

MODAL STRUCTURES IN GROUPS AND VECTOR SPACES

JOHAN VAN BENTHEM AND NICK BEZHANISHVILI

ABSTRACT. Vector spaces show a number of general structures that invite analysis in modal logics. As such, they provide an interesting counterpart to the much better-studied modal logics of topology. At the same time, vector spaces pose several challenges to this style of analysis of a mathematical practice. In this programmatic paper, we present a number of modal logics of groups and then full-fledged vector spaces, including some new logics of dependence and independence. In particular, we investigate issues of definability and axiomatization using standard techniques for modal and hybrid languages. Our discussion identifies several leads for more systematic research.

1. INTRODUCTION

Vector spaces and techniques from linear algebra are ubiquitous in applied mathematics, and they are finding ever new application in areas such as cognitive science [24], machine learning [15], computational linguistics [26], social sciences [5, 38]. Finally, an intriguing philosophical application is found in [36], inspired by a new perspective on belief revision. There has been some logical work on vector spaces, in the first-order tradition [32, 43], in relevant logic [45], and in modal logics of space [12]. Even so, much more can be done, and this paper offers a first further analysis from a modal logic perspective, identifying fruitful points of contact, while not hiding obstacles and mismatches. As it happens, the connection between logic and linear algebra can be pursued in two ways, both present in the literature. Vector spaces have been used as a source of illuminating semantic models for existing independently motivated modal languages and axiom systems. But conversely, one can also put the focus on vector spaces themselves, asking what linear algebra can be captured in which modal languages and logics. The latter approach will be our main interest in what follows, though the two directions are of course not incompatible.

For a start, here are the structures that this paper is about.

Definition 1.1. *A vector space over a field F is a set V with operations $+$: $V^2 \rightarrow V$ of vector addition and a scalar multiplication \cdot : $F \times V \rightarrow V$ such that for each $u, v, w \in V$ and $a, b, c \in F$:*

- (1) $u + (v + w) = (u + v) + w$
- (2) $u + v = v + u$
- (3) *there exists a ‘zero vector’ $0 \in V$ such that $v + 0 = v$ for all $v \in V$*
- (4) *for every $v \in V$, there is an ‘additive inverse’ $-v \in V$ such that $v + (-v) = 0$*
- (5) $a \cdot (b \cdot v) = (a \cdot b) \cdot v$
- (6) *there exists a ‘multiplicative unit’ $1 \in F$ such that $1 \cdot v = v$ for all $v \in V$*
- (7) $a \cdot (u + v) = a \cdot u + a \cdot v$
- (8) $(a + b) \cdot v = a \cdot v + b \cdot v$

Vector spaces derive their interest from their uses in an extensive mathematical theory, viz. Linear Algebra [30], whose basic notions and results set a target for logical analysis.

Our modal investigation will approach all this structure step by step. In a first part, we merely consider the group structure of vector addition, introducing modal languages and an appropriate notion of bisimulation in Section 2 to study definability of various natural spatial notions such as the Minkowski operations. In Section 3 we then consider complete axiomatizations using techniques

from hybrid logic. Finally, in Section 4 we introduce a new logic of linear closure in groups in terms of neighborhood semantics and show its completeness. Next, we move on to the richer structure of vector spaces. In a second part, our focus moves to the additional structure of the field coefficients for vectors, studied at the basic level of dependence and independence. In Section 5, we present a new modal logic for dependence which takes on board the crucial principle of Steinitz Exchange, and we bring out connections with an alternative approach taking independence as a primitive, including connections with Matroid Theory. We also clarify some interesting analogies and differences with current dependence logics. Finally, the third part of this paper offers explicit modal logics for field structure in Section 6, while Section 7 explores further ways in which modal logics can bring out crucial structures inside and in between vector spaces, such as the use of linear transformations and matrices. These are the main lines: the paper also has further points and observations that will appear along the way. Our concluding Section 8 summarizes our intention: not one of providing an alternative syntax for writing up what works perfectly well in Linear Algebra, or for redoing the foundational insights already obtained using first-order formalisms in model theory, but one of providing a ‘second opinion’ in modal frameworks. We believe that our results show the potential of an abstract modal style of thinking about vector spaces, which suggests new analogies and lines to pursue, and we illustrate this with a few concrete examples.

Related Work. Our approach is indebted to several existing lines of logical work. We will mention as they arise in our presentation, such as the semantics of relevant logic [45], categorial logic [14], complex algebra [33, 29], or dependence logics [46, 6]. In particular, the “Handbook of Spatial Logics” [1] contains a number of chapters on modal theories of space that are congenial to the present study, in particular, [12] on modal logics for topology (with an excursion to vector spaces and their ‘arrow logic’), and [4] on modal logics for geometries. A recent relevant interface is the use of substructural categorial logics with vector space semantics in bringing to light logical structures in distributional semantics for linguistic corpora [37, 44]. A yet more recent approach is that of [36], which encodes the axioms of vector spaces in a non-classical propositional logic with names for real numbers, and then goes on to explore many further structures in linear algebra, such as inner products. Leitgeb’s logic is decidable through an embedding in Tarski’s decidable first-order theory of the reals with addition and multiplication. This connection with classical first-order model theory is not a coincidence, and vector spaces have also been studied in several formats in that area, e.g., [32, 43].

2. A MODAL LOGIC FOR GROUP STRUCTURE

For convenience, we recall the definition of a group.

Definition 2.1. A group is a structure $(G, +, -, 0)$ where $+$ is a binary operation on G and $-$ is a unary operation on G and $0 \in G$ is a constant (0 -ary operation) such that for all $a, b, c \in G$:

- (1) $a + (b + c) = (a + b) + c$;
- (2) $a + 0 = 0 + a = a$;
- (3) $a + (-a) = (-a) + a = 0$.

A group G is commutative if for each $a, b \in G$: $a + b = b + a$.

2.1. Language and semantics. Our main tool is a modal language for arbitrary groups, but in keeping with our main theme, the examples we have in mind come from vector spaces.

Definition 2.2. Let Prop be the set of propositional variables, Nom the set of nominals and 0 a hybrid constant. The modal group language MGL is generated by the following grammar:

$$\varphi := \perp \mid p \mid i \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathbf{E}\varphi \mid \langle - \rangle\varphi \mid \langle + \rangle(\varphi, \varphi) \mid 0,$$

where $p \in \text{Prop}$, $i \in \text{Nom}$. We will also employ defined modalities $\mathbf{U}\varphi = \neg\mathbf{E}\neg\varphi$ and $[+](\varphi, \varphi) = \neg\langle + \rangle(\neg\varphi, \neg\varphi)$. Henceforth, $\varphi \oplus \psi$ will be shorthand for $\langle + \rangle(\varphi, \psi)$ for ease in reading formulas.

A *word of explanation*. A ‘pure’ modal language for groups would just use proposition letters and our modalities, where formulas denote sets of objects, in line with algebraic logic approaches, [47]. The additional nominals allow us to also talk about single objects, using tools of hybrid logic, [3], which sits in between modal logic and first-order logic. Our reasons for choosing this formalism are two-fold: it seems needed for some of the results that we wish to have, but also: it fits with practice in linear algebra, where basic arguments involve reference to specific vectors.

Definition 2.3. A group model is a tuple $(S, +, V)$, with a commutative group $(S, +, -, 0)$ and a valuation map $V : \text{Prop} \cup \text{Nom} \rightarrow \mathcal{P}(S)$ s.t. $|V(i)| = 1$ and $V(0) = \{0\}$ is the unit of the group.

We use the standard relational semantics on group models, with a well-known clause for binary modalities, [16]. Formulas φ of our language describe properties of group elements (vectors, in our special case of interest) according to the following truth definition:

Definition 2.4. Let $\mathfrak{M} = (S, +, V)$ be a group model, $s \in S$:

$$\begin{aligned}
 \mathfrak{M}, s &\models \perp && \text{never} \\
 \mathfrak{M}, s &\models i && \text{iff } s \in V(i) \\
 \mathfrak{M}, s &\models p && \text{iff } s \in V(p) \\
 \mathfrak{M}, s &\models \varphi \vee \psi && \text{iff } \mathfrak{M}, s \models \varphi \text{ or } \mathfrak{M}, s \models \psi \\
 \mathfrak{M}, s &\models \neg \varphi && \text{iff not } \mathfrak{M}, s \models \varphi \\
 \mathfrak{M}, s &\models E\varphi && \text{iff } \mathfrak{M}, t \models \varphi, \text{ for some } t \in G \\
 \mathfrak{M}, s &\models 0 && \text{iff } s \in V(0) \\
 \mathfrak{M}, s &\models \varphi \oplus \psi && \text{iff } \exists s_1, s_2 \text{ s.t. } \mathfrak{M}, s_1 \models \varphi, \mathfrak{M}, s_2 \models \psi \text{ and } s = s_1 + s_2 \\
 \mathfrak{M}, s &\models \langle - \rangle \varphi && \text{iff } \mathfrak{M}, -s \models \varphi
 \end{aligned}$$

The meaning of our defined modalities follows from these explanations. For instance, $[+](\varphi, \psi)$ says at point s that for each pair t, u with $s = t + u$, either $t \models \varphi$ or $u \models \psi$.

Remark 2.5 (Binary operations). In standard unary modal languages, a modality $\langle f \rangle \varphi$ for a function is true at a point s if the function value $f(s)$ makes φ true. However, this does not lift to binary operations, and the above truth condition for \oplus works in the *reverse* direction: the current s stands for the function value, and the ‘ternary successors’ s_1, s_2 for two arguments. We could have taken the same reverse line for the inverse modality $\langle - \rangle \varphi$, but we have followed standard practice there as the difference does not matter, given the idempotence of the inverse operation in groups.

We say that a subset of a group model \mathfrak{M} is *definable* if it is the denotation of some formula. Here are some illustrations of what our language can define concretely. Note the difference in flavor with standard examples in modal relational semantics.

Example 2.6 (Finding the definable sets). (a) Consider the group model based on the integers $(\mathbb{Z}, +, -, 0)$ with $V(p) = \{1\}$, and no nominals interpreted. Each set $\{z\}$ for a positive integer z is definable, by ‘summing’ p z times. Moreover, using the modality $-$, all singletons $\{-z\}$ are definable. Using disjunctions and negation, then, every finite and every cofinite subset of \mathbb{Z} is definable. The crucial final observation is that we get no more definable sets, since this collection is closed under the operations $0, -, +$ defined above and hence forms the subalgebra of the powerset generated by $V(p)$. For instance, it is easy to see that the set of all sums of numbers from two cofinite sets is itself cofinite, and so on. (b) A similar analysis works for the two-dimensional model $(\mathbb{Z} \times \mathbb{Z}, +, -, 0)$ with the valuation $V(p) = \{(0, 1)\}, V(q) = \{(1, 0)\}$. (c) However, if our initial denotations have some special invariance properties, then these may constrain what is definable. For an illustration, assume now that $V(p) = \{(0, 1), (1, 0)\}$. We can define all finite and cofinite sets that are *reflective* in the sense of being closed under the map sending points (x, y) to their reflections (y, x) along the diagonal $x = y$. The key here is an inductive proof that all modally definable sets

are reflective as this property is preserved under our operations.¹ (d) Similar illustrations work just as well for dense spaces like \mathbb{Q} or $\mathbb{Q} \times \mathbb{Q}$, and examples will be found below.

2.2. Definable notions and links to other logics. In addition to definability in specific models, there is generic definability across models. Our language contains many notions of interest.

Global modalities. Here is a first natural connection between group structure and modal logic. The global existence modality of our language can in fact be defined in group models \mathfrak{M} .

Fact 2.7. $E\varphi \leftrightarrow \varphi \oplus \top$ is valid in group models.

Proof. First let $s \models \varphi \oplus \top$. Then there are points v, u s.t. $w = v + u$ and $v \models \varphi$. In particular, there is a point where φ is true, and so $E\varphi$ is true at s . Conversely, let $s \models E\varphi$. Then φ is true at some point t , and we use the fact that in any group: $s = t + (-t + s)$ to see that $s \models \varphi \oplus \top$. \square

Even so, we will keep the global modalities in our language as they make principles easier to grasp, and rewriting them according to the preceding equivalence leads to obscure formulations.

Minkowski operations. Our second illustration is from the area of Mathematical Morphology [17], where the following two operations are used to describe shapes and operations on shapes in vector spaces for image processing. However, the notions involved are quite general.

Definition 2.8. The Minkowski operations on subsets of groups are addition $A + B = \{x + y \mid x \in A \text{ and } y \in B\}$ and subtraction $A - B = \{x \mid \text{for all } y \in B : x + y \in A\}$.

Obviously, the corresponding modal operator for Minkowski addition is our vector sum modality. But Minkowski subtraction is definable just as well.

Fact 2.9. Minkowski subtraction $A - B$ is definable by the modal formula $\neg(\langle - \rangle B \oplus \neg A)$.

Proof. Applied to a group element s the modal formula says that s cannot be written as a sum of a $t \in \neg A$ and $-u$ with $u \in B$. But transforming this sum $s = t + -u$ into the equivalent form $t = s + u$, the condition says that, if we add any B -point to s , the result must be in A . \square

Versatile modal logic. The key to the preceding fact is that a decomposition of a vector s into two vectors $s = t + u$ can be described equivalently in terms of decomposing the vectors t or u .

Remark 2.10. The preceding feature makes our modal language *versatile* in the sense of [41]. If we think of the ternary decomposition relation $Rxyz$ as interpreting the modality $\langle + \rangle$, then the binary modalities for its two associated relations

$$R'yxz := Ryxz, \quad R''zxy := Rxyz$$

are definable in our language. In particular, our modal language for groups supports shifts in perspective when describing ternary spatial patterns involving vector addition.

Substructural implication. From another perspective, Minkowski subtraction $A - B$ behaves like a logical *implication* $B \Rightarrow A$ that distinguishes different occurrences of the same formula, [2]. Typically, in our models, $\varphi \Rightarrow \psi$ is not equivalent with $\varphi \Rightarrow (\varphi \Rightarrow \psi)$. This is like the implication of relevant or categorial logic, and indeed, vector space models were introduced early on in [45] for modeling relevant implication. In its barest form, its occurrence-based character makes Minkowski subtraction a substructural implication in the categorial *commutative Lambek Calculus*, [35, 8], with Minkowski sum as the product conjunction.

For details of all this, the reader may consult the Handbook chapter [12], which also presents links with *Arrow Logic*, an abstract modal logic of arrows or ‘transitions’ which generalizes relational algebra and logics of graphs and vectors. We summarize the preceding as follows.

¹E.g., closure for sums is shown as follows. Let $(x_1, y_1) \in A, (x_2, y_2) \in B$ and consider $(x_1 + x_2, y_1 + y_2) \in A \oplus B$. Reflecting this gives $(y_1 + y_2, x_1 + x_2) = (y_1, x_1) + (y_2, x_2)$: a sum of two reflections which are in A, B by assumption.

Fact 2.11. *On group models, our modal language defines the Minkowski operations, versatile composition modalities, the operations of the commutative Lambek Calculus and basic Arrow Logic.*

Thus, the modal base logic of additive groups sits at a crossroads of themes in logic.²

2.3. Bisimulations and p -morphisms. As is common in modal logics, definability can be analyzed in terms of a structural invariance, which in the present case can be seen as a more permissive form of the basic invariance under linear transformations in Linear Algebra.

Definition 2.12. (*Bisimulation*) *Let $\mathfrak{M} = (G, +, -, 0, V)$, $\mathfrak{M}' = (G', +', -', 0', V')$ be group models. A binary relation $Z \subseteq G \times G'$ is a bisimulation if for every $w \in G$ and $w' \in G'$ with wZw' :*

- (1) $w \in V(p)$ iff $w' \in V'(p)$, $p \in \text{Prop}$
- (2) $w \in V(i)$ iff $w' \in V'(i)$, $i \in \text{Nom}$, and also $0Z0'$
- (3) $w = u + v$ implies there are $u', v' \in G'$ such that uZu' , vZv' and $w' = u' + v'$
- (4) $w' = u' + v'$ implies there are $u, v \in G$ such that uZu' , vZv' and $w = u + v$
- (5) $-wZ -' w'$
- (6) $\forall v \exists v'$ such that vZv' and $\forall v' \exists v$ such that vZv' .

We say that w and w' are bismilar if they are linked by some bisimulation.

Remark 2.13. The crucial back-and-forth clauses in this notion are just a special case of general modal bisimulations on models with a ternary accessibility relation, [16]. They would also work if we view $s = t + u$ as an abstract ternary relation Rs, tu that need not be functional. In what follows, we will also refer to this second more abstract version. While both of these versions are straightforward, some concrete instances in groups or vector spaces are worth displaying.

Example 2.14 (A finite bisimulation contraction). Instead of the earlier examples with integers, we now consider the dense order \mathbb{Q} of the rationals. Consider the model $\mathfrak{M} = (\mathbb{Q} \times \mathbb{Q}, +, -, 0)$ with $V(p) = \{(a, b) \in \mathbb{Q} \times \mathbb{Q} : a, b \geq 0\}$. It is easy to see, by the preceding definition and the symmetry in this model w.r.t. the diagonal, that two points (a, b) and (a', b') are bisimilar in this model if

- $a = b = a' = b' = 0$, the equivalence class A ,
- $a, b, a', b' \geq 0$ and $(a, b) \neq (0, 0) \neq (a', b')$, the equivalence class B ,
- $a, b, a', b' \leq 0$ and $(a, b) \neq (0, 0) \neq (a', b')$, the equivalence class C ,
- $a < 0, b > 0$ or $a > 0, b < 0$, otherwise, the equivalence class D .

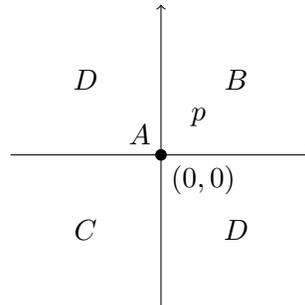


FIGURE 1. $\mathbb{Q} \times \mathbb{Q}$ and its bisimulation classes

²We will discuss later whether the above definitions also faithfully embed the relevant logical systems.

