Ludwig-Maximilians-Universität München
Institut für Informatik

Bachelor Thesis

Unification of Boolean Differential Rings Is Unitary

Fabian Lukas Grubmüller

10 september 2024

Supervisor: Felix Weitkämper DPhil (Oxon)

Abstract

The theory of Boolean differential rings is a natural extension of the theory of Boolean rings, that additionaly provides an abstract notion of differential. Boolean rings are important and extensively studied concepts arising naturally in many parts of mathematics, especially logic, and computer science. One important result is that the theory of Boolean rings has the unitary unification type. We show that the unification of Boolean differential rings can be reduced to the unification of Boolean rings and that the theory of Boolean differential rings also has the unitary unification type, and we provide an algorithm that calculates a most general unifier. We also show that terms of Boolean differential rings have a flat normal form similar to the polynomial form of terms of Boolean rings and that terms of Boolean differential rings correspond to terms of Boolean rings in a way that respects both equivalences.

Contents

This document was typeset using typst 0.14.0.

Introduction

Boolean algebras are important mathematical structures that appear in many different parts of mathematics, in particular logic, and theoretical computer science. They can be equivalently characterized in the language of algebra as Boolean rings, which enables us to use the more familiar definitions and techniques of ring theory.

One of the most important classes of Boolean algebras are the switching algebras $\mathbb{S}_n$, i.e. the sets of Boolean functions $\mathbb{2}^n \to \mathbb{2}$ for $n \in \mathbb{N}$, that inherit their algebraic properties from $\mathbb{2}$ which is isomorphic to the two-element field. Switching algebras arise naturally in computer science as they represent logical circuits. Because of their importance, Switching functions in particular, as well as Boolean algebras and Boolean rings in general, have been extensively studied.

A natural question that comes up when dealing with switching function is in which sense some Boolean functions are independent from some of the input variables. E.g. the function $f(x_1, x_2) \coloneqq x_1$ is clearly independent from x_2. There are, however, less obvious examples like the function $g(x_1, x_2) \coloneqq x_1 \vee (x_2 \wedge \neg x_2)$ which is essentially the function f, but in order to check whether g depends on x_2 one already needs to know Boolean arithmetic to see that $x_2 \wedge \neg x_2 = 0$ and therefore $x_1 \vee 0 = x_1$.

A different angle on this question is to study whether the function value changes if the input variables of interest are changed, i.e. whether $f(x_1, x_2)$ has the same value as $f(x_1, \neg x_2)$ and similarly for g. The language of Boolean differential algebras and Boolean differential rings provides us with a way of talking about this question, and it leads to a fruitful field of study that stands at the center of this thesis. The word *differential* is a reference to the same concept in $\mathbb{R}$, that also answers the question in which way a real-valued function depends on the input variables.

An extensive study of the switching algebras and the concept of differential on them has been covered in B. Steinbach and C. Posthoff [1] and particularly in B. Steinbach and C. Posthoff [2]. Here, the authors introduce the notions of simple and vectorial derivatives and extensively study the behaviour of these derivatives. Following F. Weitkämper [3], in this thesis we will study arbitary Boolean differential rings.

Unification is a way of abstractly solving equations w. r. t. some theory. The difference to ordinary equation solving is that rather than plugging in values into variables, we instead replace variables with other terms such that the terms (and not a priori the values) are equal w. r. t. some theory. It has been shown that the unification theory of Boolean rings is particularly simple in that it is *unitary*. Unitary means that every unifiable system of equations has some unifier that is most general, i. e. it generates all possible solutions.

In this thesis, we will show that we can reduce the unification theory of Boolean differential rings to the unification theory of Boolean rings and we prove that the unification theory of Boolean differential rings is unitary as well. We will also provide a unification algorithm for single as well as systems of equations of Boolean differential rings.

The algorithms in this work are given in pseudocode. The style of the code is inspired by the one used by U. Martin and T. Nipkow [4] for specifying the unification algorithm for Boolean rings. In order to avoid many nested **if** statements, we use a **match** statement as found in many programming languages, especially functional ones, where the individual cases follow the syntax $S \Rightarrow T$, where S is a constructor, in our cases mostly x or $\delta(x)$ involving variables, as well as $S_1 + S_2$, $S_1 \cdot S_2$ as well as $\delta(S)$ for sums and product as well as terms enclosed by δ.

In Section 1, we will introduce the important prerequisites for the later study. In Section 1.1, we will provide the basic logical definitions and in Section 1.2 we will introduce the concept of unification. In Section 1.3, we will introduce the theory of Boolean rings, in Section 1.4 the polynomial normal form of terms of Boolean rings and lastly in Section 1.5 we will provide the most important results regarding the unification of Boolean rings.

In Section 2, we will give show the results of our study of Boolean differential rings. In Section 2.1, we will first introduce the theory of Boolean differential rings and explain why the switching algebras constitute Boolean differential rings. In Section 2.2, we will introduce the flat normal form of terms of Boolean differential rings and prove some statements about it. In Section 2.3, we will show a way of translating terms of Boolean differential rings into terms of Boolean rings in a way that respects both equalities. Here we will also prove that the flat normal form has in fact similar properties to the polynomial normal form of Boolean rings. In Section 2.4 we will introduce some important lemmas which leads us to the final Section 2.5 in which we will state and prove our main theorems regarding the unification of Boolean differential rings. Here we will also specify a unification algorithm for single equations and systems of equations of Boolean differential rings.

1 Basic Notions

1.1 Terms, Theories and Models

In the following section, we will introduce the basic definitions of mathematical logic as can be found in H.-D. Ebbinghaus, J. Flum, and W. Thomas [5] or most other introductory books on logic. We will, however, limit ourselves to present only the parts that are relevant to the later work and make slight adjustments to definitions and notation to better suit our needs and cater to our (personal) aesthetic preferences.

DEFINITION 1. In logic, a language $\mathcal{L}$ is a tuple (F, P) where F is a set of function symbols and P is a set of predicate symbols. $\mathcal{L}$ is also equipped with a countable set $\mathcal{V} = \{x_i \mid i \in \mathbb{N}\}$ of variables, that is disjoint from F and P.

Even though $\mathcal{V}$ contains only the symbols x_i, we will also use variable names like a_i and b_i for the sake of clarity. In this case, we will simplyl view a_i or b_i as an abbreviation for an actual variable $x_j \in \mathcal{V}$ for some $j \in \mathbb{N}$ and generally assume that all the a_i as well as all the b_i are distinct.

A central notion in this thesis is the one of a *term* over $\mathcal{L}$, also called $\mathcal{L}$*-term*. The set $\mathcal{T}$ of terms over $\mathcal{L}$ is defined inductively:

DEFINITION 2. Every 0-ary function symbol of F and every element of $\mathcal{V}$ is an $\mathcal{L}$-term. For every k-ary function symbol $f \in F$, and all $\mathcal{L}$-terms $t_1, \ldots, t_k$, the expression $f(t_1, \ldots, t_k)$ is also an $\mathcal{L}$-term. In this case we say that $t_1, \ldots, t_k$ are proper subterms of $f(t_1, \ldots, t_k)$ and $f(t_1, \ldots, t_k)$ is a proper superterm of $t_1, \ldots, t_k$. An $\mathcal{L}$-term s is a subterm (resp. superterm) of an $\mathcal{L}$-tem t if it is either a proper subterm (resp. superterm), or $s = t$. If a term t contains at most the variables $\vec{x} := (x_1, \ldots, x_n)$ for some $n \in \mathbb{N}$, then we say that t is a term of $\vec{x}$ and write $t(\vec{x})$.

Note that $\mathcal{T}$ is always at least countably infinite, since there are countably infinitely many variables. It is exactly countably infinite if F and P are at most countable. The set $\mathcal{F}$ of

$\mathcal{L}$-formulas can be defined inductively in a similar fashion using the predicate symbols (plus a special binary relation "=") as well as the previously defined terms:

DEFINITION 3. If p is a k-ary prediacte of P and $t_1, \ldots, t_k$ are $\mathcal{L}$-terms, then $p(t_1, \ldots, t_k)$ is an $\mathcal{L}$-formula. Similarly, if s and t are $\mathcal{L}$-terms, then $s = t$ is a $\mathcal{L}$-formula. Finally, every first-order formula built from these atomic $\mathcal{L}$-formulas is an $\mathcal{L}$-formula.

Similarly to $\mathcal{T}$, $\mathcal{F}$ is always at least countably infinite and exactly countably infinite if F and P are at most countable. Next, we will introduce some notions of proof and model theory:

DEFINITION 4. An $\mathcal{L}$-theory T is a set of $\mathcal{L}$-formulas (called *axioms*). If Φ is a formula, then we say that T proves Φ, denoted $T \vdash \Phi$, iff there exists a finite subset $T' := \{\Psi_1, \ldots, \Psi_n\} \subseteq T$ such that there is a finite derivation proving Φ from T'. For terms s and t, we write $s \overset{T}{=} t$ to mean $T \vdash s = t$.

DEFINITION 5. Let T be an $\mathcal{L}$-theory. A set $\mathcal{M}$ is called a model of T, denoted $\mathcal{M} \vDash T$, if there is an interpretation of $\mathcal{F}$ and $\mathcal{P}$ within $\mathcal{M}$, and for every formula of T, its interpretation in $\mathcal{M}$ is true. If t is an $\mathcal{L}$-term of $\vec{x} \in \mathcal{V}^n$ and $\vec{X} \in \mathcal{M}^n$, then we denote by $t\langle\langle\vec{X}\rangle\rangle$ the interpretation of t in $\mathcal{M}$ with X_i plugged into all occurences of x_i, for all $0 < i \leq n$.

The following theorem is an important result of logic. It states that the above notions of deductive provability and model-theoretic truth are equivalent.

THEOREM 6 (Soundness and Completeness [5, Thm. IV.6.2, V.4.1])**.** It holds that $T \vdash \Phi$ if and only if for all models $\mathcal{M}$ of T it is true that $\mathcal{M} \vDash \Phi$.

1.2 Unification

The above notion of evaluating terms at (i. e. "plugging in") elements of $\mathcal{M}$ has a syntactic-deductive analogon. With substitution, the difference is that variables are evaluated at, or in this case replaced by, other terms instead of directly by elements of $\mathcal{M}$. This makes sense, since these new terms in turn correspond to elements in models and T-equality is preserved as shown in Lemma 8. In the following, we will vaguely follow F. Baader and T. Nipkow [6], but we will, again, simplify or modify definitions and notation to better suit our needs.

DEFINITION 7. Let $\sigma : \mathcal{V} \to \mathcal{T}$ be a function. We can recursively extend σ to a function $\bar{\sigma} : \mathcal{T} \to \mathcal{T}$: If $c \in F$ is 0-ary, then $\bar{\sigma}(c) := c$. If $x \in \mathcal{V}$, then $\bar{\sigma}(x) := \sigma(x)$.

If $f \in F$ is k-ary for some $k \in \mathbb{N}$ and $t_1, ..., t_k$ are $\mathcal{L}$-terms, then $\bar{\sigma}(f(t_1, ..., t_k)) \coloneqq f(\bar{\sigma}(t_1), ..., \bar{\sigma}(t_k))$. In this case, we call σ an $\mathcal{L}$-substitution and for the sake of clarity, we denote the application of σ on a term t by ${}_\sigma[t] \coloneqq \sigma(t)$.

In this thesis, we will not distinguish $\bar{\sigma}$ from σ and, in particular, we will define a substitution simply by specifying its values on $\mathcal{V}$. Similarly, if σ is defined on a subset $X \subseteq \mathcal{V}$, then we can extend it to the whole of $\mathcal{V}$ by letting $\sigma(x) \coloneqq x$ for $x \in \mathcal{V} \setminus X$.

In the rest of this thesis, we will often specify a substitution (function) σ by providing a set of ordered pairs $\mathcal{V} \times \mathcal{T}$, where a single ordered pair (x, t) means that $\sigma(x) = t$. For the sake of clarity, we will use the special notation $x \mapsto t$ for (x, t), which means that e. g. the set $\{x_1 \mapsto t_1, x_2 \mapsto t_2\}$ will correspond to the substitution sending x_1 to the term t_1 as well as x_2 to t_2, and $\{x_i \mapsto t_i \mid 0 < i \leq n\}$ to the substitution sending every variable $x_i, 0 < i \leq n$, to the term t_i. As before, we assume that both of the substitutions act like the identity on all of the variables that have not been mentioned explicitly.

If $\mathcal{K} \subseteq \mathcal{L}$ is another language and σ is a $\mathcal{K}$-substitution, we can also see σ as an $\mathcal{L}$-substitution. We will use this fact without explicit mention in the case for $\mathcal{L}_{\mathrm{BR}} \subseteq \mathcal{L}_{\mathrm{BDR}}$ later on in this work.

Next, we will show that substitutions do, in fact, preserve T-equalities.

LEMMA 8. Let s and t be $\mathcal{L}$-terms over $\mathcal{L}$ with $s \overset{T}{=} t$ and σ an $\mathcal{L}$-substitution. Then it holds that ${}_\sigma[s] \overset{T}{=} {}_\sigma[t]$.

PROOF. To show that ${}_\sigma[s] \overset{T}{=} {}_\sigma[t]$, let $\mathcal{M}$ be any model of T. Assume that s and t are $\mathcal{L}$-terms of $\vec{x} \in \mathcal{V}^n$ and ${}_\sigma[s]$ as well as ${}_\sigma[t]$ are terms of $\vec{y} \in \mathcal{V}^m$, $\vec{x}$ and $\vec{y}$ not necessarily disjoint. Let $\vec{Y} \in \mathcal{M}^m$. We need to show that ${}_\sigma[s]\langle\!\langle \vec{Y} \rangle\!\rangle = {}_\sigma[t]\langle\!\langle \vec{Y} \rangle\!\rangle$. For that, define $\overrightarrow{W} \coloneqq (W_1, ..., W_n) \in \mathcal{M}^n$ by $W_i \coloneqq {}_\sigma[x_i]\langle\!\langle \vec{Y} \rangle\!\rangle$ for $0 < i \leq n$. For all $\mathcal{L}$-terms u it holds that ${}_\sigma[u]\langle\!\langle \vec{Y} \rangle\!\rangle = u\langle\!\langle \overrightarrow{W} \rangle\!\rangle$. We prove this by induction: For 0-ary $f \in \mathcal{F}$, it holds that ${}_\sigma[f]\langle\!\langle \vec{Y} \rangle\!\rangle = f = f\langle\!\langle \overrightarrow{W} \rangle\!\rangle$. For $0 < i \leq n$ it holds that ${}_\sigma[x_i]\langle\!\langle \vec{Y} \rangle\!\rangle = W_i = x_i\langle\!\langle \overrightarrow{W} \rangle\!\rangle$. Finally, if $f \in \mathcal{F}$ is k-ary and the hypothesis holds for the $\mathcal{L}$-terms $t_1, ..., t_k$, then

$$\begin{aligned}
{}_\sigma[f(t_1, ..., t_k)]\langle\!\langle \vec{Y} \rangle\!\rangle &= f({}_\sigma[t_1], ..., {}_\sigma[t_k])\langle\!\langle \vec{Y} \rangle\!\rangle \\
&= f\Big({}_\sigma[t_1]\langle\!\langle \vec{Y} \rangle\!\rangle, ..., {}_\sigma[t_k]\langle\!\langle \vec{Y} \rangle\!\rangle\Big) \\
&= f\Big(t_1\langle\!\langle \overrightarrow{W} \rangle\!\rangle, ..., t_k\langle\!\langle \overrightarrow{W} \rangle\!\rangle\Big) \\
&= f(t_1, ..., t_k)\langle\!\langle \overrightarrow{W} \rangle\!\rangle
\end{aligned}$$

Together, this shows that it holds for all terms u. Then, using this as well as the fact that $s \overset{T}{=} t$ and therefore $s\langle\langle\vec{X}\rangle\rangle = t\langle\langle\vec{X}\rangle\rangle$ for all $\vec{X} \in \mathcal{M}^n$, we have that

$$ {}_\sigma[s]\langle\langle\vec{Y}\rangle\rangle = s\langle\langle\overrightarrow{W}\rangle\rangle = t\langle\langle\overrightarrow{W}\rangle\rangle = {}_\sigma[t]\langle\langle\vec{Y}\rangle\rangle $$

Since this holds for all models $\mathcal{M}$, we have that ${}_\sigma[s] \overset{T}{=} {}_\sigma[t]$. ∎

In the following, we will make some more general definitions regarding substitutions.

