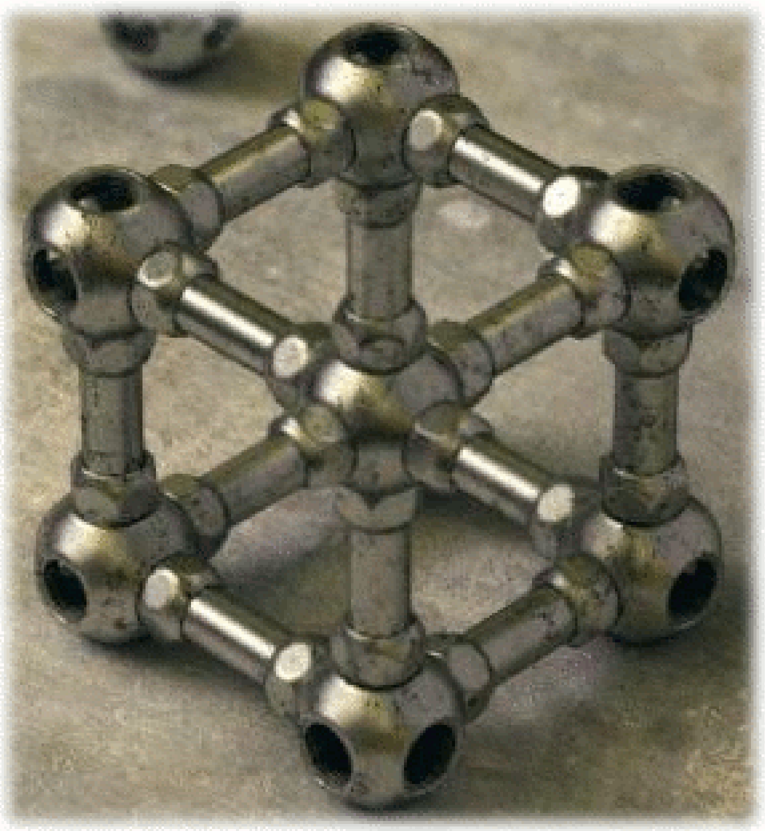

Entailment Multipliers: an Algebraic Characterization of Validity for Classical and Modal Logics [1]

Author(s):

Marcelo Finger

Mauricio S. C. Hernandes

[1] This work was supported by Fapesp Project LogProb, grant 2008/03995-5, São Paulo, Brazil.

Entailment Multipliers: an Algebraic Characterization of Validity for Classical and Modal Logics

Marcelo Finger* and Mauricio S. C. Hernandes**

Department of Computer Science
Institute of Mathematics and Statistics
University of Sao Paulo

mfinger@ime.usp.br mauhcs@gmail.com

Abstract. We propose a novel algebraic characterisation of the classical notion of validity in terms of boolean rings, called *entailment multipliers*. We demonstrate the existence of such multipliers and show how they can be used to derive stronger entailment statements. An interesting property of multipliers lies in their behaviour as invariants in a proof, a fact that is used to show how several inference systems can be employed to compute entailment multipliers. A similar characterisation of validity for modal logics is presented.

1 Introduction

The notions of logical consequence and logical validity have been explored under several points of view, mostly in terms of proof-theory and semantic entailment relations, but also in algebraic terms. In this work we propose an algebraic characterisation of the notion of logical validity, and study its relationship with proof-theoretical and semantic approaches.

Algebraic formulation of logics is usually presented in terms of boolean algebras and lattices. Here, however, we use as an underlying structure a *boolean ring*; the main motivation for the use of such structure comes from the work of Carnielli [6]. As usual, formulas can be represented algebraically as terms, and ring properties allow us to represent formulas in a more compact way.

Classical validity statements presented in terms of semantic entailment expressions or proof-theoretical sequents can be expressed as polynomials over boolean rings, where variables are inserted as *multipliers* of terms obtained from the algebraic translation of formulas in the validity statements. The main result of this work claims that such a statement is classically *valid* iff the corresponding polynomial has roots when equated to the unit (the *1-roots*).

On a different perspective, an application of this result can be seen as follows. It is quite widespread the opinion that proving a mathematical statement is

* Partly supported by CNPq grant PQ 301294/2004-6 and FAPESP project 2008/03995-5.

** Supported by CNPq grant 131263/2008-0.

more than knowing its validity. Proving brings *insight*, which may lead to a generalisation of the original statement.

The existence of entailment multipliers allows us to make such opinion formal, that is, we show how, given proof of a theorem, one can employ the *entailment multipliers* (that is, the 1-roots of the polynomial associated to the validity expression) to effectively compute a generalisation of the original theorem.

In this setting, given a proof of a validity statement $\mathcal{S}$:

$$A_1, \ldots, A_n \models B_1, \ldots, B_m$$

we compute another validity statement $\mathcal{S}'$

$$A'_1, \ldots, A'_n \models B'_1, \ldots, B'_m$$

that is stronger than $\mathcal{S}$, $\mathcal{S}' \geq \mathcal{S}$, in the sense that:

- $A_i \models A'_i$, $1 \leq i \leq n$; and
- $B'_j \models B_j$, $1 \leq j \leq m$

That is, both $\mathcal{S}$ and $\mathcal{S}'$ are valid, and $\mathcal{S}'$ has a weaker antecedent or a stronger conclusion, or both. Clearly, $\geq$ is a partial order. For example, from a Modus Ponens statement $\mathcal{S}_{MP} = A \to B, A \models B$, with the aid of entailment multipliers we can compute a stronger $S'_{MP} = A \to B, A \vee B \models B$. Several methods of computing the entailment multipliers are analysed associated to several proof methods.

1.1 Comparisons with the Literature

The method in the literature that best approaches ours is the use of Hilbert Nullstellensatz for propositional refutations, which was initially suggested by Lovász [12] and was independently proposed again in [1] and later developed in a series of works on what has bee termed the *algebraic propositional proof system* [13, 5, 2, 4].

In this approach, formulas are transformed into polynomials over a fixed algebraically closed field F. Satisfiability of a formula A is mapped as an equation $Q_A(\bar{x}) = 0$, where $Q_A(\bar{x})$ is the translation of the formula A as a polynomial over variables $\bar{x}$. Extra equations of the form $x_i^2 + x_i = 0$ are needed to ensure that each $x_i \in \bar{x}$ takes only values 0 or 1. Theorem proving is made by refutation, trying to show that a set of formulas is unsatisfiable. In such setting, one can apply Hilbert's (weak) Nullstellensatz, that states that a set a system of equations $Q_i(\bar{x}) = 0$ does not have a solution in F iff there are polynomials $P_i(\bar{x})$ such that $\sum_i P_i(\bar{x}) Q_i(\bar{x}) = 1$.

