In the present paper we consider modal propositional logic and look for the constraints that are imposed to the propositions of the special type $\Box a$ by the structure of the relevant finite Kripke frame. We translate the usual language of modal propositional logic in terms of notions of commutative algebra, namely polynomial rings, ideals, and bases of ideals. We use extensively the perspective obtained in previous works in Algebraic Statistics. We prove that the constraints on $\Box a$ can be derived through a binomial ideal containing a toric ideal and we give sufficient conditions under which the toric ideal fully describes the constraints.

1. Introduction

Propositional Modal Logic extends propositional logic by adding two operators, $\Box$ and $\Diamond$. Given a proposition $p$, one can form the propositions: $\Box p$, which can be read “necessarily $p$”; and $\Diamond p$, which can be read “possibly $p$”.

One of the two operators can be taken as primitive and the other as defined, setting

(1) $\Diamond p = \neg \Box \neg p$ or $\Box p = \neg \Diamond \neg p$.

S.A. Kripke [6] has provided a semantics for modal logic consisting in fixing a set of possible worlds and a binary relation specifying which worlds $w'$ are accessible from a given world $w$. This is formalised in the following definition, see e.g. [3].

Let $\mathcal{P}$ be the set of modal formulas, built starting with a given set of propositional variables.

Definition 1.

• A Kripke frame is a pair $\mathcal{K} = (W, \mathcal{E})$ where $W$, called the universe of $\mathcal{K}$, is a non-empty set of worlds and $\mathcal{E}$ is a binary relation on $W$.

• A Kripke frame $\mathcal{K} = (W, \mathcal{E})$ is locally finite if for every $w \in W$ the set $\{w' \in W | (w, w') \in \mathcal{E}\}$ is finite.

• A subframe of the Kripke frame $\mathcal{K} = (W, \mathcal{E})$ is a Kripke frame $\mathcal{K}' = (W', \mathcal{E}')$ such that $W' \subseteq W, \mathcal{E}' = \mathcal{E} \cap (W' \times W')$.

• A Kripke model $\mathcal{K}_\Phi = (W, \mathcal{E}, \Phi)$ is a Kripke frame $\mathcal{K} = (W, \mathcal{E})$ endowed with a function $\Phi$ from $\mathcal{P} \times W$ to the Boolean algebra $\{0, 1\}$, assigning a truth value $\Phi(p, w)$ — that can be either 0 (false) or 1 (true) — at each world $w$ for each proposition $p$. Such an assignment must satisfy the following conditions:

\begin{align*}
&\neg \Phi(\neg p, w) = 1 - \Phi(p, w) \\
&\bigwedge (\Phi(p, q, w) = \Phi(p, w)\Phi(q, w)) \\
&\bigvee (\Phi(\Box p, w) = \bigwedge_{(w, w') \in \mathcal{E}} \Phi(p, w'))
\end{align*}

From these equations one can recover the conditions on the remaining logical symbols $\lor, \to, \leftrightarrow, \Diamond$ (see also Tab. [1]).

2010 Mathematics Subject Classification. Primary 03B45, 13P25. Secondary 13P10, 62H17.
In the notation of mathematical logic, the equation $\Phi(p, w) = 1$ is often written $(\mathcal{K}_\Phi, w) \models p$. If $(\mathcal{K}_\Phi, w) \models p$ for all $w \in W$, then one can write $\mathcal{K}_\Phi \models p$; if $\mathcal{K}_\Phi \models p$ for all possible $\Phi$, this is denoted $\mathcal{K} \models p$.

Notice also that different propositions $p, q$ (i.e., $p$ and only if, the monoid $\{0, 1\}$ when the Kripke model $\mathcal{K}_0$ of this happens exactly when $\square p$ as the proposition. For instance, the proposition $\square p$ is true in a world $w$ if, and only if, $p$ is true in any world $w'$ which is accessible from $w$. So, its truth value is

$$\square p(w) = \prod_{(w, w') \in \mathcal{E}} p(w').$$

Notice also that different propositions $p, q$ may give rise to the same function $W \to \{0, 1\}$: this happens exactly when $\mathcal{K}_\Phi \models p \iff q$.

Eq. (2) defines $\square$ as a function (in fact, a morphism — see Proposition 3 below) from the monoid $\{0, 1\}^W$ (endowed with the operation of pointwise multiplication) to itself. As function $\square$ depends on the Kripke frame $\mathcal{K}$, one should denote it by $\square_{\mathcal{K}}$; however, we drop subscript $\mathcal{K}$ unless there is more than one Kripke model at stake.

Since the elements of $\{0, 1\}^W$ are the characteristic functions — or indicator functions in the probabilistic and statistical literature, where characteristic function has a different meaning — of subsets of $W$, function $\square$ can also be viewed as a function of the monoid $\mathcal{P}(W)$, the powerset of $W$ endowed with the operation of intersection, into itself, defined by

$$w \in \square A \iff \forall w' \in W \ (w \mathcal{E} w' \Rightarrow w' \in A).$$

In the present paper we discuss some properties of $\square$ with special reference to the tools of Polynomial Commutative Algebra, as it is done in Algebraic Statistics (see [7] for a general reference). Such an approach is suggested by the form of Eq. (2). In section 2 we characterize when $\square$ is an isomorphism, while in section 3 we describe an algebraic method to obtain binomial equations for range($\square$), the range of operator $\square$, seen as a subvariety of the affine space $\mathbb{C}^K$, in the case the Kripke frame is finite and has cardinality $K$.

