ALL NORMAL EXTENSIONS OF S5-SQUARED ARE FINITELY AXIOMATIZABLE

Nick Bezhanishvili and Ian Hodkinson

Abstract

We prove that every normal extension of the bi-modal system $\mathbf{S5}^2$ is finitely axiomatizable and that every proper normal extension has NP-complete satisfiability problem.

Recall that the language of $\mathbf{S5}^2$ is the propositional language based on a fixed countably infinite set of propositional variables and equipped with the two modal operators $\Box_1$ and $\Box_2$. For a formula φ we let $\Diamond_i\varphi$ abbreviate $\neg\Box_i\neg\varphi$ for $i = 1, 2$. We recall that $\mathbf{S5}^2$ is the smallest set of formulas containing all substitution instances of the following axiom schemas, for $i = 1, 2$:

1) All tautologies of the classical propositional calculus;
2) $\Box_i(p \to q) \to (\Box_i p \to \Box_i q)$;
3) $\Box_i p \to p$;
4) $\Box_i p \to \Box_i\Box_i p$;
5) $\Diamond_i\Box_i p \to p$;
6) $\Box_1\Box_2 p \leftrightarrow \Box_2\Box_1 p$;

and closed under the following rules of inference:

Modus Ponens (MP): from φ and $\varphi \to \psi$ infer ψ;
Necessitation $(\mathrm{N})_i$: from φ infer $\Box_i\varphi$.

Recall also that a set of formulas L is called a *logic* if it contains all tautologies of the classical propositional calculus and is closed under the rule of modus ponens. A modal logic is called *normal* if it contains axiom schema 2) (see above) and is closed under the rule of necessitation. A logic L_1 is an *extension* of L_2 if $L_2 \subseteq L_1$.

It is well-known that $\mathbf{S5}^2$ has the exponential size model property, and that its satisfiability problem is NEXPTIME-complete [6]. In this paper, by the complexity of a logic we will mean the complexity of its satisfiability problem. It is shown in [3] that in contrast to $\mathbf{S5}^2$, every proper normal extension L of $\mathbf{S5}^2$ has the poly-size model property. That means that there is a polynomial $P(n)$ such that any L-consistent formula φ (that is, $\neg\varphi \notin L$) has a model with at most $P(|\varphi|)$ points, where $|\varphi|$ is the length of φ.

It was conjectured in [3] that every proper normal extension of $\mathbf{S5}^2$ is finitely axiomatizable and NP-complete. In this paper we prove this conjecture. In fact, we show that for every proper normal extension L of $\mathbf{S5}^2$, there is a finite set $\mathbf{M}_L$ of finite $\mathbf{S5}^2$-frames such that an arbitrary finite $\mathbf{S5}^2$-frame is a frame for L iff it does not have any frame in $\mathbf{M}_L$ as a p-morphic image. This condition yields a finite axiomatization of L. We also show that the condition is decidable in deterministic polynomial time. This, together with the poly-size model property, implies the NP-completeness of L.

We now explain some of these notions in detail. Recall that a triple $\mathcal{F} = (W, E_1, E_2)$ is an $\mathbf{S5}^2$-frame if W is a non-empty set and E_1 and E_2 are equivalence relations on W such that

$$\mathcal{F} \models (\forall w, v, u)(wE_1v \wedge vE_2u) \rightarrow (\exists z)(wE_2z \wedge zE_1u).$$

For $i = 1, 2$ we call the E_i-equivalence classes *E_i-clusters*. The E_i-cluster containing $w \in W$ is denoted by $E_i(w)$, and for $X \subseteq W$ we let $E_i(X)$ denote $\bigcup_{x \in X} E_i(x)$.

For positive integers n and m let $\mathbf{n} \times \mathbf{m}$ denote the $\mathbf{S5}^2$-frame with domain $n \times m$ and with $(x_1, x_2)E_i(y_1, y_2)$ iff $x_i = y_i$, for $i = 1, 2$. Then it is well known that $\mathbf{S5}^2$ is complete with respect to $\{\mathbf{n} \times \mathbf{n} : n \geq 1\}$ [9].

Given two $\mathbf{S5}^2$-frames $\mathcal{F} = (W, E_1, E_2)$ and $\mathcal{G} = (U, S_1, S_2)$, a mapping $f : U \rightarrow W$ is called a *p-morphism from $\mathcal{G}$ to $\mathcal{F}$* if

$$(\forall t \in U)(\forall w \in W)(f(t)E_iw \leftrightarrow (\exists u \in U)(tS_iu \wedge f(u) = w)).$$

We say that $\mathcal{F}$ is *isomorphic* to $\mathcal{G}$ if there is a one-one p-morphism from $\mathcal{G}$ onto $\mathcal{F}$. We call $\mathcal{F}$ a *p-morphic image* of $\mathcal{G}$ if there is a p-morphism from $\mathcal{G}$ onto $\mathcal{F}$. It is well known that p-morphic images preserve validity of formulas.

We call $\mathcal{F}$ *rooted* if

$$\mathcal{F} \models (\forall w, v)(\exists u)(wE_1u \wedge uE_2v).$$

Choose a set $\mathbf{F}_{\mathbf{S5}^2}$ of representatives of isomorphism types of finite rooted $\mathbf{S5}^2$-frames. That is, for each finite rooted $\mathbf{S5}^2$-frame, there is exactly one frame in $\mathbf{F}_{\mathbf{S5}^2}$ that is isomorphic to it.

