/x]$. Then, by Rule A6, $\Delta \vdash_L (\forall z.\delta(z/y)[\alpha/x]) \rightarrow (\forall z.\delta(z/y)[\beta/x])$. Similarly for the other side of the double implication.

(c) [For L modal logic] $\gamma = \Box\delta$. From the induction hypothesis, given the proviso (*), by Rule A13, $\Delta \vdash_L \Box(\delta[\alpha/x] \rightarrow \delta[\beta/x])$. Then, using A12, $\Delta \vdash_L \Box\delta[\alpha/x] \rightarrow \Box\delta[\beta/x]$. Similarly for $\Delta \vdash_L \delta[\beta/x] \rightarrow \delta[\alpha/x]$.

The following gives an example of a schematic formula which cannot be proved in *C2*, whereas it is provable in *D2*. In [Gab81] a similar example is given with respect to the corresponding predicate calculi.

Proposition 14 $\vdash_{D2} \approx\forall x.\alpha(x) \vee \sim\alpha(x)$

pf: Follows from $\vdash_{C2} \forall x.\approx(\alpha(x) \vee \sim\alpha(x))$ using A8 and Rule A4.

The following are theorems in the logics $N \in \{NC2, ND2\}$.

Proposition 15

(a) $\vdash_N (\Box\alpha \to \Box\beta) \to \sim\Box\alpha \vee \Box\beta$
(b) $\vdash_N \approx\Box\alpha \to \Box\alpha$
(c) $\vdash_N \sim\Box\alpha \to \Box\sim\Box\alpha$
(d) $\vdash_N \Diamond\Box\alpha \to \Box\alpha$
(e) $\vdash_N (\Box\alpha \to \Box\beta) \leftrightarrow (\alpha \supset \beta)$

pf: (a) From $\vdash_N \sim\Box\alpha \vee \Box\alpha \to (\Box\alpha \to \Box\beta) \to \sim\Box\alpha \vee \Box\beta$ and Schema A14, using Modus Ponens.
(b) From a, since $\vdash_N \sim\approx\gamma \leftrightarrow \sim\gamma$.
(c) From $\vdash_N \Box(\Box\alpha \vee \sim\Box\alpha)$, follows that 1: $\vdash_N \Box\alpha \vee \Box\sim\Box\alpha$.
We have that $\vdash_N \Box\alpha \to \sim\Box\alpha \to \bot$, and so 2: $\vdash_N \Box\alpha \to \sim\Box\alpha \to \Box\sim\Box\alpha$.
Moreover, 3: $\vdash_N \Box\sim\Box\alpha \to \sim\Box\alpha \to \Box\sim\Box\alpha$.
From 2 and 3 follows 4: $\vdash_N (\Box\alpha \vee \Box\sim\Box\alpha) \to \sim\Box\alpha \to \Box\sim\Box\alpha$. Applying Modus Ponens to 1 and 4 gives q.e.d..
(d) From c and b.
(e) From a and $\vdash_N \sim\alpha \vee \beta \to \alpha \to \beta$

The following equivalences show how closely the N-modalities can be related to the *S5* modalities.

Proposition 16

$\vdash_N \Box\alpha \leftrightarrow \Diamond\Box\alpha$
$\vdash_N \Box\alpha \leftrightarrow \approx\Box\alpha$

pf: Corollary of Proposition 15.

In fact, it turns out that an alternative axiomatisation for the N-modal logics can be given by replacing A14 with the following two schemas:

$\vdash \Diamond\Box\alpha \to \Box\alpha$

$\vdash \sim\Box\alpha \rightarrow \Box\sim\Box\alpha$

However, here $\Box$ and $\Diamond$ do not show the same kind of duality than can be found either in classical modal logics. In fact, $\Diamond\,\alpha \wedge \Diamond\,\beta \rightarrow \Diamond(\alpha \wedge \beta)$ is not a theorem, in spite of Schema A15.

3.7 Kripke semantics

In this section the Kripke semantics for the logics *C2*, *D2* and for their N-modal and V-modal extensions are introduced. The models and the completeness proofs are largely based on those given in [Gab74, Gab81] for a logic equivalent to *C2*. As to *D2*, the main idea comes from the semantics of the system called *MH* in [Gab81]. In the case of the modal logics, some extra machinery is needed. I will consider first the N-modal logics, interpreted into the same frames as those of the non-modal ones. Then I will deal with the V-modal logics.

3.7.1 Models for the non-modal and N-modal logics

The following gives a definition of atomicity for pre-orders (similar to Def. 6).

Definition 14 A pre-order $(S, \leq)$ is said to be *atomic* iff, for any $\mathtt{x} \in S$, there is $\mathtt{y} \in S$, such that $\mathtt{x} \leq \mathtt{y}$, and for all $\mathtt{z} \in S$, if $\mathtt{y} \leq \mathtt{z}$ then $\mathtt{z} \leq \mathtt{y}$.
$\mathtt{y}$ is then said to be a *terminal* element, or an atom.

It is now possible to introduce the following two notions of frame.

Definition 15

1. A *Kripke C2-frame* is a structure $(S, \leq, \mathbf{0})$, where $(S, \leq)$ is a partial order on the set of points S, and $\mathbf{0} \in S$ (also called the *root* of the frame) is the minimum w.r.t. $\leq$.
2. A *Kripke D2-frame* $(S, \leq, \mathbf{0})$ is a *C2*-frame where $(S, \leq)$ is atomic.

The restriction to partial orders is quite intuitive, but not essential. Reminding that, w.r.t. $(S, \leq)$, the class of the subsets of S that are upper-closed relative to $\leq$ is denoted by $\mathcal{U}_{\leq}$, it is possible to give the following definitions for the models:

Definition 16

1. A *Kripke D2-model* (*C2-model*) in a language $\mathcal{L}_i$ is a structure $\mathcal{M} = (\mathcal{F}, \mathcal{R}, \rho)$, where $\mathcal{F} = (S, \leq, \mathbf{0})$ is a *D2*-frame (*C2*-frame), ρ is an interpretation, assigning to each $\alpha \in \mathit{Var} \cup \mathit{Const}$ an element $\|\alpha\|_\rho \in \mathcal{U}_\leq$ (i.e. an upper-closed set), and $\mathcal{R}$ is the image of ρ in $\mathcal{U}_\leq$.
   The notion of *truth* at a point $\mathtt{a} \in S$ relative to ρ (also said *forcing* relation), can be defined inductively, for all the formulæ in $\mathcal{L}_i$, as follows:
   - For $\alpha \in \mathit{Var} \cup \mathit{Const}$, $\mathtt{a} \vDash \alpha$ iff $\mathtt{a} \in \|\alpha\|_\rho$.
   - $\mathtt{a} \vDash \alpha \to \beta$ iff for every $\mathtt{b} \in S$ such that $\mathtt{a} \leq \mathtt{b}$, if $\mathtt{b} \vDash \alpha$ then $\mathtt{b} \vDash \beta$.
   - $\mathtt{a} \vDash \forall x.\alpha(x)$ iff for every $y \in \mathit{Var}$, $\mathtt{a} \vDash \alpha(y/x)$.

   The following condition must be satisfied:
   - Full Comprehension (condition *FC*): for each $\alpha \in \mathcal{L}_i$, there is $x \in \mathit{Var}$ s.t. $\mathtt{a} \vDash \alpha$ iff $\mathtt{a} \in \|x\|_\rho$.
2. A *Kripke ND2-model* (*NC2-model*) $\mathcal{M} = (\mathcal{F}, \mathcal{R}, \rho)$ in a modal language $\mathcal{L}_m$ is a Kripke *D2*-model (*C2*-model) where the notion of truth is extended to all the formulæ in $\mathcal{L}_m$, as follows:
   - $\mathtt{a} \vDash \Box\alpha$ iff $\mathbf{0} \vDash \alpha$.

The definiton of *C2*-model here is essentially the same as that of *C2h*-model in [Gab81].

The given interpretation rule for $\forall$ is different from the standard intuitionistic one, and it is not appropriate for *I2*. In fact, the present form relies on the assumption that the domain of quantification is constant throughout all the points in the frame. This assumption is satisfied whenever Schema A7 is given [Goe71], and hence in every extension of *C2*.

3.7.2 Models for *VH*

The V-modal logics require a slightly richer structure. Given a frame $(S, \leq, \mathbf{0})$, a *subframe* is a pointed subset of S w.r.t. $\leq$, i.e. an upper-closed subset generated by a single point. Exactly like the main frame, each subframe is a partial order with a minimum.

Definition 17 Given a partial order $(S, \leq)$ and a subset $A \subseteq S$, A is said here to be *closed for bounded sets* in S w.r.t. $\leq$ iff, for every subset $B \subseteq A$, whenever B has a superior bound $\mathtt{x}$ in S, then it has also a superior bound $\mathtt{y}$ in A such that $\mathtt{y} \leq \mathtt{x}$.

Definition 18 A *Kripke VD2-frame* (*VC2-frame*) is a structure $\mathcal{F} = (S, V, \leq, \mathbf{0})$, where $(S, \leq, \mathbf{0})$ is a *D2*-frame (*C2*-frame), $V \subseteq S$ is a set of *selected points*, $\mathbf{0} \in V$ and V is closed for bounded subsets in S w.r.t. $\leq$.

The definition of model differs from Def.16 only with respect to the language, the frame and the condition for $\Box$:

Definition 19 A *Kripke VD2-model* (*VC2-model*) in a modal language $\mathcal{L}_m$ is a structure $\mathcal{M} = (\mathcal{F}, \mathcal{R}, \rho)$, where $\mathcal{F} = (S, V, \leq, \mathbf{0})$ is a *VD2*-frame (*VC2*-frame), ρ is an interpretation, assigning to each $\alpha \in \mathit{Var} \cup \mathit{Const}$ an element $\|\alpha\|_\rho \in \mathcal{U}_\leq$, and $\mathcal{R}$ is the image of ρ in $\mathcal{U}_\leq$.
The notion of truth at a point $\mathtt{a} \in S$ relative to ρ, can be defined inductively, for all the formulæ in $\mathcal{L}_m$, as follows:

- For $\alpha \in \mathit{Var} \cup \mathit{Const}$, $\mathtt{a} \models \alpha$ iff $\mathtt{a} \in \|\alpha\|_\rho$.
- $\mathtt{a} \models \alpha \to \beta$ iff for every $\mathtt{b} \in S$ s. t. $\mathtt{a} \leq \mathtt{b}$, if $\mathtt{b} \models \alpha$ then $\mathtt{b} \models \beta$.
- $\mathtt{a} \models \forall x.\alpha(x)$ iff for every $y \in \mathit{Var}$, $\mathtt{a} \models \alpha(y/x)$.
- $\mathtt{a} \models \Box\alpha$ iff there exists $\mathtt{b} \in V$, $\mathtt{b} \leq \mathtt{a}$, s.t. $\mathtt{b} \models \alpha$.

The following condition must be satisfied:

- Full Comprehension (condition *FC*): for each $\alpha \in \mathcal{L}_m$, there is $x \in \mathit{Var}$ such that $\mathtt{a} \models \alpha$ iff $\mathtt{a} \in \|x\|_\rho$.

The set $\mathcal{V} = \{\mathtt{a}\uparrow : \mathtt{a} \in V\}$ is the family of the subframes, which is never empty since $S \in \mathcal{V}$.

Proposition 17 In a *VD2*-frame, let a *quasi-subframe* be any arbitrary union of subframes. Then, the family of the quasi-subframes is closed w.r.t. to arbitrary intersection too — hence, it defines an Alexandroff topology over the frame.

pf: Closure w.r.t. arbitrary intersection follows from the assumption that the collection of the selected points is closed for bounded subsets.

3.7.3 Properties of models and validity

In the following, I will consider some standard semantical notions, and give some properties of the models that have been defined.

Let $\mathcal{M} = (\mathcal{F}, \mathcal{R}, \rho)$ be a Kripke model where the frame $\mathcal{F}$ is defined over a partial order $(S, \leq)$ with minimum $\mathbf{0}$.

Definition 20 In the model $\mathcal{M}$, for any formula α, the set $\{\mathsf{a} \in S | \mathsf{a} \models \alpha\}$ denoted by $\|\alpha\|_\rho$ will be called the *truth-set* of α.

In any model $\mathcal{M}$, the following hold as consequences of the definitions:

1. Every truth-set is an upper-closed set and is a member of $\mathcal{R}$.
2. [*Hereditary condition*] Whenever $\mathsf{a} \leq \mathsf{b}$, if $\mathsf{a} \models \alpha$ then $\mathsf{b} \models \alpha$.

Definition 21

1. A formula α is said to be *valid in a model* $\mathcal{M}$, or *satisfied* by that model (this is denoted by $\models_M \alpha$) iff $\mathbf{0} \models \alpha$ in $\mathcal{M}$.
2. A formula α is said to be *semantically deducible* from a set of formulæ $\Delta = \beta_{i \in I}$ in a model $\mathcal{M}$ (this is denoted by $\Delta \models_M \alpha$) iff for every point $\mathsf{a} \in S$, whenever it is the case in $\mathcal{M}$ that $\mathsf{a} \models \beta_i$, for every $i \in I$, then $\mathsf{a} \models \alpha$.

The following is provable from the above definition by the interpretation of $\rightarrow$, showing the correspondence betweeen semantical deduction and syntactical derivability (Def. 12).

Proposition 18 In any model $\mathcal{M}$, we have that $\Delta, \beta \models_M \alpha$ iff $\Delta \models_M \beta \rightarrow \alpha$.

The following gives the interpretation for the defined logical operators.

Proposition 19

1. For every model $\mathcal{M}$, for every $\mathsf{a} \in S$:
    - $\mathsf{a} \not\models \bot$.
    - $\mathsf{a} \models \top$.
    - $\mathsf{a} \models \alpha \wedge \beta$ iff $\mathsf{a} \models \alpha$ and $\mathsf{a} \models \beta$.
    - $\mathsf{a} \models \alpha \vee \beta$ iff $\mathsf{a} \models \alpha$ or $\mathsf{a} \models \beta$.

- $\mathtt{a} \models \exists x.\alpha(x)$ iff $\mathtt{a} \models \alpha(y/x)$ for some $y \in Var$.
- $\mathtt{a} \models \sim\alpha$ iff for every $\mathtt{b} \in S$ s.t. $\mathtt{a} \leq \mathtt{b}$, $\mathtt{b} \not\models \alpha$.
- $\mathtt{a} \models \alpha \leftrightarrow \beta$ iff for every $\mathtt{b} \in S$ s.t. $\mathtt{a} \leq \mathtt{b}$, $\mathtt{b} \models \alpha$ iff $\mathtt{b} \models \beta$.

2. For every N-modal model $\mathcal{M}$, for every $\mathtt{a} \in S$:
   - $\mathtt{a} \models \sim\Box\alpha$ iff $\mathbf{0} \not\models \alpha$.
   - $\mathtt{a} \models \Diamond\alpha$ iff there exists $\mathtt{b} \in S$ s.t. $\mathtt{b} \models \alpha$.
   - $\mathtt{a} \models \alpha \supset \beta$ iff either $\mathbf{0} \not\models \alpha$ or $\mathbf{0} \models \beta$.
3. For every V-modal model based on a frame $(S, \leq, \mathbf{0}, V)$, for every $\mathtt{a} \in S$:
   - $\mathtt{a} \models \sim\Box\alpha$ iff for every $\mathtt{b} \in V$ s.t. $\mathtt{a} \leq \mathtt{b}$, there exists $\mathtt{c}$ s.t. $\mathtt{b} \leq \mathtt{c}$ and $\mathtt{c} \not\models \alpha$.

pf: By the definitions of the logical operators (Def. 8) and by the interpretation rules given in the definitions of the models (Defs. 16,19).

3.7.4 Completeness

In the following, I will consider the completeness proofs for the logics $K \in \{C2, D2, NC2, ND2, VC2, VD2\}$. $\mathcal{L}$ will be either a non-modal language $\mathcal{L}_i$ or a modal language $\mathcal{L}_m$. I will also use $[\Delta, \alpha]$ as short for $\Delta \cup \{\alpha\}$. In order to prove completeness, it is useful to introduce some notions of theory (similar to those in [Gab74]).

Definition 22

1. A *k-theory* in a language $\mathcal{L}$, is a pair $(\Delta; \Omega)$ of sets of formulæ of $\mathcal{L}$.
2. $(\Delta; \Omega)$ is said to be *consistent* w.r.t. a logic K iff for no finite subsets $\Delta' \subseteq \Delta, \Omega' \subseteq \Omega$, we have $\vdash_K \bigwedge\Delta' \rightarrow \bigvee\Omega'$.
3. $(\Delta; \Omega)$ is said to be *complete* in a language $\mathcal{L}$ iff for all the formulæ α in $\mathcal{L}$, either $\alpha \in \Delta$ or $\alpha \in \Omega$.
4. $(\Delta; \Omega)$ is said to be *saturated* in a language $\mathcal{L}$ w.r.t. a logic K iff
   a: $\Delta \vdash_K \alpha$ implies $\alpha \in \Delta$
   b: $\alpha \vee \beta \in \Delta$ implies $\alpha \in \Delta$ or $\beta \in \Delta$.
   c: $\exists x.\alpha(x) \in \Delta$ implies that for some variable y in $\mathcal{L}$, $\alpha(y/x) \in \Delta$.
5. $(\Delta; \Omega)$ is said to be *of constant domains* in a language $\mathcal{L}$ w.r.t. a logic K iff whenever $(\Delta; [\Omega, \forall x.\alpha(x)])$ is consistent, then for some propositional variable y in $\mathcal{L}$, $(\Delta; [\Omega, \alpha(y/x)])$ is consistent.

6. $(\Delta;\Omega)$ is said to be a *ck-theory* in a language $\mathcal{L}$ w.r.t. a logic K iff it is a consistent, complete, saturated k-theory of constant domain w.r.t. K in $\mathcal{L}$.
7. $(\Delta';\Omega')$ is said to *extend* $(\Delta;\Omega)$ iff $\Delta \subseteq \Delta'$ and $\Omega \subseteq \Omega'$.

The following notions are useful in order to deal with atomicity and modality.

Definition 23

1. $(\Delta;\Omega)$ is said to be *terminal* in a language $\mathcal{L}$ iff for every formula α in $\mathcal{L}$, either $\alpha \in \Delta$ or $\sim\alpha \in \Delta$.
2. An *r-theory* is a k-theory $(\Delta;\Omega)$ in a modal language $\mathcal{L}_m$ such that $\Box\alpha \in \Delta$ iff $\alpha \in \Delta$, and no other formulæ containing modal operators are in Δ.
3. $(\Delta;\Omega)$ is said to be a *root-theory* in a modal language $\mathcal{L}_m$ w.r.t. a modal logic M iff it is a ck-theory in $\mathcal{L}_m$, w.r.t. M, such that $\alpha \in \Delta$ iff $\Box\alpha \in \Delta$.
4. Given in $\mathcal{L}_m$ a root-theory $\mathtt{t} = (\Delta;\Omega)$, a ck-theory $(\Delta';\Omega')$ is said to be a $\mathtt{t}$-*dependant* theory iff $\Delta \subseteq \Delta'$.

In the canonical models that are going to be considered, points will be represented in general as ck-theories. In the N-modal cases, the root can be defined as a root-theory $\mathtt{t}$, whereas all the other points will be associated to $\mathtt{t}$-dependant theories. In the V-modal cases, all the selected points will be associated to root-theories, and the remaining points to theories depending on the root-theories below them. In the cases of *D2*, *ND2* and *VD2*, in order to satisfy the atomicity condition, it is necessary to include in the model, for any k-theory $\mathtt{a}$, a terminal k-theory that extends $\mathtt{a}$, representing an atom. It is useful to prove first some lemmas.

Proposition 20 Let $(\Delta;\Omega)$ be a consistent k-theory w.r.t. a logic K in a language $\mathcal{L}$. Then, for any formula α in $\mathcal{L}$, either $([\Delta,\alpha];\Omega)$ or $(\Delta;[\Omega,\alpha])$ is consistent.

pf: Assume both $([\Delta,\alpha];\Omega)$ and $(\Delta;[\Omega,\alpha])$ are inconsistent. Then, there must exist a conjunction δ of formulæ in Δ, and a disjunction ω of formulæ in Ω, such that (1): $\vdash_K \delta \wedge \alpha \to \omega$ and (2): $\vdash_K \delta \to \omega \vee \alpha$, whereas (3): $\nvdash_K \delta \to \omega$. From 1 follows $\vdash_K \alpha \to \delta \to \omega$, from this and 2 follows $\vdash_K \delta \to \omega \vee (\delta \to \omega)$, so $\vdash_K \delta \to (\delta \to \omega) \vee (\delta \to \omega)$. Hence $\vdash_K \delta \to \delta \to \omega$, and so $\vdash_K \delta \to \omega$, in contradiction with 3.

Proposition 21 Given a a root-theory $\mathtt{t} = (\Delta_0, \Gamma_0)$ in a modal language $\mathcal{L}_m$, w.r.t. a modal logic M, let $(\Delta;\Omega)$ be a $\mathtt{t}$-dependant theory in $\mathcal{L}_m$, with $\alpha \to \beta = \gamma \in \Omega$. Then there exists a $\mathtt{t}$-dependant theory $(\Delta';\Omega')$ in the same language, with $\alpha \in \Delta'$, $\beta \in \Omega'$, such that $\Delta \subseteq \Delta'$.

pf: From the hypothesis follows that $([\Delta,\alpha];\beta)$ is a consistent k-theory of constant domain in $\mathcal{L}_m$ (by a simple adaptation of the proof in [Gab74], Lemma 3).

Let $\alpha_1, \alpha_2, \ldots$ be an enumeration of the formulæ in $\mathcal{L}_m$. I will define inductively a sequence of k-theories $(\Delta_n;\Omega_n)$ such that for each n, $\Delta_n \subseteq \Delta_{n+1}$ and $\Omega_n \subseteq \Omega_{n+1}$.

Base case: $(\Delta_0;\Omega_0) = ([\Delta,\alpha];\beta)$.

Step case: it can be assumed that $\mathtt{p}_n = (\Delta_n;\Omega_n)$ is defined and consistent, in order to define $\mathtt{p}_{n+1} = (\Delta_{n+1};\Omega_{n+1})$. There are two main cases.

A) $(\Delta_n;[\Omega_n,\alpha_n])$ is consistent.

A1) $\alpha_n = \beta \to \gamma \mid \Box\beta$; then $\Delta_{n+1} = \Delta_n$ and $\Omega_{n+1} = [\Omega_n, \alpha_n]$.

A2) $\alpha_n = \forall x.\beta(x)$. Then, since $\mathtt{p}_n$ has the constant domain property in $\mathcal{L}_m$, there must be in $\mathcal{L}_m$ a variable y such that $\mathtt{p}_{n+1} = (\Delta;[\Omega,\alpha_n, \beta(y/x)])$ is consistent. $\mathtt{p}_{n+1}$ turns out to be of constant domains in $\mathcal{L}_m$ (by adaptation of [Gab74], Lemma 2).

B) $(\Delta_n;[\Omega_n,\alpha_n])$ is inconsistent. Then $([\Delta_n,\alpha_n];\Omega_n)$ is consistent, by Proposition 20. So, one can take $\Delta_{n+1} = [\Delta_n,\alpha_n]$ and $\Omega_{n+1} = \Omega_n$.

Let $\Delta' = \bigcup_{n\in N}\Delta_n$ and $\Omega' = \bigcup_{n\in N}\Omega_n$. Then, by construction, $\mathtt{q} = (\Delta',\Omega')$ is complete, saturated, of constant domain, and $\Delta \subseteq \Delta'$ in $\mathcal{L}_m$. Besides, it cannot prove an inconsistency, otherwise some $\mathtt{p}_n$ would have to prove it. So, $\mathtt{q}$ is a $\mathtt{t}$-dependant theory in $\mathcal{L}_m$.

Proposition 22 Let $(\Delta;\Omega)$ be a consistent r-theory in a modal language $\mathcal{L}_m$ w.r.t. a modal logic M. Then it can be extended to a root-theory $(\Delta';\Omega')$, in a language $\mathcal{L}'_m$ with possibly $\aleph_0$ more propositional variables.

pf: Let $\alpha_1, \alpha_2, \ldots$ be an enumeration of the formulæ in $\mathcal{L}'_m$. It is possible to define inductively a sequence of k-theories $(\Delta_n;\Omega_n)$ such that for each n, $\Delta_n \subseteq \Delta_{n+1}$ and $\Omega_n \subseteq \Omega_{n+1}$.

Base case: $(\Delta_0;\Omega_0) = (\Delta;\Omega)$.

Step case: suppose $(\Delta_n; \Omega_n)$ is defined and consistent. We define $(\Delta_{n+1}; \Omega_{n+1})$. There are two main cases.

A) $(\Delta_n; [\Omega_n, \alpha_n])$ is consistent. Then also $([\Delta_n]; [\Omega_n, \alpha_n, \Box\alpha_n])$ is consistent. In fact, $([\Delta_n, \Box\alpha_n]; [\Omega_n, \alpha_n])$ is inconsistent, using A10.

A1) $\alpha_n = \beta \to \gamma \mid \Box\beta$. Then let $\Delta_{n+1} = \Delta_n$ and $\Omega_{n+1} = [\Omega_n, \alpha_n, \Box\alpha_n]$.

A2) $\alpha_n = \forall x.\beta(x)$.
Then let $\Delta_{n+1} = \Delta_n$ and $\Omega_{n+1} = [\Omega_n, \alpha_n, \beta(y/x), \Box\alpha_n, \Box\beta(y/x)]$, where y is the first new variable not used before. This gives a consistent theory in $\mathcal{L}'_m$ (by adaptation of [Gab74], Lemma 1).

B) $\mathtt{p}_n = (\Delta_n; [\Omega_n, \alpha_n])$ is inconsistent.
Then let $\Delta_{n+1} = [\Delta_n, \alpha_n, \Box\alpha_n]$ and $\Omega_{n+1} = \Omega_n$.
We can prove that $(\Delta_{n+1}; \Omega_{n+1})$ is consistent.
By construction, $\alpha \in \Delta_n$ iff $\Box\alpha \in \Delta_n$ (in the base case, this holds by definition of r-theory). Besides, since $\mathtt{p}_n$ is inconsistent, for appropriate δ, ω, such that δ is a conjunction of formulæ in Δ and ω is a disjunction of formulæ in Ω, we have $\vdash_M \delta \to \omega \vee \alpha_n$. Then $\vdash_M \Box(\delta \to \omega \vee \alpha_n)$, by Rule A13. Then $\vdash_M \Box\delta \to \Box(\omega_1 \vee \alpha_n)$, using Schema A12. Then $\vdash_M \Box\delta \to \Box\omega_1 \vee \Box\alpha_n$, using A15. Then $\vdash_M \Box\delta \to \omega_1 \vee \Box\alpha_n$. It follows that $(\Delta_n; [\Omega_n, \Box\alpha_n])$ is inconsistent. So, by Proposition 20, $([\Delta_n, \Box\alpha_n]; \Omega_n)$ must be consistent.

Then, let $\Delta' = \bigcup_{n\in N} \Delta_n$ and $\Omega' = \bigcup_{n \in N} \Omega_n$. By construction, $\mathtt{q} = (\Delta'; \Omega')$ is a consistent, complete, saturated k-theory of constant domain that extends $(\Delta; \Omega)$ in $\mathcal{L}'_m$ w.r.t. M, and $\alpha \in \Delta_n$ iff $\Box\alpha \in \Delta_n$. So, $\mathtt{q}$ is a root-theory.

It is also useful to prove the following (similar to [Gab81, Lemma 3.4.3]).

Proposition 23 Let $\mathtt{t}$ be a root-theory in a language $\mathcal{L}$ w.r.t. a logic K, and let $(\Delta; \Omega)$ be a $\mathtt{t}$-dependant theory. Then there exists a terminal $\mathtt{t}$-dependant theory $(\Delta'; \Omega')$ in the same language, such that $\Delta \subseteq \Delta'$.

pf: Let $\gamma = \forall x.x \vee \sim x$. Since $\vdash_K \approx\gamma$ (by Proposition 14), it must be $\gamma \to \bot \in \Omega$. Hence, by Proposition 21, there exists a $\mathtt{t}$-dependant theory $\mathtt{p} = (\Delta'; \Omega')$ in $\mathcal{L}$, such that $[\Delta, \gamma] \subseteq \Delta'$. For every formula α in $\mathcal{L}$, $\alpha \vee \sim\alpha \in \Delta'$, as $\gamma \vdash_M \alpha \vee \sim\alpha$ and $\mathtt{p}$ is saturated. But then, again by saturation of $\mathtt{p}$, either $\alpha \in \Delta'$ or $\sim\alpha \in \Delta'$.

3.7.4.1 Completeness for the non-modal and the N-modal logics

Theorem 1 [Soundness and completeness for *C2*] For any formula α in a language $\mathcal{L}_i$, $\vdash_{C2} \alpha$ iff, for every *C2*-model $\mathcal{M}$, $\models_M \alpha$.

pf: As in [Gab81] (completeness of *C2h*).

Here I am going to present a completeness proof for *ND2*, pointing out, besides, how it is possible to simplify it into a completeness proof for *D2*. Another lemma is needed, first.

Proposition 24 Given a root-theory $\mathtt{t} = (\Delta; \Omega)$ in a language $\mathcal{L}_m$ w.r.t. an N-modal logic M, for any consistent k-theory $(\Delta'; \Omega')$ such that $\Delta \subseteq \Delta'$, it is the case that $\Box\alpha \in \Delta'$ iff $\Box\alpha \in \Delta$, and that $\sim\Box\alpha \in \Delta'$ iff $\sim\Box\alpha \in \Delta$.

pf: Follows from the fact that a root-theory is saturated and the logic has Schema A14. So, for any $\alpha \in \mathcal{L}_m$, either $\Box\alpha \in \Delta$ or $\sim\Box\alpha \in \Delta$.

It is now possible to move on to the proof of the main theorem, in all similar to that presented in [TSB02].

Theorem 2 [Soundness and completeness for *ND2*] For any formula α in a language $\mathcal{L}_m$, $\vdash_{ND2} \alpha$ iff, for every *ND2*-model $\mathcal{M}$, $\models_M \alpha$.

pf: *Left to right.* It is routine to check that the axioms are valid, and that the inference rules are validity-preserving in every model defined according to Def.16.

Right to left. The idea is to show, given a non-theorem, how to build a counter-model, where the minimum is a root-theory (referred to as $\mathtt{t}$), and the other elements of the frame are $\mathtt{t}$-dependant theories. The interpretation is the canonical one (each propositional letter is interpreted as itself).

