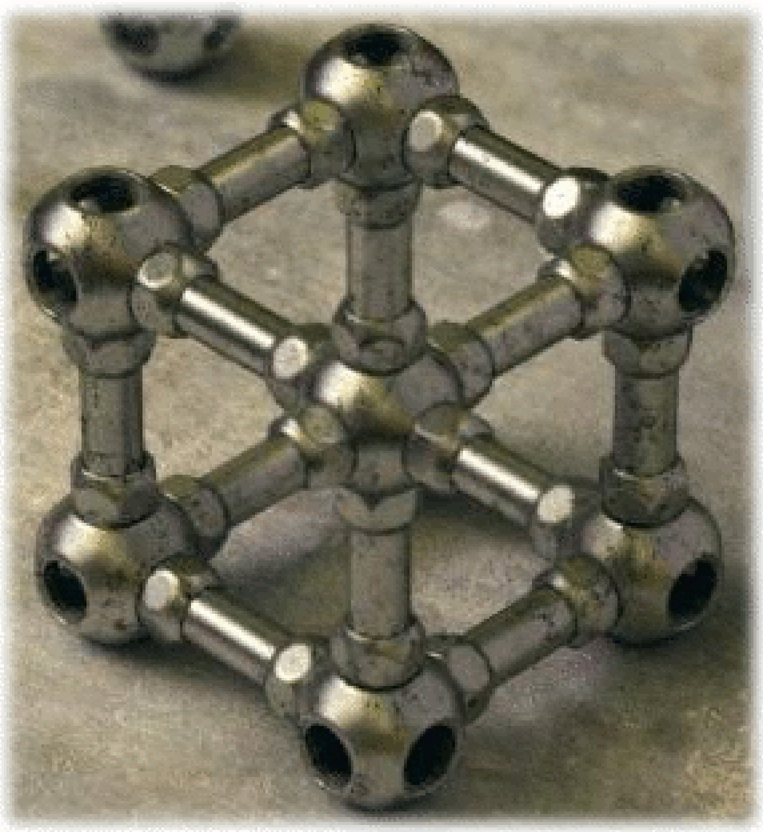

Entailment Multipliers: an Algebraic Characterization of Validity for Classical and Many-Valued Logics [1]

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 Many-Valued 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 for many-valued logics, called *entailment multipliers.* We demonstrate the existence of such multipliers for many-valued logics in an algebraic presentation of polynomial rings over finite-valued matrices. A set of conditions is present such that, if a logic can express operators satisfying those conditions, than the existence of entailment multipliers is guaranteed. Classical logic is a special case of importance and the existence and computation of entailment multipliers is discussed at length both over boolean rings and over boolean algebras.

1 Introduction

In this work we study an algebraic characterisation of the notion of logical validity for many-valued logics, which include classical logic as a special, two-valued case.

The notions of logical consequence and logical validity have been explored under several points of view, which include proof-theory and semantic entailment relations, but here the algebraic view is at the centre. We also explore the relationship between this algebraic view of validity characterisation with proof-theoretical and semantic approaches.

The current work is a deeper exploration of the initial results obtained in [8], which explored an algebraic characterisation of validity over *boolean rings.* The starting point of that study lies at Carnielli's result relating polynomial rings over finite-valued fields with the representation of connectives in many-valued logics. Here we extend those results to a much wider class of logics, expanding the scope of this new form of validity characterisation to an infinite number of many-valued logics. Those results not only cover any logic described by rings of polynomials over finite fields, but also applies to *boolean algebras.*

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

[⋆⋆] Partly supported by CNPq.

In this sense, this paper is a "coming home". For we departed from the usual algebraic presentation of classical logic in terms of boolean algebras to be able to present an algebraic characterisation of validity over *boolean rings* [8]. Now, when extending those results to many-valued logics, we show that they can be applied to boolean algebras as well.

Classical validity statements presented in terms of semantic entailment expressions or proof-theoretical sequents can be expressed as polynomials over boolean rings or over boolean algebras. In [8] it was shown that a characteristic polynomial could be built for boolean rings inserting variables as *multipliers* of terms obtained from the algebraic translation of formulas in the validity statements, and adding all such terms. A statement is classically *valid* iff the corresponding polynomial has roots when equated to the unit (the *1-roots*).

Here we show how a similar characterisation of validity can be applied to a large class of many-valued logics whose algebraic presentation satisfy a set of *multiplier matrix conditions.* A set of detailed of examples of entailment multipliers for some 3-valued logics is presented.

We then show that, as a particular case, boolean algebras also satisfy the multiplier matrix conditions, and detail the relationship between boolean algebraic multipliers and classical inference methods.

1.1 Comparisons with the Literature

As mentioned before, this work constitutes a a deeper exploration of the initial results obtained in [8]. That method has some common points in the literature with the use of Hilbert Nullstellensatz for propositional refutations, which was initially suggested by Lovász [11] 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* [12, 4, 2, 3].

In such an 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 $\sum_i P_i(\bar{x})Q_i(\bar{x}) = 1$.

The approach developed here has a much wider range of logics, not only classical logic. Both the approach using boolean rings and boolean algebras employ translation to polynomials that are essentially distinct from that work. However, no similarity occurs between our proposed method for many-valued logics and that approach.

1.2 Organisation of the Paper

After presenting some definitions and notation, Section 2 introduces boolean, two-valued rings and shows the existence of entailment multipliers for valid statements. We then generalise this notion for many-valued logics, providing in Section 3 a general result based on the formulation of special conditions over polynomial rings for algebraic matrices of many-valued logics. We then note that boolean algebras satisfy those conditions, and present in Section 4 methods for computing entailment multipliers over boolean rings which are derived from classical inference systems.

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 over Boolean Rings

We present here the results of [8]. For that purpose, a *ring* is considered as 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. Every element is its own inverse, $x + x = 0$ and the power of any variable is at most 1. As 0 is defined by (b_2), a boolean ring is sometimes represented as $\mathfrak{B} = \langle \mathcal{B}, \cdot, +, 1\rangle$. As usual, we write ab for $a \cdot b$.