Let L be a normal extension of $\mathbf{S5}^2$. An $\mathbf{S5}^2$-frame $\mathcal{F}$ is called an *L-frame* if $\mathcal{F}$ validates all formulas in L. Let $\mathbf{F}_L$ be the set of all L-frames in $\mathbf{F}_{\mathbf{S5}^2}$. Then L is complete with respect to $\mathbf{F}_L$ [1]. Thus, for our purposes it suffices to consider only finite rooted $\mathbf{S5}^2$-frames. From now on, we will use the term "frame" to mean this.

For $\mathcal{F}, \mathcal{G} \in \mathbf{F}_{\mathbf{S5}^2}$ we put

$$\mathcal{F} \leq \mathcal{G} \text{ iff } \mathcal{F} \text{ is a } p\text{-morphic image of } \mathcal{G}.$$

Then it is routine to check that $\leq$ is a partial order on $\mathbf{F}_{\mathbf{S5}^2}$. We write $\mathcal{F} < \mathcal{G}$ if $\mathcal{F} \leq \mathcal{G}$ and $\mathcal{G} \not\leq \mathcal{F}$. Then $\mathcal{F} < \mathcal{G}$ implies $|\mathcal{F}| < |\mathcal{G}|$ and we see that there are no infinite descending chains in $(\mathbf{F}_{\mathbf{S5}^2}, <)$. Thus, for any non-empty $A \subseteq \mathbf{F}_{\mathbf{S5}^2}$, the set $\min(A)$ of minimal elements of A is non-empty, and for any $\mathcal{G} \in A$ there is $\mathcal{F} \in \min(A)$ such that $\mathcal{F} \leq \mathcal{G}$.

Now we recall the Jankov-Fine formulas for $\mathbf{S5}^2$ (see [4, §3.4] and [5, §8.4 p.392]). Consider a frame $\mathcal{F} = (W, E_1, E_2)$. For each point $p \in W$ we introduce a propositional variable, denoted also by p, and consider the formulas

$$\begin{aligned}
\alpha(\mathcal{F}) &= \Box_1\Box_2\Big(\bigvee_{p\in W}(p \wedge \neg \bigvee_{p'\in W\setminus\{p\}} p') \\
&\qquad \wedge \bigwedge_{\substack{i=1,2\\ p,p'\in W, pE_ip'}} (p \to \Diamond_i p') \quad \wedge \bigwedge_{\substack{i=1,2\\ p,p'\in W, \neg(pE_ip')}} (p \to \neg\Diamond_i p')\Big), \\
\chi(\mathcal{F}) &= \neg\alpha(\mathcal{F}).
\end{aligned}$$

Lemma 1. *For any frames $\mathcal{F} = (W, E_1, E_2)$ and $\mathcal{G} = (U, S_1, S_2)$ we have that $\mathcal{F}$ is a p-morphic image of $\mathcal{G}$ iff $\mathcal{G} \not\models \chi(\mathcal{F})$.*

Proof. (Sketch) Suppose $\mathcal{F}$ is a p-morphic image of $\mathcal{G}$. Define a valuation V on $\mathcal{F}$ by putting $V(p) = p$ for any $p \in W$. Then $\mathcal{F} \not\models_V \chi(\mathcal{F})$ by the definition of $\chi(\mathcal{F})$. Now if $\mathcal{G} \models \chi(\mathcal{F})$, then since p-morphic images preserve validity of formulas, we would also have $\mathcal{F} \models \chi(\mathcal{F})$, a contradiction. Therefore, $\mathcal{G} \not\models \chi(\mathcal{F})$.

For the converse, we use the argument of [5, Claim 8.36]. Suppose $\mathcal{G} \not\models \chi(\mathcal{F})$. Then there is a valuation V' on $\mathcal{G}$ and a point $u \in U$ such that $\mathcal{G}, u \not\models_{V'} \chi(\mathcal{F})$. Therefore, $\mathcal{G}, u \models_{V'} \alpha(\mathcal{F})$. Define a map $f : U \to W$ by putting $f(t) = p \iff \mathcal{G}, t \models_{V'} p$, for every $t \in U$ and $p \in W$. From $\mathcal{G}$ being rooted and the truth of the first conjunct of $\alpha(\mathcal{F})$ it follows that f is well defined. The truth of the first two conjuncts of $\alpha(\mathcal{F})$ together with $\mathcal{F}$ being rooted implies that f is surjective. Finally, the truth of the second and third conjuncts of $\alpha(\mathcal{F})$ guarantees that f is a p-morphism. Therefore, $\mathcal{F}$ is a p-morphic image of $\mathcal{G}$. □

If L is a proper normal extension of $\mathbf{S5}^2$, then by completeness of $\mathbf{S5}^2$ with respect to $\mathbf{F}_{\mathbf{S5}^2}$, the set $\mathbf{F}_{\mathbf{S5}^2} \setminus \mathbf{F}_L$ is non-empty. Let $\mathbf{M}_L = \min(\mathbf{F}_{\mathbf{S5}^2} \setminus \mathbf{F}_L)$.