Contracting these four regions to single points, we obtain the *bisimulation contraction* of the preceding model, with a ternary relation Rs, tu for the binary modality which holds when there exist $x = y + z$ in the model \mathfrak{M} where x gets mapped to s , y to t and z to u . This is enough to guarantee the required back-and-forth clauses. We just list some of the most informative triples in this relation: $R(A, C, B)$, $R(A, D, D)$, $R(D, D, D)$, $R(D, C, D)$, $R(D, B, D)$, $R(D, B, C)$, $R(C, C, D)$, $R(C, C, A)$, $R(C, D, A)$, and similarly for ternary decompositions of A . Typically, we do *not* have: $R(A, B, B)$, $R(A, C, C)$, $R(A, B, D)$, $R(D, A, B)$, and likewise, the other regions lack some decompositions.

Note that the contraction is no longer a group model, since the preceding ternary relation is not the graph of a function $+$: e.g., D, D produce both A and D .

What we see here is the abstraction of a modal perspective. Vector models can be bisimilar to, sometimes much simpler, abstract models that contain the same modal information but that are no longer inside the usual realm of Linear Algebra. One can see this as a drawback, or as a virtue of abstraction: giving us new structures that highlight basic content of a modal nature.

Note also that bisimulation as defined here does not just preserve structure of a group or vector space: it also preserves what may be called *patterns* of atomic propositions in these groups or spaces. These patterns are usually essential in applications: e.g., ‘shapes’ in Mathematical Morphology⁷ are named subsets of vector spaces. However, modal logic can also focus on the pure underlying structure, characterizing properties that only refer to the group or vector structure.³ Our next example illustrates the difference, and leads up to some further notions.

Example 2.15 (Invariance and nondefinability of dimension). This time, we consider a bisimulation between two group models, viz. $(\mathbb{Q} \times \mathbb{Q}, +, -, 0)$ and $(\mathbb{Q}, +, -, 0)$, where the valuation is ignored. The projection map sending (x, y) to $(x, 0)$ is a bisimulation in the above sense. Going from $(\mathbb{Q} \times \mathbb{Q}, +, -, 0)$ to $(\mathbb{Q}, +, -, 0)$, the ‘forth’ clause is obvious from the definition of the projection map. In the opposite direction, for the ‘back’ clause, let $(x, 0) = (x_1, 0) + (x_2, 0)$. Then there clearly exist $(x_1, y_1), (x_2, y_2)$ such that $(x_1, y_1) + (x_2, y_2) = (x, y)$, and the projections of these two vectors are $(x_1, 0), (x_2, 0)$ as required. In a sense to be made precise now, this example shows in particular that the notion of *dimension* is not definable in our modal language.

Dimension is not a ‘pattern property’ in the above sense, but a structural property of vector spaces. In that case, another well-known notion of definability from modal logic makes sense. Let us call a formula φ true in a *frame*, that is, a model without a valuation function, if φ is true at all points under all valuations. This second-order notion differs in significant ways from truth on models, cf. the textbook [16]. Now we can ask whether dimension is frame-definable, something left open by its undefinability on models.⁴ But the preceding example also refutes frame-definability. The reason is that the projection map is a function of the following sort.

Definition 2.16. A map f between group models is a p -morphism if

- (1) $f(v + v') = f(v) + f(v')$ and $f(-v) = -f(v)$
- (2) If $f(v) = v'_1 + v'_2$ then there are v_1, v_2 with $v = v_1 + v_2$, $f(v_1) = v'_1$ and $f(v_2) = v'_2$.⁵

Modal p -morphisms look close to the familiar mathematical notion of a group homomorphism. In fact, on group models, they are just the surjective homomorphisms.

Fact 2.17. Given Condition (1), Condition (2) for a p -morphism is equivalent to surjectivity of f .

³What follows reflects the two sides of semantic analysis in standard modal logic, where bisimulation compares annotated graphs and first-order truth in *models*, but modal frame correspondence concentrates on capturing pure properties of accessibility relations in terms of second-order truth in *frames*.

⁴For a standard modal analogue, compare the undefinability of *functionality* for an accessibility relation on models: we can duplicate function values modulo bisimulation, with the frame definability by the formula $\diamond \top \wedge (\diamond p \rightarrow \Box p)$.

⁵We leave out some clauses for dealing with nominals that are not relevant here.

Proof. (a) Let f satisfy Condition (2). For any y in the codomain, we can write $f(x) = y + (f(x) - y)$. Therefore, there is a v such that $f(v) = y$. (b) Conversely, if $f(x) = y + z$, then, by surjectivity, choose y', z' s.t. $f(y') = y$ and $f(z') = z$. Now, $x = y' + (z' + (x - y' - z'))$, and by (1) it follows that $f(z' + (x - y' - z')) = z + (fx - y - z) = z + 0 = z$. \square

2.4. Invariance and definability. Here is how the notions of invariance introduced here relate to the expressive power of our modal language. The proofs of the following facts use well-known standard arguments from modal logic, [16, Sec. 2.2].

Fact 2.18. *Bisimilar points in two models satisfy the same modal formulas.*

Fact 2.19. *Let $f : G \rightarrow G'$ be a p -morphism from a group G_1 onto group G_2 . Then every modal formula true in the frame G_1 is also true in the frame G_2 .*

The latter fact was our reason for saying that dimension cannot even be frame-defined on groups.⁶

Remark 2.20 (Further bisimulation topics.). There are also known converse results to the preceding facts. One that is easy to prove by general modal techniques, (see, e.g., [16, Sec. 2.2]), is this. For any two points w, v in two *finite* models that satisfy the same modal formulas, there exists a bisimulation between the models connecting w to v . There are much stronger results of this sort in standard modal logic, but instead of pursuing these, we point at a feature of groups that might lead to new results without counterparts in standard modal logic. Suppose we have sets of generators G_1, G_2 for the groups in two group models $\mathfrak{M}_1, \mathfrak{M}_2$, and a total relation Z between G_1, G_2 . Is there an automatic extension to a bisimulation on the whole models? To illustrate this, consider $\mathbb{Z}_3 = \{0, 1, 2\}$ and $\mathbb{Z}_5 = \{0', 1', 2', 3', 4'\}$. For a start, we must have a match $0Z0'$, where this link for a nominal is unique. Let $Z = \{(0, 0'), (1, 1')\}$. We now follow the clauses for a bisimulation to place further links as required. First, since $1Z1'$ and $1 = 2 + 2$ and $1' = 3' + 3'$ we must have $2Z2'$ [there are no other ways of writing $1'$ as a sum $x + x$.] Now using the clause for inverses, we must also put $2, 4', 1, 2'$. However, this is not a bisimulation yet. Consider the link $1, 1'$ and the fact that $1' = 2' + 4'$. To witness this in \mathbb{Z}_3 , the only candidate is $1 = 2 + 2$, and therefore, we must put $2, 2'$. Continuing in the way, we see that the smallest bisimulation between our models has all links between non-unit elements.⁷ The procedure in this example can be turned into an algorithm for a bisimulation extension of a given relation between generators whose detail we omit here.

Our final topic is a digression on the role of the chosen modal language in our definability results. The following assertion is easy to prove.

Fact 2.21. *Functionality of the group operation $+$ is defined on frames by the modal formula $((n \wedge \mathbf{E}m) \rightarrow \mathbf{E}(m \oplus n)) \wedge (\mathbf{E}(n \wedge m \oplus k) \rightarrow \mathbf{U}(m \oplus k \rightarrow n))$.*

Note that this formula uses nominals, and in truth on frames, we quantify over all possible objects as denotations for these. The role of nominals is essential here, and this was one of our reasons for including them in our language from the start. The next fact already follows from Example 2.14. However, we find the new example in the proof informative about the more abstract models that our language supports.

Fact 2.22. *Functionality of $+$ is not expressible in the modal language without nominals.*

Proof. Let \mathbb{N} and \mathbb{N}' be two isomorphic copies of the natural numbers. Let $\mathfrak{M} = \mathbb{N} \cup \mathbb{N}' \cup \{\alpha\}$. We define a binary function $+$ by setting

$$x + y = \begin{cases} n', & \text{if } x = n \text{ and } y = n + 1, \\ \alpha, & \text{otherwise.} \end{cases}$$

⁶The surjectivity of p -morphisms relates to the earlier fact that the universal modality is definable in group models.

⁷We leave the matter of finding more interesting bisimulation extensions to the reader.

We also set $0 = \alpha$ and $-x = x$ for each $x \in X$. In the figure for this model included below, if $x = y + z$, then we draw lines from y and z to x .

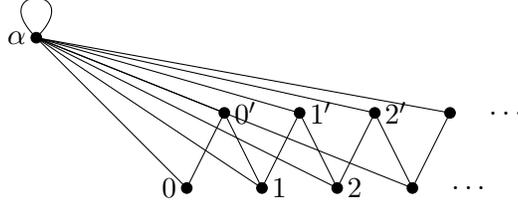


FIGURE 2. The model \mathfrak{M}

Next we define a model $\mathfrak{N} = \{a, b, c, d, \beta\}$. We let R be a ternary relation on Y such that $R = \{(a, c, d), (b, c, d)\} \cup \{(\beta, x, y) : x, y \in Y\}$. We also set $0 = \beta$ and $-y = y$ for each $y \in Y$. Again see the figure below for a concrete depiction of this model.

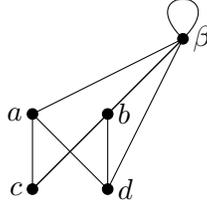


FIGURE 3. The model \mathfrak{N}

Next, we define a map $f : \mathfrak{M} \rightarrow \mathfrak{N}$ by setting

$$f(x) = \begin{cases} c, & \text{if } x \in \mathbb{N} \text{ is odd,} \\ d, & \text{if } x \in \mathbb{N} \text{ is even,} \\ a, & \text{if } x \in \mathbb{N}' \text{ is odd,} \\ b, & \text{if } x \in \mathbb{N}' \text{ is even,} \\ \beta, & \text{otherwise} \end{cases}$$

It is easy to check that f is a p -morphism for our modal language (but note the absence of nominals except for the name of the zero vector). Now the model \mathfrak{M} is functional for $+$ while R is not a functional relation on \mathfrak{N} . If functionality of ternary relations were modally definable then, as p -morphisms preserve frame truth of formulas, we would have a contradiction. \square

3. MODAL VALIDITIES, AXIOM SYSTEM AND COMPLETENESS

Our next topic is determining the valid principles of reasoning in our formalism. What the modal language with nominals captures in thinking about groups is reasoning of two kinds: about objects (group elements, vectors) and sets of objects (which stand for the earlier-mentioned ‘patterns’). Accordingly, our proof system will have two components: (a) purely modal principles expressing basic reasoning about sets, and (b) hybrid logic principles allowing us to use nominals as names

of specific objects, like individual constants in first-order logic, and then formalize the simple equational-style first-order arguments we have employed before. One can see this as serving two purposes: in reasoning about objects, we stay close to mathematical practice in Linear Algebra, but in adding the modal set principles, we extend the scope of the patterns that we can describe and identify interesting laws that are not specific to objects.

We will describe this system of validities in several steps. First we present a proof system that mixes principles that use nominals and principles in a standard modal format. We illustrate how this system works, and what can be derived. Next we prove completeness, based on known results in hybrid logic, noting that an even more austere (though somewhat less informative) nominal version would also be complete. Next, we return to the presence of more general modal laws in the system and how these can be made explicit. This connects to the field of ‘Complex Algebra’, as will be explained in the text. The outcome will be an interesting balance between reasoning about points and about sets, and we end with some discussion of further issues and open problems.⁸

3.1. A proof system.

Definition 3.1. *The Modal Logic of Commutative Groups LCG has the following axioms:*

- (1) *All tautologies of classical propositional logic*
- (2) $(\varphi \vee \psi) \oplus \chi \leftrightarrow (\varphi \oplus \chi) \vee (\psi \oplus \chi)$
- (3) $\langle - \rangle(\varphi \vee \psi) \leftrightarrow \langle - \rangle\varphi \vee \langle - \rangle\psi$
- (4) $\varphi \rightarrow E\varphi$
- (5) $EE\varphi \rightarrow E\varphi$
- (6) $\varphi \rightarrow UE\varphi$
- (7) $\varphi \oplus \psi \rightarrow E\varphi$
- (8) $\langle - \rangle\varphi \rightarrow E\varphi$
- (9) Ei ⁹
- (10) $E(\varphi \wedge i) \rightarrow U(i \rightarrow \varphi)$
- (11) $\langle - \rangle\neg\varphi \leftrightarrow \neg\langle - \rangle\varphi$
- (12) $(\varphi \wedge E\psi) \rightarrow E(\varphi \oplus \psi)$
- (13) $(\varphi \wedge m \oplus n) \rightarrow U(m \oplus n \rightarrow \varphi)$
- (14) $\varphi \oplus (\psi \oplus \chi) \leftrightarrow (\varphi \oplus \psi) \oplus \chi$
- (15) $\varphi \oplus \psi \leftrightarrow \psi \oplus \varphi$
- (16) $\varphi \oplus 0 \leftrightarrow \varphi$
- (17) $i \oplus \langle - \rangle i \leftrightarrow 0$

The rules of inference for LCG are

Modus Ponens, Replacement of Provable Equivalentents, and Substitution in the following form: arbitrary formulas can be substituted for formula variables φ , while for nominals, we can only substitute nominal terms formed from nominals using the functional modalities $\langle - \rangle$, \oplus .

Moreover, we have the following rules governing (and entangling) nominals and modalities:

⁸Much of what we find in this section is not confined to just groups, but we will not pursue generalizations.

⁹Here and in the principles below, i ranges over all nominals in our language.

Necessitation Rules: $\frac{\neg\varphi, \neg\psi}{\vdash \neg(\varphi \oplus \psi)}, \frac{\neg\varphi}{\neg(-)\varphi}, \frac{\neg\varphi}{\neg E\varphi}$

Naming Rule: $\frac{j \rightarrow \theta}{\theta}$ and

Witness Rules: $\frac{E(j \wedge \varphi) \rightarrow \theta}{E\varphi \rightarrow \theta}, \frac{\langle - \rangle(j \wedge \varphi) \rightarrow \theta}{\langle - \rangle\varphi \rightarrow \theta}, \frac{(j \oplus k \wedge E(j \wedge \varphi) \wedge E(k \wedge \psi)) \rightarrow \theta}{(\varphi \oplus \psi) \rightarrow \theta}$.

In the Naming and Witness rules, j, k are nominals distinct from i that do not occur in φ, ψ or θ .

The first axioms in this system are standard for normal existential modalities, next comes the basic hybrid machinery with global modalities and nominals, then principles fixing the functional structure for inverse and addition, and finally some specific axioms that essentially transcribe the definition of commutative groups. The derivation rules are standard, and they allow us, in particular, to carry out elementary equational reasoning about groups.¹⁰ Moreover, the very powerful Naming and Witness rules allow us to reason with nominals in the style of individual constants in first-order logic, and through their analysis of our existential modalities, lift nominal principles to general modal ones.¹¹ All this will become clearer with the examples to follow.

With these explanations in place, here is a soundness result.

Theorem 3.2. *All theorems of the system LCG are valid on group models.*

Proof. The preceding explanations should largely suffice. For instance, Axiom (12) says that if we have φ true at any point x and ψ at a point y , then there exists a point, namely $x + y$ where $\varphi \oplus \psi$ is true. In fact, this axiom enforces precisely that addition is defined on any two points. In addition, Axiom (13) then says that these function values are unique. As another example, the Witness Rule for the \oplus modality, read contrapositively, says the following. If we have $@_i(\varphi \oplus \psi) \wedge \neg\theta$ true at any point x in any model, we can add fresh names for a witnessing pair y, z s.t. $x = y + z, y \models \varphi, z \models \psi$ and make the antecedent of the premise conditional true, while keeping θ false. This mirrors exactly how introducing witnesses for existential quantifiers works in proof systems for first-order logic. \square

Remark 3.3. Given the earlier-mentioned Sahlqvist form of all our axioms, it is also easy to run a standard *frame correspondence* argument, and show that truth in a frame of the above principles taken together forces the frames underlying our models to be commutative groups.

More concrete information about the system LCG requires a look at a few formal derivations.

Example 3.4. The formula $i \rightarrow (E(i \wedge \varphi) \leftrightarrow \varphi)$ is provable. First, $i \wedge \varphi$ implies $E(i \wedge \varphi)$ by Axiom (4). Vice versa, $E(i \wedge \varphi)$ implies $U(i \rightarrow \varphi)$ by Axiom (10), and together with i , this implies φ .

Example 3.5 (Surjectivity of addition). The formula $\top \oplus \top$ says that each point is a sum of two points. This is provable from Axiom (16) by instantiating φ to obtain $\top \rightarrow (\top \oplus 0)$, and then applying the upward monotonicity of \oplus [a standard consequence of Axiom (2) – suitably modified by Axiom (15)] to the occurrence of 0 triggered by the propositionally provable implication $0 \rightarrow \top$.

Example 3.6 (Definition of the existential modality). The equivalence $E\varphi \leftrightarrow \varphi \oplus \top$ stated at the start of this paper can be proved as follows. From right to left, using Axiom (7), $\varphi \oplus \top$ immediately implies $E\varphi$. From left to right, using nominals, we first represent the earlier argument for Fact 2.7 in our proof system. (a) $i \rightarrow j \oplus \top$ is provable as follows for any two nominals [we will not state all the obvious uses of LCG principles being used here]: i implies $i \oplus 0$, which implies $i \oplus (j \oplus \langle - \rangle j)$, which implies $j \oplus (i \oplus \langle - \rangle j)$, which implies $j \oplus \top$. (b) Then we also get, as in the preceding example, that $(i \wedge E(j \wedge \varphi)) \rightarrow \varphi \oplus \top$, or rearranged in propositional logic: $(E(j \wedge \varphi)) \rightarrow (i \rightarrow \varphi \oplus \top)$. (c)

¹⁰One might object that this is mere notational transcription of something already understood in other terms, and indeed, some uses of hybrid logic have that character. But as we will see below, our system will then allow us to do something more, namely, investigate the interaction of this base component with new general modal principles.

¹¹Notice also that all our axioms have modal Sahlqvist form, which simplifies completeness arguments, [16, 3].

Now we use the first Witness Rule to conclude $E\varphi \rightarrow (i \rightarrow \varphi \oplus \top)$, and rearranging once more, we get $i \rightarrow (E\varphi \rightarrow \varphi \oplus \top)$. (d) Finally, we apply the Naming Rule to obtain the desired $E\varphi \rightarrow \varphi \oplus \top$.