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

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

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

The statement $A_1, \ldots, A_n \models B_1, \ldots, B_m$ is valid iff $(\prod_{i=1}^n A_i^t) \cdot \Big(\prod_{j=1}^m (B_i^t + 1)\Big) = 0$, so we can move backwards and forwards from the logic to the algebraic settings.

Definition 1 (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 $CP(\mathcal{S}) = x_1 \cdot (A_1^t + 1) + \ldots + x_n \cdot (A_n^t + 1) + y_1 \cdot B_1^t + \ldots + y_m \cdot B_m^t$.

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

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

In this case we say that the terms $a_1, \ldots, a_n, b_1, \ldots, b_m$ are entailment multipliers.

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

A direct proof of this theorem is presented in [8], but here it can be seen as a direct consequence of Theorem 2 in Section 3.2.

We use the notation of Labelled Deduction System (LDS) [9] to designate a formula and its corresponding entailment multiplier as the label:

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

Example 1. Consider the statement $A, C \to \neg A, B \to C \models \neg B, C \to D$. Its characteristic (ring) polynomial is:

$$x_1 \cdot (a+1) + x_2 \cdot (ca) + x_3 \cdot (b(c+1)) + y_1 \cdot (b+1) + y_2 \cdot (c(d+1)+1).$$

By making $x_1 = x_2 = 1$, $x_3 = a$, $y_1 = a(c+1)$ and $y_2 = 0$ and applying the rules of boolean rings, we see that the characteristic polynomial is equal to 1, so by Theorem 1 the statement is valid and we write

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

Note that 0-labelled formulas play no part in the validity of the statement. Also note that multipliers are not unique, for the following also represent a possible set of multipliers for the same validity statement

$$c(d+1) : A, (d+1) : C \to \neg A, 0 : B \to C \models 0 : \neg B, 1 : C \to D$$

The two different sets of multipliers represent different two different proofs for the same statement. □

In [8] it was shown several ways to compute boolean-ring entailment multipliers according to several classical proof methods, which we will be presented for boolean algebras in Section 4.

3 Algebraic Multipliers for Many-valued Logics

We now generalise the notion of algebraic multipliers to a class of many-valued logics. We first introduce a matrix presentation of multi-valued entailment. In that setting, the a general notion of entailment multiplier is shown to exist.

In principle, a logic can have any number of connectives and truth values. So consider initially an *algebraic alphabet* as a set $\mathfrak{F}$ of functional symbols in which every symbol $f \in \mathfrak{F}$ is associated to a non-negative integer n, namely the symbol's *arity*. Let $\mathfrak{F}_n \subseteq \mathfrak{F}$ be the set of functional symbols of arity n.

An *algebra* $\mathcal{A}$ of type $\mathfrak{F}$ is a pair $\mathcal{A} = \langle \mathcal{A}, \mathcal{F} \rangle$ where $\mathcal{A}$ is a non-empty set[1] called the *universe* of the algebra, and $\mathcal{F}$ is a family of operators in $\mathcal{A}$ indexed by the alphabet $\mathfrak{F}$ such that for each n-ary symbol $f \in \mathfrak{F}$ there corresponds an n-ary operator $f^{\mathcal{A}} \in \mathcal{F}$; the elements of $\mathcal{F}$ are called the *fundamental operators* in $\mathcal{A}$. Further on, we will also deal with *derived operators*.

Example 2. We present some well-known algebraic concepts in the light of those definitions.

(a) A *group* is a triple $\langle G, +, 0 \rangle$ where $\mathfrak{F} = \mathfrak{F}_0 \cup \mathfrak{F}_2$, $\mathfrak{F}_0 = \{0\}$ and $\mathfrak{F}_2 = \{+\}$ such that for $a, b, c \in G$:
   - $(a+b)+c = a+(b+c)$;

[1] We follow the tradition of using the same symbol both for the algebra and for its universe set.

- $0 + a = a + 0 = a$;
- there is a $-a \in G$ such that $a + (-a) = (-a) + a = 0$.

A group is *commutative* if it satisfies:

- $a + b = b + a$.

(b) A *(simple) ring* is a 4-tuple $\langle R, +, \cdot, 0\rangle$ where $\mathfrak{F}_0 = \{0\}$ and $\mathfrak{F}_2 = \{+, \cdot\}$ satisfying:

- $\langle R, +, 0\rangle$ is a commutative group;
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- $(a \cdot (b + c) = a \cdot b + a \cdot c)e((a + b) \cdot c = a \cdot c + b \cdot c)$.

A group is commutative if it satisfies:

- $a \cdot b = b \cdot a$.

The ring *has a unit* if

- there is $1 \in \mathcal{A}$ such that $1 \cdot a = a \cdot 1 = a$.

(c) A *field* is a 5-tuple $\langle K, +, \cdot, 0, 1\rangle$ where $\mathfrak{F}_0 = \{0, 1\}$ and $\mathfrak{F}_2 = \{+, \cdot\}$ such that:

- $\langle K, +, \cdot, 0\rangle$ is a commutative ring with unit 1;
- $1 \neq 0$;
- If $a \neq 0$ then there is $a^{-1} \in K$ such that $a \cdot a^{-1} = 1$. □

Here is another well-known algebra that is very useful in the present work.

Example 3. 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) $a + a = 0$

Note that in a boolean ring, $-a = a$. □

The logical notion of formula is represented by that of *algebraic terms*. Let X be a non-empty set of variables, $X \cap \mathcal{A} = \varnothing$. The set of *$\mathcal{A}$-terms* $\mathrm{Term}_{\mathcal{A}}$ over X is the smallest set such that

i. $X \cup \mathfrak{F}_0 \subset \mathrm{Term}_{\mathcal{A}}$;
i. if $a_1, \ldots, a_n \in \mathrm{Term}_{\mathcal{A}}$ and $f^{\mathcal{A}} \in \mathfrak{F}_n$ then $f^{\mathcal{A}}(a_1, \ldots, a_n) \in \mathrm{Term}_{\mathcal{A}}$.