Theorem 2. *For any proper normal extension L of $\mathbf{S5}^2$ and $\mathcal{G} \in \mathbf{F}_{\mathbf{S5}^2}$, $\mathcal{G} \in \mathbf{F}_L$ iff no $\mathcal{F} \in \mathbf{M}_L$ is a p-morphic image of $\mathcal{G}$.*

Proof. Let $\mathcal{G} \in \mathbf{F}_L$; then since p-morphisms preserve validity of formulas, every p-morphic image of $\mathcal{G}$ belongs to $\mathbf{F}_L$ and hence can not be in $\mathbf{M}_L$. Conversely, if $\mathcal{G} \in \mathbf{F}_{\mathbf{S5}^2} \setminus \mathbf{F}_L$ then there is $\mathcal{F} \in \mathbf{M}_L$ such that $\mathcal{F} \leq \mathcal{G}$ — that is, $\mathcal{F}$ is a p-morphic image of $\mathcal{G}$. □

Theorem 3. *Every proper normal extension L of $\mathbf{S5}^2$ is axiomatizable by the axioms of $\mathbf{S5}^2$ plus $\{\chi(\mathcal{F}) : \mathcal{F} \in \mathbf{M}_L\}$.*

Proof. Let $\mathcal{G} \in \mathbf{F}_{\mathbf{S5}^2}$. Then by Theorem 2, $\mathcal{G} \in \mathbf{F}_L$ iff there is no $\mathcal{F} \in \mathbf{M}_L$ with $\mathcal{F} \leq \mathcal{G}$, iff (by Lemma 1) there is no $\mathcal{F} \in \mathbf{M}_L$ with $\mathcal{G} \not\models \chi(\mathcal{F})$, iff $\mathcal{G} \models \chi(\mathcal{F})$ for all $\mathcal{F} \in \mathbf{M}_L$. Thus, $\mathcal{G} \models \{\chi(\mathcal{F}) : \mathcal{F} \in \mathbf{M}_L\}$ iff $\mathcal{G} \in \mathbf{F}_L$.

Let L' be the logic axiomatized by the axioms of $\mathbf{S5}^2$ plus $\{\chi(\mathcal{F}) : \mathcal{F} \in \mathbf{M}_L\}$. From the above it is clear that $\mathbf{F}_{L'} = \mathbf{F}_L$. But L (L') is sound and complete with respect to $\mathbf{F}_L$ ($\mathbf{F}_{L'}$, respectively). So, $L' = L$. □

It follows that $L \supset \mathbf{S5}^2$ is finitely axiomatizable whenever $\mathbf{M}_L$ is finite. We now proceed to show that $\mathbf{M}_L$ is indeed finite for every proper normal extension L of $\mathbf{S5}^2$.

Suppose $\mathcal{G} \in \mathbf{F}_{\mathbf{S5}^2}$. For $i = 1, 2$, we say that the E_i*-depth* of $\mathcal{G}$ is n, and write $d_i(\mathcal{G}) = n$, if the number of E_i-clusters of $\mathcal{G}$ is n.

Fix a proper normal extension L of $\mathbf{S5}^2$. Since $\mathbf{S5}^2$ is complete with respect to $\{\mathbf{n} \times \mathbf{n} : n \geq 1\}$, there is $n \geq 1$ such that $\mathbf{n} \times \mathbf{n} \notin \mathbf{F}_L$. Let $n(L)$ be the least such.

Lemma 4. *Let L be as above, and write n for $n(L)$.*

1. *If $\mathcal{G} \in \mathbf{F}_L$, then $d_1(\mathcal{G}) < n$ or $d_2(\mathcal{G}) < n$.*

2. *If $\mathcal{G} \in \mathbf{M}_L$, then $d_1(\mathcal{G}) \leq n$ or $d_2(\mathcal{G}) \leq n$.*

Proof. 1. If $\mathcal{G} \in \mathbf{F}_L$ and $d_1(\mathcal{G}) \geq n$ and $d_2(\mathcal{G}) \geq n$, then by [3, Lemma 5], $\mathbf{n} \times \mathbf{n}$ is a p morphic image of $\mathcal{G}$. So, $\mathbf{n} \times \mathbf{n} \in \mathbf{F}_L$, a contradiction.

2. If $\mathcal{G} \in \mathbf{M}_L$ and both depths of $\mathcal{G}$ are greater than n, then again $\mathbf{n} \times \mathbf{n}$ is a p-morphic image of $\mathcal{G}$. Therefore, $\mathbf{n} \times \mathbf{n} < \mathcal{G}$. However, $\mathcal{G}$ is a minimal element of $\mathbf{F}_{\mathbf{S5}^2} \setminus \mathbf{F}_L$, implying that $\mathbf{n} \times \mathbf{n}$ belongs to $\mathbf{F}_L$, which is false. □

Corollary 5. *$\mathbf{M}_L$ is finite iff $\{\mathcal{F} \in \mathbf{M}_L : d_i(\mathcal{F}) = k\}$ is finite for every $k \leq n(L)$ and $i = 1, 2$.*

Proof. By Lemma 4, $\mathbf{M}_L = \bigcup_{k \leq n(L)} \{\mathcal{F} \in \mathbf{M}_L : d_1(\mathcal{F}) = k\} \cup \bigcup_{k \leq n(L)} \{\mathcal{F} \in \mathbf{M}_L : d_2(\mathcal{F}) = k\}$. Thus, $\mathbf{M}_L$ is finite if and only if $\{\mathcal{F} \in \mathbf{M}_L : d_i(\mathcal{F}) = k\}$ is finite for every $k \leq n(L)$ and $i = 1, 2$. □

Since $\mathbf{M}_L$ is a $\leq$-antichain in $\mathbf{F}_{\mathbf{S5}^2}$, to show that $\{\mathcal{F} \in \mathbf{M}_L : d_i(\mathcal{F}) = k\}$ is finite for every $k \leq n(L)$ and $i = 1, 2$, it is enough to prove that for any k, the set $\{\mathcal{F} \in \mathbf{F}_{\mathbf{S5}^2} : d_i(\mathcal{F}) = k\}$ does not contain an infinite $\leq$-antichain. Without loss of generality we can consider the case when $i = 2$.