Finally, we discuss how the system lifts basic facts derivable in the elementary equational logic of groups to modal ‘pattern validities’.

Example 3.7 (Exporting equational validities to LCG). As is well-known, the group axioms imply that inverse is idempotent. We now sketch how this is represented in our proof system via nominals, and next, lift its outcome to a modal validity. In equational logic, one can reason like this:

$$\begin{aligned} x + -x = 0, (x + -x) + - - x = 0 + - - x, x + (-x + - - x) = - - x, \\ x + 0 = - - x, x = - - x \end{aligned}$$

This same reasoning can be represented as a proof of the nominal validity

$$n \leftrightarrow \langle - \rangle \langle - \rangle n$$

where we use the associativity axiom plus Replacement of Equivalents plus the Substitution Rule for nominal terms in LCG. Next, using the Naming and Witnessing rules as above, we lift this to arbitrary formulas. For instance, we can first prove the following implications using nominals as witnesses for the two iterated inversion modalities:

$$\begin{aligned} (n \wedge \langle - \rangle k \wedge E(k \wedge \langle - \rangle l) \wedge E(l \wedge \varphi)) \rightarrow (n \wedge \langle - \rangle \langle - \rangle l \wedge E(l \wedge \varphi)) \text{ [using suitable axioms]} \\ \rightarrow (n \wedge l) \wedge E(l \wedge \varphi) \text{ [using the already derived idempotence for nominals]} \rightarrow \varphi \end{aligned}$$

Now two applications of the Witness rule derive $\langle - \rangle \langle - \rangle \varphi \rightarrow \varphi$. For deriving the converse direction, one can appeal to the principle just proved with $\neg\varphi$ instead of φ and then use the functionality axiom plus propositional contraposition. Finally, combining these two results, we have proved a modal principle that might have looked like an axiom needed in defining the proof system LCG:

$$\varphi \leftrightarrow \langle - \rangle \langle - \rangle \varphi$$

The reader may want to apply similar formal proof techniques to derive the following modal version of one more basic equational law for groups:

$$\langle - \rangle (\varphi \oplus \psi) \leftrightarrow (\langle - \rangle \varphi \oplus \langle - \rangle \psi)$$

More can be said about the styles of reasoning available in our proof system, and we will return to this in the final part of this section. But for now, we turn to an important meta-property.

3.2. Completeness.

Theorem 3.8. *LCG is complete with respect to models over commutative groups.*

Proof. We can largely use the standard canonical model argument for hybrid logic with global modalities and nominals, cf. [16, 3], to which we refer for details. We merely outline the main steps of the construction and some key assertions. As usual, one proves the completeness theorem by showing that any consistent set is satisfied at some point in some model.

One first constructs a family of maximally consistent sets [as in standard modal completeness arguments] with some crucial further features built in by adding successive layers of new nominals as witnesses to the initial language, on the analogy of the Henkin witness construction in the completeness proof for first-order logic.¹² The result is a family of maximally consistent sets Γ , where each consistent set occurs in at least one maximally consistent one, but with the following

¹²Here is where our Naming and Witness rules are crucial, in showing that suitable fresh names can be added consistently, just like the corresponding rules for the existential quantifier in the proof for first-order logic.

special properties. Each maximally consistent set is *named*: it contains a unique nominal, and these sets are also *witnessing* in the following sense:¹³

- If $\mathbf{E}(n \wedge \mathbf{E}\varphi) \in \Gamma$, then, for some nominal i not occurring in $n \wedge \varphi$: $\mathbf{E}n \wedge \mathbf{E}(i \wedge \varphi) \in \Gamma$
- If $\mathbf{E}(n \wedge \langle - \rangle \varphi) \in \Gamma$ then, for some fresh nominal i : $\mathbf{E}(n \wedge \langle - \rangle i) \wedge \mathbf{E}(i \wedge \varphi) \in \Gamma$
- If $\mathbf{E}(n \wedge \varphi \oplus \psi) \in \Gamma$, then for fresh nominals i, j : $\mathbf{E}(n \wedge i \oplus j) \wedge \mathbf{E}(i \wedge \varphi) \wedge \mathbf{E}(j \wedge \psi) \in \Gamma$

Now we define some relations on this universe. First we have an interpretation for the propositional constant 0 since we had $\mathbf{E}0$ in all our sets. Next, we define the usual accessibility relations for the existential modalities \mathbf{E} and $\langle - \rangle$. For instance, we set

$$\Sigma R_{\mathbf{E}} \Delta \text{ if for every formula } \alpha \in \Delta : \mathbf{E}\alpha \in \Sigma.$$

Given our axioms for \mathbf{E} , this is an equivalence relation. Moreover, by the axioms (7), (8), all relations for inverse and later on also for addition cannot cross between such equivalence classes. Also in a standard manner, Axiom (11) enforces that the relation for inverse is a function, which is even idempotent thanks to Axiom (17).

For what follows we fix one particular maximally consistent set Σ^\bullet containing the consistent set we want a model for. This set contains all the information that we need, and hence we shall often refer to it as the *guidebook*. We restrict attention to all maximally consistent sets reachable from Σ^\bullet in the relation $R_{\mathbf{E}}$: this standard move ensures that the global existential modality will get its correct interpretation. Recall that each maximally consistent set here contains a unique nominal. Now we define a ternary relation on these sets represented by their nominals by setting

$$R_{\oplus}(n, i, j) \text{ if } \mathbf{E}(n \wedge i \oplus j) \in \Sigma^\bullet$$

All this amounts to the definition of a model whose points are the nominals for our maximally consistent sets, with zero and the inverse function defined as above, and so far, a ternary relation for addition. However, using the presence of the Axioms (12), (13) in the system LCG, we can show that this ternary relation is in fact *functional*.¹⁴

Now Axioms (14)–(17) enforce immediately via a standard argument that the functions defined here satisfy the conditions for a group. Thus, we have defined a group model \mathfrak{M} .

It remains to show the usual Truth Lemma in a suitable form: truth in the model thus defined is in harmony with the syntactic content of its sets. The following result is easily shown by induction, making use of the Boolean decomposition properties of maximally consistent sets plus the special witnessing properties for our existential modalities put in place above.

Fact 3.9. *For all formulas φ and all points n in \mathfrak{M} , the following are equivalent:*

- (a) $\mathfrak{M}, n \models \varphi$, (b) $\mathbf{E}(n \wedge \varphi) \in \Sigma^\bullet$.

This concludes our outline of the proof that each LCG-consistent set is satisfiable in a group model, and hence of the completeness theorem for our proof system. \square

¹³In the hybrid literature, the conditions that follow are usually stated in terms of the $@_i\varphi$ operator defined as $\mathbf{E}(i \wedge \varphi)$ – but we have chosen to stick with nominals and the global modalities for greater ease in our setting.

¹⁴As an illustration, we show how Axiom (13) yields partial functionality of the relation R_{\oplus} . Let $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ be maximally consistent sets named by n_1, n_2, i, j , respectively. We then have by definition that $\mathbf{E}(n_1 \wedge j \oplus k)$ and $\mathbf{E}(n_2 \wedge j \oplus k)$ are both in Σ^\bullet . But then, using Axiom (13) and the deductive closure of maximally consistent sets, we get that $\mathbf{E}(i_1 \wedge i_2) \in \Sigma^\bullet$. But this implies that n_1, n_2 must name the same set.

The above proof largely follows a standard completeness argument in the area of hybrid logic.¹⁵ In fact, inspecting its details, we can see the following.

Fact 3.10. *LCG is also complete if we replace Axioms (14)–(16) by their nominal versions.*

This reflects a standard result in hybrid logic that classes of frames defined by universal first-order axioms are axiomatizable using pure nominal axioms [3]. We have chosen to define our proof system with a mixture of nominal and modal principles to better bring out its content, and in what follows, we make some further observations about this balance.

3.3. Point and set principles in the modal logic of groups. We conclude this section with some further comments on how to understand the proof system LCG. If the only aim were to represent first-order equational reasoning about groups, it would have sufficed to use only nominals, and essentially transcribe the group axioms. But as we have said earlier, the modal part of the language extends the analysis from objects to sets and allows us to reason about what we called ‘patterns’. In particular, what we see then is that some validities at the nominal level are valid more generally for arbitrary formulas, standing for subsets of our models. For instance, $n \oplus 0 \leftrightarrow n$ is valid, but so is $\varphi \oplus 0 \leftrightarrow \varphi$, which is why we put the latter version as an axiom.

Here is an illustration of the proof techniques involved here. We give some detail to display the various formal moves available in our proof system.¹⁶

Example 3.11 (The modal associativity law). Suppose we only have the associativity law for nominals, i.e., $n \oplus (k \oplus l) \leftrightarrow (n \oplus k) \oplus l$. Then Axiom (14) $\varphi \oplus (\psi \oplus \chi) \leftrightarrow (\varphi \oplus \psi) \oplus \chi$ in its full generality can still be derived. We only consider the direction from left to right, and analyze what principles with nominals added would suffice by the Witness Rule for the \oplus modality. First it suffices to show (a) $(k \oplus l \wedge \mathbf{E}(k \wedge \varphi) \wedge \mathbf{E}(l \wedge \psi \oplus \chi)) \rightarrow (\varphi \oplus \psi) \oplus \chi$ for some fresh nominals k, l . (b) Next we rearrange this to the task of proving the propositionally equivalent $\mathbf{E}(l \wedge \psi \oplus \chi) \rightarrow ((k \oplus l \wedge \mathbf{E}(k \wedge \varphi)) \rightarrow (\varphi \oplus \psi) \oplus \chi)$. (c) Next, we use the easily shown fact [by the axioms for the global modality] that LCG can prove an implication of the form $\mathbf{E}\alpha \rightarrow \beta$ iff it can prove $\alpha \rightarrow \mathbf{U}\beta$. This reduces the preceding task to proving $(l \wedge \psi \oplus \chi) \rightarrow \mathbf{U}((k \oplus l \wedge \mathbf{E}(k \wedge \varphi)) \rightarrow (\varphi \oplus \psi) \oplus \chi)$, or equivalently $\psi \oplus \chi \rightarrow (l \rightarrow \mathbf{U}((k \oplus l \wedge \mathbf{E}(k \wedge \varphi)) \rightarrow (\varphi \oplus \psi) \oplus \chi))$. (d) By the Witness Rule once more, it suffices to derive $(m \oplus n \wedge \mathbf{E}(m \wedge \psi) \wedge \mathbf{E}(n \wedge \chi)) \rightarrow (l \rightarrow \mathbf{U}((k \oplus l \wedge \mathbf{E}(k \wedge \varphi)) \rightarrow (\varphi \oplus \psi) \oplus \chi))$, with fresh nominals m, n , or equivalently $(l \wedge m \oplus n \wedge \mathbf{E}(m \wedge \psi) \wedge \mathbf{E}(n \wedge \chi)) \rightarrow \mathbf{U}((k \oplus l \wedge \mathbf{E}(k \wedge \varphi)) \rightarrow (\varphi \oplus \psi) \oplus \chi)$. What remains is a provability task with complete naming of all points involved, and the crux is then to note that $l \wedge m \oplus n$ implies that $\mathbf{U}(l \rightarrow m \oplus n)$, so we can replace the subformula $k \oplus l$ in the antecedent of the consequent by $k \oplus (m \oplus n)$. Then we appeal to our assumed nominal version of Associativity to replace this by $(k \oplus m) \oplus n$, and using further principles in LCG for nominals, we put the formulas φ, ψ, χ back in place to obtain the desired modal formula $(\varphi \oplus \psi) \oplus \chi$.

Behind this example lies a general issue of lifting laws for algebras to set versions.

Remark 3.12 (Complex algebra). The theory of *complex algebras* studies set liftings of standard algebraic structures. A standard example is the set-lifting of standard Boolean algebras $(B, \wedge, \vee, \neg, 0)$.

¹⁵We have followed a style of presentation which makes the model constructed for a given consistent set of formulas resemble the canonical models used in modal logic. However, there are some crucial differences too. At heart, hybrid completeness proofs are closer to the less canonical construction in the Henkin-style completeness proof for first-order logic. First, our taking a generated submodel to enforce the standard interpretation of the global modalities amounts to choosing one particular maximally consistent set of globally true formulas, and second, all the information that we need is really already contained in the single guidebook Σ^\bullet , as is clear in the Truth Lemma. From a first-order point of view, the main technical point of a completeness proof like ours is that the usual Henkin argument can be carried out in a much weaker sublanguage by choosing axioms and rules appropriate to that restricted setting.

¹⁶Of course, by the completeness theorem for the purely nominal version of the group axioms, such formal derivations must exist. However, a completeness proof seldom gives direct information for specific cases, and a constructive demonstration may add an epsilon of certainty for many readers, and perhaps even authors themselves.

Define the complex algebra $(\mathcal{P}(B), \wedge, \vee, \neg, \{0\})$, where we set (a) $A \wedge B = \{a \wedge b : a \in A, b \in B\}$, (b) $A \vee B = \{a \vee b : a \in A, b \in B\}$, and (c) $\neg A = \{\neg a : a \in A\}$. The result is a new richer kind of algebra where the lifted conjunction and disjunction show similarities with our product modality, [11]. Complex algebras can be defined over any algebraic structure, and we refer to [28, 19] for applications and more details of their theory. One old question in the area is when valid equations for the underlying algebras transfer to the set-lifted versions of their operations. Gautam's Theorem [25] shows that this is rare: happening only when each variable occurs at most once on each side of the equation. This is precisely the sort of phenomenon we have noticed in the above.

The preceding examples in this section of modal lifting of nominal principles worked because all axioms involved had Gautam form. If we do not have such a form, then there may still be workarounds. The lifting need not be literal from equations to corresponding modal equivalences, but could also have other formats, as in the following illustration.

Example 3.13 (Group inverses). We expressed the basic law $v + (-v) = 0$ as follows in our logic, using nominals: $i \oplus \langle - \rangle i \leftrightarrow 0$. This cannot be lifted to sets in a direct manner, since $\varphi \oplus \langle - \rangle \varphi \leftrightarrow 0$ is clearly not a valid formula if φ denotes more than one object. However, there is a formula in our language that does the same job without nominals [except for the special case of the constant nominal 0 for the zero vector, which we viewed as a unary modality in the signature]. On the frames underlying our models, the following formula

$$E\varphi \rightarrow E((\varphi \oplus \langle - \rangle \varphi) \wedge 0)$$

is easily seen to enforce the basic law of inverses we started with.

Again there is a background in Complex Algebra here, where axiomatizations in other non-literal formats have been proposed. In particular, [33] give a general game-based technique for turning equational axiomatizations for classes of algebras into axiomatizations of the theory of their complex algebras. Such results may also apply here, though we do not just have the complex algebra by itself, but also the standard Booleans in our language, and only want to use a minimal auxiliary hybrid apparatus of global modalities and nominals.

Remark 3.14 (A congenial modal approach). Closer to our setting is the approach in [29] whose authors axiomatize the complex algebra of Boolean algebras [with the standard Booleans thrown in, now as standard modal operations at the set level] using a modal logic based on a *difference modality* saying that a formula is true at some point different from the current one. Amongst other things, this device allows for defining truth in single points, while also facilitating the formulation of a family of new derivation rules that ensure completeness. A particularly interesting feature of the approach in [29] is that the difference modality is definable via the standard Boolean connectives of classical logic plus the modal operator $\langle - \rangle$ obtained by lifting the Boolean implication \rightarrow . The authors suggest that this approach is also available for groups, since a difference modality can be defined there as well.¹⁷ A comparison of this alternative style of axiomatization with ours in terms of nominals and global modalities seems of interest, but we will not pursue this here.

Much more can be said about the preceding topic. For a model-theoretic perspective, Gautam equations translate into formulas where the proposition letters or formula variables for the algebraic variables are in *distributive* position, which allows for taking them out by single existential quantifiers.¹⁸ From a proof-theoretic perspective, our earlier examples illustrate why equations in Gautam form allow for set lifting, and indeed, it can be shown that every such lifting is available in LCG. More general questions arise here, but they are beyond the scope of this paper.

¹⁷Indeed, the formula $\varphi \oplus \neg 0$ in our language defines the difference modality. If it is true for a point s , then $s = y + u$ with $t \models \varphi$ and $u \neq 0$, and hence, by the group axioms, it follows that $s \neq t$.

¹⁸There are analogies here with the correspondence analysis of existential quantifiers in the antecedent of Sahlqvist-type axioms, [16, Ch. 3], which get replaced by prefix quantifiers over individual worlds.

However, one can also drop this all-or-nothing perspective, and rather ask which mixed principles with nominals as needed and formula variables wherever possible are derivable. This may start from a purely nominal principle and test for φ -type generalizations of some nominals, Or vice versa, we can start with an invalid purely modal principle, and ask which replacements of formula variables by nominals might lead to validity. Here is a concrete illustration where this makes good sense, which goes back to an earlier section about notions definable in our basic modal language.

Example 3.15 (Proving facts about categorical implication). Nominals are natural in studying vector spaces, though they are not always needed. A case in point is Mathematical Morphology, where some laws for shapes only need our basic modal logic without nominals, whereas others need more. Consider the following principle for Minkowski subtraction, aka categorical implication:

$$(\psi \Rightarrow (\varphi \oplus \alpha)) \Leftrightarrow ((\psi \Rightarrow \varphi) \oplus \alpha)$$

From right to left, this principle is derivable using Associativity for \oplus plus the following law for implication: $(\alpha \oplus \beta) \Rightarrow \gamma \rightarrow (\beta \Rightarrow (\alpha \Rightarrow \gamma))$. It is easily seen that the latter implication principle is derivable from our general modal axioms under the translation given in Section 2.