Let us assume $\nvdash_{ND2} \alpha$, for α in $\mathcal{L}_m$. Then, there must be a consistent r-theory (Δ, Ω) in $\mathcal{L}_m$, with $\alpha \in \Omega$, and consequently, by Proposition 22, also a root-theory $\mathtt{t} = (\Delta_0, \Omega_0)$ which extends (Δ, Ω) in an extended language $\mathcal{L}'_m$. Then a counter-model $\mathcal{K} = (\mathcal{S}, \mathcal{R}, \rho)$ in $\mathcal{L}'_m$, with $\mathcal{S} = (S, \leq, \mathbf{0})$, can be built as follows.

1. Let S be the set of all the $\mathtt{t}$-dependant theories (Δ', Ω') such that $\Delta \subseteq \Delta'$.
2. Let $(\Delta', \Omega') \leq (\Delta''; \Omega'')$ iff $\Delta' \subseteq \Delta''$.

3. Let $\mathbf{0} = (\Delta_0; \Omega_0)$.
4. For any variable $x \in \mathcal{L}'_m$, let $\rho(x) = \{(\Delta; \Omega) | x \in \Delta\}$.
5. Let $\mathcal{R} = \{X | X = \{(\Delta; \Omega) | \alpha \in \mathcal{L}'_m \; \& \; \alpha \in \Delta\}\}$.

A) $\mathcal{S}$ is a *D2*-frame.

a) By construction, $(S, \leq)$ is a partial order and has a minimum.

b) $\mathcal{S}$ satisfies the atomicity condition. In fact, as a consequence of Proposition 23, for each $\mathtt{a} \in S$ there is a terminal $\mathtt{b} \in S$ such that $\mathtt{a} \leq \mathtt{b}$.

c) $\mathcal{S}$ satisfies condition *FC*. In fact, since all the instances of Schema A9 are in Δ, for any formula β in $\mathcal{L}'_m$ there must be a variable x such that $\|\beta\|_\rho = \|x\|_\rho$ (by saturation of the theory).

B) $\mathcal{K}$ is a *ND2*-model.

In order to prove this, it is by now enough to show that the canonical interpretation can be extended to all the formulæ, as follows.

B') Given $(\Delta; \Omega) \in S$, for any formula γ in $\mathcal{L}'_m$, $(\Delta; \Omega) \in \|\alpha\|_\rho$ iff $\gamma \in \Delta$.

Both halves of this proof (LtR and RtL) are given by induction on the complexity of formulæ.

LtR) Assume $(\Delta; \Omega) \in \|\gamma\|_\rho$, to prove $\gamma \in \Delta$.

a1) $\gamma = \alpha \to \beta$. If $\gamma \notin \Delta$, then $\gamma \in \Omega$, since any $\mathtt{t}$-dependant theory is complete. Then, by Proposition 21, there exists a $\mathtt{t}$-dependant theory $(\Delta'; \Omega')$ in the same language, with $\alpha \in \Delta'$, $\beta \in \Omega'$, $\Delta \subseteq \Delta'$. The induction hypothesis can be applied. So $(\Delta; \Omega) \leq (\Delta'; \Omega')$, $(\Delta'; \Omega') \vDash_M \alpha$ and $(\Delta'; \Omega') \nvDash_M \beta$. Given the interpretation rule for $\to$ in Def. 16, this is not compatible with $(\Delta; \Omega) \in \|\gamma\|_\rho$.

a2) $\gamma = \forall x.\alpha(x)$. Since $(\Delta; \Omega)$ is of constant domain, if $\gamma \in \Omega$, then, for some variable $y \in \mathcal{L}'_m$, $\alpha(y/x) \in \Omega$. Applying the induction hypothesis and the interpretation rule for $\forall$, we get a contradiction.

a3) $\gamma = \Box\alpha$. Since $(\Delta; \Omega)$ is a $\mathtt{t}$-dependant theory, if $\gamma \in \Omega$, then $\alpha \notin \Delta_0$. Applying the induction hypothesis, $(\Delta_0; \Omega_0) \nvDash_M \alpha$, and then, applying the interpretation rule for $\Box$, $(\Delta; \Omega) \nvDash_M \Box\alpha$, in contradiction with the assumption.

RtL) Assume $\gamma \in \Delta$, to prove $(\Delta; \Omega) \in \|\gamma\|_\rho$.

b1) $\gamma = \alpha \to \beta$. If $(\Delta;\Omega) \notin \|\gamma\|_\rho$ then, by Def. of interpretation, there exists $(\Delta';\Omega') \in W$ such that $(\Delta;\Omega) \leq (\Delta';\Omega')$, and so $\Delta \subseteq \Delta'$, with $(\Delta';\Omega') \vDash \alpha$ and $(\Delta';\Omega') \nvDash \beta$. So, by LtR (first half of the proof), $\alpha \in \Delta'$ and, by induction hypothesis, $\beta \notin \Delta'$. Since $\gamma \in \Delta'$ by assumption, it follows by saturation of the theory that $\beta \in \Delta'$, a contradiction.

b2) $\gamma = \forall x.\alpha$. If $(\Delta;\Omega) \notin \|\gamma\|_\rho$ then, applying the interpretation rule for $\forall$, $(\Delta;\Omega) \notin \|\alpha(y/x)\|_\rho$ for some $y \in \mathcal{L}'_m$. Hence, by induction hypothesis, $\alpha(y/x) \notin \Delta$. A contradiction follows.

b3) $\gamma = \Box\alpha$. If $(\Delta;\Omega) \notin \|\gamma\|_\rho$ then, by Def. of interpretation, $(\Delta_0;\Omega_0) \notin \|\alpha\|_\rho$. Then, by induction hypothesis, $\alpha \notin \Delta_0$. Since $(\Delta;\Omega)$ is a $\mathtt{t}$-dependant theory, by Proposition 24, it follows $\Box\alpha \notin \Delta$.

This concludes the proof of the completeness theorem for *ND2*.

This proof can be modified in order to show the completeness of *D2* and *ND2*.

Theorem 3 [Soundness and completeness for *D2*] For any formula α in a language $\mathcal{L}_i$, $\vdash_{D2} \alpha$ iff, for every *D2*-model $\mathcal{M}$ in that language, $\vDash_M \alpha$.

pf: The proof of Theorem 2 can be modified by omitting all the aspects related to modality. So, the canonical model is just a set of ck-theories in $\mathcal{L}_i$.

Theorem 4 [Soundness and completeness for *NC2*] For any formula α in a language $\mathcal{L}_m$, $\vdash_{NC2} \alpha$ iff, for every *NC2*-model $\mathcal{M}$, $\vDash_M \alpha$.

pf: The proof of Theorem 2 can be modified omitting all the aspects related to terminability (so, Proposition 23 is not used).

The following shows that the correspondence between modal and N-modal models is one-to-one. Essentially, N-modalities do not add anything new — they just reflect in the language something that is otherwise expressed at the meta-level.

Proposition 25 Every *D2*-model (*C2*-model) $(\mathcal{F}, \mathcal{R}, \rho)$ can be extended in a unique way into a *ND2*-model (*NC2*-model) $(\mathcal{F}, \mathcal{R}', \rho')$, so that for every formula α that does not contain modal operators, $\|\alpha\|_\rho = \|\alpha\|_{\rho'}$. Moreover, every *ND2*-model (*NC2*-model) can be obtained this way.

pf: By the interpretation rule for $\Box$, every N-modal model can be uniquely determined by a frame together with an interpretation of the formulæ that do not contain modal operators.

3.7.4.2 Completeness for the V-modal logics

The following lemmas will be used in the completeness proof.

Proposition 26 Let $\mathtt{t} = (\Delta_0; \Omega_0)$ be a root-theory in a language $\mathcal{L}_m$, w.r.t. a V-modal logic M, and let $\mathtt{p} = (\Delta; \Omega)$ be a $\mathtt{t}$-dependant theory. Then there exists a $\mathtt{t}$-dependant root-theory $\mathtt{t}' = (\Delta'; \Omega')$ s.t. for every formula α, $\Box\alpha \in \Delta$ iff $\Box\alpha \in \Delta'$.

pf: The construction of Proposition 22 can be used. Here, for the base case, one can take a consistent r-theory $\mathtt{s} = (\Delta''; \Omega'')$ of constant domain that is extended by $\mathtt{p}$, and such that $\alpha \in \Delta''$ iff $\Box\alpha \in \Delta$. Taking $\mathtt{s}$ to be of constant domain saves us from extending the language.

Proposition 27 Let $\mathtt{t}_{i\in I} = (\Delta_i; \Omega_i)$ be a family of root-theories in a language $\mathcal{L}_m$, for a V-logic M. Then, in case $\mathtt{d} = (\bigcup_{i\in I} \Delta_i; \bigcap_{i\in I} \Omega_i)$ is consistent, it is a root-theory.

pf: By the definition of $\mathtt{d} = (\Delta; \Omega)$ it follows that, if it is consistent, it is indeed a consistent, complete, k-theory of constant domains, saturated w.r.t. M. Moreover, it can be proved (by induction on the length of the derivation) that $\alpha \in \Delta$ iff $\Box\alpha \in \Delta$. So, in that case, $\mathtt{d}$ is a root-theory.

It is now possible to prove the main theorem.

Theorem 5 [Soundness and completeness for *VD2*] For any formula α in a language $\mathcal{L}_m$, $\vdash_{VD2} \alpha$ iff, for every *VD2*-model $\mathcal{M}$, $\models_M \alpha$.

pf: *Left to right.* It is routine to check that the axioms are valid, and that the inference rules are validity-preserving in every model defined according to Def.19.

Right to left. Assume $\nvdash_{VD2} \alpha$, for α in $\mathcal{L}_m$. Then, there must be a consistent r-theory (Δ, Ω) in $\mathcal{L}_m$, with $\alpha \in \Omega$, and consequently by Proposition 22, also a root-theory $\mathtt{t} = (\Delta_0, \Omega_0)$ such that $\Delta \subseteq \Delta_0$, in an extended language $\mathcal{L}'_m$. Then a counter-model $\mathcal{K} = (\mathcal{S}, \mathcal{R}, \rho)$ in $\mathcal{L}'_m$, with $\mathcal{S} = (S, \leq, \mathbf{0}, V)$, can be built as follows:

1. Let S the set of all the ck-theories (Δ', Ω') such that $\Delta \subseteq \Delta'$.
2. Let V be the set of all the root-theories (Δ', Ω') such that $\Delta \subseteq \Delta'$.
3. Let $(\Delta', \Omega') \leq (\Delta''; \Omega'')$ iff $\Delta' \subseteq \Delta''$.

4. Let $\mathbf{0} = (\Delta_0; \Omega_0)$.
5. For any variable $x \in \mathcal{L}'_m$, let $\rho(x) = \{(\Delta; \Omega) | x \in \Delta\}$.
6. Let $\mathcal{R} = \{X | X = \{(\Delta; \Omega) | \alpha \in \mathcal{L}'_m \;\&\; \alpha \in \Delta\}\}$.

A) $\mathcal{S}$ is a *VD2*-frame.

Here it suffices to show that the set V is closed for bounded subsets. In fact, by Proposition 27, if w.r.t. $\leq$ the least upper bound of a family of root-theories is a consistent k-theory, then it is a root-theory.
For the rest, the proof of point A is in all similar to the corresponding proof in Thm. 1.

B) $\mathcal{K}$ is a *VD2*-model.

It is enough to show that the canonical interpretation can be extended to all the formulæ, as follows.

B') Given $(\Delta; \Omega) \in S$, for any formula γ in $\mathcal{L}'_m$, $(\Delta; \Omega) \in \|\alpha\|_\rho$ iff $\gamma \in \Delta$.

LtR) Assume $(\Delta; \Omega) \in \|\gamma\|_\rho$, to prove $\gamma \in \Delta$. The proof is by induction on the complexity of formulæ.

a1) $\gamma = \alpha \to \beta \mid \forall x.\alpha(x)$. Similar to the corresponding cases in Thm. 1.

a3) $\gamma = \Box\alpha$. First observe that $(\Delta; \Omega)$ extends some root theory. Let $(\Delta'; \Omega')$ be any of them. So, if $\gamma \in \Omega$, then $\alpha \notin \Delta'$. Applying the induction hypothesis, $(\Delta'; \Omega') \not\models_M \alpha$, and then, applying the interpretation rule for $\Box$, $(\Delta; \Omega) \not\models_M \Box\alpha$, in contradiction with the assumption.

RtL) Assume $\gamma \in \Delta$, to prove $(\Delta; \Omega) \in \|\alpha\|_\rho$ (proof by induction).

b1) $\gamma = \alpha \to \beta \mid \forall x.\alpha(x)$. Similar to the corresponding cases in Thm. 1.

b3) $\gamma = \Box\alpha$. If $(\Delta; \Omega) \notin \|\gamma\|_\rho$ then, by definition of interpretation, every root-theory $\mathtt{q} = (\Delta'; \Omega')$ which is extended by $(\Delta; \Omega)$ is such that $\mathtt{q} \notin \|\alpha\|_\rho$. So, by induction hypothesis, $\alpha \notin \Delta'$. Hence, by applying Proposition 26, $\Box\alpha \notin \Delta$.

Theorem 6 [Soundness and completeness for *VC2h*] For any formula α in a language $\mathcal{L}_m$, $\vdash_{VC2} \alpha$ iff, for every *VC2*-model $\mathcal{M}$, $\models_M \alpha$.

pf: The proof of Theorem 5 can be modified omitting all the aspects related to terminal theories.

The semantics of V-modal logics can be naturally associated to the idea of a multiplicity of N-modal frames, all of them included in a most comprehensive one. This idea will be briefly expanded in Section 5.4.

Chapter 4

Spatial structures

Order topologies (or Alexandroff spaces, see Section 2.4), although quite incompatible with the metrics of continuous geometry, can be useful in order to give a topological foundation for digital representation [Kop92]. The logics that have been presented in Chapter 3 can be used to express spatial notions, whenever the space that is represented can be abstracted into an order topology. Before discussing the actual encodings (in the next chapter), first I will present the topological semantics associated to the Kripke models of those logics. I will then extend slightly the notion of topological interpretation, in order to make the encoding of topological constraints easier. I will introduce semantically the connectivity relations that matter the most in our context. I will finally introduce a notion of granular model for those relations.

4.1 Topological semantics

Topological semantics for intuitionistic logic (both for *IPL* and for predicate calculus) have been introduced in [Tar56, RS63] and widely investigated since then [RS63, Gab81, FS79, Moe82]. Topological semantics for an axiomatisable ISPL can be introduced in analogy with those for predicate calculus. As it has been already observed, the results in Section 2.8 could already be used to define topological models for some of the logics. Here, however, I prefer to introduce topological models on top of the Kripke semantics, restricting to Alexandroff spaces. The reason for doing this is, essentially, the fact that here the main goal is to interleave logical notions (truth, consequence) and topological ones.

The topological semantics that is given here rests on the identification of Kripke frames with Alexandroff spaces, where the upper-closed sets are the opens. The only opens that are represented in the logical language, however, are those that correspond to truth-sets for some formula. Those are the opens over which substitutional quantification can range. It is useful to remind that it is not possible to consider a complete semantics based exclusively on the *principal* models, i.e. on those models in which quantification ranges over all the opens [Kre97, Skv97]. This fact might be regarded as a reason for overlooking the relationship between topology and ISPL. On the other hand, as it has been discussed in the Introduction (Section 1.2), the restriction to models where the spatial objects are denumerable has a positive value here, since then the regions may be regarded as computational objects. This suggests a sense in which the second-order incompleteness of an axiomatisable ISPL may come together with something useful, from the point of view of computational topology.

4.1.1 Kripke models and topology

It is useful to state here the following consequences of the definitions given in Sections 2.4, 3.7.1:

Proposition 28

1. There is a one-to-one correspondence, up to isomorphism, between (partial) orders and (T_0) Alexandroff spaces, such that the order is isomorphic to the specialisation order of the corresponding topology. That is, (T_0) Alexandroff spaces can be represented as (partial) orders and vice-versa.
2. Kripke *C2*-frames can be represented as T_0 prime, Alexandroff spaces, and vice-versa.
3. *D2*-frames can be represented as T_0, prime, atomic, Alexandroff spaces, and vice-versa.

pf:

1. Consequence of the definitions and of the observations in Section 2.4.
2. By Def. 15, observing that prime spaces (Def. 2) correspond to those partial orders that have a minimum.
3. The atomicity condition for pre-orders (Def. 14) corresponds to the topological atomicity condition (Def. 6).

As an immediate consequence, every Kripke model $((S, \leq, \mathbf{0}), \mathcal{R}, \rho)$ can be regarded as an interpretation into a topological space $(S, \mathcal{U}_{\leq})$. Moreover, given the hereditary condition (see Section 3.7.3), every formula is interpreted as an open set in the Alexandroff space associated to the Kripke frame. Hence, $\mathcal{R}$ can be interpreted as a subset of the opens.

In order to give a topological interpretation of the N-modality, the Boolean values can be represented as opens (*true* as the whole space and *false* as the empty set). Then, the relations $=$, $\neq$, $\sqsubseteq$ and $\not\sqsubseteq$ (called here *extensional relations*) can be associated to functions $\mathcal{R} * \mathcal{R} \mapsto \{\top, \bot\}$, as follows.

Definition 24 In a space $(S, \mathcal{O})$, for $A, B \in \mathcal{O}$:

$$\begin{array}{lll} A =^t B & = S & \text{iff } A = B, \\ & = \varnothing & \text{otherwise.} \\ A \neq^t B & = S & \text{iff } A \neq B, \\ & = \varnothing & \text{otherwise.} \\ A \sqsubseteq^t B & = S & \text{iff } A \sqsubseteq B, \\ & = \varnothing & \text{otherwise.} \\ A \not\sqsubseteq^t B & = S & \text{iff } A \not\sqsubseteq B, \\ & = \varnothing & \text{otherwise.} \end{array}$$

It is now possible to introduce formally a notion of topological model, by defining a notion of topological interpretation into a Kripke model. Given the one-to-one correspondence between Kripke frames and prime Alexandroff spaces, interpreting into a frame turns out to be equivalent to interpreting into a space.

Proposition 29 Given a Kripke model $\mathcal{M} = ((S, \leq, \mathbf{0}), \mathcal{R}, \rho)$ for a logic $H \in \{C2, D2, NC2, ND2\}$, in a language $\mathcal{L}$, let the *topological interpretation* of each formula be defined as its truth-set w.r.t. to ρ, ie $\|\alpha\|_\rho$ (see Def. 20). Then:

(a) For any formula α, the topological interpretation satisfies the following:

1. $\|\alpha \to \beta\|_\rho = \|\alpha\|_\rho \Rightarrow \|\beta\|_\rho$
2. $\|\forall x.\alpha(x)\|_\rho = \bigwedge_{y \in Var} \|\alpha(y/x)\|_\rho$
3. $\|\bot\|_\rho = \varnothing$
4. $\|\top\|_\rho = S$
5. $\|\alpha \wedge \beta\|_\rho = \|\alpha\|_\rho \sqcap \|\beta\|_\rho$
6. $\|\alpha \vee \beta\|_\rho = \|\alpha\|_\rho \sqcup \|\beta\|_\rho$
7. $\|\exists x.\alpha(x)\|_\rho = \bigvee_{y \in Var} \|\alpha(y/x)\|_\rho$

8. $\| \sim \alpha \|_\rho = \|\alpha\|_\rho^*$ (pseudo-complement)
9. $\| \approx \alpha \|_\rho = \|\alpha\|_\rho^{**}$ (regularisation).
10. $\|\alpha \leftrightarrow \beta\|_\rho = (\|\alpha\|_\rho \Leftrightarrow \|\beta\|_\rho)$
    where $\|\alpha\|_\rho \Leftrightarrow \|\beta\|_\rho = (\|\alpha\|_\rho \Rightarrow \|\beta\|_\rho) \sqcap (\|\beta\|_\rho \Rightarrow \|\alpha\|_\rho)$ (equivalence).

(b) Moreover, in the models for the N-modal logics:

1. $\|\Box\alpha\|_\rho = \|\alpha\|_\rho =^t S$
2. $\| \sim \Box\alpha\|_\rho = \|\alpha\|_\rho \neq^t S$
3. $\| \Diamond \alpha\|_\rho = \|\alpha\|_\rho \neq^t \varnothing$ (non-emptiness).
4. $\|\alpha \supset \beta\|_\rho = \|\alpha\|_\rho \sqsubseteq^t \|\beta\|_\rho$.
5. $\|\Box(\alpha \to \beta)\|_\rho = \|\alpha\|_\rho \sqsubseteq^t \|\beta\|_\rho$.
6. $\| \sim \Box(\alpha \to \beta)\|_\rho = \|\alpha\|_\rho \not\sqsubseteq^t \|\beta\|_\rho$.

(c) For any point $\mathsf{p} \in S$, for any $\alpha \in \mathit{Wff}$, forcing and satisfiability can be expressed topologically, as follows.
For any point $\mathsf{p} \in S$, let $\mathsf{p} \uparrow_{\mathcal{R}} = \bigwedge\{X \in \mathcal{R} : \mathsf{p} \in X\}$.
Let $\mathsf{p} \Vdash \alpha$ hold iff $\mathsf{p} \uparrow_{\mathcal{R}} \sqsubseteq \|\alpha\|_\rho$ (*topological forcing*).
Let $\Vdash_M \alpha$ hold iff $\|\alpha\|_\rho = S$ (*topological satisfaction*).

1. $\mathsf{p} \models \alpha$ iff for every $A \in \mathcal{R}$ s.t. $\mathsf{p} \in A$, it holds $A \sqsubseteq \|\alpha\|_\rho$.
2. $\mathsf{p} \models \alpha$ iff $\mathsf{p} \Vdash \alpha$.
3. Given $A \in \mathcal{O}$, the relation $A \sqsubseteq \|\alpha\|$ holds iff for every $\mathsf{p} \in A$, it is the case that $\mathsf{p} \Vdash \alpha$.
4. $\models_M \alpha$ iff $\Vdash_M \alpha$.

pf: (a) and (b) follows from the definition of Kripke models (Def. 16) and from those of the topological operators (Section 2.7 and Def. 24).
(c) follows from Def. 21 and the consequences of Def. 20.

Although essentially equivalent, the Kripke interpretation and the topological one are conceptually different. The topological interpretation associates formulæ with topological "objects" — the opens. The logical operators may be interpreted as topological operators — something that transform objects into other objects. On the other hand, the Kripke interpretation is based on a notion of forcing, i.e. of truth of a formula at a point. The logical operators may then be interpreted in terms of meta-logic concepts. Since each point can be associated to the opens in which it is contained, forcing can also be represented as a relation between subspaces and formulæ (i.e. as topological forcing, as defined in Proposition 29 *c*).

This parallel is what essentially gives the possibility of using the language of ISPL in order to express the objects, the functions and the relations of a simple, region-based ontology, as suggested in Section 1.3.

In particular, it seems natural to assume that a simple object can be obtained as the interpretation of a propositional constant. Objects that are more complex can be built from the simple ones by using topological operators. A simple topological relation can be expressed as an expression (either an equality or an inequality) between such objects. Logic then allows more complex relations to be defined from the simpler ones. The topological interpretation of forcing makes it possible to express if a relation holds on a subspace. On the other hand, the fact that a relation holds on certain subspaces defines an object, and this aspect gives to the ontology an intrinsically higher-order character. After all, the different "roles" (objects, operators and relations) are covered by the same "actors" — the primitives of an ISPL language, possibly extended with the N-box operator. In order to make it possible to distinguish between the spatial aspect and the logical aspect, it seems useful, to introduce a "reflective" extension of the language of ISPL, by allowing certain topological expressions into it (see the next section).

4.1.2 Definability and spatial models

Topology can be given a computational interpretation. In a general sense, such an interpretation is one that associates open sets with computations [Smy92, Vic89].

In the spatial context, a computation can be taken to be a program that defines a region — i.e. essentially, a program that is particularly significant from the point of view of the spatial *information* that it can give. The obvious example could be that of a program that reads a sensor input and produces, as an effect, a spatial representation. When regions are considered as a way of specifying such programs, it does not seem necessary to require that all of them are associated with terminating computations. For example, "the smallest region such that etc." may ultimately rest on an infinitely detailed picture, but still may be associated to a computational meaning, even if, in real life, that picture has to be replaced with some approximation. Of course, admitting at the level of specification objects that are not computationally finite does not mean expecting that they are actually computed — an analogy could be made with the lazy evaluation of functions allowed by some programming languages [Hud00].

On the other hand, even when specifications do not generally lead to actual computations, it seems important to assume that they can be compared in order to decide whether they are identical or not. Hence, it can be useful to assume that they are recursively defined. So, w.r.t. a topological space $\mathcal{S}$ and an enumerable language $\mathcal{L}$, once a topological interpretation of the formulæ of $\mathcal{L}$ into $\mathcal{S}$ has been fixed, the idea here is to take spatial objects to be the opens that are expressible (or definable) as formulæ of $\mathcal{L}$. It should be observed that what matters here is not the recursive characterisation of the objects, rather that of the expressions that are referring to them.

In the following, I am going to associate the Kripke models of ISPL to a specification language — indeed, a very simple one, defined by extending the logical language ($\mathcal{L}_i$ or $\mathcal{L}_m$) with the topological expressions that are obtained by interpreting topologically the formulæ of that language. This can be thought of as adding new constants to the logical language. Depending only on the model, these constants are always going to be interpreted as themselves. This extension, without substantially increasing the expressive power of the language, makes it possible to write down expressions in which a distinction can be made between specifying the computational content of a region with a topological expression, and expressing logically some topological information about it. The notion of model must be extended correspondingly.

The topological expressions that are allowed here are those that can be built by using the operators of a complete Heyting algebra (compare Proposition 29 with Section 2.8), possibly extended with the extensional relations (as given in Def. 24). It turns out unnecessary to introduce those operators as primitive ones, as they can be obtained by topological interpretation of the logical ones, instead.

Definition 25 Let $\mathcal{S} = (S, \mathcal{O})$ be a T_0, prime Alexandroff space — by Proposition 28, this means that there is an isomorphic Kripke frame $(S, \leq, \mathbf{0})$ — and let $\mathcal{M} = ((S, \leq, \mathbf{0}), \mathcal{R}, \rho)$ be a Kripke model based on it, for a logic $H \in \{C2, D2, NC2, ND2\}$ in a language $\mathcal{L}$.

Let τ be the topological interpretation determined by ρ (defined as in Proposition 29).

Let $\mathcal{L}_e$ be the extension of $\mathcal{L}$, where the set *EvalExp* of the *evaluable expressions* (meta-variables $\omega, \psi, \ldots$) is defined as the smallest one that includes the propositional variables and constants *Var* $\cup$ *Const* of $\mathcal{L}$, together with the expressions for the opens in $\mathcal{R}$ (meta-variables $A, B, \ldots$), and such that it is closed w.r.t. the constructs $\omega \to \psi$, $\forall x.\omega(x)$, $\tau(\omega)$ and, for the modal logics, $\Box\omega$.

Then, let τ be extended to an interpretation for all the evaluable expressions, defined as follows (I recall here all the clauses and conditions, see Def. 16):

1. $\tau(A) = A$, for every $A \in \mathcal{R}$.
2. $\tau(\alpha) \in \mathcal{R}$, for every propositional variable or constant $\alpha \in \mathcal{L}$.
3. $\tau(\omega \to \psi) = \tau(\omega) \Rightarrow \tau(\psi)$
4. $\tau(\forall x.\omega(x)) = \bigwedge_{Y \in \mathcal{R}} \tau(\omega[Y/x])$
5. [for the modal logics]: $\tau(\Box\omega) = \tau(\omega) =^t S$
6. Full Comprehension (condition *FC*): for every formula α in the language $\mathcal{L}$, there exists a variable x such that $\tau(\alpha) = \tau(x)$.

The extended τ will also be said to be an *evaluation* for *EvalExp*.

The structure $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ is said to be a *spatial model* based on $\mathcal{S}$ and determined by $\mathcal{R}$ (the reference to τ will be often omitted — see the comment below).

$\mathcal{R}$ is said to be the *collection of the definable opens* (the *DO-set* for short) of $\mathcal{Z}$.

Let the *topological forcing* relation $\Vdash$ (as defined in Proposition 29) be extended to the evaluable expressions, w.r.t. the extended τ.

An evaluable expression ω is said to be *valid* (or *satisfied*) in $\mathcal{Z}$ iff $\tau(\omega) = S$, where this is also written $\Vdash_Z \omega$.

From the condition *FC*, since $\mathcal{R}$ is by definition the image of τ, it follows that $\bigwedge_{Y \in \mathcal{R}} \tau(\omega[Y/x])$ is an equivalent way to write $\bigwedge_{y \in Var} \tau(\omega(y/x))$.

Although an evaluation is used to define a model, the important element here is the collection of the definable opens. Clearly, for every two spatial models $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$, $\mathcal{Z}' = (S, \mathcal{O}, \mathcal{R}, \tau')$ that differ with each other only for the evaluation, for any $A \in \mathcal{R}$, $\tau(A) = \tau'(A)$, and for any expression ω, $\Vdash_Z \omega$ iff $\Vdash_{Z'} \omega$. We can say that $\mathcal{Z}$ and $\mathcal{Z}'$ are equivalent as spatial models. I will sometimes refer to the equivalence class $(S, \mathcal{O}, \mathcal{R})$ as to a *generic* spatial model, determined by a DO-set on a topological space, omitting any explicit reference to the evaluation, whenever this does not cause confusion.

A DO-set can also be regarded as an Heyting algebra that has all — and only — the arbitrary meets and joins that can be represented using the quantifiers. In fact, $\top$ (or S), $\bot$ (or $\varnothing$) and the operators $\sqcap, \sqcup, \bigvee$ can be defined — via the logical definition of the corresponding logical operators (see Def. 8 and Proposition 29).

A DO-set does not give in general a topology, since arbitrary joins and arbitrary meets of definable opens are not in general definable opens. However, some topological notions can be adapted. This is the case for the notions of prime set (Def. 2) and of atom (Def. 5). In the following, let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R})$ be a generic spatial model.

Definition 26 In $\mathcal{Z}$, $A \in \mathcal{O}$ is said to be an $\mathcal{R}$-prime iff, for every open cover $\mathcal{D} \subseteq \mathcal{R}$ of A, there exists $B \in \mathcal{D}$ such that $A \sqsubseteq B$.

Definition 27 In $\mathcal{Z}$, $A \in \mathcal{O}$ is said to be an $\mathcal{R}$-atom iff, for every non-empty $X \in \mathcal{R}$, if $X \sqsubseteq A$ then $X = A$.