Fix $k \in \omega$. For every $n \in \omega$ let $\mathcal{M}_n$ denote the set of all $n \times k$ matrices (m_{ij}) with coefficients in ω ($i < n$, $j < k$). Let $\mathcal{M} = \bigcup_{n \in \omega} \mathcal{M}_n$. Define $\preccurlyeq$ on $\mathcal{M}$ by putting $(m_{ij}) \preccurlyeq (m'_{ij})$ if we have $(m_{ij}) \in \mathcal{M}_n$, $(m'_{ij}) \in \mathcal{M}_{n'}$, $n \leq n'$, and there is a surjection $f : n' \to n$ such that $m_{f(i)j} \leq m'_{ij}$ for all $i < n'$ and $j < k$. It is easy to see that $(\mathcal{M}, \preccurlyeq)$ is a quasi-ordered set (i.e., $\preccurlyeq$ is reflexive and transitive).

Let $\mathbf{F}^k_{\mathbf{S5}^2} = \{\mathcal{F} \in \mathbf{F}_{\mathbf{S5}^2} : d_2(\mathcal{F}) = k\}$. For each $\mathcal{F} \in \mathbf{F}^k_{\mathbf{S5}^2}$ we fix enumerations $F_0, \ldots, F_{n-1}$ of the E_1-clusters of $\mathcal{F}$ (where $n = d_1(\mathcal{F})$) and $F^0, \ldots, F^{k-1}$ of the E_2-clusters of $\mathcal{F}$. Define a map $H : \mathbf{F}^k_{\mathbf{S5}^2} \to \mathcal{M}$ by putting $H(\mathcal{F}) = (m_{ij})$ if $|F_i \cap F^j| = m_{ij}$ for $i < d_1(\mathcal{F})$ and $j < k$.

Lemma 6. *$H : (\mathbf{F}^k_{\mathbf{S5}^2}, \leq) \to (\mathcal{M}, \preccurlyeq)$ is an order-reflecting injection.*

Proof. Since $\mathbf{F}_{\mathbf{S5}^2}$ consists of non-isomorphic frames, H is one-one. Now let $\mathcal{F} = (W, E_1, E_2)$, $\mathcal{G} = (U, S_1, S_2)$, $\mathcal{F}, \mathcal{G} \in \mathbf{F}^k_{\mathbf{S5}^2}$, and $(m_{ij}), (m'_{ij}) \in \mathcal{M}$ be such that $H(\mathcal{F}) = (m_{ij})$, $H(\mathcal{G}) = (m'_{ij})$, and $(m_{ij}) \preccurlyeq (m'_{ij})$. We need to show that $\mathcal{F} \leq \mathcal{G}$. Suppose $(m_{ij}) \in \mathcal{M}_n$ and $(m'_{ij}) \in \mathcal{M}_{n'}$. Then there is surjective $f : n' \to n$ such that $m_{f(i)j} \leq m'_{ij}$ for $i < n'$ and $j < k$. Then $|G_i \cap G^j| \geq |F_{f(i)} \cap F^j|$ for any $i < n'$ and $j < k$. Hence there exists a surjection $h_i^j : G_i \cap G^j \to F_{f(i)} \cap F^j$. Define $h : U \to W$ by putting $h(u) = h_i^j(u)$, where $i < n', j < k$, and $u \in G_i \cap G^j$. It is obvious that h is well defined and onto.

Now we show that h is a p-morphism. If uS_1v, then $u, v \in G_i$ for some $i < n'$. Therefore, $h(u), h(v) \in F_{f(i)}$, and so $h(u)E_1h(v)$. Analogously, if uS_2v, then $u, v \in G^j$ for some $j < k$, $h(u), h(v) \in F^j$, and so $h(u)E_2h(v)$. Now suppose $u \in G_i \cap G^j$ for some $i < n'$ and $j < k$. If $h(u)E_2h(v)$, then $h(u), h(v) \in F^j$ and $v \in G^j$. As both u and v belong to G^j it follows that uS_2v. Finally, if $h(u)E_1h(v)$, then $h(u) \in F_{f(i)} \cap F^j$ and $h(v) \in F_{f(i)} \cap F^{j'}$, for some $j' < k$. Therefore, there exists $z \in G_i \cap G^{j'}$ (since $z \in G_i$ we have uS_1z) such that $h(z) = h(v)$. Thus, h is an onto p-morphism, implying that $\mathcal{F} \leq \mathcal{G}$. Thus, H is order reflecting. □

Corollary 7. *If $\Delta \subseteq \mathbf{F}^k_{\mathbf{S5}^2}$ is a $\leq$-antichain, then $H(\Delta) \subseteq \mathcal{M}$ is a $\preccurlyeq$-antichain.*

Proof. Immediate. □

Now we will show that there are no infinite $\preccurlyeq$-antichains in $\mathcal{M}$. For this we define a quasi-order $\sqsubseteq$ on $\mathcal{M}$ included in $\preccurlyeq$ and show that there are no infinite $\sqsubseteq$-antichains in $\mathcal{M}$. To do so we first introduce two quasi-orders $\sqsubseteq_1$ and $\sqsubseteq_2$ on $\mathcal{M}$ and then define $\sqsubseteq$ as the intersection of these quasi-orders. For $(m_{ij}) \in \mathcal{M}_n$ and $(m'_{ij}) \in \mathcal{M}_{n'}$, we say that:

- $(m_{ij}) \sqsubseteq_1 (m'_{ij})$ if there is a one-one order-preserving map $\varphi : n \to n'$ (i.e., $i < i' < n$ implies $\varphi(i) < \varphi(i')$) such that $m_{ij} \leq m'_{\varphi(i)j}$ for all $i < n$ and $j < k$;
- $(m_{ij}) \sqsubseteq_2 (m'_{ij})$ if there is a map $\psi : n' \to n$ such that $m_{\psi(i)j} \leq m'_{ij}$ for all $i < n'$ and $j < k$.