A many-valued *interpretation* is a function $\tau : \mathrm{Term}_{\mathcal{A}} \to \mathcal{A}$ that associates each term a to an element of the algebra, a^τ, such that

$$(f(a_1, \ldots, a_n))^\tau = f^{\mathcal{A}}(a_1^\tau, \ldots, a_n^\tau) \qquad a_1, \ldots, a_n \in \mathrm{Term}_{\mathcal{A}}, f \in \mathfrak{F}_n.$$

We drop the algebra index when no confusion arises. The actual notion of a *formula* is obtained by replacing the set of variables X with a set of propositional symbols $\mathcal{P}$, and the translation between terms and formulas is then immediate.

To generalise the notion of classical truth table, we employ the notion of algebraic matrices. The matrix presentation of an n-ary operator f in an m-valued algebra contains m^n cells, such that the cell corresponding to $\langle a_1, \ldots, a_n\rangle$ contains the value of $f(a_1, \ldots, a_n) \in \mathcal{A}$, $|\mathcal{A}| = m$. A *matrix* $\mathfrak{M} = \langle \mathcal{A}, \mathcal{D}\rangle$ is a pair where $\mathcal{A}$ is an algebra and $\mathcal{D} \subsetneq \mathcal{A}$ is the set of *designated values*, which represent the "true" values in a many-valued setting.

We now present a few examples of matrices. We start with the well know notion of a boolean ring.

Example 4. A boolean ring is by the following matrix:

$\mathcal{A} = \{0, 1\}$
$\mathcal{F} = \{\cdot, +, \top\}$
$\mathcal{D} = \{1\}$

$\cdot$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

	$\neg$
0	1
1	0

Note that these matrices are consistent with the definitions in Section 2. □

And now we present the matrix for the well-known 3-valued logic Ł$_3$.

Example 5. The Łukasiewicz 3-valued logic Ł$_3$ can be defined by the following matrix:

$\mathcal{A} = \{0, 1, 2\}$
$\mathcal{F} = \{\neg, \rightarrow\}$
$\mathcal{D} = \{2\}$

$\rightarrow$	0	1	2
0	2	2	2
1	1	2	2
2	0	1	2

	$\neg$
0	2
1	1
2	0

In such a logic, $p \models p$ and $\models p \rightarrow p$ but $p \rightarrow (p \rightarrow q) \not\models p \rightarrow q$. □

The important notion here is that of a *multi-valued entailment* over a matrix $\mathfrak{M}$ or a class of matrices $\mathcal{M}$. If Γ and Δ be sets of $\mathcal{A}$-terms we say that Γ entails Δ over $\mathcal{M}$, $\Gamma \models_{\mathcal{M}} \Delta$, if for every $\langle \mathcal{A}, \mathcal{D} \rangle \in \mathcal{M}$ and for every interpretation τ, if $A^\tau \in \mathcal{D}$ for all $A \in \Gamma$ then $B^\tau \in \mathcal{D}$ for some $B \in \Delta$. We also omit the class of matrices $\mathcal{M}$ when it is clear from the context.

In such a many-valued setting, a generalised notion of multiplier can be obtained if some conditions are respected. For that, first we need to establish a class of proof polynomials.

3.1 Polynomials

A fundamental concept in this study is that of a polynomial. Given an algebra $\mathcal{A} = \langle \mathcal{A}, \mathcal{F} \rangle$, we define the set $\mathcal{A}[X]$ of *polynomials* induced by $\mathcal{A}$ on variables $X = \{x_1, \ldots, x_n\}$ as the smallest set such that:

i. $X \cup \mathcal{A} \subset \mathcal{A}[X]$;
ii. if $P_1, \ldots, P_n \in \mathcal{A}[X]$ and $f \in \mathfrak{F}_n$, then $f^{\mathcal{A}}(P_1, \ldots, P_n) \in \mathcal{A}[X]$.

Note that the set of $\mathcal{A}$-terms is a subset of the set of polynomial defined by $\mathcal{A}$. In this sense, it is possible to generalise the notion of a term valuation τ to the set of all polynomials by fixing, for each variable $x \in X$, $x^\tau \in \mathcal{A}$ and then generalising the notion of valuation for polynomials in the usual way: $(f(a_1, \ldots, a_n))^\tau = f(a_1^\tau, \ldots, a_n^\tau)$.

An m-ary operator g is (explicitly) *definable* in algebra $\mathcal{A}$ if there is a term $a(x_1, \ldots, x_m)$ on variables $x_1, \ldots, x_m$ in which g does not occur such that, for every interpretation τ, $g(x_1, \ldots, x_m)^\tau = (a(x_1, \ldots, x_m))^\tau$.

Polynomials are of interest because they enable us to define algebraic operators. In fact, we say that a polynomial $P(x_1, \ldots, x_m)$ *defines* an operator

$f : \mathcal{A}^n \to \mathcal{A}$ over $\mathcal{A}$ if, when applied to elements of $\mathcal{A}$ (ie, to truth values), the polynomial yields $f^{\mathcal{A}}$'s matrix. For example, consider $\mathcal{A} = \{0, 1, 2\}$ as the 3-valued universe of logic Ł$_3$ and $\cdot$ and $+$ as product and sum modulo 3. Then the polynomial $P_{\neg}(x) = 2 \cdot x + 2$ defines the operator $\neg$ in Ł$_3$ as presented in example 5. In fact, $P_{\neg}(0) = 2$, $P_{\neg}(1) = 2 \cdot 1 + 2 = 1$ and $P_{\neg}(2) = 2 \cdot 2 + 2 = 0$.