DEFINITION 9. Let σ and τ be $\mathcal{L}$-substitutions. Then the composition $\sigma\tau := \sigma \circ \tau$ is simply the function composition, i. e. for all $x \in \mathcal{V}$ we have that ${}_{\sigma\tau}[x] := {}_\sigma[{}_\tau[x]]$.

DEFINITION 10. Let σ and τ be $\mathcal{L}$-substitutions. We say that σ and τ are T-equal, denoted $\sigma \overset{T}{=} \tau$, iff for all $x \in \mathcal{V}$ it holds that ${}_\sigma[x] \overset{T}{=} {}_\tau[x]$. In this case it is clear that for all $\mathcal{L}$-terms t it holds that ${}_\sigma[t] \overset{T}{=} {}_\tau[t]$.

This allows us to define a notion of *generality* between substitutions. A substitution is more general if the other substitution is simply a specialization of it.

DEFINITION 11. Let T be an $\mathcal{L}$-theory. Then we define the partial order $\overset{T}{\leq}$ by letting $\sigma \overset{T}{\leq} \tau$, for all $\mathcal{L}$-substitutions σ and τ, if and only if there exists an $\mathcal{L}$-substitution ϑ such that $\tau \overset{T}{=} \vartheta\sigma$. In this case we say that σ is at least as general as τ and we will usually just write $\leq$ instead of $\overset{T}{\leq}$ if the theory is clear from the context. It is easy to verify that $\leq$ is in fact a preorder on the set of $\mathcal{L}$-substitutions.

We now have all the necessary definitions to define the central subject of this thesis, unification theory. (Equational) unification is a technique of solving equations both syntactically and w. r. t. a theory. In a way, unification in relation to finding solutions of an equation is what substitution is in relation to "plugging in" values.

DEFINITION 12. Let $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$ be $\mathcal{L}$-terms. A substitution σ is a T-unifier of the finite system of equations $\{s_1 = t_1, \ldots, s_n = t_n\}$, called a *$T$-unification problem*, if and only if ${}_\sigma[s_i] \overset{T}{=} {}_\sigma[t_i]$ for all $0 < i \leq n$. We say that a system of equations E is T-unifiable if and only if there is a T-unifier of E. If s and t are terms, we will often simply write $s = t$ instead of the singleton set $\{s = t\}$.

Unification can also be done purely syntactically. In this case, the equations ${}_\sigma[s_i] \overset{T}{=} {}_\sigma[t_i]$ in Definition 12 would be replaced by the syntactic equations ${}_\sigma[s_i] = {}_\sigma[t_i]$. In the following, however, "unification" will always mean "equational unification" in the sense of Definition 12.

Suppose that s and t are $\mathcal{L}$-terms and σ is a T-unifier of $s = t$ with ${}_\sigma[s]$ and ${}_\sigma[t]$ being terms of $\vec{x}$. If $\mathcal{M}$ is a model of T, then we have, for all $\vec{X} \in \mathcal{M}^n$, that ${}_\sigma[s]\langle\langle \vec{X} \rangle\rangle = {}_\sigma[t]\langle\langle \vec{X} \rangle\rangle$ and therefore unification constitutes a powerful method of generating concrete solutions of equations or showing that a given set of equations does not have any solution otherwise. It is now clear to see that unifiers that are more general substitutions will also generate more general concrete solutions. Due to this observation, it is in our interest to characterize the unifiers that are the most general.

DEFINITION 13 ([6, Def. 10.1.4])**.** Let T be an $\mathcal{L}$-theory and E a finite system of $\mathcal{L}$-equations. A set Ω of T-unifiers of E is minimal complete (mcsu), if for all T-unifiers τ of E, there is a $\sigma \in \Omega$ such that $\sigma \leq \tau$, and for all $\sigma, \sigma' \in \Omega$, if $\sigma \leq \sigma'$, then $\sigma = \sigma'$. If $|\Omega| = 1$, then we call $\sigma \in \Omega$ a most general T-unifier (mgu) of E.

Note that $\varnothing$ is an mcsu if and only if E is not unifiable. Moreover, in general, mcsu, and, in particular, mgu are not unique, but they can be transformed into each other w. r. t. T.

An mcsu allows us to generate all possible solutions for a system of equations with as few unifiers as possible. Larger mcsu intuitively mean that finding solutions is more difficult. It turns out that we can classify theories by how complex, or rather by how large, their mcsu can be.

DEFINITION 14 ([6, Def. 10.1.7])**.** Let T be an $\mathcal{L}$-theory. T can have the following unification types:

(i) *unitary*: If and only if every system of equations has a T-mcsu of cardinality ≤ 1, i. e. a T-mgu in case it is T-unifiable.
(ii) *finitary*: If and only if every system of equations has a finite T-mcsu.
(iii) *infinitary*: If and only if every system of equation has a T-mcsu and there is some system of equations that has an infinite T-mcsu.
(iv) *zero*: If there is a system of equations that does not have a T-mcsu.

It turns out that many theories are actually unitary, or at least finitary. In particular, it holds that the theory of Boolean rings and Boolean algebras is unitary. It is the aim of this thesis to show that the theory of Boolean differential rings and Boolean differential algebras is unitary as well.

The next theorem states that if every single equation has an mcsu of size ≤ 1, then every (finite) system of equations has an mcsu of size ≤ 1, i. e. the theory is unitary. This allows us later to deduce the unification type while only ever having to deal with single equations.

THEOREM 15. Let T be an $\mathcal{L}$-theory such that for all L-terms s and t the statement

$\Psi(s,t) \coloneqq$ either the equation $s = t$ has a T-mgu or it is not T-unifiable

holds. Then T is unitary.

PROOF. Suppose that $E \coloneqq \{s_1 = t_1, \ldots, s_n = t_n\}$ is T-unifiable by some ϑ. We want to show that E has a T-mgu. To show that, define $\tau_0 \coloneqq \mathrm{id}$. We will prove by induction that for every $0 < k \leq n$ the $\tau_k \coloneqq \sigma_k \tau_{k-1}$ where σ_k is a T-mgu of ${}_{\tau_{k-1}}[s_k] = {}_{\tau_{k-1}}[t_k]$ is well-defined and that τ_k is a T-mgu of $E_k \coloneqq \{s_1 = t_1, \ldots, s_k = t_k\}$.

The case for $k = 1$ is trivial: Since ${}_{\vartheta}[s_1] \overset{T}{=} {}_{\vartheta}[t_1]$, this means that $s_1 = t_1$ is T-unifiable and by $\Psi(s_1, t_1)$ this means that there exists a T-mgu σ_1 of

$$ {}_{\tau_0}[s_1] = s_1 = t_1 = {}_{\tau_0}[t_1] $$

and $\tau_1 \coloneqq \sigma_1 \tau_0 = \sigma_1$ is by definition a T-mgu of E_1.

Now suppose that the induction hypothesis holds for some $0 < k < n$. Since ϑ is a T-unifier of E, it is also a T-unifier of E_k and therefore there is some substitution φ such that $\vartheta \overset{T}{=} \varphi\tau_k$. Since ϑ is a T-unifier of $s_{k+1} = t_{k+1}$, it holds that

$$ \varphi[{}_{\tau_k}[s_{k+1}]] = {}_{\vartheta}[s_{k+1}] \overset{T}{=} {}_{\vartheta}[t_{k+1}] = \varphi[{}_{\tau_k}[t_{k+1}]] $$

which means that ${}_{\tau_k}[s_{k+1}] = {}_{\tau_k}[t_{k+1}]$ is T-unifiable. By $\Psi({}_{\tau_k}[s_{k+1}], {}_{\tau_k}[t_{k+1}])$, this means that there exists a T-mgu σ_{k+1} of this equation. This lets us define $\tau_{k+1} \coloneqq \sigma_{k+1}\tau_k$. Clearly by construction, τ_{k+1} is a T-unifier of E_{k+1}. It remains to show that is also most general.

To show this, suppose that $\tilde{\vartheta}$ is another T-unifier of E_{k+1}. Since it is also a T-unifier of E_k, there exists some substitution $\tilde{\varphi}$ such that $\tilde{\vartheta} \overset{T}{=} \tilde{\varphi}\tau_k$. Since

$$ \tilde{\varphi}[{}_{\tau_k}[s_{k+1}]] = {}_{\tilde{\vartheta}}[s_{k+1}] \overset{T}{=} {}_{\tilde{\vartheta}}[t_{k+1}] = \tilde{\varphi}[{}_{\tau_k}[t_{k+1}]] $$

and σ_{k+1} is most general for the equation ${}_{\tau_k}[s_{k+1}] = {}_{\tau_k}[t_{k+1}]$, it holds that there exists some substitution $\tilde{\psi}$ such that $\tilde{\varphi} \overset{T}{=} \tilde{\psi}\sigma_{k+1}$. Together we have that

$$ \tilde{\vartheta} \overset{T}{=} \tilde{\varphi}\tau_k \overset{T}{=} \tilde{\psi}\sigma_{k+1}\tau_k = \tilde{\psi}\tau_{k+1} $$

i.e. τ_{k+1} is most general.

By induction, it follows that for all $0 < k \leq n$ the substitution τ_k is a T-mgu of E_k. In particular, τ_n is a T-mgu of $E_n = E$, which concludes the proof. ∎

The proof of Theorem 15 suggests a way of specifying an algorithm for finding the mgu of a system of equations given an algorithm for finding the mgu of a single equation.

ALGORITHM 16. Let T be a unitary $\mathcal{L}$-theory and unify_T a function, specified, for all $\mathcal{L}$-terms s and t, by a finitary algorithm, with $\mathrm{unify}_T(s = t)$ either a T-mgu of $s = t$

in case the equation is T-unifable and $\bot$ in case the equation is not T-unifiable. We will recursively specify the function unify_T^n for all $n \in \mathbb{N}, 1 \leq n$, that calculates the T-mgu of the system of $\mathcal{L}$-equations $\{s_1 = t_1, \ldots, s_n = t_n\}$ in case it is T-unifiable, and returns $\bot$ in case it is not T-unifiable. For the base case we define $\mathrm{unify}_T^1 := \mathrm{unify}_T$. For the recursive case, suppose unify_T^n has already been defined for some $n \in \mathbb{N}, 1 \leq n$. Let $s_1, \ldots, s_{n+1}$ as well as $t_1, \ldots, t_{n+1}$ be $\mathcal{L}$-terms. We specify unify_T^{n+1} by the following algorithm:

$$
\begin{array}{l}
\mathrm{unify}_T^{n+1}(s_1 = t_1, \ldots, s_{n+1} = t_{n+1}) := \\
\quad \textbf{let } \tau_n := \mathrm{unify}_T^n(s_1 = t_1, \ldots, s_n = t_n) \\
\quad \textbf{in if } \tau_n = \bot \\
\quad\quad \textbf{then } \bot \\
\quad\quad \textbf{else let } \sigma_{n+1} := \mathrm{unify}_T({}_{\tau_n}[s_{n+1}] = {}_{\tau_n}[t_{n+1}]) \\
\quad\quad\quad \textbf{in if } \sigma_{n+1} = \bot \\
\quad\quad\quad\quad \textbf{then } \bot \\
\quad\quad\quad\quad \textbf{else } \sigma_{n+1}\tau_n
\end{array}
$$

The correctness of Algorithm 16 follows from the induction part of the proof of Theorem 15.

1.3 Boolean Rings and Algebras

We will now proceed to define Boolean rings and Boolean algebras. Boolean algebras are important structures present in many parts of mathematics and computer science. The notion of Boolean rings is equivalent to that of Boolean algebras, in the sense that every Boolean ring can be equipped with a Boolean algebra structure and vice versa. While the notion of Boolean algebras is convient to work with in set theory and some other fields, using the notion of Boolean rings allows us to talk about algebraic properties using notations and techniques from algebra. We will generally follow F. Baader and T. Nipkow [6, Sec. 10.4], but will adapt it to better suit our needs.

DEFINITION 17. The language $\mathcal{L}_{\mathrm{BR}}$ of Boolean rings consists of the 0-ary function symbols "0" and "1", as well as the binary function symbols "+" and "·". As usual, we will write $a + b$ instead of $+(a, b)$, $a \cdot b$ or simply ab instead of $\cdot(a, b)$ and we will use the usual rules of precedence in order to avoid parentheses. The theory T_{BR} consists of the following axioms:

(i) $\forall_{a,b,c}((a+b)+c=a+(b+c))$
(ii) $\forall_{a,b,c}((a\cdot b)\cdot c=a\cdot(b\cdot c))$
(iii) $\forall_a(0+a=a)$
(iv) $\forall_a(1\cdot a=a)$
(v) $\forall_a(a+a=0)$
(vi) $\forall_a(a\cdot a=a)$
(vii) $\forall_{a,b}(a+b=b+a)$
(viii) $\forall_{a,b}(a\cdot b=b\cdot a)$
(ix) $\forall_{a,b,c}(a\cdot(b+c)=a\cdot b+a\cdot c)$
(x) $\forall_a(0\cdot a=0)$

We will use these axioms in the rest of the work without explicitly mentioning them. For the sake of convenience, we will use "BR" to refer to both $\mathcal{L}_{\mathrm{BR}}$ and T_{BR}. E.g. we will say that $s \overset{\mathrm{BR}}{=} t$, $\mathrm{BR} \vdash \Phi$ and write "BR-term". Furthermore, in anticipation of Boolean differential rings later, we will avoid using the variable name z. The equalities in the next Lemma follow immediately from BR, and will be used extensively in this thesis:

LEMMA 18.
(i) For all x it holds that $x\cdot(x+1)=0$
(ii) For all x and y it holds that $x=y$ if and only if $x+y=0$.

PROOF. It holds that $x\cdot(x+1)=x\cdot x+x\cdot 1=x+1\cdot x=x+x=0$. If $x=y$, then $x+y=x+x=0$. If conversely $x+y=0$, then

$$x=x+(y+y)=(x+y)+y=0+y=y$$

which concludes the proof. ∎

Next, we define Boolean algebras using the characterization of Boolean rings.