Let $\sqsubseteq$ be the intersection of $\sqsubseteq_1$ and $\sqsubseteq_2$.

Lemma 8. *For any $(m_{ij}), (m'_{ij}) \in \mathcal{M}$, if $(m_{ij}) \sqsubseteq (m'_{ij})$, then $(m_{ij}) \preccurlyeq (m'_{ij})$.*

Proof. Suppose $(m_{ij}) \in \mathcal{M}_n$ and $(m'_{ij}) \in \mathcal{M}_{n'}$. If $(m_{ij}) \sqsubseteq (m'_{ij})$, then $(m_{ij}) \sqsubseteq_1 (m'_{ij})$ and $(m_{ij}) \sqsubseteq_2 (m'_{ij})$. By $(m_{ij}) \sqsubseteq_1 (m'_{ij})$ there is a one-one order-preserving map $\varphi : n \to n'$ with $m_{ij} \leq m'_{\varphi(i)j}$ for all $i < n$ and $j < k$;

and by $(m_{ij}) \sqsubseteq_2 (m'_{ij})$ there is a map $\psi : n' \to n$ such that $m_{\psi(i)j} \leq m'_{ij}$ for all $i < n'$ and $j < k$. Let $\mathrm{rng}(\varphi) = \{\varphi(i) : i < n\}$. Define $f : n' \to n$ by putting

$$f(i) = \begin{cases} \varphi^{-1}(i), & \text{if } i \in \mathrm{rng}(\varphi), \\ \psi(i), & \text{otherwise.} \end{cases}$$

Then f is a surjection. Moreover, for $i < n'$ and $j < k$, if $i \in \mathrm{rng}(\varphi)$, then $m_{f(i)j} = m_{\varphi^{-1}(i)j} \leq m'_{ij}$ by the definition of $\sqsubseteq_1$; and if $i \notin \mathrm{rng}(\varphi)$, then $m_{f(i)j} = m_{\psi(i)j} \leq m'_{ij}$ by the definition of $\sqsubseteq_2$. Therefore, $m_{f(i)j} \leq m'_{ij}$ for all $i < n'$ and $j < k$. Thus, $(m_{ij}) \preccurlyeq (m'_{ij})$. □

Thus, it is left to show that there are no infinite $\sqsubseteq$-antichains in $\mathcal{M}$. For this we use the theory of *better-quasi-orderings (bqos).* Our main source of reference is Laver [7].

For any set $X \subseteq \omega$ let $[X]^{<\omega} = \{Y \subseteq X : |Y| < \omega\}$, and for $n < \omega$ let $[X]^n = \{Y \subseteq X : |Y| = n\}$. We say that Y is an initial segment of X if there is $n \in \omega$ such that $Y = \{x \in X : x \leq n\}$.

Definition 9. *Let X be an infinite subset of ω. We say that $\mathcal{B} \subseteq [X]^{<\omega}$ is a* barrier on X *if $\emptyset \notin \mathcal{B}$ and:*

- *for every infinite $Y \subseteq X$, there is an initial segment of Y in $\mathcal{B}$;*
- *$\mathcal{B}$ is an antichain with respect to $\subseteq$.*

A barrier *is a barrier on some infinite $X \subseteq \omega$.*

Note that for any $n \geq 1$, $[\omega]^n$ is a barrier on ω.

Definition 10.

1. *If s, t are finite subsets of ω, we write $s \lhd t$ to mean that there are $i_1 < \ldots < i_k$ and j $(1 \leq j < k)$ such that $s = \{i_1, \ldots, i_j\}$ and $t = \{i_2, \ldots, i_k\}$.*
2. *Given a barrier $\mathcal{B}$ and a quasi-ordered set $(Q, \leq)$, we say that a map $f : \mathcal{B} \to Q$ is* good *if there are $s, t \in \mathcal{B}$ such that $s \lhd t$ and $f(s) \leq f(t)$.*

Let $(Q, \leq)$ be a quasi-order. We call $\leq$ a *better-quasi-ordering (bqo)* if for every barrier $\mathcal{B}$, every map $f : \mathcal{B} \to Q$ is good.

Proposition 11. *If $(Q, \leq)$ is a bqo, then there are no infinite antichains in Q.*

Proof. Let $(\xi_n)_{n\in\omega}$ be an infinite sequence of distinct elements of Q. As we pointed out, $\mathcal{B} = [\omega]^1 = \{\{n\} : n < \omega\}$ is a barrier. Define a map $\theta : \mathcal{B} \to Q$ by putting $\theta(\{n\}) = \xi_n$. Since $(Q, \leq)$ is a bqo, θ is good. Therefore, there are $\{n\}, \{m\} \in \mathcal{B}$ such that $\{n\} \lhd \{m\}$ (i.e., $n < m$) and $\xi_n \leq \xi_m$. So, no infinite subset of Q forms an antichain. □

Thus, it suffices to show that $\sqsubseteq$ is a bqo. It follows from [7, Lemma 1.7] that the intersection of two bqos is again a bqo. Hence, it is enough to prove that both $\sqsubseteq_1$ and $\sqsubseteq_2$ are bqos. [7, Theorem 1.10] implies that $(\mathcal{M}, \sqsubseteq_1)$ is a bqo.[1] Therefore, we only need to show that $(\mathcal{M}, \sqsubseteq_2)$ is a bqo.