As a further example, consider the boolean connectives $\{\neg, \wedge, lor, \rightarrow\}$ and the representation in a boolean ring $\langle +, \cdot, 1\rangle$:

$$\begin{aligned}
&P_{\neg}(x) = x + 1\\
&P_{\wedge}(x, y) = x + y\\
&P_{\vee}(x, y) = x \cdot y + x + y\\
&P_{\rightarrow}(x, y) = x \cdot y + x + 1
\end{aligned}$$

In the study of algebraic properties of finite-valued logics, we are interested in polynomials induced by *finite fields*, which are algebraic fields with finitely many elements; see Example 2(c). There are well-known interesting properties of finite fields [10]:

- Every finite field has exactly p^n elements, where p is a prime number and n a positive integer.
- For every prime p and positive integer n there is a finite field of size p^n
- Two finite fields of same size are isomorphic.

As finite fields of the same cardinality are all isomorphic, they can be brought to a "normal form", as follows. For $n \in \mathbb{N}$ and $z \in \mathbb{Z}$, let $\bar{z}_k$ denote:

$$\bar{z}_k = \{x \in Z | x - z \text{ is divisible by } k\}.$$

In this case $\bar{1}_2 = \{\ldots, -1, 1, 3, 5, 7, \ldots\}$, $\bar{0}_2 = \{\ldots, -2, 0, 2, 4, \ldots\}$, and $\bar{1}_3 = \bar{4}_3 = \bar{7}_3 = \overline{10}_3 = \{\ldots, -2, 1, 4, 7, 10, \ldots\}$. It is clear that $\bar{k}_k = \bar{0}_k$, $\overline{(k+1)}_k = \bar{1}_k$, etc. Let $\mathbb{Z}_k = \{\bar{0}_k, \bar{1}_k, \ldots, \overline{(k-1)}_k\}$ and define the following operations on $\mathbb{Z}_k$:

1. $\bar{a}_k +_k \bar{b}_k = \overline{(a+b)}_k$;
2. $\bar{a}_k \cdot_k \bar{b}_k = \overline{(a \cdot b)}_k$.

The algebra $\mathbb{Z}_k = \langle \mathbb{Z}_k, 0_k, 1_k, +_k, \cdot_k \rangle$ is a commutative ring with unit, and every finite field is isomorphic to some $\mathbb{Z}_{p^n}$ for some prime p and integer $n > 0$ with $k = p^n$.

In the study of many-valued logic, Carnielli [5] proved an important representation theorem relating finite field with many-valued logics.

Proposition 1 ([5]). *Let $\mathcal{A}$ be a non-empty finite set of truth values, and let $f : \mathcal{A}^m \to \mathcal{A}$ be an m-ary operation on $\mathcal{A}$. Then f can be represented by a polynomial over $\mathbb{Z}_{p^n}[x_1, \ldots, x_m]$ for any p prime and integer n such that $p^n \geq |\mathcal{A}|$.*

This means that every connective in a finite valued logic with m truth values can be represented as a polynomial in $\mathbb{Z}_{p^n}$, for $p^n \geq m$. The particular case when $m = p^1$ is also important, as most finite-valued logics of interest are found in that case, in which we have that $mx = 0$ and $x^m = x$.

Example 6. Let us continue the example on Łukasiewicz 3-valued logic Ł$_3$ to illustrate the result of Proposition 1. In this case, we have that $|A| = 3$, $p = 3$ and $n = 1$, such that the matrix of example 5 can be represented by the following polynomials (recall that the truth values are $\{0, 1, 2\}$ and the only designated value is 2):

- Operator $\neg$ is represented in $\mathbb{Z}_3[x, y]$ by
$$P_\neg(x) = 2x + 2;$$
- Operator $\rightarrow$ is represented in $\mathbb{Z}_3[x, y]$ by
$$P_\rightarrow(x, y) = 2x \cdot (y + 1) \cdot (x \cdot y + y + 1) + 2.$$

In this way, the valid formula $x \rightarrow x$ is represented by the polynomial $P_{x\rightarrow x}(x) = 2x(x + 1)(x^2 + x + 1) + 2 = (2x^2 + 2x)(x^2 + x + 1) + 2 = 2(x^4 + 2x^3 + 2x^2 + x) + 2$. As in $\mathbb{Z}_3[X]$ we have that $x^3 = x$ and $3x = 0$, we can further simplify $P_{x\rightarrow x}(x) = 2(x^2 + 2x + 2x^2 + x) + 2 = 2(3x^2 + 3x) + 2 = 3 \cdot 0 + 2 = 2$, so $x \rightarrow x$ is represented by a polynomial that is equal to the constant designated truth value 2.

In fact, it follows from the Proposition above that every valid formula in Ł$_3$ is represented by a polynomial identical to 2. □

We are now in a position to state and prove the main result for algebraic multipliers in multiplicative logics

3.2 Algebraic Multipliers for Many-valued Logics

Given a matrix $\mathfrak{M} = \langle\langle\mathcal{A}, \mathcal{F}\rangle, \mathcal{D}\rangle$, suppose $\mathcal{A}$ is bi-partitioned in $\mathcal{D}$ (designated values) and $\mathcal{N}$ (non-designated values).

We say that $\mathfrak{M}$ is a *multiplier matrix* if it is possible to define operators $\neg \in \mathfrak{F}_1$ and $+, \cdot \in \mathfrak{F}_2$ satisfying the following restrictions, for $d, d_1, d_2 \in \mathcal{D}$, $n, n_1, n_2 \in \mathcal{N}$ and $a, b, c \in \mathcal{A}$:

(mm_1) $\neg d \in \mathcal{N}$;
(mm_2) $a \cdot n \in \mathcal{N}$;
(mm_3) $n \cdot a \in \mathcal{N}$;
(mm_4) $d_1 \cdot d_2 \in \mathcal{D}$;
(mm_5) $a + (b + c) = (a + b) + c$;
(mm_6) $a + b = b + a$;
(mm_7) $n_1 + n_2 \in \mathcal{N}$;
(mm_8) $d + n \in \mathcal{D}$.