### 2. Operator $\square$ as a morphism

We denote by $\mathcal{F}(W)$ the set of all complex-valued functions on $W$. So $\{0, 1\}^W$ is a subset of $\mathcal{F}(W)$, namely it is the set of those functions $a$ such that $a^2 = a$.

Given a Kripke frame $\mathcal{K} = (W, \mathcal{E})$, the adjacency matrix of $\mathcal{K}$ is the matrix $E : W \times W \to \{0, 1\}$ such that $w \mathcal{E} w'$ if, and only if, $E(w, w') = 1$. Each $w \in W$ has a set of neighbors $N(w) = \{w' \in W \mid E(w, w') = 1\}$: we call this set the neighborhood of $w$.

Eq. (2), together with Eq. (1), defines modal operators on $\{0, 1\}^W$. However, when $\mathcal{K}$ is locally finite, such a definition extends to the entire set of functions $\mathcal{F}(W)$.

| $\neg a$       | $1 - a$       |
|---------------|--------------|
| $a \wedge b$  | $ab$         |
| $a \vee b$    | $a + b - ab$ |
| $a \rightarrow b$ | $1 - a + ab$ |
| $a \leftrightarrow b$ | $1 - a - b + 2ab$ |

**Table 1.** Algebraic translation of logical operators
**Definition 2 (Modal operators on complex-valued functions).** If $\mathcal{K}$ is locally finite, we define the operators $\Box : \mathcal{F}(W) \to \mathcal{F}(W)$ and $\Diamond : \mathcal{F}(W) \to \mathcal{F}(W)$ by

\[
\Box a(w) = \prod_{w' \in N(w)} a(w') \quad \text{and} \quad \Diamond a(w) = 1 - \Box(1 - a)(w) .
\]

Consider the adjacency matrix $E$ of the Kripke frame. We can write (3) as

\[
\Box a(w) = \prod_{w' \in W} a(w')^{E(w, w')} .
\]

**Proposition 3.** The modal operator $\Box$ is a homomorphism of the multiplicative monoid $\{0, 1\}^W$. If $\mathcal{K}$ is locally finite, then it extends to a homomorphism of the multiplicative monoid $\mathcal{F}(W)$.

**Proof.** In fact, $\Box 1 = 1$ and

\[
\Box(a \land b)(w) = \prod_{w' \in W} (a(w')b(w'))^{E(w, w')} = \prod_{w' \in W} a(w')^{E(w, w')} \prod_{w' \in W} b(w')^{E(w, w')} = (\Box a \land \Box b)(w) .
\]

A **cycle** in a Kripke frame $\mathcal{K} = (W, \mathcal{E})$ is a finite subframe $(\{x_0, \ldots, x_n\}, \mathcal{E'})$ such that $x_0 \mathcal{E} \ldots x_n \mathcal{E} x_0$, and the relation $\mathcal{E}'$ does not hold for any other pair of elements of $\{x_0, \ldots, x_n\}$ (notice that for $n = 0$ this means $x_0 \mathcal{E} x_0$, i.e., every loop is a cycle). A **line** is a subframe $(\{x_i\}_{i \in \mathbb{Z}}, \mathcal{E}')$ such that $\forall i, j \in \mathbb{Z}$ $(x_i \mathcal{E} x_j \iff j = i + 1)$ (in particular, lines are infinite and do not contain cycles).

We are now able to show that $\Box$ is an isomorphism if and only if the Kripke frame is a disjoint union of its cycles and lines.

**Theorem 4.** Let $\{(W_i, \mathcal{E}_i)\}_{i \in I}$ be the collection of all cycles and lines of the Kripke frame $\mathcal{K} = (W, \mathcal{E})$. Then modal operator $\Box : \{0, 1\}^W \to \{0, 1\}^W$ is an isomorphism if and only if:

- $W = \bigcup_{i \in I} W_i$ and this is a disjoint union; and
- $\mathcal{E} = \bigcup_{i \in I} \mathcal{E}_i$ and this is a disjoint union.

**Proof.** Assume first that the condition on the Kripke frame holds. Then for every $w \in W$ there is exactly one element $S(w) \in W$ such that $w \mathcal{E} S(w)$; similarly, there is exactly one element $P(w) \in W$ such that $P(w) \mathcal{E} w$, and functions $S, P : W \to W$ are bijections such that $P = S^{-1}$. So, $\forall a \in \{0, 1\}^W \forall w \in W \Box a(w) = aS(w)$. Consequently, given any $b \in \{0, 1\}^W$ one has $\forall w \in W b(w) = \Box(bP)(w)$, showing that $b = \Box(bP)$ and that $\Box$ is surjective. On the other hand, let $a, a' \in \{0, 1\}^W$ be such that $a(w) \neq a'(w)$ for some $w \in W$; then $\Box a(P(w)) = a(w) \neq a'(w) = \Box a'(P(w))$, establishing the injectivity of $\Box$.

Conversely, assume that $\Box$ is bijective.