Let $(Q, \leq)$ be a quasi-ordered set and $\wp(Q)$ be the power set of Q. The order $\leq$ can be extended to $\wp(Q)$ as follows: For $\Gamma, \Delta \in \wp(Q)$, we say that $\Gamma \leq \Delta$ if for all $\delta \in \Delta$ there is $\gamma \in \Gamma$ with $\gamma \leq \delta$. It can be shown by adapting the proof of [7, Lemma 1.3] that if $(Q, \leq)$ is a bqo, then $(\wp(Q), \leq)$ is also a bqo.[2]

Lemma 12. $(\mathcal{M}, \sqsubseteq_2)$ *is a bqo.*

Proof. For a matrix $(m_{ij}) \in \mathcal{M}_n$ let $m_i = (m_{i0}, \ldots, m_{ik-1})$ denote the i-th row of (m_{ij}). Note that each row of (m_{ij}) is a $1 \times k$ matrix, and so $m_i \in \mathcal{M}_1$ for any $i < n$. We write $\mathrm{row}(m_{ij})$ for the set $\{m_i : i < n\}$. Obviously, $\mathrm{row}(m_{ij}) \in \wp(\mathcal{M}_1) \subseteq \wp(\mathcal{M})$. Consider an arbitrary barrier $\mathcal{B}$ and a map $f : \mathcal{B} \to \mathcal{M}$. We need to show that f is good with respect to $\sqsubseteq_2$. Define $g : \mathcal{B} \to \wp(\mathcal{M})$ by $g(s) = \mathrm{row}(f(s))$. Since $(\mathcal{M}, \sqsubseteq_1)$ is a bqo, $(\wp(\mathcal{M}), \sqsubseteq_1)$ is also a bqo. Hence, there are $s, t \in \mathcal{B}$ such that $s \lhd t$ and $g(s) \sqsubseteq_1 g(t)$. Therefore, for each $\delta \in g(t)$ there is $\gamma \in g(s)$ with $\gamma \sqsubseteq_1 \delta$.

Now we show that $f(s) \sqsubseteq_2 f(t)$. Write (m_{ij}) for $f(s)$ and (m'_{ij}) for $f(t)$. Suppose that $(m_{ij}) \in \mathcal{M}_n$ and $(m'_{ij}) \in \mathcal{M}_{n'}$. We define $\psi : n' \to n$ as follows. Let $i < n'$. Then $m'_i \in g(t)$. By the above, we may choose $\psi(i) < n$ such that $m_{\psi(i)} \sqsubseteq_1 m'_i$. This defines ψ, and we have $m_{\psi(i)j} \leq m'_{ij}$ for any $i < n'$ and $j < k$. Thus, $f(s) \sqsubseteq_2 f(t)$, f is a good map, and so $(\mathcal{M}, \sqsubseteq_2)$ is a bqo. □

It follows that $(\mathcal{M}, \sqsubseteq)$ is a bqo. Therefore, there are no infinite $\sqsubseteq$-antichains in $\mathcal{M}$. Thus, by Lemma 8 there are no infinite $\preccurlyeq$-antichains in $\mathcal{M}$.

Now we are in a position to prove the main theorem of this paper.

[1]To apply this theorem, we needed to require in the definition of $\sqsubseteq_1$ on $\mathcal{M}$ that φ is order preserving. This is the only time this assumption is used.

[2]This last statement fails for well-quasi-orders. An example of Rado [8] can be used to show this.

Theorem 13. *Every normal extension of* $\mathbf{S5}^2$ *is finitely axiomatizable.*

Proof. Clearly, $\mathbf{S5}^2$ is finitely axiomatizable. Suppose L is a proper normal extension of $\mathbf{S5}^2$. Then by Theorem 3 L is axiomatizable by the $\mathbf{S5}^2$ axioms plus $\{\chi(\mathcal{F}) : \mathcal{F} \in \mathbf{M}_L\}$. Since there are no infinite $\preccurlyeq$-antichains in $\mathcal{M}$, by Corollary 7 there are no infinite antichains in $\mathbf{F}^k_{\mathbf{S5}^2}$, for each $k \in \omega$. Therefore, $\{\mathcal{F} \in \mathbf{M}_L : d_i(\mathcal{F}) = k\}$ is finite for every $k \leq n(L)$ and $i = 1, 2$. Thus, $\mathbf{M}_L$ is finite by Corollary 5. It follows that L is finitely axiomatizable. □

Corollary 14. *The lattice of normal extensions of* $\mathbf{S5}^2$ *is countable.*

Proof. Immediately follows from Theorem 13 since there are only countably many finitely axiomatizable normal extensions of $\mathbf{S5}^2$. □

Remark 15. In algebraic terminology, Corollary 14 says that the lattice of subvarieties of the variety $\mathbf{Df}_2$ of two-dimensional diagonal-free cylindric algebras is countable. This is in contrast with the variety $\mathbf{CA}_2$ of two-dimensional cylindric algebras (with diagonals), since, as was shown in [2], the cardinality of the lattice of subvarieties of $\mathbf{CA}_2$ is that of continuum.