Note that the conditions force $\cdot$ to be neither associative nor commutative. We note some immediate consequences of the conditions above which will be used in the proof of Theorem 1.

- if $a_1 + \ldots + a_n \in \mathcal{D}$ then some $a_i \in \mathcal{D}$, by (mm_5), (mm_6), (mm_7) and (mm_8);

- if $a_1 + \ldots + a_n + b_1 + \ldots + b_m \in \mathcal{D}$ and all $b_j \in \mathcal{N}$ then $a_1 + \ldots + a_n \in \mathcal{D}$, by (mm_5), (mm_6), (mm_7) and (mm_8);
- $a \cdot b \in \mathcal{D}$ iff $a, b \in \mathcal{D}$, by (mm_2), (mm_3) and (mm_4);

It is clear that Boolean Rings are multiplier matrices, satisfying all conditions (mm_1)–(mm_8). An example of 3-valued logic that immediately satisfies conditions (mm_1)–(mm_8) is ϵ_3 that will be described in Example 7. A more complex situation when we consider the 3-valued logic Ł$_3$, which will be discussed as well.

We now generalise the notion of a characteristic polynomial.

Definition 2 (Many-valued Characteristic Polynomial). Given an entailment statement $\mathcal{S} = a_1, \ldots, a_n \models b_1, \ldots, b_m$ over a many-valued multiplier matrix $\mathfrak{M} = \langle\langle \mathcal{A}, \mathcal{F}\rangle, \mathcal{D}\rangle$ satisfying $(mm_1 - -mm_9)$ above, its *characteristic polynomial* over variables $x_1, \ldots, x_n, y_1, \ldots, y_m$ is

$$CP_{\mathcal{S}}(x_1, \ldots, x_n, y_1, \ldots, y_m) = x_1 \cdot (\neg a_1) + \ldots + x_n \cdot (\neg a_n) + y_1 \cdot b_1 + \ldots + y_m \cdot b_m$$

.

The characteristic polynomial has $\mathcal{D}$-*roots* if there are terms $p_1, \ldots, p_n, q_1, \ldots, q_m$ such that for any valuation τ

$$p_1^\tau \cdot (\neg a_1^\tau) + \ldots + p_n^\tau \cdot (\neg a_n^\tau) + q_1^\tau \cdot b_1^\tau + \ldots + q_m^\tau \cdot b_m^\tau \in \mathcal{D}.$$

The terms $p_1, \ldots, p_n, q_1, \ldots, q_m$ are entailment multipliers.

Theorem 2 (Many-valued Entailment Multipliers). *An entailment statement $\mathcal{S} = a_1, \ldots, a_n \models b_1, \ldots, b_m$ over a many-valued multiplier matrix $\mathfrak{M} = \langle\langle \mathcal{A}, \mathcal{F}\rangle, \mathcal{D}\rangle$ is valid iff its characteristic polynomial $CP_{\mathcal{S}}(X)$ has $\mathcal{D}$-roots.*

Proof. Let n and d be elements of $\mathcal{N}$ and $\mathcal{D}$, respectively.

($\Rightarrow$) Suppose that $a_1, \ldots, a_n \models b_1, \ldots, b_m$ is valid. Fix a valuation τ such that $a_k^\tau \in \mathcal{D}$ for $1 \leq k \leq n$. Then by the multiplier matrix conditions, we have that

$$\begin{aligned} CP_{\mathcal{S}}(X) \in \mathcal{D} &\Longrightarrow x_1 \cdot (\neg a_1) + \ldots + x_n \cdot (\neg a_n) + y_1 \cdot b_1 + \ldots + y_m \cdot b_m \in \mathcal{D} \\ &\Longrightarrow y_1 \cdot b_1 + \ldots + y_m \cdot b_m \in \mathcal{D}. \end{aligned}$$

Due to validity, there exits a b_r with $b_r^\tau \in \mathcal{D}$. If we take $y_r \in \mathcal{D}$ and $y_j \in \mathcal{N}$ for $j \neq r, 1 \leq j \leq m$, then we have that

$$\begin{aligned} CP_{\mathcal{S}}(X) \in \mathcal{D} &\Longrightarrow y_1 \cdot b_1 + \ldots + y_m \cdot b_m \in \mathcal{D} \\ &\Longrightarrow y_r \cdot b_r \in \mathcal{D}. \end{aligned}$$

and the latter is a true statement by (mm_4), so $CP_{\mathcal{S}} \in \mathcal{D}$.

($\Leftarrow$) Now suppose there are entailment multipliers $p_1, \ldots, p_n, q_1, \ldots, q_m$ such that

$$p_1^\tau \cdot (\neg a_1^\tau) + \ldots + p_n^\tau \cdot (\neg a_n^\tau) + q_1^\tau \cdot b_1^\tau + \ldots + q_m^\tau \cdot b_m^\tau \in \mathcal{D}$$

for every valuation τ. Suppose also that $a_i^\tau \in \mathcal{D}$ for $1 \leq i \leq n$. Then clearly $q_1^\tau \cdot b_1^\tau + \ldots + q_m^\tau \cdot b_m^\tau \in \mathcal{D}$. By the multiplier matrix conditions, it must be the case that for every τ there exists $p_j^\tau \cdot b_j^\tau \in \mathcal{D}$, $1 \leq j \leq m$, which again by those conditions imply that $b_j^\tau \in \mathcal{D}$. Among $b_1^\tau, \dots, b_m^\tau$ which $b_j^\tau \in \mathcal{D}$ may depend on τ, but the fact that there always exists one such b_j guarantees that $\mathcal{S} = a_1, \dots, a_n \models b_1, \dots, b_m$ is valid.

As the conditions of multiplier matrices apply to boolean rings, it follows that for classical logic, when translated to boolean rings, any valid logical entailment has an associated set of entailment multipliers. Thus Theorem 1 is an instance of Theorem 2.