In the opposite direction, our initial principle is not valid on vector spaces, witness the following counter-example which also shows how our implications work semantically. Consider the vector space of the integers over the two-element field (many other structures would do), and let φ denote the set $\{1, 2\}$, ψ the set $\{2, 3\}$, and α the set $\{1, 3\}$. Then $\varphi \Rightarrow \psi$ denotes $\{1\}$, $\psi \oplus \alpha$ denotes $\{3, 4, 5, 6\}$, $\varphi \Rightarrow (\psi \oplus \alpha)$ denotes $\{2, 3, 4\}$, while $(\varphi \Rightarrow \psi) \oplus \alpha$ denotes the set $\{2, 4\}$.¹⁹

However, now consider the following variant of the above principle:

$$(\psi \Rightarrow (\varphi \oplus n)) \Leftrightarrow ((\psi \Rightarrow \varphi) \oplus n)$$

This principle is valid on vector spaces. We only show the non-trivial direction. Let x satisfy the formula $\psi \Rightarrow (\varphi \oplus n)$, and write x as the sum $(x - n) + n$. Now, let y be any vector satisfying ψ : then $(x - n) + y = (x + y) - n$ where by the assumption, $x + y$ satisfies $\varphi \oplus n$. But then $(x + y) - n$ and hence also $(x - n) + y$ satisfies φ , and therefore $x - n$ satisfies $\psi \Rightarrow \varphi$. Now the decomposition $x = (x - n) + n$ shows that x also satisfies $(\psi \Rightarrow \varphi) \oplus n$.

The preceding semantic argument can be reproduced in our formal proof system by making use of the rules for nominals. But our main point here is a different one. In the categorial implicational connection, of course, we want as many generally valid principles as we can get in terms of formula variables. But beyond these, there is a serious mathematical interest in principles whose validity require a certain modicum of reference to objects.²⁰

We conclude with a problem left open by our mixed style of proof analysis. Given the first-orderness of the group axioms, it can be seen that the purely modal valid principles in our language, with no occurrences of nominals, are a computably enumerable set. What would be a complete pure modal axiomatization for this subsystem?

¹⁹These calculations amount to a *generalized arithmetic* with fixed and ‘loose’ numbers. We have specific numbers k , but also variables X whose value we only know as a set of numbers. Then the above valid principle says that the standard arithmetical equality $(y + k) - x = (y - x) + k$ lifts to the still valid generalized equality $(Y + k) - X = (Y - X) + k$, but that $(Y + Z) - X = (Y - X) + Z$ would no longer be valid. Of course, this is just one instance of what can and cannot be preserved in moving from sharp numbers to also include fuzzier numbers X, Y , etc.

²⁰Our analysis has shown that our basic modal logic of groups can embed Minkowski-style or substructural categorial logics of product conjunction and implication. What we have not shown is whether this embedding is *faithful*. For instance, whether the commutative Lambek Calculus is complete for vector space semantics, or perhaps even for standard Euclidean vector spaces, appears to have been an open problem since 2000.

4. MODAL LOGIC OF LINEAR CLOSURE

An important notion in groups is closure of subsets to *subgroups* that are closed under taking group sums and inverses, with linear subspaces of vector spaces as an important example.²¹

4.1. Language and definability. This suggests adding a new modality to our language.

Definition 4.1. $\mathfrak{M}, s \models C\varphi$ iff s is obtained from the set $\{t \mid \mathfrak{M}, t \models \varphi\}$ by finitely many consecutive uses of the binary operation $+$, the unary operation $-$ and the nullary operation 0 .

Note that $C\varphi$ is not an ordinary modality, in that it does not distribute over either conjunctions or disjunctions, as is clear from the behavior of closure in groups or vector spaces. Accordingly, our analysis in this section will use ideas from *neighborhood semantics* for modal logic, [42].

Remark 4.2 (Further definable notions). The following notion of stepwise closure with explicit arguments is already definable in our modal base language:

$$\mathfrak{M}, v \models D^+(\varphi_1, \dots, \varphi_n) \text{ iff } v \text{ is a sum of } n \text{ points } v_1, \dots, v_n \text{ where } v_i \text{ satisfies } \varphi_i.$$

We can also introduce an abstract dependence notion $Dep_\varphi\psi$ as $U(\psi \rightarrow C\varphi)$, saying that each point satisfying ψ is a sum of points satisfying φ . This induces natural validities such as the following:

$$Dep_\varphi\psi \wedge Dep_\xi\eta \rightarrow Dep_{\varphi\vee\xi}(\psi \oplus \eta), \quad Dep_{\varphi\vee\xi}\psi \leftrightarrow D_{\varphi\oplus\xi}\psi \quad ^{22}$$

Perhaps the best way of understanding what makes the closure modality tick involves a well-known modal fixed-point logic, [18].

Fact 4.3. $C\varphi$ is definable in the μ -calculus extension of our basic modal language.

The relevant definition is as the following smallest fixed-point:

$$\mu p. (0 \vee \varphi \vee \langle - \rangle p \vee (p \oplus p))$$

Given the invariance of μ -calculi for the same bisimulations as their underlying basic modal logics, it follows that $C\varphi$ is invariant for our earlier *bisimulations of group models*. However, we will not pursue this model-theoretic perspective here.

As for valid principles of reasoning with the closure modality, the preceding μ -calculus-style definition suggests the following two principles:

- $(0 \vee \varphi \vee \langle - \rangle C\varphi \vee C\varphi \oplus C\varphi) \rightarrow C\varphi$
- if $0 \rightarrow \alpha, \varphi \rightarrow \alpha, \langle - \rangle \alpha \rightarrow \alpha$ and $\alpha \oplus \alpha \rightarrow \alpha$ are valid, then so is $C\varphi \rightarrow \alpha$.²³

4.2. Dependence as a neighborhood modality. One can view $C\varphi$ as a monotonic neighborhood modality, describing points that are related to the set of points $\{t \mid \mathfrak{M}, t \models \varphi\}$. One can generalize this to an abstract neighborhood relation NsX with the upward monotonic truth definition

$$\mathfrak{M}, s \models C\varphi \text{ iff } \exists X \forall x \in X : \mathfrak{M}, x \models \varphi$$

This framework allows for an abstract modal *frame correspondence analysis*, [7, 16], of the content of natural principles governing the closure modality on group models. The following assertions rely on the earlier notion of frame truth for modal formulas.

²¹One can also think of closure as a form of dependence: everything in the closure of a set X is uniquely determined by the objects in X , and hence depends on X . This perspective will be pursued in the next section.

²²Such valid principles will all be derivable in our later proof system.

²³This implication between validities also holds when replacing validity by global truth in a model, and it can then be formulated as one valid formula using the universal modality.

Fact 4.4. *The following frame correspondences hold for the fixed-point principles governing the dependence modality in abstract neighborhood frames:*

- $p \rightarrow \mathsf{C}p$ defines $\forall x : Nx \{x\}$
- $0 \rightarrow \mathsf{C}p$ defines $\forall x : Nx \emptyset$ iff $x = 0$
- $\langle - \rangle \mathsf{C}p \rightarrow \mathsf{C}p$ defines $\forall x, Y : Nx Y$ iff $N_{-x} Y$
- $\mathsf{C}p \oplus \mathsf{C}p \rightarrow \mathsf{C}p$ defines $\forall x, y, z, U, V : \text{if } Rx, yz \text{ and } NyU \text{ and } NzV, \text{ then } NxU \cup V$
- *The fixed-point rule, with premises read as global truth at all points in a model, enforces that the neighborhood relation is contained in the finite closure in the definition of $\mathsf{C}\varphi$.*

Proof. These facts follow by straightforward modal correspondence arguments. For instance, the LGC-axioms for inverse enforce in standard Sahlqvist style, [16, Ch. 3], that inverse is an idempotent function. Then, clearly, whatever valuation we choose for p on a given frame, $\langle - \rangle \mathsf{C}p \rightarrow \mathsf{C}p$ is going to be true when the stated condition holds, given our neighborhood-style truth definition for the modality C . Vice versa, if $\langle - \rangle \mathsf{C}p \rightarrow \mathsf{C}p$ is true for all valuations on a frame, and we have $N - x, Y$, then setting $V(p) = Y$ makes the antecedent $\langle - \rangle \mathsf{C}p$ true at x , whence we also have the consequent $\mathsf{C}p$ true at x , which implies that Nx, Y . The sum axiom can be analyzed in the same Sahlqvist style, though here, the reader may find it easier to use the equivalent version $\mathsf{C}\varphi \oplus \mathsf{C}\psi \rightarrow \mathsf{C}(\varphi \vee \psi)$ without repetitions of p in the antecedent. Finally, the proof for the last step is again a Sahlqvist-style argument, but in this case, without a first-order definition for the minimal valuation. This can be done just like the way [10] shows that the Induction Axiom of propositional dynamic logic PDL enforces that the accessibility relation for the modality \Box^* is the reflexive transitive closure of the original accessibility relation R for the basic modality \Box . \square

4.3. Axiomatization and completeness. While the modality $\mathsf{C}\varphi$ does not distribute over conjunction or disjunction, it is obviously *upward monotonic*: $\mathsf{C}\varphi \rightarrow \mathsf{C}(\varphi \vee \psi)$ is valid. In combination with our earlier observations about validities, this suggests the following proof system.

Definition 4.5. *The proof system MCL consists of the following components:*

- (a) *The earlier complete modal logic of group models, including the basic principles of hybrid logic for the universal modality and the nominals.*
- (b) *The minimal monotonic neighborhood logic for the unary modality C .*
- (c) *The following two principles for smallest fixed-points:*
 - $(0 \vee \varphi \vee \langle - \rangle \mathsf{C}\varphi \vee \mathsf{C}\varphi \oplus \mathsf{C}\varphi) \rightarrow \mathsf{C}\varphi$
 - *if $\vdash 0 \rightarrow \alpha, \varphi \rightarrow \alpha, \langle - \rangle \alpha \rightarrow \alpha$ and $\alpha \oplus \alpha \rightarrow \alpha$, then $\vdash \mathsf{C}\varphi \rightarrow \alpha$.*

Here are some provable formulas showing how the system works.

Example 4.6 (Formally derivable closure principles).

- The formula $\mathsf{C}\varphi \oplus \mathsf{C}\psi \rightarrow \mathsf{C}(\varphi \vee \psi)$ is provable using upward monotonicity in both arguments to $\varphi \vee \psi$ and then applying the fixed-point axiom.
- The formula $0 \leftrightarrow \mathsf{C}\perp$ is provable. From left to right, the fixed-point axiom gives $0 \rightarrow \mathsf{C}\varphi$ for any formula φ . From right to left, use a straightforward instance of the induction rule, noting that 0 satisfies all the premises.
- The formula $\mathsf{C}\mathsf{C}\varphi \rightarrow \mathsf{C}\varphi$ expressing that the linear closure operator C is idempotent is valid in our semantics, and can be derived by taking both φ and α in the proof rule to be $\mathsf{C}\varphi$.

Soundness of the above proof system is immediate by the given intuitive explanations.

The completeness result that follows now is the best we have been able to obtain so far. It refers to the earlier-mentioned ‘abstract group models’ where, instead of a function $x = y + z$, we have a

not necessarily functional ternary relation Rx, yz satisfying the axioms of the system. We include the result all the same since the proof does present several features of interest.²⁴

Theorem 4.7. *The above proof calculus MCL is complete for our modal base language extended with $C\varphi$ over abstract group models.*

Proof. We proceed as in the well-known completeness proof for propositional dynamic logic, (see e.g., [16, Sec. 4.8]), but thinking in the reverse direction for the function values as happens in our basic semantics, and using a neighborhood semantic base for the closure modality.

Consider any formula φ that is consistent in our logic, where consistency is defined as usual with respect to the above proof system: we show that φ is satisfiable in an abstract group model.

First fix a finite set F of relevant formulas as in the Fisher-Ladner filtration for PDL. F contains φ , and is closed under (a) subformulas, (b) single negations, and (c) if $C\varphi$ is in F , then so are $\langle - \rangle\varphi$, $C\varphi \oplus C\varphi$.²⁵ This will be our language in what follows.

Now we construct the *finite Henkin model* \mathfrak{M} whose points are all maximally consistent sets of formulas in the finite set F , endowed with the following structure. The 0 point is the unique maximally consistent set containing the nominal 0. Group inverses are treated as follows, using the axioms for the inversion modality in our proof system.

Fact 4.8. *The stipulation $inv(\Sigma) = \{\varphi \mid \langle - \rangle\varphi \in \Sigma\}$ defines a function.*

Finally, the ternary relation $R\Gamma, \Delta\Sigma$ is defined as follows:

$$conj(\Gamma) \wedge (conj(\Delta) \oplus conj(\Sigma)) \text{ is consistent}$$

where $conj$ denotes the conjunction of all formulas in the set argument.

Next, we show a Truth Lemma for maximally consistent sets and relevant formulas:

Fact 4.9. *A formula φ belongs to a set Γ iff φ is true at Γ in the finite Henkin model \mathfrak{M} .*

Proof. The induction is straightforward for atoms, Booleans, and modalities $\varphi \oplus \psi$ by the usual modal completeness argument in a filtration format. The crucial case is that for $C\varphi$.

(a) Suppose $C\varphi$ belongs to the set Γ . Consider the set \mathfrak{D} that contains all maximally consistent sets containing φ , plus all sets that can be obtained, successively, by iterating: binary combination and unary inverse as defined above, as well as adding the unique set for the nominal denoting zero. The family \mathfrak{D} is finite, given that our Henkin model is finite, and hence it can be described by one formula δ , the disjunction of all conjunctions for its member sets. This formula δ satisfies the conditions of the fixed-point proof rule [by some simple arguments about consistent sets], so we have $C\varphi \rightarrow \delta$ provable, and hence Γ is consistent with δ , and therefore, Γ must be in the family \mathfrak{D} described. Finally, given the inductive hypothesis, membership and truth for φ coincide for all maximally consistent sets, and it follows that $C\varphi$ is true at Γ in the finite Henkin model \mathfrak{M} .

(b) Conversely, let Γ make $C\varphi$ true in \mathfrak{M} . Then Γ belongs to the finite family \mathfrak{D} described above, where we again use the inductive hypothesis for φ to identify sets where φ is true with sets containing this formula. Now, we prove by induction on the depth of the decomposition for Γ that $\varphi \in \Gamma$, by a repeated appeal to the fixed-point axiom plus properties of our closure. The base cases are obvious, we just consider the sum modality. Suppose Γ is a sum of Γ_1, Γ_2 in \mathfrak{D} with decompositions of lower depth. By the inductive hypothesis, $C\varphi$ belongs to both Γ_1, Γ_2 . Now $C\varphi \oplus C\varphi$ belongs to the initial set F by one of our closure conditions, and using the definition of the ternary sum modality, it follows that $C\varphi \oplus C\varphi$ is consistent with Γ and thus belongs to it. But then by the fixed-point axiom, the formula $C\varphi$ is consistent with Γ too, and hence belongs to it. \square

²⁴The argument to follow is in essence the one first given for ‘Dynamic Arrow Logic’ in [9].

²⁵That a set with these closure conditions can stay finite follows by a standard argument.

The global existential modality and nominals do not pose a problem in this completeness argument. A maximally consistent set with a relevant nominal in the finite language is unique. \square

Remark 4.10 (Comparison with PDL). As we stated, $C\varphi$ is not a normal modality: it only satisfies monotonicity. Given the strong analogies of the above proof with the completeness proof for the normal iteration modality $\Box^*\varphi$ in PDL, the lack of appeal to distribution may seem surprising. But as it happens, monotonicity is the only active principle in the latter case, too: distribution over conjunction is not used in that well-known proof, being *derivable*. We now proceed to show this perhaps not so well-known fact. For better comparison with the existential flavor of $C\varphi$, we show distribution over disjunctions for the existential iteration modality $\Diamond^*\varphi$: distribution for the base modality \Diamond suffices plus the fixed-point principles for the inductive definition $\mu p. (\varphi \vee \Diamond p)$.

- (a) We have directly from the PDL fixed-point axiom that $(\varphi \vee \psi) \rightarrow (\Diamond^*\varphi \vee \Diamond^*\psi)$.
- (b) Also, $\Diamond(\Diamond^*\varphi \vee \Diamond^*\psi)$ implies $\Diamond\Diamond^*\varphi \vee \Diamond\Diamond^*\psi$ by distribution for the base modality, and this again implies $\Diamond^*\varphi \vee \Diamond^*\psi$ by the fixed-point axiom.
- (c) Applying the PDL fixed-point rule to (a) and (b) yields $\Diamond^*(\varphi \vee \psi) \rightarrow (\Diamond^*\varphi \vee \Diamond^*\psi)$.

This example provides an interesting instance of how adding mathematical principles such as induction can boost the propositional modal base logic one started from.

Perhaps the major question left open by the preceding result is how to achieve completeness of modal closure logic for genuine group models where $+$ is a *function*.²⁶ We have not been able to adjust our filtration method to achieve this feature, and must leave this as an open problem.

5. DEPENDENCE AND INDEPENDENCE IN VECTOR SPACES

We now move from group structure to the richer structure of vector spaces. In that setting, linear dependence is a basic notion, making it an obvious target for qualitative analysis in our style. At the same time, dependence is a topic of growing importance in the broader logical literature [46]. In particular, [6] have initiated a modal approach to dependence and explored some first connections with Linear Algebra. In this section, we take this modal line further, bringing in independence as well. However, toward the end we identify a simple but important conceptual difference between our logics and those in the cited literature. Our treatment will focus on dependence and independence per se, an integration with our earlier complete logics is possible, but will not be undertaken here.

5.1. Linear dependence of vectors and Steinitz Exchange. Linear closure as studied earlier is analogous to dependence in vector spaces: a vector x depends on a set of vectors X if x is in the linear closure of X . Yet despite this analogy, we are still missing some crucial features since linear combinations of vectors also use coefficients from a field that is part of the vector space. The difference shows up formally in new valid principles.

Example 5.1. The law of *Steinitz Exchange* says that, for finite sets of vectors X ,

If vector z depends on $X \cup \{y\}$, then either z depends on X or y depends on $X \cup \{z\}$.

Steinitz Exchange is the crucial property underlying the elementary theory of dependence and dimension in vector spaces, [20]. Its validity, though simple to see, depends essentially on the field properties in vector spaces. If z is a linear combination of the form $c_1.x_1 + \dots + c_k.x_k + d.y$, then there are two cases. Either $d = 0$ and z depends on X alone, or $d \neq 0$, and we can divide the equality by d to obtain, after suitably transposing terms, that y depends on $X \cup \{z\}$.

In what follows, abstract dependence relations in vector spaces will be denoted by

$$D_X y : \quad y \text{ is a linear combination of vectors in the set } X.$$

²⁶This seems urgent since so much of Linear Algebra calculates with operations on vectors.

We will also use the notation $D_X Y$ for $\forall y \in Y : D_X y$.