Although there is a similarity between this approach and ours, the main difference lies in the fact that it deals with fields, so that variables can take any variables over a field. This makes the translation of a polynomial back into a formula somewhat different. By using boolean rings, the translation back into formulas is immediate, and this fact will be used to proof-theoretical applications

1.2 Organisation of the Paper

The rest of the paper develops as follows. After introducing some definitions and notation, Section 2 introduces boolean rings and proves the existence of entailment multipliers for valid statements. In Section 2.1 we show how the existence of “small multipliers” is related to the problem NP=coNP, and in Section 2.2 we show how entailment multipliers can be used to generate stronger entailment statements. In Section 3 we show how to compute entailment multipliers along the proof constructions using the inference systems of Resolution and Gentzen Sequent Calculus. We then show how the idea of multipliers generalises to extensions of propositional classical logics, such as Normal Modal Logics in Section 4. The paper concludes with some remarks and proposals of future work.

Notation

We consider formulas built over a countable set of propositional atoms $\mathcal{P} = \{p_0, p_1, \ldots\}$ and connectives $\neg$, $\wedge$, $\vee$ and $\rightarrow$. We represent formulas by upper case Latin letters: A, B, C, etc. We represent sets or multisets of formulas by upper case Greek letters, such as Γ, Δ, Φ and Ψ. A valuation is a function that maps each atomic symbol in $\mathcal{P}$ in $\{0,1\}$, which is then generalised to formulas in the usual way; a valuation v is said to satisfy formula A if $v(A) = 1$. A set of formulas Γ is *satisfiable* if there is a v such that for every $A \in \Gamma$, $v(A) = 1$.

An *entailment statement* is an expression of the form $\Gamma \models \Delta$; such a statement is *valid* if every valuation that satisfies every $A \in \Gamma$ also satisfies some $B \in \Delta$. The proof-theoretic counterpart of entailment statements are *sequents*, which are expressions of the form $\Gamma \vdash \Delta$, where Γ is the sequent's antecedent and Δ its consequent. A sequent may be proven using several distinct *inference systems*, represented by $\vdash_I$; such a system is sound and complete with respect to the semantic entailment iff $\Gamma \models \Delta$ iff $\Gamma \vdash_I \Delta$.

Algebraic terms are represented by lower case Latin letters: a, b, c, etc. Algebraic variables are represented by x, y, z, etc. All representations may be subscripted or superscripted.

2 Entailment Multipliers

For the purposes of this paper, a *ring* is an algebraic structure $\mathfrak{R} = \langle \mathcal{R}, \cdot, +, 0, 1\rangle$ where $\mathcal{R}$ is a set, $0, 1 \in \mathcal{R}$ and for every $a, b, c \in \mathcal{R}$ the following holds:

(r_1) $(a + b) + c = a + (b + c)$;
(r_2) $0 + a = a + 0 = a$;
(r_3) there is $-a \in \mathcal{R}$ such that $a + (-a) = (-a) + a = 0$;
(r_4) $a + b = b + a$;
(r_5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
(r_6) $a \cdot b = b \cdot a$;
(r_7) $1 \cdot a = a \cdot 1 = a$;
(r_8) $a \cdot (b + c) = a \cdot b + a \cdot c$.

A *boolean ring* $\mathfrak{B} = \langle \mathcal{B}, \cdot, +, 0, 1\rangle$ is a ring subjected to the conditions, for every $a \in \mathcal{B}$:

(b_1) $a \cdot a = a$;
(b_2) $a + a = 0$

In a boolean ring, the structure $\cdot$ is interpreted as conjunction, $+$ is exclusive-or, 0 is the bottom and 1 is the top. Note that every element is its own inverse, $x + x = 0$ (that is, $(\mathcal{B}, +, 0)$ is an Abelian group of order 2). Also note that the power of any variable is at most 1. As 0 is defined by (b_2), a boolean ring is sometimes represented as $\mathfrak{B} = \langle \mathcal{B}, \cdot, +, 1\rangle$. The *degree* of the term is defined as usual, namely, $\mathit{degree}(0) = \mathit{degree}(1) = 0$, $\mathit{degree}(x_i) = 1$, $\mathit{degree}(a + b) = \max\{\mathit{degree}(a), \mathit{degree}(b)\}$, $\mathit{degree}(a \cdot b) = \mathit{degree}(a) + \mathit{degree}(b)$. As usual, we sometimes write ab for $a \cdot b$.

For every propositional formula A, let A^t be its standard translation as a term of $\mathfrak{A}$; similarly, let if a is a term of $\mathfrak{A}$, a^φ is its formula translation. The *term* and *formula translations* are defined as follows.

$$\begin{array}{ll|lll}
\top^t & = 1 & 1^\varphi & = \top & \\
\bot^t & = 0 & 0^\varphi & = \bot & \\
p_i^t & = x_i & x_i^\varphi & = p_i & \\
(\neg A)^t & = A^t + 1 & (a \cdot b)^\varphi & = a^\varphi \wedge b^\varphi & \\
(A \wedge B)^t & = A^t \cdot B^t & & & \\
(A \vee B)^t & = (A^t + 1) \cdot (B^t + 1) + 1 & (a + b)^\varphi & = \left\{ \begin{array}{ll} \neg a^\varphi & , b = 1 \\ (a^\varphi \wedge \neg b^\varphi) \vee & \\ \quad (\neg a^\varphi \wedge b^\varphi) & , b \neq 1 \end{array} \right. & \\
(A \to B)^t & = A^t \cdot (B^t + 1) + 1 & & &
\end{array}$$

It is immediate that $a = (a^\varphi)^t$ and that $A \equiv (A^t)^\varphi$.

The relationship between boolean rings and sequents is established by the following result.

Proposition 21 *The statement $A_1, \ldots, A_n \models B_1, \ldots, B_m$ is valid iff*

$$\left(\prod_{i=1}^{n} A_i^t\right) \cdot \left(\prod_{j=1}^{m} (B_i^t + 1)\right) = 0 \qquad (1)$$

Lemma 22 *Suppose $\{A_1, \ldots, A_n\}$ is an unsatisfiable set of propositional formulas. Then there are terms $a_1, \ldots, a_n$ such that*

$$\sum_{i=1}^{n} a_i \cdot (A_i^t + 1) = 1. \qquad (2)$$

Proof By induction on n. For the base case, consider $n = 1$, so that A_1 is an inconsistent formula. As a result $A_1^t = 0$, and take $a_1 = 1$. Then $a_1 \cdot (A_1^t + 1) = 1 \cdot (0 + 1) = 1$.