First notice that given any $w \in W$ there must be some $w' \in W$ with $w \mathcal{E} w'$; otherwise for any $a \in \{0, 1\}^W$ one would have $\Box a(w) = 1$, contradicting the surjectivity of $\Box$. We claim now that for every $w \in W$ there is $y \in W$ such that $w \mathcal{E} y$ and for no $z \neq w$ one has $z \mathcal{E} y$. Otherwise, if $w$ is such that every time $w \mathcal{E} y$ there is $z \neq w$ such that $z \mathcal{E} y$, given $a$ with $\Box a(w) = 0$ there would exist $z \neq w$ such that $\Box a(z) = 0$. But then the function taking value $0$ in $w$ and $1$ elsewhere would not be in the range of $\Box$, reaching a contradiction. So let $S : W \to W$ be a function assigning to each $w$ an element $y$ as above.
Analogously, given any \( w \in W \) there exists \( w' \in W \) such that \( w' \mathcal{E} w \) : otherwise if \( a, a' \in \{0, 1\}^W \) agree everywhere except on \( w \), then \( \Box a = \Box a' \), against the injectivity of \( \Box \). Moreover, for every \( w \in W \) there exists \( y \in W \) such that \( y \mathcal{E} w \) and for no \( z \neq w \) one has \( y \mathcal{E} z \). Indeed, if \( w \) were such that each time \( y \mathcal{E} w \) there exists \( z \neq w \) with \( y \mathcal{E} z \), let \( a, a' \in \{0, 1\}^W \) be such that:

- \( a(z) = 0 \) whenever there is \( y \in W \) such that \( y \mathcal{E} w, y \mathcal{E} z \) both hold (in particular, \( a(w) = 0 \))
- \( a' \) agrees with \( a \) on \( W \setminus \{w\} \), but \( a'(w) = 1 \)

Then \( \Box a = \Box a' \), contradicting the fact that \( \Box \) is injective. This allows to define a function \( P : W \to W \) assigning to every \( w \) an element \( y \) as above.

Notice now that, for all \( w \in W \), one has both \( PS(w) = w \) and \( SP(w) = w \), that is \( P = S^{-1} \). This implies that for every \( w \in W \) there is a unique \( y \in W \) such that \( w \mathcal{E} y \), namely \( y = S(w) \); similarly, there is a unique \( z \in W \) such that \( z \mathcal{E} w \), namely \( z = P(w) \). So the desired decomposition of \( \mathcal{K} \) into cycles and lines follows. \( \square \)

As a consequence, on a finite frame, operator \( \Box \) is an isomorphism if and only if the frame is the disjoint union of its cycles.

**Corollary 5.** Let \( \mathcal{K} = (W, \mathcal{E}) \) be a finite Kripke frame, and let \( \{(W_i, \mathcal{E}_i)\}_{i \in I} \) be the collection of all cycles of \( \mathcal{K} \). Then the modal operator \( \Box : \{0, 1\}^W \to \{0, 1\}^W \) is injective if and only if it is surjective, if and only if for every \( W_i \) is a partition of \( W \) and \( \mathcal{E}_i \), \( i \in I \), is a partition of \( \mathcal{E} \).

**Proof.** The first equivalence holds as \( \{0, 1\}^W \) is finite. As for the second one, use Theorem 4 and the observation that every line is infinite. \( \square \)

An inspection of the proof of Theorem 4 provides also the following fact, which seems to have independent interest.

**Proposition 6.** Let \( \mathcal{K} \) be a finite Kripke frame, and suppose that all \( b \in \{0, 1\}^W \) assuming exactly once value 0 are in the range of \( \Box \). Then \( \Box \) is an isomorphism.

**Proof.** The argument in the proof of Theorem 4 shows the existence of a function \( S : W \to W \) such that, for each \( w \in W \), the element \( S(w) \) is such that \( w \mathcal{E} S(w) \) and for no \( z \neq y \) one has \( z \mathcal{E} S(w) \). In particular, \( S \) is injective. Fix any \( w_0 \in W \) and, for every \( n \in \mathbb{N} \), let \( w_n = S^n(w_0) \). By the finiteness of \( W \), there is a least \( n \in \mathbb{N} \) such that there is \( m > n \) with \( w_m = w_n \). Let \( m \) be the least such. If \( n > 0 \), then \( w_{n-1} \mathcal{E} w_n = S(w_{n-1}), w_{m-1} \mathcal{E} w_n = S(w_{m-1}) \), contradicting the injectivity of \( S \). So \( n = 0 \), and \( \mathcal{K}' = (\{w_0, \ldots, w_{m-1}\}, \mathcal{E}') \) is a cycle in \( \mathcal{K} \), where \( \mathcal{E}' \) coincides with the graph of the restriction of \( S \) to \( \{w_0, \ldots, w_{m-1}\} \).

Repeating the argument starting with an element in \( W \setminus \{w_0, \ldots, w_{m-1}\} \), if any, and then iterating it a finite number of times, yields \( W \) as a disjoint finite union of cycles. Notice that if \( w, w' \) belong to different cycles then \( (w, w') \notin \mathcal{E} \), since \( w' = S(w'') \) for some \( w'' \) in the same cycle as \( w' \); consequently \( w'' \) is the unique element \( z \) such that \( z \mathcal{E} w' \). It follows that the condition of Corollary 5 is satisfied, and \( \Box \) is an isomorphism. \( \square \)

**Remark 7.** The monoid \( \{0, 1\}^W \) carries also a partial order \( \leq \) defined by letting \( a \leq b \Leftrightarrow \forall w \in W \ a(w) \leq b(w) \). The operator \( \Box \) satisfies the following properties concerning this partial order:

- \( a \leq b \Rightarrow \Box a \leq \Box b \)
- \( \mathcal{E} \subseteq \mathcal{E}' \Rightarrow \forall a \in \{0, 1\}^W \ \Box_{(W, \mathcal{E}')} a \leq \Box_{(W, \mathcal{E})} a \)
- For any \( b \) in the range of \( \Box \), there is a \( \leq \)-least \( a \) such that \( \Box a = b \).
In the next section we present an algorithmic way to describe the range of $\square$ through systems of binomial equations, assuming that the Kripke frame is finite.