Note that Theorem 13, and the fact that every normal extension L of $\mathbf{S5}^2$ is complete with respect to a class of finite frames ($\mathbf{F}_L$) for which (up to isomorphism) membership is decidable, imply that L is decidable. The final part of the paper will be devoted to showing that if L is a proper normal extension, then it is NP-complete. Fix such an L. We will see in Corollary 18 below that NP-completeness of L follows from the poly-size model property if we can decide in time polynomial in $|W|$ whether a finite structure $\mathcal{A} = (W, R_1, R_2)$ is in $\mathbf{F}_L$ (up to isomorphism). It suffices to decide in polynomial time (1) whether $\mathcal{A}$ is a (rooted $\mathbf{S5}^2$-) frame; (2) whether a given frame is in $\mathbf{F}_L$. The first is easy. We concentrate on the second.

By Lemma 4(1), there is $n(L) \in \omega$ such that for each frame $\mathcal{G} = (U, S_1, S_2)$ in $\mathbf{F}_L$ we have $d_1(\mathcal{G}) < n(L)$ or $d_2(\mathcal{G}) < n(L)$. So, if both depths of a given frame $\mathcal{G}$ are greater than or equal to $n(L)$ (which obviously can be checked in polynomial time in the size of $\mathcal{G}$), then $\mathcal{G} \notin \mathbf{F}_L$. So, without loss of generality we can assume that $d_1(\mathcal{G}) < n(L)$.

By Theorem 2, $\mathcal{G}$ is in $\mathbf{F}_L$ iff it has no p-morphic image in $\mathbf{M}_L$. Because $\mathbf{M}_L$ is a fixed finite set, it suffices to provide, for an arbitrary fixed frame $\mathcal{F} = (W, E_1, E_2)$, an algorithm that decides in time polynomial in the size of $\mathcal{G}$ whether there is a p-morphism from $\mathcal{G}$ onto $\mathcal{F}$. If we considered every map $f : U \to W$ and checked whether it is a p-morphism, it would take exponential time in the size of $\mathcal{G}$ (since there are $|W|^{|U|}$ different maps from U to W). Now we will give a different algorithm to check in polynomial time in $|U|$ whether the fixed frame $\mathcal{F}$ is a p-morphic image of a given frame $\mathcal{G} = (U, S_1, S_2)$ with $d_1(\mathcal{G}) < n(L)$.

Recall that a map $f : U \to W$ is a p-morphism iff the f-image of every S_i-cluster of $\mathcal{G}$ is an E_i-cluster of $\mathcal{F}$, for $i = 1, 2$.

Lemma 16. *$\mathcal{F}$ is a p-morphic image of $\mathcal{G}$ iff there is a partial surjective map $g : U \to W$ with the following properties:*

1. *For each $u \in U$, there is $v \in \mathrm{dom}(g)$ such that uS_1v.*
2. *For each $v \in \mathrm{dom}(g)$, the restriction $g \restriction (\mathrm{dom}(g) \cap S_1(v))$ is one-one and has range $E_1(g(v))$.*
3. *For each $u \in U$ there is $w \in W$ such that*
   (a) *$g(v)E_2w$ for all $v \in \mathrm{dom}(g) \cap S_2(u)$,*
   (b) *for each $w' \in W$,*

$$\left|\Big(E_1(w') \cap E_2(w)\Big) \setminus \mathrm{rng}(g \restriction S_2(u))\right| \leq$$

$$\left|\Big(S_2(u) \cap S_1(g^{-1}(E_1(w')))\Big) \setminus \mathrm{dom}(g)\right|.$$

Proof. Suppose there is a surjective p-morphism $f : U \to W$. Then for each S_1-cluster $C \subseteq U$, the map $f \restriction C$ is a surjection from C onto $E_1(f(u))$ for any $u \in C$, so we may choose $C' \subseteq C$ such that $f \restriction C'$ is a bijection from C' onto $E_1(f(u))$. Let $U' = \bigcup\{C' : C \text{ is an } S_1\text{-cluster of } \mathcal{G}\}$. Then it is easy to check that $g = f \restriction U'$ satisfies conditions 1–3 of the lemma.

Conversely, let g be as stated. We will extend g to a surjective p-morphism $f : U \to W$. Since U is a disjoint union of S_2-clusters, it is enough to define f on an arbitrary S_2-cluster of $\mathcal{G}$. Pick $u \in U$. We will extend $g \restriction S_2(u)$ to the whole of $S_2(u)$. Pick $w \in W$ according to condition 3 of the lemma. By condition 3(a), $\mathrm{rng}(g \restriction S_2(u)) \subseteq E_2(w)$. Now we extend g to f such that $\mathrm{rng}(f \restriction S_2(u)) = E_2(w)$ and $f(x)E_1g(v)$ whenever $v \in \mathrm{dom}(g)$ and $x \in S_2(u) \cap S_1(v)$.