DEFINITION 19. The language $\mathcal{L}_{\mathrm{BA}}$ of Boolean algebras consists of the 0-ary function symbols "0" and "1", as well as the unary function symbol "$\neg$" and the binary function symbols "$\wedge$" as well as "$\vee$". The theory T_{BA} consists of the axioms of T_{BR}, with the following replacements applied for all $\mathcal{L}_{\mathrm{BR}}$-terms s and t [6, Sec. 10.4]:

$$s+t \overset{\mathrm{BA}}{\mapsto} (s\wedge\neg t)\vee(\neg s\wedge t) \qquad s\cdot t \overset{\mathrm{BA}}{\mapsto} s\wedge t$$

This gives the usual definition of a Boolean algebra. The following proposition supports our claim that T_{BA} and T_{BR} are merely two different but interchangeable ways to talk about the same objects.

PROPOSITION 20.
(i) Every model of T_{BA} is a model of T_{BR} with the substitutions $\overset{\mathrm{BA}}{\mapsto}$ above.
(ii) Every model of T_{BR} is a model of T_{BA} with the following substitutions, defined for all $\mathcal{L}_{\mathrm{BA}}$-terms s and t:

$$\neg s \overset{\text{BR}}{\mapsto} s + 1 \qquad s \wedge t \overset{\text{BR}}{\mapsto} s \cdot t \qquad s \vee t \overset{\text{BR}}{\mapsto} s + t + s \cdot t$$

PROOF. Part (i) is clear from the definition of T_{BA}. For part (ii), it suffices to see that $s \cdot t \overset{\text{BA}}{\mapsto} s \wedge t \overset{\text{BR}}{\mapsto} s \cdot t$ as well as

$$\begin{aligned}
s + t &\overset{\text{BA}}{\mapsto} (s \wedge \neg t) \vee (\neg s \wedge t) \\
&\overset{\text{BR}}{\mapsto} (s \cdot (t + 1)) + ((s + 1) \cdot t) + (s \cdot (t + 1))((s + 1) \cdot t) \\
&\overset{\text{BR}}{=} (st + s) + (st + t) + (st + s)(st + t) \\
&\overset{\text{BR}}{=} (st + s) + (st + t) + (stst + stt + sst + st) \\
&\overset{\text{BR}}{=} (st + s) + (st + t) + (st + st + st + st) \\
&\overset{\text{BR}}{=} (st + st) + (s + t) + 0 \\
&\overset{\text{BR}}{=} s + t
\end{aligned}$$

since T_{BR} consists of the axioms of T_{BA} with the replacements $\overset{\text{BR}}{\mapsto}$, which in turn consists of the axioms of T_{BR} with the replacements $\overset{\text{BA}}{\mapsto}$. ∎

We call the models of T_{BR} *Boolean rings* and the models of T_{BA} *Boolean algebras*. In the following, we will introduce some important examples of Boolean algebras/Boolean rings.

Propositional logic. One of the arguably most important examples of a Boolean algebra is $\mathbb{2}$, the set $\{0, 1\}$ interpreted as truth values and equipped with "$\neg$", "$\wedge$" and "$\vee$" corresponding to the logical negation, conjunction and disjunction. $\mathbb{2}$ is a Boolean ring where "$\cdot$" is the logical conjunction and "$+$" is the logical operation XOR. Incidentally, $\mathbb{2}$ is isomorphic to the field $\mathbb{F}_2$. The importance of $\mathbb{2}$ as the basic Boolean algebra stems from the following theorem. It is even reflected by our choice of symbols of $\mathcal{L}_{\text{BA}}$.

THEOREM 21 ([6, Thm. 10.4.3]). Let S and T be BR-terms. Then it holds that $S \overset{\text{BR}}{=} T$ if and only if $\mathbb{2} \vDash S = T$.

Powersets. Another important example of Boolean algebras is the one of the powersets. If x is some set, then $\mathcal{P}(x)$, the powerset of x, is a Boolean algebra with "$\neg$", "$\wedge$" and "$\vee$" being the set-theoretic complement (in x), intersection and union, i. e. for all $y \subseteq x$ and $z \subseteq x$, it holds that

$$\neg y = x \setminus y \qquad y \wedge z = y \cap z \qquad y \vee z = y \cup z$$

As a Boolean ring, "+" and "·" correspond to the set-theoretic symmetric difference and union. Powersets are important, since, by Stone's Theorem [1, Thm. 3.12], every finite Boolean algebra is isomorphic to $\mathcal{P}(x)$ for some set x. Therefore all finite Boolean algebras have cardinality 2^n for some $n \in \mathbb{N}$. E.g. $\mathbb{2}$ is isomorphic to $\mathcal{P}(\varnothing) = \{\varnothing, \{\varnothing\}\}$.

Algebras over $\mathbb{F}_2$. Every commutative algebra over $\mathbb{F}_2$ already directly fulfils most of the axioms, namely the ones that are related to commutativity, associativity and distributivity hold, as well as the roles of 0 and 1. Additionally, it holds that

$$x + x = 1_{\mathbb{F}_2} x + 1_{\mathbb{F}_2} x = \left(1_{\mathbb{F}_2} + 1_{\mathbb{F}_2}\right) x = 0_{\mathbb{F}_2} x = 0$$

However, the last axiom, $x \cdot x = x$, does not necessarily hold in all commutative algebras over $\mathbb{F}_2$, since e.g. in $\mathbb{F}_2[X]$, it holds that $X \cdot X = X^2 \neq X$.

An example for where it holds is the $\mathbb{F}_2$-algebra $(\mathbb{F}_2)^X$ of all the functions from X to $\mathbb{F}_2$, for any set X. The ring structure is trivially defined by

$$(f + g)(x) \coloneqq f(x) + g(x) \qquad (f \cdot g)(x) \coloneqq f(x) \cdot g(x)$$

as well as $0(x) \coloneqq 0$ and $1(x) \coloneqq 1$, and the scalar multiplication is given in the obvious way by $(\lambda f)(x) \coloneqq \lambda f(x)$, for all $f, g \in (\mathbb{F}_2)^X$ and $x \in X$. Clearly it also holds that $f \cdot f = f$, since for all $x \in X$, we have that $(f \cdot f)(x) = f(x) \cdot f(x) = f(x)$, by application of the same axiom inside $\mathbb{F}_2$. Therefore, $(\mathbb{F}_2)^X$ is a Boolean ring.

An important instance of this are the finite Boolean functions. By the previous argument, for every $n \in \mathbb{N}$, the set $\mathbb{S}_n \coloneqq \mathbb{2}^{\mathbb{2}^n}$ of n-dimensional Boolean functions is a Boolean ring. Due to the obvious connection to logic gates, we also call $\mathbb{S}_n$ the n-dimensional switching algebra, and its elements n-dimensional switching functions.

1.4 The Polynomial Form of BR-Terms

As outlined in F. Baader and T. Nipkow [6, Ch. 10.4.1], terms of Boolean rings have a normal form called the *polynomial form*.

DEFINITION 22. The BR-constants 0 and 1, as well as all variables x are BR-atoms. A BR-monomial is a product of BR-atoms, and a BR-polynomial is a sum of BR-monomials.

In order to define the polynomial form of a BR-term, we first need to introduce some definitions.

DEFINITION 23.

(i) Let m_1 and m_2 be BR-monomials. If 0 is contained in either one of the monomials, then we define $m_1 * m_2 \coloneqq 0$. If m_1 and m_2 only contain BR-atoms that are 1, then

we define $m_1 * m_2 = 1$. Otherwise, $m_1 * m_2$ is the monomial $m_1 \cdot m_2$ with all but one of duplicate BR-atoms as well as all occurences of 1 removed.

(ii) Let p_1 and p_2 be BR-polynomials that contain only monomials that are either 0 or a product of pairwise different variables (i. e. reduced in the above sense). Then we define $p_1 \oplus p_2$ to be the sum of monomials $p_1 + p_2$ with all pairs of BR-equal monomials as well as all occurences of 0 removed. If this reduces to the empty sum, we set $p_1 \oplus p_2 := 0$.

(iii) Let p_1 and p_2 be BR-polynomials. If $p_1 = \sum_{i=1}^{k} m_i$ and $p_2 = \sum_{i=1}^{l} n_i$ for BR-monomials $m_1, \ldots, m_k$ and $n_1, \ldots, n_l$. Then we define

$$p_1 \odot p_2 := \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l} m_i * n_j$$

From the definitions and by the axioms of T_{BR}, it is clear that $m_1 * m_2 \overset{\mathrm{BR}}{=} m_1 \cdot m_2$, as well as $p_1 \oplus p_2 \overset{\mathrm{BR}}{=} p_1 + p_2$ and $p_1 \odot p_2 \overset{\mathrm{BR}}{=} p_1 \cdot p_2$. Moreover, $m_1 * m_2 = m_1 \odot m_2$, and $m_1 * m_2$ is clearly a BR-monomial while $p_1 \oplus p_2$ as well as $p_1 \odot p_2$ are clearly BR-polynomials.

This lets us now define the polynomial form $t\!\downarrow$ of a BR-term t.

ALGORITHM 24. Let t be a BR-term. We specify $t\!\downarrow$ recursively as follows:

$$\begin{aligned} t\!\downarrow := \ & \textbf{match } t \\ & \mid \{0, 1, x\} \Rightarrow t \\ & \mid t_1 + t_2 \Rightarrow t_1\!\downarrow \oplus t_2\!\downarrow \\ & \mid t_1 \cdot t_2 \Rightarrow t_1\!\downarrow \odot t_2\!\downarrow \end{aligned}$$

The polynomial form of a BR-term is unique up to permutations of the monomials and the atoms inside the monomials. We can imagine that there is some ordering on the BR-atoms that extends to some lexicographic ordering of monomials. We can assume that the monomials and atoms inside the monomials of $t\!\downarrow$ are ordered in this way. Then the following holds:

THEOREM 25 ([6, Thm. 10.4.3])**.** Let s and t be BR-terms. It holds that $s \overset{\mathrm{BR}}{=} t$ if and only if $s\!\downarrow = t\!\downarrow$.

1.5 Unification of Boolean Rings

Unification of Boolean rings has already been extensively studied. An important result is that the theory of Boolean rings has the unitary unification type. In this part, we will discuss two approach to this problem: Löwenheim's Theorem and a recursive unification algorithm. Löwenheim's Theorem allows us to compute an mgu, if we already have a unifier. This is technically enough to show that unification of Boolean rings is unitary, however, the second approach provides us with a way of explicitly constructing an mgu from scratch.

THEOREM 26 (Löwenheim's Theorem [7])**.** Let s and t be BR-terms over $\vec{x}$. Suppose that τ is a BR-unifier of $s = t$. Then the substitution

$$\sigma := \{x_i \mapsto x_i + (s + t)(x_i +_\tau [x_i]) \mid 0 < i \leq n\}$$

is a BR-mgu of $s = t$.

This allows us to prove the following theorem.

THEOREM 27. Let s and t be BR-terms. Then the equation $s = t$ either has a BR-mgu or it is not R-unifiable.

PROOF. Suppose that $s = t$ is BR-unifiable. This means that there exists a BR-unifier τ of $s = t$. By Theorem 26 there is a BR-mgu σ of $s = t$. This concludes the proof. ∎

Löwenheim's Theorem shows us how to construct an mgu from any unifier. It does not, however, help us to find a unifier in the first place. Checking whether an equation is unifiable and finding an explicit unifier in case it is unifiable is an entirely separate task. E.g. one could first look for a particular solution, i.e. a substitution with $t \in \{0, 1\}$ for every $(x, t) \in \sigma$, of the equation in the model $\mathbb{2}$, which, by Theorem 21, is then also a BR-unifier. Applying Löwenheim's Theorem to this unifier will result in a BR-mgu of the original equation.

In the following we will introduce a recursive algorithm that directly computes the mgu of an equation, if it exists. We will mainly follow the approach of U. Martin and T. Nipkow [4], but adapt it to match our notation. First, we will simplify our problem slightly. By the axioms of BR, it holds that $s \overset{\text{BR}}{=} t$ if and only if $s + t = 0$. Therefore, in the following, we can consider only equations of the form $u = 0$, for some BR-term u, instead. The algorithm is based on the fact that, if t is a term of $\vec{x} = (x_1, \ldots, x_n)$, then the equation $t = 0$ is BR-unifiable if and only if ${}_{\{x_1 \mapsto 0\}}[t] \cdot {}_{\{x_1 \mapsto 1\}}[t] = 0$ is BR-unifiable.

Note that we then interpret ${}_{\{x_1\mapsto 0\}}[t] \cdot {}_{\{x_1\mapsto 1\}}[t]$ as a term of $(x_2, \ldots, x_n)$, which is possible since in both cases, the variable x_1 has been "eliminated" by either 0 or 1.

This fact allows us to successively eliminate variables from t until we reach a closed term that is either 0 or 1. If we reach 1, then the equation is not unifiable, and if we reach 0, then we propagate our solution (in the bottom case this is the identity substitution) back up to the top.

ALGORITHM 28 ([4]). Let s and t be BR-terms in $\vec{x}$. The following algorithm returns a BR-mgu σ of $t = 0$ in case that it is BR-unifiable and $\bot$ if it is not BR-unifiable.

$\mathrm{unify}_{\mathrm{BR}}(t(\vec{x})) :=$
  if $\vec{x} = ()$
  then if $t \overset{\mathrm{BR}}{=} 0$
    then $\varnothing$
    else $\bot$
  else let $\sigma := \mathrm{unify}({}_{\{x_1\mapsto 0\}}[t] \cdot {}_{\{x_1\mapsto 1\}}[t])$
    in $\{x_1 \mapsto ({}_{\{x_1\mapsto 0\}\cup\sigma}[t] + {}_{\{x_1\mapsto 1\}\cup\sigma}[t] + 1) \cdot x_1 + {}_{\{x_1\mapsto 0\}\cup\sigma}[t]\} \cup \sigma$

Note that, in practice, we often know whether $t \overset{\mathrm{BR}}{=} 0$ or $t \overset{\mathrm{BR}}{=} 1$ well before $\vec{x} = ()$. If for every recursive call instead of some term we pass its polynomial form, then the checks $t \overset{\mathrm{BR}}{=} 0$ and $t \overset{\mathrm{BR}}{=} 1$ simply become $t = 0$ and $t = 1$. Furthermore, since Algorithm 28 does not simplify the output mgu at all, it might contain many complicated subterms that are actually BR-equal to 0. Therefore, the following algorithm might be more efficient in some cases and will return a simplified mgu.

ALGORITHM 29. Let s and t be BR-terms in $\vec{x}$. Like Algorithm 28, this algorithm returns a BR-mgu σ of $t = 0$ in case that it is BR-unifiable and $\bot$ if it is not BR-unifiable.

$\mathrm{unify}'_{\mathrm{BR}}(t(\vec{x})) :=$
  if $t = 0$
  then $\varnothing$
  else if $t = 1$
    then $\bot$
    else let $\sigma := \mathrm{unify}(({}_{\{x_1\mapsto 0\}}[t] \cdot {}_{\{x_1\mapsto 1\}}[t])\downarrow)$
      in $\{x_1 \mapsto (({}_{\{x_1\mapsto 0\}\cup\sigma}[t] + {}_{\{x_1\mapsto 1\}\cup\sigma}[t] + 1) \cdot x_1 + {}_{\{x_1\mapsto 0\}\cup\sigma}[t])\downarrow\} \cup \sigma$

We could now use either Algorithm 28 or Algorithm 29 to prove Theorem 27 instead of Löwenheim's Theorem in order to prove Theorem 27. In any case, we can prove the following theorem.