3. An application of toric ideals

Throughout this section a finite Kripke frame $K = (W,E)$ is given, where we can assume that $W = \{1, \ldots, K\}$. The adjacency matrix of $E$ is denoted by $E$ and $e_w$ is the $w$-th row of $E$. Since we deal with functions $a : W \to \{0, 1\}$, so with elements of $\{0, 1\}^K$, the range of $\square$ is a subset of $\{0, 1\}^K$. We want to obtain equations for range($\square$) as a subvariety of $\mathbb{C}^K$ — the use of the field $\mathbb{C}$ allowing us to apply well established results in Commutative Algebra.

Recall that, given an ideal $I$ in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$, the variety of $I$ is the set

$$V(I) = \{a \in \mathbb{C}^n | \forall f \in I \ f(a) = 0\}.$$ 

Conversely, for $A \subseteq \mathbb{C}^n$, the ideal of $A$ is

$$\text{Ideal}(A) = \{f \in \mathbb{C}[x_1, \ldots, x_n] | \forall a \in A \ f(a) = 0\}.$$ 

Since every ideal is finitely generated we write $I = \langle f_1, \ldots, f_r \rangle$ for the ideal generated by the polynomials $f_1, \ldots, f_r$.

From the definition of the modal operator in Eq. (3) we see that each value $\square a(w)$ has the algebraic form of a square-free monomial in the indeterminates $a(w')$, $w' \in W$. We are in the special case where the value of each indeterminate is either 0 or 1. We thus consider two sets of indeterminates:

- $t_w = a(w), \ w \in W$;
- $z_w = \square a(w), \ w \in W$,

and work in the polynomial ring $\mathbb{C}[t_w, z_w : w \in W]$.

Since $a(w) \in \{0, 1\}$ for all $w$, we define a first set of equations and the corresponding ideal

$$t_w^2 - t_w = 0, \quad w \in W; \quad \mathcal{I}_L = \langle t_w^2 - t_w : w \in W \rangle.$$ 

From Eq. (3), we define a second set of equations involving the $z$’s and the corresponding ideal

$$z_w - \prod_{w' \in N(w)} t_{w'} = 0, \quad w \in W; \quad \mathcal{I}_T = \left\langle z_w - \prod_{w' \in N(w)} t_{w'} : w \in W \right\rangle.$$ 

The ideal $\mathcal{I}_T$ in Eq. (5) is a toric ideal in the indeterminates $z_w, w \in W$. Toric ideals are special binomial ideals, see e.g. [9] Ch. 4] for a general reference on toric ideals. They are applied in many contexts, and especially in Algebraic Statistics for contingency tables, to describe varieties (i.e., statistical models) for finite sample spaces, see e.g. [8].

Now, define the ideal

$$\mathcal{I} = \mathcal{I}_L + \mathcal{I}_T$$

and consider the affine space $\mathbb{C}^{2K} = \mathbb{C}_t^K \times \mathbb{C}_z^K$.

So, in the space $\mathbb{C}^{2K}$ we can define the varieties $V(\mathcal{I}_L), V(\mathcal{I}_T)$, and $V(\mathcal{I})$. While the variety $V(\mathcal{I}_L)$ is clearly the set of all points whose $t$-coordinates are 0 or 1, the other two varieties are more interesting. In particular, note that the variety $V(\mathcal{I}_T)$ is the toric variety of the adjacency matrix $E$ of the graph.
The projections of such varieties onto the affine space \( \mathbb{C}_z^K \) are denoted with

\[
\widetilde{V}(I_L) = \text{pr}_{\mathbb{C}_z^K} V(I_L) \quad \widetilde{V}(I_T) = \text{pr}_{\mathbb{C}_z^K} V(I_T) \quad \widetilde{V}(I) = \text{pr}_{\mathbb{C}_z^K} V(I).
\]

Notice that \( \widetilde{V}(I) = \text{range}(\square) \).

On the other hand, let the elimination ideals of the \( t \)'s indeterminates be:

\[
\widetilde{I}_L = \text{Elim} \left( (t_w)_{w \in W}, I_L \right) \quad \widetilde{I}_T = \text{Elim} \left( (t_w)_{w \in W}, I_T \right) \quad \widetilde{I} = \text{Elim} \left( (t_w)_{w \in W}, I \right).
\]

It is known, see e.g. [3], that the varieties of such elimination ideals are the Zariski closure of the above projections. Since every finite variety is Zariski closed, we can conclude that

\[
\text{range}(\square) = \widetilde{V}(I) = V(\widetilde{I})
\]

Consequently, any set of generators of \( \widetilde{I} \) provides a system of equations for \( \text{range}(\square) \). Moreover, notice that the ideal \( \widetilde{I} \) is both an elimination ideal and a binomial ideal (see e.g. [3]). Thus, a set of generators of such an ideal can be computed through Gröbner bases with symbolic software (in the examples at the end of this section we have used CoCoA, see [2]).