Spatial models can be said to be have a basis w.r.t. their DO-sets, in the following sense:

Proposition 30 In $\mathcal{Z}$, for any $\mathtt{p} \in S$, let $\mathtt{p}\uparrow_{\mathcal{R}} = \bigwedge\{X \in \mathcal{R} | \mathtt{p} \in X\}$ be the $\mathcal{R}$-pointed subset determined by $\mathtt{p}$. Let $\mathcal{B} = \{\mathtt{p}\uparrow_{\mathcal{R}} | \mathtt{p} \in S\}$. Then:
(a) $\mathcal{B} \subseteq \mathcal{O}$, and every $X \in \mathcal{R}$ can be obtained as an arbitrary join on elements of $\mathcal{B}$ — hence $\mathcal{B}$ is also said to be an $\mathcal{R}$-basis in $\mathcal{Z}$.
(b) $\mathcal{B}$ is the set of the $\mathcal{R}$-primes in $\mathcal{Z}$.

pf: (a) For every $\mathtt{p} \in S$, $\mathtt{p}\uparrow_{\mathcal{R}}$ exists and is open — although not necessarily a definable open — since the topology $(S, \mathcal{O})$ is Alexandroff. Clearly, every $X \in \mathcal{R}$ is covered by the join of the $\mathcal{R}$-pointed subsets determined by its elements.
(b) Similar to Proposition 5 a.

A restriction of the specialisation order to the definable opens can be introduced as follows:

Definition 28 [$\mathcal{R}$-specialisation order] In $\mathcal{Z}$, $\mathtt{p} \prec_{\mathcal{R}} \mathtt{q}$ iff, for every $A \in \mathcal{R}$, $\mathtt{p} \in A$ implies $\mathtt{q} \in A$.

A notion of restriction can be defined, as follows.

Definition 29 In a spatial model $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$, let $A \in \mathcal{O}$ be an $\mathcal{R}$-prime. The restriction of $\mathcal{Z}$ to A can be defined as $\mathcal{Z}|A = (A, \{X \sqcap A | X \in \mathcal{O}\}, \{Y \sqcap A | Y \in \mathcal{R}\}, \tau')$, where $\tau'(\omega) = \tau(\omega) \sqcap A$.

It can be checked that $\mathcal{Z}|A$ gives a spatial model, by identifying all $\mathtt{p} \in S$ such that $\mathtt{p} \uparrow_{\mathcal{R}} = A$.

In general, I will say that a spatial model based on the space $\mathcal{S}$ has a topological property whenever $\mathcal{S}$ has it, provided that property does not depend on $\mathcal{R}$.

4.2 Spatial qualitative relations

Given a domain D of regions and a family $\mathcal{F}$ of n-ary relations on D, the relations in $\mathcal{F}$ are said to be jointly exhaustive, pairwise disjoint (JEPD) whenever they determine a partition over D^n. JEPD relations can play a significant role in taxonomic tasks, and hence in qualitative reasoning.

As an example, properties such as connectedness, primeness, atomicity, can be quite naturally associated to notions of component, and hence they can lead to classifications based on component counting — i.e. there can be classifications of regions based on the number of their connected (prime, atomic) components.

On the other hand, families of JEPD binary relations such as those introduced, in the context of the RCC system, as $RCC5$ and $RCC8$ [RCC92], as well as similar [CDF95] and related ones [CG96, BS98, CDF97], can be used to represent the information about connectivity.

Here I am going to focus on binary relations between opens sets, that can be defined in a topological space $\mathcal{S} = (S, \mathcal{O})$ and that can be compared, from a semantical point of view, with the $RCC5$ and $RCC8$ ones. In order to introduce those relations semantically, it is useful first to consider the following way to classify points w.r.t. on open set:

Proposition 31 Given the space $\mathcal{S}$, for every $A \in \mathcal{O}$, A determines on S a partition such that, for each $\mathtt{p} \in S$:

1. $\mathtt{p}$ is an *internal* point of A iff $\mathtt{p} \in A$.
2. $\mathtt{p}$ is an *external* point of A iff $\mathtt{p} \in A^*$.
3. $\mathtt{p}$ is an *internal boundary* point of A iff $\mathtt{p} \notin A$ and $\mathtt{p} \in A^{**}$.
4. $\mathtt{p}$ is an *external boundary* point of A iff $\mathtt{p} \notin A^*$ and $\mathtt{p} \notin A^{**}$.

The following are essentially set-theoretical relations, although here they will be treated in a topological context. The simplest topological models for these relations can be found by interpreting regions as open sets in a discrete space. Characteristically, in such spaces boundary points do not exists, since every subset is clopen (open and closed) — and so, complement and pseudo-complement coincide.

Definition 30 For any discrete space $(S, \mathcal{O})$, with $A, B \in \mathcal{O}$:

1. $A \sqsubseteq B$: A is a *part* of (or *includes*) B.
2. $A \sqsubseteq B$ and $A \neq B$: A is a *proper part* of B.
3. $A = B$: A and B are *equivalent.*
4. $A \sqcap B = \varnothing$: A and B are *disjoint.*
5. $A \sqcap B \neq \varnothing$: A and B are *overlapping.*
6. $A \sqcap B \neq \varnothing$ and $A \sqcap B^* \neq \varnothing$: A and B are *partially overlapping.*

The JEPD relations that correspond to the $RCC5$ ones are the following: proper part and its inverse, equivalence, disjointness and partial overlap [RCC92].

The topological aspect becomes more significant when the boundary points do exist. Then, it is useful to introduce the following distinction:

Definition 31 In $\mathcal{S}$, for $A, B \in \mathcal{O}$:

1. A and B are tangential with one another in a *loose* sense, iff they share some external boundary point — they are non-tangential otherwise.
2. A and B are tangential with one another in a *strict* sense, iff they share a non-empty open subset of their boundaries (i.e., for some open set, its non-empty intersection with the boundary) — they are non-tangential otherwise.

In each of the two senses, the following relations can be defined:

Definition 32 In $\mathcal{S}$, for $A, B \in \mathcal{O}$:

1. A is a *tangential proper part* of B iff A is a proper part of B, and they are tangential.
2. A is a *non-tangential part* of B iff A is a part of B and they are non-tangential.
3. A and B are *externally connected* (or *adjacent*) iff A and B are disjoint and tangential.

4. A and B are *inter-disconnected* (disconnected with each other) iff A and B are disjoint and non-tangential.
5. A and B are *interconnected* (connected with each other) iff they are either overlapping or adjacent.

Strict interconnection is closely related to the notion of *firm connection* in [CBGG97].

The JEPD relations that correspond to the $RCC8$ ones are the following ones: tangential proper part and inverse, non-tangential part and inverse, equivalence, partial overlap, disjointness, apartness [RCC92].

Intuitively, when two opens A and B are adjacent in the strict sense, there exists a path from one to the other which lays in their regularised union $(A \sqcup B)^{**}$. This is not generally the case, when A and B are only adjacent in the loose sense. The following can be proved:

Proposition 32 In the space $\mathcal{S}$, the opens A and B are adjacent in the strict sense iff $(A \sqcup B)^{**} \neq A^{**} \sqcup B^{**}$.

pf: Any point belonging to an open subset of the boundary that A and B have in common is an internal boundary point of $A^{**} \sqcup B^{**}$ (and vice-versa) — hence it does not belong to $A^{**} \sqcup B^{**}$, but it belongs to $(A \sqcup B)^{**}$.

In RCC, the $RCC8$ relations are all defined in terms of interconnection, which is the only primitive one, and they can be interpreted in the loose sense [Ren98]. Some of the RCC definitions involve quantification over regions. It is useful to observe here that all the $RCC8$ relations can be encoded elementarily (without using quantification) once inclusion, adjacency, disjointness and overlapping are given — this is essentially the line followed by the encodings given in Section 5.3.4).

On the other hand, in the logics that are considered here, the relations that have been defined can be expressed only in the strict sense. This is essentially due to the fact that these logics are interpreted into prime spaces — by Proposition 1, this is enough to make every two non-empty open sets loosely interconnected. It is possible to have representations based on modal ISPL that allow for both the strict and the loose senses, by weakening the modal axioms in order to drop the primeness restriction, but they will not be covered in this thesis (see Chapter 8).

With respect to primeness, the following shows that any connected space can be transformed into a prime one, in such a way that preserves emptiness, inclusion and

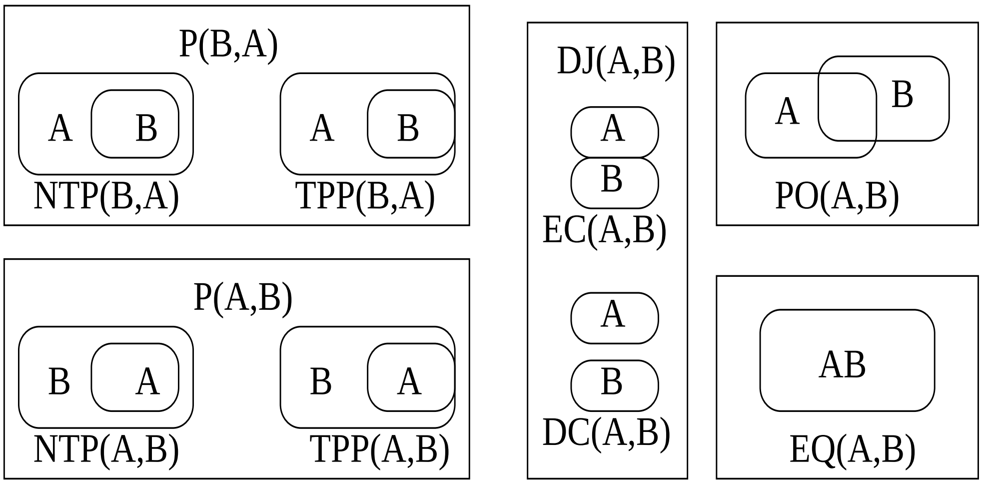

Figure 4.1: $RCC8$ (Non-Tangential Part, Tangential Proper Part, External Connection, DisConnection, Partial Overlap, EQuality) and $RCC5$ (Part, DisJointness, PO, EQ).

strict adjacency — hence, also disjointness and overlapping, and so all of the $RCC8$ strict relations.

Proposition 33 Let $\mathcal{S} = (S, \mathcal{O})$ be a connected space. Let $\mathcal{S}'$ be the one-point compactification of $\mathcal{S}$, as defined in Proposition 2. Then, for every $A, B \in \mathcal{O}$:

1. $A \sqsubseteq B$ holds in $\mathcal{S}$ iff it holds in $\mathcal{S}'$.
2. $A = \varnothing$ holds in $\mathcal{S}$ iff it holds in $\mathcal{S}'$.
3. When $A \sqcap B = \varnothing$, for A, B non-empty, $(A \sqcup B)^{**} = A^{**} \sqcup B^{**}$ holds in $\mathcal{S}$ iff it holds in $\mathcal{S}'$.

pf: 1 and 2 are immediate. For 3, it is enough to note that, since $\mathcal{S}$ is connected, $A^{**} \sqcup B^{**} = S$ iff either $A^{**} = S$ or $B^{**} = S$, given the conditions.

This means that shifting to prime spaces is essentially not a problem from the point of view of the strict relations.

4.3 Granularity

Spatial models for computers are generally digital ones . This is trivially true for the raster models. It is true also for the vector models, insofar as these are associated with tessellations of an abstract geometrical representation. These operations, normally associated to polyhedral decompositions (triangulations, in the two-dimensional case), or to partitions by regular grids (quadrangular, hexagonal, etc.), produce meshes that can be viewed, from an abstract point of view, as digital spaces [LT92, OBS92].

The basic elements in a mesh are the cells. From a high-level point of view, cells may be treated like black boxes, quite independently from their internal details, geometry and implementation. The level of detail in the representation may vary. It generally depends on how fine is the decomposition, just as in a raster model it can be associated to the resolution (i.e. the number of pixels used to represent a unit region).

The *granularity* of a mesh may be regarded as an abstract measure of its level of detail. Different meshes may share the same level of granularity. As an example, two different translations of the same grid on an image will give two meshes that have the same granularity, although they might show different details.

In general, notions of granular models are introduced in order to compare digital representations at different levels of detail, from an abstract point of view [Ste00b, SW98, BDFM95]. A notable example is given by the *multi-resolution models* presented in [BDFM95] and proposed as a high-level framework for cartographic operations. In [Ber98] they are used in order to define a categorial model for "safe" map transformation.

The notion of *abstract cell complex* (ACC), arising from the discretisation of geometrical space, has been proposed as a theoretical foundation for digital geometry [Kop92, Kov92]. An ACC can be defined on $\Re^n$, as a partition of the points in i-dimensional, connected, regular subspaces (the cells), with $0 \leq i \leq n$. As an example, a 2-dimensional space can be partitioned in disjoint open sets, open lines and points. Regions can be associated to sets of cells. Multi-resolution models are based on ACCs — hence, they are not strictly speaking region-based [Ber98]. Each level in the model is an ACC. At each level, topological information defines a *horizontal* structure (inclusion and adjacency relations) that is preserved by the mappings between different levels. These mappings are surjective, continuous functions, that determine a *vertical* structure (i.e. different representations of the same region). The mappings preserve the relations of inclusion and interconnection (by continuity) and apartness (by an additional requirement).

The idea of granular model that is introduced here is essentially that of an abstract, region-based representation that is given at different levels of detail, that can be embedded into a spatial model (as defined in Section 4.1.2) and that can be expressed, at least up to a point, in the language of an N-modal ISPL. In contrast with the multi-resolution models in [Ber98], here each level of detail can be represented as a discrete space — i.e. as a plain set of disjoint subsets, embedded in the spatial model. Hence, the horizontal structure is defined by the relations corresponding to the $RCC5$ family, whereas adjacency is represented globally. This yields some aspects of the preservation property w.r.t. adjacency for free, but also means that many points may have to be added to the original representation, in order to obtain a faithful model, and in such a way that deserves some explanation.

A discrete space (see the definition in Section 2.1) may be regarded as a naive topological description for a mesh — each atom, simply disjoint from all the other atoms and possibly given as a singleton, represents a cell. The fact that adjacency cannot be represented in a discrete space gives a well-known problem in graphics [RS02]. One way to cope with it is by dealing with the adjacency relation explicitly and independently from any topological definition. An alternative approach is based on digital topology [Kop92]. The main idea there is to embed the discrete space $\mathcal{S}$ into a T_0 order topology $\mathcal{S}'$, in which the terminal points represent the points of $\mathcal{S}$. All the other points in $\mathcal{S}'$ represent connections — more precisely, they represent boundaries between adjacent cells. This approach, as it appears in [Kop92], is based on order topologies that are quite specific (they are products of the Khalimski line — a space that is homeomorphic to the topology of the natural intervals on the real line). In the models that I am presenting here, this kind of solution is adopted in a quite more general way.

4.3.1 Granular models

Cell complexes can be used to represent abstractly geographic maps of different granularity — in particular, the unit regions in each map can be associated to a class of cells in an abstract model. Different levels of granularity correspond to different classes of cells — where cells of coarser levels are meant to be comparatively larger. Within a model, geographic entities may be represented at different levels of granularity. Each representation can be regarded as a region, in an abstract sense, and different representations can be compared — so, for example, given two such, it could be asked, whether they both have the same granularity, or whether they both represent the same entity at different levels. Granular models are meant to be a framework for such applications.

Given the atomic spatial model $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R})$ in a generic sense (i.e. we do not need to worry about τ), it is possible to build into it a notion of granular

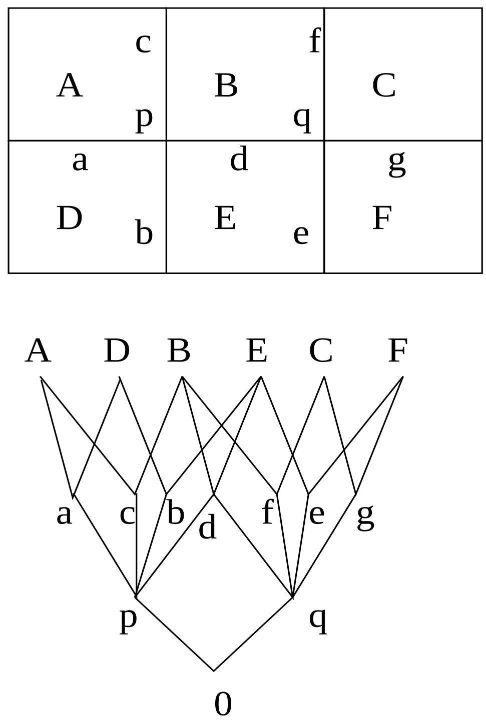

Figure 4.2: A cell complex, represented as a planar graph (above), can be associated to a partial order (below), using the following convention: in the cell complex, upper-case letters denote regions (open sets, without boundary), lower-case $a, \ldots$ denote boundary lines (without ending points), whereas $p, \ldots$ denote boundary end-points. The partial order is represented as a directed, acyclic graph where the elements are labelled nodes. 0 is an extra element added for strong compactification. Regions are associated to the upper-closed sets in the partial order. The upper-case letters are used in order to label nodes, as well as to denote the upper-closed sets determined by the corresponding nodes (clearly, in this example, all these sets are singletons).

model according to the following guidelines. Each level of granularity (i.e. each abstract mesh) can be regarded as a set of cells, where the cells of the same level are represented as definable opens that are disjoint with each other. Moreover, cells are always in some sense undecomposable units — the notion of $\mathcal{R}$-primeness can be helpful in order to model this aspect (Def. 26). It seems a reasonable simplification here to assume that there exists a coarsest level at which the whole space is treated as a single cell, as well as a finest, *terminal* level. At the terminal level the cells may be said to be *atomic* and can be represented as the smallest regular opens in the model. These are the opens that are obtained by regularisation of $\mathcal{R}$-atoms (Def. 27).

The terminal points are the only ones that represent the actual locations, as they may be defined by embedding the terminal level into the geometric space. All the other points in the spatial model represent clusters of atomic cells that may correspond to the cells of some coarser level.

All the levels ultimately cover the same space — this can be understood by saying that for each atomic cell A and for each level of granularity $\mathcal{G}$, there is one and only one cell B of that level, that contains all the terminal elements of A, i.e. such that $A \sqsubseteq B^{**}$.

Given the assumption that $\mathcal{Z}$ is atomic (see Def. 6), the sum (or regularised union) of all the cells of the same level always gives the whole space. The idea of a vertical relation between cells of different levels may be generalised, so to introduce a natural order of refinement between levels of granularity. More formally:

Definition 33 Given the atomic spatial model $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R})$:

1. A subset $\mathcal{A} \subseteq \mathcal{R}$ can be said to be an *abstract mesh* (or *level of granularity*) in $\mathcal{Z}$ iff the following conditions are satisfied:
   - For each $A \in \mathcal{A}$, A is $\mathcal{R}$-prime.
   - For each $A, B \in \mathcal{A}$, either $A = B$ or $A \sqcap B = \bot$.
   - $(\bigvee\{X | X \in \mathcal{A}\})^{**} = S$.
2. Given two abstract meshes $\mathcal{A}, \mathcal{B}$, it can be said that $\mathcal{A}$ is *finer* than $\mathcal{B}$ (or that $\mathcal{B}$ is *coarser* than $\mathcal{A}$, written $\mathcal{A} \ll \mathcal{B}$), iff for every $A \in \mathcal{A}$ there is a $B \in \mathcal{B}$ such that $A \sqsubseteq B^{**}$. B is then said to *generalise* A.
3. Given $\mathcal{A} \ll \mathcal{B}$, a surjective function $c : \mathcal{A} \mapsto \mathcal{B} \cup \{\bot\}$ is said to be a *coarsening* of $\mathcal{A}$ into $\mathcal{B}$ iff it maps the cells of $\mathcal{A}$ either into the cells of $\mathcal{B}$ that generalise them or into $\bot$. It is said to be a *maximal* coarsening iff it never maps into $\bot$.
   An injective function $r : \mathcal{B} \mapsto \wp(\mathcal{A})$ is said to be the *refinement* of $\mathcal{B}$ into $\mathcal{A}$ w.r.t. the coarsening c iff it maps each cell $B \in \mathcal{B}$ into the inverse image of B w.r.t. c, i.e. iff, for every $A \in \mathcal{A}$ s.t. $c(A) \in \mathcal{B}$, there holds $A \in r(c(A))$.

Coarsenings and refinements can be used as a way to extend the class of the definable opens. In fact, a region might have been originally given as a definable union of cells at a certain level of granularity. This open set can then be mapped at other levels.

Definition 34 A *granular model* can be defined as a structure $\mathcal{G} = (\mathcal{Z}, \mathcal{P}, \Delta, \ll, \Omega)$, where;

1. $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R})$ is an atomic spatial model.

2. $\mathcal{P}$ is the collection of the $\mathcal{R}$-primes in $\mathcal{Z}$, and $\mathcal{P} \subseteq \mathcal{R}$.
3. Δ is a collection of abstract meshes in $\mathcal{Z}$, such that $\{\top\} \in \Delta$ and $\mathcal{P} \in \Delta$.
4. $\ll$ is the order of granular refinement.
5. Ω is a collection of coarsenings (with corresponding refinements) in Δ, such that whenever $\mathcal{A} \ll \mathcal{B}$ and $c : \mathcal{A} \mapsto \mathcal{B}$ is a maximal coarsening, then $c \in \Omega$.

A point to be further investigated could be, what kind of constraints on the mappings in Ω may correspond to the notion of abstract mesh. Seemingly, a Galois connection [Bir40] could be defined from a granular model — however this issue will not be pursued here.

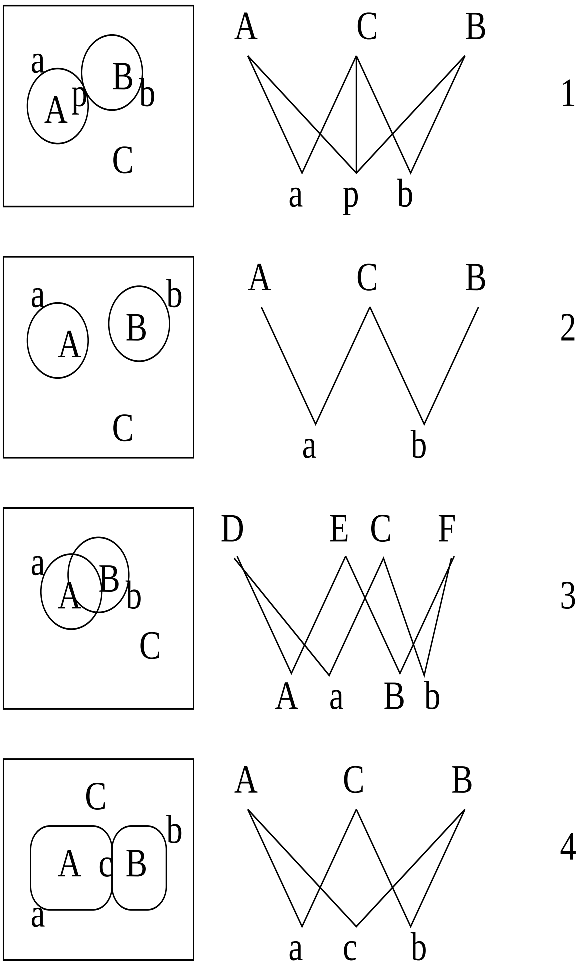

Figure 4.3: The cell complexes, represented as planar graphs on the right, can be associated to the partial orders on the left, following the convention defined in Fig. 4.2. The regions (open sets) C, D, E, F are defined topologically as $C = (A \sqcup B)^*$, $D = A \sqcap B^*$, $E = A \sqcap B$ and $F = B \sqcap A^*$. a and b are meant to be the open boundaries between A and C and between B and C, respectively. c is the open boundary between A and B. p is a single boundary point. It can be noted that in the model 1, the regions A and B are loosely adjacent. In 4 they are strictly adjacent. In 2 they are apart. In 3 they partially overlap.

Chapter 5

Spatial representation

In the previous chapter, the basic semantical structures have been introduced. Here, it will be shown how some of the notions related to granularity and connectivity can be expressed in the language of ISPL and of modal ISPL, relying on the syntax introduced with the spatial models (Def. 25). I will start by considering the expression of basic spatial notions related to granular models (Section 5.1), then I will move on to the encoding of relations (Section 5.2) and to specific properties of spaces (Section 5.3).

By saying that a notion can be expressed in a logic, I mean that there are expressions of that logic that represent it — by default at the object-level, in the sense that has been clarified in Section 1.5).

5.1 Spatial objects

The ontology of the granular models introduced in Section 4.3.1 is essentially based on atomic cells, cells, regions and meshes. In the following section I will examine how these notions can be expressed formally.

5.1.1 Atomic cells

Given a granular model and its embedding in a generic spatial model $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R})$, it seems natural to associate the cells of the terminal level (i.e. the atomic cells) with elements that are maximal w.r.t. the specialisation order, or better, to stay closer to logical definability, w.r.t. the $\mathcal{R}$-specialisation order ($\prec_{\mathcal{R}}$, Def. 28). The points that are maximal w.r.t. $\prec_{\mathcal{R}}$ (including the terminal points) are in fact exactly those that are contained in some of the $\mathcal{R}$-atoms (Def. 27). The $\mathcal{R}$-atoms are not generally regular — they may well have internal boundary points, something that is not really wanted. This can be fixed, by taking their regularisation instead. For this reason, I refer to the regularisations of $\mathcal{R}$-atoms as to the atomic cells. Since these cells can be intuitively associated to the raster level of a spatial representation, I will also refer to the union over all of them (i.e. the union over the terminal level) as to the *screen*. In any atomic space, the screen turns out to be dense — i.e. its regularisation covers the whole space — following immediately from the fact that it contains all the terminal points.

Proposition 34 Given $\mathcal{Z}$ as above:
(*a*) $A \in \mathcal{O}$ is an atom iff A is non-empty and for every $X \in \mathcal{O}$, either $A \sqsubseteq X$ or $A \sqsubseteq X^*$.
(*b*) $A \in \mathcal{O}$ is an atomic cell iff A is regular, non-empty and for every $X \in \mathcal{R}$, either $A \sqsubseteq X^{**}$ or $A \sqsubseteq X^*$.
(*c*) The screen is $\bigwedge_{X \in \mathcal{R}}(X^{**} \sqcup X^*)$.

pf: (*a*) *Left to right.* Since A is an atom, it cannot be divided into two proper parts, hence either $X \sqcap A$ or $X^* \sqcap A$ must be empty.
Right to left. Assume that there exists $X \in \mathcal{O}$ that is a non-empty proper part of A. Then $A \not\sqsubseteq X$ and $A \not\sqsubseteq X^*$.
(*b*) Similar to (*a*).
(*c*) From (*b*) follows that a point $\mathsf{p} \in S$ is in the screen iff, for every $X \in \mathcal{R}$, either $\mathsf{p} \in X^{**}$ or $\mathsf{p} \in X^*$ — hence $\mathsf{p} \in X^{**} \sqcup X^*$.

This shows that the screen is in general a definable open. On the other hand, the fact that $\mathcal{R}$-atoms and atomic cells can be specified, does not mean in general that single ones are definable.

Proposition 35 Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model, and let α, β be formulæ in a modal language that is interpreted by τ.

1. A formula α denotes a regular open in $\mathcal{Z}$ iff, for
   $\mathsf{regl}(\alpha) = {\approx}\alpha \leftrightarrow \alpha$
   the following holds:
   $\Vdash_Z \mathsf{regl}(\alpha)$
2. A formula α denotes an atomic cell in $\mathcal{Z}$ iff, for
   $\mathsf{atmcell}(\alpha) = \Diamond(\alpha) \wedge \Box\mathsf{regl}(\alpha) \wedge \forall x.\Box(\alpha \rightarrow {\approx}x) \vee \Box(\alpha \rightarrow {\sim} x)$
   $\Vdash_Z \mathsf{atmcell}(\alpha)$

3. The screen in $\mathcal{Z}$ is denoted by $\mathsf{screen} = \forall x. \approx x \vee \sim x$.
4. The screen can be constrained to be the union of the atomic cells that are definable — which also gives that all the atomic cells are definable in $\mathcal{Z}$ — once taken

   $\Lambda_1 = \exists x.(\Box \mathsf{atmcell}(x) \wedge x)$

   by adding the following constraint:

   $\Vdash_Z \mathsf{screen} \leftrightarrow \Lambda_1$

pf:

1. For any $A \in \mathcal{R}$, by the properties of τ (Def. 25 and Proposition 29), $\mathsf{regl}(A)$ evaluates to the same as $A^{**} \Leftrightarrow A$, and so $\Vdash_Z \mathsf{regl}(\alpha)$ iff $\Vdash_Z A^{**} =^t A$, which specifies regularity.
2. By Proposition 34 (b), the fact that A is an atomic cell in $\mathcal{Z}$ can be specified with the following expression:

   $(A \neq^t \varnothing) \wedge (A =^t A^{**}) \wedge \forall x.(A \sqsubseteq^t (\tau(x))^{**}) \vee (A \sqsubseteq^t (\tau(x))^{*})$

   For $\tau(\alpha) = A$, this expression evaluates to the same as $\mathsf{atmcell}(\alpha)$ in $\mathcal{Z}$ — in particular, it is valid iff $\mathsf{atmcell}(\alpha)$ is valid.
3. From Proposition 34 (c),

   $\Vdash_Z \mathsf{screen} \leftrightarrow \forall x.(\tau(x))^{**} \sqcup (\tau(x))^{*}$
4. $\Vdash_Z \Lambda_1$ iff $\Vdash_Z \mathsf{screen} \leftrightarrow \bigvee_{X \in \mathcal{R}} \tau(\Box \mathsf{atmcell}(X) \wedge X)$

   The expression on the right of the equality gives the definition for the open that is obtained as a join of all the atomic cells, since $\tau(\Box \mathsf{atmcell}(X) \wedge X)$ can be read as: X such that $\mathsf{atmcell}(X)$ is valid.

5.1.2 Cells

In the generic spatial model $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R})$, it seems natural to associate cells to undecomposable units, and hence to regular $\mathcal{R}$-primes (Def. 26). In fact, whenever a cell A can be decomposed into the cells $B_{i \in I}$ at a finer level, it seems useful to distinguish between A represented as the sum over $B_{i \in I}$, i.e. $A = (\bigvee_{i \in I} B_i)^{**}$, and the union over its decomposition, i.e. $\bigvee_{i \in I} B_i$. This distinction is essential in order to express an aspect related to connectivity: A can be regarded as a cluster of finer cells that are relatively close to one another. Such a distinction could not be made in a discrete spaces, where for every open set, we have $X = X^{**}$; whereas in general, $X^{**} \sqsubseteq X$ but not vice-versa.

The fact that the cell A is an $\mathcal{R}$-prime, also means that A contains some points that are minimal w.r.t. the $\mathcal{R}$-specialisation order and that are indistinguishable from each other w.r.t. $\mathcal{R}$ — hence, A behaves like a submodel. This requires that the spatial model contains, in addition to the terminal points, at least one more point for each cell which is not atomic. It seems reasonable to assume that, at the coarsest level of granularity, the whole space is treated as a single cell — hence the requirement for the spatial model to be prime itself.