THEOREM 30. The unification of Boolean rings and Boolean algebras is unitary.

PROOF. The case for Boolean rings is an immediate consequence of Theorem 27 using Theorem 15. The case for Boolean algebras follows from the fact that every BA-equation is equivalent to the the BR-equation that is the same equation with $\overset{\text{BR}}{\mapsto}$ applied, and the same holds for a system of BA-equations. "Equivalent" here means that they hold in the same models, in the sense of Proposition 20. This means that, if an equation holds in all Boolean rings, then it also holds in all Boolean algebras. Therefore, if we apply $\overset{\text{BA}}{\mapsto}$ to the terms of a BR-unifier, this gives a BA-unifier and vice versa, and the mgu property is also preserved. ∎

The function that returns the mgu of a system of n BR-equations $\{t_1 = 0, \ldots, t_n = 0\}$, in case it is BR-unifiable, and $\bot$ otherwise, is given by $\mathsf{unify}^n_{\text{BR}}$ as specified in Algorithm 16. Algorithm 28, Algorithm 29 or any other such algorithm, could be chosen for the base case function.

Examples

In the following, we will look at four short examples in order to demonstrate how to calculate the BR-mgu of single equations and systems of equations. For the sake of clarity, we will simplify the returned unifier after every step. In the second example we will not, however, simplify the terms in the recursive calls, in order to show how using $\mathsf{unify}'_{\text{BR}}$ over $\mathsf{unify}_{\text{BR}}$ can save some calculation effort.

EXAMPLE 31. Consider $s(x, y) := x + y + 1$. Then, first we calculate

$$\begin{aligned} s' &:= {}_{\{x\mapsto 0\}}[s] \cdot {}_{\{x\mapsto 1\}}[s] = (0 + y + 1) \cdot (1 + y + 1) \\ s'' &:= {}_{\{x\mapsto 0\}}[s'] \cdot {}_{\{x\mapsto 1\}}[s'] \\ &= (0 + 0 + 1) \cdot (1 + 0 + 1) \cdot (0 + 1 + 1) \cdot (1 + 1 + 1) \\ &\overset{\text{BR}}{=} 1 \cdot 0 \cdot 0 \cdot 1 \\ &\overset{\text{BR}}{=} 0 \end{aligned}$$

Therefore, we have that $\sigma'' := \varnothing$ is an mgu of $s'' = 0$. Now, unwrapping the recursion, we have that

$$\begin{aligned}
\sigma' &:= \left\{y \mapsto \left({}_{\{y\mapsto 0\}\cup\sigma''}[s'] + {}_{\{y\mapsto 1\}\cup\sigma''}[s'] + 1\right)\cdot y + {}_{\{y\mapsto 0\}\cup\sigma''}[s']\right\} \cup \sigma'' \\
&\overset{\text{BR}}{=} \{y \mapsto ((0+0+1)\cdot(1+0+1) + (0+1+1)\cdot(1+1+1) + 1)y \\
&\quad +(0+0+1)\cdot(0+1+1)\} \cup \varnothing \\
&\overset{\text{BR}}{=} \{y \mapsto (1\cdot 0 + 0\cdot 1 + 1)y + 1\cdot 0\} \\
&\overset{\text{BR}}{=} \{y \mapsto 1y + 0\} \\
&\overset{\text{BR}}{=} \{y \mapsto y\} \\
&\overset{\text{BR}}{=} \varnothing
\end{aligned}$$

Lastly, we receive the following substitution:

$$\begin{aligned}
\sigma &:= \left\{x \mapsto \left({}_{\{x\mapsto 0\}\cup\sigma'}[s] + {}_{\{x\mapsto 1\}\cup\sigma'}[s] + 1\right)\cdot x + {}_{\{x\mapsto 0\}\cup\sigma'}[s]\right\} \cup \sigma' \\
&= \{x \mapsto ((0+y+1) + (1+y+1) + 1)x + (0+y+1)\} \cup \sigma' \\
&\overset{\text{BR}}{=} \{x \mapsto (y+1+y+1)x + y + 1\} \cup \varnothing \\
&\overset{\text{BR}}{=} \{x \mapsto 0x + y + 1\} \\
&\overset{\text{BR}}{=} \{x \mapsto y + 1\}
\end{aligned}$$

which is the mgu of $s = 0$ as expected.

EXAMPLE 32. The next example is not unifiable. Consider $t(x, y) := xy(xy + x) + 1$. Then it holds that

$$\begin{aligned}
t' &:= {}_{\{x\mapsto 0\}}[t] \cdot {}_{\{x\mapsto 1\}}[t] = (0y(0y+0)+1)\cdot(1y(1y+1)+1) \\
t'' &:= {}_{\{x\mapsto 0\}}[t'] \cdot {}_{\{x\mapsto 1\}}[t'] \\
&= (0\cdot 0\cdot(0\cdot 0+0)+1)\cdot(1\cdot 0\cdot(1\cdot 0+1)+1) \\
&\quad \cdot(0\cdot 1\cdot(0\cdot 1+0)+1)\cdot(1\cdot 1\cdot(1\cdot 1+1)+1) \\
&\overset{\text{BR}}{=} 1\cdot 1\cdot 1\cdot 1 \\
&\overset{\text{BR}}{=} 1
\end{aligned}$$

which means that t'', and therefore t' as well as t are not unifiable. One could have noticed already that

$$xy(xy+x)+1 \overset{\text{BDR}}{=} xy(x+1)+1 \overset{\text{BDR}}{=} 0+1 \overset{\text{BDR}}{=} 1$$

and therefore the algorithm $\mathsf{unify}'_{\text{BR}}$ would have immediately returned $\bot$ without any recursive call.

EXAMPLE 33. Now consider the system of BR-equations

$$E := \{x + y + 1 = 0, a + x = 0\}$$

By Example 32, it holds that $\tau_1 \coloneqq \{x \mapsto y + 1\}$ is the mgu of the first equation. Since ${}_{\tau_1}[a + x] = a + y + 1$, this means that $\sigma_2 \coloneqq \{a \mapsto y + 1\}$ is a unifier of ${}_{\tau_1}[a + x] = 0$. Together, we have that

$$\tau_2 \coloneqq \sigma_2\tau_1 = \{x \mapsto y + 1, a \mapsto y + 1\}$$

is the unifier of the system of equations E.

EXAMPLE 34. All the individual equations of the system of BR-equations

$$F \coloneqq \{x + y + 1 = 0, xy + 1 = 0\}$$

are clearly unifiable. However, applying the unifier $\tau_1 \coloneqq \{x \mapsto y + 1\}$ to the second equation, we receive ${}_{\tau_1}[xy + 1] = (y + 1)y + 1 \overset{\text{BDR}}{=} 0 + 1 = 1$ which is not unifiable with 0. Therefore F is not BR-unifiable.

2 Boolean Differential Rings

2.1 Definitions and Characterizations

We will now define the language and theory of Boolean differential rings and list some important propositions. We will generally follow F. Weitkämper [3] but adapt it to our needs.

DEFINITION 35 ([3, Def. 11])**.** The language $\mathcal{L}_{\mathrm{BDR}}$ of Boolean differential rings contains all the function and predicate symbols of $\mathcal{L}_{\mathrm{BR}}$, as well as the 0-ary function symbol z and the unary function symbol δ. The theory T_{BDR} of Boolean differential rings consists of the axioms of T_{BR} as well as the following (abbreviated) axioms:

(i′) $\sigma := \mathrm{id} + \delta$ is an involution of Boolean rings.
(ii′) $\mathrm{Ker}(\delta) \vDash T_{\mathrm{BR}}$
(iii′) $\delta(z) = 1$

As with the axioms of T_{BR}, we will, for the sake of convenience, usually use the axioms of T_{BDR} without explicitly mentioning them. Note that axioms (i') and (ii') are merely abbreviations of respective sets of axioms. Axiom (i') gives us the desired properties of δ and (ii') states that $\mathrm{Ker}(\delta)$ is always a subring. The following two lemmas provide alternative characterizations of axioms (i') and (ii').

LEMMA 36. Under the assumption of T_{BR} as well as axioms (ii') and (iii'), axiom (i') is equivalent to the following axioms:

(a) $\delta(1) = 0$
(b) $\forall_{a,b}(\delta(a + b) = \delta(a) + \delta(b))$
(c) $\forall_{a,b}(\delta(a \cdot b) = \delta(a) \cdot b + a \cdot \delta(b) + \delta(a) \cdot \delta(b))$
(d) $\forall_a(\delta(\delta(a)) = 0)$

PROOF. Suppose that axiom (i') holds. First, we see that $\delta(x) = 1 + 1 + \delta(x) = 1 + \sigma(x)$ for all x. Then, $\delta(1) = 1 + \sigma(1) = 1 + 1 = 0$. Furthermore, since σ is a ring homomorphism, it holds that

$$\begin{aligned}\delta(a+b) &= (a+b) + \sigma(a+b)\\ &= a + b + \sigma(a) + \sigma(b)\\ &= (a + \sigma(a)) + (b + \sigma(b))\\ &= \delta(a) + \delta(b)\end{aligned}$$

as well as

$$\begin{aligned}\delta(a \cdot b) &= a \cdot b + \sigma(a \cdot b)\\ &= a \cdot b + \sigma(a) \cdot \sigma(b)\\ &= a \cdot b + (a + \delta(a)) \cdot (b + \delta(b))\\ &= a \cdot b + a \cdot b + \delta(a) \cdot b + a \cdot \delta(b) + \delta(a)\delta(b)\\ &= \delta(a) \cdot b + a \cdot \delta(b) + \delta(a) \cdot \delta(b)\end{aligned}$$

and, since σ is an involution (i.e. $\sigma \circ \sigma = \sigma$), further

$$\begin{aligned}\delta(\delta(a)) &= \delta(a) + \sigma(\delta(a))\\ &= a + \sigma(a) + \sigma(a + \sigma(a))\\ &= a + \sigma(a) + \sigma(a) + \sigma(\sigma(a))\\ &= a + 0 + a\\ &= 0\end{aligned}$$

for all a and b. Now, conversely assume axioms (a)-(d). Then, first note that we have $\sigma(1) = 1 + \delta(1) = 1 + 0 = 1$. Furthermore, it holds that

$$\begin{aligned}\sigma(a+b) &= a + b + \delta(a+b)\\ &= a + b + \delta(a) + \delta(b)\\ &= (a + \delta(a)) + (b + \delta(b))\\ &= \sigma(a) + \sigma(b)\end{aligned}$$

as well as

$$\begin{aligned}\sigma(a \cdot b) &= a \cdot b + \delta(a \cdot b)\\ &= a \cdot b + \delta(a) \cdot b + a \cdot \delta(b) + \delta(a) \cdot \delta(b)\\ &= (a + \delta(a)) \cdot (b + \delta(b))\\ &= \sigma(a) \cdot \sigma(b)\end{aligned}$$

and finally

$$\begin{aligned}\sigma(\sigma(a)) &= \sigma(a) + \delta(\sigma(a)) \\ &= \sigma(a) + \delta(a + \delta(a)) \\ &= \sigma(a) + \delta(a) + \delta(\delta(a)) \\ &= \sigma(a) + a + \sigma(a) + 0 \\ &= a\end{aligned}$$

for all a and b. This concludes the proof. ∎

LEMMA 37. Axiom (ii') follows from T_{BR} as well as axiom (i').

PROOF. We need to show that $\mathsf{Ker}(\delta)$ is a Boolean subring, i. e. it is an additive subgroup, closed under multiplication and contains 1. Clearly, the rest of the axioms of T_{BR}, i. e. $a + a = 0$, $a \cdot a = a$ as well as associativity, commutativity and distributivity, hold for $\mathsf{Ker}(\delta)$, since they already hold globally. The first part holds since by (i'), δ is an additive group homomorphism and therefore $\mathsf{Ker}(\delta)$ is a subgroup. Also by (i'), we have that $1 \in \mathsf{Ker}(\delta)$ and for all $a, b \in \mathsf{Ker}(\delta)$ it holds that

$$\delta(a \cdot b) = \delta(a) \cdot b + a \cdot \delta(b) + \delta(a) \cdot \delta(b) = 0 + 0 + 0 = 0$$

i. e. $a \cdot b \in \mathsf{Ker}(\delta)$. Together, axiom (ii') holds. ∎

This shows that T_{BDR} abbreviates a finite axiomatization of Boolean differential rings. As with Boolean rings, we will often write "BDR" when we actually mean $\mathcal{L}_{\mathrm{BDR}}$ or T_{BDR}. Moreover, we call models of T_{BDR} "Boolean differential rings". Since $\mathcal{L}_{\mathrm{BDR}}$ is an extension of $\mathcal{L}_{\mathrm{BR}}$, we can view every BR-term as a BDR-term. For the converse, consider first the following definition.

DEFINITION 38. A term T is z-free, if z is not a subterm of T. T is δ-free if it does not contain a subterm of the form $\delta(S)$.

In other words, a term is z-free if it does not contain z and δ-free if it does not contain δ. We can view every z-free and δ-free BDR-term as a BR-term. In the rest of this thesis, we will simply write "term" to mean BDR-term and specify that it is z-free and δ-free by stating that it is a BR-term, in the above sense. In contrast to general $\mathcal{L}$-terms, we will usually give upper case letter names to BDR-terms.

Next, we will define the syntactic analogon of $\mathsf{Ker}(\delta)$.

DEFINITION 39. A term T is δ-vanishing if $\delta(T) \overset{\mathrm{BDR}}{=} 0$.

This allows us to consider the following specializations of the product rule.

LEMMA 40.

(i) If S and T are terms and S is δ-vanishing, then $\delta(S \cdot T) \overset{\text{BDR}}{=} S \cdot \delta(T)$.

(ii) If S is a δ-vanishing term, then $\delta(Sz) \overset{\text{BDR}}{=} S$.

(iii) If A and B are δ-vanishing terms, then $\delta(Az + B) \overset{\text{BDR}}{=} A$.

PROOF. The proofs follow immediately from the product rule. I. e. it holds that:

$$\begin{aligned}\delta(S \cdot T) &\overset{\text{BDR}}{=} \delta(S) \cdot T + S \cdot \delta(T) + \delta(S) \cdot \delta(T) \\ &\overset{\text{BDR}}{=} 0 \cdot T + S \cdot \delta(T) + 0 \cdot \delta(T) \\ &\overset{\text{BDR}}{=} S \cdot \delta(T)\end{aligned}$$

Further we have that $\delta(Sz) \overset{\text{BDR}}{=} S \cdot \delta(z) \overset{\text{BDR}}{=} S \cdot 1 \overset{\text{BDR}}{=} S$ and

$$\delta(Az + B) \overset{\text{BDR}}{=} \delta(Az) + \delta(B) \overset{\text{BDR}}{=} A + 0 \overset{\text{BDR}}{=} A$$

which completes the proof. ∎

Part (ii) suggests that for all models of T_{BDR}, $\mathsf{Ker}(\delta) = \mathsf{Im}(\delta)$. In the following, we will give two ways to represent any term in the form $Az + B$ for δ-vanishing terms A and B.