Let us now examine a 3-valued logic that is also a multiplier matrix.

Example 7. Consider a 3-valued logic with truth values $\{0, \epsilon, 1\}$ in which ϵ is a truth value "just above 0", with connectives $\{\cdot, +, \neg\}$, and call it ϵ_3-logic. Consider its matrix:

$\mathcal{A} = \{0, \epsilon, 1\}$
$\mathcal{F} = \{\cdot, +, \neg\}$
$\mathcal{D} = \{1\}$

$+$	0	ϵ	1
0	0	ϵ	1
ϵ	ϵ	ϵ	1
1	1	1	ϵ

$\cdot$	0	ϵ	1
0	0	0	0
ϵ	0	ϵ	ϵ
1	0	ϵ	1

	$\neg$
0	1
ϵ	1
1	0

Clearly this is a multiplier matrix, for which by Theorem 2 a sequent is valid iff there are entailment multipliers. Note that $\epsilon \models \epsilon$ as for $x = 1$ and $y = 0$ we have that $x \cdot \neg\epsilon + y \cdot \epsilon = 1$, but $1 \not\models \epsilon$ as the equation $x \cdot \neg 1 + y \cdot \epsilon = 1$ has no roots. □

Note that the conditions for multiplier matrices do not impose $\cdot$ to be either associative nor commutative. In fact, had we defined a small variant of logic ϵ_3 with a non-commutative multiplication given by

$\cdot$	0	ϵ	1
0	0	0	0
ϵ	0	ϵ	ϵ
1	0	0	1

this would still be a multiplier matrix for which the theorem applies. In the following we analyse interesting cases of entailment multipliers.

3.3 Entailment Multipliers and Łukasiewicz 3-valued Logic

In the case of Łukasiewicz 3-valued logic Ł$_3$ with , we cannot apply immediately Theorem 2, for there is no immediately available multiplication and sum. In this case there are two options, namely either try to define negation, sum and multiplication operators satisfying multiplier matrix conditions (mm_1)–(mm_8) using the existing operators or extend the algebra's type so as to include such operators. As it We start by the latter, as it is straightforward.

In fact, Proposition 1 allows us to consistently extend a k-valued matrix, for $k = p^n$ as above, with the addition of operators $+_k$ and $\cdot_k$. In fact, as the original operators can be expressed in terms of a polynomial employing constants and

$+_k$ and $\cdot_k$, the addition of such operators will not add any inconsistencies. In that case, the extended Ł$_3$-matrix will contains operators $\{\neg, \rightarrow, \cdot, +\}$ where the latter two operator satisfy:

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The extended Ł$_3$-matrix satisfy all conditions (mm_1)–(mm_8), so entailment multipliers do exist for Ł$_3$-valid logical entailment. Even if the Ł$_3$-valid has no occurrence of the operators $+$ and $\cdot$, those operators can occur in the multipliers.

Example 8. Consider the Ł$_3$-valid entailment statements:

- $\models a \rightarrow a$. Its characteristic polynomial is $CP(x) = x \cdot 2$, so with $x = 1$, $CP(x) = 2 \in \mathcal{D}$.
- $a \models a$. Its characteristic polynomial is $CP(x, y) = x \cdot (2a + 2) + y \cdot a$, so with $x = y = 1$ one obtains $CP(x, y) = 3a + 2 = 2 \in \mathcal{D}$.
- $a \models b \rightarrow a$. Its characteristic polynomial is $CP(x, y) = x \cdot (\neg a) + y \cdot (a \rightarrow b) = x \cdot (2a+2) + y \cdot (2b(a+1)(ab+a+1)+2)$, then with multipliers $x = 2b(ab+a+1)$ and $y = 1$ one obtains $CP(x, y) = 6b(a + 1)(ab + a + 1) + 2 = 2 \in \mathcal{D}$.

Note that in this last case the multipliers contain operators $+$ and $\cdot$ but not the valid entailment. □

Now let us go back to the case where no new operators are added. Is it possible to apply Theorem 2? We will see that the answer is positive, by defining Ł$_3$-operators in terms of $\{\neg, \rightarrow\}$ only.

Recall the original definition of the Ł$_3$ matrix as

$$\begin{aligned} \mathcal{A} &= \{0, 1, 2\} \\ \mathcal{F} &= \{\neg, \rightarrow\} \\ \mathcal{D} &= \{2\} \end{aligned}$$

$\rightarrow$	0	1	2
0	2	2	2
1	1	2	2
2	0	1	2

	$\neg$
0	2
1	1
2	0

Now consider the following definitions

$$\begin{aligned} -a &= a \rightarrow 1 \\ a \odot b &= -(a \rightarrow -b) \\ a \times b &= \neg - (a \odot b) \\ a \Delta b &= -(\neg A \odot \neg b) \\ a \oplus b &= ((-a) \times b) \Delta (a \times (-b)) \end{aligned}$$

which generate the following matrices for operators $\odot, \oplus$ and $-$

$\odot$	0	1	2
0	1	1	1
1	1	1	1
2	1	1	2

$\oplus$	0	1	2
0	1	1	2
1	1	1	2
2	2	2	1

	$-$
0	2
1	2
2	1

Clearly, those operators satisfy the multiplier matrix conditions (mm_1)–(mm_8). So we can apply Theorem 2 in for valid Ł$_3$-entailment. As for the associated polynomials, in terms of ring operations $\cdot, +$ and $\neg$:

$$\begin{aligned} \neg a &= 2 \cdot a + 2 \\ a \to b &= 2 \cdot a \cdot (b+1) \cdot (a \cdot b + b + 1) + 2 \end{aligned}$$

and the polynomials for the newly defined operators are:

$$\begin{aligned} -a &= a^2 + 2a + 2 \\ a \odot b &= a^2b^2 + 2a^2b + 2ab^2 + ab + 1 \\ a \oplus b &= a^2b^2 + 2a^2b + 2ab^2 + ab + 2a^2 + 2b^2 + a + b + 1 \end{aligned}$$

So we can express the characteristic polynomials of valid entailment statements in terms of those equalities.