Suppose the set $\{A_1, \ldots, A_{n+1}\}$ with $n + 1$ elements is inconsistent; then the set $\{A_1, \ldots, A_n \wedge A_{n+1}\}$ with n elements is clearly inconsistent, and we can apply the induction hypothesis, so there are $a_1, \ldots, a_n$ such that

$$\left(\sum_{i=1}^{n-1} a_i \cdot (A_i^t + 1)\right) + a_n \cdot (A_n^t \cdot A_{n+1}^t + 1) = 1. \qquad (3)$$

To solve (3), it suffices to provide a'_n, a'_{n+1} such that

$$a'_n \cdot (A^t_n + 1) + a'_{n+1} \cdot (A^t_{n+1} + 1) = a_n \cdot (A^t_n \cdot A^t_{n+1} + 1). \tag{4}$$

There are many possible solutions to (4). One could make $a'_n = a_n \cdot A^t_{n+1}$ and $a'_{n+1} = a_n$; or $a'_n = a_n \cdot (A^t_n \cdot A^t_{n+1} + 1)$ and $a'_{n+1} = a_n \cdot A^t_n$. In either case, we have a set of multipliers for $\{A_1, \ldots, A_{n+1}\}$. ⊣

Note that the possible multipliers for a given inconsistent set are not unique. In fact, in the proof above, the inductive case can generate a potentially different set of multipliers for every pair of formulas chosen in $\{A_1, \ldots, A_{n+1}\}$. The sum is called a *1-sum*.

Example 23 Consider the inconsistent set of formulas $A, C \to \neg A, B \to C, B$. It is easy to verify that

$$1 \cdot (a + 1) + 1 \cdot (ca) + a \cdot (b(c + 1)) + a(c + 1) \cdot (b + 1) = 1 \tag{5}$$

so a possible attribution of multipliers to this set is $1, 1, a, a(c + 1)$. ⊣

The converse of Lemma 22 also holds.

Lemma 24 *Let $\Gamma = \{A_1, \ldots, A_n\}$ be a set of formulas such that $\sum_{i=1}^n a_i \cdot (A^t_i + 1) = 1$ for terms $a_1, \ldots, a_n$. Then Γ is unsatisfiable.*

Proof We prove by induction on n. For the base case $n = 1$, so $a_1 \cdot (A^t_1 + 1) = 1$, which holds iff $a_1 = A^t_1 + 1 = 1$. So $A^t = 0$ and Γ is inconsistent.

Consider now $\sum_{i=1}^n a_i \cdot (A^t_i + 1) = 1$. By multiplying both sides by $A^t_1 \cdot A^t_2$ the first two terms of the sum are cancelled and after some regrouping we obtain

$$\sum_{i=3}^{n} (A^t_1 \cdot A^t_2 \cdot a_i) \cdot (A^t_i + 1) = A^t_1 \cdot A^t_2. \tag{6}$$

Adding $A^t_1 \cdot A^t_2 + 1$ to both sides of (6) yields

$$\left(\sum_{i=3}^{n} (A^t_1 \cdot A^t_2 \cdot a_i) \cdot (A^t_i + 1) \right) + (A^t_1 \cdot A^t_2 + 1) = 1 \tag{7}$$

The left hand side of (7) is a sum of $n - 1$ terms, where the multiplier of the last term is 1. By the induction hypothesis, we obtain that the set $\{A_1 \wedge A_2, A_3, \ldots, A_n\}$ is unsatisfiable, so Γ is unsatisfiable. ⊣

Definition 25 (Characteristic Polynomial) Given an entailment statement $\mathcal{S} = A_1, \ldots, A_n \models B_1, \ldots, B_m$, its *characteristic polynomial* over variables $x_1, \ldots, x_n, y_1, \ldots, y_m$ is $\mathit{cp}(\mathcal{S}) = x_1 \cdot (A^t_1 + 1) + \ldots + x_n \cdot (A^t_n + 1) + y_1 \cdot B^t_1 + \ldots + y_m \cdot B^t_m$.

The characteristic polynomial has *1-roots* if there are terms $a_1, \ldots, a_n, b_1, \ldots, b_m$ such that

$$\textstyle\sum_{i=1}^{n} a_i \cdot (A_i^t + 1) + \sum_{j=1}^{m} b_j \cdot B_j^t = 1. \qquad (\textit{1-roots})$$

Theorem 26 (Entailment Multipliers) *A classical entailment statement $\mathcal{S}$ is valid iff its characteristic polynomial $cp(\mathcal{S})$ has 1-roots.*

Proof If $A_1, \ldots, A_n \models B_1, \ldots, B_m$ then the set $\{A_1, \ldots, A_n, \neg B_1, \ldots, \neg B_m\}$ is unsatisfiable. So, by applying Lemma 22, the 1-roots are obtained.

Conversely, if $cp(S)$ has 1-roots, by Lemma 24, $\{A_1, \ldots, A_n, \neg B_1, \ldots, \neg B_m\}$ is an unsatisfiable set, so $A_1, \ldots, A_n \models B_1, \ldots, B_m$ holds. ⊣

We use the notation of Labelled Deduction System (LDS) [10] to designate a formula and its corresponding entailment multiplier as the label. So a statement is now represented as:

$$x_1 : A_1, \ldots, x_n : A_n \models y_1 : B_1, \ldots, y_m : B_m$$

to indicate that the statement $A_1, \ldots, A_n \models B_1, \ldots, B_m$ is valid with the corresponding 1-roots.

Example 27 Consider the statement $A, C \to \neg A, B \to C, B \models (A \vee B) \wedge C$. As its antecedent is the unsatisfiable set of Example 23, we obtain the following multiplier labelled sequent:

$$1 : A, 1 : C \to \neg A, a : B \to C, a(c+1) : B \models 0 : (A \vee B) \wedge C$$

Note that 0-labelled formulas play no part in the validity of the statement. ⊣

There is a naive way to compute multipliers. Let $A_1, \ldots, A_n$ be a set of inconsistent formulas, then we we compute multipliers $a_1, \ldots, a_n$ by making $a_1 = 1$ and for $2 \leq i \leq n$

$$a_i = \prod_{j=1}^{i-1} A_j^t \qquad (8)$$

that is, $a_2 = A_1^t$, $a_3 = A_1^t \cdot A_2^t$, …, $a_n = A_1^t \cdots A_{n-1}^t$. This is a direct consequence of the equation

$$\sum_{i=1}^{n} \left(\prod_{j=1}^{i-1} A_j^t \right) \cdot (A_i^t + 1) = 1, \qquad (9)$$

which can be easily verified.

It is important to note that the multipliers computed by (8) depends on the order of the formulas. It is also possible to simplify those multipliers.