LEMMA 41. Let T be any term. The following equalities hold:

(i) $T \overset{\text{BDR}}{=} \delta(T)z + (T + \delta(T)z)$

(ii) $T \overset{\text{BDR}}{=} \delta(T)z + \delta(T(z + 1))$.

PROOF. Part (i) is trivial as clearly $\delta(T)$ is δ-vanishing, and also $T + \delta(T)z$ is δ-vanishing, since

$$\delta(T + \delta(T)z) \overset{\text{BDR}}{=} \delta(T) + \delta(\delta(T)z) \overset{\text{BDR}}{=} \delta(T) + \delta(T) \overset{\text{BDR}}{=} 0$$

Using this, as well as the abbreviations $A \coloneqq \delta(T)$ and $B \coloneqq T + \delta(T)z$, we get for Part (ii) that

$$\begin{aligned}
\delta(T)z + \delta(T(z+1)) &\overset{\text{BDR}}{=} Az + \delta((Az+B)\cdot(z+1)) \\
&\overset{\text{BDR}}{=} Az + \delta(Az(z+1) + B(z+1)) \\
&\overset{\text{BDR}}{=} Az + \delta(0 + Bz + B) \\
&\overset{\text{BDR}}{=} Az + \delta(Bz) + \delta(B) \\
&\overset{\text{BDR}}{=} Az + B + 0 \\
&\overset{\text{BDR}}{=} T
\end{aligned}$$

which completes the proof. ∎

The following theorem is the syntactic analogon to Proposition 10 of F. Weitkämper [3], which states that every Boolean differential ring is a free algebra over its kernel generated by 1 and z.

PROPOSITION 42.

(i) For all terms T, there are δ-vanishing terms A and B such that $T \overset{\text{BDR}}{=} Az + B$.

(ii) If A and B are δ-vanishing terms, then it holds that $Az + B \overset{\text{BDR}}{=} 0$ if and only if $A \overset{\text{BDR}}{=} 0$ and $B \overset{\text{BDR}}{=} 0$.

PROOF. Part (i) is immediate from Lemma 41. For part (ii), the direction where $A \overset{\text{BDR}}{=} 0$ and $B \overset{\text{BDR}}{=} 0$ implies $Az + B \overset{\text{BDR}}{=} 0$ is trivial, since in this case we have that

$$Az + B \overset{\text{BDR}}{=} 0z + 0 \overset{\text{BDR}}{=} 0$$

Now conversely suppose that $Az + B \overset{\text{BDR}}{=} 0$. Then clearly also

$$A \overset{\text{BDR}}{=} \delta(Az + B) \overset{\text{BDR}}{=} \delta(0) \overset{\text{BDR}}{=} 0$$

and therefore $0 \overset{\text{BDR}}{=} Az + B \overset{\text{BDR}}{=} 0z + B \overset{\text{BDR}}{=} B$, which concludes the proof. ∎

Boolean differential algebras are defined through Boolean differential rings in the same way Boolean algebras are defined through Boolean rings. For this, we define the replacments $\overset{\text{BDA}}{\mapsto}$ in the same way as $\overset{\text{BA}}{\mapsto}$, by naturally extending the definition to all BDR-terms.

DEFINITION 43. The language $\mathcal{L}_{\text{BDA}}$ of Boolean differential algebras consists of all of the symbols of $\mathcal{L}_{\text{BA}}$ as well as the 0-ary function symbol z and the unary function symbol δ. The theory T_{BDA} of Boolean differential algebras consists of all the (expanded) axioms of T_{BDR}, with the replacements $\overset{\text{BDA}}{\mapsto}$.

The idea of Proposition 20, suggests that also Boolean differential rings and Boolean differential algebras are essentially two ways of talking about the same objects. Again by construction, the following proposition holds.

PROPOSITION 44. Consider the replacements $\overset{\text{BDR}}{\mapsto}$ and $\overset{\text{BDA}}{\mapsto}$, which are the natural extensions of $\overset{\text{BR}}{\mapsto}$ and $\overset{\text{BA}}{\mapsto}$ to all $\mathcal{L}_{\text{BDR}}$ and $\mathcal{L}_{\text{BDA}}$-terms respectively.

(i) Every model of T_{BDA} is a model of T_{BDR} with the replacements $\overset{\text{BDA}}{\mapsto}$.

(ii) Every model of T_{BDR} is a model of T_{BDA} with the replacements $\overset{\text{BDR}}{\mapsto}$, that are defined by naturally extending $\overset{\text{BR}}{\mapsto}$, to all BDA-terms.

Example

The canonical example and original motivation of Boolean differential rings are the switching algebras $\mathbb{S}_n$ that we introduced earlier. Next to computing the value of a switching function for certain arguments, an important aspect in the study of switching algebras is certainly the question whether changing the arguments of a function will affect the function value. E.g. one could ask how the function value will change if we change the first variable, or even the second and third variable simultaneously, from 0 to 1. This study naturally gives rise to what B. Steinbach and C. Posthoff [1] call a *single simple derivative* and a *single vectorial derivative*. To be precise, the idea is to join the value before and after the change of arguments with a logical exclusive or (i.e. "+" of $\mathbb{S}_n$), since this will precisely give 0 if both are the same (i.e. nothing changes) and 1 if they are different. In the following, we will define the vectorial derivative ∂_S where we look at the change of value if all the i-th variables for $i \in S$ change.

Let $n \in \mathbb{N}$ and $S \subseteq \{1, \ldots, n\}$. Then we first define the function $\rho_S : \mathbb{2}^n \to \mathbb{2}^n$ by

$$\left(\rho_S(\vec{x})\right)_i := \begin{cases} x_i + 1 \text{ if } i \in S \\ x_i \qquad \text{otherwise} \end{cases}$$

which now lets us define the vectorial derivate w.r.t. S as the function $\partial_S : \mathbb{S}_n \to \mathbb{S}_n$ and

$$\partial_S(f)(\vec{x}) = f(\vec{x}) + f(\rho_S(\vec{x}))$$

We further define the function $z_S \in \mathbb{S}_n$ by $z_S(\vec{x}) := \prod_{i \in S} x_i$. It remains to show that this actually constitutes a Boolean differential ring in the sense of Definition 35.

First, we will show that $\sigma_S := \mathrm{id} + \partial_S$ is a Boolean ring involution. By definition, we have that

$$\sigma_S(f)(\vec{x}) = f(\vec{x}) + \partial_S(f)(\vec{x}) = f(\vec{x}) + f(\vec{x}) + f(\rho(\vec{x})) = f(\rho(\vec{x}))$$

Therefore it is easy to see that

$$\sigma_S(f+g)(\vec{x}) = (f+g)(\rho(\vec{x})) = f(\rho(\vec{x})) + g(\rho(\vec{x})) = \sigma_S(f)(\vec{x}) + \sigma_S(g)(\vec{x})$$

as well as

$$\sigma_S(f \cdot g)(\vec{x}) = (f \cdot g)(\rho(\vec{x})) = f(\rho(\vec{x})) \cdot g(\rho(\vec{x})) = \sigma_S(f)(\vec{x}) \cdot \sigma_S(g)(\vec{x})$$

and $\sigma_S(1)(\vec{x}) = 1(\rho(\vec{x})) = 1$. The involution property holds, since

$$(\rho(\rho(\vec{x})))_i = \begin{Bmatrix} \rho_S(x_i)+1 & \text{if } i \in S \\ x_i & \text{otherwise} \end{Bmatrix} = \begin{Bmatrix} x_i+1+1 & \text{if } i \in S \\ x_i & \text{otherwise} \end{Bmatrix} = x_i$$

and therefore $\sigma_S(\sigma_S(f))(\vec{x}) = \sigma_S(f)(\rho(\vec{x})) = f(\rho(\rho(\vec{x}))) = f$. Together, axiom (i') holds. Lastly, it holds that

$$\partial_S(z_S)(\vec{x}) = z_S(\vec{x}) + z_{\rho(\vec{x})} = \prod_{s \in S} x_i + \prod_{s \in S}(x_i + 1) = x_i + x_i + 1 = 1$$

Since, by Lemma 37 axiom (ii') follows from the other axioms, it holds that $\mathbb{S}_n$ together with ∂_S and z_S is a Boolean differential ring.

2.2 On the Shape of BDR-Terms

In the following we will define some basic properties of BDR-terms as well as a normal form of BDR-terms that is similar to the polynomial form of BR-terms. The analogon of polynomials will be flat terms and we will define the flattening function $\downarrow$ in a way that coincides with the polynomial form function $\downarrow$ on BR-terms.

DEFINITION 45. We say that a subterm S of T is enclosed (by δ) if it occurs as a subterm of a subterm of T of the form $\delta(U)$. S is immediately enclosed (by δ) if the smallest proper superterm of S inside T is $\delta(S)$.

Since dealing with arbitary BDR-terms is quite cumbersome, we want to mostly deal with terms that are *polynomial-like* in the sense that they are sums of products of atoms. We also call these terms *flat* since polynomial-like terms do not have any nested δ and all δ only apply directly to some variable. Luckily, it turns out that every BDR-term can be rewritten as such a term.

DEFINITION 46. A BDR-atom is a BDR-term that is either a constant $c \in \{0, 1, z\}$, or x or $\delta(x)$ for some variable x. Then a BDR-term is monomial-like if it is a product of BDR-atoms and it is polynomial-like or *flat*, if it is a sum of monomials.

We can extend Definition 23 in a natural way to define for BDR-monomials M_1 and M_2, as well as BDR-polynomials P_1 and P_2 the terms

$$M_1 * M_2 \qquad P_1 \oplus P_2 \qquad P_1 \odot P_2$$

so that $M_1 * M_2 \overset{\text{BDR}}{=} M_1 \odot M_2 \overset{\text{BDR}}{=} M_1 \cdot M_2$, $P_1 \oplus P_2 \overset{\text{BDR}}{=} P_1 + P_2$ and $P_1 \odot P_2 \overset{\text{BDR}}{=} P_1 \cdot P_2$.

This lets us define a function that returns for every term T a flattened term $T{\downarrow}$.

ALGORITHM 47. Let T be any term. We define $T{\downarrow}$ recursively in the following way:

$T{\downarrow} \coloneqq$ **match** T
- $\{0, 1, z, x\} \Rightarrow T$
- $T_1 + T_2 \Rightarrow T_1{\downarrow} \oplus T_2{\downarrow}$
- $T_1 \cdot T_2 \Rightarrow T_1{\downarrow} \odot T_2{\downarrow}$
- $\delta(S) \Rightarrow$ **match** S
  - $\{0, 1\} \Rightarrow 0$
  - $z \Rightarrow 1$
  - $x \Rightarrow \delta(x)$
  - $S_1 + S_2 \Rightarrow \delta(S_1){\downarrow} \oplus \delta(S_2){\downarrow}$
  - $S_1 \cdot S_2 \Rightarrow \delta(S_1){\downarrow} \odot S_2{\downarrow} \oplus S_1{\downarrow} \odot \delta(S_2){\downarrow} \oplus \delta(S_1){\downarrow} \odot \delta(S_2){\downarrow}$
  - $\delta(U) \Rightarrow 0$

As with Algorithm 24, we can take some ordering of the BDR-atoms that extends to a lexicographic ordering on monomial-like terms and assume $T{\downarrow}$ is defined in such a way that all monomial-like terms and all BDR-atoms within the monomial-like terms are ordered. The following two propositions show that this definition of $T{\downarrow}$ is sensible, in that $T{\downarrow}$ is actually flat and equival to T, as well as minimal in the sense that applying ${\downarrow}$ a second time will not change anything.

PROPOSITION 48. Let T be any term. Then $T{\downarrow}$ is flat and it holds that $T \overset{\text{BDR}}{=} T{\downarrow}$.

PROOF. We will prove this by induction on the shape of T.

(i) If $T = c \in \{0, 1, z\}$ or $T = x$ for a variable x, then T is already flat.

(ii) If $T = T_1 + T_2$ for terms T_1 and T_2 that satisfy the induction hypothesis. Then $T{\downarrow} = T_1{\downarrow} \oplus T_2{\downarrow}$ is clearly flat and
$$T = T_1 + T_2 \overset{\text{BDR}}{=} T_1{\downarrow} + T_2{\downarrow} \overset{\text{BDR}}{=} T_1{\downarrow} \oplus T_2{\downarrow} = T{\downarrow}$$

(iii) The case $T = T_1 \cdot T_2$ works analogously.

(iv) Suppose that $T = \delta(S)$ for a term S that satisfies the induction hypothesis. We will prove by induction on the shape of S that $\delta(S){\downarrow}$ is flat and $\delta(S) \overset{\text{BDR}}{=} \delta(S){\downarrow}$:

(i) If $S = c \in \{0, 1\}$ or $S = \delta(x)$ for a variable x, then $T\downarrow = 0$ which is flat, and also $T \overset{\text{BDR}}{=} \delta(S\downarrow) \overset{\text{BDR}}{=} 0 = T\downarrow$.

(ii) Similarly, if $S = z$, then $T\downarrow = 1$ is flat and $T \overset{\text{BDR}}{=} 1 = T\downarrow$.

(iii) Likewise, if $S = x$, then $T\downarrow = \delta(x)$ is flat and $T = \delta(x) = T\downarrow$.

(iv) Suppose $S = S_1 + S_2$ for flat terms S_1 and S_2 that satisfy the induction hypothesis. Then $T\downarrow = \delta(S_1)\downarrow \oplus \delta(S_2)\downarrow$ which is flat since the summands are. In addition, the following holds:

$$T = \delta(S_1 + S_2) \overset{\text{BDR}}{=} \delta(S_1) + \delta(S_2) \overset{\text{BDR}}{=} \delta(S_1)\downarrow \oplus \delta(S_2)\downarrow = \delta(S)\downarrow$$

(v) The case $S = S_1 \cdot S_2$ works similarly, with the only additional argumentation step being the assumption of the outer induction hypothesis that $S_1\downarrow$ and $S_2\downarrow$ are flat and that $S_1 \overset{\text{BDR}}{=} T\downarrow$ as well as $S_2 \overset{\text{BDR}}{=} T\downarrow$. Then it holds that

$$\begin{aligned}\delta(S) &= \delta(S_1 \cdot S_2)\\ &\overset{\text{BDR}}{=} \delta(S_1) \cdot S_2 + S_1 \cdot \delta(S_2) + \delta(S_1) \cdot \delta(S_2)\\ &\overset{\text{BDR}}{=} \delta(S_1)\downarrow \odot S_2\downarrow \oplus S_1\downarrow \odot \delta(S_2)\downarrow \oplus \delta(S_1)\downarrow \odot \delta(S_2)\downarrow\\ &= \delta(S)\downarrow\end{aligned}$$

with the last term being clearly flat since all factors are flat by assumption.

(vi) If $U = \delta(S)$, then $T\downarrow = 0$ which is flat and also $T \overset{\text{BDR}}{=} 0 = T\downarrow$.