Example 9. Consider the Ł$_3$-valid entailment statement $a \models a$, which according to the connectives above has as characteristic polynomial

$$\begin{aligned} &(x \odot -a) \oplus (y \odot a) = \\ &\qquad (x^2(2a^2 + a + 2) + x(a^2 + 2a + 1) + 1) \oplus (y^2(a^2 + 2a) + y(2a^2 + a) + 1) \end{aligned}$$

In this case, if we make $x = 2$ and $y = 2$ we obtain

$$(a^2 + 2a + 2) \oplus (2a^2 + a + 1) = 2 \in \mathcal{D}.$$

Thus we have presented entailment multipliers for Ł$_3$ without extending it with more expressive operators. □

This example leaves an open question: is it possible to determine if a given set of fundamental operators can define a set of operators satisfying multiplier matrix conditions (mm_1)–(mm_8)?

4 Entailment Multipliers for Boolean Algebras

The study of entailment multipliers was motivated by Carnielli's result on the expressivity of many-valued logics over many-valued rings. In case of two-valued logics, that lead us to focus on classical *boolean rings* as the object of the study. So entailment multipliers were proven to exist for boolean rings.

It remains the question on whether entailment multipliers exist for *boolean rings*. But one only has to note that boolean algebras satisfy all the multiplier matrix conditions (mm_1)–(mm_8). In fact, if we consider a classical boolean algebra $\langle \mathcal{A}, \wedge, \vee, \neg, 0, 1 \rangle$ and consider, as usual, $\wedge$ as multiplication and $\vee$ as sum, it is immediate that Theorem 2 can be applied to boolean algebras.

In fact, given a classical statement $A_1, \ldots, A_n \models B_1, \ldots, B_m$, its associated *characteristic polynomial over boolean algebras* is

$$CP(x_1, \ldots, x_n, y_1, \ldots, y_m) = x_1 \wedge (\neg A_1^t) \vee \ldots \vee x_n \wedge (\neg A_n^t) \vee y_1 \wedge B_1^t \vee \ldots \vee y_m \wedge B_m^t.$$

The following result comes directly from the observation that $\{\wedge, \vee, \neg\}$ satisfy the multiplier matrix restrictions, $\mathcal{D} = \{1\}$ and $\mathcal{N} = \{0\}$.

Corollary 1. *A classical entailment statement is valid iff there are terms for which its characteristic polynomial over boolean algebras is equal to* 1.

In the following, we consider $\cdot = \wedge$ and $+ = \vee$. We reexamine Example 1 under a boolean algebra setting.

Example 10. Consider the valid statement $A, C \to \neg A, B \to C \models \neg B, C \to D$. Its characteristic polynomial over boolean algebras is

$$x_1 \cdot (\neg a) + x_2 \cdot (ca) + x_3 \cdot (b\neg c) + y_1 \cdot (\neg b) + y_2 \cdot (\neg c + d).$$

By making $x_1 = x_2 = 1$, $x_3 = a$, $y_1 = a(\neg c)$ and $y_2 = 0$, the characteristic polynomial becomes equal to 1. Note that this corresponds to exactly the same multipliers as those for boolean rings in Example 1. However, due to the boolean algebra equivalence $1 + x = 1$, unlike boolean rings, the 0-multipliers could be a changed for absolutely any term, thus obtaining as multipliers, for instance, $x_3 = a$, $y_1 = a(\neg c)$ and $y_2 = abc$. □

Each inference system may provide at least one method of computing entailment multipliers, as each sound inference method consists of a set of transformations that preserve the validity, thus obtaining a new set of multipliers from previous ones. Therefore, at each transformation step one can compute new multipliers from previous ones. In analogy to what was done in [8] for boolean rings, we now investigate how such transformation operates over boolean algebras for two proof methods: resolution and Gentzen Sequent Calculus.

4.1 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. Consider the characteristic polynomial for the resolvents, and make $y(\neg B^t)$ the multiplier of the resolvent $A \vee p_i$ and $y(\neg A^t)$ the resolvent of $p_i \vee B$, thus obtaining:

$$y(\neg B^t)(\neg A^t)p_i + y(\neg A^t)(\neg B^t)(\neg p_i) = y(\neg B^t)(\neg A^t)$$

which shows how y becomes the multiplier of the resolved formula $A \vee B$ when it is used as a subsequent resolvent.

If we look at this resolution step from bottom to the top, we see that the term corresponding to the bottom formula is multiplied by p_i on the resolvent where $\neg p_i$ occurs, and the term corresponding to the bottom formula is multiplied by $\neg p_i$ on the resolvent where p_i occurs. This gives us the basic rule for constructing algebraic multipliers via resolution.

Example 11. To show by resolution that $\neg s \vee q, \neg p \vee q, p \vee s \models q$, we have to show that 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 labelled resolution graph in Figure 1, in which each edge is labelled with the term corresponding to the negation of the resolved literal.

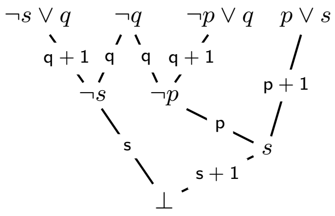

Fig. 1. Edge-labelled resolution graph

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:

$$\begin{array}{rr}(\neg\mathsf{q})\mathsf{s} : \neg s \vee q, & \mathsf{qs} + \mathsf{qp}(\neg\mathsf{s}) : \neg q,\\ (\neg\mathsf{q})\mathsf{p}(\neg\mathsf{s}) : \neg p \vee q, & (\neg\mathsf{p})(\neg\mathsf{s}) : p \vee s\end{array}$$

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

$$\begin{array}{rr}1 : \neg s \vee q, & \mathsf{s} + \mathsf{p}(\neg\mathsf{s}) : \neg q,\\ (\neg\mathsf{s}) : \neg p \vee q, & 1 : p \vee s\end{array}$$

Finally, we note that the verification of the 1-sum is isomorphic to the resolution graph, as shown in Figure 2.