Proposition 36 Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model.

1. A formula α denotes an $\mathcal{R}$-prime in $\mathcal{Z}$ iff, for
   $\mathsf{prime}(\alpha) = \sim\Box(\alpha \to \exists x.x \wedge \sim\Box(\alpha \to x))$
   $\Vdash_{\mathcal{Z}} \mathsf{prime}(\alpha)$
2. A formula α denotes a cell in $\mathcal{Z}$ iff, for
   $\mathsf{cell}(\alpha) = \mathsf{regl}(\alpha) \wedge \mathsf{prime}(\alpha)$
   $\Vdash_{\mathcal{Z}} \mathsf{cell}(\alpha)$
3. Every non-empty definable open in $\mathcal{Z}$ is a union of cells iff, for
   $\Lambda_2 = \forall x. \Diamond x \to \Box(x \leftrightarrow \exists y.y \wedge \Box\mathsf{cell}(y) \wedge \Box(y \to x))$
   $\Vdash_{\mathcal{Z}} \Lambda_2$

pf:
1. From Def. 26 b, for any $A \in \mathcal{R}$, an $\mathcal{R}$-prime A in $\mathcal{Z}$ can be characterised by saying that it is not covered by the join of its definable proper parts, using the following evaluable expression:
   $A \not\sqsubseteq^t \bigvee_{X \in \mathcal{R}} \tau(X \wedge (A \not\sqsubseteq^t X))$
   For $\tau(\alpha) = A$, this expression is valid in $\mathcal{Z}$ iff $\mathsf{prime}(\alpha)$ is valid.
2. Since $\Vdash_{\mathcal{Z}} \mathsf{cell}(\alpha)$ iff $\Vdash_{\mathcal{Z}} \mathsf{regl}(\alpha)$ and $\Vdash_{\mathcal{Z}} \mathsf{prime}(\alpha)$.
3. By correspondence with the expression
   $(A \neq^t \varnothing) \to (A =^t \bigvee_{Y \in \mathcal{R}} \tau(Y \wedge \Box\mathsf{cell}(Y) \wedge (Y \sqsubseteq^t A)))$

A method to generate a spatial model from an actual representation, can be devised by recursively applying the strong-compactification technique considered in Propositions 2, 33.

5.1.3 Regions and meshes

Regions intuitively correspond to sets of cells. Since cells of the same level are assumed to be disjoint, any subset of them can also be represented algebraically, in the way of mereology, i.e. as the union over its elements. A union of regular opens is not generally a regular open. However, in an atomic spatial model, the correspondence between unions of atomic cells and their sums (i.e. regularised unions) is one-to-one. This fits well with the idea that, at the terminal level, every region can be represented indifferently either as a union of cells or as a sum. At coarser levels the correspondence between sums and unions is not generally one-to-one. In fact, there may be many different opens that share the same regularisation. This makes it possible to distinguish between the *absolute representation* of a region as a sum of cells — a regular open — and its *granular representation* as a union of cells, corresponding to a particular level of granularity. The granular representation of a region at the terminal level may also be called its *terminal representation.*

For each region such that A is its absolute representation and B is its terminal one, for any granular representation X of that region, it is straightforward to see that $B \sqsubseteq X$ and $X \sqsubseteq A$.

Not all the definable opens in the model need to represent well-behaved decompositions — indeed, some of them might not be acceptable as regions in the granular sense either. It is possible however to write down an expression that forces every non-empty definable open to be a join of cells (Proposition 36).

The notion of abstract mesh, as a set of disjoint cells such that their sum gives the whole space, is probably hard to capture without resorting to third-order expressions (not treated here). However, it is at least possible to specify the relation between a mesh and its cells, as follows:

Proposition 37 Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model. In $\mathcal{Z}$, the formulæ α, β may denote respectively an abstract mesh and one of its cells, iff, for

$\mathsf{cell\_of\_mesh}(\beta, \alpha) = \mathsf{cell}(\beta) \wedge (\beta \rightarrow \alpha) \wedge (\alpha \rightarrow \beta \vee \sim \beta)$

the following constraints are satisfied:

$\Vdash_Z \approx \alpha$

$\Vdash_Z \mathsf{cell\_of\_mesh}(\beta, \alpha)$

$\Vdash_Z \forall xy. \mathsf{cell\_of\_mesh}(x, \alpha) \wedge \mathsf{cell\_of\_mesh}(y, \alpha) \supset (x \leftrightarrow y) \vee \sim(x \wedge y)$

pf: $\mathsf{cell\_of\_mesh}(\beta, \alpha)$ can be read as saying that β is a cell of α. In fact $\alpha \rightarrow \beta \vee \sim \beta$ evaluates the same as $\tau(\alpha) \sqsubseteq^t \tau(\beta) \sqcup (\tau(\beta))^*$, meaning intuitively that $\tau(\alpha)$ does not include any of the boundary points of $\tau(\beta)$.

5.2 Connectivity

It is now possible to consider how high-level information about connectivity can be expressed, in terms of properties and relations between regions. First connectedness will be considered, then the relations that can be associated to $RCC8$.

5.2.1 Connectedness

By a definition of connectedness that is equivalent to that given in Section 2.1, proving that an open set A is connected in a topological space $\mathcal{S} = (S, \mathcal{O})$, is equivalent to showing that there exist two non-emtpy open subsets B, C that divide A, i.e. such that $A \sqcap B \neq \varnothing$, $A \sqcap C \neq \varnothing$, and $A = B \sqcup C$ [Kel55]. This can be simplified by observing that whenever $B, C \in \mathcal{O}$ divide $A \in \mathcal{O}$, then also B, B^* divide A (I will then just say that B divides, or *splits*, A).

Definition 35 Let it be said that $B \in \mathcal{O}$ *does not split* $A \in \mathcal{O}$ in $\mathcal{S}$ iff, either $A \not\sqsubseteq B \sqcup B^*$, or $A \sqsubseteq B$, or $A \sqsubseteq B^*$.

The following then gives another way to define connectedness: $A \in \mathcal{O}$ is connected in $\mathcal{S}$ iff, for every $X \in \mathcal{O}$, X does not split A.

It is convenient now to introduce a weaker definition that refers to definable opens only. Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model in the following.

Definition 36 $A \in \mathcal{O}$ is said to be $\mathcal{R}$-*connected* in $\mathcal{Z}$ iff, for every $X \in \mathcal{R}$, X does not split A.

It is also useful to introduce the following, stronger notions:

Definition 37

1. Let it be said that $B \in \mathcal{O}$ *splits nowhere* $A \in \mathcal{O}$ in $\mathcal{Z}$ iff $(A \Rightarrow B \sqcup B^*) \sqsubseteq (A \Rightarrow B) \cup (A \sqsubseteq B^*)$.
2. $A \in \mathcal{O}$ is said to be *strongly* $\mathcal{R}$-*connected* in $\mathcal{Z}$ (or strongly r-connected) iff, for every $\mathcal{R}$-prime X, it holds that A is $\mathcal{R}$-connected in $\mathcal{Z}|X$ (i.e. in the restriction of $\mathcal{Z}$ to X, see Def. 29).

It is now possible to formalise these notions as follows.

Proposition 38

1. The open denoted by the formula α does not split the open denoted by the formula β iff, for

$\mathsf{ndiv}(\beta, \alpha) = \Box(\beta \to \alpha \vee \sim\alpha) \to \Box(\beta \to \alpha) \vee \Box(\beta \to \sim\alpha)$

$\Vdash_Z \mathsf{ndiv}(\beta, \alpha)$

2. The open denoted by the formula α is $\mathcal{R}$-connected in $\mathcal{Z}$ iff, for

   $\mathsf{con}(\alpha) = \forall x.\mathsf{ndiv}(\alpha, x)$

   $\Vdash_Z \mathsf{con}(\alpha)$

3. The open denoted by the formula α splits nowhere the open denoted by the formula β iff, for

   $\mathsf{ndiv}_s(\beta, \alpha) = (\beta \to \alpha \vee \sim\alpha) \to (\beta \to \alpha) \vee (\beta \to \sim\alpha)$

   $\Vdash_Z \mathsf{ndiv}_s(\beta, \alpha)$

4. The open denoted by the formula α is strongly $\mathcal{R}$-connected in $\mathcal{Z}$ iff, for

   $\mathsf{con}_s(\alpha) = \forall x.\mathsf{ndiv}_s(\alpha, x)$

   $\Vdash_Z \mathsf{con}_s(\alpha)$

pf:

1. From the properties of τ in Proposition 29 and in Def. 25, and from Def. 35.

2. From the general semantical properties as before, using Def. 36. In particular, the expression

   $\forall x.(A \sqsubseteq^t \tau(x) \sqcup (\tau(x))^*) \supset (A \sqsubseteq^t \tau(x)) \vee (A \sqsubseteq^t \tau(x)^*)$

   evaluates to the same as $\mathsf{con}(\alpha)$ for $\tau(\alpha) = A$, and gives a straightforward formalisation of the informal definition.

3. As before, using Def. 38.

4. Expanding the definitions,

   $\mathsf{con}_s(\alpha) = \forall x.(\alpha \to x \vee \sim x) \to (\alpha \to x) \vee (\alpha \to \sim x)$.

   This evaluates the same as the expression

   $\forall x.(A \Rightarrow \tau(x) \sqcup (\tau(x))^*) \to ((A \Rightarrow \tau(x)) \vee (A \Rightarrow \tau(x)^*))$

   for $\tau(\alpha) = A$.

   So, by the definition of evaluation (Def. 25), $\Vdash_Z \mathsf{con}_s(\alpha)$ iff, for all $B \in \mathcal{R}$, $\Vdash_Z (A \Rightarrow B \sqcup B^*) \to (A \Rightarrow B) \vee (A \Rightarrow B^*)$.

   Equivalently, by the definition of topological forcing in Proposition 29, for all $B \in \mathcal{R}$, for all $\mathsf{p} \in S$, if $\mathsf{p} \Vdash A \Rightarrow B \sqcup B^*$ then $\mathsf{p} \Vdash (A \Rightarrow B) \vee (A \Rightarrow B^*)$.

   Equivalently, for all $B \in \mathcal{R}$, for all $\mathsf{p} \in S$, if $\mathsf{p} \Vdash A \Rightarrow B \sqcup B^*$ then either $\mathsf{p} \Vdash A \Rightarrow B$ or $\mathsf{p} \Vdash A \Rightarrow B^*$.

   Equivalently, using Proposition 30 (b) and the definition of $\Rightarrow$ in Section 2.7, for all the $\mathcal{R}$-primes $X \in \mathcal{O}$, if $X \sqcap A \sqsubseteq B \sqcup B^*$ then either $X \sqcap A \sqsubseteq B$

or $X \sqcap A \sqsubseteq B^*$. But this is equivalent to saying that for all the $\mathcal{R}$-primes $X \in \mathcal{O}$, A is $\mathcal{R}$-connected in $\mathcal{Z}|X$, using Def. 29 and Def. 38.

By imposing some constraints on the spatial model, it is possible to force strong $\mathcal{R}$-connectedness to coincide with $\mathcal{R}$-connectedness, for the definable opens that are also regular. It is useful to introduce some properties first.

Definition 38 In the spatial model $\mathcal{Z}$, a subspace $T \in \mathcal{O}$ is said to be *degenerate* iff for every regular $A \in \mathcal{R}$, it holds $T \sqsubseteq \tau(\mathsf{con}_s(A))$ — i.e. iff for every $\mathcal{R}$-prime $X \sqsubseteq T$, it is the case that A is strongly $\mathcal{R}$-connected in $\mathcal{Z}|X$. Otherwise, T is said to be *non-degenerate.*

Definition 39 The spatial model $\mathcal{Z}$ is said to be *disjunctive* iff for every $A \in \mathcal{R}$, either $A = S$, or A is degenerate.

Now it is possible to prove the following.

Proposition 39 Whenever the generic spatial model $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R})$ is disjunctive, for any regular $A \in \mathcal{R}$, A is $\mathcal{R}$-connected iff it is strongly $\mathcal{R}$-connected.

pf: *Left to right.* Straightforward, since from the definitions, in any prime space, strong $\mathcal{R}$-connectedness implies $\mathcal{R}$-connectedness.
Right to left. If $A \in \mathcal{R}$ is regular and is not strongly $\mathcal{R}$-connected in $\mathcal{Z}$ then, for some $B \in \mathcal{R}$, there must be an open $F = A \Rightarrow B \sqcup B^*$ such that $A \Rightarrow B \sqcup B^* \not\sqsubseteq (A \Rightarrow B) \sqcup (A \Rightarrow B^*)$. Then F is not degenerate, since $F \not\sqsubseteq \tau(\mathsf{con}_s(A))$. Since $\mathcal{Z}$ is $\mathcal{R}$-disjunctive, it follows that $F = S$. So A cannot be $\mathcal{R}$-connected in $\mathcal{Z}$.

5.2.2 Non-emptiness

Although in general the N-modal operator $\Diamond$ is needed to express non-emptiness, it can be shown here that there is a close relationship between non-emptiness and a non-modally definable ISPL operator.

The following proposition is a corollary of Definition 38:

Proposition 40 Let $\mathsf{degnr} = \forall x.\mathsf{con}_s(\approx x)$. Then, $\mathcal{Z}$ is degenerate iff $\Vdash_{\mathcal{Z}} \mathsf{degnr}$.

In fact, a spatial model is degenerate whenever all the definable opens that are regular are also strongly $\mathcal{R}$-connected. As a corollary of Definition 39, the following can be obtained.

Proposition 41 Let $\mathcal{Z}$ be a disjunctive, non-degenerate spatial model. Then:

1. For every $A \in \mathcal{R}$, it is the case that $A \sqsubseteq \tau(\mathsf{degnr})$ iff $A \neq S$.
2. Let $\mathsf{nempty}(\alpha) = {\sim}\alpha \to \mathsf{degnr}$. Then, $\Vdash_{\mathcal{Z}} \mathsf{nempty}(\alpha)$ iff $\tau(\alpha) \neq \varnothing$.

pf:
1. Follows immediately from Def. 39.
2. If $\tau(\alpha) = \varnothing$, then $\tau({\sim}\alpha) = S$ and so, since $\mathcal{Z}$ is non-degenerate, $\tau({\sim}\alpha) \not\sqsubseteq \tau(\mathsf{degnr})$. Vice-versa, if $\tau(\alpha) = \varnothing$, then $\tau({\sim}\alpha) \neq S$ and so, since $\mathcal{Z}$ is disjunctive, $\tau({\sim}\alpha) \sqsubseteq \tau(\mathsf{degnr})$.

Of course, it seems hardly possible to express at the object level that the spatial model is non-degenerate without using a modality. Anyway, particularly in disjunctive spatial models, nempty turns out to share significant properties with non-emptiness — so it may be labelled as a *weak* expression of non-emptiness. In particular, the following can be proved, already in *I2*:

Proposition 42 $\vdash_{I2} \mathsf{nempty}(\alpha \wedge \beta) \wedge \mathsf{con}_s(\alpha) \wedge \mathsf{con}_s(\beta) \to \mathsf{con}_s({\approx}(\alpha \vee \beta))$

pf: Mechanised proof carried out with Isabelle (see Section 7.4.3).

Semantically, this means that in any disjunctive spatial model, whenever the intersection between two $\mathcal{R}$-connected opens is weakly non-empty, then also their sum is $\mathcal{R}$-connected.

5.2.3 Interconnection and apartness

Some of the following definitions are already familiar and may be recalled, with reference to Section 4.2. Here they are reintroduced (only in the *strict* sense), for the ease of the reader and for immediate comparison with other notions. Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model.

Definition 40 In $\mathcal{Z}$, for every $A, B \in \mathcal{O}$:

1. A and B are said to be *overlapping* with each other iff their intersection is not empty. Otherwise, they are said to be *disjoint* with each other.

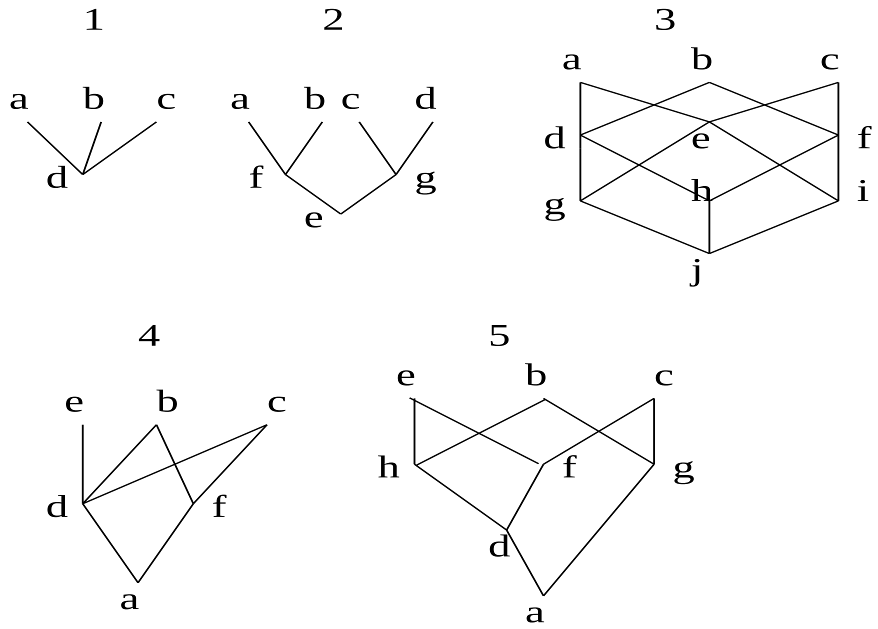

Figure 5.1: A generic spatial model can be defined for each of the frames above, where elements are labelled nodes, by taking $\mathcal{O} = \mathcal{U}_{\leq}$ and $\mathcal{R} = \mathcal{O}$. The models 1, 2 and 3 are $\mathcal{R}$-disjunctive, whereas this is not the case for 4 and 5. In fact, in both 4 and 5, the set $((b\uparrow) \sqcup (c\uparrow))^{**}$ is $\mathcal{R}$-connected in $a\uparrow$, but fails to be so in $d\uparrow$.

2. A and B are said to be *interconnected* iff either they are overlapping, or if the intersection of their closures includes an open subset of their boundaries. Otherwise, they are said to be *apart* from each other.

3. A and B are said to be *strongly interconnected* iff there exist not-empty $X, Y \in \mathcal{R}$ s.t. $X \sqsubseteq A, Y \sqsubseteq B$ and $(X \sqcup Y)^{**}$ is $\mathcal{R}$-connected. Otherwise, they are said to be *weakly apart* from each other.

The difference between the two notions of interconnection that are defined here is exemplified in Figure 5.1. There, in Model 1, the regions $a\uparrow$ and $(b\uparrow) \sqcup (c\uparrow)$ are interconnected but not strongly interconnected.

The following shows how the relations can be formalised.

Proposition 43 In $\mathcal{Z}$, the opens A, B resp. denoted by the formulæ α, β are:

1. disjoint iff

   $\Vdash_Z \sim(\alpha \wedge \beta)$

2. overlapping iff

   $\Vdash_Z \Diamond(\alpha \wedge \beta)$

3. apart iff, for

   $\mathsf{ap}(\alpha,\beta) = \ \sim(\alpha \wedge \beta) \wedge (\approx(\alpha \vee \beta) \rightarrow (\approx\alpha \vee \approx\beta))$

   $\Vdash_Z \mathsf{ap}(\alpha,\beta)$

4. interconnected iff, for

   $\mathsf{ic}(\alpha,\beta) = \sim\Box\mathsf{ap}(\alpha,\beta)$

   $\Vdash_Z \mathsf{ic}(\alpha,\beta)$

5. strongly interconnected iff, for

   $\mathsf{ic}_s(\alpha,\beta) = \exists xy.\Diamond x \wedge \Diamond y \wedge (x \rightarrow \alpha) \wedge (y \rightarrow \beta) \wedge \mathsf{con}(\approx(x \vee y))$

   $\Vdash_Z \mathsf{ic}_s(\alpha,\beta)$

6. weakly apart iff, for

   $\mathsf{ap}_w(\alpha,\beta) = \sim\Box\mathsf{ic}_s(\alpha,\beta)$

   $\Vdash_Z \mathsf{ap}_w(\alpha,\beta)$

7. strongly interconnected, when $\mathcal{Z}$ is disjunctive, iff, for

   $\mathsf{ic}_i(\alpha,\beta) = \exists xy.\mathsf{nempty}(x)\wedge\mathsf{nempty}(y)\wedge(x \rightarrow \alpha)\wedge(y \rightarrow \beta)\wedge\mathsf{con}_s(\approx(x\vee y))$

   $\Vdash_Z \mathsf{ic}_i(\alpha,\beta)$

8. overlapping, when $\mathcal{Z}$ is disjunctive and non-degenerate, iff

   $\Vdash_Z \mathsf{nempty}(\alpha \wedge \beta)$

pf:

1. Since $A \sqcap B =^t \varnothing$ is valid iff $\sim(A \wedge B)$ is.
2. Since $A \sqcap B \neq^t \varnothing$ is valid iff $\Diamond(A \wedge B)$ is.
3. $\Vdash_Z \mathsf{ap}(A,B)$ iff $\Vdash_Z \sim(A \wedge B)$ and $\Vdash_Z (A \sqcup B)^{**} \sqsubseteq^t (A^{**} \sqcup B^{**})$. Then, Proposition 32 and Def. 40 can be used.
4. Straightforward from the previous.
5. By Def. 40, since $\Vdash_Z \mathsf{ic}_s(A,B)$ iff there exist $C, D \in \mathcal{R}$ s.t. $\Vdash_Z (C \neq^t \varnothing) \wedge (D \neq^t \varnothing) \wedge (C \sqsubseteq^t A) \wedge (D \sqsubseteq^t A) \wedge \mathsf{con}((C \sqcup D)^{**})$.
6. Straightforward.
7. Assume that $\mathcal{Z}$ is non-degenerate. Then, using Propositions 39, 41, the same argument as for $\mathsf{ic}_s(A,B)$ can be applied. On the other hand, if $\mathcal{Z}$ is degenerate, by Proposition 40, for every regular open A which is definable, $\Vdash_Z \mathsf{con}_s(A)$, and so also $\Vdash_Z \mathsf{con}_s((A \sqcup B)^{**})$.
8. Consequence of Proposition 41.

The following states a relationship between apartness and $\mathcal{R}$-connectedness.

Proposition 44 For any $A \in \mathcal{O}$, the regular open A^{**} is $\mathcal{R}$-connected in $\mathcal{Z}$ iff there do not exist non-empty $B, C \in \mathcal{R}$ which are apart, and which divide A (i.e., such that $A \sqsubseteq B \sqcup C$, $A \sqcap B \neq \varnothing, A \sqcap C \neq \varnothing$).

pf: *Left to right.* If A is divided by some $B, C \in \mathcal{R}$ that are apart from each other, then A^{**} is divided by B^{**}, C^{**}, and so A^{**} cannot be $\mathcal{R}$-connected, as follows from Def. 36.

Right to left. Assume that A^{**} is not $\mathcal{R}$-connected. Then, there is some $X \in \mathcal{R}$ such that $A^{**} \sqsubseteq X \sqcup X^*$, $A^{**} \not\sqsubseteq X$, $A^{**} \not\sqsubseteq X^*$. Now assume that the disjoint opens $(A \sqcap X)$ and $(A \sqcap X^*)$ are not apart. Hence, also $(A^{**} \sqcap X)$ and $(A^{**} \sqcap X^*)$ are not apart. Then, by Def. 40 and Proposition 32, there must be a point $\mathtt{b} \in S$ such that $\mathtt{b} \in (A^{**} \sqcap (X \sqcup X^*))^{**}$, $\mathtt{b} \notin (A^{**} \sqcap X)^{**}$ and $\mathtt{b} \notin (A^{**} \sqcap X^*)^{**}$. So $\mathtt{b} \in A^{**}$ and $\mathtt{b} \notin X \sqcup X^*$. But then, $A^{**} \not\sqsubseteq X \sqcup X^*$, which gives a contradiction. So $(A \sqcap X)$ and $(A \sqcap X^*)$ must be apart, after all.

The relationship between the "strong" and "weak" notions is the expected one.

Proposition 45 For any $A, B \in \mathcal{R}$ in $\mathcal{Z}$:

1. If A and B are apart, then they are weakly apart.
2. If A and B are strongly interconnected, then they are interconnected.

pf:

1. *Left to right.* If one of A and B is empty, then, by the definitions, they are both apart and weakly apart. Assume then that they are both non-empty. If A and B were strongly interconnected (i.e., not weakly apart), there should be some non-empty opens C, D such that $C \sqsubseteq A$ and $D \sqsubseteq B$, where $(C \sqcup D)^{**}$ is $\mathcal{R}$-connected. But, since A and B are apart, $A^{**} \sqcup B^{**} = (A \sqcup B)^{**}$. Hence $A^{**} \sqcup B^{**} \sqsubseteq A^{**} \sqcup A^*$. But $(C \sqcup D)^{**} \sqsubseteq A^{**} \sqcup B^{**}$, and so $(C \sqcup D)^{**} \sqsubseteq A \sqcup A^*$. However, $(C \sqcup D)^{**} \not\sqsubseteq A$ and $(C \sqcup D)^{**} \not\sqsubseteq A^*$, contradicting the $\mathcal{R}$-connectedness of $(C \sqcup D)^{**}$.
2. Consequence of 1 and of the definitions.

5.2.4 Tangential and non-tangential parts

Still with reference to the strict relations in Section 4.2, it is possible to give the following definitions. Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model.

Definition 41 In $\mathcal{Z}$, for any $A, B \in \mathcal{O}$:

1. A can be said to be a *non-tangential part* (*weakly non-tangential part*) of B iff A is included in B and is apart (weakly apart) from B^*.
2. A can be said to be a *tangential part* (*strongly tangential part*) of B iff A is included in B and is interconnected (strongly interconnected) with B.

In particular, A is a non-tangential part of B^{**} iff A is apart from B^* — similarly for the corresponding weak relations.

The following can be proved immediately from the definitions.

Proposition 46 In $\mathcal{Z}$, for any $A, B \in \mathcal{R}$ such that $A \sqsubseteq B$, the open A is a (weakly) non-tangential part of B iff A is not a (strongly) tangential part of B.

These relations can be formalised as follows.

Proposition 47 In $\mathcal{Z}$, the opens A, B respectively denoted by the formulæ α, β:

1. are in the relation of non-tangential part iff, for
   $\mathsf{ntp}(\alpha, \beta) = (\alpha \to \beta) \wedge \mathsf{ap}(\alpha, \sim\beta)$
   $\Vdash_Z \mathsf{ntp}(\alpha, \beta)$
2. are in the relation of tangential part iff, for
   $\mathsf{tp}(\alpha, \beta) = (\alpha \to \beta) \wedge \mathsf{ic}(\alpha, \sim\beta)$
   $\Vdash_Z \mathsf{tp}(\alpha, \beta)$
3. are in the relation of weakly non-tangential part iff, for
   $\mathsf{ntp}_w(\alpha, \beta) = (\alpha \to \beta) \wedge \mathsf{ap}_w(\alpha, \sim\beta)$
   $\Vdash_Z \mathsf{ntp}_w(\alpha, \beta)$
4. are in the relation of strongly tangential part iff, for
   $\mathsf{tp}_s(\alpha, \beta) = (\alpha \to \beta) \wedge \mathsf{ic}_s(\alpha, \sim\beta)$
   $\Vdash_Z \mathsf{tp}_s(\alpha, \beta)$
5. are in the relation of strongly tangential part iff, for $\mathcal{Z}$ disjunctive, for
   $\mathsf{tp}_i(\alpha, \beta) = (\alpha \to \beta) \wedge \mathsf{ic}_i(\alpha, \sim\beta)$
   $\Vdash_Z \mathsf{tp}_i(\alpha, \beta)$

pf: Quite straightforward, from Def. 41 and Proposition 43.

5.3 Spatial extensions

In the following, I am going to consider some axiomatic extensions of the logics that have been presented in Chapter 3. These extensions can yield some restrictions that turn out to be quite significant, from the point of view of their spatial interpretation.

In Section 5.3.1 I will focus on some extentions that do not involve any modality. In Section 5.3.2 I will deal with aspects that can be related to graphical effectiveness. In Section 5.3.3 I will focus on dimension.

5.3.1 Non-modal restrictions

The disjunctiveness property (Def. 39) can be expressed logically as follows. Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model.

Proposition 48 $\mathcal{Z}$ is disjunctive iff $\Vdash_{\mathcal{Z}} \Sigma_1$, for

$$\Sigma_1 = \forall x. x \vee (x \rightarrow \mathsf{degnr})$$

pf: Straightforward from Defs. 39, 25 and Proposition 40.

In Section 5.2.3 two semantical notions of interconnection have been considered. There is a condition that makes it possible to identify them, and that can be expressed without modalities.

Proposition 49 Let $\mathcal{Z}$ be a disjunctive spatial model such that $\Vdash_{\mathcal{Z}} \Sigma_2$, for

$$\Sigma_2 = \forall xy. \mathsf{ap}(x, y) \vee \mathsf{ic}_i(x, y)$$

Then, for any non-empty $A, B \in \mathcal{R}$:

1. Either A and B are apart or they are strongly interconnected.
2. A and B are apart, iff they are weakly apart.
3. A and B are interconnected, iff they are strongly interconnected.
4. Whenever $A \sqsubseteq B$, A is non-tangential part of B iff A is not strongly tangential part of B.

pf:

1. Straightforward from Proposition 43 and the properties of interpretation.
2. *Left to right.* By Proposition 45. *Right to left.* A and B are not strongly interconnected, by Def. 40. Hence, by 1 and the primeness of $\mathcal{Z}$, they must be apart.
3. Consequence of 2 and the definitions.
4. Consequence of 2,3 and Def. 41.

5.3.2 Connection and diagrams

A connected, regular open set A in a geometric two-dimensional space of coordinates x and y can be represented graphically in an effective way when the boundary of A can be described by a finite number of curve segments, where each curve is obtained as a continuous function of one of the coordinates into the other one.

In Section 1.2 graphical effectiveness has been pointed out as a desirable requirement, from the point of view of a common-sense account of regions.

In general, in a normal space it is possible to have a regular open $A = (\bigcup_{i \in I} A_i)^{**}$ such that it is interconnected with another regular open B, whereas for each $i \in I$, it turns out that A_i and B are apart. These situation can be associated with configurations that are pathological from the point of view of effectiveness. An example is given in [PS98]. A similar one can be built using the function $f(x) = (1/x) * (\mathrm{Sin}(1/x))$, that has no limit as x tends to 0 (see Fig. 5.2). The regions $A = \{(x,y)|x > 0, y > f(x)\}$, $B = \{(x,y)|x > 0, y < f(x)\}$ and $C = \{(x,y)|x < 0\}$ are indeed such that $(A \sqcup B)^{**}$ is interconnected with C, whereas neither A nor B are.