Example 28 Consider again the set of inconsistent formulas in Example 23. By applying equation 9 we obtain the multipliers:

$$1 : A, a : C \to \neg A, a(ca+1) : B \to C, a(ca+1)(b(c+1)+1) : B$$

On the other hand, by considering the same set in reverse order we obtain

$$b(b(c+1)+1)(ca+1) : A, b(b(c+1)+1) : C \to \neg A, b : B \to C, 1 : B$$

or

$$bc : A, b : C \to \neg A, 1 : B \to C, 1 : B$$

after some simplification. $\dashv$

In this method, prior to simplification, the degree of the last multiplier is $n-1$, which indicates that this may not be a good way to obtain small multipliers. Section 3 presents other ways of computing entailment multipliers, which are associated to proof systems.

2.1 Multipliers and the NP = coNP Problem

There is a basic asymmetry between NP-complete problems and coNP-complete problems, which is reflected in logic as well. If a set of formulas is satisfiable, it suffices to provide a valuation to have a polynomial-time computable witness of satisfiability. No such tractable witness is known to exist for unsatisfiability (or validity).

Here, we propose that entailment multipliers as a candidate for validity witness. The complexity of the verification is the number of operations (sums, products, fatorings or other forms of term simplification) to transform the left-hand side of the 1-sum to 1.

In this case, a *small witness* for the validity of a sequent would be a set of entailment multipliers such that the number of operations to verify the 1-sum is bounded by a polynomial on the number of distinct atomic formulas in the sequent. However, it is not clear that such a set of multipliers always exists.

Lemma 29 *If every valid sequent has a small witness set of entailment multipliers, then NP=coNP.*

Proof The existence of a small witness set of entailment multipliers provides an NP algorithm for deciding classical propositional validity, which is a coNP problem. This implies NP=coNP [11]. $\dashv$

The search space of multipliers for a given entailment can be quite big, as the set of multipliers for a given entailment is far from unique. In fact, each proof method may compute a different set of multipliers, which we investigate in Section 3.

2.2 Strengthening Entailment Expressions

The use of entailment multipliers suggests a way to strengthen entailment expressions.

Theorem 210 (Stronger Entailment) *Let $\mathcal{S} = A_1, \ldots, A_n \models B_1, \ldots, B_m$ be a valid statement with multipliers $a_1, \ldots, a_n$,$b_1, \ldots, b_m$. Then:*

(a) For $1 \leq k \leq n$, the statement $\mathcal{S}' = A_1, \ldots, (\neg a_k^{\varphi}) \vee A_k, \ldots, A_n \models B_1, \ldots, B_m$ is valid with multipliers $a_1, \ldots, a_{k-1}, 1, a_{k+1}, \ldots, a_n$,$b_1, \ldots, b_m$, such that $\mathcal{S}' \geq \mathcal{S}$.

(b) *For $1 \leq l \leq m$, the statement $\mathcal{S}'' = A_1, \ldots, A_n \models B_1, \ldots, b_l^\varphi \wedge B_l, \ldots, B_m$ is valid with multipliers $a_1, \ldots, a_n$,$b_1, b_{j-1}, 1, b_{j+1}, \ldots, \ldots, b_m$, such that $\mathcal{S}'' \geq \mathcal{S}$.*

Proof From the fact that $\mathcal{S}$ is valid with multipliers $a_1, \ldots, a_n$,$b_1, \ldots, b_m$ we have that

$$\sum_{i=1}^{n} a_i \cdot (A_i^t + 1) + \sum_{j=1}^{m} b_j \cdot B_j^t = 1. \tag{10}$$

Then:

(a) The term translation $[(\neg a_k^\varphi) \vee A_k]^t = ((a_k+1)+1)(A_k^t+1)+1 = a_k(A_k^t+1)+1$, such that (10) can be rewritten as

$$\left(\sum_{i=1, i\neq k}^{n} a_i \cdot (A_i^t + 1) + \sum_{j=1}^{m} b_j \cdot B_j^t \right) + 1 \cdot (a_k(A_k^t + 1) + 1 + 1) = 1. \tag{11}$$

By Theorem 26 we have that $\mathcal{S}'$ is valid with multipliers $a_1, \ldots, a_{k-1}, 1, a_{k+1}, \ldots, a_n$, $b_1, \ldots, b_m$. We also have that $A_i = A_i'$ for $1 \leq i \neq k \leq n$, $B_j = B_j'$ for $1 \leq j \leq m$ and $A_k \models (\neg a_k^\varphi) \vee A_k$, so $\mathcal{S}' \geq \mathcal{S}$.

(b) Totally analogous. ⊣

Theorem 210 implies that, if we start with a valid statements $\mathcal{S}$ we "incorporate" one of its multipliers into new a statement $\mathcal{S}' \geq \mathcal{S}$; clearly, $\mathcal{S}'$ is strictly stronger than $\mathcal{S}$ when the multiplier is not 1. But then we can again apply Theorem 210 to $\mathcal{S}'$, choosing a different non-unit multiplier, obtaining an even stronger valid statement. This process can be iterated until we obtain a statement whose multipliers are all 1.

Corollary 211 *Given a valid entailment statement $\mathcal{S}$*

$$\mathcal{S} = a_1 : A_1, \ldots, a_n : A_n \models b_1 : B_1, \ldots, b_m : B_m$$

we can build a lattice of valid entailment statements $(\mathbb{S}, \Gamma)$ where the elements of $\mathbb{S}$ are valid statements obtained by applying Theorem 210 to every subset of formulas in $\mathcal{S}$. The statement $\mathcal{S}$ is the bottom of the lattice and the top statement is $\mathcal{S}^\top$:

$$\neg a_1^\varphi \vee A_1, \ldots, \neg a_n^\varphi \vee A_n \models b_1^\varphi \wedge B_1, \ldots, b_m^\varphi \wedge B_m$$

3 Computing Entailment Multipliers

The naive method to compute entailment multipliers has a series of inconveniences. It may take an exponential number of steps, which may even lead to the storage of an exponential number of terms. As a result, the multipliers may use exponential space.

However, we believe that each kind of inference system may provide at least one method of computing entailment multipliers. In fact, each sound inference method consists of a set of transformations that preserve the validity, or the truth value, such that at each step the 1-sum is an invariant. Therefore, at each transformation step one can compute new multipliers from previous ones. We now investigate this statement for two proof methods: resolution and Gentzen Sequent Calculus.