For any \( \alpha \in \mathbb{Z}^K \), let \( \alpha_+, \alpha_- \in \mathbb{N}^K \) have disjoint support and be such that \( \alpha = \alpha_+ - \alpha_- \). The following proposition uses the theory of toric ideals of Sturmfels, see [9], and it describes the generators of the ideals \( \widetilde{I}_T \) and \( \widetilde{I} \). Recall that, given \( \beta \in \mathbb{N}^K \), a compact expression like \( z^\beta \) denotes the product \( \prod_{i=1}^{K} z_i^{\beta(i)} \).

**Proposition 8.**

(1) The ideal \( \widetilde{I}_T \) is generated by the binomials

\[
z^{\alpha_+} - z^{\alpha_-}, \quad \alpha \in \mathbb{Z}^K \cap \text{Ker} (E^t) ;
\]

(2) The ideal \( \widetilde{I} \) is generated by the binomials

\[
z_w^2 - z_w, \quad w \in W
\]

and by the square-free binomials of the form \( z^u - z^v \) with \( u, v \in \{0,1\}^K \) such that \( \text{supp}(E^t u) = \text{supp}(E^t v) \)

**Proof.** (1) This is, for instance, [10, Lemma 1.1(a)].

(2) Since \( \widetilde{I} \) is a binomial ideal, we only need to find the generators of \( \widetilde{I} \) by looking at the binomials of \( \mathbb{C}[z] \) belonging to \( \widetilde{I} \).

Ideal \( \widetilde{I} \) contains the binomials

\[
z_w^2 - z_w, \quad w \in W.
\]

Moreover, \( \widetilde{I} \) contains a square-free binomial of the form \( z^u - z^v \) with \( u, v \in \{0,1\}^K \) if and only if \( \text{supp}(E^t u) = \text{supp}(E^t v) \). In fact, in \( \mathbb{C}[z,t] \) we have

\[
z^u - z^v = \prod_{w \mid u(w) = 1} \prod_{w' \in N(w)} t_{w'} - \prod_{w \mid v(w) = 1} \prod_{w' \in N(w)} t_{w'}
\]

\[
= \prod_{w'} t_{\sum_{w' \mid E(u = 1, w')} = 1} - \prod_{w'} t_{\sum_{w' \mid E(1, w')} = 1}
\]

and this binomial belongs to \( \widetilde{I} \) if and only if \( \text{supp}(E^t u) = \text{supp}(E^t v) \).

**Remark 9.**

(1) If \( \alpha \in \mathbb{Z}^K \cap \text{Ker} (E^t) \), letting \( u, v \in \{0,1\}^K \) be defined by

\[
u(w) = \min(1, \alpha_+(w)), \quad u(w) = \min(1, \alpha_-(w))
\]

then \( \text{supp}(E^t u) = \text{supp}(E^t v) \); in other words, each of the binomials generating \( \widetilde{I}_T \) as for Proposition 8(1) gives rise to a binomial in the set of generators for \( \widetilde{I} \).
described in Proposition 8(2). In fact, \( \widehat{\mathcal{T}} \subseteq \widehat{\mathcal{I}} \). However the binomials obtained in this way, together with the binomials \( z_w^2 - z_w \), are in general not enough to generate \( \widehat{\mathcal{I}} \): see, for instance, Examples 14, 15, and 16 below. We give in Proposition 12 a condition under which they suffice.

(2) Proposition 8(1) says that all \( \Box a \), in addition to assuming values in \( \{0, 1\} \), are subject to the following constraints:

\[
\prod_{w \in W} (\Box a(w))^{\alpha(w)} = \prod_{w \in W} (\Box a(w))^{\alpha(w)}, \quad \alpha \in \mathbb{Z}^K \cap \text{Ker} (E').
\]

Similarly as what remarked above, the equations (6), together with the requirements of taking values in \( \{0, 1\} \), are in general not enough to define the range of \( \Box \): see Examples 14 and 16.

We want now to show that if the Kripke frame has the property that any two neighborhoods (see section 2) are either disjoint or they coincide, then range(\( \Box \)) can be defined by a system of equations using only the generators of \( \widehat{\mathcal{T}} + \langle z_w^2 - z_w : w \in W \rangle \).

**Definition 10.** We say that the Kripke frame \( \mathcal{K} \) is a cut-frame if

\[
\forall w, w' \in W \ (N(w) \cap N(w') \neq \emptyset \Rightarrow N(w) = N(w')).
\]

Notice indeed that if \( \mathcal{K} \) is a cut-frame, then the neighborhoods \( N(w) \) cut \( \bigcup_{w \in W} N(w) \) into a partition.

Examples of cut-frames are those for which \( \Box \) is an isomorphism (Corollary 3): for such frames, \( \widehat{\mathcal{T}} \) is the null ideal, and \( \widehat{\mathcal{I}} = \langle z_w^2 - z_w : w \in W \rangle \). Also, all \( \mathcal{K} \) = \( (W, E) \) with \( E \) an equivalence relation are cut-frames: this is the class of Kripke frames defined by epistemic logic S5, that is the logic characterized by the axioms \( \square p \to p \) and \( \Diamond p \to \square \Diamond p \), see e.g. 3. Other notable examples of cut frames are bipartite graphs.

Denote \( J = \widehat{\mathcal{T}} + \langle z_w^2 - z_w : w \in W \rangle \).