By induction, it holds that $\delta(S)\downarrow$ is flat and $\delta(S) \overset{\text{BDR}}{=} \delta(S)\downarrow$. The statement now follows by the outer induction. ∎

From the proof of Proposition 48, it is clear that $\downarrow$ preserves variables, as well as BDR-atoms and monomial-like terms, in the sense of the following lemma.

LEMMA 49.

(i) If T is a term of $\vec{x}$, then $T\downarrow$ is a term of $\vec{x}$ as well.

(ii) If A is a BDR-atom, then $A\downarrow = A$.

(iii) If M is a monomial-like term, then $M\downarrow$ is a monomial-like term.

In addition, the following lemma holds.

LEMMA 50. Let T be any term. Then $T\downarrow\downarrow = T\downarrow$.

PROOF. We will show this by induction on the shape of $T\downarrow$:

(i) If $T\downarrow = c \in \{0, 1, z\}$ or $T\downarrow = x$ or $T\downarrow = \delta(x)$ for a variable x, then $T\downarrow\downarrow = T\downarrow$ holds by definition.

(ii) Suppose that $T{\downarrow} = T_1 + T_2$ for flat terms T_1 and T_2 that satisfy the induction hypothesis. T_1 and T_2 are, as a result of $T{\downarrow}$, clearly do not contain 0 and their monomial-like subterms are pairwise different. Therefore, it holds that
$$T{\downarrow}{\downarrow} = T_1{\downarrow} \oplus T_2{\downarrow} = T_1 \oplus T_2 = T_1 + T_2 = T{\downarrow}$$
(iii) If $T{\downarrow} = T_1 \cdot T_2$ for flat terms T_1 and T_2 that satisfy the induction hypothesis. Since $T{\downarrow}$ is flat, this means that T_1 and T_2 are monomial-like. Furthermore, by the above reasing, neither T_1 or T_2 contain 0 or 1 and their atoms are pairwise different. Therefore $T_1 * T_2 = T_1 \cdot T_2$ and further
$$T{\downarrow}{\downarrow} = T_1{\downarrow} * T_1{\downarrow} = T_1 * T_2 = T{\downarrow}$$

The statement now follows by induction. ∎

Next, we will define what it means for a term to be *benign* and we will see that benign terms act very much like BR-terms in $\mathsf{Ker}(\delta)$.

DEFINITION 51. A term T is benign if it is z-free, flat and all occurences of variables are immediately enclosed by δ.

LEMMA 52. Every benign term is δ-vanishing.

PROOF. Let T be a benign term. We prove this by induction on the shape of T.

(i) If $T = c$ for $c \in \{0, 1\}$, then $\delta(T) = \delta(c) \overset{\text{BDR}}{=} 0$.
(ii) If $T = \delta(x)$ for some variable x, then $\delta(T) = \delta(\delta(x)) \overset{\text{BDR}}{=} 0$.
(iii) If $T = S_1 + S_2$ for S_1 and S_2 satisfying the induction hypothesis. Since S_1 and S_2 are clearly also benign, we have that
$$\delta(T) = \delta(S_1 + S_2) \overset{\text{BDR}}{=} \delta(S_1) + \delta(S_2) \overset{\text{BDR}}{=} 0 + 0 \overset{\text{BDR}}{=} 0$$
(iv) If $T = S_1 \cdot S_2$ for S_1 and S_2 satisfying the induction hypothesis. Clearly S_1 and S_2 are also benign, and therefore
$$\begin{aligned}\delta(T) &= \delta(S_1 \cdot S_2)\\ &\overset{\text{BDR}}{=} \delta(S_1) \cdot S_2 + S_1 \cdot \delta(S_2) + \delta(S_1) \cdot \delta(S_2)\\ &\overset{\text{BDR}}{=} 0 \cdot S_2 + S_1 \cdot 0 + 0 \cdot 0\\ &\overset{\text{BDR}}{=} 0 + 0 + 0\\ &\overset{\text{BDR}}{=} 0\end{aligned}$$

The statement now follows by induction. ∎

In the following, we work towards showing that every term that a big class of terms can be presented as $Az + B$ for benign terms A and B.

PROPOSITION 53. Let T be a term that has all variable occurences immediately enclosed by δ. Then $T\downarrow$ also has all variable occurences immediately enclosed by δ. If furthermore all occurences of z are enclosed by δ, then $T\downarrow$ is benign.

PROOF. We will prove this by induction on the shape of T:

(i) If $T = c \in \{0, 1, z\}$, then clearly $T\downarrow = T$ contains no variables, and therefore the statement holds trivially. The case $T = z$ does not apply for the second part, and since 0 and 1 do not contain z, the statement holds trivially.

(ii) If $T = T_1 + T_2$ for terms T_1 and T_2 that satisfy the induction hypothesis. Since all variable occurences of T are immediately enclosed by δ, the same holds for T_1 and T_2. Similarly, all occurences of z in T_1 and T_2 are enclosed by δ, if it already holds in T. Therefore, by induction hypothesis, $T\downarrow = T_1\downarrow \oplus T_2\downarrow$ has all variable occurences immediately enclosed by δ, and also all occurences of z enclosed by δ, if T does.

(iii) The case $T = T_1 \cdot T_2$ works analogously.

(iv) If $T = \delta(z)$, then $T\downarrow = 1$ and 1 trivially satisfies both parts of the statement.

(v) Suppose that $T = \delta(S)$ for a term S that satisfies the induction hypothesis. We will prove by induction on the shape of S that $\delta(S)\downarrow$ has all variable occurences immediately enclosed by δ, and all occurences of z enclosed by δ, if S does.

  (i) If $S = c \in \{0, 1\}$ or $S = \delta(x)$ for a variable x, then $T\downarrow = 0$ which trivially satisfies both parts of the statement.

  (ii) Likewise, if $S = x$, then $T\downarrow = \delta(x)$ which has all variable occurences immediately enclosed by δ and also does not contain z and therefore trivially satisfies the second part of the statement.

  (iii) Suppose $S = S_1 + S_2$ for flat terms S_1 and S_2 that satisfy the outer and inner induction hypotheses. Since T has all variable occurences immediately enclosed, so do S_1 and S_2, since $T = \delta(S_1 + S_2)$. Therefore, by the inner induction hypothesis, $T\downarrow = \delta(S_1)\downarrow \oplus \delta(S_2)\downarrow$ has all variable occurences immediately enclosed by δ. Similarly, if T has all occurences of z enclosed by δ, then so do S_1 and S_2, and therefore, by the inner induction hypothesis, so does $T\downarrow$.

  (iv) The case $S = S_1 \cdot S_2$ works similarly, with the only additional argumentation step being the assumption of the outer induction hypothesis, that $S_1\downarrow$ and $S_2\downarrow$

have all variable occurences immediately enclosed by δ, and all occurences of z enclosed by δ, if T does. Then

$$\delta(S)\downarrow = \delta(S_1)\downarrow \odot S_2\downarrow \oplus S_1\downarrow \odot \delta(S_2)\downarrow \oplus \delta(S_1)\downarrow \odot \delta(S_2)\downarrow$$

satisfies both parts of the statement.

(v) If $U = \delta(S)$, then $T\downarrow = 0$ which trivially satisfies both parts of the statement.

By the inner induction, it holds that $\delta(S)\downarrow$ has all variable occurences immediately enclosed by δ, and all occurences of z enclosed by δ, if S does. Both parts of the original statement now follow by the outer induction. ∎

PROPOSITION 54. Let T be a term with all variable occurences immediately enclosed by δ. Then there are benign terms A and B such that $T \overset{\text{BDR}}{=} Az + B$.

PROOF. By Lemma 41, it holds that $T \overset{\text{BDR}}{=} \delta(T)z + \delta(T(z+1))$. $\delta(T)$ as well as $\delta(T(z+1))$ clearly have all variable occurences immediately enclosed by δ and all occurences of z enclosed by δ. Therefore, by Proposition 53, it holds that there are benign terms A and B such that $\delta(T) \overset{\text{BDR}}{=} A$ and $\delta(T(z+1)) \overset{\text{BDR}}{=} B$. Together, it holds that

$$T \overset{\text{BDR}}{=} \delta(T)z + \delta(T(z+1)) \overset{\text{BDR}}{=} Az + B$$

concluding the proof. ∎

2.3 Making BDR-Terms Into BR-Terms

The idea behind flat terms is that they essentially behave like BR-terms in the sense that the δ only affect individual variable occurences and also there is no immediate way of applying the only relevant additional property of z. Therefore, $\delta(x_i)$ and z behave like ordinary variables and it makes intuitive sense that we should get the same resulting equalities if we actually substitute them for ordinary variables. In the following, we will make this intuition more precise, starting with the definition of an associated BR-term $\|T\|$ for every flat term T. We will see that T and $\|T\|$ behave essentially the same w.r.t. equalities.

DEFINITION 55. Let $T(\vec{x})$ be a flat term and $\vec{x}$ as well as Z variables not occuring in T. Then we define the BR-term $|T|$ as follows

(i) $|c| := c$ for $c \in \{0, 1\}$

(ii) $|z| := Z$

(iii) $|x_i| \coloneqq \bar{x}_i$
(iv) $|\delta(x_i)| \coloneqq x_i$
(v) $|S_1 + S_2| \coloneqq |S_1| + |S_2|$
(vi) $|S_1 \cdot S_2| \coloneqq |S_1| \cdot |S_2|$
Furthermore, define the following substitutions:

$$\varepsilon_{\vec{x}} \coloneqq \{x_i \mapsto x_i z \mid 0 < i \leq n\}$$
$$\eta_{\vec{x}} \coloneqq \{x_i \mapsto \delta(x_i), \bar{x}_i \mapsto x_i \mid 0 < i \leq n\} \cup \{Z \mapsto z\}$$

The way that we defined $|x_i|$ as $\bar{x}_i$ and $\delta(x_i)$ as x_i, and not the other way round, is due to the fact that in the later part, we will apply $|\cdot|$ only to benign terms and it is more convenient to have T as well as $|T|$ be terms over the same variables. Next, we will show that $\eta_{\vec{x}}$ is the syntactic inverse of $|\cdot|$ and the BDR-inverse of $\eta_{\vec{x}}$ for some terms with specific properties.

LEMMA 56. For every flat term $T(\vec{x})$ it holds that $T = {}_{\eta_{\vec{x}}}[|T|]$.

PROOF. We prove this by induction on the shape of T.
(i) If $T = c$ with $c \in \{0, 1\}$, then ${}_{\eta_{\vec{x}}}[|c|] = {}_{\eta_{\vec{x}}}[c] = c$.
(ii) If $T = z$, then ${}_{\eta_{\vec{x}}}[|z|] = {}_{\eta_{\vec{x}}}[Z] = z$.
(iii) If $T = x_i$, for $0 < i \leq n$, then ${}_{\eta_{\vec{x}}}[|x_i|] = {}_{\eta_{\vec{x}}}[\bar{x}_i] = x_i$.
(iv) If $T = \delta(x_i)$, for $0 < i \leq n$, then ${}_{\eta_{\vec{x}}}[|\delta(x_i)|] = {}_{\eta_{\vec{x}}}[x_i] = \delta(x_i)$.
(v) Suppose $T = S_1 + S_2$, for flat terms S_1 and S_2 that satisfy the induction hypothesis. Then it holds that

$${}_{\eta_{\vec{x}}}[|S_1 + S_2|] = {}_{\eta_{\vec{x}}}[|S_1| + |S_2|] = {}_{\eta_{\vec{x}}}[|S_1|] + {}_{\eta_{\vec{x}}}[|S_2|] = S_1 + S_2$$

(vi) And similarly, the statement holds for the case $T = S_1 \cdot S_2$.
The statement follows by induction. ∎

LEMMA 57. For every flat BR-term $T(\vec{x}, \vec{\bar{x}}, Z)$, it holds that $T = |_{\eta_{\vec{x}}}[T]|$.

PROOF. We prove this by induction on the shape of T.
(i) If $T = c$ with $c \in \{0, 1\}$, then $|_{\eta_{\vec{x}}}[c]| = |c| = c$.
(ii) If $T = Z$, then $|_{\eta_{\vec{x}}}[Z]| = |z| = Z$.
(iii) If $T = x_i$, for $0 < i \leq n$, then $|_{\eta_{\vec{x}}}[x_i]| = |\delta(x_i)| = x_i$.
(iv) If $T = \bar{x}_i$, for $0 < i \leq n$, then $|_{\eta_{\vec{x}}}[\bar{x}_i]| = |x_i| = \bar{x}_i$.

(v) Suppose $T = S_1 + S_2$, for flat terms S_1 and S_2 that satisfy the induction hypothesis. Then it holds that

$$|\eta_{\vec{x}}[S_1 + S_2]| = |\eta_{\vec{x}}[S_1] + \eta_{\vec{x}}[S_2]| = |\eta_{\vec{x}}[S_1]| + |\eta_{\vec{x}}[S_2]| = S_1 + S_2 = T$$

(vi) And similarly, the statement holds for the case $T = S_1 \cdot S_2$.

The statement follows by induction. ∎

LEMMA 58. Let $T(\vec{x})$ be a term with all variables immediately enclosed. Then $\eta_{\vec{x}}\varepsilon_{\vec{x}}[T] \overset{\text{BDR}}{=} T$.

PROOF. We prove this by induction on the shape of T. The base cases $T = c$ with $c \in \{0, 1, z\}$ and the inductive cases $T = S_1 + S_2$, $T = S_1 \cdot S_2$ for terms S_1 and S_2, as well as the case $T = \delta(S)$, for S not a single variable, are trivial. The only non-trivial case is the one for $T = \delta(x)$ for some variable x. Here we have that

$$\eta_{\vec{x}}\varepsilon_{\vec{x}}[\delta(x)] = \eta_{\vec{x}}[\delta(xz)] = \delta(\delta(x)z) \overset{\text{BDR}}{=} \delta(x)$$

since clearly $\delta(x)$ is δ-vanishing. The statement now follows by induction. ∎

The following theorem and its corollaries make our previous intuition, that flat terms behave like BR-terms, precise.

THEOREM 59. Let $T(\vec{x})$ be a flat term. Then it holds that $T \overset{\text{BDR}}{=} 0$ if and only if $|T| \overset{\text{BR}}{=} 0$.

PROOF. Suppose that $|T| \overset{\text{BR}}{=} 0$. Then it holds that $|T| \overset{\text{BDR}}{=} 0$ since BDR extends BR and further $T \overset{\text{BDR}}{=} \eta_{\vec{x}}[|T|] \overset{\text{BDR}}{=} \eta_{\vec{x}}[0] \overset{\text{BDR}}{=} 0$. We will prove the other direction by contraposition. For that, suppose that $\text{BR} \nvdash |T| \overset{\text{BR}}{=} 0$. By Theorem 21, that means that there is already a counterexample of $|T| \overset{\text{BR}}{=} 0$ within $\mathbb{2}$. If T is a term in $\vec{x}$, then $|T|$ is a term in $\vec{x}$, $\vec{x}$ and Z, but for clarity we will write $\vec{y}$ instead of $\vec{x}$. We therefore have tuples $\vec{X}$ and $\vec{Y}$ of $\mathbb{2}$ as well as $\hat{Z} \in \mathbb{2}$ such that $|T|\,\langle\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\rangle = 1$.