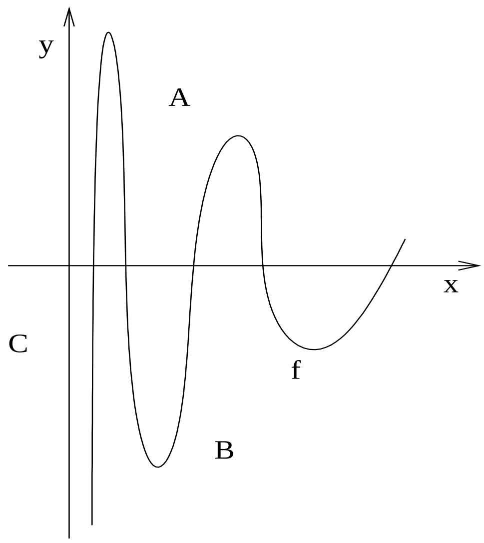

Figure 5.2: The function f and the partition which is determined by it.

A significant step in the direction of a common-sense account of regions, as well as in the direction of graphical effectiveness, seems to be then the introduction of a restriction, very close to that presented in [PS98], that makes it possible to avoid the aforementioned possibility.

Proposition 50 Let $\mathcal{Z}$ be a spatial model such that $\Vdash_{\mathcal{Z}} \Sigma_3$, for

$\Sigma_3 = \forall xyz.\mathsf{ap}(x,y) \wedge \mathsf{ap}(x,z) \rightarrow \mathsf{ap}(x, y \sqcup z)$

For any $\mathcal{R}$-prime T in $\mathcal{Z}$, for any $A, B, C \in \mathcal{R}$, if A and C are apart in $\mathcal{S}|T$, and if B and C are apart in $\mathcal{S}|T$, then $A \sqcup B$ and C are also apart in $\mathcal{S}|T$.

pf: By Def. 43, the definition of restriction (Section 2.1) and the properties of interpretation (Proposition 29).

The following shows the corresponding property for interconnection.

Proposition 51 Whenever $\mathcal{Z}$ satisfies Σ_1, Σ_2 and Σ_3, for any $A, B, C \in \mathcal{R}$, if $(A \sqcup B)^{**}$ and C are interconnected, then either A and C or B and C are interconnected.

pf: By Propositions 49 and 50, observing that $(A \sqcup B)^{**}$ and C are interconnected iff $A \sqcup B$ and C are.

Fig. 5.3 shows an interesting counter-model for Σ_3.

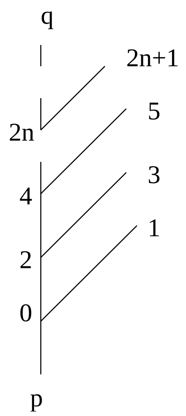

Figure 5.3: The tree above represents a frame where p is the root, q is a terminal element, and the other elements are labelled by the positive integers — the odd numbers label the terminal elements, the even numbers label the elements that are below q. An atomic spatial model can be defined on this frame, by taking $\mathcal{O} = \mathcal{U}_{\leq}$ and $\mathcal{R} = \mathcal{O}$, fails to satisfy Σ_3. Taking $A = \{4 * n + 1\}$, $B = \{2 * (2 * n + 1) + 1\}$, and $C = \{q\}$, both A and B are apart from C, whereas $A \sqcup B$ is not.

5.3.3 Dimension

The discussion in this section arises from the observation that, in a quite specific sense, it is possible to associate granularity with an abstract notion of dimension. Lower dimensional representations can be intuitively associated to less detailed ones.

For example, in a standard, two-dimensional geographic map, a road can be represented as a one-dimensional feature (a curve). This representation is normally less precise than a two-dimensional one that takes into account the width of the road.

In the following I am going to consider how the definition of topological dimension can be adapted, in order to make it significant for atomic spatial models. A preliminary definition is needed.

Definition 42 In a space $(S, \mathcal{O})$, a collection $\mathcal{A} \subseteq \mathcal{O}$ is said to have *order* n iff n is the largest integer s.t. $\mathcal{A}$ includes a family of $n+1$ sets with a non-empty intersection.

Given $\mathcal{A}, \mathcal{B} \subseteq \mathcal{O}$, $\mathcal{B}$ is said to be a *shrinking* of $\mathcal{A}$ iff for every $B \in \mathcal{B}$ there is $A \in \mathcal{A}$ s.t. $B \sqsubseteq A$.

The following gives a standard definition of topological dimension for normal spaces [Eng78]:

Definition 43 A normal space $\mathcal{S} = (S, \mathcal{O})$ has *covering dimension* equal or less than n if and only if, for every open cover $\mathcal{A}$ of S, there is an open cover $\mathcal{B}$ of S that is a shrinking of $\mathcal{A}$, such that $\mathcal{B}$ has order at most n. If there is no such bound, the covering dimension is ∞. If $\mathcal{S}$ has covering dimension less than or equal to n and does not have it less than or equal to $n-1$, then it is said to have covering dimension n.

With respect to non-metric spaces, this definition turns out to be quite problematic. In fact, rather unintuitively, the covering dimension of a non-metric space may turn out to be smaller than that of some of its subspaces. In particular, the definition has little significance w.r.t. prime spaces, since these always have covering dimension 0. In the following, I introduce a weaker notion. This essentially arises as the greatest covering dimension of all the subspaces. Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be an atomic spatial model.

Definition 44 The value Δ is defined in $\mathcal{Z}$ as the maximum that satisfies the following:

$\Delta(\mathcal{Z}) \leq n$ iff for every subspace $T \sqsubseteq S$, for every cover $\mathcal{A} \subseteq \mathcal{R}$ of T, there is a cover $\mathcal{B} \subseteq \mathcal{R}$ of T such that $\mathcal{B}$ is a shrinking of $\mathcal{A}$, and has order at most n.

$\Delta(\mathcal{Z}) = \infty$, otherwise.

The next proposition gives a useful characterisation for Δ.

Proposition 52 In $\mathcal{Z}$, $\Delta \leq n$ if and only if, for any $T \in \mathcal{O}$, whenever, given $A_{i \in I} \in \mathcal{R}$ for $I = \{1, \ldots, n+2\}$, such that $T = \bigvee_{i \in I} A_i$, there exist $B_{i \in I} \in \mathcal{R}$ such that $B_i \sqsubseteq A_i$, for all $i \in I$, and moreover $T = \bigvee_{i \in I} B_i$ and $\bigwedge_{i \in I} B_i = \varnothing$.

pf: The proof can be adapted from that of [Eng78], Theorem 1.6.10.

The general idea, here, is to have the atomic cells representing n-dimensional regions, whenever $\Delta = n$. Lower-dimensional features can be represented only insofar as they are on the boundary between n-dimensional regions. Each representable feature can then be associated to the set of the atomic cells for which it is a boundary element — or to the union of those cells (which is equivalent).

Fig. 5.5 gives an example of a model that validates Dim(2), corresponding to a 2-d cell complex.

It is now possible to show that, in an atomic spatial model, the weak notion of dimension given by Δ has a quite intuitive property.

Proposition 53 When $\Delta = n$ in $\mathcal{Z}$, for any atomic cell $A \in \mathcal{R}$, there can be at most n disjoint, non-empty definable opens that are interconnected with A.

pf: Assume that, for $I = \{1, \ldots, n+1\}$, there are non-empty, disjoint $B_{i \in I}$ such that each of them is interconnected with A. Then, there must be an open boundary subset shared for each pair $A, B_{i \in I}$. But then, $\{(A \sqcup B_{i \in I})^{**}\}$ is a subspace that contradicts $\Delta \leq n$.

So, from the point of view of interconnection, whenever $\Delta = 2$, the atomic cells behave like triangles (possibly degenerate ones). This fits in well from the point of view of a decomposition in terms of simplicial complexes [OBS92].

On the other hand, treating Δ as a measure of dimension can be problematic from the point of view of a decomposition based on a square grid, as shown by the following example.

In the finite spatial model pictured in Figure 5.4, where A, B, C, D, E are atomic cells, Δ is greater than 2. In fact, the cover $H_{\{4\}}$ of S, formed by $H_1 = (\bigvee\{A, B, C, E\})^{**}$, $H_2 = (\bigvee\{A, C, D, E\})^{**}$, $H_3 = (\bigvee\{A, B, D, E\})^{**}$, $H_4 = (\bigvee\{A, B, C, D\})^{**}$, violates the condition for $\Delta = 2$, since $\bigwedge H_4 = A$, but no refinement of $H_{\{4\}}$ can contain the point p. This happens to be the case just because p is a boundary point of four distinct definable opens.

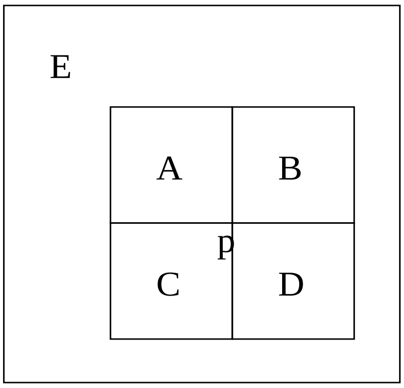

Figure 5.4: A planar graph. A, B, C, D, E are regions, p is a boundary point shared by A, B, C, D.

The characterisation that has been given of Δ makes it possible to give the following logical encoding.

Proposition 54 A spatial model $\mathcal{Z}$ has $\Delta \leq n-2$ iff $\Vdash_Z \mathrm{Dim}(n-2)$, for

$$\mathrm{Dim}(n-2) = \forall y_1 \ldots y_n . \exists z_1 \ldots z_n . (z_1 \to y_1) \wedge \ldots \wedge (z_n \to y_n) \wedge \\ \sim(z_1 \wedge \ldots \wedge z_n) \wedge (y_1 \vee \ldots \vee y_n) \to (z_1 \vee \ldots \vee z_n)$$

pf: Using Proposition 52, the condition for $\Delta \leq n-2$ can be formalised into the following expression, which is equivalent to the condition for $\mathrm{Dim}(n-2)$:

$$\Vdash_Z \forall y_1 \ldots y_n . \exists z_1 \ldots z_n . (z_1 \sqsubseteq^t y_1) \wedge \ldots \wedge (z_n \sqsubseteq^t y_n) \wedge ((z_1 \sqcap \ldots \sqcap z_n) =^t \varnothing) \\ \wedge ((y_1 \sqcup \ldots \sqcup y_n) \sqsubseteq^t (z_1 \sqcup \ldots \sqcup z_n))$$

5.3.4 JEPD relations

In Section 4.2 it has been highlighted the importance of jointly exhaustive, pairwise disjoint (JEPD) sets of relations, and the $RCC8$ relations [RCC92] have been treated as a significant example. In Section 5.2 it has been shown how similar relations can be represented in the spatial models introduced with Def. 25. In this section, those results are summed up in propositions that state how the $RCC8$-style relations can be encoded in some extensions of ISPL. Let $H \in \{C2, D2, NC2, ND2\}$. Let $\mathcal{Z} = (S, \mathcal{O}, \mathcal{R}, \tau)$ be a spatial model for H.

Proposition 55 Given a logic H and a spatial model $\mathcal{Z}$ for H, such that $\Vdash_Z \Sigma_1 \wedge \Sigma_2$, if $\not\Vdash_Z$ degnr, then for every formulæ α, β, one and only one of the following binary relations holds between them (i.e. the following are jointly exhaustive, pairwise disjoint relations):

$\Vdash_Z \approx\alpha \leftrightarrow \approx\beta$	[equivalence]
$\Vdash_Z \mathsf{nempty}(\alpha \wedge \beta) \wedge \mathsf{nempty}(\alpha \wedge \sim\beta)$	[partial overlap]
$\Vdash_Z \mathsf{nempty}(\beta) \wedge \mathsf{ntp}(\alpha, \approx\beta)$	[non-tangential part]
$\Vdash_Z \mathsf{nempty}(\alpha) \wedge \mathsf{ntp}(\beta, \approx\alpha)$	[inverse non-tangential part]
$\Vdash_Z \mathsf{tp}_i(\alpha, \approx\beta) \wedge \mathsf{nempty}(\sim\alpha \wedge \beta)$	[tangential proper part]
$\Vdash_Z \mathsf{tp}_i(\beta, \approx\alpha) \wedge \mathsf{nempty}(\alpha \wedge \sim\beta)$	[inverse tangential proper part]
$\Vdash_Z \mathsf{nempt}(\alpha) \wedge \mathsf{nempt}(\beta) \wedge \mathsf{ap}(\alpha, \beta)$	[apartness]
$\Vdash_Z \mathsf{tp}_i(\alpha, \sim\beta)$	[tangential connection]

pf: The proof relies on Propositions 48, 49, 40 for the conditions on the model, and on Propositions 35, 38, 41, 43, 47 for the encoding of the relations.
The semantics of the relations guarantee that they are JEDP. Only two cases are non-trivial. Since we are considering only regular opens, Propositions 48, 49, 47 allow the representation of the tangential part relation by tp_i. Proposition 41 allows the representation of non-emptiness and of overlapping using nempty.

The restriction to regular opens is not necessary, as it is required by Proposition 39 (for con_s) but not by Proposition 43 (for ic_i). It is not necessary to exclude the empty set, either, although regions are usually meant to be non-empty. In fact the empty set here does not raise any problem from the point of view of the classification: either $\Vdash_Z \mathsf{nempt}(\alpha) \wedge \mathsf{ntp}(\bot, \alpha)$ or $\Vdash_Z \bot \leftrightarrow \alpha$, but not both.

In the non-modal case, the restriction to non-degenerate models takes the form of a semantical condition — i.e. $\nVdash_Z \mathsf{degnr}$, whereas in the modal case it can also be expressed as $\Vdash_Z \sim\Box\mathsf{degnr}$.

However, in an N-modal logic, it is possible to give altogether simpler encodings for $RCC8$-style relations, without introducing any additional schema. Moreover, the restriction to regular opens can be lifted. One can actually have two distinct encodings, one (Proposition 56, A) based on interconnection and apartness, the other one (Proposition 56, B) based on strong interconnection and weak apartness, as given in Def. 40. The two encodings are equivalent when one restricts to models that satisfy Σ_2.

Proposition 56 Given a logic NH and a spatial model $\mathcal{Z}$, for every formulæ α, β, the following are JEDP binary relations:

A)

$\Vdash_Z \approx\alpha \leftrightarrow \approx\beta$	[equivalence]
$\Vdash_Z \Diamond(\alpha \wedge \beta) \wedge \Diamond(\alpha \wedge \sim\beta)$	[partial overlap]
$\Vdash_Z \Diamond\beta \wedge \mathsf{ntp}(\alpha, \approx\beta)$	[non-tangential part]
$\Vdash_Z \Diamond\alpha \wedge \mathsf{ntp}(\beta, \approx\alpha)$	[inverse non-tangential part]
$\Vdash_Z \mathsf{tp}(\alpha, \approx\beta) \wedge \Diamond(\sim\alpha \wedge \beta)$	[tangential proper part]
$\Vdash_Z \mathsf{tp}(\beta, \approx\alpha) \wedge \Diamond(\alpha \wedge \sim\beta)$	[inverse tangential proper part]
$\Vdash_Z \Diamond\alpha \wedge \Diamond\beta \wedge \mathsf{ap}(\alpha, \beta)$	[apartness]
$\Vdash_Z \mathsf{tp}(\alpha, \sim\beta)$	[tangential interconnection]

B)

$\Vdash_Z \approx\alpha \leftrightarrow \approx\beta$	[equivalence]
$\Vdash_Z \Diamond(\alpha \wedge \beta) \wedge \Diamond(\alpha \wedge \sim\beta)$	[partial overlap]
$\Vdash_Z \Diamond\beta \wedge \mathsf{ntp}_w(\alpha, \approx\beta)$	[weakly non-tangential part]
$\Vdash_Z \Diamond\alpha \wedge \mathsf{ntp}_w(\beta, \approx\alpha)$	[inverse weakly non-tangential part]
$\Vdash_Z \mathsf{tp}_s(\alpha, \approx\beta) \wedge \Diamond(\sim\alpha \wedge \beta)$	[strongly tangential proper part]
$\Vdash_Z \mathsf{tp}_s(\beta, \approx\alpha) \wedge \Diamond(\alpha \wedge \sim\beta)$	[inverse strongly tangential proper part]
$\Vdash_Z \Diamond\alpha \wedge \Diamond\beta \wedge \mathsf{ap}_w(\alpha, \beta)$	[weak apartness]
$\Vdash_Z \mathsf{tp}_s(\alpha, \sim\beta)$	[strong tangential interconnection]

pf: Similar to Proposition 55.

Considering non-regular opens makes it possible to introduce a richer set of jointly exhaustive, pairwise disjoint relations, by refining the relation represented by $\alpha \to \approx\beta$ (which gives the underlying notion of part in all the above encodings) into the disjoint relations represented by $\alpha \to \beta$ and $(\alpha \to \approx\beta) \wedge \sim\Box(\alpha \to \beta)$. This makes it possible to get a more discriminating set of JEPD relations, that cannot be treated here, by taking into account granular representations.

5.4 Views

Quite informally and briefly, I will sketch a few semantical ideas that justify the inclusion of the V-modal logics in Chapter 3. These suggestions bear some relationship with the logic of vision [VDDVL00]. Here I consider the V-modalities quite independently from the interpretation of the N-modalities, discussed up to now.

A non-modal Kripke frame, as given in Def. 15, can be regarded as a *view* of the external space, taken from a *view point* represented by $\mathbf{0}$. Definable opens are the representations of visible objects. This idea can be generalised when one considers a V-modal frame (Def. 18), by allowing for different views of the space, ordered under conditions that match those of the formal definition.

The example given in Figs.5.6, 5.7, 5.8 suggests a possible association of views with projections. The 3-dimensional scene in Fig. 5.6 is represented abstractly by the two models in Fig. 5.7. The view from the point *v1* shows B as covered by A (indeed, *v1* itself is contained in A), whereas the view from *v2* shows A and B as disjoint. The *VD2*-model $\mathcal{M}$ (see Def. 19) that can be defined on the frame in Fig. 5.8, by taking $\mathcal{R} = U_{\leq}$, $\mathbf{0} = v0$ and $V = \{v0, v1, v2\}$ joins together the two views in a picture, that can be seen, as a whole, from *v0*. Some extra points are added (x and y), in order to preserve the $\mathcal{R}$-connectedness of A and B.

In the V-modal logics, the operator $\Diamond$ does not generally correspond to non-emptiness (see Lemma 19). Indeed, here $\Diamond\,\alpha$ means that α is non-empty in every view. This meaning may apply to a region that can be associated in some sense to a "real object". In the example, both A and B are such regions. In fact $\models_M \Diamond\, A$ and $\models_M \Diamond\, B$. On the other hand, $A \sqcap B$ can only be associated to a "shadow" — it is non-empty only in one of the projections — and correspondingly, $\not\models_M \Diamond(A \wedge B)$.

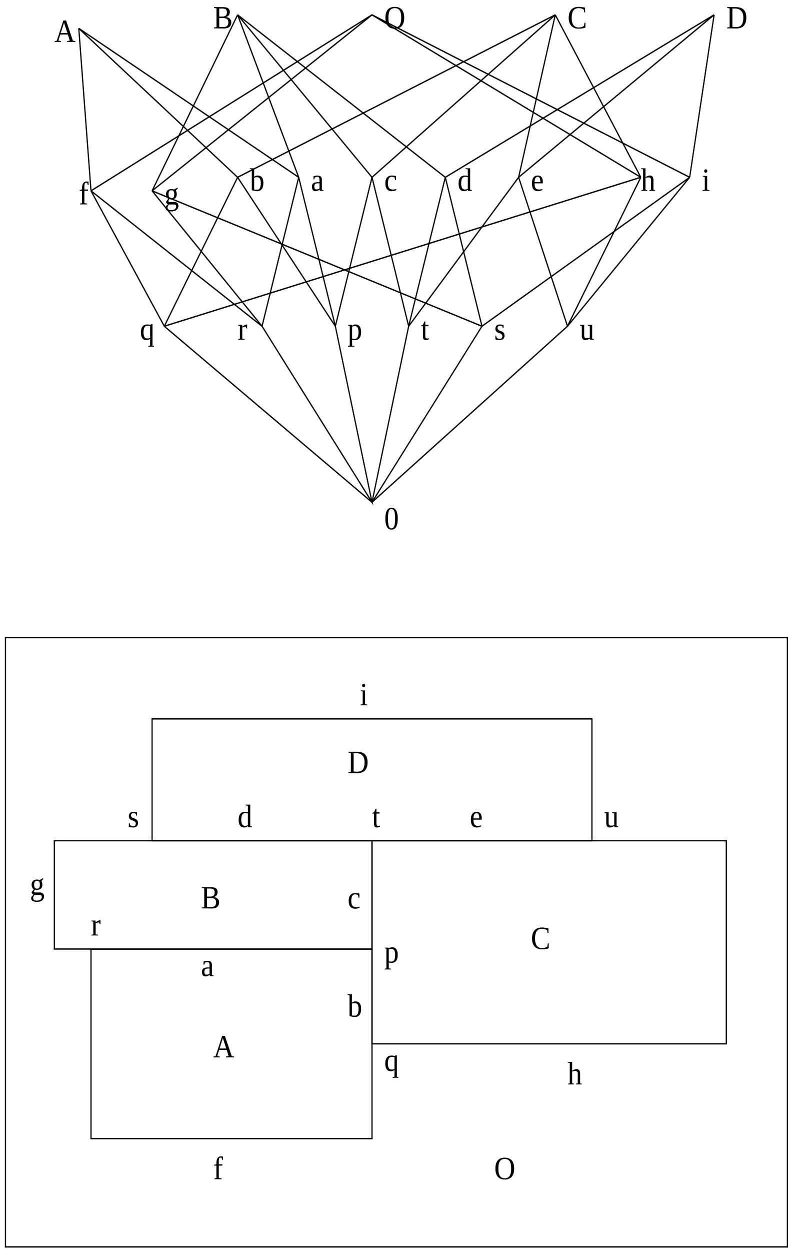

Figure 5.5: The frame above, taking $\mathcal{O} = \mathcal{U}_{\leq}$ and $\mathcal{R} = \mathcal{O}$, gives a finite, non-degenerate spatial model that satisfies Σ_1, Σ_2, Σ_3 and Dim(2). It can be associated in a natural way with the 2-d cell complex below, represented as a planar graph, following the labelling convention described in Fig 4.2. In contrast, it can be noted that in Fig. 5.1, 1 and 2 are models that fail to satisfy Σ_3, whereas 3 gives a degenerate model.

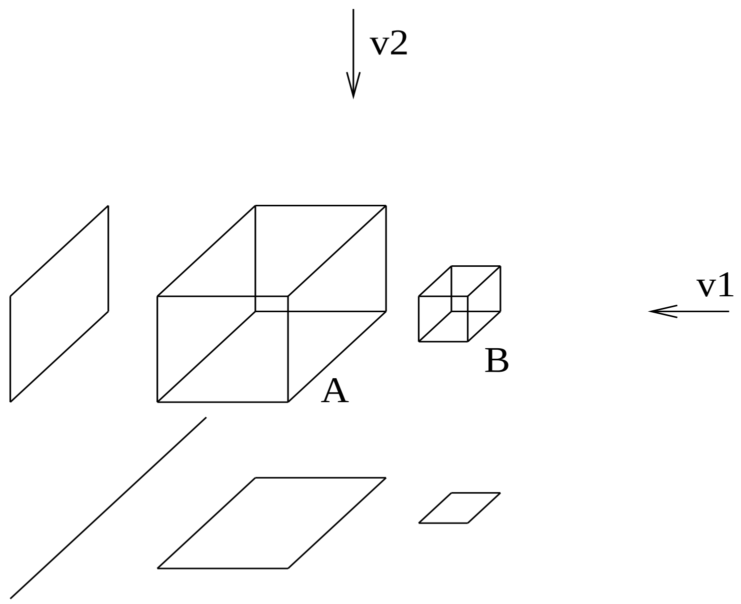

Figure 5.6: A 3-d object and two of its 2-d projections.

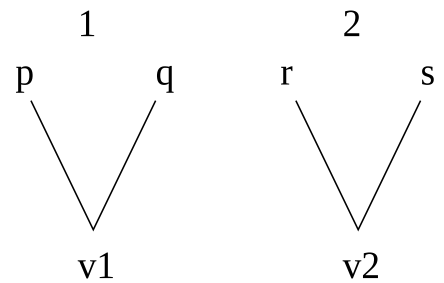

Figure 5.7: Models for the projections. In 1, $A = v1\uparrow$ and $B = q\uparrow$. In 2, $A = r\uparrow$ and $B = s\uparrow$.

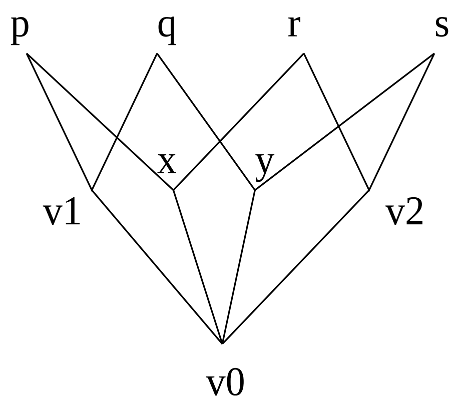

Figure 5.8: A model that joins together the two projections and preserves the topology of the 3-d object, taking $A = (v1\uparrow) \sqcup (x\uparrow)$ and $B = y\uparrow$.

Chapter 6

A decision procedure

In this chapter, a partial decidability result is given for *D2*. I will first show that the negative formulæ in this logic are decidable by embedding them into classical logic. Further, I will show how a decision procedure for those formulæ can be built within *D2*. The mechanisation of this procedure will be discussed in the next chapter (Section 7.4.2).

6.1 Classical propositional logic

Classical propositional logic (*CPL*) can be axiomatised in a language $\mathcal{L}'$ with primitives $\rightarrow, \sim$, where $\wedge, \vee$ can be classically defined, by adding to any axiomatisation of *IPL* the following schema (*Excluded Middle*):

$\alpha \vee \sim \alpha$ [**EM**]

From EM and the intuitionistic schemas it is possible to derive $(\sim \alpha \rightarrow \alpha) \rightarrow \alpha$ and $\approx\alpha \rightarrow \alpha$.

In *CPL* propositional quantification does not increase the expressive power, since the universal quantifier can be defined as follows.

$\forall x.\alpha(x) = \alpha[\top/x] \wedge \alpha[\bot/x]$ [**PQD**]

Then, the existential quantifier can be defined with $\exists x.\alpha(x) = \sim \forall x. \sim \alpha(x)$. However, replacing quantifiers with their definitions causes an increase in the size of the formula which is exponential in the number of their occurrences.

Alternatively, and equivalently from the point of view of provability, it is possible to extend the language with $\forall$ as a primitive, and then to extend *CPL* with Schema 5, Rule 6 (Section 3.4), together with the following:

$\alpha(\top/x) \wedge \alpha[\bot/x] \rightarrow \forall x.\alpha(x)$ [**PQA**]

I will refer to the logic given by this "redundant" axiomatisation as to *CPL'*.

6.2 An embedding into CPL

The semantical completeness of *D2* can be used in order to establish the following:

Proposition 57 The schema

$\approx(\alpha[\top/x] \wedge \alpha[\bot/x] \rightarrow \forall x.\alpha(x))$ [**NQE**]

is valid in *D2*.

pf: Let $\gamma = \alpha[\top/x] \wedge \alpha[\bot/x] \rightarrow \forall x.\alpha(x)$. Assume $\nvdash_{2D} \approx\gamma$. Then, by semantical completeness (Theorem 2), $\nvDash_{2D} \approx\gamma$. So, for some Kripke frame $\mathcal{S} = (S, \mathbf{0}, \leq)$ and some Kripke model $\mathcal{M} = (\mathcal{S}, \mathcal{R}, \rho)$, for some element $\mathtt{a} \in S$, $\mathtt{a} \vDash \sim\gamma$. Then, for all $\mathtt{x} \in S, \mathtt{a} \leq \mathtt{x}$, it must be $\mathtt{x} \nvDash \gamma$. But, for any terminal $\mathtt{y} \in S$, $\mathtt{y} \vDash \gamma$, as the interpretation does not depend on any other point. So $\vdash_{2D} \approx\gamma$.

A class of formulæ Δ in the language $\mathcal{L}_1$ for a logic L_1 can be *embedded* into the language $\mathcal{L}_2$ for a logic L_2, w.r.t. provability, whenever there is a mapping $\theta : \Delta \mapsto \mathcal{L}_2$ such that for every formula $\alpha \in \Delta$, α is provable in L_1 iff $\theta(\alpha)$ is provable in L_2.

A *negative formula* is one that has form $\sim\alpha$. A *negative theorem* is a provable negative formula. The following can be proved, showing that the negative formulæ of *D2* can be embedded into *CPL'* w.r.t. provability, by mapping the intuitionistic formulæ into the corresponding classical ones. An similar result for *IPL* was proved by Glivenko [Gli29].

Proposition 58 For every formula α in $\mathcal{L}_i$, $\vdash_{2D} \approx\alpha$ iff $\vdash_{CPL'} \alpha$.

pf: *Left to right.* Every axiom in *D2* is a theorem in *CPL'*, and every rule in *D2* is also a rule in *CPL'*. So, if $\vdash_{2D} \approx\alpha$ then $\vdash_{CPL'} \approx\alpha$. It is then possible to apply $\vdash_{CPL'} \approx\alpha \rightarrow \alpha$.

Right to left. By induction on the length of the proof. The base can be established by noting that, for every α s.t. it is an axiom in *CPL*, $\approx\alpha$ is a theorem in *IPL*, and so also in *D2*. This holds for PQA, too, by Proposition 57. The induction step requires checking the rules. The case of Modus Ponens (Rule A4) is straightforward. As to Rule A6, assume $\vdash_{CPL'} \alpha \rightarrow \beta(x)$ (x not free in α). Then, by the induction hypothesis, $\vdash_{2D} \approx(\alpha \rightarrow \beta(x))$. Then $\vdash_{2D} \forall x.\approx(\alpha \rightarrow \beta(x))$ and so $\vdash_{2D} \approx\forall x.(\alpha \rightarrow \beta(x))$. Then, $\vdash_{2D} \approx(\alpha \rightarrow \forall x.\beta(x))$, as we wanted, since, when x is not free in α, $\vdash_{2D} (\forall x.\alpha \rightarrow \beta(x)) \rightarrow (\alpha \rightarrow \beta(x))$, by DE (Proposition 12).

It is then possible to prove the following.