**Lemma 11.** Assume that \( \mathcal{K} \) is a cut-frame. Then \( J \) is a radical ideal.

**Proof.** Under the hypothesis, matrix \( E \) has the property that given any two rows \( e_{w_0}, e_{w_1} \), either they are equal — and this happens when \( N(w_0) = N(w_1) \) — or they never have a 1 on the same column. This implies that if \( N(w_0) = N(w_1) \), for some \( w_0 \neq w_1 \), and if \( \alpha \in \mathbb{Z}^K \) is such that

\[
\begin{align*}
\alpha(w_0) &= 1 \\
\alpha(w_1) &= -1 \\
\alpha(w) &= 0 \text{ for } w \in W \setminus \{w_0, w_1\}
\end{align*}
\]

then \( \alpha \in \text{Ker} (E') \), so \( z_{w_0} - z_{w_1} \in \widehat{\mathcal{T}} \). Also, if \( N(w) = \emptyset \) and \( \alpha \in \mathbb{Z}^K \) is such that

\[
\begin{align*}
\alpha(w) &= 1 \\
\alpha(w') &= 0 \text{ for } w' \in W \setminus \{w\}
\end{align*}
\]

then \( \alpha \in \text{Ker} (E') \), whence \( z_w - 1 \in \widehat{\mathcal{T}} \). In fact, every element of \( \mathbb{Z}^K \cap \text{Ker} (E') \) is a linear combination of vectors as in (8) and (9) with integer coefficients.

Let \( J' = \langle z_{w_0} - z_{w_1} : N(w_0) = N(w_1) \rangle + \langle z_w - 1 : N(w) = \emptyset \rangle + \langle z_w^2 - z_w : w \in W \rangle \).

**Claim.** \( J = J' \).

**Proof of the claim.** Every generator of \( J' \) is a generator of \( J \). For the converse, it is enough to consider the binomials \( z^{\alpha +} - z^{\alpha -} \), where \( \alpha \in \mathbb{Z}^K \cap \text{Ker} (E') \).
Let \( \tilde{W} = \{ w \in W \mid N(w) \neq \emptyset \} \). On \( \tilde{W} \) define the equivalence relation \( \sim \) by letting \( w \sim w' \iff N(w) = N(w') \). Notice that \( \alpha \in \ker (E') \) if and only if, for every equivalence class \( C \), one has \( \sum_{w \in C} \alpha(w) = 0 \). This implies that, for such \( \alpha, C \),
\[
\exists w \in C \alpha(w) > 0 \iff \exists w \in C \alpha(w) < 0 .
\]
So, if \( \alpha \in \mathbb{Z}^K \cap \ker (E') \), using the generators of \( J' \) of the form \( z_{w_0} - z_{w_1} \) (for \( N(w_0) = N(w_1) \)) and \( z_w^2 - z_w \) (for \( w \in W \)), one can find \( u, v \in \{ 0, 1 \}^K \) satisfying the equality
\[
z^{a+}_u - z^{a-}_v + J' = z^u - z^v + J'
\]
and such that
- if \( w \in \tilde{W} \), then \( u(w) = v(w) \)
- in each equivalence class there is at most one element \( w \) such that \( u(w) = v(w) = 1 \)
- if \( w \in \tilde{W} \) and \( \{ w \} \) is a singleton equivalence class, then \( u(w) = v(w) = 0 \)
- if \( w \in W \setminus \tilde{W} \), then at most one between \( u(w), v(w) \) equals 1
Using now the generators of \( J' \) of the form \( z_w - 1 \), for \( w \in W \setminus \tilde{W} \), one obtains that \( z^u - z^v \in J' \), that is \( z^{a+} - z^{a-} \in J' \), concluding the proof of the claim. \( \square \)

To conclude the proof of the lemma, let \( f \in \mathbb{C}[z] \) be such that \( (f + J')^n \neq f^n + J' = J' \), in order to prove \( \widetilde{f} + J' = J' \). Let \( W^* \) be a maximal subset of \( W \) of pairwise inequivalent elements with respect to \( \sim \). It can be assumed that \( f = \sum_{w \in \{ 0, 1 \}^K} c_w z^w \). Any monomial \( M_u = c_u z^u \) in \( f \) corresponds to a subset of \( W^* \), namely \( W_u = \{ w \in W^* \mid u(w) = 1 \} \); the product \( M_{u_1} \cdots M_{u_p} \) of a subset of such monomials is equivalent, modulo \( J' \), to a monomial of the form \( (c_{u_1} \cdots c_{u_p})M_u \), where \( W_v = W_{u_1} \cup \ldots \cup W_{u_p} \). So \( f^n + J' = \sum_{w \in \{ 0, 1 \}^K} c_w^{2n} z^w + J' \), where each \( c_w' \) is obtained as a polynomial without term of degree 0 in the values \( c_{u'} \) for \( W_u \subseteq W_{u'} \). Since all \( c_{u'} \) are null, by induction on the number of components of \( u \) that are equal to 1 it follows that all \( c_u \) must equal 0, that is \( f + J' = J' \).

**Proposition 12.** Assume that \( K \) is a cut-frame. Then \( \tilde{I} = J \).

**Proof.** On the one hand \( J \subseteq \tilde{I} \), since all generators of \( J \) belong to \( \tilde{I} \).

Assume now that \( b \in V(J) \). This implies that \( b(w) \in \{ 0, 1 \} \) for all \( w \in W \), and that \( b(w_0) = b(w_1) \) whenever \( N(w_0) = N(w_1) \). So define \( a \in \{ 0, 1 \}^K \) by letting \( a(w') = b(w) \), for any \( w \) such that \( w' \in N(w) \), and defining \( a(w') \) arbitrarily if \( w' \in W \setminus \bigcup_{w \in W} N(w) \).