Consider then the switching algebra $\mathbb{S}_1$ of switching functions $\mathbb{2} \to \mathbb{2}$, equipped with the non-standard definition of z given by $z(0) := \hat{Z}$, $z(1) := \hat{Z} + 1$. We define the elements $\vec{f} := (f_1, \ldots, f_n)$ as follows:

$$f_i(0) := Y_i \qquad f_i(1) := \begin{cases} Y_i & \text{if } X_i = 0 \\ Y_i + 1 & \text{if } X_i = 1 \end{cases}$$

We will show by induction on the shape of T that $(T\langle\!\langle \vec{f} \rangle\!\rangle)(0) = |T| \, \langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle$:

(i) The case for $T = c$ where $c \in \{0, 1\}$ is clear and so are the inductive cases $T = S_1 S_2$ as well as $T = S_1 + S_2$.

(ii) If $T = z$, then $(z\langle\!\langle \vec{f} \rangle\!\rangle)(0) = z(0) = \hat{Z} = Z\langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle = |z| \, \langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle$.

(iii) If $T = x_i$, then $(x_i\langle\!\langle \vec{f} \rangle\!\rangle)(0) = f_i(0) = Y_i = y_i\langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle = |x_i| \, \langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle$.

(iv) If $T = \delta(x_i)$, then, by definition of the derivative in switching algebras, we have that

$$\left(\delta(x_i)\langle\!\langle \vec{f} \rangle\!\rangle\right)(0) = \delta(f_i) = \left\{ \begin{array}{l} 0 \text{ if } X_i = 0 \\ 1 \text{ if } X_i = 1 \end{array} \right\} = X_i = x_i\langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle = |\delta(x_i)| \, \langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle$$

Therefore it follows that $(T\langle\!\langle \vec{f} \rangle\!\rangle)(0) = |T| \, \langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle$, which now shows that $T\langle\!\langle \vec{f} \rangle\!\rangle \neq 0$, as $(T\langle\!\langle \vec{f} \rangle\!\rangle)(0) = |T| \, \langle\!\langle \vec{X}, \vec{Y}, \hat{Z} \rangle\!\rangle = 1$. Therefore $\mathbb{S}_1 \not\models T = 0$ which means that BDR $\not\vdash T = 0$, completing the proof. ∎

We can restate Theorem 59 in an equivalent, but slightly more useful way.

COROLLARY 60. Let S and T be flat terms. Then it holds that $S \overset{\text{BDR}}{=} T$ if and only if $|S| \overset{\text{BR}}{=} |T|$.

PROOF. The proof follows from Theorem 59 due to the fact that $S \overset{\text{BDR}}{=} T$ if and only if $S + T \overset{\text{BDR}}{=} 0$ as well as $|S| \overset{\text{BR}}{=} |T|$ if and only if $|S| + |T| \overset{\text{BR}}{=} 0$, i. e.

$$S \overset{\text{BDR}}{=} T \Leftrightarrow S + T \overset{\text{BDR}}{=} 0 \Leftrightarrow |S| + |T| = |S + T| \overset{\text{BR}}{=} 0 \Leftrightarrow |S| \overset{\text{BR}}{=} |T|$$

∎

Until now, $|\cdot|$ has only been defined for flat terms. Corollary 60, together with the help of Algorithm 47, now allows us to generalize the notion of $|\cdot|$ to all terms in a natural way by first applying $\downarrow$.

DEFINITION 61. Let T be any term. Then $\|T\| := |T\downarrow|$.

The next proposition states that this definition is natural in the sense that it also preserves equalities. This is not a trivial result, since arbitrary terms with z and δ can behave quite differently than terms with T_{BR}.

COROLLARY 62. Let S and T be any terms. Then it holds that $S \overset{\text{BDR}}{=} T$ if and only if $\|S\| \overset{\text{BR}}{=} \|T\|$.

PROOF. Since $S \overset{\text{BDR}}{=} S\downarrow$ and $T \overset{\text{BDR}}{=} S\downarrow$, it holds follows from Corollary 60 that

$$S \overset{\text{BDR}}{=} T \Leftrightarrow S{\downarrow} \overset{\text{BDR}}{=} T{\downarrow} \Leftrightarrow \|S\| = |S{\downarrow}| \overset{\text{BR}}{=} |T{\downarrow}| = \|T\|$$

∎

An expected special case of this is that, for BR-terms, T_{BDR} does not allow for any additional equalities over T_{BR}.

COROLLARY 63. Let S and T be BR-terms. Then $S \overset{\text{BDR}}{=} T$ if and only if $S \overset{\text{BR}}{=} T$.

PROOF. If $S \overset{\text{BR}}{=} T$, then clearly also $S \overset{\text{BDR}}{=} T$ since BDR extends BR. For the converse direction, suppose that $S \overset{\text{BDR}}{=} T$ and assume that S and T are terms of $\vec{x}$. Recall that, by Proposition 48, it holds that $U \overset{\text{BR}}{=} U{\downarrow}$ for all BR-terms U. Consider then the self-inverse substitution $\sigma := \{x_i \mapsto \bar{x}_\iota, \bar{x}_\iota \mapsto x_i \mid 0 < i \leq n\}$ for which it holds that ${}_\sigma[V] = \|V\|$ for all flat BR-terms V of $\vec{x}$. By Corollary 62 it holds that $\|S\| \overset{\text{BR}}{=} \|T\|$, and therefore

$$S \overset{\text{BR}}{=} S{\downarrow} = {}_{\sigma\sigma}[S{\downarrow}] = {}_\sigma[|S{\downarrow}|] = {}_\sigma[\|S\|] \overset{\text{BR}}{=} {}_\sigma[\|T\|] = {}_\sigma[|T{\downarrow}|] = {}_{\sigma\sigma}[T{\downarrow}] = T{\downarrow} \overset{\text{BR}}{=} T$$

which completes the proof. ∎

Next, we will show that Lemma 56 and Lemma 57 still hold for $\|\cdot\|$ in weaker version. However, we need a short lemma first.

LEMMA 64. Let T be a BR-term of $(\vec{x}, \vec{\bar{x}}, Z)$. Then it holds that ${}_{\eta_{\vec{x}}}[T{\downarrow}] \overset{\text{BDR}}{=} {}_{\eta_{\vec{x}}}[T]{\downarrow}$.

PROOF. We will show this by induction on the shape of T.

(i) If $T = c$ with $c \in \{0, 1\}$, then ${}_{\eta_{\vec{x}}}[c{\downarrow}] = c = {}_{\eta_{\vec{x}}}[T]{\downarrow}$.
(ii) If $T = Z$, then ${}_{\eta_{\vec{x}}}[Z{\downarrow}] = z = {}_{\eta_{\vec{x}}}[T]{\downarrow}$.
(iii) If $T = x_i$, for $0 < i \leq n$, then ${}_{\eta_{\vec{x}}}[x_i{\downarrow}] = \delta(x_i) = {}_{\eta_{\vec{x}}}[T]{\downarrow}$.
(iv) If $T = \bar{x}_i$, for $0 < i \leq n$, then ${}_{\eta_{\vec{x}}}[\bar{x}_i{\downarrow}] = x_i = {}_{\eta_{\vec{x}}}[\bar{x}_i]{\downarrow}$.
(v) Suppose $T = S_1 + S_2$, for flat terms S_1 and S_2 that satisfy the induction hypothesis. Then it holds that

$$\begin{aligned}
\eta_{\vec{x}}[T\downarrow] &= \eta_{\vec{x}}[S_1\downarrow \oplus S_2\downarrow] \\
&= \eta_{\vec{x}}[S_1\downarrow] \oplus \eta_{\vec{x}}[S_2\downarrow] \\
&\overset{\text{BDR}}{=} \eta_{\vec{x}}[S_1]\downarrow \oplus \eta_{\vec{x}}[S_2]\downarrow \\
&= \Big(\eta_{\vec{x}}[S_1] + \eta_{\vec{x}}[S_2]\Big)\downarrow \\
&= \eta_{\vec{x}}[T]\downarrow
\end{aligned}$$

where the second equality holds since clearly $\eta_{\vec{x}}$ and $\oplus$ commute in the same way $\eta_{\vec{x}}$ and $+$ do.

(vi) The statement holds for the case $T = S_1 \cdot S_2$ holds similarly.

Together, the statement for every T now follows by induction. ∎

PROPOSITION 65.

(i) For every term T of $\vec{x}$ it holds that $T \overset{\text{BDR}}{=} \eta_{\vec{x}}[\|T\|]$.

(ii) For every BR-term T of $(\vec{x}, \vec{\vec{x}}, Z)$ it holds that $T \overset{\text{BR}}{=} \|\eta_{\vec{x}}[T]\|$.

PROOF. *(i):* It holds, by Lemma 56, that

$$\eta_{\vec{x}}[\|T\|] = \eta_{\vec{x}}[|T\downarrow|] = T\downarrow \overset{\text{BDR}}{=} T$$

(ii): It holds, by Lemma 64 and Lemma 57, that

$$\|\eta_{\vec{x}}[T]\| = |\eta_{\vec{x}}[T]\downarrow| \overset{\text{BDR}}{=} |\eta_{\vec{x}}[T\downarrow]| \overset{\text{BR}}{=} T\downarrow \overset{\text{BR}}{=} T$$

Since this is an equality between BR-terms, the desired BR-equality now holds due to Corollary 63. ∎

In the following, we will show that the flat form $T\downarrow$ has properties analogous to Theorem 25. This will follow from Corollary 63 and the following lemmas:

LEMMA 66.

(i) Let T_1 and T_2 be flat terms. Then $|T_1\downarrow \oplus T_2\downarrow| = \|T_1\| \oplus \|T_2\|$.

(ii) Let M_1 and M_2 be monomial-like terms. Then $|T_1\downarrow \odot T_2\downarrow| = \|T_1\| \odot \|T_2\|$.

PROOF. *(i):* Note that $\|T_1\| \oplus \|T_2\| = |T_1\downarrow| \oplus |T_2\downarrow|$. Therefore Part (i) states that the application of $|\cdot|$ and $\oplus$ commute for flattened terms. If either $T_1\downarrow$ or $T_2\downarrow$ are 0, then the statement is obvious. For the general statement, follows, since a monomial-like summand

M of $T_1{\downarrow} + T_2{\downarrow}$ is removed by $\oplus$ on the left-hand side if and only if the monomial summand $|M|$ of $\|T_1\| + \|T_2\|$ is cancelled by $\oplus$ on the right-hand side. I. e. on both sides, the same monomials of $|T_1{\downarrow} + T_2{\downarrow}| = \|T_1\| + \|T_2\|$ are removed.

(ii): Note that $\|M_1\| \odot \|M_2\| = |M_1{\downarrow}| \odot |M_2{\downarrow}|$. By Lemma 49, it holds that $M_1{\downarrow}$ and $M_2{\downarrow}$ are also monomial-like, and therefore we can replace all the $\odot$ by $*$ for the sake of clarity. Then statement is clear if one of the terms $M_1{\downarrow}$ or $M_2{\downarrow}$ contains 0 or 1 as a BDR-atom. As in Part (i), the general statement follows, because an atom A of $M_1{\downarrow}$ and $M_2{\downarrow}$ gets removed by $*$ on the left-hand side if and only the atom $|A|$ gets removed by $*$ on the right-hand side, i. e. on both sides the same atoms of $|M_1{\downarrow} \cdot M_2{\downarrow}| = \|M_1\| \cdot \|M_2\|$ are removed. ∎

LEMMA 67. Let T be any term. Then $\|T\| = \|T\|{\downarrow}$.

PROOF. Let T be a term of $\vec{x}$. We will first show the statement for flat terms by induction:

(i) If $T = c \in \{0, 1\}$, then $\|T\| = T = \|T\|{\downarrow}$.

(ii) If $T = z$, then $\|T\| = Z = \|T\|{\downarrow}$.

(iii) If $T = x$ for a variable x, then $\|T\| = \bar{x} = \|T\|{\downarrow}$.

(iv) If $T = \delta(x)$ for a variable x, then $\|T\| = x = \|T\|{\downarrow}$.

(v) Suppose that $T = T_1 + T_2$ for flat terms T_1 and T_2 that satisfy the induction hypothesis. Then, with Lemma 66 as well as the induction hypothesis, it holds that
$$\|T\| = |T_1{\downarrow} \oplus T_2{\downarrow}| = \|T_1\| \oplus \|T_2\| = \|T_1\|{\downarrow} \oplus \|T_2\|{\downarrow} = (\|T_1\| + \|T_2\|){\downarrow} = \|T\|{\downarrow}$$

(vi) Suppose that $T = T_1 \cdot T_2$ with T_1 and T_2 as above. Since T is flat, this means that T_1 and T_2 are monomial-like. By Lemma 66 and the induction hypothesis, we have that
$$\|T\| = |T_1{\downarrow} \odot T_2{\downarrow}| = \|T_1\| \odot \|T_2\| = \|T_1\|{\downarrow} \odot \|T_2\|{\downarrow} = (\|T_1\| \cdot \|T_2\|){\downarrow} = \|T\|{\downarrow}$$

By induction the statement follows for all flat terms T. Now let T be any term. Then, by definition $\|T\| = |T{\downarrow}|$, and together with Lemma 50 and the above argument, it holds that
$$\|T\| = \|T{\downarrow}\| = \|T{\downarrow}\|{\downarrow} = \|T\|{\downarrow}$$
i. e. the general statement holds. ∎

THEOREM 68. Let S and T be any terms. Then it holds that $S \overset{\text{BDR}}{=} T$ if and only if $S{\downarrow} = T{\downarrow}$.

PROOF. Let S and T be terms of $\vec{x}$. Suppose that $S \overset{\text{BDR}}{=} T$. Then, by Corollary 62, it holds that $\|S\| \overset{\text{BR}}{=} \|T\|$. By Theorem 25, this means that $\|S\|{\downarrow} = \|T\|{\downarrow}$ and it follows with Lemma 67 that

$$S{\downarrow} = \eta_{\vec{x}}[|S{\downarrow}|] = \eta_{\vec{x}}[\|S\|] = \eta_{\vec{x}}[\|S\|{\downarrow}] = \eta_{\vec{x}}[\|T\|{\downarrow}] = \eta_{\vec{x}}[\|T\|] = \eta_{\vec{x}}[|T{\downarrow}|] = T{\downarrow}$$

The converse holds, since in this case $S \overset{\text{BDR}}{=} S{\downarrow} = T{\downarrow} \overset{\text{BDR}}{=} T$. ∎

2.4 Some Useful Substitutions

In this section, we will define some substitutions and state some propositions about them, that will help us later.

DEFINITION 69. Let $\vec{x}$ be variables. We define the following substitutions:

$$\kappa_{\vec{x}} := \left\{x_i \mapsto \delta\left(a_i^{\vec{x}}\right)z + \delta\left(b_i^{\vec{x}}\right) \mid 0 < i \leq n\right\}$$

$$\lambda_{\vec{x}} := \left\{a_i^{\vec{x}} \mapsto x_i, b_i^{\vec{x}} \mapsto (x_i + \delta(x_i)z)z \mid 0 < i \leq n\right\}$$

$$\nu_{\vec{x}} := \left\{a_i^{\vec{x}} \mapsto a_i^{\vec{x}} + \delta\left(\hat{a}_i^{\vec{x}}\right), b_i^{\vec{x}} \mapsto b_i^{\vec{x}} + \delta\left(\hat{b}_i^{\vec{x}}\right) \mid 0 < i \leq n\right\}$$

where all of the $a_i^{\vec{x}}$, $b_i^{\vec{x}}$, $\hat{a}_i^{\vec{x}}$ and $\hat{b}_i^{\vec{x}}$ are fresh variables different from the $\vec{x}$.