Fact 5.2. *Dependence in vector spaces satisfies the following properties:*

- | | |
|--|--------------------------|
| (a) $D_X x$ for $x \in X$ | <i>Reflexivity</i> |
| (b) $D_X y$ and $X \subseteq Z$ imply $D_Z y$ | <i>Monotonicity</i> |
| (c) $D_X Y, D_Y Z$ imply $D_X Z$ | <i>Transitivity</i> |
| (d) $D_{X,y} z$ implies $D_X z$ or $D_{X,z} y$ | <i>Steinitz Exchange</i> |

To bring such facts into a logic, we introduce a formal modality $D\varphi$ for vector dependence:

$D\varphi$ is true at just those points which are linear combinations of points satisfying φ .

Then the preceding abstract properties express simple valid modal principles. In particular, we get (a) $\varphi \rightarrow D\varphi$, (b) $D\varphi \rightarrow D(\varphi \vee \psi)$, (c) $D\varphi \rightarrow DD\varphi$ – all true for the earlier modality C as well – while (d) Steinitz Exchange can be defined using one general formula variable plus nominals:

$$m \wedge D(\varphi \vee n) \rightarrow (D\varphi \vee E(n \wedge D(\varphi \vee m)))$$

However, this principle does not hold for our earlier linear closure in additive groups.

Example 5.3. Steinitz Exchange can fail when dependence is just linear closure.

In the group model $\mathbb{Z} \times \mathbb{Z}$ with \mathbb{Z} the integers, $(3, 2)$ depends on $\{(1, 1), (2, 1)\}$, but not on $(1, 1)$ alone, while $(2, 1)$ does not depend on $\{(1, 1), (3, 2)\}$.²⁷

Next we formulate a useful observation for our later axiomatization.

Remark 5.4 (Generalized Steinitz). Dependence relations in vector spaces satisfy the following generalized version of Steinitz Exchange:

$$D_{X \cup Y} z \text{ implies } D_X z \text{ or, for some } y \in Y : D_{X, Y - y + z} y \quad (GS)$$

This can be proved by induction on the size of Y [here the finiteness is used essentially]. The base case is ordinary Steinitz. Now suppose GS holds for sets Y of size n , we consider the case $n + 1$: or in other words, $Y + u$ with $|Y| = n$. By Steinitz, $D_{X, Y, u} z$ implies $D_{X, Y} z$ (i) or $D_{X, Y, z} u$ (ii). Case (ii) satisfies our description. In Case (i), by the inductive hypothesis, there is some $y \in Y$ s.t. $D_{X, Y - y + z} y$. By monotonicity, this implies $D_{X, Y - y + z + u} y$, which again satisfies our description.

Our final observation concerns an abstract perspective on linear dependence.

Remark 5.5. Like the earlier $C\varphi$, the new $D\varphi$ can be seen as a *neighborhood modality* interpreted in the format $\mathfrak{M}, s \models D\varphi$ iff $\exists X \forall x \in X : \mathfrak{M}, x \models \varphi$. Similar points apply to those made earlier. In particular, a *frame correspondence* analysis applies, and the preceding formula expressing Steinitz Exchange then enforces the abstract version of this property for the neighborhood relation.

5.2. A modal logic of dependence for vectors. A complete proof system for our new modal dependence logic should contain (a) all the principles of our earlier complete logic LCG for group models plus (b) suitable axioms and rules for the new dependence modality D adapting those found for our earlier system MCL. Here we merely focus on a basic new ingredient which comes to light in this way. It now makes sense to analyze the contribution of the field in its own terms.

We add a new modal operator to our language, describing the behavior of ‘field multiples’:

$$m\varphi : \text{ some multiple } ax \text{ makes } \varphi \text{ true for some field element } a$$

²⁷Viewed in another way, this example also shows how the absence of a field allows for broader types of models and dependence than those found in vector spaces.

Then we can define $D\varphi$ by means of a smallest fixed-point formula as for linear closure, but now folding the earlier disjuncts used in MCL for the zero-vector and for additive inverses under the new operator, given the definition of a vector space:

$$\mu p.(\varphi \vee \mathbf{m}p \vee p \oplus p)$$

What is the complete modal logic of \mathbf{d} ? This modality clearly satisfies the following laws:

- (1) $\mathbf{m}(\varphi \vee \psi) \leftrightarrow \mathbf{m}(\varphi \vee \mathbf{d}\psi)$
- (2) $\varphi \rightarrow \mathbf{m}\varphi$
- (3) $\mathbf{m}\mathbf{m}\varphi \rightarrow \mathbf{m}\varphi$
- (4) $(\varphi \wedge \mathbf{m}(\neg 0 \wedge \psi)) \rightarrow \mathbf{m}(\psi \wedge \mathbf{m}\varphi)$
- (5) $0 \rightarrow \neg \mathbf{m}\neg 0$

This is very close to the standard normal modal logic S5, in a language with one special nominal added. The second and third principles express reflexivity and transitivity, while the fourth expresses symmetry except for the case where the successor is the zero vector. The fifth principle says that the only multiple of 0 is 0 itself. It is easy to see that the binary relational frames for this logic consist of a family of equivalence classes plus one unique endpoint 0 which is accessible from everywhere inside any equivalence class (but not vice versa).

Fact 5.6. *The complete modal logic of $\mathbf{m}\varphi$ is axiomatized by the above five principles.*

Proof. By standard arguments, [16], any non-provable formula φ in the above axiom system can be falsified at either 0 or some point in some equivalence. By invariance for generated submodels, we can restrict attention to one equivalence class plus the 0 point. The valuation only has to assign truth values at points for the finitely many proposition letters occurring in φ , yielding a finite partition of the equivalence class. Still without loss of generality, as for S5, we can even assume that each partition element occurs only once in the equivalence class. Now it is straightforward to reproduce this valuation pattern on, say, the vector space of the reals, by making sure each partition element induced by the valuation occurs in the reals, and no others do. The obvious map back from the reals to the given model sends points with a particular partition to its representative in the original model. It is easy to show that this is map a bisimulation, and hence our initial modal formula can also be falsified with the true ‘multiple relation’ on the reals. \square

Remark 5.7 (A connection with a classical system). Interestingly, the logic of $\mathbf{m}\varphi$ identified here in vector spaces is close to a well-known system in the modal literature. Disregarding the role of the nominal 0, it is the ‘pin logic’ of [22, 39], which was shown to be a largest non-tabular logic below S5, while it does have the Finite Model Property. Thus we can immediately apply known results to the modal logic of vector multiples. Conversely, our setting suggests that adding new vocabulary to the existing modal setting which brings out the special nature of the frames [e.g., it is very natural to name the special element, and perhaps further notions make sense], might pose some interesting new questions in the modal literature on pre-tabular logics.

A complete axiom system for our full language would incorporate this base logic, while adapting the earlier base logic for linear closure with fixed-point principles using \mathbf{m} , such as

$$(\mathbf{m}C\varphi \vee C\varphi \oplus C\varphi) \rightarrow C\varphi$$

where we also assume some obvious auxiliary principles such as $0 \rightarrow \mathbf{m}\varphi$ and $\langle - \rangle \mathbf{m}\varphi \rightarrow \mathbf{m}\varphi$.²⁸ We leave the precise details of such a combined complete logic to another occasion.

²⁸We may also need a form of Generalized Steinitz, which, given the earlier discussion in Remark 5.4, should behave according to this heuristic principle: “ $(n \wedge D(\varphi \vee \psi)) \rightarrow \exists m : E(m \wedge \psi \wedge D(\varphi \vee (\psi \wedge \neg m) \vee n))$ ”. In modal logic, as we have seen with the proof system LCG, such behavior is typically enforced by adding an appropriate derivation rule to the system guaranteeing the existence of the appropriate witnesses in the canonical model.

5.3. From dependence to independence, the abstract way. In Linear Algebra, *independence* of sets of vectors is arguably just as important as dependence, since it underlies the fundamental notions of basis and dimension. Independence can be seen as just the negation of the earlier dependence in the following sense: $\neg D_X y$ says that y cannot be written as a linear combination of vectors in Y . However, a more common and useful related notion is that of an *independent set*, which we can view as follows in an abstract format.

Definition 5.8. *An independence predicate I satisfies the following conditions:*

- (a) $I(X)$ and $Y \subseteq X$ imply $I(Y)$ *Downward Monotonicity*
- (b) if $I(X)$ and $I(Y)$ and $|X| < |Y|$, then there is some $y \in Y - X$ s.t. $I(X \cup \{y\})$.

In the finite case, there is a unique maximal size of independent sets, the ‘dimension’.

Remark 5.9 (Matroid Theory). The preceding definition states the crucial properties of a *matroid*, a well-known abstraction out of vector spaces. Abstracting out of linearly independent sets, a *matroid* is a finite family \mathbf{F} of finite sets (i) containing the empty set, (ii) closed under subsets, and satisfying an abstract analogue of Steinitz Exchange (iii) if A, B are in \mathbf{F} , and $|B| > |A|$, then there exists a $b \in B$ s.t. $A \cup \{b\} \in \mathbf{F}$. Matroids have both vector and graph interpretations, and lead to non-trivial issues of just when a representation in vector spaces is possible, [48]. The restriction to the finite case has been lifted recently, but we will return to this matter later on.

Before turning to a modal perspective on independence, we note that the two abstract approaches: via dependence relations and independence predicates are equivalent. We state some relevant results, that can also be found in Matroid Theory, [20], with set-theoretic proofs in a form that might be a bit more easily accessible to logicians placed in an Appendix.

Definition 5.10. *The induced predicate I^D of a dependence relation D holds precisely for all sets X s.t. for no $x \in X$, $D_{X-\{x\}} x$.*

Fact 5.11. *The I^D are independence predicates.*

There is also a converse to this result.

Definition 5.12. *The induced relation D^I of an independence predicate I is defined as follows: $D^I_X y$ iff either (a) $y \in X$, or (b) there exists some $X' \subseteq X : I(X') \wedge \neg I(X' \cup \{y\})$.*

Fact 5.13. *The induced relation D^I is a dependence relation.*

Of course, we can also compose the two constructions I^D and D^I , but we will not continue at this level of generality in this paper. Abstract analyses like this can be seen as a sort of ‘proto-logic’: we now turn to a richer modal language which includes Boolean structure.

Remark 5.14 (Matroid theory revisited). The above results heavily depend on the use of finite sets. However, recently, [20], a natural notion of infinite matroid has been introduced. It extends the conditions for the finite case with the following second-order statement:

- (M) Take any subset X of the total domain of objects. Any independent set I contained in X can be extended to a maximally independent set *among the subsets of X* .

This is a familiar notion: well-foundedness of the inclusion order among independent sets satisfying some property. Well-founded partial orders are captured by the modal logic **S4.Grz** [21, Ch. 3], and so there might be an angle for modal logic on infinite matroids as well as finite ones. However, making this idea work would require a two-sorted language extension going well beyond what we have offered here, describing both objects and sets of objects.

5.4. A modal logic of independence. One special logical interest to the above notion of independence is its type: it is not a modal operator on formulas, but rather a *predicate* that can hold or not of a given formula. It is somewhat surprising that the two approaches turned out to have the same content set-theoretically. Let us now pursue the predicate view.

We introduce the following new syntactic construction

$$I\varphi : \varphi \text{ defines an independent set.}$$

This is truly a new notion compared to what we had before:

Fact 5.15. *I is not definable using the earlier D-modality.*

Proof. One can use the bisimulation of Example 2.14. The set of vectors $\{(1, 1), (1, -1)\}$ is independent in the model \mathfrak{M} defined there, but the contraction image $\{A, B\}$ is not independent, since we have RA, BB since we can add up the vectors $(-1, 2), (2, -1)$, both mapped to B , to obtain $(1, 1)$ in A . And RA, BB is the relational generalization of the sum assertion $A = B + B$. \square

The preceding fact means in particular that the earlier set-theoretic map I^D has no modal definition. Even so, some of the above set-theoretic conditions have reflections in the modal language, some do not. E.g., downward monotonicity is expressed by

- The fact that I is a property of sets is reflected $(\neg)I\varphi \rightarrow U(\neg)I\varphi$
- Downward monotonicity is expressed by $I\varphi \rightarrow I(\varphi \wedge \psi)$
- In addition, we have In for all nominals n except 0.

One can view I as a more complex relative of global modalities like E, U which express simple permutation-invariant properties of sets. We leave an axiomatization of its logic as an open problem.

But it may well be that the more interesting logic to analyze here is one which combines our modal syntax for dependence and independence.

Example 5.16. Here are two valid principles combining D and I which express the modally expressible directions of the earlier transformations between the abstract D and I predicates:

- $(I\varphi \wedge \neg I(\varphi \vee n)) \rightarrow E(n \wedge D\varphi)$
- $(n \wedge D\varphi \wedge I(\varphi \vee n)) \rightarrow E(n \wedge \varphi)$

Again, we leave a complete axiomatization as an open problem.

5.5. Excursion: Connections with logics of dependence and independence. The modal logics of dependence and independence presented here invite comparison with current dependence logics, [46, 6]. These logics work on sets of assignments or more abstract states where not all possible states (maps from variables to values in their ranges) need to be available in the model. In this setting, functional dependence is ‘determination’: fixing the values of X fixes the value of y uniquely on the available assignments. This semantic determination has a counterpart in functional definability: it holds iff there is a map F from values to values s.t. for all states s in the model, $s(y) = F(\mathbf{s}(X))$. This, of course, seems close to our notion of dependence as definability in a vector space.²⁹ What, in particular, the recent dependence logic LFD shares with the present paper is a modal-style approach taking a local perspective (formulas are always interpreted at a given assignment), and yielding modal-style axiomatizations.

Even so, there are also some striking differences in the notion of *independence* of y from X , whose definition in LFD is as follows at a state s : fixing the local values of X at s still leaves y free to take on all its possible values in the available assignments of the model. This is by no means the negation of local semantic dependence, which is much weaker. What is going on?

²⁹The additional requirement that the function be linear means that we are dealing with an even more demanding notion of semantic determination, which could be captured by imposing further semantic invariance properties.

We need to make a distinction here. If we define dependence in an algebraic *value setting*, then it means definability by some term in the similarity type of the algebra. Independence is then just the negation of this. This is how the notions are connected in our group and vector models. But LFD and other dependence logics *lift* this value setting to a *function setting*. Slightly rephrasing our earlier observation, the variables are really functions from ‘states’ into a value algebra, and semantic dependence of y on X is equivalent to saying that there exists a term T for a partial function in that algebra such that, for all states s , $y(s) = T[X(s)]$. In these richer function spaces, more complex notions become available, and in particular, independence now means something else from the value setting, namely, that the functions take their values independently.³⁰

Despite our distinction, vector-style value dependence could be introduced into dependence logics, or in current *causal logics* whose notions sometimes have a vector-style independence character.³¹ As for further cross-overs, our modality $I\varphi$ also makes sense in the functional setting of LFD, offering a very different approach from that in the undecidable modal logic LFD + I, [6].

6. FIELDS AND VECTOR SPACES

With our basic modal approach in place, and having made some forays into the dependence structure in vector spaces, we now turn to the modal logic of vector spaces in the full sense of our introduction. Vector spaces include a field whose members can be seen as actions, in fact, linear transformations, on the additive group of vectors. Algebraic notations for these objects serve as coefficients in linear terms defining linear transformations. In this section, we extend our earlier modal logic of groups (now thought of as the additive group of vectors) to also include this field structure. The thinking behind the formal language to follow is like that for propositional dynamic logic PDL: formulas describe properties of states, but there are also terms for actions from the field that denote transition relations between states, in our case: functions from vectors to vectors.

6.1. Language and semantics.

Definition 6.1. *The terms of the modal language of vector spaces MVL are given by the following schema, starting with some set of variables x , while 0 , 1 are individual constants:*

$$t := x \mid 0 \mid 1 \mid t + t \mid -t \mid t.t \mid t^{-1}$$

This definition also includes the term 0^{-1} or $(x + -x)^{-1}$ which do not denote objects in fields, and as a result, our semantics to come will have to deal with terms lacking a denotation.

Next we define formulas extending the earlier modal language of groups. Here, we use the new non-standard notation 0 to denote the zero vector, in order to distinguish this from the zero element of the field of the vector space.

Definition 6.2. *Formulas are defined as follows, starting with proposition letters p and nominals i from given sets, and using t to denote an arbitrary term as defined just now:*

$$\varphi := p \mid i \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathbf{E}\varphi \mid 0 \mid \langle - \rangle\varphi \mid \varphi \oplus \varphi \mid \langle t \rangle\varphi$$

Clearly, this modal language extends the earlier one of the group logic LCG. The new modality $\langle t \rangle\varphi$ describes the crucial product of vectors and field coefficients linking the two components of a vector space. Note also that the modal notation distinguishes some notions that mathematical notation for vector spaces collapses with a benign ambiguity: the zero of the field and the zero vector, product between field elements and between field elements and vectors. This prising apart is not just pedantry, since it allows us a finer look at the reasoning principles involved.

³⁰One might think that the ‘value setting/function setting’ distinction matches up with the basic distinction between vector spaces and their associated *dual spaces*. However, we have not been able to make this analogy work.

³¹E.g., [31] Halpern defines ‘causal influence’ of y on x by saying that $D_V AR - \{x\}x \wedge \neg D_V AR - \{x, y\}x$.

Remark 6.3 (More redical modalization). Our language does not treat vectors and field elements in exactly the same style. A more thorough modalization would have two sorts of objects: vectors and field elements, and instead of terms, it would have formulas that can be true or false of field elements. For an analogy, cf. the ‘arrow logic’ version of PDL in [9].

Now, we set up our semantic structures.