Proposition 59 For every intuitionistic formula α, the provability problem for $\sim\alpha$ w.r.t. *D2* is decidable and PSPACE-complete.

pf: This follows from the fact that $\models_{2D} \sim\alpha$ iff $\models_{2D} \sim\approx\alpha$, from Proposition 58 and from the fact that the provability problem for *CPL* with quantified Boolean formulæ is PSPACE-complete [GJ79].

From the point of view of the spatial representation, the following result can be obtained.

Proposition 60 For any finite set Δ of formulæ of $\mathcal{L}_i$, the problem whether there is an atomic spatial model that satisfies all the formulæ in Δ is decidable.

pf: One can show that such a model exists, by proving $\Delta \nvdash_{2D} \perp$. This turns out to be decidable, by Proposition 59, using the deduction equivalence.

So, constraint satisfaction in *D2* is at worst PSPACE-hard, even without any restriction on the number of variables. However, it must be observed that this result is significant only when we consider constraints that do not involve non-emptiness. In fact, the interpretation of $\mathsf{nempt}(x)$ collapses into triviality whenever the model is degenerate (Section 5.2.2). This fact makes it hard to check satisfaction for any constraint that involves overlapping. Hence, degenerate models are a problem from the point of view of the $RCC8$-style relations — see Proposition 55. It turns out that it is not useful, in this logic, to check the consistency of constraints involving apartness and interconnection — indeed, as it can be proved quite easily, $\vdash_{2D} \forall xy.{\approx}\mathsf{ap}(x,y)$ and $\vdash_{2D} \forall xy.{\approx}\mathsf{ic}_i(x,y)$. On the other hand, satisfiability and derivability problems for sets of constraints involving disjointness $({\sim}(\alpha \wedge \beta)$ and inclusion into regular opens $(\alpha \rightarrow {\approx}\beta)$ turn out to be a feasible application.

6.3 A mechanisable procedure

In Proposition 59, the proof that the class of the negative formulæ of *D2* is decidable is based on a semantical step — the embedding into classical logic. When one wishes to formalise the proof on a theorem prover, the translation between the two logics may turn out to be an undesired complication. It seems then useful to develop a decision procedure based on a syntactical derivation within *D2*.

The two equivalent procedures that are presented in the next sections are quantifier elimination procedures for the negative formulæ of *D2*. The quantifier-free formulæ that are left can then be solved using standard decision methods for *IPL*.

6.3.1 Quantifier elimination for the negative formulæ

Two ways in which the provability problem for a *D2* negative formula can be turned into the same problem for a quantifier-free formula are given in the following. In both cases, the essential steps involve NQE (Proposition 57).

6.3.1.1 Meta-level proof

The most intuitive way to reason about quantifier elimination is explicitly based on meta-level reasoning.

Proposition 61 The schema

$\sim\pi[\forall x.\phi(x)/y] \leftrightarrow \ \sim\pi[\phi[\top/x] \wedge \phi[\bot/x]/y]$ [**ANQE**]

is valid in *D2*.

pf: By NQE (Proposition 57) and RE (Proposition 13). I refer to the mechanised proof discussed in Section 7.4.2 for more details.

It is now possible to prove the following:

Proposition 62 In *D2*, any negative formula is logically equivalent to a quantifier-free formula.

pf: Assume that $\alpha = \sim\gamma$. Then, it is possible to obtain an equivalent quantifier-free formula by the following steps:

Step 1. Eliminate each occurrence of $\exists$, by rewriting with its definition.

Step 2. Eliminate each occurrence of $\forall$, by applying ANQE through RE.

6.3.1.2 Step-by-step proof

Quantifier elimination as described above is comparatively elegant, but from the point of view of mechanisation, the use of ANQE (Proposition 61) as a rewrite rule relies rather heavily on higher-order unification, and this may give some problem.

Quantifier elimination can also be done in simpler steps, as shown by the following. Here I will also include the elimination of all the logical symbols except $\rightarrow, \bot$. It is useful to introduce some auxiliary notions first.

Definition 45

1. A negative formula $\sim\alpha$ is said to be totally negative (a *TN formula*) iff the only non-primitive logical symbols that are contained in it are $\approx, \sim$, and moreover, for every occurrence β of a non-negative sub-formula, $\sim\beta$ is also a sub-formula of α.
2. A formula is said to be in $[\rightarrow \wedge \sim]$-form (an *ICN formula*) iff it contains only $\rightarrow, \wedge, \sim, \approx$.
3. A formula is said to be in $[\rightarrow \bot]$-form (an *IF formula*) iff it contains only $\rightarrow, \bot$.
4. A formula is said to be in conjunctive $[\rightarrow \bot]$-form (a *CIF formula*) iff it is a conjunction of IF formulæ.

Proposition 63 The following are derivable in *D2*:

$\sim\alpha \leftrightarrow \sim\approx\alpha$	[t1]
$\approx(\alpha \rightarrow \beta) \leftrightarrow \approx(\approx\alpha \rightarrow \approx\beta))$	[t2]
$\approx(\forall x.\alpha(x)) \leftrightarrow \approx\forall x.\approx\alpha(x)$	[t3]
$\approx\approx\alpha \leftrightarrow \approx\alpha$	[t4]
$(\alpha \wedge \beta \rightarrow \gamma) \leftrightarrow (\alpha \rightarrow \beta \rightarrow \gamma)$	[t5]
$(\alpha \rightarrow \beta \wedge \gamma) \leftrightarrow (\alpha \rightarrow \beta) \wedge (\alpha \rightarrow \gamma)$	[t6]

pf: I refer to the mechanised proof mentioned in Section 7.4.2.

Proposition 64 In *D2*, any negative formula $\alpha = \sim\gamma$ is logically equivalent to a TN formula.

pf: By applying to α the sequence of transformations described below. The logical equivalences in Proposition 63 are used here as rewrite rules, applied from left to right through RE (Proposition 13).

Step 1. Eliminate $\exists, \wedge, \vee, \leftrightarrow$ by rewriting with the definitions.

Step 2. Replace the new goal by [t1].

Step 3. Since the goal is now $\sim\approx\gamma'$, replace each sub-formula of γ' by [t2] and [t3]. This step already yields a TN formula.

Step 4. Rewrite exhaustively by [t4] — this just eliminates redundant negations, still leaving us with a TN formula.

For example, $\sim(\alpha \wedge \beta \rightarrow \forall x.\gamma(x))$ becomes
$\sim\approx(\approx(\forall y.(\approx\alpha \rightarrow \approx\beta \rightarrow \approx y) \rightarrow \approx y) \rightarrow \approx\forall x.\approx\gamma(x))$.

It is now possible to show how quantifiers can actually be eliminated.

Proposition 65 In *D2*, for each negative formula γ there is an IF formula γ'' such that γ is provable iff γ'' is.

pf: Step 1. γ is converted into a TN formula γ', by Proposition 64.

Step 2. All the occurrences of $\forall$ are eliminated by rewriting exhaustively with NQE (Proposition 57). This gives an ICN formula.

Step 3. Rewrite exhaustively with the definitions of $\approx$ and $\sim$.

Step 4. The occurrences of $\wedge$ are eliminated by [t5] or else pushed outside by [t6]. This gives a CIF formula.

Step 5. Rewrite the outermost $\wedge$ with its definition.

Step 6. One is left with $\forall x.(\alpha_1 \wedge \ldots \wedge \alpha_{n-1} \rightarrow \alpha_n \rightarrow x) \rightarrow x$.
This can be rewritten exhaustively with [t5].

Step 7. One is left with $\forall x.\delta(x)$, where $\delta(x)$ is an IF formula.
But then, $\vdash \forall x.\delta(x)$ iff $\vdash \delta(x)$.

Proposition 62, by stating that for each negative formula, there is a quantifier-free one which is equivalent in *D2*, gives a guarantee over the completeness of quantifier elimination. Inspection can show that also the procedure given in Proposition 65 is complete.

6.3.2 Decidability

The following shows that when the quantifiers are eliminated from a negative formula of *D2*, what is left is an *IPL* formula.

Proposition 66 *D2* is a conservative extension of *IPL*.

pf: *D2* extends *IPL*, since the axioms and rules for *D2* include those for the implicative fragment of *IPL*, whereas $\vee, \wedge, \sim$ are 2nd-order definable (see Sections 3.3, 3.4).
On the other hand, it can be verified that every Kripke model for *IPL* (as given in [Gab81]) can be extended to a model for *C2* by adding the interpretation rule for $\forall$. Moreover, we know that the axiom schema A9 is satisfied by any

C2 model that is atomic, and hence also by any finite one. *IPL* has the finite model property (i.e. every non-theorem has a finite counter-model [Gab81]). So every formula that has a counter-model for *IPL* has also one for *D2*.

It follows immediately that any proof procedure for *IPL* can be embedded in *D2*. Examples of decision procedures for *IPL* can be found in [Dyc92, Min92].

Proposition 59 could then be restated and proved from Proposition 66, by using either Proposition 62 or Proposition 65 for the quantifier elimination part, and by relying on [Min92] for a similar complexity result.

6.4 Meta-level and object-level proofs

Before starting the discussion about the mechanisation of *D2*, let us consider the aspect of meta-level reasoning. In both Propositions 62, 65, it has been used RE (Proposition 13) — as I recall it here:

$$\Delta \vdash_{D2} \alpha \leftrightarrow \beta \ \text{ implies } \Delta \vdash_{D2} \gamma[\alpha/x] \leftrightarrow \gamma[\beta/x] \quad [\mathbf{RE}]$$

This principle is not usually treated as part of the logic, since it can be proved at the meta-level, by induction. It turns out simpler to write it using the impredicative substitution (formula-for-variable).

RE is a very useful principle, in general, since it allows us to import into a formal proof pieces of equational reasoning that are often suggested by the semantics. RE can also be used to derive other meta-level rules. For example, as it has been proved with Isabelle:

$$\Delta \vdash_{D2} \approx((\alpha \leftrightarrow \beta) \vee (\alpha \leftrightarrow \gamma)) \ \text{ implies}$$
$$\Delta \vdash_{D2} \approx((\phi[\alpha/x] \leftrightarrow \phi[\beta/x]) \vee (\phi[\alpha/x] \leftrightarrow \phi[\gamma/x])) \quad [\mathbf{DNDRE}]$$

The following formula, closely related to RE, is also valid in *D2* — it can be proved by RE and Deduction Equivalence, for y, z not free in α, β:

$$(\alpha \leftrightarrow \beta) \rightarrow \forall yz.(y \leftrightarrow \alpha) \wedge (z \leftrightarrow \beta) \rightarrow \gamma(y/x) \leftrightarrow \gamma(z/x) \quad [\mathbf{RE'}]$$

Whereas RE superficially looks like the corresponding first-order principle, RE' does not at all. However, here both RE and RE' are second order expression: in RE, a formula is substituted for a variable; in RE', a variable is taken to be equivalent to a formula.

Every instance of RE' can be derived in *D2*. However, this does not seem to apply to the schema RE' itself. In fact, in the axiomatisation of Section 3.4, no postulate can link together two different uses of the same variable, one as a variable in a substitution (in $\gamma(y/x)$) and the other one as a propositional variable (in $y \leftrightarrow \alpha$). In a certain sense, one could even say that the notion of derivation based on the given axiomatisation is incomplete w.r.t. the valid *schemas*.

On the other hand, it does not seem useful to add a schema such as RE' to the axiom list. This would not alter the stock of the theorems, whereas the meta-level proof of RE' suffices, just as it suffices that given for RE. This example shows that, with propositional quantification, it is possible to have a schema that is valid (every instance is provable) and that cannot be derived within the logic (i.e. it can be proved only at the meta-level).

The schema NQE, which has been proved semantically (Proposition 57), and which is also used in Propositions 62, 65, is another example of the same kind — i.e. the schema cannot be derived within the logic, however it is a valid schema (every instance is provable) since it can be derived at the meta-level, using RE.

In order to make this idea more concrete here, I will just sketch the proof of NQE that has been given with Isabelle, by listing its main sub-goals (in reverse order, if one thinks of a forward proof):

SG1 $\vdash \approx(\phi[\top/x] \wedge \phi[\bot/x] \rightarrow \forall x.\phi(x))$

SG2 $\vdash \approx((\phi[\top/x] \rightarrow \phi[y/x]) \vee (\phi[\bot/x] \rightarrow \phi[y/x]))$ (ϕ does not contain y)

SG3 $\vdash \approx((y \leftrightarrow \top) \vee (y \leftrightarrow \bot))$

Proving SG1 from SG2 involves using Schema A8. Proving SG2 from SG3 involves using DNDRE. SG3 is closely related to $\approx(\alpha \vee \sim\alpha)$.

Chapter 7

Mechanisation

Making formal proofs manually can be tedious and error-prone. For this reason, mechanised proof-checking can be useful, even when a complete automation is not achievable. When the problem is tractable and an efficient solution is sought, a direct implementation in a programming language may be the best option. In case the problem is to mechanise proofs in an undecidable logic, it may turn out more convenient to give a formalisation in a meta-language that is clear, reliable and expressive enough to allow reasoning not only within, but also about the logic. Interactive theorem provers, and particularly those based on classical higher-order logic (*HOL*) are particularly useful to this purpose [Bun83].

Isabelle is an interactive theorem prover that has significant facilities for the implementation of new object logics, and has a well-supported formalisation of *HOL* [Pau96].

In the following, I will present a mechanisation of the logics *I2*, *C2* and *D2* in Isabelle. The mechanisation of *D2* will be used in order to proof-check the procedures for quantifier elimination discussed in Section 6.3. This will not give a fully automated implementation of quantifier elimination, rather it will give a correct and complete method to eliminate quantifiers from the negative formulæ. Since Propositions 62, 65 use meta-level reasoning, *HOL* turns out to be an appropriate environment.

7.1 Formalising proofs

A derivation of a formula α from a set of formulæ Δ, also said to be a deduction of α from Δ, can be defined as a sequence of steps that moves from the assumptions in Δ towards the conclusion α (Def. 12). However, in the search and in the presentation of a proof, it is often useful to go the other way round, starting from the thesis (the *goal*) and applying the inference rules backwards. This process generates *subgoals* that must be discharged either as axioms or as assumptions. Reasoning backwards may give a better control on the proofs, since inference rules have always a single conclusion but sometimes more than one premiss. Backward rules that correspond to the inference rules are also called *tactics* [Pau96]. Interactive theorem provers that are particularly designed for backward reasoning, are also said to be *tactic-based*.

Sequent calculus and natural deduction give two different ways to formalise derivations, in alternative to Hilbert systems. In natural deduction, the primitive rules represent elementary deduction steps corresponding to the meaning of the logical operators — each of them can be associated to a pair of *introduction-elimination* rules. In sequent calculus for intuitionistic logic, the expression $\Delta \vdash \alpha$, where α is a formula (the *consequence*) and Δ is a list of formulæ (the *antecedents*) is treated formally as a sequent, instead than as a meta-theoretical expression. In general, a sequent calculus rule has form:

$$\frac{S_0}{S_1 \ \dots \ S_n}$$

where the sequents $S_1 \ \dots \ S_n$ are the premisses and the sequent S_0 is the conclusion. A derivable sequent represents a deduction (i.e. a derivation of a formula from a set of formulæ).

Sequent calculus systems are usually defined by some axiom schemas, a set of structural rules, and a set of operational rules. The axioms represent elementary deductions. The structural rules are determined by the notion of derivation, and may include a rule called *Cut* — closely related to Modus Ponens. The operational ones are usually given as a pair of *left-right* rules for the introduction of each primitive operator, respectively, in one of the antecedents and in the consequence. Usually, all the rules except Rule Cut are such that the conclusions are formally more complex than each of the premisses — for this reason they are sometimes called *analytic* rules. In a proof that does not use Cut (also said to be *cut-free*), by reading the rules backwards, every sub-formula which is contained in the subgoals turns out to be already contained in the goal. This property, known as the *sub-formula property*, makes sequent calculus systems particularly useful for backward reasoning [TS00, Bun83].

Natural deduction proofs lend themselves to be read backwards as well. In contrast with sequent calculus though, natural deduction allows an easy interleaving between the backward application of the rules to the goal, and their forward application to the assumptions. This makes the handling of assumptions more intuitive, and hence it makes natural deduction particularly useful in dealing with complex proofs [Pau89].

7.1.1 Interactive theorem proving

A previous result in the formalisation of mereotopology (documented in [GCMP99] and related to the theory in [BCTH00c]) has been obtained using the HOL theorem-prover [GCMP99]. HOL is essentially a tactic-based implementation of the logic *HOL*.

Like HOL, Isabelle is written in ML — a strongly typed functional language based on typed lambda calculus with polymorphism [Pau91] — and has an ML interface (the higher-level interface ISAR is not used here). In contrast with HOL, Isabelle is implemented as a logical framework — i.e. as a computational logic that can be used as a meta-language for the formalisation of different object logics. The Isabelle meta-logic (also called M) is essentially a fragment of higher-order intuitionistic logic, with a primitive sort for propositions, and with primitive rules in the style of natural deduction for implication (denoted by `==>` and right associative, in the notation of the ML interface), universal quantification (denoted by `!!`, with a standard binder syntax) and equality (`==`). Isabelle syntax allows the use of meta-variables (also called schematic variables — in the following they will be denoted by Roman capital letters). The terms are those of simply typed lambda-calculus — constants, variables, abstractions (denoted by `% x. A`) and applications (`A B`, with an associated typing information `A::u=>v`, `B::u`) [Pau89, Pau02].

An object logic can be formalised as a theory that may be loaded on top of the meta-logic. Each theory includes the following:

1. Information about the dependency on other theories.
2. A signature, with the types and the declarations of some constants, each of them inclusive of an abstract syntax (given as a higher-order constant) and, possibly, of a concrete one (a macro).
3. The definitions of the constants.
4. Possibly some axioms.

The ML command `use_thy "T"` loads the theory T together with all its dependencies.

The expressions of the object logic can be formalised into expressions of typed lambda calculus, whereas the inference rules can be expressed as formulæ in the meta-logic. A rule in which `A_1`, ..., `A_n` are the premisses and `C` is the conclusion can be formalised in M as `[| A_1; ...; A_n |] ==> C` — an abbreviation for `A_1 ==> ...==> A_n ==> C` .

Object-level variables and substitution can be handled in terms of function arguments and application. The dependence of the conclusion on some variable that cannot be free in a premiss (`A_1`) can be expressed using meta-level quantification: `[| !! x. A_1; ...; A_n |] ==> C` .

The inference engine of Isabelle is based on a higher-order resolution rule, as described in [Pau89]. Writing D^s for the application of a substitution $s = [t_1/x_1, \ldots, t_i/x_i]$ to an expression D, the resolution rule turns out to be the following one:

$$\frac{[|A_1; \ldots; A_l|] ==> D \qquad [|B_1; \ldots; B_m|] ==> C}{[|A_1^s; \ldots; A_{j-1}^s; A_{j+1}^s; \ldots; A_l^s; B_1^s; \ldots; B_m^s|] ==> D^s} \; A_j^s == C^s$$

In a forward proof, all the inference rules are applied by means of resolution. Backward proofs are turned into forward ones by Isabelle. The tactic constructors that are provided allow the forward application of inference rules in a way that imitates their application as tactics in a backward proof [Pau89]. The constructor `res_tac` (for *resolve* tactic) can be used in order to imitate a backward application of any natural deduction rule to a goal. The constructor `eres_tac` (for *elimination* tactic) can be used in order to imitate, with an elimination rule, a backward application of a left rule to a goal. The constructor `dres_tac` (for *destruction* tactic) can be used in order to imitate a forward application of an elimination rule to one of the assumptions.

Although Isabelle is essentially an interactive theorem-prover, it has considerable facilities from the point of view of automation. In particular, the classical reasoner `blast_tac` can be used to deal semi-automatically with the application of analytic rules, whereas `simp_tac` gives a powerful simplifier for equational reasoning. The tactic `auto_tac` is a useful combination of methods.

7.1.2 Higher-order syntax

Higher-order logics such as *HOL* and Isabelle M allow typed higher-order variables and the possibility of writing functions, equivalently, either in curried or uncurried form (i.e. Fxy is equivalent to $F(x, y)$). Higher-order syntax can be used in order to express substitution and quantification. Substitution is dealt with by lambda-abstraction and function application. The meta-linguistic expression $\alpha(x/y)$, i.e. the formula resulting from the substitution of x for y in α, can be formalised as $(\lambda x.F(x))y$, which reduces to $F(y)$ by beta-reduction.

In contrast with the meta-linguistic reading of α, the corresponding formalisation F in the lambda-expression is a propositional function. Taking F to be a formula simply would not work: $(\lambda x.F)y$ beta-reduces to F, and the substitution of $G(x)$ for F is not allowed, since $(\lambda y.\lambda x.y)(G(x))$ violates a proviso against variable capture in lambda calculus [Bar92].

With higher-order syntax, binders have generally type $(\mathsf{term} \mapsto \mathsf{wff}) \mapsto \mathsf{wff}$. Provisos against variable capture can often be stated implicitly — this can be very useful. For example, in $\forall x.G \vee (F(x))$, the term F is a function, whereas the term G is a proposition — so x cannot occur free in G.

The higher-order notion of substitution for terms is of type $(\mathsf{term} \mapsto \mathsf{wff}) \mapsto \mathsf{term} \mapsto \mathsf{wff}$. This can be in contrast with some applications of the meta-linguistic notion of substitution. As an alternative, it is possible to formalise substitution by a first-order expression of type $(\mathsf{wff}, \mathsf{term}, \mathsf{term}) \mapsto \mathsf{wff}$. This one is also called *explicit substitution* [BM02].

7.2 ISPL in the Isabelle meta-logic

I will now show how a rule system that is equivalent to the logic *I2* (Section 3.4) can be embedded in the meta-logic M. I will refer to this embedding as to $I2_m$ — the full theory is in Section B.3.

A type `o` of class `logic` (the built-in class of the logical types) is declared for the formulæ of the object logic:

```
types o
arities o :: logic
```

The declaration of the constants follows. The function `Trueprop` is a coercion that maps $I2_m$-formulæ into meta-level ones (`prop` is their built-in type). The concrete syntax that is indicated on the right side, actually makes this coercion "invisible".

The other constants are for the logical symbols, resp. $\top, \bot, \rightarrow, \sim, \wedge, \vee, \leftrightarrow, \forall, \exists$. The concrete syntax associated to the declarations makes it possible to have right-associative binary operators. The binder declaration for the quantifiers, allows a translation between the purely higher-order syntax `All (% x. A)` (where `%` is for λ) and the concrete syntax `ALL x. A` (similarly for `Ex` and `EX`).

```
consts
  Trueprop      :: "o => prop"                  ("(_)" 5)
  True          :: o
  False         :: o
  -->           :: "[o, o] => o"                (infixr 10)
  Not           :: "o => o"                     ("~ _" [40] 40)
  &             :: "[o, o] => o"                (infixr 35)
  |             :: "[o, o] => o"                (infixr 30)
  <->           :: "[o, o] => o"                (infixr 25)
  All           :: "(o => o) => o"             (binder "ALL " 10)
  Ex            :: "(o => o) => o"             (binder "EX " 10)
```

The type of the propositional quantifiers given here is the obvious one, based on higher-order syntax. Substitution is defined impredicatively — any formula can be substituted for a variable.

The following natural deduction rules are those for the primitive operators, as they can be expressed in M using the coercion function. The meta-logic quantification of the premiss in the introduction rule for universal quantification (`allI`) enforces the standard proviso against the capture of free variables.

```
rules
  impI        "(P ==> Q) ==> (P-->Q)"
  mp          "[| P-->Q;  P |] ==> Q"
  allI        "(!!x. P(x)) ==> (ALL x. P(x))"
  spec        "(ALL x. P(x)) ==> P(x)"
  exI         "P(x) ==> (EX x. P(x))"
  exE         "[| EX x. P(x);  !!x. P(x) ==> R |] ==> R"
```

When the theory is loaded, these rules are added to the meta-logic as new axioms. The theory contains the definitions for the remaining operators (corresponding to Def. 8).

```
defs
  False_def    "False  == ALL x. x"
  True_def     "True  == False-->False"
  not_def      "~ P == P-->False"
  and_def      "P&Q  == ALL x. (P-->(Q-->x))-->x"
  or_def       "P|Q  == ALL x. (P-->x)-->(Q-->x)-->x"
  iff_def      "P<->Q == (P-->Q) & (Q-->P)"
```

Proving the equivalence of $I2_m$ with the Hilbert axiomatisation given for $I2$ in Section 3.4 is a straightforward matter. Since substitution is impredicative, no explicit comprehension principle (i.e. one corresponding to Schema A9) is needed.

Proofs in $I2_m$ can be given by applying the inference rules through the tactics that is possible to build with constructors such as `res_tac`, `eres_tac` and `dres_tac` (`rtac`, `etac` and `dtac` for short). Each of these functions takes the name of a rule and the number of the subgoal to which the rule must be applied. The tactic `atac` can be used in order to prove a subgoal directly from the assumptions. Other tactics can be defined in order to apply definitions as rewrite rules (by `rewrite_goals_tac`, which takes as argument a list of definitions and applies them to all the subgoals). The following is an example of proof code. The `qed` command is used to store the theorem with a name.

```
Goal "(ALL x. P(x))-->~(EX x.~(P(x)))";
by (rtac impI 1);
by (rewrite_goals_tac [not_def]);
by (rtac impI 1);
by (etac exE 1);
by (dtac spec 1);
by (dtac mp 1);
by (atac 1);
by (atac 1);
qed "al_im_nexn";
```

A general drawback of the formalisations based on M like this one, is that new axioms need to be added. The object logic is actually an axiomatic extension of the meta-logic. This put at risk the consistency of the whole framework. The fact that meta-level reasoning is rather hard to handle in M, points out another serious drawback of this approach, that we would like to overcome.

7.3 ISPL in Isabelle-HOL

Isabelle-HOL is the implementation of the logic *HOL* in Isabelle [Pau90,Pau03]. The meta-logic formalisation of *HOL* is based on natural deduction rules similar to those of first-order classical predicate calculus. The primitive operators are implication (`-->`), universal quantification (`ALL`) and the Hilbert description operator (`THE`).

All terms are typed, according to simple type theory, and quantification ranges over all the formulae. This is possible, because the formalisation relies on a *reflection principle*, which establishes an isomorphism between the *HOL* formulæ and the terms of type `bool`. Reflection is enforced by two operators: `term`, mapping formulae into terms, and `form`, mapping terms into formulae [Pau90].

The set of the theorems of a logic such as the ISPLs under consideration can be defined inductively, as the least fixed point generated by the axioms and the inference rules. In Isabelle-HOL, inductive definitions of this kind are well-supported. Formalising an object logic using an inductive definition turns out to be more convenient, when this is possible, than doing it by introducing new axioms. The object logic can then be treated as a conservative extension, i.e. it can be embedded into *HOL*, without putting at risk the consistency of the general framework. Moreover, the language of *HOL* is very expressive and particularly useful to reason at the meta-level. An example of this approach may be found in [DG02], where a framework for substructural logics is embedded into *HOL* in order to mechanise cut-elimination proofs.

Isabelle-HOL has an implementation of monotone inductive definitions associated to recursive data-types, that can be used to handle semi-automatically inductive proofs [Pau90]. The package tries to discharge automatically the monotonicity assumptions that are associated to the definition. Whenever these proofs succeed, the corresponding principle of structural induction is obtained for free.

Hence, it turns out that embedding a new logic in Isabelle-HOL can give significant advantages over formalising it in M, from the point of view of reliability as well as from those of expressiveness and automation.

7.3.1 Two embeddings

In the following, I am going to present two different formalisations of *I2* in Isabelle-HOL. Each of them will then be extended into formalisations of *C2* and *D2*. In order to define the logic inductively, compatibly with the constraints imposed by the Isabelle-HOL implementation of such definitions, it is important that substitution is predicative. The main difference between the two formalisations is in the way the second-order character is accounted for, compatibly with that restriction. One of the embeddings is based on an analogue of the reflection principle (hence, it will be also called the *reflection embedding* — the full theory is in Section B.1). The other one is based on an analogue of the Full Comprehension Schema (i.e. A9) and so it will be also called the *comprehension embedding* (Section B.2).

The reflection embedding of *I2* will be referred to as $I2_r$, and its comprehension embedding as $I2_c$ — accordingly, $C2_r$, $C2_c$, $D2_r$, $D2_c$ will be used in order to refer to the extensions.

As in the case of $I2_m$, I am going to rely on a formalisation based on inference rules. In contrast with that formalisation however, here it is possible to get closer to the style of the proofs that can be given with Hilbert-style systems, by proving the admissibility of the replacement principle. Another difference, lies in the fact that here the primitive inference rules are those of sequent calculus rather than those of natural deduction — this is also related to the implementation of inductive definitions in Isabelle.

7.3.2 Formulæ, comprehension and substitution

Isabelle requires inductive definitions to be *positive*, in the sense that there must be no negative occurrences, in the argument of a constructor, of the type that is being defined [Pau03].

In $b \mapsto a$, the occurrence of a is positive and that of b is negative. If $b \mapsto a$ is a positive occurrence in α, a is also positive, b is negative. If $b \mapsto a$ is a negative occurrence, then b is positive and a is negative.

In the positive inductive definition of a datatype wff, there cannot be any constructor of type $(\mathsf{wff} \mapsto \mathsf{wff}) \mapsto \mathsf{wff}$, since the type of the argument, $\mathsf{wff} \mapsto \mathsf{wff}$, contains a negative occurrence of wff. This is clearly a problem, when we want to formalise propositional quantification. In fact, from the point of view of a representation in terms of higher-order syntax, a quantifier over formulae should be exactly a function that maps $\mathsf{wff} \mapsto \mathsf{wff}$ into wff (as it is the case in $I2_m$).

Hence, it becomes necessary to introduce a distinction between formulae and terms. The closest to ISPL that can be embedded into *HOL*, compatibly with that distinction, is intuitionistic first-order predicate logic (*IPC*). The strategy here is then to embed *IPC* in *HOL*, and then to represent second-order propositional quantification in terms of first-order quantification. In the case of the embedding based on reflection, the $\to, \forall$ fragment of *IPC* turns out to be enough. In the case of the embedding based on comprehension, the whole of *IPC* is needed.

Since object-level propositional variables cannot be admitted explicitly, it is necessary to introduce a unary predicate `VAR` to obtain them from the individual variables. Given the *individual variable* `x`, one can say that `VAR x` represents the *propositional variable* associated to it.

In order to distinguish the logical symbols of the object logic from those of *HOL*, I will use the following ones: `->,AL2,&&,||,false,true,No,EX2,<-->` respectively for $\to, \forall, \wedge, \vee, \bot, \top, \sim, \exists, \leftrightarrow$. Since it is not necessary to make any specific assumption about the type of the terms, they can also be typed by a variable.