3.1 Resolution

Propositional resolution is a refutation method in which one shows the inconsistency of a set of formulas in clausal form by deriving $\perp$ from it. The main inference step is the resolution rule

$$\frac{A \vee p_i \quad \neg p_i \vee B}{A \vee B}$$

This inference step can be simulated as an algebraic operation. Note that $(x_i + 1)$ is a factor of $(A \vee p_i)^t + 1$, and similarly, x_i is a factor of $(\neg p_i \vee B)^t + 1$. We can construct multipliers m_A and m_B for the resolvents such that $m_A \cdot ((A \vee p_i)^t + 1) = y \cdot (x_i + 1)$ and $m_B \cdot ((\neg p_i \vee B)^t + 1) = y \cdot x_i$. In this case, the resolution step can be simulated by the algebraic operation

$$y \cdot (x_i + 1) + y \cdot x_i = y \tag{12}$$

The multipliers for an original formula is the multiplication of all those factors that label the path from the formula to the final contradiction, $\perp$; if more than one path exists, take the sum of them. This method is better understood by means of an example.

Example 31 The set of formulas $\{\neg s \vee q, \neg p \vee q, p \vee s, \neg q\}$, is inconsistent. This can be shown by a labeled resolution graph in Figure 1, in which each edge is labeled with the term corresponding to the negation of the resolved literal.

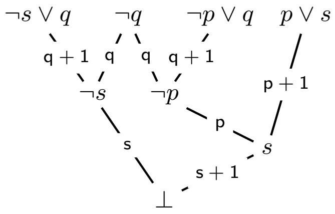

Fig. 1. Edge-labeled resolution graph

The term corresponding to a path going from a top formula to $\perp$ is the product of all labels. The multiplier of a top formula is the sum of all path terms. In this way, we compute the multipliers for each formula:

$$(\mathsf{q}+1)\mathsf{s} : \neg s \vee q, \quad \mathsf{qs}+\mathsf{qp}(\mathsf{s}+1) : \neg q,$$
$$(\mathsf{q}+1)\mathsf{p}(\mathsf{s}+1) : \neg p \vee q, \; (\mathsf{p}+1)(\mathsf{s}+1) : p \vee s$$

The multipliers a of $a : A$ can be simplified by deleting from it the factors occurring in $A^t + 1$, so we end up with

$$1 : \neg s \vee q, \, \mathsf{s}+\mathsf{p}(\mathsf{s}+1) : \neg q,$$
$$(\mathsf{s}+1) : \neg p \vee q, \qquad 1 : p \vee s$$

Finally, we note that the verification of the 1-sum is isomorphic to the resolution graph, as shown in Figure 2; each transformation step is an application of (12). In this sense, we can say that resolution is simulated by algebraic methods. $\dashv$

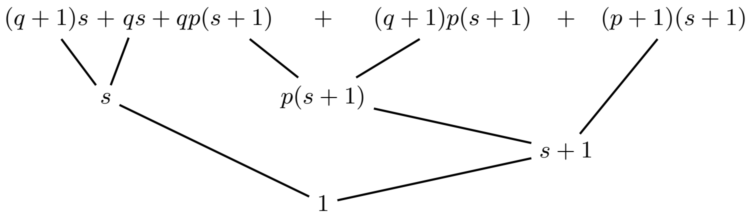

Fig. 2. Reduction of 1-sum isomorphic to resolution graph in Figure 1

Formally, define an *edge-labeled resolution graph* as a resolution graph in which edges are labeled with a term $(\neg p)^t$, where p is the reduced literal. This is the input for Algorithm 3.1 computing entailment multipliers.

Algorithm 3.1 Resolution-based computation of entailment multipliers

Input: an edge-labeled resolution graph G.
Output: entailment multipliers for the top nodes of G.

```
Let $A_1, \dots, A_n$ be the top nodes of $G$, an inconsistent set of formulas.
for each path $P$ from a top node to $\bot$ do
    $\mathrm{term}(P) = \prod\{l | l \text{ is a label in } P\}$
end for
for $i = 1$ to $n$ do
    $a_i = \sum\{\mathrm{term}(P) | P \text{ starts at } A_i\}$
    delete from $a_i$ factors occurring in $(A_i^t + 1)$
end for
return the set $\{a_i : A_i | 1 \leq i \leq n\}$
```

Theorem 32 *Algorithm 3.1 computes a set of multipliers such that the verification of the 1-sum as a set of applications of (12) is isomorphic to the input edge-labeled resolution graph.* $\dashv$

3.2 Sequent Calculus

There are many presentations of the sequent calculus. As our interest lies in calculi that promote the use of non-analytic cuts, we present a *cut-based* sequent calculus, in which the cut rule is *not* eliminable, and is in fact the only branching rule [9]. This version of the sequent calculus is closely related to KE tableau [8], which is a decision procedure for full propositional classical logic.

In the sequent calculus, the 1-sum is seen as an *invariant* over each deduction step, such that every rule that transforms a provable sequent into another provable sequent has to preserve it. In this way, the multipliers of a sequent rule's conclusion will be described as a combination of the multipliers of the rule's premises.

So in this presentation formulas are labeled with entailment multiplier, and in a sequent $\Gamma \vdash \Delta$, the antecedent Γ and the consequent Δ are *multisets* of term labeled formulas of the form $a : A$; if $\Gamma = a_1 : A_1, \ldots, a_n : A_n$, by $b : \Gamma$ we mean $b \cdot a_1 : A_1, \ldots, b \cdot a_n : A_n$.

$$\frac{\Gamma, a : A, b : B \vdash \Delta}{\Gamma, a(A^t + 1) + b(B^t + 1) : A \wedge B \vdash \Delta}\,(\wedge\vdash)$$

$$\frac{\Gamma \vdash \Delta, a : A}{\Gamma, aA^t : B \vdash \Delta, a : A \wedge B}\,(\vdash\wedge_1) \qquad \frac{\Gamma \vdash \Delta, a : A}{\Gamma, aA^t : B \vdash \Delta, a : B \wedge A}\,(\vdash\wedge_2)$$

$$\frac{\Gamma \vdash \Delta, a : A, b : B}{\Gamma \vdash \Delta, aA^t + bB^t : A \vee B}\,(\vdash\vee)$$

$$\frac{\Gamma, a : A \vdash \Delta}{\Gamma, a : A \vee B \vdash \Delta, a(A^t + 1) : B}\,(\vee\vdash_1) \qquad \frac{\Gamma, a : A \vdash \Delta}{\Gamma, a : B \vee A \vdash \Delta, a(A^t + 1) : B}\,(\vee\vdash_2)$$

$$\frac{\Gamma, a : A \vdash \Delta, b : B}{\Gamma \vdash \Delta, a(A^t + 1) + bB^t : A \to B}\,(\vdash\to)$$

$$\frac{\Gamma, b : B \vdash \Delta}{\Gamma, b : A \to B, b(B^t + 1) : A \vdash \Delta}\,(\to\vdash_1) \qquad \frac{\Gamma \vdash a : A, \Delta}{\Gamma, a : A \to B \vdash \Delta, aA^t : B}\,(\to\vdash_2)$$

$$\frac{\Gamma \vdash \Delta, a : A}{\Gamma, a : \neg A \vdash \Delta}\,(\neg\vdash) \qquad \frac{\Gamma, a : A \vdash \Delta}{\Gamma \vdash \Delta, a : \neg A}\,(\vdash\neg)$$

Fig. 3. Connective rules propagating multipliers from premiss to conclusion

As usual in sequent presentation, there are *connective rules* and *structural rules*, and the 1-sum invariant must be kept in all of them. Figure 3 presents the connective rules for cut-based sequent propositional inferences and the structural rules are presented in Figure 4. If labels are omitted from Figures 3 and 4, one obtains the cut-based rules of [9].