Definition 6.4. A vector model over a field V is a structure $\mathfrak{M} = (S, F, V, h)$ where S is a commutative group as described in Section 2 and following, F is a field, and V is a valuation for proposition letters on S . Next, the assignment map h sends basic variable terms to objects in the field F . This map can be uniquely extended to a partial map from the whole set of terms to objects in F , which will also be denoted by h . Here the convention is that (a) complex terms with undefined components do not get a value, (b) if a term t has value 0, then t^{-1} does not get a value.³²

The semantics for our language is the same as in earlier sections, with the following addition. Note here that terms t denote the same object throughout a vector model, while the modality $\langle t \rangle \varphi$ describes their effect as actions on vectors:

$$(S, V, h), v \models \langle t \rangle \varphi \quad \text{iff} \quad \text{there exists a vector } w \text{ such that}$$

$$(i) (S, V, h), w \models \varphi, \quad (ii) h(t) \cdot w \text{ is defined and equals } v$$

Remark 6.5 (Two directions). This choice of semantics needs explanation. We treat $\langle t \rangle \varphi$ in the same ‘reverse’ style here as the earlier group addition modality $\varphi \oplus \psi$ of LCG. Instead, one might have expected the ‘forward’ formulation that $h(t) \cdot v \models \varphi$ for the current point v , in analogy with the treatment of program modalities in PDL – but we found that this generates difficulties in stating perspicuous valid principles. Even so, the two styles seem expressively equivalent, as the two transition relations are converses of each other. In line with this, modulo some care with undefined terms, one can also view the syntax of our modal logic as including a two-directional *tense logic*, since the modalities $\langle t \rangle$ and $\langle t^{-1} \rangle$ function largely as converses. A reformulation of the system presented here in this bidirectional style might be of interest in its own right.

6.2. Bisimulation and expressive power. As in Section 2.3, the extended modal language MVL comes with a notion of bisimulation, where more structure now needs to be preserved. Again, we can define this between abstract structures, but the following will suffice for an illustration.

Definition 6.6. A field bisimulation between two vector models $\mathfrak{M}_1, \mathfrak{M}_2$ over possibly different sets of vectors and fields is a relation Z between vectors in the two models satisfying all the conditions of Definition 2.12 for bisimulations between group models plus the following extra item for each term t of the language and each Z -related pair v, w :

- If $v = h_1(t) \cdot v'$, then there exists a w' s.t. $v' Z w'$ and $w = h_2(t) \cdot w'$
- Likewise in the opposite direction.

Remark 6.7 (Operations that are safe for bisimulation.). In propositional dynamic logic PDL, one only needs a bisimulation between atomic actions, and this is then automatically a bisimulation for the transition relations of complex programs by the *safety* of the program operations, [16]. One might expect a similar extension property here. Indeed, it is easy to see by spelling out the preceding definition that, if Z is a field bisimulation for terms t and t' , then it is also a field bisimulation for the term $t \cdot t'$. But there are two obstacles. First, consider safety for inverse terms s^{-1} . Here reducing $v = s^{-1} \cdot w$ to $w = s \cdot v$ requires our bisimulation to also work in the converse direction. This might be solved by making field bisimulations two-sided, on the the earlier-noted analogy of our modal vector logic with a tense-logical one. However, here is one more problem. If

³²For example, assignments h are undefined on the terms 0^{-1} and $(x + (-x))^{-1}$.

Z is a field bisimulation for terms t and t' , it is not clear that Z is also a bisimulation for $t+t'$, since the assumption that $v = h_1(t+t') \cdot v'$ means that $v = h_1(t) \cdot v' + h_1(t') \cdot v'$ and the double occurrence of v' requires Z -links to the same point in the opposite model, which bisimulation typically does not guarantee. We feel that more can be said here, but must leave this for further investigation.

Fact 6.8. *Field-bisimilar points in two vector models satisfy the same MVL-formulas.*

Example 6.9. The bisimulation in Example 2.15 between $\mathbb{Q} \times \mathbb{Q}$ and \mathbb{Q} extends immediately to a field bisimulation where the values $h(t)$ are the same in both models.

Example 6.10. Some bisimulations between group models do not extend to field bisimulations. Consider the vector space \mathbb{R} over the field \mathbb{R} . The relation vZv' defined by

- $v, v' \in \mathbb{Z}$
- $v, v' \in \mathbb{R} - \mathbb{Z}$

is a bisimulation between the underlying group models. To see this, note first that (a) every $a \in \mathbb{R}$ can be written as a sum $a = u + v$ with $u, v \in \mathbb{R} - \mathbb{Z}$, (b) if $a \in \mathbb{R} - \mathbb{Z}$, then $a = u + v$ for $u \in \mathbb{Z}$ and $v \in \mathbb{R} - \mathbb{Z}$ [take $u = 0$ and $v = a$], and (c) if $a \in \mathbb{Z}$, then $a = u + v$ with $u, v \in \mathbb{Z}$ [again take $u = 0$, and $v = a$]. Now let $x, x' \in \mathbb{R}$ and xZx' . Suppose $x = y + z$. Then if $y, z \in \mathbb{R} - \mathbb{Z}$, by (a) we have $y', z' \in \mathbb{R} - \mathbb{Z}$ with $x' = y' + z'$. So we have yZy' and zZz' . If $y, z \in \mathbb{Z}$, then $x \in \mathbb{Z}$ and so $x' \in \mathbb{Z}$. Then we apply (c). Finally, if $y \in \mathbb{Z}$ and $z \in \mathbb{R} - \mathbb{Z}$, then $x = y + z$ belongs to $\mathbb{R} - \mathbb{Z}$. Therefore, $x' \in \mathbb{R} - \mathbb{Z}$ and we apply (b). The bisimulation clause for the inverse – follows from the fact $x \in \mathbb{Z}$ iff $-x \in \mathbb{Z}$. However, the relation Z is not a field bisimulation, since, say, $0 Z 1$ and $0 = 0 \cdot 1/3$, but there is no p with $1/3 Z p$, i.e., $p \in \mathbb{R} - \mathbb{Z}$, such that $0 Z (1 \cdot p)$, i.e., such that $p \in \mathbb{Z}$.

We will not continue with model-theoretic aspects of vector models here. Our focus in the rest of this section will be on valid reasoning principles.

6.3. Exploring the valid principles of modal vector logic. Before stating any formal results, we will first discuss some crucial valid principles in the system MVL just defined. As we have included the earlier system LCG for vector addition, everything we have seen about that remains true here. Our discussion will be in a semi-formal style, so as to motivate the later formal proof system where things will be made more precise.

First, we consider *definedness of terms*. The formula

$$E\langle s \rangle \top$$

holds at a point (in fact, at any point) if some vector x equals $s \cdot y$ for some vector y . Given our semantics, definedness of a term holds globally, so our formula expresses that the value of the term s is defined. But then we can express all our stipulations for definedness of terms as principles in our modal language. For instance, the formula

$$E\langle s + t \rangle \top \leftrightarrow (E\langle s \rangle \top \wedge E\langle t \rangle \top)$$

says that sum terms are defined iff their summands are. The most complex case here was that of terms s^{-1} for multiplicative inverse. This time, s does not just need to be defined, but its value must also not be the additive zero-element of the field. For this, we can use the following formula:

$$E(-0 \wedge \langle s \rangle \top)$$

This says that the value of the term s is defined, but also that some vector can be multiplied by s to produce a non-zero vector. This can only happen if the value of s differs from the additive zero of the field, given the definition of vector spaces.

Next, consider the field structure. In our style of semantics, the structure of field elements is represented indirectly through the structure of the associated linear transformations on vectors.³³ Accordingly, we must first discuss *linear transformations* $s \cdot x$. First, we can make sure that the linear transformation associated with a field element s is a *function*

$$\langle t \rangle i \wedge \varphi \rightarrow \mathbf{U}(\langle t \rangle i \rightarrow \varphi)$$

Next, we consider the two basic distributive laws of vector spaces that regulate the modality $\langle s \rangle$. First, the algebraic identity $a \cdot (x + y) = a \cdot x + a \cdot y$ underlies the following fact:

$$\langle t \rangle (\varphi \oplus \psi) \leftrightarrow (\langle t \rangle \varphi \oplus \langle t \rangle \psi) \text{ is valid}$$

Proof. From left to right, if $v = h(t) \cdot w$ with $w \models \varphi \oplus \psi$, then $w = x + y$ for some $y \models \varphi, z \models \psi$. So, $v = h(t) \cdot x + h(t) \cdot y$ and the right hand side follows. From right to left, if $v = x + y$ with $x \models \langle t \rangle \varphi$ and $y \models \langle t \rangle \psi$ then $x = a \cdot x'$ for some $x' \models \varphi$, and $y = a \cdot y'$ for some $y' \models \psi$, and using the algebraic equality once more, $v = a \cdot (x' + y')$ and the left-hand side follows. \square

Next consider the second distributive law $(a + b) \cdot x = a \cdot x + b \cdot x$. The modal formula $\langle s + t \rangle \varphi \rightarrow (\langle s \rangle \varphi \oplus \langle t \rangle \varphi)$ is valid. If $v = (s + t) \cdot w$ with $w \models \varphi$, then $v = s \cdot w + t \cdot w$, which implies the right-hand side. But the converse $(\langle s \rangle \varphi \oplus \langle t \rangle \varphi) \rightarrow \langle s + t \rangle \varphi$ is not valid.³⁴ However, it is easy to see the following fact, replacing the formula φ which can hold at more than one point by a nominal denoting a single point, thereby staying closer to our distribution law:

$$\langle s + t \rangle i \leftrightarrow (\langle s \rangle i \oplus \langle t \rangle i) \text{ is valid}$$

In our later axiom system, we will use this principle strengthened by a rule of substitution for ‘point formulas’ denoting unique vectors, which are our modal analogue of algebraic terms.

What remains is to see which valid principles express the definition of a *field*. For the *additive structure* of the field, to some extent, the earlier distribution laws help us enlist the additive structure of the vectors.³⁵ Here is an illustration, showing how our modal language works.

Associativity for nominals can be demonstrated as follows. The formula $\langle s + (t + u) \rangle i$ is equivalent, using the last distribution principle mentioned above twice, to $\langle s \rangle i \oplus (\langle t \rangle i \oplus \langle u \rangle i)$ and now we can use the associativity of \oplus in LCG (and hence DVL) and then use the distribution equivalence backwards. *Commutativity* can be derived in a similar manner. As we shall see later, our informal discussion here will be reflected in formal derivations in our proof system, where we can even replace the nominal i by arbitrary formulas φ .

This leaves the zero element of the field, for which we have the valid equivalence

$$\langle 0 \rangle \varphi \leftrightarrow (0 \wedge \mathbf{E}\varphi)^{36}$$

With this in place, the modal form of the valid identity $t + (-t) = 0$ will follow directly from the properties of vector inverse by the following clearly valid formula

$$\langle -t \rangle \varphi \leftrightarrow \langle - \rangle \langle t \rangle \varphi$$

³³Readers who know propositional dynamic logic may find the analogy helpful with the way denotations for program expressions are defined as binary transition relations between states.

³⁴For a counter-example, take the rationals, set $a = 0.5, b = 1$ and let φ be true just at 1, 2. The vectors 0.5 and 2 satisfy $\langle a \rangle \varphi$ and $\langle b \rangle \varphi$, respectively, but their sum 2.5 is not a 1.5 multiple of any point satisfying φ .

³⁵Many algebraic structures can be represented in Linear Algebra, as shown in the rich area of Representation Theory, [23]. We believe that many such representation results have natural reflections in logic.

³⁶This may even be formally derivable, but we are not aiming for an absolutely minimal presentation here.

It remains to deal with the *multiplicative structure* of the field. Some properties of the product operation are again immediate. In particular, *associativity* follows merely through the syntactic properties of our modal language. We have that

$$\langle s \cdot (t \cdot u) \rangle \varphi \leftrightarrow \langle s \rangle \langle t \cdot u \rangle \varphi \leftrightarrow \langle s \rangle \langle t \rangle \langle u \rangle \varphi, \quad \text{which can be recombined to } \langle s \cdot t \rangle \langle u \rangle \varphi$$

In addition, the following modal principle is obviously valid for the unit element:

$$\langle 1 \rangle \varphi \leftrightarrow \varphi$$

However, in general, algebraic properties of the field product cannot be read off from the additive structure of the vectors. For instance, there is no easy derivation for *commutativity*. One will just have to postulate the following valid equivalences as principles in our system:

$$\langle s \rangle \langle t \rangle \varphi \leftrightarrow \langle t \rangle \langle s \rangle \varphi^{37}$$

The hardest task remaining arises with the properties of division in a field, i.e., the inverse of the product operation. We need to find a modal equivalent for the algebraic equality $t \cdot t^{-1} = 1$ based on an understanding of how inverse functions. Here a first observation is that we can partially define the modality for term inverse in line with our truth definition. Precise details of the relevant principles are found in our proof system, but here is one useful validity, where the second conjunct to the right is the above definition for the term s being defined and having a non-zero value:

$$(i \wedge \langle s^{-1} \rangle j) \leftrightarrow (\mathbf{E}(j \wedge \langle s \rangle i) \wedge \mathbf{E}(-\mathbf{0} \wedge \langle s \rangle \top))$$

For the law of inverses, using the preceding principle or by direct inspection, we get the validity

$$\mathbf{E}(-\mathbf{0} \wedge \langle s \rangle \top) \rightarrow \langle s \rangle \langle s^{-1} \rangle \varphi \leftrightarrow \varphi^{38}$$

Remark 6.11. The preceding observations can be summed up in the following modal *frame correspondence result*. When interpreted in terms of their frame truth, the preceding principles express exactly that an abstract bimodal modal with a product map is a vector space. We do not provide details for this result, since the proof of our completeness theorem to follow is more informative about the content of our modal system.

6.4. A complete proof system. With the preceding analysis in place, we can now introduce a formal proof system. But first, we define a useful auxiliary notion of *point formulas* as follows:

- (i) nominals are point formulas,
- (ii) if P is a point formula, then so is $\langle s \rangle P$, for every term s .

In our semantics, when defined, point formulas clearly just denote one vector, so they function in our modal language as counterparts to algebraic terms over the field.

Definition 6.12. *The proof calculus of dynamic vector logic DVL consists of*

- All axioms and rules of the proof system LCG from Section 3, now for the present language.
- The following additional modules:
 - (a) Axioms for definedness of terms:
 - (a1) $\mathbf{E}\langle s + t \rangle \top \leftrightarrow \mathbf{E}\langle s \rangle \top \wedge \mathbf{E}\langle t \rangle \top$
 - (a2) $\mathbf{E}\langle s \cdot t \rangle \top \leftrightarrow \mathbf{E}\langle s \rangle \top \wedge \mathbf{E}\langle t \rangle \top$
 - (a3) $\mathbf{E}\langle -s \rangle \top \leftrightarrow \mathbf{E}\langle s \rangle \top$

³⁷This may be a momentous move for the complexity of our system, since multimodal logics with the universal modality plus commutation axioms are usually *undecidable*, [40].

³⁸In fact the direction from left to right does not need the antecedent condition here.

$$(a4) \ E\langle s^{-1} \rangle \top \leftrightarrow E(\neg 0 \wedge \langle s \rangle \top).$$

(b) *Axioms for coefficient-vector product:*

$$(b1) \ \langle s \rangle (\varphi \vee \psi) \leftrightarrow \langle s \rangle \varphi \vee \langle s \rangle \psi$$

$$(b2) \ \langle s \rangle \varphi \rightarrow E\varphi$$

$$(b3) \ E(\neg 0 \wedge \langle s \rangle \top) \rightarrow (\langle s \rangle \neg \varphi \leftrightarrow (\langle s \rangle \top \wedge \neg \langle s \rangle \varphi))$$

$$(b4) \ \langle s \cdot t \rangle \varphi \leftrightarrow \langle s \rangle \langle t \rangle \varphi$$

$$(b5) \ \langle t \rangle (\varphi \oplus \psi) \leftrightarrow (\langle t \rangle \varphi \oplus \langle t \rangle \psi)$$

$$(b6) \ \langle s + t \rangle i \leftrightarrow \langle s \rangle i \oplus \langle t \rangle i$$

(c) *Further laws for field addition and multiplication:*

$$(c1) \ \langle 0 \rangle \varphi \leftrightarrow (0 \wedge E\varphi)$$

$$(c2) \ \langle 1 \rangle \varphi \leftrightarrow \varphi$$

$$(c3) \ \langle -s \rangle \varphi \leftrightarrow \langle - \rangle \langle s \rangle \varphi$$

$$(c4) \ \langle s \cdot t \rangle \varphi \leftrightarrow \langle t \cdot s \rangle \varphi$$

$$(c5) \ (i \wedge \langle s^{-1} \rangle j) \leftrightarrow (E(\neg 0 \wedge \langle s \rangle \top) \wedge E(j \wedge \langle s \rangle i))$$

$$(c6) \ (E(\neg 0 \wedge \langle s \rangle \top) \wedge i) \rightarrow \langle s^{-1} \rangle \langle s \rangle i$$

- *The additional rules of inference for DVL over LCG are as follows.*

Necessitation Rules: $\frac{\neg \varphi}{\langle s \rangle \varphi}$ for each term s

Extra Witness Rule: $\frac{\langle s \rangle (j \wedge \varphi) \rightarrow \theta}{\langle s \rangle \varphi \rightarrow \theta}$, where the nominal j does not occur in φ or θ .

Substitution Rule: *Nominals in provable formulas can be replaced by point formulas.*

The reader may have missed some obvious counterparts of field axioms in the preceding list, but these turn out to be derivable in the system as presented here. Before giving examples and details, we state two facts that will be used throughout.

Lemma 6.13.