In $I2_r$ (the embedding of *I2* based on reflection), the recursive data-type of the formulæ (`'a wff`), depending on the type variable for the terms (`'a`), can be defined as follows — each constructor is given with its arguments, the concrete syntax is mandatory:

```
datatype
      'a wff = "VAR"    ('a)
             | "->"     ('a wff) ('a wff)    (infixr 25)
             | "Al2"   "('a) => ('a wff)"    (binder "AL2 " 10)
```

In $I2_c$ (the comprehension embedding of *I2*), where the whole of *IPC* is needed, the type of the formulæ is the following:

```
datatype
      'a wff =  "VAR" ('a)
             |   false
             |  "->" ('a wff) ('a wff)    (infixr 25)
             |  "&&" ('a wff) ('a wff)    (infixr 30)
             |  "||" ('a wff) ('a wff)    (infixr 30)
             |  "Al2" "('a) => ('a wff)"  (binder "AL2 " 10)
             |  "Ex2" "('a) => ('a wff)"  (binder "EX2 " 10)
```

In order to formalise propositional quantification with Full Comprehension, as required (Section 3.4), it is necessary to guarantee that for each formula there is an individual variable representing it. This is obtained quite differently in the two embeddings.

The idea behind the reflection embedding is to recast terms into formulæ and vice-versa. The predicate `VAR` already works as a coercion of terms into formulæ. For the other way round, which is needed in order to instantiate variables adequately, the idea here is to extend the language by an operator `TERM`, that converts formulæ into terms, and such that the equivalence `VAR (TERM A) <--> A` holds, for every formula `A`. The result of substituting a formula `A` for `x` in `B(x)` can then be expressed as `B(TERM A))`.

Introducing comprehension explicitly, on the other hand, seems to stand closer to the Hilbert axiomatisation given in Section 3.4. Essentially, in the comprehension embedding, a version of Full Comprehension (Schema A9) is added as part of the inductive definition of provability. Then, for every formula there has to be a variable that represents it, and so the substitution of `A` for `x` in `B(x)` can be expressed as `(VAR(y) <--> A) && B(y)`.

Another issue comes with the fact that the higher-order syntax for substitution makes it difficult, in meta-level proofs, to apply structural induction on formulæ. It is useful then to consider a way to replace the higher-order syntax with a first-order one, when this is convenient. For this reason, I have introduced in both the embddings an explicit substitution operator `SUBST:: 'a wff => 'a => 'a => 'a wff` such that `SUBST(C(x),B,x) <--> C(TERM B)`. This extension does not change the expressive power of the logic in any way, since `SUBST` can always be eliminated in favour of the high-order notation, whenever one is making proofs within the object logic. However, `SUBST` makes it considerably easier to prove properties of the object logic at the meta-level.

7.3.3 Sequents and inference rules

There are different senses in which a logic can be defined inductively. In particular, it is possible to define either the provable formulæ, or the provable sequents.

An Hilbert axiomatisation like one of those in Section 3.4 yields more naturally an inductive definition of provable formula. However, proofs in Hilbert systems may turn out to be rather cumbersome. On the other hand, natural deduction cannot be used, since the rule for the introduction of implication has already a rule on the left hand-side, i.e.:

```
[ A ==> B ] ==> A -> B
```

hence it is not acceptable as part of a monotone inductive definitions. So, in the end, sequent calculus turns out to be the best option.

A sequent is defined as a pair formed by a multiset of formulae for the antecedents (instead than a list) and a formula for the consequence, with syntax `H |- A`.

For the theory of multisets, I have relied on an existing Isabelle-HOL library (where the notation `{#A#}` is used for singletons, and `+` is the multiset union). The set that is going to be defined inductively is `seqs`, i.e. the set of the provable sequents.

```
"|-"   :: [('a wff) multiset, 'a wff] => bool        (infixl 5)
translations  "H |- A" == "(H, A) : seqs"
"seqs" :: "((('a wff) multiset) * ('a wff)) set"
```

The rules that are used are essentially those of intuitionistic first-order predicate calculus [TS00, Pau89]. The structural rules depend on the representation of the sequents — since here I am using multisets, no explicit rule is needed for Permutation. Although the form in which the rules are written allows for arbitrary antecedents, Weakening is needed as a rule. Contraction is needed too — however, an equivalent, contraction-free system could be obtained by modifying some of the operational rules on the same line of [Dyc92]. The rule Cut is needed for some of the extensions, i.e., in general, whenever axioms other than identity (`GAx` here) need to be used.

```
GAx      "H + {#A#} |- A"
Weak     "H |- P  ==> H + K |- P"
Cont     "H + {#A#} + {#A#} |- B ==> H + {#A#} |- B"
Cut      "[| H |- A;  H + {#A#} |- B |]  ==> H |- B"
```

The primitives, and hence the operational rules, differ depending on the kind of the embedding. In the case of $I2_r$, the only standard operational rules that are needed as primitive ones are those for `->` and `AL2`:

```
impR        "H + {#A#} |- B ==> H |- A->B"
impL        "[| H + {#B#} |- C;  H |- A |]
                                    ==> H + {#A->B#} |- C"
allR        "[| !!x::'a. H |- A(x) |] ==> H |- (AL2 x. A(x))"
allL        "H + {#A(x)#} |- B ==> H + {#AL2 x. A(x)#} |- B"
```

In fact, in the reflexion embeddings the definability of logical operators other than `->` and `AL2` is preserved.

```
"Ex2"    :: ('a => 'a wff) => 'a wff          (binder "EX2 " 10)
"&&"     :: ['a wff, 'a wff] => 'a wff        (infixr 35)
"||"     :: ['a wff, 'a wff] => 'a wff        (infixr 30)
"No"     :: 'a wff => 'a wff                  ("No _" [40] 40)
"<-->"   :: ['a wff, 'a wff] => 'a wff        (infixr 25)
"false"  :: 'a wff
"true"   :: 'a wff
```

The definitions are those by now familiar (Def. 8).

```
false_Def   "false == AL2 x. VAR(x)"
true_Def    "true == false -> false"
and_Def     "A && B == AL2 x. (A -> (B -> VAR(x))) -> VAR(x)"
or_Def      "A || B == AL2 x. (A -> VAR(x)) -> (B -> VAR(x))
                                        -> VAR(x)"
dimp_Def    "A <--> B == (A -> B) && (B -> A)"
not_Def     "No A == A -> false"
ex_Def      "Ex2 (A) == AL2 y. (AL2 x. A(x) -> VAR(y)) -> VAR(y)"
```

The operator `TERM :: 'a wff => 'a` is the coercion of formulæ into terms that is needed in order to have reflexion, and so, indirectly, also comprehension. `TERM` does not need to be defined explicitly. Its behaviour can be defined by the following inference rules:

```
compR       "H |- A ==> H |- VAR(TERM A)"
compL       "H + {#A#} |- B ==> H + {#VAR(TERM A)#} |- B"
```

Another possibility would be to extend the logic with a description operator, such as the one considered in [Sco79], and then to define `TERM` from it. However, this seems rather as an unnecessary complication from the point of view of the present purpose.

Besides, since the plan is to make meta-level proofs for this embedding, it is useful to include the operator `SUBST :: 'a wff => 'a wff => 'a => 'a wff` for explicit substitution. It is possible to give the following recursive definition:

```
primrec
```

```
"SUBST (VAR y) A x = (if y = x then VAR (TERM A) else VAR y)"
"SUBST (B -> C) A x = (SUBST B A x -> SUBST C A x)"
"SUBST (A12 B) A x =  A12 (%y. SUBST (B y) A x)"
```

However, the following rules give all that is really essential:

```
indR   "H |- B (TERM A) ==> H |- SUBST (B y) A y"
indL   "H + {#B (TERM A)#} |- C ==> H + {#SUBST (B y) A y#} |- C"
```

The reason that makes the recursive definition helpful, although not essential, is that it can be used by the Isabelle simplifier, making the replacement of `SUBST` semi-automatic. On the other hand, it does not seem possible to derive the rules from the recursive definition — so I choose to have both.

In the case of $I2_c$, Full Comprehension (corresponding to Schema A9 in Section 3.4) need to be introduced explicitly as an axiom in the sequent system:

```
FC          "H |- EX2 x. A <--> VAR(x)"
```

This extension makes the use of Rule Cut necessary. In fact, with the handling of assumptions that is allowed by sequent calculus, the normal way in which `FC` can be used in a proof, is by adding it as an assumption and then by discharging it with an application of Cut.

Moreover, with `FC`, derivations come to depend on a property of the existential quantifier, and so it turns out to be impossible to define all the connectives in terms of implication and universal quantification. In contrast with the reflection embedding, `&&`, `||` `EX2` and `false` are needed as primitives, with the corresponding operational rules (also in this case, those are the standard ones for *IPC*):

```
exR      "H |- A(x) ==> H |- EX2 x. A(x)"
exL      "[| !!(x::'a). H + {#A(x)#} |- B |] ==>
                                  H + {#EX2 x. A(x)#} |- B"
andR     "[| H |- A; H |- B |] ==> H |- A && B"
andL     "H + {#A#} + {#B#} |- C ==> H + {#A && B#} |- C"
orR1      "H |- A ==> H |- A || B"
orR2     "H |- B ==> H |- A || B"
orL     "[| H + {#A#} |- C; H + {#B#} |- C |] ==>
                                       H + {#A || B#} |- C"
ex_falso  "H |- false ==> H |- A"
```

It is now possible to extend each of the two embeddings with the rules corresponding to the Hilbert schemas A7 (for the Constant Domain condition) and A8 (Atomicity), used in Section 3.4 to axiomatise the logics *C2* and *D2*:

```
cdR   "H |- (AL2 x. A || B(x)) ==> H |- A || (AL2 x. B(x))"
mhR   "H |- AL2 x. No No A(x) ==> H |- No No (AL2 x. A(x))"
```

It is quite straightforward to show that the sequent systems $I2_r$ and $I2_c$ are equivalent to *I2* (the original Hilbert system). This can be done by translating the first-order language of the Isabelle-HOL theories into the second-order propositional language of the M formalisation (with `->` corresponding to `-->`, `AL2` to `ALL` etc.), by replacing uniformly `VAR x` with `x`, and (in the case of $I2_r$) `TERM A` with `x` (under the assumption `A <-> x`). In the case of $I2_c$, it can be observed that Full Comprehension is derivable in $I2_m$.

Similarly, $C2_r$ and $C2_c$, obtained by extending $I2_r$ and $I2_c$ with `cdR`, can be proved equivalent to *C2*. $D2_r$ and $D2_c$, obtained by extending $C2_r$ and $C2_c$ with `mhR`, can be proved equivalent to *D2*.

Of course, the way of extending the basic logics that is proposed here makes it rather hard to eliminate all the applications of Cut. It is possible to modify the notion of sequent in order to give a Cut-free formalisation of *C2* (using an approach similar to [LE81]). It seems too, that by modifying adequately the notion of sequent, a Cut-free formalisation for *D2* is obtainable. However, one has to bear in mind that even if Cut-free formalisations for the main logics — including some of their modal extensions — seem feasible, it might well still not be possible to have similar results for the spatial extensions considered in Section 5.3.

7.4 Examples of proofs

Although the comprehension embedding is comparatively closer to the original formulation of the logic, the reflection embedding make proofs easier. For this reason I have focused on $I2_r$ and on its extensions (see Section B.1). I will first give some examples of simple proofs, then I will move on to the verification of the decision procedure presented in Chapter 6, proving RE on the way. Finally, I will prove a theorem about spatial notions.

In order to derive a sequent, the inference rules can be applied backwards by *rtac* (short for *res_tac*). In the following example, `false` is rewritten with its definition, then `alljL` and `compL` are applied (backwards). The last subgoal is resolved against the axiom `GAx`.

```
Goalw[false_Def] "H + {#false#} |- A";
by (rtac alljL 1);
by (rtac compL 1);
by (rtac GAx 1);
qed "notjAx";
```

The following gives an example of the automation provided by `blast_tac`, taking as arguments a list of rules to be applied by `rtac`, regardless of the order, and the subgoal number.

```
Goalw[false_Def] "H + {#false#} |- A";
by (blast_tac ((claset() addIs [alljL,compL,GAx])) 1);
qed "notjAx";
```

Elimination rules in the style of natural deduction can be derived, typically by use of the Cut, as in the following:

```
Goal "H |- AL2 x. P(x) ==> H |- P(x)";
by (rtac Cut 1);
ba 1;
by (rtac alljL 1);
by (rtac GAx 1);
qed "alljD";
```

The application of rules to the antecedents is dealt by `res_tac` and left rules (such as `alljL` in the example).

Tactics formed by `dtac` (short for `dres_tac`) turn out to be useful when rules must be applied to sequents that are taken as assumptions. `auto()` combines together resolution with axioms, simplification and proof by assumption.

```
Goal "[| H |- AL2 x. A(x); H + {#A(x)#} |- B |] ==> H |- B";
br Cut 1;
by (dtac alljD 1);
auto();
qed "alljE";
```

The above can also be proved in one step, using `blast_tac`, as follows.

```
Goal "[| H |- AL2 x. A(x); H + {#A(x)#} |- B |] ==> H |- B";
by (blast_tac (claset() addIs [Cut] addDs [alljD]) 1);
qed "alljE";
```

In $I2_r$, all the sequent calculus rules for the defined logical operators can be derived quite easily, without using Cut.

7.4.1 Replacement

A significant example of meta-level reasoning is the inductive proof that $I2_r$ satisfies RE (Replacement of Equivalents — the proof for *I2* is given in Proposition 13).

A formalisation of RE in Isabelle-HOL can be given as follows.

```
H |- A <--> B  ==>  H |- C(TERM A) <--> C(TERM B)
```

Indeed, this rule turns out to be equivalent to the following:

[Sequent RE]

```
H + {#A <--> B#} |- C(TERM A) <--> C(TERM B)
```

In fact, the higher-order syntax for substitution forbids the capture of the free variables of `A` in `C(TERM(A))` (similarly for `B` and `C(TERM(B))`), without the need of adding any explicit proviso.

All the instances of Sequent RE are provable using the inference rules of $I2_r$. In order to prove RE in its general form, as a schema, induction on the complexity of formulæ is needed (see the discussion in Section 6.4).

Since the formulæ of $I2_r$ have been introduced as a recursive type (`'a wff`), the corresponding structural induction schema is produced automatically (`wff.induct` denotes it). The following variant (`wff_induct`) can be proved automatically from `wff.induct`:

```
 !!P. [| !!a. P (VAR a) &&
   !!wff1 wff2. P wff1 && P wff2 |] --> P (wff1 -> wff2) &&
   !!fun. (!!x. P (fun x)) --> P (Al2 fun) |] ==> P wff
```

This principle cannot be used directly in the proof of Sequent RE. The induction term in Sequent RE is `C`, that has type `'a => 'a wff`, whereas structural induction is on type `'a  wff`.

So, it turns out convenient to recast the expression `C(TERM(A))` into an equivalent one where `C(x)`, which is of type `'a wff`, can be treated as the induction term. This can be made by using the explicit substitution operator `SUBST`. In fact, `SUBST(A,B,x)` expresses that `TERM B` is substituted for `x` in `A`. One can rely on this, and write `SUBST(C(x),B,x)` instead of `C(TERM(B))`, since the following can be proved:

```
H |- SUBST(C(x),B,x) <--> C(TERM(B))
```

Now the following formalisation of RE can then be given:

[Sequent RE']

```
H + {#A <--> B#} |- AL2 x. (SUBST C(x) TERM(A) x) <-->
                                          (SUBST C(x) TERM(B) x)
```

This can be fed into Isabelle-HOL as a goal. After eliminating `<-->`, `&&` and `AL2`, one is left with the following expression:

```
!!x. H + {#A -> B#} + {#B -> A#} |-
     (SUBST C A x -> SUBST C B x) && (SUBST C B x -> SUBST C A x)
```

The induction principle can be applied without problems this time. The instantiation of the induction predicate `P` has to be made explicitly — for this reason, `res_inst_tac` is used instead of `res_tac`:

```
by (res_inst_tac [("P","%c::'a wff.
      H + {#A -> B#} + {#B -> A#} |-
        (SUBST c A x -> SUBST c B x) &&
        (SUBST c B x -> SUBST c A x)")] wff_induct 1);
```

This step generates three subgoals that can be proved by using object-level inference rules. Finally, Sequent RE and Sequent RE' can be be proved to be equivalent. This proof can be turned quite immediately into proofs for the extensions $C2_r$ and $D2_r$, since for the way the schemas are given, arbitrary antecedents are allowed.

7.4.2 Verification of the decision procedure

The eliminability of quantifiers from the negative formulæ of $D2$, as proved in Proposition 62, follows immediately from the proof of the schematic formula in Proposition 61 (ANQE). In $D2_r$ ANQE can be formalised as follows:

```
Goal "!! H :: ('a wff) multiset. !! F :: 'a => 'a wff.
  !! C :: 'a => 'a wff.
    H |- No (F (TERM (AL2 x. (C x)))) <-->
      No (F (TERM (C (TERM true) && C (TERM false))))";
```

This can be proved by the following steps (`br` is short for `by rest_tac`):

```
br schema_b1 1;
br dimp_sym 1;
br schema_b1 1;
br dneg_dimp_imp2_rule 1;
br replacement_dneg_rule 1;
br all_elim_r 1;
qed "de_quantification_eq";
```

The lemmas used in the proof steps are the following ones:

```
schema_b1 = H |- No No No A <--> C ==> H |- No A <--> C
dimp_sym = H |- A <--> B ==> H |- B <--> A
dneg_dimp_imp2_rule = H |- No No (A <--> B) ==>
                         H |- No No A1 <--> No No B

replacement_dneg_rule = H |- No No (A <--> B) ==>
                H |- No No (C (TERM A) <--> C (TERM B))
all_elim_r =  H |- No No (C (TERM true) &&
                      C (TERM false) <--> (AL2 x. C x))
```

The proof of `replacement_dneg_rule` is of based on RE. The proof of `all_elim_r` uses the rule `mhR` (the only one which is specific for $D2_r$). It is also possible to derive ANQE in $I2_r$, by including `mhR` as an assumption, in the following way:

```
!! H :: ('a wff) multiset. !! F :: 'a => 'a wff.
 !! C :: 'a => 'a wff. EX A.
   (H + {#(AL2 x. No (No A(x))) -> No (No (AL2 x. A(x)))#}
      |- No (F (TERM (AL2 x. (C x)))) <-->
           No (F (TERM (C (TERM true) && C (TERM false)))))
```

Indeed, this schema is provable in $I2_r$ without any essential use of Cut.

7.4.3 A spatial theorem

In the following, I give an example of mechanised proof that is relevant from the point of view of the spatial representation discussed in the previous chapters. In Section 5.2.2 it has been argued that the expression $\mathsf{nempty}(\alpha)$ can be used to represent non-emptiness, in the models for certain extensions of $D2$.

Proposition 42 expresses a relationship between non-emptiness and connectedness, which is quite significant from an intuitive point of view: whenever the intersection of two $\mathcal{R}$-connected regions is non-empty, their sum is $\mathcal{R}$-connected.

Indeed, it turns out that in $I2$ it is already possible to prove the formal expression given in Proposition 42, where $\mathcal{R}$-connectedness (for regular opens) is represented with the operator con_s (by Proposition 38). Since the proof of this theorem is long and involves lots of subcases, the mechanisation has turned out to be quite helpful.

It is useful first to prove the following lemma, which is basically suggested by the topological interpretation and Proposition 38.

[Auxiliary Lemma]

```
H |- (AL2 x. (A -> (No (No VAR(x))) || No VAR(x)) ->
         (A -> (No (No  VAR(x)))) || (A -> No VAR(x))) <-->
      (AL2 x. (A -> VAR(x) || No VAR(x)) ->
           (A -> VAR(x)) || (A -> No VAR(x)))
```

Considering the definition of ndiv_s in Proposition 38, this simply means that
$(\forall x.\mathsf{ndiv}_s(\alpha, x)) \leftrightarrow (\forall x.\mathsf{ndiv}_s(\alpha, \approx x))$

is provable in *I2*.

Bearing in mind that

$\mathsf{nempty}(\alpha) = \sim\alpha \rightarrow \forall xy.\mathsf{ndiv}_s(x, y)$

(by Proposition 41) and that $\mathsf{con}_s(\alpha) = \forall x.\mathsf{ndiv}_s(\alpha, x)$, by Proposition 38, it turns out convenient to extend $I2_r$ with the following definition, corresponding to $\mathsf{ndiv}_s(\alpha, \approx\beta)$:

```
NDIV A B == (A -> ((No (No B)) || (No B))) ->
             ((A -> (No (No B))) || (A -> (No B)))
```

It has been possible then to prove the following:

[NEMPTY Lemma]

```
H |- ((No (A && B)) ->
      (AL2 v. AL2 x.  (NDIV ((VAR v) (VAR x))))) &&
      (AL2 u. (NDIV A (VAR u))) && (AL2 u. (NDIV B (VAR u)))
        -> (AL2 u. (NDIV (No (No (A || B))) (VAR u)))
```

Given the Auxiliary Lemma and RE, the NEMPTY Lemma turns out to be equivalent to the schema in Proposition 42.

This gives an example of how the mechanisation of ISPL can be used in topological reasoning. It also reinforces the suggestion that, in the context of interactive theorem-proving, meta-level reasoning can be quite helpful, insofar as certain intuitions coming from the semantics may be usefully adopted as guidelines for a proof.

Chapter 8

Conclusions and further issues

It has been shown that super-intuitionistic logics, obtained as extensions of *IPL*, can be used to represent topological notions, in a way that could be significant from the point of view of applications to spatial reasoning. This result can be regarded as a widening of the scope of the result about *IPL* in [Ben96]. Distinctively, the semantics of the logics that are introduced in the present work lend themselves quite naturally to represent certain aspects of granularity. The practical value of these acquisitions rests on the general interest that region-based techniques have from the point of view of spatial information systems, as discussed in the Introduction.

The extensions of *IPL* that have been considered are some of those based on propositional quantification and intuitionistic modalities (Chapter 3) as well as some of the axiomatic ones (Section 5.3 and Section 5.1; see Appendix A for a summary). The logical operators in these logics can be used in order to convey their standard logical meaning, as well as to represent spatial notions. The syntax introduced in Section 4.1.2 in relationship with the notion of spatial models (Def. 25) is used in Chapter 5 in order to mark the difference between the logical and the spatial meaning. This distinction can make the expressions more readable, although it is not essential from the proof-theoretical point of view.

Finally, it has been shown how to formalise intuitionistic second-order propositional logic (ISPL) into a state-of-the-art interactive theorem prover, Isabelle-HOL, relying on an approach that allows also proofs at the meta-level (Chapter 7).

8.1 Computational issues

The logics that have been discussed in Chapter 3 are largely undecidable. This is the case for *I2* and *C2* [Gab81], and it is probably the case for *D2* as well (although here I cannot produce an argument for this claim). The fact that these logics are conservative extensions of *IPL* means however that their quantifier-free fragments are decidable (Proposition 66). The algorithms that solve the decision problem for *IPL* are at best PSPACE-complete [Dyc92] — in contrast with the NP-completeness of the corresponding problem for classical propositional logic. However, [RN99] defines a tractable fragment of *RCC* which is closely related to the *IPL* encoding of the *RCC*8 relations in [Ben96, Ben98].

The result concerning *D2* about the negative formulæ (Proposition 59) marks a significant difference with more standard, weaker forms of ISPL. This difference seems particularly interesting insofar as *D2* has an interpretation that seems quite natural, from the point of view of digital representation (Sections 4.3, 5.1).

The modal logic that is obtained by adding to *IPL* the quantifier-free schemas used for the axiomatisation of the N-modality (Schemas A10 - A12, A14 and Rule A13, in Section 3.5) turns out to be decidable. In fact, it can be regarded as an axiomatic extension of the modal intuitionistic logic *IntS4* [WZ99] that has the finite model property.

Significantly enough, the encoding of the *RCC*8-style relations in Proposition 56 (A) does not require quantification, and hence yields a decidable fragment. This fact is not surprising, considering the result in [Ben96]. The encoding of apartness that is given here (ap in Section 5.2.3) is different, though, from the encoding of the corresponding relation in that paper (i.e. the relation there called *disconnection*). In [Ben96], in fact, the models are based on connected spaces, and the formulæ α and β represent open sets that are apart from each other iff $\sim\alpha \vee \sim\beta$ is satisfied by the model. This idea does not fit well under the stronger assumption that the space is prime. That assumption has been made here because it seems more natural from the point of view of granularity (see Section 4.3.1). Moreover, primeness is necessary in order to encode $\mathcal{R}$-connectedness by con_s (as in Proposition 39).

On the other hand, it does not seem difficult to relax the primeness assumption in the modal case. When the modal schemas A12 and A17 are dropped from the axiomatisation of N-modality, the logics that are obtained could be proved complete w.r.t. frames that correspond to Alexandroff connected spaces (the details cannot be included here). This would make it possible to have a spatial language with propositional quantification, allowing for two forms of apartness, that would be quite precisely an extention of the language in [Ben96].

A topic for further enquiry is whether there are significant fragments of ISPL that are decidable. A result in [Pit92] states the possibility of representing ISPL in

IPL. However, that representation turns out to give a logic that is too strong for the topological interpretation considered here, as it appears from [Pol98].

On the other hand, the system $I2_r$ in Section 7.3 shows that ISPL can be represented by extending a fragment of monadic first-order intuitionistic predicate calculus (*IPC*) with a reflection principle (in fact, `VAR` is the only predicate). Although the monadic formulæ of *IPC* are not generally decidable (in contrast with the classical case), a decision procedure for a subclass (the monadic formulæ that contain only one variable within the scope of those quantifiers that appears in negative positions) can be found in [Tam96]. This could be an interesting possibility, especially in relationship with the modality-free encoding of qualitative relations given in Proposition 55.

8.2 Proof-theoretical issues

The proof systems in Section 7.3 are based on the standard formalisation of *IPC* as a sequent calculus [TS00]. This does not raise problems from the point of view of interactive theorem-proving. However, there are significant improvements that could be made, in view of a possible automation (at least partial) of the object-level proofs. It is known that sequent systems including Rule Contraction do not lead naturally to terminating algorithms, even when the system is decidable, unless a specific check for loop-detection is added. In order to avoid the need of such extra-logical features, contraction-free systems have been devised. In particular, the contraction-free systems for *IPL* in [Dyc92] involves a minimum of change with respect to the standard formalisation. By modifying accordingly the present formalisation of $I2_r$, it should not be hard to obtain a contraction-free system for *I2* and for its extensions.

The issue about the elimination of Rule Cut is also quite substantial from the point of view of automation, as observed in Section 7.1. For this problem, I refer to the comment at the end of Section 7.3.3.

8.3 Conclusions

Further investigation into the computational properties of super-intuitionistic logics (inclusive of ISPLs and IMLs) can be useful for theorem-proving in topology as well as for spatial reasoning applications. The Isabelle-HOL implementation suggests that a mechanised, interactive support can be useful in order to check proofs, analyse their content and validate semantical hypothesis, also in the context of non-classical logics, which are more often associated to automated theorem-proving and model-checking techniques.

Non-classical logics can be regarded as a promising framework for several branches of AI reasoning, allowing for a modular, reliable development of specific reasoners. Within spatial reasoning, granularity seems to be one of the key issues in order to manage information efficiently and safely. Super-intuitionistic logics look like a promising field from the point of view of computational topology, insofar as these logics make it possible to combine together a granular characterisation of the models and an expression of connectivity, with a remarkable simplicity from the logical point of view, allowing the introduction of a notion of parallel development between high-level specifications and computations in spatial systems, that could have interesting applications in remote sensing, pattern recognition and image processing.

Bibliography

[Aie02] M. Aiello. A modal walk through space. *Journal of Applied Non-Classical Logics*, 12(3–4):319–363, 2002.

[AvB02] M. Aiello and J. van Benthem. Logical patterns in space. In *Words, Proofs, and Diagrams*, pages 5–25. CSLI, 2002.

[Bar92] H. P. Barendregt. Lambda calculi with types. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 2, pages 117–309. Oxford – Clarendon Press, 1992.

[BCTH00a] B. Bennett, A. G. Cohn, P. Torrini, and S. M. Hazarika. Describing rigid body motions in a qualitative theory of spatial regions. In Henry A. Kautz and Bruce Porter, editors, *Proceedings of AAAI-2000*, pages 503–509. AAAI Press, 2000.

[BCTH00b] B. Bennett, A. G. Cohn, P. Torrini, and S. M. Hazarika. A foundation for region-based qualitative geometry. In W. Horn, editor, *Proceedings of ECAI-2000*, pages 204–208. IOS Press, 2000.

[BCTH00c] B. Bennett, A. G. Cohn, P. Torrini, and S. M. Hazarika. Region-based qualitative geometry. Technical Report 2000.7, School of Computing, University of Leeds, 2000.

[BCWZ02] B. Bennett, A. G. Cohn, F. Wolter, and M. Zakharyaschev. Multi-dimensional modal logic as a framework for spatio-temporal reasoning. *Applied Intelligence*, 17(3):239–251, 2002.

[BDCTV97] P. Balbiani, L. F. Del Cerro, T. Tinchev, and D. Vakarelov. Modal logics for incidence geometries. *Journal of Logic and Computation*, 7(1):59–78, 1997.

[BDFM95] M. Bertolotto, L. De Floriani, and P. Marzano. A unifying framework for multilevel description of spatial data. In *Proceedings of COSIT'95 (LNCS 988)*. Springer, 1995.

[Ben96] B. Bennett. Modal logics for qualitative spatial reasoning. *Bulletin of the Interest Group in Pure and Applied Logic (IGPL)*, 4(1):23–45, 1996.

[Ben97] B. Bennett. *Logical Representations for Automated Reasoning about Spatial Relationships*. PhD thesis, School of Computer Studies, University of Leeds, 1997.

[Ben98] B. Bennett. Determining consistency of topological relations. *Constraints*, 3(2&3):213–225, June 1998.

[Ber98] M. Bertolotto. *Geometric Modeling of Spatial Entities at Multiple Levels of Resolution*. PhD thesis, DISI, Univ. Genova, 1998.

[BGM96] S. Borgo, N. Guarino, and C. Masolo. A pointless theory of space based on strong congruence and connection. In L. Carlucci Aiello and J. Doyle, editors, *Principles of Knowledge Representation and Reasoning, Proceedings of the 5th International Conference, KR96*. Morgan Kaufmann, 1996.

[Bir40] G. Birkhoff. *Lattice Theory*, volume 25. Amer. Math. Soc. Coll. Pub., 1940.

[BM02] D. Basin and S. Matthews. Logical frameworks. In Dov Gabbay and Franz Guenthner, editors, *Handbook of Philosophical Logic, second edition*, volume 9, pages 89–164. Kluwer Academic Publishers, Dordrecht, 2002.