Pick any $w' \in W$ and consider $X_{w'} = S_2(u) \cap S_1(g^{-1}(E_1(w'))$. By conditions 1 and 2, $S_2(u) = \bigcup\{X_{w'} : w' \in W\}$ and $X_{w'} \cap X_{w''} = \emptyset$ whenever $\neg(w'E_1w'')$. We take the restriction of g to $X_{w'}$ (this restriction may be empty), and extend it to a surjection from $X_{w'}$ onto $E_1(w') \cap E_2(w)$. By condition 3, we have $|X_{w'} \setminus \mathrm{dom}(g)| \geq |E_1(w') \cap E_2(w) \setminus \mathrm{rng}(g \upharpoonright S_2(u))|$. So, there exists a surjection $f_{X_{w'}} : X_{w'} \to E_1(w') \cap E_2(w)$ extending g. Repeating this for a representative w' of each E_1-cluster in turn yields an extension of g to $S_2(u)$. Repeating for a representative u of each S_2-cluster in turn yields an extension of g to U as required.

It is left to show that f is a p-morphism. But it follows immediately from the construction of f that $f \upharpoonright S_i(u) : S_i(u) \to E_i(f(u))$ is surjective for each $u \in U$ and each $i = 1, 2$. As we pointed out above this implies that f is a p-morphism. □

Corollary 17. *It is decidable in polynomial time in the size of $\mathcal{G}$, whether $\mathcal{F}$ is a p-morphic image of $\mathcal{G}$.*

Proof. By Lemma 16 it is enough to check whether there exists a partial map $g : U \to W$ satisfying conditions 1–3 of the lemma. There are at most $n(L)$ E_1-clusters in $\mathcal{G}$, and the restriction of g to each E_1-cluster is one-one; hence, $d = |\mathrm{dom}(g)| \leq n(L) \cdot |W|$, and this is independent of $\mathcal{G}$. There are at most $d^{|W|}$ maps from a set of size at most d onto W. Obviously, there are $\binom{|U|}{d} \leq |U|^d$ subsets of U of size d. Hence there are at most $d^{|W|}|U|^d$ partial maps which may satisfy conditions 1 and 2 of the lemma. Our algorithm enumerates all partial maps from U to W with domain of size at most d, and for each one, checks whether it satisfies conditions 1–3 or not. It is not hard to see that this check can be done in p-time; indeed, it is clear that conditions 1 and 2 can be checked in time polynomial in $|U|$ and there is a first-order sentence $\sigma_{\mathcal{F}}$ such that $\mathcal{G} \models \sigma_{\mathcal{F}}$ iff $\mathcal{G}$ satisfies condition 3. The algorithm states that $\mathcal{F}$ is a p-morphic image of $\mathcal{G}$ if and only if it finds a map satisfying the conditions. Therefore, this is a p-time algorithm checking whether $\mathcal{F}$ is a p-morphic image of $\mathcal{G}$. □

Corollary 18. *Let L be a proper normal extension of* $\mathbf{S5}^2$.

1. *It can be checked in polynomial time in $|U|$ whether a finite* $\mathbf{S5}^2$*-frame $\mathcal{G} = (U, S_1, S_2)$ is an L-frame.*
2. *L is NP-complete.*

Proof. 1. Follows directly from Theorem 2, Corollary 17, and the fact that $\mathbf{M}_L$ is finite.

2. It is a well-known result of modal logic (see, e.g., [4, Lemma 6.35]) that if L is a consistent normal modal logic having the poly-size model property, and the problem of whether a finite structure $\mathcal{A}$ is an L-frame is decidable in time polynomial in the size of $\mathcal{A}$, then the satisfiability problem of L is NP-complete. The poly-size model property of every $L \supset \mathbf{S5}^2$ is proven in [3, Corollary 9]. (1) implies that the problem $\mathcal{G} \in \mathbf{F}_L$ can be decided in polynomial time in the size of $\mathcal{G}$. The result follows.

□

Acknowledgments The authors thank Szabolcs Mikulás, David Gabelaia, Yde Venema and Clemens Kupke for helpful discussions and encouragement. The second author was partially supported by UK EPSRC grant GR/S19905/01.

References

[1] N. Bezhanishvili, *Varieties of two-dimensional cylindric algebras. Part I: Diagonal-free case*, Algebra Universalis, 48 (2002), pp. 11–42.

[2] N. Bezhanishvili, *Varieties of two-dimensional cylindric algebras. Part II*, Algebra Universalis, to appear.

[3] N. Bezhanishvili and M. Marx, *All proper normal extensions of* **S5**-*square have the polynomial size model property*, Studia Logica, 73 (2003), pp. 367–382.

[4] P. Blackburn, M. de Rijke, Y. Venema, *Modal Logic*, Cambridge University Press, 2001.

[5] D. Gabbay, A. Kurucz, F. Wolter, M. Zakharyaschev, *Many-Dimensional Modal Logics: Theory and Applications*, Studies in Logic, vol. 148, North-Holland, 2003.

[6] E. Grädel, P. Kolaitis, M. Vardi. *On the decision problem for two-variable first order logic.* Bulletin of Symbolic Logic, 3 (1997), pp. 53–69.

[7] R. Laver, *Better-quasi-orderings and a class of trees,* in: Studies in Foundations and Combinatorics, Gian-Carlo Rota, ed., vol. 1 of Advances in Mathematics Supplementary Studies, Academic Press, 1978, pp. 31–48.

[8] R. Rado, *Partial well ordering of sets of vectors*, Mathematica, 1 (1954), pp. 89–95.

[9] K. Segerberg, *Two-dimensional modal logic*, Journal of Philosophical logic, 2 (1973), pp. 77–96.

ILLC
University of Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands
nbezhani@science.uva.nl

Department of Computing
Imperial College London
South Kensington Campus
London SW7 2AZ
UK
imh@doc.ic.ac.uk