- $\vdash U(\varphi \leftrightarrow \psi) \rightarrow U(\chi \leftrightarrow \chi[\varphi/\psi]).$
- *If $\vdash \langle s \rangle i \leftrightarrow \langle t \rangle i$, then $\vdash \langle s \rangle \varphi \leftrightarrow \langle t \rangle \varphi$*

Proof. The first fact is standard for modal logics with global modalities. The second fact may be seen as follows. Let j be a nominal not occurring in φ . By the substitution rule, we have $\vdash \langle s \rangle j \leftrightarrow \langle t \rangle j$. Therefore, $\langle s \rangle (j \wedge \varphi)$ implies $\langle t \rangle j$. We also have the hybrid law $E(j \wedge \varphi) \rightarrow U(j \rightarrow \varphi)$. Therefore we get $\langle t \rangle \varphi$. Now apply the Witness Rule for modalities $\langle s \rangle$ to get the desired conclusion. \square

Example 6.14. Here are some derivable formulas in the logic DVL:

- (1) $\langle (s + t) + u \rangle \varphi \leftrightarrow \langle s + (t + u) \rangle \varphi$
- (2) $\langle s + t \rangle \varphi \leftrightarrow \langle t + s \rangle \varphi$
- (3) $\langle s + 0 \rangle \varphi \leftrightarrow \langle s \rangle \varphi$
- (4) $\langle s + (-s) \rangle \varphi \leftrightarrow \langle 0 \rangle \varphi$
- (5) $\langle (s \cdot t) \cdot u \rangle \varphi \leftrightarrow \langle s \cdot (t \cdot u) \rangle \varphi$
- (6) $\langle s \cdot 1 \rangle \varphi \leftrightarrow \langle s \rangle \varphi$
- (7) $\langle s \cdot (t + u) \rangle \varphi \leftrightarrow \langle s \cdot t + s \cdot u \rangle \varphi$
- (8) $E(\neg 0 \wedge \langle s \rangle \top) \rightarrow (\langle s^{-1} \cdot s \rangle \varphi \leftrightarrow \langle 1 \rangle \varphi).$

For all the equivalences here, by Lemma 6.13, it suffices to show the case where φ is a nominal i . (i) E.g. for principle (2), $\langle s+t \rangle i$ is provably equivalent to $\langle s \rangle i \oplus \langle t \rangle i$ by Axiom (b6), which is equivalent to $\langle t \rangle i \oplus \langle s \rangle i$ by the commutativity of \oplus in the proof system LCG, and using Axiom (b6) once more, we derive $\langle t+s \rangle i$. (ii) $\langle (s \cdot t) \cdot u \rangle i \leftrightarrow \langle s \cdot (t \cdot u) \rangle i$ is proved by applying Axiom (b4) a number of times and recombining in an obvious way. (iii) $\langle s + (-s) \rangle i \leftrightarrow \langle 0 \rangle i$ is proved as follows. Using Axiom (c1) we can replace $\langle 0 \rangle i$ by $0 \wedge E i$, where the right-hand conjunct is provable, whence we get the provable equivalent 0 . The left-hand side $\langle s + (-s) \rangle i$ is provably equivalent to $\langle s \rangle i \oplus \langle -s \rangle i$ and so, by Axiom (c3), to $\langle s \rangle i \oplus \langle - \rangle \langle s \rangle i$ which is provably equivalent to 0 already in the initial proof system LCG. (iv) Principle (8) simplifies up to provable equivalence to $E(-0 \wedge \langle s \rangle \top) \rightarrow (\langle s^{-1} \rangle \langle s \rangle \varphi \leftrightarrow \varphi)$, and by a reasoning similar to that establishing Lemma 6.13.(ii) it suffices to derive the nominal form $E(-0 \wedge \langle s \rangle \top) \rightarrow (\langle s^{-1} \rangle \langle s \rangle i \leftrightarrow i)$. From left to right, we assume $j \wedge \langle s^{-1} \rangle \langle s \rangle i$, and use Axiom (c5), substituting the point formula $\langle s \rangle i$ for i , to derive $j \wedge E(\langle s \rangle i \wedge \langle s \rangle j)$, which implies in hybrid logic that $E(i \wedge j)$, which together with j implies i . Then we drop the assumption j by the Naming Rule. For the direction from right to left, we appeal to Axiom (c6).³⁹

Theorem 6.15. *The proof calculus DVL is sound and complete for validity in vector models.*

Proof. Soundness is obvious from the earlier semantic explanation of the axioms.

The proof of completeness follows the same pattern as that of Theorem 3.8 for the logic LCG w.r.t. commutative groups, so we suppress details of the proof that work analogously. We start with some consistent set Σ and create a family of maximally consistent sets forming one equivalence class of the modal accessibility relation for the global modalities that are each named by a nominal, and where additional nominals witness the new modalities in our system. In particular we have a designated *guidebook*: a maximally consistent set Σ^\bullet containing Σ which contains all the information that is needed to create a vector model as desired.

As before, we first use the guidebook to define a commutative additive group on the maximally consistent sets, viewed as standing for vectors. Next, we need to define a field.

We first define an equivalence relation $s \sim t$ on terms of our language by setting

$$s \sim t \quad \text{iff} \quad U(\langle s \rangle P \leftrightarrow \langle t \rangle P) \in \Sigma^\bullet \quad \text{for every point formula } P$$

The elements of our field will be the equivalence classes $[t]^\sim$ of this relation for *defined terms* t in the sense of having the formula $E\langle t \rangle \top$ present in Σ^\bullet .

Remark 6.16. As a consequence of our definition, two equivalent terms s, t are either both defined or both undefined according to the guidebook. Suppose that $E\langle s \rangle \top \in \Sigma^\bullet$. Then by our witness construction, some maximally consistent set Γ exists named by a unique nominal j s.t. $\langle s \rangle \top \in \Gamma$, and this again implies the existence of a maximally consistent set Δ named by some k such that $E(j \wedge \langle s \rangle k) \in \Sigma^\bullet$. Now by the definition of $s \sim t$, $U(\langle s \rangle k \leftrightarrow \langle t \rangle j) \in \Sigma^\bullet$. But then by the properties of derivability in DVL, $E(j \wedge \langle t \rangle j) \in \Sigma^\bullet$, which in its turn implies $E\langle t \rangle \top \in \Sigma^\bullet$. By similar reasoning, we see that in fact, the following formulas must be in Σ^\bullet :

$$U(E\langle s \rangle \top \leftrightarrow E\langle t \rangle \top), \quad U(E(-0 \wedge \langle s \rangle \top) \leftrightarrow E(-0 \wedge \langle t \rangle \top))$$

Next, we must define the field operations on these equivalence classes. This can be done in the obvious way, setting, for instance, $[s]^\sim + [t]^\sim$ equal to $[s+t]^\sim$, and so on for all other functions in the signature. However, to see that this is well-defined, we must show a number of facts:

Lemma 6.17. *For all terms s, s', t, t' we have:*

$$(1) \quad \text{If } s \sim s' \text{ and } t \sim t', \text{ then } s + t \sim s' + t',$$

³⁹For another exercise, the reader may want to prove $E(-0 \wedge \langle s \rangle \top) \rightarrow U(\langle s^{-1} \rangle \top \wedge \langle s \rangle \top)$. Incidentally, we have not aimed for a minimal set of principles for inverse in the system DVL, and simplifications may be possible.

- (2) If $s \sim s'$ and $t \sim t'$, then $s \cdot t \sim s' \cdot t'$,
 (3) If $s \sim t$, then $-s \sim -t$,
 (4) If $s \sim t$, then $s^{-1} \sim t^{-1}$.

Proof. We will rely heavily on theorems in DVL which either belong automatically to Σ^\bullet , or justify closure properties of the guidebook.

For (1), let $s \sim s'$, $t \sim t'$. Then we have $\mathbf{U}(\langle s \rangle P \leftrightarrow \langle s' \rangle P) \in \Sigma^\bullet$ and $\mathbf{U}(\langle t \rangle P \leftrightarrow \langle t' \rangle P) \in \Sigma^\bullet$, for every point formula P . But the formula $\mathbf{U}(\langle s \rangle P \leftrightarrow \langle s' \rangle P) \wedge \mathbf{U}(\langle t \rangle P \leftrightarrow \langle t' \rangle P) \rightarrow \mathbf{U}(\langle s + t \rangle P \leftrightarrow \langle s' + t' \rangle P)$ is a theorem of DVL. Therefore, $\mathbf{U}(\langle s + t \rangle P \leftrightarrow \langle s' + t' \rangle P) \in \Sigma^\bullet$, and so $s + t \sim s' + t'$.

For (2), let $s \sim s'$, $t \sim t'$. Then we have $\mathbf{U}(\langle s \rangle P \leftrightarrow \langle s' \rangle P) \in \Sigma^\bullet$ and $\mathbf{U}(\langle t \rangle P \leftrightarrow \langle t' \rangle P) \in \Sigma^\bullet$, for every point formula P . We also have $\mathbf{U}(\langle s \cdot t \rangle P \leftrightarrow \langle s \rangle \langle t \rangle P) \in \Sigma^\bullet$. Then $\mathbf{U}(\langle s \rangle \langle t \rangle P \leftrightarrow \langle s \rangle \langle t' \rangle P) \in \Sigma^\bullet$ and thus $\mathbf{U}(\langle s \rangle \langle t \rangle P \leftrightarrow \langle s' \rangle \langle t' \rangle P) \in \Sigma^\bullet$.⁴⁰ So $\mathbf{U}(\langle s \cdot t \rangle P \leftrightarrow \langle s' \rangle \langle t' \rangle P) \in \Sigma^\bullet$, and hence $s \cdot t \sim s' \cdot t'$.

For (3), let $s \sim t$. Then $\mathbf{U}(\langle s \rangle P \leftrightarrow \langle t \rangle P) \in \Sigma^\bullet$, and hence also $\mathbf{U}(\langle - \rangle \langle s \rangle P \leftrightarrow \langle - \rangle \langle t \rangle P) \in \Sigma^\bullet$. But we also have $\mathbf{U}(\langle -s \rangle P \leftrightarrow \langle - \rangle \langle s \rangle P) \in \Sigma^\bullet$, $\mathbf{U}(\langle -t \rangle P \leftrightarrow \langle - \rangle \langle t \rangle P) \in \Sigma^\bullet$ as instances of theorems. Therefore, $\mathbf{U}(\langle -s \rangle P \leftrightarrow \langle -t \rangle P) \in \Sigma^\bullet$ and $-s \sim -t$.

For (4), let $s \sim t$. We have to show that $\mathbf{U}(\langle s^{-1} \rangle P \leftrightarrow \langle t^{-1} \rangle P) \in \Sigma^\bullet$. Axiom (c5) plus the Substitution Rule for the point term P and Necessitation for \mathbf{U} gives us the theorem $\mathbf{U}((i \wedge \langle s^{-1} \rangle P) \leftrightarrow (\mathbf{E}(-0 \wedge \langle s \rangle \top) \wedge \mathbf{E}(P \wedge \langle s \rangle i)))$, which will then be in Σ^\bullet . Now we have $\mathbf{U}(\langle s \rangle P \leftrightarrow \langle t \rangle P) \in \Sigma^\bullet$, and therefore also the formula $\mathbf{U}((i \wedge \langle s^{-1} \rangle P) \leftrightarrow (\mathbf{E}(-0 \wedge \langle s \rangle \top) \wedge \mathbf{E}(P \wedge \langle t \rangle i)))$. Moreover, by Remark 6.16, we have $\mathbf{U}(\mathbf{E}(-0 \wedge \langle s \rangle \top) \leftrightarrow \mathbf{E}(-0 \wedge \langle t \rangle \top)) \in \Sigma^\bullet$, and we immediately also get $\mathbf{U}((i \wedge \langle s^{-1} \rangle P) \leftrightarrow (i \wedge \langle t^{-1} \rangle P)) \in \Sigma^\bullet$. It remains to remove the nominal i . We show this in one direction only [the other is symmetric] by appealing to the following closure property:.

Claim 6.18. For each formula φ , if $\mathbf{U}(i \rightarrow \varphi) \in \Sigma^\bullet$ for all nominals i not in φ , then $\mathbf{U}\varphi \in \Sigma^\bullet$.

Proof. We can assume, thanks to the Witness Rules in DVL that, if $\mathbf{E}\varphi \in \Sigma^\bullet$, then there is a maximal consistent set Δ containing φ which is named by some nominal k that does not occur in φ . In other words, $\mathbf{E}(k \wedge \varphi) \in \Sigma^\bullet$. Now we show that $\mathbf{U}\varphi \in \Sigma^\bullet$. Let $\mathbf{U}\varphi \notin \Sigma^\bullet$. Then by maximal consistency, $\mathbf{E}\neg\varphi \in \Sigma^\bullet$. But the preceding observation about witnessing nominals in the set Σ^\bullet then gives a formula $\mathbf{E}(k \wedge \neg\varphi) \in \Sigma^\bullet$ with k not occurring in $\neg\varphi$, and we arrive at a contradiction. \square

This completes the proof of Lemma 6.17. \square

Given the preceding well-defined operations $+$, $-$, \cdot on equivalences classes of terms, our next task is to show that these classes form a field.

Lemma 6.19. The set $\mathbb{F} = \{[t]^\sim : \mathbf{E}\langle t \rangle \top \in \Sigma^\bullet\}$ forms a field.

Proof. We need to check that all the axioms of a field are satisfied according to what is present in the guidebook Σ^\bullet . In principle, this is taken care of by either explicit axioms in DVL or derivable theorems in the list of Example 6.14. We only display two examples. (a) For associativity, consider the set $([s]^\sim + [t]^\sim) + [u]^\sim$. By the above definition, this equals $[(s + t) + u]^\sim$. We need to show that this set coincides with $[s + (t + u)]^\sim$. That is, we have to show that $(s + t) + u \sim s + (t + u)$. This means that $\mathbf{U}(\langle (s + t) + u \rangle P \leftrightarrow \langle s + (t + u) \rangle P) \in \Sigma^\bullet$, for every point formula P . But this follows immediately from the derivable associativity theorem about field addition listed as Example 6.14.(1). (b) Likewise, to verify that $[s]^\sim \neq 0$ implies $[s]^\sim \cdot ([s]^\sim)^{-1} = [1]^\sim$, we use Axiom (c6) and item (8) in the list of derivabilities in Example 6.14. \square

Given this definition of the field, the *assignment function* h of our model is now straightforward: for all terms t with $\mathbf{E}\langle t \rangle \top \in \Sigma^\bullet$, we set $h(t) = [t]^\sim$.

⁴⁰Here we make crucial use of the fact that, if P is a point formula, then so is $\langle t \rangle P$.

Lemma 6.20. *The assignment function h is well-defined.*

Proof. We need to show that h is defined in the sense of Definition 6.4 for every term t such that $E\langle t \rangle \top \in \Sigma^\bullet$. This is easily done by induction on terms starting with basic variables by using the axioms of DVL that govern definedness of terms. \square

Our next task is to define the *field-vector product* of field elements and vectors in the sense of our syntactic model. This requires a little twist given our semantics for the modality $\langle t \rangle \varphi$. Let us assume that the set Δ is named by the nominal i . Then we set:

$$[t]^\sim \cdot \Delta = \{\alpha \mid E(\langle t \rangle i \wedge \alpha) \in \Sigma^\bullet\}$$

Given our Functionality axiom for the field modalities $\langle t \rangle$, it is easy to see that this stipulation defines a unique maximally consistent set.

The product thus defined satisfies the distribution axioms for vector spaces.

Lemma 6.21. *The set of all named maximal consistent sets Δ such that $E\langle t \rangle i \in \Sigma^\bullet$, where i is the nominal naming Δ forms a vector space over \mathbb{F} .*

Proof. Again we rely on the proof principles available in the calculus DVL. For an illustration, we spell out the case of $[t]^\sim \cdot (\Delta + \Gamma) = [t]^\sim \cdot \Delta + [t]^\sim \Gamma$. The argument that follows here looks complex, but it consists essentially in just spelling out definitions.

Suppose that the name of Δ is j and the name of Γ is k . As in the completeness proof for LCG, there is a unique maximally consistent set forming the vector sum $j \oplus k$, named by m say, where we have $E(m \wedge j \oplus k)$ in the guidebook Σ^\bullet . Now by the definition of field-vector product, the function value on the left-hand side is $\{\alpha \mid E(\langle t \rangle m \wedge \alpha) \in \Sigma^\bullet\}$. Using some basic hybrid principles for nominals and global modalities, we can also view this set as $\{\alpha \mid E(\langle t \rangle (j \oplus k) \wedge \alpha) \in \Sigma^\bullet\}$.

Next consider the right-hand side of our equality. Let n_1 be the name for the maximally consistent set $[t]^\sim \cdot \Delta$, and n_2 for $[t]^\sim \Gamma$. Again by the presence of unique sums of vectors in our model, there is a maximally consistent set m' s.t. the following three formulas are in the guidebook Σ^\bullet : $E(m' \wedge n_1 \oplus n_2)$, $E(n_1 \wedge \langle t \rangle j)$, $E(n_2 \wedge \langle t \rangle k)$. With some obvious manipulations in the logic, we can view the set associated with m' as $\{\alpha \mid E(\langle t \rangle j \oplus \langle t \rangle k \wedge \alpha) \in \Sigma^\bullet\}$.

With this description, the only difference is the presence of the formula $\langle t \rangle (j \oplus k)$ on the left, and $\langle t \rangle j \oplus \langle t \rangle k$ on the right. But these are provably equivalent by Axiom (b5).

The case of the other distribution law is similar. \square

It remains to prove a *Truth Lemma* for DVL in the same format as the one for the system LCG in Section 3, now with respect to the vector model \mathfrak{M} defined by combining all the above definitions.

Lemma 6.22 (Truth lemma). *Let Δ be the maximal consistent set named by the nominal i . Then*

$$\mathfrak{M}, \Delta \models \varphi \text{ iff } E(i \wedge \varphi) \in \Sigma^\bullet \text{ for all formulas } \varphi$$

Proof. As before, a straightforward induction on formulas φ is all that is required. \square

The completeness theorem now follows from the Truth Lemma and Lemma 6.21. \square

6.5. Discussion: concretizations and extensions. We end by discussing some variations on the style of analysis presented here. First, it may be possible to simplify our axiom system still further, in the spirit of the discussion of hybrid logic and links with complex algebra in Section 3.3. We will not pursue this proof-theoretic line here. Instead, we mention a few other topics.

Concretizations. A concrete version of our system arises when we *fix the field F* we are working on, say, the rationals or the reals, drop the algebraic terms, and just add names for the elements of our field to our language, making the modalities $\langle a \rangle \varphi$ refer to concrete elements $a \in F$. We will

still have completeness now, be it that the above construction becomes easier since we have the field present as it is in the terms of the language.

Alternatively, one may consider *concrete classes of fields*, e.g., those with a finite characteristic. There are some issues how to formulate this. We could express, say, $1 + 1 = 0$ in terms of nominals as $i \oplus i \leftrightarrow i$, but we can also use the more modal-style axiom $\mathbf{E}\varphi \rightarrow \mathbf{E}((\varphi \oplus \varphi) \wedge 0)$. However, we do not know yet how such structural properties can be built into our completeness proof.

A perhaps more ambitious concrete result would be an analogue of the Tarski-McKinsey Theorem for modal topology, where the reals, or any metric space without isolated points, are complete for the logic. Do invalid principles in our logic always have counterexamples in a restricted class of vector spaces, maybe only countable ones?