Then \( b = \square a \in \text{range}(\square) = V(\tilde{I}) \).

We have thus proved that \( V(J) \subseteq V(\tilde{I}) \), so that
\[
\tilde{I} \subseteq \sqrt{\tilde{I}} = \text{Ideal}(V(\tilde{I})) \subseteq \text{Ideal}(V(J)) = \sqrt{J} = J .
\]

Observe that \( (7) \) is not a necessary condition for the equality \( \tilde{I} = J \) (so neither for the equality \( \text{range}(\square) = V(J) \)). Let indeed \( W = \{ 1, 2, 3 \} \), with incidence matrix
\[
E = \begin{bmatrix}
1 & 2 & 3 \\
1 & 1 & 0 \\
2 & 0 & 1 \\
3 & 0 & 0 \\
\end{bmatrix} .
\]

Then \( \tilde{I} = J = \langle z_3 - 1, z_2 - z_1, z_1^2 - z_2, z_2^2 - z_3 \rangle \).

Moreover, the equality \( \tilde{I} = J \) is not a necessary condition for the equality \( \text{range}(\square) = V(J) \); see Example 15. 8
It is then natural to ask the following.

**Question 1.** Are there nice characterizations of the classes of Kripke frames $K$ such that

1. $J$ is a radical ideal?
2. the equality $\text{range}(\Box) = V(J)$ holds?
3. the equality $\tilde{I} = J$ holds?

The following is another example of a cut-frame, and it is also a simple illustration of the procedure discussed above.

**Example 13** (The symmetric 4-cycle). Consider the Kripke frame $K = (\{1,2,3,4\}, E)$, with adjacency matrix

$$E = \begin{bmatrix}
1 & 2 & 3 & 4 \\
1 & 0 & 1 & 0 \\
2 & 0 & 1 & 0 \\
3 & 0 & 1 & 0 \\
4 & 0 & 1 & 1
\end{bmatrix}.$$  

Notice that this Kripke frame is not a disjoint union of cycles, so by Corollary 5 the range of $\Box a$ is a proper subvariety of $\{0,1\}^4$.  

Eq. (11) becomes

$$\begin{cases}
\Box a(1) = a(2)a(4) \\
\Box a(2) = a(1)a(3) \\
\Box a(3) = a(2)a(4) \\
\Box a(4) = a(1)a(3)
\end{cases}.$$

Let $\gamma = (\gamma(1), \gamma(2), \gamma(3), \gamma(4))$ be a non-zero integer vector such that $E^t \gamma = 0$, so that

$$\begin{cases}
0 = \gamma(2) + \gamma(4) \\
0 = \gamma(1) + \gamma(3)
\end{cases}.$$

The solutions are all vectors of the form $(u, v, -u, -v)$ for $u, v \in \mathbb{Z}$. The vectors $(1,0,-1,0), (0,1,0,-1)$ generate with integer coefficients all such solutions, and have disjoint supports. These vectors can be split as

$$(1, 0, 0, 0) - (0, 0, 1, 0) = (1, 0, -1, 0), (0, 1, 0, 0) - (0, 0, 0, 1) = (0, 1, 0, -1).$$

So the ideal $\tilde{I}_T$ is generated by the binomials

$$(10) \quad z_1 - z_3, z_2 - z_4.$$

To generate $\tilde{I}$, in this case it is enough to add the binomials $z_w^2 - z_w$, since $K$ satisfies condition $\Box$. In conclusion the range of the necessitation operator $\Box$ consists of the 4 points

$$(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1).$$

Since the toric ideal $\tilde{I}_T$ associated to the adjacency matrix $E$ is a subset of the relevant binomial ideal $\tilde{I}$, this implies that a subset of the generators can be computed through specialized software for toric ideals (for instance, with 4ti2, see [11]). Such a computation exploits the special structure of toric ideals and therefore makes possible some computations also for large frames, where the elimination technique fails.

When the equality $\tilde{I} = J$ fails, the computation of $\tilde{I}$ is more complex. We present here some examples where such a computation has been carried out in CoCoA, [2].
Figure 1. The reflexive symmetric 4-cycle and its adjacency matrix.

\[
E = \begin{bmatrix}
1 & 2 & 3 & 4 \\
1 & 1 & 0 & 1 \\
2 & 1 & 1 & 0 \\
3 & 0 & 1 & 1 \\
4 & 1 & 0 & 1 \\
\end{bmatrix}
\]

Example 14 (The reflexive symmetric 4-cycle). Let us now consider the graph displayed in Fig. 1 together with its adjacency matrix. This is the reflexive version of Example 13. The corresponding elimination ideal is generated by:

\[
z_2z_3 - z_3z_4, -z_2z_4 + z_3z_4, -z_1z_3 + z_3z_4, -z_1z_4 + z_3z_4, -z_1z_2 + z_3z_4
\]

plus the binomials \(z_i^2 - z_i, i = 1, \ldots, 4\). In this example the toric ideal \(\widetilde{I}T\) is the null ideal.