Structural rules have several peculiarities. The cut rule affects all multipliers in the sequent; in all other rules, only a restricted set of multipliers are affected. As we are dealing with multisets, there is no need to define structural rules for commutativity and associativity. We deal with multisets instead of sets to deal properly with the right and left contraction rules, in which the multipliers of contracted formulas have to be added. The *weakening* structural rule (also called *monotonicity*) is taken care of by the presence of Γ and Δ in the Axiom rule; Γ and Δ may be empty, or they may contain formulas which are irrelevant to the deduction, and are thus 0-labeled. The Axiom rule has no premiss and produces a 1-label to the relevant formulas.

$$\frac{}{0:\Gamma, 1:A \vdash 1:A, 0:\Delta}\,(\text{Axiom}) \qquad \frac{\Gamma_1 \vdash \Delta_1, a_1 : A \quad a_2 : A, \Gamma_2 \vdash \Delta_2}{A^t+1:\Gamma_1, A^t:\Gamma_2 \vdash A^t+1:\Delta_1, A^t:\Delta_2}\,(\text{Cut})$$

$$\frac{\Gamma, a_1 : A, a_2 : A \vdash \Delta}{\Gamma, (a_1+a_2) : A \vdash \Delta}\,(\text{Contract} \vdash) \qquad \frac{\Gamma \vdash \Delta, a_1 : A, a_2 : A}{\Gamma \vdash \Delta, (a_1+a_2) : A}\,(\vdash \text{Contract})$$

Fig. 4. Structural rules propagating multipliers

A *sequent proof tree* is a tree whose leaves are instantiations of Axiom, and whose internal nodes are sequents obtained by the application of some connective or structural rule. A sequent $\mathcal{S}$ is *provable* if there is a sequent proof tree with $\mathcal{S}$ at its root.

Example 33 As an example, consider the proof, of $A \to B, C \to A \vdash C \to B$:

$$\cfrac{\cfrac{\cfrac{1:B \vdash 1:B}{1:A\to B, b+1:A \vdash 1:B}\,(\to\vdash)}{1:A\to B, b+1:C\to A, (b+1)(a+1):C \vdash 1:B}\,(\to\vdash)}{1:A\to B, b+1:C\to A \vdash (b+1)(a+1)(c+1)+1:C\to B}\,(\vdash\to)$$

The entailment multipliers are computed simultaneously with the deduction. ⊣

It is worth noting that at each deduction step in Example 33 the 1-sum holds. This is called *1-sum-invariant propagation.*

Lemma 34 (1-sum-invariant propagation) *For every sequent rule in Figures 3 and 4, if the 1-sum holds for the premises it also holds for the conclusion.*

Proof We first note that the (Axiom) rule has no premiss. In its conclusion we have $1 \cdot (B^t) + 1 \cdot B = 1$, so (Axiom) keeps the 1-sum.

We show propagation of one connective and one structural rule. Consider rule $(\vdash \wedge_1)$, and let C correspond to the sum of members of Γ and D to that of Δ. Assuming the 1-sum holds for the rules antecedent, we have:

$$C + D + aA^t = 1. \tag{13}$$

But the we have that

$$aA^t(B^t + 1) + aA^tB^t = aA^t, \tag{14}$$

such that, by substituting (14) into (13) we obtain

$$C + D + aA^t(B^t + 1) + aA^tB^t = 1 \tag{15}$$

which corresponds to the conclusion of $(\vdash \wedge_1)$.

Now consider the cut rule. The left and right sequents in the premiss correspond to, respectively,

$$C_1 + D_1 + a_1A^t = 1 \qquad [\times(A^t + 1)] \tag{16}$$

$$C_2 + D_2 + a_2(A^t + 1) = 1 \qquad [\times A^t] \tag{17}$$

such that, by multiplying (16) by $(A^t + 1)$ and (17) by A^t and adding both equations we obtain:

$$(A^t + 1)C_1 + (A^t + 1)D_1 + A^tC_2 + A^tD_2 = (A^t + 1) + A^t = 1 \tag{18}$$

which corresponds to the conclusion of the cut rule, as desired. The other cases are analogous and are omitted. ⊣

Theorem 35 *The labeled sequent rules in Figures 3 and 4 correctly compute a set of entailment multipliers.*

Proof By induction on the length of the proof. The basic case is one application of (Axiom). The induction cases are dealt by Lemma 34. ⊣

The labeled rules of Figures 3 and 4 are not the only possible ones, and many other 1-sum-invariant ways to propagate entailment multipliers are possible.

4 Multipliers for Normal Modal Logics

As modal logics are extensions of classical propositional logic, the result on entailment multipliers extends quite naturally to those logics. We consider here only normal modal logics, that can be dealt with in algebraic terms by *boolean algebras with operators* [3], which in our case becomes a boolean ring with operators.

On the logic side, we extend the propositional language by considering the unary connective $\Box$, and we extend the formula formation rules such that if A is a modal formula $\Box A$ is also a modal formula, which is read "A is necessary". The connective $\Diamond$ is considered a derived connective, $\Diamond A =_{\text{def}} \neg\Box\neg A$, which is read as "$A$ is possible". A axiomatisation of normal modal logics is given by a set of axioms and a set of inference rules. The minimal modal logic **K** is axiomatised by the following axioms:

A0 All propositional classical tautologies
K $\Box(p \to q) \to (\Box p \to \Box q)$

and the inference rules of Modus Ponens (from $\vdash A \to B$ and $\vdash A$ infer $\vdash B$) and of Necessitation (from $\vdash A$ infer $\vdash \Box A$). A *deduction* of a formula A is a sequence of formulas $A_1, \ldots, A_n = A$ such that each A_i is an instance of an axiom or is obtained from previous formulas in the sequence by an application of an inference rule. If A is deducible, we represent it by $\vdash A$ and call it a *modal theorem*. Different modal logics are generated by adding extra axioms, and we represent $\vdash_M A$ to represent theoremhood in modal logic M.