The pure modal fragment. Our completeness proof depends heavily on the use of nominals and global modalities, which allow us to reproduce elementary reasoning in linear algebra. Accordingly, it resembles a Henkin-style completeness proof for a fragment of a first-order language more than a modal canonical model argument. Can we also axiomatize the pure modal logic of vector spaces in an illuminating way? Axiomatizing this fragment of our hybrid modal language might need a much deeper algebraic analysis of axioms than we have provided.

Language extensions. The simple hybrid modal language of DVL stays close to the similarity type and algebraic laws for vector spaces. The most urgent issue for this paper is clearly how to add the earlier *dependence* and *independence* modalities of Section 5 to our language. This is a natural companion to the explicit field coefficients in DVL, and adds expressive power about undefinability. We have not yet found the right way of achieving this combination. ⁴¹

7. FURTHER DIRECTIONS

Richer languages for more linear algebra structures Our modal languages so far only describe the basic structure of vector spaces. Our languages do not talk yet about such important notions as bases, dimension, angles, orthogonality, inner product, outer product, eigenvectors, and other staples of linear algebra. While some of these notions have been studied by logicians, cf. [27] on modal logics of abstract orthogonality, and [36] for uses of angles between vectors, a stepwise incorporation into our framework remains to be undertaken. A further direction of analysis would be to determine what minimal logical formalisms are needed to represent and derive basic benchmark results in linear algebra such as the Dimension Theorem for linear maps [30], the sufficiency of orthonormal bases, or other highlights of its elementary theory.

Bringing linear transformations and group actions into the logic One extension seems particularly natural, given our logic for vector spaces where elements a of a field are linear transformations on the set of vectors. Structure-preserving maps are internalized into a logical language in dynamic topological logic, [34], which adds an abstract modality $\langle F \rangle$ referring to a continuous function on the state space which commutes with the modality for topological interior. In the same style, we could analyze logics of maps F satisfying commutation axioms such as

$$\langle F \rangle(\varphi \oplus \psi) \leftrightarrow (\langle F \rangle\varphi \oplus \langle F \rangle\psi)$$

Also on this road toward abstraction, in Section 6, we stressed analogies between our logic for vector spaces with propositional dynamic logic of actions on a state space. This analogy suggests an interest to logics of arbitrary groups of actions over any class of models.

However, one can also be more concrete in extending the languages studied in Section 6. Given a basis, linear transformations are given by *matrices*, so we can also put matrices inside our modalities, either concrete or in symbolic form, and work with natural axioms such as the following:

⁴¹One might also increase expressive power by exploiting the analogy with the dynamic program modalities of PDL further, for instance by introducing iterative operations on terms, suitably interpreted on vector models.

$$\langle \mathbf{M}_1 \rangle \langle \mathbf{M}_2 \rangle \varphi \leftrightarrow \langle \mathbf{M}_1 \times \mathbf{M}_2 \rangle \varphi$$

One could view the resulting systems as combining general logical reasoning about patterns in vector spaces with concrete computations in linear algebra involving matrices and vectors. A further development of this perspective must be left to a future occasion.

8. CONCLUSION

This paper has presented a first exploration of modal structures in groups and vector spaces. We have shown how notions and techniques of bisimulation and modal-style axiomatization apply, with some adjustments to the special topic. Also, we found new modal logics in the process, e.g., of linear closure and dependence, or of field multiples, that seem interesting in their own right.

Our treatment left many technical questions open. For instance, we did not axiomatize the purely modal fragments of our languages without hybrid nominals, and we also left questions about axiomatizing linear closure in functional structures. We also did not pursue the model theory of group models and vector spaces in their own terms. Perhaps most importantly, we have not investigated matters of *decidability* and computational complexity for our systems.⁴²

But perhaps the most relevant questions concern the point of a modal approach to vector spaces. So far, we have captured only very little of Linear Algebra, up to dependence, independence and matrices. We did not formalize further powerful notions such as inner products, orthogonality, or eigenvectors, and our logics do not yet represent basic results at the heart of Linear Algebra.

One can think about this distance to the target in several ways. If a logical approach faithfully copies an existing mathematical theory, it may just offer restatement in another syntax.⁴³ However, one could see distance also as a beneficial source of new abstract structures and perspectives, as in our discussion of bisimulations for vector spaces. This might be comparable to the way in which non-vector models for Matroid Theory are considered a benefit rather than a drawback.

Finally, another way of continuing the program of this paper might be to stick with the simple modal-style apparatus that we have introduced, not logicize much more of the structure of vector spaces, and then rather *combine* these logics with a computational component from Linear Algebra, in the cooperative style of ‘qualitative plus quantitative’ advocated in [13].

Acknowledgements For interesting comments and suggestions we thank Alexandru Baltag, Peter van Emde Boas, Valentin Goranko, Hannes Leitgeb and Anand Pillay. A preliminary version of this paper was presented at the workshop “Logics with Vector Space Models” organized by Fenrong Liu and Lingyuan Ye at the Joint Research Center in Logic at Tsinghua University (November 2020). We thank the organizers and attendees for a warm atmosphere and stimulating discussions.

REFERENCES

- [1] M Aiello, I. Pratt-Hartmann, and J. van Benthem, editors. *Handbook of Spatial Logics*. Springer, 2007.
- [2] M. Aiello and J. van Benthem. A modal walk through space. *J. Appl. Non Class. Logics*, 12(3-4):319–364, 2002.
- [3] C. Areces and B. ten Cate. Hybrid logics. In P. Blackburn, J. van Benthem, and F. Wolter, editors, *Handbook of Modal Logic*, volume 3 of *Studies in logic and practical reasoning*, pages 821–868. North-Holland, 2007.
- [4] P. Balbiani, V. Goranko, R. Kellerman, and D. Vakarelov. Logical theories for fragments of elementary geometry. In *Handbook of spatial logics*, pages 343–428. Springer, 2007.
- [5] A. Baltag, Z. Christoff, R. Rendsvig, and S. Smets. Dynamic epistemic logics of diffusion and prediction in social networks. *Stud Logica*, 107(3):489–531, 2019.
- [6] A. Baltag and J. van Benthem. A simple logic of functional dependence. *J. Philos. Log.*, 50(5):939–1005, 2021.
- [7] J. van Benthem. Correspondence theory. In *Handbook of philosophical logic*, pages 167–247. Springer, 1984.

⁴²It may be the case that the ‘grid structure’ of vector spaces poses serious obstacles here, [16, Ch. 6].

⁴³Faithful formalization can be helpful for developing automated deduction tools of course. And sometimes also, deep foundational results emerges in this way, such as Tarski’s analysis of elementary geometry, showing its decidability and precise algebraic content in real-closed fields.

- [8] J. van Benthem. *Language in Action: Categories, Lambdas and Dynamic Logic*. MIT Press, 1995.
- [9] J. van Benthem. *Exploring Logical Dynamics*. Studies in logic, language and information. CSLI, 1996.
- [10] J. van Benthem. Modal frame correspondences and fixed-points. *Stud Logica*, 83(1-3):133–155, 2006.
- [11] J. van Benthem. Relational patterns, partiality, and set lifting in modal semantics. *Saul Kripke on Modality*, 2022.
- [12] J. van Benthem and G. Bezhanishvili. Modal logics of space. In M. Aiello, I. Pratt-Hartmann, and J. van Benthem, editors, *Handbook of Spatial Logics*, pages 217–298. Springer, 2007.
- [13] J. van Benthem and T. Icard. Interfacing logic and counting. 2021. ILLC Prepublication Series.
- [14] K. Bimbó and M. Dunn. *Generalized Galois Logics: Relational Semantics of Nonclassical Logical Calculi*. CSLI Publications, Stanford, 2008.
- [15] C. Bishop. *Pattern Recognition and Machine Learning*. Springer, 2006.
- [16] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. Cambridge University Press, 2001.
- [17] I. Bloch, H. Heijmans, and C. Ronse. Mathematical morphology. In *Handbook of spatial logics*, pages 857–944. Springer, 2007.
- [18] J. Bradfield and C. Stirling. Modal μ -calculi. In *Handbook of Modal Logic*, pages 721–756. Springer, 2007.
- [19] C. Brink. Power structures. *Algebra Universalis*, 30(2):177–216, 1993.
- [20] H. Bruhn, R. Diestel, M. Kriesell, R. Pendavingh, and P. Wollan. Axioms for infinite matroids. *Advances in Mathematics*, 239:18–46, 2013.
- [21] A. Chagrov and M. Zakharyashev. *Modal Logic*. The Clarendon Press, New York, 1997.
- [22] L. Esakia and V. Meskhi. Five critical modal systems. *Theoria*, 43(1):52–60, 1977.
- [23] W. Fulton and J. Harris. *Representation Theory: A First Course*, volume 129. Springer, 2013.
- [24] P. Gärdenfors. *Conceptual Spaces - the Geometry of Thought*. MIT Press, 2000.
- [25] N. Gautam. The validity of equations of complex algebras. *Archiv für mathematische Logik und Grundlagenforschung*, 3(3):117–124, 1957.
- [26] Y. Goldberg. A primer on neural network models for natural language processing. *Journal of Artificial Intelligence Research*, 57:345–420, 2016.
- [27] R. Goldblatt. Semantic analysis of orthologic. *J. Philos. Log.*, 3(1-2):19–35, 1974.
- [28] R. Goldblatt. Varieties of complex algebras. *Ann. Pure Appl. Log.*, 44(3):173–242, 1989.
- [29] V. Goranko and D. Vakarelov. Hyperboolean algebras and hyperboolean modal logic. *J. Appl. Non Class. Logics*, 9(2-3):345–368, 1999.
- [30] W. Greub. *Linear Algebra*, volume 23. Springer, 2012.
- [31] J. Halpern. Axiomatizing causal reasoning. *J. Artif. Intell. Res.*, 12:317–337, 2000.
- [32] W. Hodges. *Model Theory*, volume 42 of *Encyclopedia of mathematics and its applications*. Cambridge University Press, 1993.
- [33] I. Hodkinson, S. Mikulás, and Y. Venema. Axiomatizing complex algebras by games. *Algebra Universalis*, 46(4):455–478, 2001.
- [34] P. Kremer and G. Mints. Dynamic topological logic. In *Handbook of Spatial Logics*, pages 565–606. Springer, 2007.
- [35] J. Lambek. The mathematics of sentence structure. *The American Mathematical Monthly*, 65(3):154–170, 1958.
- [36] H. Leitgeb. On the logic of vector space models. 2020. A talk at the international workshop “Logic with Vector Space Models”.
- [37] M. Lewis, D. Marsden, and M. Sadrzadeh. Semantic spaces at the intersection of nlp, physics, and cognitive science. *FLAP*, 7(5):677–682, 2020.
- [38] F. Liu, J. Seligman, and P. Girard. Logical dynamics of belief change in the community. *Synth.*, 191(11):2403–2431, 2014.
- [39] L. Maksimova. Pretabular superintuitionistic logics. *Algebra and Logic*, 11(5):558–570, 1972.
- [40] M. Marx. Complexity of modal logic. In *Handbook of Modal Logic*, pages 139–179. Springer, 2007.
- [41] M. Marx and Y. Venema. *Multi-dimensional modal logic*, volume 4 of *Applied logic series*. Kluwer, 1997.
- [42] E. Pacuit. *Neighborhood Semantics for Modal Logic*. Springer, 2017.
- [43] A. Pillay. Model theory and diophantine geometry. *Bulletin of the American Mathematical Society*, 34(4):405–422, 1997.
- [44] M. Sadrzadeh and R. Muskens. Static and dynamic vector semantics for lambda calculus models of natural language. *J. Lang. Model.*, 6(2):319–351, 2018.
- [45] A. Urquhart. Semantics for relevant logics. *The Journal of Symbolic Logic*, 37(1):159–169, 1972.
- [46] J. Väänänen. *Dependence Logic - A New Approach to Independence Friendly Logic*, volume 70 of *London Mathematical Society student texts*. Cambridge University Press, 2007.
- [47] Y. Venema. Algebras and coalgebras. In P. Blackburn, J. van Benthem, and F. Wolter, editors, *Handbook of modal logic*, pages 331–426. Elsevier, 2007.
- [48] D. Welsh. *Matroid Theory*. Courier Corporation, 2010.

9. APPENDIX. PROOFS FOR SOME RESULTS IN SECTION 5.3

Proof of Fact 5.11

Proof. Downward Monotonicity is obvious from the universally quantified definition of I^D , using also the Upward Monotonicity of the relation D in its X -argument. However, the second condition requires more work.

Suppose that X, Y satisfy the conditions, but that for no $y \in Y - X, I(X \cup \{y\})$. In this case [these things will be formulated as lemmas in the final version], we have that $D_X y$ for all $y \in Y - X$. Here is why. Since $\neg I(X \cup \{y\})$, either $D_X y$, and we are done, or, for some $x \in X, D_{X-x+y} x$. By Steinitz, this yields either (i) $D_{X-x} x$, which is impossible since $I(X)$ holds, or (ii) $D_X y$ again. In all then, we have that $D_X y$. [Here is a related useful lemma for our defined independence notion: if $I(X)$, then $D_X y$ iff $\neg I(X \cup \{y\})$. This last observation may even be equivalent to Steinitz.]

We now show that, in the situation we arrived at last, we cannot find a larger number of independent points in the X -dependent set Y than the cardinality of X . In general, X, Y may overlap: set $Z = X \cap Y$. Clearly, $|(X - Y)| < |(Y - X)|$. Now pick any object $y \in Y - X$. We have that $D_X y$, i.e., $D_{X-Y, Z} y$. By Generalized Steinitz, we have either $D_Z y$, which is impossible since $I(Y)$ holds, or for some $x \in X - Y : D_{Z, X-x+y} x$. This implies $D_{Z, X-x+y} X$ [recall the definition of this notation with sets X as a conjunction] using Reflexivity for the members of X different from the just-found object x . Next, by Transitivity of D applied to the fact that $D_X Y$, we get that $D_{Z, X-x+y} Y$. What this means is that we have now exchanged one element in $X - Y$ with one in $Y - X$ while still having all of Y dependent on the new set after the exchange. Repeating this process, we exhaust $X - Y$, and get a proper subset of Y [here we use that $|(X - Y)| < |(Y - X)|$] on which each object in Y is dependent. But this contradicts $I(Y)$. \square

Proof of Fact 5.13:

Proof. Reflexivity and Monotonicity are straightforward. Next, we prove *Steinitz Exchange*. Suppose that $D_{X, y} z$, that is either (a) $z \in X \cup \{y\}$, or (b) for some $X' \subseteq X \cup \{y\}, I(X') \wedge \neg I(X' \cup \{z\})$. In Case (a), we either have $z \in X$, and so by definition $D_X z$, or $z = y$, and then $D_{X, y} z$ implies $D_{X, z} y$. We are done in both cases. In Case (b), there are two subcases. Case (b1.) The set X' does not contain y . Then by definition, $D_X z$. Case (b2): No set as in case (b1) exists, and therefore $y \in X'$. This implies in particular that $I(X' - y + z)$. But we also had that $\neg I(X' \cup \{z\})$, and $X' \cup \{z\} = (X' - y + z) + y$. By definition, this means that $D_{X+z} y$.

Next we need to prove *Transitivity* of the defined relation D . Suppose that $D_X y$ for all $y \in Y$ and $D_Y z$: we must show that $D_X z$. I sketch the main steps. For a start, there are some special cases to consider first, such as $z \in Y$ or $z \in X$. In both these cases, the conclusion follows immediately by the definition of D . So we can assume that z is a new object.

Some comments before the main argument. Independence is an absolute property of sets. But *maximal independence* inside the subsets of a given set X depends essentially on X , and may change truth value when we change that background. We will use the latter changes repeatedly in combination with the next observation. The Extension Property can be used easily to show the following fact [recall that all our sets are finite], noted earlier.

Any two maximally independent sets inside a given set have the same cardinality.

[In matroid theory, this is the basis of using ‘rank’.] Finally, here is one more useful observation.

Let X, Y be two maximally independent subsets of a set U : then X, Y have the same dependent objects z outside of U in the sense of the above definition.

Proof. Let $D_X z$. Since $z \notin U$ and $z \notin X$, the second clause of the definition applies, and we have $\neg I(X \cup \{z\})$ with X independent. This means that X is also maximally independent in the extended set $U \cup \{z\}$, and hence it has the largest size of an independent set there. But then, the

independent set Y of the same size is maximally independent in $U \cup \{z\}$, too, and therefore, adding the further object z to it results in a non-independent set: $\neg I(Y \cup \{z\})$. \square

Now we consider the general situation for Transitivity. We have the above two sets X, Y with all $y \in Y$ dependent [in our defined sense] on X , and z dependent on Y . Since $z \notin Y$, this means that there is some independent $Y' \subseteq Y$ with $\neg I(Y' \cup \{z\})$. Clearly also $D_X Y'$, by the conjunctive definition of the relation D for set arguments Y . Thus, it suffices to consider Y' instead of Y , or equivalently, without loss of generality, we can take the above set Y to be independent.

Now consider the elements of $Y - X$. Case 1: There are no such elements, and $Y \subseteq X$. Then we are done, since Y is then an independent subset of X which loses independence when adding z , and this implies that $D_X z$ holds in our defined sense. Case 2: there are such elements. For each such u , there exists an independent subset X' of X with $\neg I(X' \cup \{u\})$. Obviously, we can extend X' to a maximally independent inside X , and we still have $\neg I(X' \cup \{u\})$ by the downward monotonicity of the independence predicate I . Moreover, for all these u , we can take the same maximally independent subset, by the above observation: call this set X^\bullet . We claim that this is the required independent subset of X with $\neg I(X^\bullet \cup \{z\})$. It remains to establish this fact.

First note that the set $I(X^\bullet)$ is maximally independent in the set $X \cup Y$. For, the only further elements one could add are either (i) objects in X : but this is impossible since X^\bullet was maximally independent in X , or (ii) objects in $Y - X$: but this is impossible since by the assumption $D_X Y$ as analyzed above, adding such objects to X^\bullet would make the resulting set non-independent. Next, consider the independent set Y and extend it to a maximally independent set Y^+ in $X \cup Y$ (as can always be done). We still have that $D_{X^+} z$, by our definition and the downward monotonicity of independence. Now we use our earlier observation that two maximally independent sets inside some set have the same dependent objects outside of that set to conclude that $D_{X^\bullet} z$.

This completes the proof of our representation result for D from I . \square