Example 15 (The reflexive oriented 4-cycle). We slightly modify the adjacency matrix above by choosing an orientation in the 4-cycle. The graph and the adjacency matrix are displayed in Fig. 2.

In this case the elimination ideal \(\widetilde{I}\) is generated by:

\[
z_1z_3 - z_2z_4, -z_2z_3z_4 + z_2z_4, z_1z_2z_4 - z_2z_4
\]

plus the binomials \(z_i^2 - z_i, i = 1, \ldots, 4\). Here, the binomial \(z_1z_3 - z_2z_4\) belongs to the toric ideal \(\widetilde{I}_T\) and the toric ideal is actually a principal ideal generated by this binomial.

Notice that though in this example \(\widetilde{I} \neq J\), nevertheless the equality \(\text{range}(\Box) = V(\widetilde{I}) = V(J)\) holds.

Example 16. Let us consider the reflexive frame displayed in Fig. 3. In this tree-like structure, the value of \(\Box a\) at a given world depends on the value of \(a\) at the worlds that come from the same parent or are immediate descendants. Apart from the binomials \(z_i^2 - z_i, i = 1, \ldots, 10\), the binomial ideal \(\widetilde{I}\) is generated by 7 binomials:

\* 5 linear binomials, the generators of the toric ideal \(\widetilde{I}_T\):

\[
z_9 - z_{10}, z_7 - z_8, z_5 - z_6, z_3 - z_4, z_2 - z_4;
\]

\* 2 further reducible binomials not belonging to the toric ideal:

\[
-z_1z_6z_8z_{10} + z_4z_6z_8z_{10}, z_1z_4 - z_4.
\]
Remark 17. The operator ♦ can be described with the same technique. In fact,

\[ ♦ a_w = 1 - \prod_{w' \in N(w)} (1 - t_{w'}) \]

and one can use the theory above through the following substitutions:

\[ t'_w \mapsto 1 - t_w \quad z'_w \mapsto 1 - z_w. \]

Notice that the substitution \( t'_w \mapsto 1 - t_w \) together with \( t^2_w - t_w = 0 \) implies that \( (t'_w)^2 - t'_w = 0 \).

We close the paper with a general question. The techniques presented here rely on the finiteness of the Kripke frame \( K \) to produce the equations for the range of the modal operator \( \Box \) using algorithms and tools from Algebraic Statistics. So the following question arises.

**Question 2.** Can the methods discussed in this paper be adapted to give information for infinite \( K \)?

**Acknowledgements**

The authors would like to thank G. D’Agostino (University of Udine) and C. Bocci (University of Siena) for their criticism and comments on some earlier drafts of the paper. G. Pistone acknowledges the support of de Castro Statistics and of Collegio Carlo Alberto. He is a member of GNAMPA-INdAM. This research has a financial support of the Università del Piemonte Orientale.

**References**

[1] 4ti2 team, *4ti2—A software package for algebraic, geometric and combinatorial problems on linear spaces*, Available at www.4ti2.de.

[2] John Abbott, Anna M. Bigatti, and Giovanni Lagorio, *CoCoA-5: a system for doing Computations in Commutative Algebra*, Available at http://cocoa.dima.unige.it.
[3] Patrick Blackburn, Maarten de Rijke, and Yde Venema, *Modal logic*, Cambridge Tracts Theoret. Comput. Sci., Cambridge University Press, 2001.

[4] David Cox, John Little, and Donald O’Shea, *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra*, 4 ed., Undergrad. Texts Math., Springer, 2015.

[5] David Eisenbud and Bernd Sturmfels, *Binomial ideals*, Duke Math. J. **84** (1996), no. 1, 1–45.

[6] Saul A. Kripke, *Semantical analysis of modal logic. I. Normal modal propositional calculi*, Z. Math. Logik Grundlagen Math. **9** (1963), 67–96.

[7] Giovanni Pistone, Eva Riccomagno, and Henry P. Wynn, *Algebraic statistics: Computational commutative algebra in statistics*, Monogr. Statist. Appl. Probab., vol. 89, Chapman & Hall/CRC, 2001.

[8] Fabio Rapallo, *Toric statistical models: parametric and binomial representations*, Ann. Inst. Statist. Math. **59** (2007), no. 4, 727–740.

[9] Bernd Sturmfels, *Gröbner bases and convex polytopes*, Univ. Lecture Ser., vol. 8, American Mathematical Society, 1996.

[10] Bernd Sturmfels, *Equations Defining Toric Varieties*, Algebraic geometry Santa Cruz 1995, Proc. Sympos. Pure Math., vol. 62, American Mathematical Society, 1997, pp. 437–449.

**DEPARTMENT OF MATHEMATICAL SCIENCES «JOSEPH-LOUIS LAGRANGE», POLITECNICO DI TORINO, CORSO DUCA DEGLI ABRUZZI 24, 10129 TORINO — ITALY**

_E-mail address_: riccardo.camerlo@polito.it

**DE CASTRO STATISTICS, COLLEGGIO CARLO ALBERTO, PIAZZA VINCENZO ARBARELLO 8, 10122 TORINO — ITALY**

_E-mail address_: giovanni.pistone@carloalberto.org

**DIPARTIMENTO DI SCIENZE E INNOVAZIONE TECNOLOGICA, UNIVERSITÀ DEL PIEMONTE ORIENTALE, VIALE TERESA MICHEL 11, 15121 ALESSANDRIA — ITALY**

_E-mail address_: fabio.rapallo@uniupo.it