Furthermore, if Γ is a finite set of modal formulas, we represent $\Gamma \vdash_M A$ is $\vdash_M \bigwedge \Gamma \to A$. If Γ is an infinite set of modal formulas, we write $\Gamma \vdash_M A$ if there is a finite set $\Gamma_0 \subset \Gamma$ such that $\Gamma_0 \vdash_M A$.

On the semantic side, we employ the usual Kripke-structures for normal modal logics, which consists of a pair $\langle W, R\rangle$, where W is a set, usually called a set of *possible worlds* and $R \subseteq W \times W$ is a binary relation on W, usually called an *accessibility relation* [7]. A Kripke model for modal logics is a triple $\mathcal{M} = \langle W, R, g\rangle$, where $\langle W, R\rangle$ is a Kripke-structure and $g : \mathcal{P} \to 2^W$ is a modal valuation that associates each (atomic) propositional symbol to a set of possible worlds, namely the worlds in which the symbol is true. If $w \in W$ is a possible world, $\mathcal{M}$ is a Kripke-model and A is a modal formula, we write $\mathcal{M}, w \models A$ if A is true at work w in model $\mathcal{M}$, which is inductively defined as:

- $\mathcal{M}, w \models p$ iff p is atomic and $w \in g(p)$;
- $\mathcal{M}, w \models \neg A$ iff $\mathcal{M}, w \not\models A$;
- $\mathcal{M}, w \models A \wedge B$ iff $\mathcal{M}, w \models A$ and $\mathcal{M}, w \models B$;
- $\mathcal{M}, w \models \Box A$ iff for every w' accessible from w (that is, Rww' holds) then $\mathcal{M}, w' \models A$.

The formula A is modally *valid*, $\models A$ if $\mathcal{M}, w \models A$ for every world $w \in W$ and for every model $\mathcal{M}$. Different normal modal logics are created by imposing restrictions on the accessibility relation R. For modal logic M, we write the *(local) modal entailment expression* $A_1, \ldots, A_n \models_M B_1, \ldots, B_m$ if for every model $\mathcal{M} = \langle W, R, g\rangle$ in the class of models of M, and for every $w \in W$, if $\mathcal{M}, w \models A_i$ for all $1 \leq i \leq n$, then for some B_j, $1 \leq j \leq m$, $\mathcal{M}, w \models B_j$.

On the algebraic side, we consider a *boolean ring with operator* $\blacksquare$, $\mathfrak{B} = \langle \mathcal{B}, \cdot, +, 1, \blacksquare\rangle$. In *normal* modal logics, the operator $\blacksquare$ respects the following restrictions, for every $a, b \in \mathcal{B}$:

(op$_1$) $\blacksquare 1 = 1$;

(op$_2$) $\blacksquare(a \cdot b) = (\blacksquare a) \cdot (\blacksquare b)$.

A modal term a is algebraically *valid* if we can show that $a = 1$. For other normal modal logics, extra equations involving $\blacksquare$ have to be added.

In the translation from formulas to terms and from terms to formulas, we have to add the following:

$$(\Box A)^t = \blacksquare A^t \qquad\qquad (\blacksquare a)^\varphi = \Box a^\varphi$$

As modal logics are extensions of classical propositional logics and modal validity is taken care of by $\blacksquare$-equations, it is expected that entailment multipliers generalise to modal logics. We first see a few examples relating to modal logic **K**.

Example 41 Consider the statement

$$\Box(p \to q), \Box p \vdash_{\mathbf{K}} \Box q$$

for which the modal polynomial is

$$x_1 \cdot (\blacksquare(p(q+1)+1)+1) + x_2 \cdot (\blacksquare p + 1) + y \cdot (\blacksquare q)$$

and we see that this polynomial has 1-roots for $x_1 = y = \blacksquare p$ and $x_2 = 1$:

$$\begin{aligned}
&\blacksquare p \cdot (\blacksquare(pq+p+1)+1) + (\blacksquare p + 1) + \blacksquare p \cdot \blacksquare q \\
&= \blacksquare p \cdot \blacksquare(pq+p+1) + \cancel{\blacksquare p} + \cancel{\blacksquare p} + 1 + \blacksquare(pq) \\
&= \blacksquare(pq + \cancel{p} + \cancel{p}) + 1 + \blacksquare(pq) \\
&= \cancel{\blacksquare(pq)} + 1 + \cancel{\blacksquare(pq)} \\
&= 1
\end{aligned}$$

Normality conditions are applied in the first and second steps; simplifications are indicated. ⊣

Now consider modal logic **T**, which extends modal with an axiom:

(T) $\Box p \to p$

On the algebraic side, we have to add an equality that corresponds to the validity of that axiom, namely

$$\begin{aligned}
&(\Box p \to p)^t = 1 \\
&\Leftrightarrow p \cdot \blacksquare p + \blacksquare p + 1 = 1 \\
&\Leftrightarrow p \cdot \blacksquare p = \blacksquare p
\end{aligned}$$

On the semantic side this logic **T** forces the accessibility relation to be reflexive, namely

$$\forall w(Rww)$$

Example 42 We take as an example the following statement

$$\Box(p \to q), p \vdash_{\mathbf{T}} q$$

for which the modal polynomial is

$$x_1 \cdot (\blacksquare(p(q+1)+1)+1) + x_2 \cdot (p+1) + y \cdot q$$

and we see that this polynomial has 1-roots for $x_1 = p(q+1)$, $x_2 = 1$ and $y = p$:

$$\begin{aligned}
&p(q+1) \cdot \uwave{\blacksquare(p(q+1)+1)+1)} + (p+1) + p \cdot q \\
&= \xcancel{p(q+1) \cdot (p(q+1)+1)} \cdot \blacksquare(p(q+1)+1) + p(q+1) + p + 1 + pq \\
&= \cancel{pq} + \cancel{p} + \cancel{p} + 1 + \cancel{pq} \\
&= 1
\end{aligned}$$

where the first step uses the property $\blacksquare x = x \blacksquare x$, and then we use $x \cdot (x+1) = 0$ to eliminate the only subterm containing a $\blacksquare$. $\dashv$

We proceed by considering modal logic **S4**, which extends modal logic **T** with the axiom:

(4) $\Box p \to \Box\Box p$

Again, on the algebraic side, besides the algebraic equation for logic **T**, we have to add an equality that corresponds to the validity of that axiom, namely

$$\begin{aligned}
&(\Box p \to \Box\Box p)^t = 1 \\
&\Leftrightarrow \blacksquare\blacksquare p \cdot \blacksquare p + \blacksquare p + 1 = 1 \\
&\Leftrightarrow \blacksquare\blacksquare p \cdot \blacksquare p = \blacksquare p
\end{aligned}$$