[BS98] T. Bittner and J. G. Stell. A boundary-sensitive approach to qualitative location. *Annals of Mathematics and Artificial Intelligence*, 24:93–114, 1998.

[Bun83] A. Bundy. *The computer modelling of mathematical reasoning*. Academic Press, 1983.

[CBGG97] A. G. Cohn, B. Bennett, J. Gooday, and N. Gotts. RCC: a calculus for region based qualitative spatial reasoning. *GeoInformatica*, 1:275–316, 1997.

[CDF95] E. Clementini and P. Di Felice. A comparison of methods for representing topological relationships. *Information Sciences*, 3:149–178, 1995.

[CDF97] E. Clementini and P. Di Felice. Approximate topological relations. *International Journal of Approximate Reasoning*, 16:173–204, 1997.

[CG96] A.G. Cohn and N.M. Gotts. A mereological approach to representing spatial vagueness. In J. Doyle L. C. Aiello and S. Shapiro, editors, *Principles of Knowledge Representation and Reasoning, Proc. 5th Conference*, pages 230–241. Morgan Kaufmann, 1996.

[CH01] A. G. Cohn and S. M. Hazarika. Qualitative spatial representation and reasoning: An overview. *Fundamenta Informaticae*, 46(1-2):1–29, 2001.

[Che80] B. F. Chellas. *Modal Logic: An Introduction.* Cambridge University Press, 1980.

[Cla81] B. L. Clarke. A calculus of individuals based on 'connection'. *Notre Dame Journal of Formal Logic*, 23(3):204–218, July 1981.

[CV98] A. G. Cohn and A. Varzi. Connection relations in mereotopology. In H. Prade, editor, *Proceedings of the 13th European Conference on Artificial Intelligence (ECAI-98)*, pages 150–154. Wiley, August 1998.

[DG02] E. J. Dawson and R. Gore. Formalised cut admissibility for display logic. In *Proc. 15th International Conference on Theorem Proving in Higher Order Logic (TPHOL02), LNCS 2410*, pages 131–147. Springer, 2002.

[Dor98] C. Dornheim. Undecidability of plane polygonal mereotopology. In Anthony G. Cohn, Leonard Schubert, and S. Shapiro, editors, *Principles of Knowledge Representation and Reasoning: Proceedings of the 6th International Conference (KR-98)*, pages 342–353. Morgan Kaufman, 1998.

[Dyc92] R. Dyckhoff. Contraction-free sequent calculi for intuitionistic propositional logic. *Journal of Symbolic Logic*, 57(3):795–807, 1992.

[Eng78] R. Engelking. *Dimension and Theory.* North-Holland, 1978.

[FG82] M. P. Fourman and R. J. Grayson. Formal spaces. In A. S. Troelstra and D. van Dalen, editors, *The L. E. J. Brouwer Centenary Symposium*, pages 107–122. Noth Holland, 1982.

[Fit69] M. Fitting. *Intuitionistic logic – model theory and forcing.* North-Holland, 1969.

[Fle01] J. D. Fleuriot. Theorem proving in infinitesimal geometry. *Logic Journal of the IGPL*, 9(3):447–474, 2001.

[FS79] M. P. Fourman and D. Scott. Sheaves and logic. In *Springer Lecture Notes in Mathematics No. 753*, pages 302–402. Springer Verlag, 1979.

[Gab74] D. M. Gabbay. On 2-nd order intuitionistic propositional calculus with full comprehension. *Arch.f.Math.Log.u.Grund.Math.*, 16:177–186, 1974.

[Gab81] D. M. Gabbay. *Semantical Investigation in Heyting intuitionistic logic.* Number 148 in Synthese. Reidel, 1981.

[GCMP99] M. Gordon, A. Cohn, T. Melham, and A. Pitts. *The HOL system description - version 3 (for HOL90.9).* SRI International, February 1999.

[Ger95] G. Gerla. Pointless geometries. In F. Buekenhout, editor, *Handbook of Incidence Geometry*, pages 1015–1031. Elsevier, 1995.

[GJ79] M. R. Garey and D. S. Johnson. *Computers and intractability : a guide to the theory of NP-completeness.* Freeman, 1979.

[GKWZ03] D. M. Gabbay, A. Kurucz, F. Wolter, and M. Zakharyaschev. *Many-Dimensional Modal Logics: Theory and Applications.* Elsevier, 2003.

[Gli29] V. Glivenko. Sur qulques points de la logique de m. brouwer. *Bulletins de la classe des sciences*, 15:183–188, 1929.

[Goe71] S. Goernemann. A logic stronger than intuitionism. *Journal of Symbolic Logic*, 36:249–261, 1971.

[Hud00] P. Hudak. *The Haskell School of Expression.* Cambridge University Press, 2000.

[JAN02] Spatial logics (special issue). In P. Balbiani, editor, *Journal of Applied Non-Classical Logics*, volume 12. Lavoisier, 2002.

[Joh82] P. T. Johnstone. *Stone Spaces.* Cambridge University Press, 1982.

[Kel55] J. L. Kelley. *General Topology.* Van Nostrand, 1955.

[Kop92] R. Kopperman. The Khalimsky line as a foundation for digital topology. In O. Ying-Lie, A. Toet, D. Foster, H.J.A.M. Heijmans, and P. Meer, editors, *Shape in picture*, pages 3–20. Springer-Verlag, 1992.

[Kov92] V. A. Kovalevsky. A new concept for digital geometry. In O. Ying-Lie, A. Toet, D. Foster, H.J.A.M. Heijmans, and P. Meer, editors, *Shape in picture*, pages 37–52. Springer-Verlag, 1992.

[Kre97] P. Kremer. On the complexity of propositional quantification in intuitionistic logic. *Journal of Symbolic Logic*, 62(2):529–544, 1997.

[KSS+03] O. Kutz, H. Sturm, N.Y. Suzuki, F. Wolter, and M. Zakharyaschev. Logics of metric spaces. *Transactions on Computational Logic (to appear)*, 2003.

[LE81] E. G. K. Lopez-Escobar. On the interpolation theorem for the logic of constant domains. *Journal of Symbolic Logic*, 46:87–88, 1981.

[Lei94] D. Leivant. Higher order logic. In D.M. Gabbay, C.J. Hogger, and J.A. Robinson, editors, *Handbook of Logic in Artificial Intelligence and Logic Programming*, volume 2, pages 229–331. Oxford – Clarendon Press, 1994.

[Leś31] S. Leśniewski. O podstawach matematyki. *Przeglad Filozoficzny*, 30–34, 1927–1931.

[Loe76] M. H. Loeb. Embedding first order predicate logic in fragment of intuitionistic logic. *Journal of Symbolic Logic*, 41:705–718, 1976.

[LP96] O. Lemon and I. Pratt. On the incompleteness of modal logics of space: advancing complete modal logics of place. In M. Kracht, M. de Rijke, and M. Zakharyaschev, editors, *Advances in Modal Logic '96*, pages 115–132. CSLI Publications, 1996.

[LT92] R. Laurini and D. Thompson. *Fundamentals of Spatial Information Systems.* Academic Press, 1992.

[Min92] G. Mints. Complexity of subclasses of the intuitionistic propositional calculus. *BIT*, 32(1):64–69, 1992.

[Moe82] I. Moerdijk. Some topological spaces which are universal for intuitionistic predicate logic. *Nederl. Akad. Wetensch. Indag. Math.*, 44(2):227–235, 1982.

[MRL+00] R. Mueller, T. Roefer, A. Lankenau, A. Musto, K. Stein, and Eisenkolb A. *Coarse Qualitative Descriptions in Robot Navigation*, pages 265–276. Number 1849 in Lecture Notes in Artificial Intelligence. Springer, 2000.

[MT48] J. C. C. McKinsey and A. Tarski. Some theorems about the sentential calculi of Lewis and Heyting. *Journal of Symbolic Logic*, 13:1–15, 1948.

[MV99] C. Masolo and L. Vieu. Atomicity vs. infinite divisibility of space. In C. Freska and D. Mark, editors, *Spatial Information theory. Proceedings of COSIT'99*, pages 235–250. Springer, 1999.

[OBS92] A. Okabe, B. Boots, and K. Sugihara. *Spatial Tessellations – concepts and applications of Voronoi diagrams.* John Wiley, Chichester, 1992.

[Pau89] L. C. Paulson. The foundation of a generic theorem prover. *Journal of Automated Reasoning*, 5(3):363–397, 1989.

[Pau90] L. C. Paulson. A formulation of the simple theory of types (for Isabelle). In *COLOG-88: International Conf. in Computer Logic*, number 417 in LNCS, pages 246–274. Springer, 1990.

[Pau91] L. C. Paulson. *ML for the working programmer.* Cambridge University Press, 1991.

[Pau96] L. C. Paulson. Tool support for logics of programs. In M. Broy, editor, *Mathematical Methods in Program Development (Summer School Marktoberdorf 1996)*, pages 461–498. Springer-Verlag, 1996.

[Pau02] L. C. Paulson. *The Isabelle Reference Manual.* University of Cambridge, electronic publication, 2002.

[Pau03] L. C. Paulson. *Isabelle's Logics: HOL.* University of Cambridge, electronic publication, 2003.

[PH02] I. Pratt-Hartmann. A topological constraint language with component counting. *Journal of Applied Non-Classical Logics*, 12(3–4):441–468, 2002.

[Pit92] A. Pitts. On an interpretation of second-order quantification in first-order intuitionistic logic. *Journal of Symbolic Logic*, 57(1):33–52, 1992.

[Pol98] T. Polacik. Propositional quantification in the monadic fragment of intuitionistic logic. *Journal of Symbolic Logic*, 63(1):269–300, 1998.

[Pra65] D. Prawitz. *Natural Deduction: A Proof-Theoretical Study.* Almqvist and Wiksell, 1965.

[PS98] I. Pratt and D. Schoop. A complete axiom system for polygonal mereotopology of the real plane. *Journal of Philosophical Logic*, 27:621–658, 1998.

[RCC92] D. A. Randell, Z. Cui, and A. G. Cohn. A spatial logic based on regions and connection. In *Proc. 3rd Int. Conf. on Knowledge Representation and Reasoning*, pages 165–176. Morgan Kaufmann, 1992.

[Ren98] J. Renz. A canonical model of the Region Connection Calculus. In A.G. Cohn, L. Schubert, and S. Shapiro, editors, *Principles of Knowledge Representation and Reasoning: Proc. of the 6th Int. Conference (KR-98)*, pages 330–341. Morgan Kaufman, 1998.

[RHB02] K. F. Riley, M. P. Hobson, and S. J. Bence. *Mathematical Methods for Physics and Engineering.* Cambridge University Press, 2002.

[RN98] J. Renz and B. Nebel. Efficient methods for qualitative spatial reasoning. In H. Prade, editor, *Proceedings of the 13th European Conference on Artificial Intelligence (ECAI-98)*, pages 562–566. Wiley, August 1998.

[RN99] J. Renz and B. Nebel. On the complexity of qualitative spatial reasoning: a maximal tractable fragment of the Region Connection Calculus. *Artificial Intelligence*, 108(1–2):69–123, 1999.

[RS63] H. Rasiowa and R. Sikorski. *The Mathematics of Metamathematics.* Polish Academy, 1963.

[RS02] A. J. Roy and J. G. Stell. A qualitative account of discrete space. In M.J. Egenhofer and D.M. Mark, editors, *Proceedings of GIScience 2002*, volume 2478 of *Lecture Notes in Computer Science*, pages 276–290. Springer-Verlag, 2002.

[Sam89] G. Sambin. Intuitionistic formal spaces and their neighbourhood. In *Logic Colloquium 88*, pages 261–285. North Holland, 1989.

[Sco79] D. Scott. Identity and existence in intuitionistic logic. In *Springer Lecture Notes in Mathematics No. 753*, pages 660–696. Springer Verlag, 1979.

[She99] V. Shehtman. 'Everywhere' and 'here'. *Journal of Applied Non-Classical Logics*, 9(2-3):369–279, 1999.

[Skv97] D. Skvortsov. Non-axiomatisable second order intuitionistic propositional logic. *Annals of pure and applied logic*, 86:33–46, 1997.

[Smy92] M. B. Smyth. Topology. In S. Abramsky, D.M. Gabbay, and T.S.E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 1, pages 641–761. Oxford – Clarendon Press, 1992.

[Ste00a] J. G. Stell. Boolean connection algebras: a new approach to the region-connection calculus. *Artificial Intelligence*, 122:111–136, 2000.

[Ste00b] J. G. Stell. The representation of discrete multi-resolution spatial knowledge. In A. G. Cohn, F. Giunchiglia, and B. Selman, editors, *KR-2000*, pages 38–49. Morgan Kaufmann, 2000.

[SVV96] G. Sambin, S. Valentini, and P. Virgili. Constructive domain theory as a branch of intuitionistic pointfree topology. *Theoretical Computer Science*, 159:319–341, 1996.

[SW97] J. G. Stell and M. F. Worboys. The algebraic structure of sets of regions. In Stephen C. Hirtle and Andrew U. Frank, editors, *Proceedings of COSIT'97*, volume 1329 of *LNCS*, pages 163–174. Springer, 1997.

[SW98] J. G. Stell and M. F. Worboys. Stratified map spaces: a formal basis for multi-resolution spatial databases. In *Proceedings of the 8th International Symposium on Spatial Data Handling, SDH'98*, pages 180–189, 1998.

[Tam96] T. Tammet. A resolution theorem prover for intuitionistic logic. In *CADE-13 (LNCS 1104)*, pages 2–16. Springer, 1996.

[Tar56] A. Tarski. Sentential calculus and topology. In *Logic, Semantics, Metamathematics*. Oxford University Press, 1956.

[Tor01] P. Torrini. Connectedness in Alexandroff spaces with intuitionistic 2nd-order propositional logic. Technical Report 2001.13, School of Computing, University of Leeds, 2001.

[TS00] A. S. Troelstra and H. Schwitchtenberg. *Basic Proof Theory*. Cambridge University Press, 2000.

[TSB02] P. Torrini, J. G. Stell, and B. Bennett. Mereotopology in 2nd-order and modal extensions of intuitionistic logic. *Journal of Applied Non-Classical Logics*, 12(3–4):495–525, 2002.

[VDDB02] D. Vakarelov, G. Dimov, I. Düntsch, and B. Bennett. A proximity approach to some region-based theories of space. *Journal of Applied Non-Classical Logics*, 12, 2002.

[VDDVL00] J. Van Der Does and M. Van Lambalgen. A logic of vision. *Linguistics and Philosophy*, 23:1–92, 2000.

[Ven99] Y. Venema. Points, lines and diamonds: a two-sorted modal logic for projective planes. *Journal of Logic and Computation*, 9(5):601–621, 1999.

[Vic89] S. Vickers. *Topology via logic*. Cambridge University Press, 1989.

[Wor95] M. Worboys. *GIS: a computing perspective*. Taylor and Francis, 1995.

[WZ99] F. Wolter and M. Zakharyaschev. Intuitionistic modal logic. In *Logic and Foundations of Mathematics*, pages 227–238. Synthese Library, Kluwer, 1999.

[WZ00] F. Wolter and M. Zakharyaschev. Spatio-temporal representation and reasoning based on RCC-8. In A. G. Cohn, F. Giunchiglia, and B. Selman, editors, *Proceedings of KR'00*, pages 3–14. Morgan-Kaufman, 2000.

[WZ02] F. Wolter and M. Zakharyaschev. Qualitative spatio-temporal representation and reasoning: a computational perspective. In *Exploring Artificial Intelligence in the New Millenium*. Morgan-Kaufmann, 2002.

[ZWC02] M. Zakharyaschev, F. Wolter, and A. Chagrov. Advanced modal logics. In H. Guenthner D. Gabbay, editor, *Handbook of Philosophical Logic, Second Edition*, volume 3, pages 83–266. Kluwer, 2002.

Appendix A

Notation

1. - $\mathcal{S} = (S, \mathcal{O})$ is a topological space, where S is a set, $\mathcal{O}$ is the collection of the open sets.
   - $\mathcal{C}$ is the collection of the closed sets in $\mathcal{S}$.
   - $\prec$ is the specialisation order.

2. - $(S, <)$ is a pre-order on S.
   - $\mathcal{U}_<$ is the collection of the sets that are upper-closed w.r.t. $<$.
   - $\mathsf{a}\uparrow$ is the pointed set generated by a — i.e. the smallest upper-closed set that contains a.

3. - $(S, \leq, \mathbf{0})$ is a Kripke frame (Def. 15), $(S, V, \leq, \mathbf{0})$ is a V-modal Kripke frame (Def. 18).
   - Where $\mathcal{F}$ is a Kripke frame, $(\mathcal{F}, \mathcal{R}, \rho)$ is a Kripke model (Def. 16, Def. 19).
   - $\models_M$ is used for validity in a Kripke model $\mathcal{M}$.

4. - $(S, \mathcal{O}, \mathcal{R}, \tau)$ is a spatial model (Def. 25; τ may be dropped).
   - $\Vdash_Z$ is used for validity in a spatial model $\mathcal{Z}$.
   - $\prec_{\mathcal{R}}$ is the $\mathcal{R}$-specialisation order.
   - $\mathsf{a}\uparrow_{\mathcal{R}}$ is the $\mathcal{R}$-pointed set generated by a — i.e. the intersection of all the definable opens that contain a.

Symbol	*Topological meaning*	*Algebraic meaning*
$\sqsubseteq$	inclusion	partial order
$\sqcap$	intersection (binary)	meet
$\sqcup$	union (binary)	join
$\bigwedge$	intersection (over arbitrary collections)	arbitrary meet
$\bigvee$	union (over arbitrary collections)	arbitrary join
$-$	set-theoretic complement	Boolean complement
$\mathsf{I}A$	$\bigvee\{X \in \mathcal{O} \mid X \sqsubseteq A\}$	interior of A
$\mathsf{C}A$	$\bigwedge\{X \in \mathcal{C} \mid A \sqsubseteq X\}$	closure of A
A^*	$\mathsf{I}(-A)$	pseudo-complement of A
A^{**}	regularisation of A	double pseudo-complement of A
$A + B$	$(A \sqcup B)^{**}$	mereological sum of A and B
$A \Rightarrow B$	$\mathsf{I}(-A \sqcup B)$	pseudo-complement of A relative to B

Symbol	*Meaning*	*Definition*
regl	regular open	Prop.35
atmcell	atomic cell	–
screen	screen	–
prime	$\mathcal{R}$-prime	Prop. 36
ndiv	not split by	Prop. 38
con	$\mathcal{R}$-connected	–
ndiv_s	nowhere split by	–
con_s	strongly $\mathcal{R}$-connected	–
degnr	degenerate	Prop. 40
nempty	weakly non-empty	Prop. 41
ap	apart	Prop. 43
ic	interconnected	–
ic_s	strongly interconnected	–
ap_w	weakly apart	–
ic_i	strongly interconnected (without modality)	–
ntp	non-tangential part	Prop. 47
tp	tangential part	–
ntp_w	weakly non-tangential part	–
tp_s	strongly tangential part	–
tp_i	strongly tangential part (without modality)	–
$=^t, \neq^t, \sqsubseteq^t, \not\sqsubseteq^t$	extensional relations	Def. 24

Intermediate axioms:

1. $\Sigma_1 = \forall x.x \vee (x \rightarrow \mathsf{degnr})$
   Prop. 48

2. $\Sigma_2 = \forall xy.\mathsf{ap}(x,y) \vee \mathsf{ic}_i(x,y)$
   Prop. 49

3. $\Sigma_3 = \forall xyz.\mathsf{ap}(x,y) \wedge \mathsf{ap}(x,z) \rightarrow \mathsf{ap}(x, y \sqcup z)$
   Prop. 50

4. $\mathrm{Dim}(n-2) = \forall y_1 \ldots y_n.\exists z_1 \ldots z_n.(z_1 \rightarrow y_1) \wedge \ldots \wedge (z_n \rightarrow y_n) \wedge \sim(z_1 \wedge \ldots \wedge z_n) \wedge (y_1 \vee \ldots \vee y_n) \rightarrow (z_1 \vee \ldots \vee z_n)$
   Prop. 54.

Strong granularity axioms:

1. $\Lambda_1 = \exists x.(\Box\mathsf{atmcell}(x) \wedge x)$
   Prop. 35.

2. $\Lambda_2 = \forall x. \Diamond x \rightarrow \Box(x \leftrightarrow \exists y.y \wedge \Box\mathsf{cell}(y) \wedge \Box(y \rightarrow x))$
   Prop. 36.

Appendix B

Isabelle theories

B.1 Reflection embeddings

The following is the Isabelle-HOL theory for the logic $I2_r$ and for its extensions $C2_r$, $D2_r$:

```
D2r = Multiset +

(* recursive type of the formulae *)
datatype
      'a wff = "VAR" ('a)
             | "->"   ('a wff) ('a wff)  (infixr 25)
             | "Al2" "('a) => ('a wff)"  (binder "AL2 " 10)

(* declarations of constants *)

consts  (* declarations of the logical operators - with concrete syntax *)

  "Ex2"    ::  ('a => 'a wff) => 'a wff        (binder "EX2 " 10)
  "&&"     ::  ['a wff, 'a wff] => 'a wff      (infixr 35)
  "||"     ::  ['a wff, 'a wff] => 'a wff      (infixr 30)
  "No"     ::  'a wff => 'a wff                ("No _" [40] 40)
  "<-->"   ::  ['a wff, 'a wff] => 'a wff      (infixr 25)
  "false"  ::  'a wff
  "true"   ::  'a wff
```

```
  "NDIV"    ::  ['a wff , 'a wff] => 'a wff

(* other constants *)

  "|-"     ::  [('a wff) multiset, 'a wff] => bool    (infixl 5)
  "seqs"   :: "((('a wff) multiset) * ('a wff)) set"
  "TERM"   ::  'a wff => 'a
  "SUBST"  :: "'a wff => 'a wff => 'a => 'a wff"
  "==="    ::  [('a), ('a)] => 'a wff                 (infixl 40)

defs  (* definitions *)

   false_Def    "false == AL2 x. VAR(x)"
   true_Def     "true == false -> false"
   and_Def      "A && B == AL2 x. (A -> (B -> VAR(x))) -> VAR(x)"
   or_Def       "A || B == AL2 x. (A -> VAR(x)) -> (B -> VAR(x))
                                           -> VAR(x)"
   dimp_Def     "A <--> B == (A -> B) && (B -> A)"
   not_Def      "No A == A -> false"
   ex_Def       "Ex2 (A) == AL2 y. (AL2 x. A(x) -> VAR(y)) -> VAR(y)"
   ndiv_Def     "NDIV A B == (A -> ((No (No B)) || (No B))) -> ((A ->
                  (No (No B))) || (A -> (No B)))"
   eq_Def       "(a === b) == VAR(a) <--> VAR(b)"

(* primitive recursive definition *)
primrec
   "SUBST (VAR y) A x = (if y = x then VAR (TERM A) else VAR y)"
   "SUBST (B -> C) A x = (SUBST B A x -> SUBST C A x)"
   "SUBST (Al2 B) A x =  Al2 (%y. SUBST (B y) A x)"

translations   (* syntactic sugar *)

   "H |- A" == "(H, A) : seqs"

(* inductive definition of derivable sequent *)
```

```
inductive "seqs"
  intrs

(* standard rules for the implication-forall fragment of
   first-order intuitionistic logic *)

(* identity axiom *)
  GAx       "H + {#A#} |- A"

(* rule Weakening *)
  Weak      "H |- P  ==> H + K |- P"

(* rule Contraction *)
  Cont      "H + {#A#} + {#A#} |- B ==> H + {#A#} |- B"

(* rule Cut *)
  Cut       "[| H |- A;  H + {#A#} |- B |]  ==> H |- B"

(* implication right rule *)
  impR      "H + {#A#} |- B ==> H |- A->B"

(* implication left rule *)
  impL      "[| H + {#B#} |- C;  H |- A |]
                                       ==> H + {#A->B#} |- C"

(* forall right rule *)
  allR      "[| !!x::'a. H |- A(x) |] ==> H |- (AL2 x. A(x))"

(* forall left rule *)
  allL      "H + {#A(x)#} |- B ==> H + {#AL2 x. A(x)#} |- B"


(* rules for the extensions of 2Ir *)

(* rules for constant domains - logics 2Cr and 2Dr *)
  cdR       "H |- (AL2 x. A || B(x)) ==> H |- A || (AL2 x. B(x))"
```

```
(* rules for atomicity - logic 2Dr *)
  mhR        "H |- AL2 x. No No A(x) ==> H |- No No (AL2 x. A(x))"

(* rules for the reflexion operator *)

(* comprehension right rule *)
  compR      "H |- A ==> H |- VAR(TERM A)"

(* comprehension left rule *)
  compL      "H + {#A#} |- B ==> H + {#VAR(TERM A)#} |- B"


(* rules for explicit substitution *)
  indR  "H |- B (TERM A) ==> H |- SUBST (B y) A y"
  indL  "H + {#B (TERM A)#} |- C ==> H + {#SUBST (B y) A y#} |- C"

end
```

B.2 Comprehension embeddings

The following is the Isabelle-HOL theory for the logics $I2_c$, $C2_c$, $D2_c$:

```
D2c = Multiset +

datatype
      'a wff = "VAR" ('a)
             | false
             | "->"   ('a wff) ('a wff)  (infixr 25)
             | "&&"   ('a wff) ('a wff)  (infixr 30)
             | "||"   ('a wff) ('a wff)  (infixr 30)
             | "Al2" "('a) => ('a wff)"  (binder "AL2 " 10)
             | "Ex2" "('a) => ('a wff)"  (binder "EX2 " 10)

consts
  "|-"    ::  [('a wff) multiset, 'a wff] => bool   (infixl 5)
  "seqs"  :: "((('a wff) multiset) * ('a wff)) set"
  "SUBST" :: "'a wff => 'a => 'a => 'a wff"
  "==="   ::  [('a), ('a)] => 'a wff                (infixl 40)

(* logical operators *)
  "No"   :: 'a wff => 'a wff                  ("No _" [40] 40)
  "<-->" :: ['a wff, 'a wff] => 'a wff        (infixr 25)
  "true"  :: 'a wff

defs   (* logical operators *)

   true_Def    "true == false -> false"
   dimp_Def    "A <--> B == (A -> B) && (B -> A)"
   not_Def     "No A == A -> false"
   eq_Def      "(a === b) == VAR(a) <--> VAR(b)"

primrec
   "SUBST (VAR y) z x = (if y = x then (VAR z) else (VAR y))"
   "SUBST false y x = false"
```

```
   "SUBST (B -> C) y x = (SUBST B y x -> SUBST C y x)"
   "SUBST (A && B) y x = ((SUBST A y x) && (SUBST B y x))"
   "SUBST (A || B) y x = ((SUBST A y x) || (SUBST B y x))"
   "SUBST (Al2 B) z x =  Al2 (%y. SUBST (B y) z x)"
   "SUBST (Ex2 B) z x =  Ex2 (%y. SUBST (B y) z x)"

translations
   "H |- A" == "(H, A) : seqs"

inductive "seqs"
  intrs

(* standard rules for first-order intuitionistic logic *)
  GAx      "H + {#A#} |- A"

  Weak     "H |- P  ==> H + K |- P"

  Cont     "H + {#A#} + {#A#} |- B ==> H + {#A#} |- B"

  Cut      "[| H |- A;  H + {#A#} |- B |]  ==> H |- B"

  impR     "H + {#A#} |- B ==> H |- A->B"

  impL     "[| H + {#B#} |- C;  H |- A |]
                                      ==> H + {#A->B#} |- C"

  allR     "[| !!(x::'a). H |- A(x) |] ==> H |- (AL2 x. A(x))"

  allL     "H + {#A(x)#} |- B ==> H + {#AL2 x. A(x)#} |- B"

(* existential right rule *)
  exR      "H |- A(x) ==> H |- EX2 x. A(x)"

(* existential left rule *)
  exL  "[| !!(x::'a). H + {#A(x)#} |- B |] ==>
                              H + {#EX2 x. A(x)#} |- B"
```

```
(* and right rule *)
  andR     "[| H |- A; H |- B |] ==> H |- A && B"

(* and left rule *)
  andL     "H + {#A#} + {#B#} |- C ==> H + {#A && B#} |- C"

(* or right rule 1 *)
  orR1     "H |- A ==> H |- A || B"

(* or right rule 2 *)
  orR2     "H |- B ==> H |- A || B"

(* or left rule *)
  orL    "[| H + {#A#} |- C; H + {#B#} |- C |] ==>
                                  H + {#A || B#} |- C"

(* false elimination rule *)
  ex_falso  "H |- false ==> H |- A"

(* rules for the extensions of 2Ic - 2Cc and 2Dc *)

  cdR   "H |- (AL2 x. A || B(x)) ==> H |- A || (AL2 x. B(x))"
  mhR   "H |- AL2 x. No No A(x) ==> H |- No No (AL2 x. A(x))"

(* Full comprehension axiom for VAR *)

  varA         "H |- EX2 x. A <--> VAR(x)"

(* rules for explicit substitution *)

  indR      "H |- (B x) ==> H |- SUBST (B y) x y"
  indL      "H + {#B x#} |- C ==> H + {#SUBST (B y) x y#} |- C"

end
```

B.3 Meta-Logic formalisation

The following Isabelle theory contains the Meta-Logic formalisation of the logic $I2_m$:

```
I2m = CPure +

global
types  o
arities  o :: logic

consts
  Trueprop       :: "o => prop"               ("(_)" 5)
  True           :: o
  False          :: o

  (* Operators *)
  "-->"            :: "[o, o] => o"              (infixr 10)
  Not            :: "o => o"                   ("~ _" [40] 40)
  "&"              :: "[o, o] => o"              (infixr 35)
  "|"            :: "[o, o] => o"              (infixr 30)
  "<->"            :: "[o, o] => o"              (infixr 25)

  (* Quantifiers *)
  All            :: "(o => o) => o"            (binder "ALL " 10)
  Ex             :: "(o => o) => o"            (binder "EX " 10)

  (* new axioms - natural deudction rules for I2m *)
rules

  impI         "(P ==> Q) ==> (P-->Q)"
  mp           "[| P-->Q;  P |] ==> Q"
  allI         "(!!x. P(x)) ==> (ALL x. P(x))"
  spec         "(ALL x. P(x)) ==> P(x)"
  exI          "P(x) ==> (EX x. P(x))"
  exE          "[| EX x. P(x);  !!x. P(x) ==> R |] ==> R"
```

```
  (* definitions *)
defs

  False_def     "False  == ALL x. x"
  True_def      "True  == False-->False"
  not_def       "~ P == P-->False"
  and_def       "P&Q  == ALL x. (P-->(Q-->x))-->x"
  or_def        "P|Q  == ALL x. (P-->x)-->(Q-->x)-->x"
  iff_def       "P<->Q == (P-->Q) & (Q-->P)"

end
```