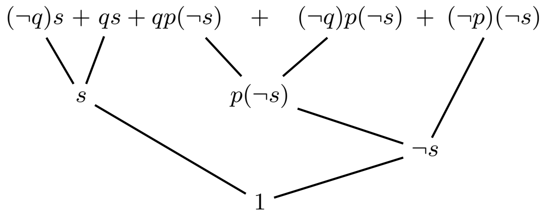

Fig. 2. Reduction of 1-sum isomorphic to resolution graph in Figure 1

Each transformation step is an application of $ab + a(\neg b) = a$. In this sense, we can say that resolution is simulated by algebraic methods. This may not remain true if we apply boolean algebraic equivalences to the multipliers, e.g., $s + p(\neg s) = s + p$. □

Formally, define an *edge-labelled resolution graph* as a resolution graph in which edges are labelled with a term $(\neg p)^t$, where p is the reduced literal. This is the input for Algorithm 4.1 computing entailment multipliers.

Algorithm 4.1 Resolution-based computation of entailment multipliers

```
Input: an edge-labelled 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 $(\neg A_i^t)$
  end for
  return the set $\{a_i : A_i | 1 \leq i \leq n\}$
```

Theorem 3. *Algorithm 4.1 computes a set of multipliers such that the verification of the 1-sum as a set of applications of $ab + a(\neg b) = a$ is isomorphic to the input edge-labelled resolution graph.* □

We note that this procedure is totally analogous to that used to compute multipliers in a boolean ring in [8]. However, this observation does not remain valid for the method for computing multipliers based on the sequent calculus.

4.2 Sequent Calculus

We focus on a presentation of the sequent calculus that promotes the use of non-analytic cuts, called a *cut-based* sequent calculus [7]. In a cut-based sequent calculus, the cut rule is *not* eliminable, and is in fact the only branching rule. This version of the sequent calculus is closely related to KE tableau [6], which is a decision procedure for full propositional classical logic.

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

The sequent calculus is presented by means of *connective rules* and *structural rules*; the 1-sum is kept invariant in all of them. Figure 3 presents the connective rules for cut-based sequent propositional inferences and the structural rules are

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

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

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

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

$$\frac{\Gamma, a : A \vdash \Delta, b : B}{\Gamma \vdash \Delta, a + b : A \rightarrow B}\,(\vdash\rightarrow)$$

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

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

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

presented in Figure 4. If labels are omitted from Figures 3 and 4, one obtains the cut-based rules of [7].

Note that in the cut rule all multipliers in the sequent are changed; in all other rules, only the multipliers of main formulas are affected. There is no need to define structural rules for commutativity and associativity as both antecedents and consequents are multisets. Repeated formulas in a multiset are dealt with by the right and left contraction rules. 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 0-labelled. The Axiom rule has no premiss and produces a 1-label to the relevant formulas.

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

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

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

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

The entailment multipliers are computed simultaneously with the deduction. Note that at the last step, the multiplier of $C \to B$ was simplified from $(\neg b)(\neg a) + 1$ to 1. □

It is worth noting that at each deduction step in example 12 the 1-sum holds. This is called *1-sum-invariant propagation.*

Lemma 1 (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 $1 \cdot (\neg A^t) + 1 \cdot A = 1$, so (Axiom) keeps the 1-sum.

We show propagation of the 1-sum for 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:

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

But we also have that

$$aA^t(\neg B^t) + aA^tB^t = aA^t, \tag{2}$$

such that, by substituting (2) into (1) we obtain

$$C + D + aA^t(\neg B^t) + aA^tB^t = 1 \tag{3}$$

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,

$$C_1 + D_1 + a_1A^t = 1 \qquad [\times(\neg A^t)] \tag{4}$$

$$C_2 + D_2 + a_2(\neg A^t) = 1 \qquad [\times A^t] \tag{5}$$

such that, by multiplying (4) by $(\neg A^t)$ and (5) by A^t and adding both equations we obtain:

$$(\neg A^t)C_1 + (\neg A^t)D_1 + A^tC_2 + A^tD_2 = (\neg A^t) + A^t = 1 \tag{6}$$

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

Theorem 4. *The labelled 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 1.

The labelled 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.

Comparing the entailment multipliers presented here for boolean algebras with those presented for boolean rings in [8], we can say that the multipliers for boolean algebras are always smaller than or equal. In fact, the multipliers for all structural rules and those for rules $(\vdash \wedge), (\vee \vdash)$ and $(\to\vdash)$ are exactly the same, and the multipliers for rules $(\wedge vdash), (\vdash \vee)$ and $(\vdash\to)$ are smaller than those for boolean rings. Furthermore, as example 12 illustrated, the multipliers for boolean algebras presented here can be simplified in some cases, which makes those multipliers even smaller.

5 Conclusion

Entailment multipliers are a characterisation of validity for many valued propositional logics. Classical logic is a special case of interest, for which the presence of entailment multipliers was shown both for boolean rings and boolean algebras. Entailment multipliers can be applied as a proof invariants over inference systems, which allows for the computation of multipliers in parallel with a proof-construction.

The existence of entailment multipliers for modal logics via boolean algebras with operators can be developed in total analogy to the exposition made for boolean rings with operators in [8].

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 and 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] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] Marcelo Finger and Mauricio S. C. Hernandes. Entailment multipliers: An algebraic characterization of validity for classical and modal logics. In Anuj Dawar and Ruy J. G. B. de Queiroz, editors, *WoLLIC*, volume 6188 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2010.

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

[10] Nathan Jacobson. *Basic Algebra I.* Dover Publications, New York, 2009.

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

[12] 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.