On the semantic side the logic **S4** forces the accessibility relation to be reflexive and transitive, namely

$$\forall w(Rww) \wedge \forall w \forall w' \forall w''(Rww' \wedge Rw'w'' \to Rww'')$$

Example 43 We take as a final **S4**-example the following statement

$$\Box(p \to q), \Box\Box p \vdash_{\mathbf{S4}} \Box\Box q$$

for which the modal polynomial is

$$x_1 \cdot (\blacksquare(p(q+1)+1)+1) + x_2 \cdot (\blacksquare\blacksquare p + 1) + y \cdot \blacksquare\blacksquare q$$

and we see that this polynomial has 1-roots for $x_1 = \blacksquare\blacksquare p$, $x_2 = 1$ and $y = \blacksquare\blacksquare p$:

$$\begin{aligned}
&\blacksquare\blacksquare p \cdot (\blacksquare(pq+p+1)+1) + (\blacksquare\blacksquare p + 1) + \blacksquare\blacksquare p \cdot \blacksquare\blacksquare q \\
&= \blacksquare\blacksquare p \cdot \blacksquare(pq+p+1) + \cancel{\blacksquare\blacksquare p} + \cancel{\blacksquare\blacksquare p} + 1 + \blacksquare\blacksquare p \cdot \blacksquare\blacksquare q
\end{aligned}$$

$$\begin{aligned}
&= \blacksquare(\blacksquare p \cdot (pq + p + 1)) + 1 + \blacksquare\blacksquare p \cdot \blacksquare\blacksquare q \\
&= \blacksquare(q\utilde{p\blacksquare}p + \utilde{p\blacksquare}p + \blacksquare p) + 1 + \blacksquare\blacksquare p \cdot \blacksquare\blacksquare q \\
&= \blacksquare(q\blacksquare p + \cancel{\blacksquare p} + \cancel{\blacksquare p}) + 1 + \blacksquare\blacksquare p \cdot \blacksquare\blacksquare q \\
&= \underline{\blacksquare q} \cdot \blacksquare\blacksquare p + 1 + \blacksquare\blacksquare p \cdot \utilde{\blacksquare\blacksquare q} \\
&= \cancel{\blacksquare q \cdot \blacksquare\blacksquare q \cdot \blacksquare\blacksquare p} + 1 + \cancel{\blacksquare\blacksquare p \cdot \blacksquare\blacksquare q \cdot \blacksquare q} \\
&= 1
\end{aligned}$$

where the first step uses the distribution property; the second step uses the normality condition to join $\blacksquare\blacksquare p$ and $\blacksquare(pq+p+1)$; the third step applies distribution laws; the forth step applies $\blacksquare x = x\blacksquare x$; after some further simplification, the sixth step applies both $\blacksquare x\blacksquare\blacksquare x = \blacksquare x$ and $\blacksquare x = x\blacksquare x$, and some final simplification leads to the desired equality to the unit. $\dashv$

Theorem 44 *Let $\boldsymbol{M}$ be a normal modal logic defined with a finite set of axioms $A_1, \ldots, A_n$. On the algebraic side, suppose the equalities $A_i^t = 1$ hold, $1 \leq i \leq n$. Then a modal statement $\Gamma \vdash_M A$ is derivable iff its associated modal polynomial has 1-roots.*

Proof Sketch $\Gamma \vdash_{\mathbf{M}} A$ is provable iff $\vdash_{\mathbf{M}} \bigwedge\Gamma \to A$ is deducible from the axioms. In this deduction, the algebraic translation of every formula must be equal to 1. When the last step is reached, we have that $(\bigwedge\Gamma \to A)^t = 1$, such that by classical manipulations we obtain the multipliers for $\Gamma \vdash_{\mathbf{M}} A$.

On the other hand, if there are multipliers for $\Gamma \vdash_{\mathbf{M}} A$, by classical manipulations we obtain a multiplier a for $\vdash_{\mathbf{M}} \bigwedge\Gamma \to A$. Using the same modal algebraic equalities that were used to show that the multipliers are 1-roots to the statement, we show that $a = 1$. $\dashv$

4.1 Conclusion

Entailment multipliers are a characterisation of validity for propositional and modal classical logics. Furthermore, entailment multipliers can be seen as a proof invariants for several inference systems, which allows for the computation of multipliers in parallel with a proof-construction.

Future work on the interactions of algebraic and proof-theoretical methods aims at investigating the use of entailment multipliers to the computation of non-analytic cuts that allow for the computation of short proofs.

We also plan to investigate entailment multipliers for first-order logic, many-valued logics and other non-classical logics.

References

[1] P. Beame, S. Cook, J. Edmonds, R. Impagliazzo, and T. Pitassi. The relative complexity of NP search problems. In *Proceedings of the 27th ACM Symposium on Theory of Computing*, pages 303–314, 1995.

[2] P. Beame, R. Impagliazzo, J. Kraj'icek, T. Pitassi, and P. Pudl'ak. Lower bounds on hilbert's nullstellensatz and propositional proofs. In *Proceedings of the London Mathematical Society*, volume 73, pages 1–26, 1996.

[3] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*, volume 53 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, Cambridge, 2001.

[4] S. Buss, Russell Impagliazzo, Jan Krajicek, Pavel Pudlak, Alexander A. Razborov, and Jiri Sgall. Proof complexity in algebraic systems and bounded depth frege systems with modular counting. *Computational Complexity*, 6(3):256–298, 1997.

[5] Sam Buss and Toniann Pitassi. Good degree bounds on Nullstellensatz refutations of the induction principle. In *Proceedings from the 11th IEEE Conference on Computational Complexity*, pages 233–242, 1996.

[6] Walter Carnielli. Polynomial ring calculus for many-valued logics. In *Proceedings of 35th International Symposium on Multiple-Valued Logic*, pages 20–25, Calgary, Canad, 2005. IEEE Computer Society.

[7] B. F. Chellas. *Modal Logic — an Introduction*. Cambridge University Press, 1980.

[8] Marcello D'Agostino and Marco Mondadori. The taming of the cut. Classical refutations with analytic cut. *Journal of Logic and Computation*, 4:285–319, 1994.

[9] Marcelo Finger and Dov Gabbay. Cut and pay. *Journal of Logic, Language and Information*, 15(3):195–218, October 2006.

[10] Dov Gabbay. *Labelled Deductive Systems*, volume 1. Oxford University Press, 1996.

[11] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Freeman, 1979.

[12] Lászl'o Lovász. Bounding the independence number of a graph. *Annals of Discrete Mathematics*, 16:213–223, 1982.

[13] T. Pitassi. Algebraic propositional proof systems. In N. Immerman and P. Kolaitis, editors, *Descriptive Complexity and Finite Models*, volume 31 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 214–244. DIMACS, 1996.