In the following we will always omit the superscript $\vec{x}$, and only use superscript $\vec{y}$ for the variables introduced by $\kappa_{\vec{y}}$, $\lambda_{\vec{y}}$, $\nu_{\vec{y}}$, etc, in case $\vec{x} \neq \vec{y}$.

The idea behind $\kappa_{\vec{x}}$ is that every element x of a Boolean ring can be presented as $cz + d$ with $c, d \in \mathrm{Ker}(\delta)$. And since every element of $\mathrm{Ker}(\delta)$ is in the image of δ, there are a and b such that $x = \delta(a)z + \delta(b)$. Since our intuition tells us that $\kappa_{\vec{x}}$ does not add or remove any information, we naturally expect it to be reversible. And it turns out that $\lambda_{\vec{x}}$ is exactly the desired left-inverse of $\kappa_{\vec{x}}$.

LEMMA 70. It holds that $\lambda_{\vec{x}}\kappa_{\vec{x}} \overset{\text{BDR}}{=} \mathrm{id}$.

PROOF. We need to show that $\lambda_{\vec{x}}\kappa_{\vec{x}}[x_i] \overset{\text{BDR}}{=} x_i$ for all $0 < i \leq n$. Fix such i. Then we have that

$$\begin{aligned}\lambda_{\vec{x}}\kappa_{\vec{x}}[x_i] &= \lambda_{\vec{x}}[\delta(a_i)z + \delta(b_i)] \\ &= \delta(x_i)z + \delta((x_i + \delta(x_i)z)z) \\ &\overset{\text{BDR}}{=} \delta(x_i)z + x_i + \delta(x_i)z \\ &\overset{\text{BDR}}{=} x_i\end{aligned}$$

Where the first BDR-equality holds since $x_i + \delta(x_i)z$ is δ-vanishing, and therefore $\delta((x_i + \delta(x_i)z)z) \overset{\text{BDR}}{=} x_i + \delta(x_i)z$. ∎

LEMMA 71. It holds that $\nu_{\vec{x}}\kappa_{\vec{x}} \overset{\text{BDR}}{=} \kappa_{\vec{x}}$

PROOF.

$$\nu_{\vec{w}}\kappa_{\vec{x}}[x_i] = \nu_{\vec{x}}[\delta(a_i)z + \delta(b_i)] = \delta(a_i + \delta(\hat{a}_i))z + \delta\big(b_i + \delta\big(\hat{b}_i\big)\big) \overset{\text{BDR}}{=} \delta(a_i)z + \delta(b_i) = \kappa_{\vec{x}}[x_i]$$

∎

Next, we will prove some more useful statements about the behaviour of our previously defined substitutions.

LEMMA 72. Let σ be a BR-substitution and let $_\sigma[x]$ be a term in $\vec{y}$. Then it holds that

$$\|_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[\delta(x)]\| \overset{\text{BR}}{=} {}_\sigma[x]$$

PROOF. We first prove the corresponding BDR-equality by induction on the shape of $_\sigma[x]$.

(i) If $_\sigma[x] = c$ for $c \in \{0, 1\}$, then $\|_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[\delta(x)]\| \overset{\text{BDR}}{=} c = {}_\sigma[x]$.

(ii) If $_\sigma[x] \overset{\text{BR}}{=} y$ for a variable y, then

$$\begin{aligned}\|_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[\delta(x)]\| &= \|_{\eta_{\vec{y}}\sigma}[\delta(xz)]\| \\ &= \|_{\eta_{\vec{y}}}[\delta(yz)]\| \\ &= \|\delta(\delta(y)z)\| \\ &\overset{\text{BDR}}{=} \|\delta(y)\| \\ &= y \\ &= {}_\sigma[x]\end{aligned}$$

(iii) If $_\sigma[x] = S_1 + S_2$ and suppose the hypothesis already holds for $\sigma_1 \coloneqq \{x \mapsto S_1\}$ and $\sigma_2 \coloneqq \{x \mapsto S_2\}$. Then we have that

$$\begin{aligned}
\|_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[\delta(x)]\| &= \|_{\eta_{\vec{y}}\sigma}[\delta(xz)]\| \\
&= \|_{\eta_{\vec{y}}}[\delta(S_1 + S_2)z]\| \\
&\overset{\text{BDR}}{=} \|_{\eta_{\vec{y}}}[\delta(S_1 z)]\| \oplus \|_{\eta_{\vec{y}}}[\delta(S_2 z)]\| \\
&= \|_{\eta_{\vec{y}}\sigma_1\varepsilon_{\vec{x}}}[\delta(x)]\| \oplus \|_{\eta_{\vec{y}}\sigma_2\varepsilon_{\vec{x}}}[\delta(x)]\| \\
&\overset{\text{BDR}}{=} {}_{\sigma_1}[x] \oplus {}_{\sigma_2}[x] \\
&= S_1 \oplus S_2 \\
&\overset{\text{BDR}}{=} S_1 + S_2 \\
&= {}_\sigma[x]
\end{aligned}$$

(iv) If $_\sigma[x] = S_1 \cdot S_2$ and suppose the hypothesis already holds for σ_1 and σ_2 as defined above. Then it holds that

$$\begin{aligned}
\|_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[\delta(x)]\| &= \|_{\eta_{\vec{y}}}[\delta(S_1 S_2 z)]\| \\
&= \|\delta\Big(_{\eta_{\vec{y}}}[S_1]_{\eta_{\vec{y}}}[S_2]z\Big)\| \\
&\overset{\text{BDR}}{=} \|_{\eta_{\vec{y}}}[S_1]_{\eta_{\vec{y}}}[S_2]\| \\
&= \|_{\eta_{\vec{y}}}[S_1]\| \odot \|_{\eta_{\vec{y}}}[S_2]\| \\
&\overset{\text{BDR}}{=} \|\delta\Big(_{\eta_{\vec{y}}}[S_1]z\Big)\| \odot \|\delta\Big(_{\eta_{\vec{y}}}[S_2]z\Big)\| \\
&= \|_{\eta_{\vec{y}}\sigma_1\varepsilon}[\delta(x)]\| \odot \|_{\eta_{\vec{y}}\sigma_2\varepsilon}[\delta(x)]\| \\
&\overset{\text{BDR}}{=} {}_{\sigma_1}[x] \odot {}_{\sigma_2}[x] \\
&= S_1 \odot S_2 \\
&\overset{\text{BDR}}{=} S_1 \cdot S_2 \\
&= {}_\sigma[x]
\end{aligned}$$

By induction it follows that $\|_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[\delta(x)]\| \overset{\text{BDR}}{=} {}_{\sigma}[x]$ for all BR-substitutions σ. Since this is an equality between BR-terms, by Corollary 63 it follows that $\|_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[\delta(x)]\| \overset{\text{BR}}{=} {}_{\sigma}[x]$. ∎

LEMMA 73. Let $T(\vec{x})$ be a benign term and σ a BR-substitution such that ${}_{\sigma}[\|T\|]$ is a term in $\vec{y}$. Then it holds that ${}_{\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}}[T] \overset{\text{BDR}}{=} {}_{\eta_{\vec{y}}\sigma}[\|T\|]$.

PROOF. We can prove this by induction on the shape of T. The base case $T = c$ for $c \in \{0, 1\}$ and the induction cases $T = S_1 + S_2$ and $T = S_1 S_2$ are immediate. The only non-trivial case is $T = \delta(x)$. Here it holds by Proposition 65 and Lemma 72 that

$$\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}[\delta(x)] \overset{\text{BDR}}{=} \eta_{\vec{y}}[\|\eta_{\vec{y}}\sigma\varepsilon_{\vec{x}}[\delta(x)]\|] \overset{\text{BDR}}{=} \eta_{\vec{y}}[{}_{\sigma}[x]] = \eta_{\vec{y}}\sigma[\|\delta(x)\|]$$

∎

LEMMA 74. Let $T(\vec{x})$ be a BDR-term and σ as well as τ BR-substitutions. Suppose that ${}_{\tau\kappa_{\vec{x}}}[T]$ is a term in $\vec{y}$ and ${}_{\sigma\tau\kappa_{\vec{x}}}[T]$ is a term in $\vec{v}$. If $\vec{w} := (\vec{a}, \vec{b})$, then it holds that:

$$\eta_{\vec{v}}\sigma\varepsilon_{\vec{y}}\eta_{\vec{y}}\tau\varepsilon_{\vec{w}}\kappa_{\vec{x}} \overset{\text{BDR}}{=} \eta_{\vec{v}}\sigma\tau\varepsilon_{\vec{w}}\kappa_{\vec{x}}$$

PROOF. It suffices to show that it holds for $T = x_i$. By induction it holds for all $T(\vec{x})$. Therefore, using Lemma 73 and Proposition 65:

$$\begin{aligned}
\eta_{\vec{v}}\sigma\varepsilon_{\vec{y}}\eta_{\vec{y}}\tau\varepsilon_{\vec{w}}\kappa_{\vec{x}}[x_i] &\overset{\text{BDR}}{=} \eta_{\vec{v}}\sigma\varepsilon_{\vec{y}}[\eta_{\vec{y}}\tau\varepsilon_{\vec{w}}\kappa_{\vec{x}}[x_i]] \\
&\overset{\text{BDR}}{=} \eta_{\vec{v}}\sigma[\|\eta_{\vec{y}}\tau\varepsilon_{\vec{w}}\kappa_{\vec{x}}[x_i]\|] \\
&\overset{\text{BDR}}{=} \eta_{\vec{v}}\sigma[\tau\varepsilon_{\vec{w}}\kappa_{\vec{x}}[x_i]] \\
&\overset{\text{BDR}}{=} \eta_{\vec{v}}\sigma\tau\varepsilon_{\vec{w}}\kappa_{\vec{x}}[x_i]
\end{aligned}$$

∎

2.5 Unification of Boolean Differential Rings

In this chapter we will prove our main result that the theory of Boolean rings has the unitary unification type. The proof is based on the fact that the BDR-equations $T = 0$

and ${}_{\kappa_{\vec{x}}}[T] = 0$ are equivalent. Since ${}_{\kappa_{\vec{x}}}[T]$ has all occurences of variables immediately enclosed by δ, there are benign terms A and B such that ${}_{\kappa_{\vec{x}}}[T] = Az + B$. And since $A \overset{\text{BDR}}{=} 0$ and $B \overset{\text{BDR}}{=} 0$ if and only if $\|A\| \overset{\text{BR}}{=} 0$ and $\|B\| \overset{\text{BR}}{=} 0$, this lets us reduce the BDR-unification problem $T = 0$ to the BR-unification problem $\{\|A\| = 0, \|B\| = 0\}$ that we already know how to solve.

We will first prove that we can construct from any BR-unifier of the system of BR-equations a BDR-unifier of the single BDR-equation, and vice versa. Then, we will show that the two constructions are inverse to each other. Finally, we will show that the first construction conserves the mgu-property, and therefore we can construct a BDR-mgu for the single BDR-equation in case it is unifiable. In the following, for the sake of convenience, we define $\vec{w} := (\vec{a}, \vec{b})$.

THEOREM 75. Let $T(\vec{x})$ be any term, and $A(\vec{w})$ and $B(\vec{w})$ benign such that ${}_{\kappa}[T] \overset{\text{BDR}}{=} Az + B$. If σ is a BR-unifier of $\{\|A\| = 0, \|B\| = 0\}$ such that ${}_{\sigma}[\|A\|]$ and ${}_{\sigma}[\|B\|]$ are terms in $\vec{y}$, then $\overline{\sigma} := \eta_{\vec{y}}\sigma\varepsilon_{\vec{w}}\kappa_{\vec{x}}$ is a BDR-unifier of $T = 0$.

PROOF. By Lemma 73 it holds that

$$\eta_{\vec{y}}\sigma\varepsilon_{\vec{w}}\kappa_{\vec{x}}[T] \overset{\text{BDR}}{=} \eta_{\vec{y}}\sigma\varepsilon_{\vec{w}}[Az + B] \overset{\text{BDR}}{=} \eta_{\vec{y}}\sigma[\|Az + B\|] \overset{\text{BDR}}{=} \eta_{\vec{y}}\sigma[\|A\|]Z + \eta_{\vec{y}}\sigma[\|B\|] \overset{\text{BDR}}{=} 0$$

since $\|Az + B\| = \|A\| \odot Z \oplus \|B\| \overset{\text{BDR}}{=} \|A\|\, Z + \|B\|$. ∎

THEOREM 76. Let $T(\vec{x})$ be any term, and $A(\vec{w})$ and $B(\vec{w})$ benign such that ${}_{\kappa}[T] \overset{\text{BDR}}{=} Az + B$. If τ is a BDR-unifier of $T = 0$, then there is a BR-unifier $\|\tau\|$ of $\{\|A\| = 0, \|B\| = 0\}$ such that $\tau \overset{\text{BDR}}{=} \overline{\|\tau\|}$.

PROOF. Let $\vec{y}$ be variables such that ${}_{\tau}[T]$ is a term in $\vec{y}$. For every i, we define the substitution $\|\tau\|$ as

$${}_{\|\tau\|}[w_i] := \|_{\tau\lambda_{\vec{x}}\eta_{\vec{w}}}[w_i]\|$$

such that $\tau\lambda_{\vec{x}}\eta_{\vec{w}} \overset{\text{BDR}}{=} \eta_{\vec{y}}\,\|\tau\|$. To show that $\|\tau\|$ is a unifier of $\{\|A\| = 0, \|B\| = 0\}$, first note that:

$$\begin{aligned}
{}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|A\|\,z+\|B\|] &\overset{\text{BDR}}{=} {}_{\kappa_{\vec{y}}\tau\lambda_{\vec{x}}\eta_{\vec{w}}}[\|A\|\,z+\|B\|] \\
&\overset{\text{BDR}}{=} {}_{\kappa_{\vec{y}}\tau\lambda_{\vec{x}}}[Az+B] \\
&\overset{\text{BDR}}{=} {}_{\kappa_{\vec{y}}\tau}[T] \\
&\overset{\text{BDR}}{=} 0
\end{aligned}$$

Since it holds that ${}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|A\|\,z+\|B\|] \overset{\text{BDR}}{=} {}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|A\|]z + {}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|B\|]$ and by Proposition 53, ${}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|A\|]\!\downarrow$ as well as ${}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|B\|]\!\downarrow$ are benign and therefore δ-vanishing, by Proposition 42, this means that we have that

$${}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|A\|] \overset{\text{BDR}}{=} {}_{\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|B\|] \overset{\text{BDR}}{=} 0$$

and therefore

$${}_{\eta_{\vec{y}}\,\|\tau\|}[\|A\|] \overset{\text{BDR}}{=} {}_{\lambda_{\vec{y}}\kappa_{\vec{y}}\eta_{\vec{y}}\,\|\tau\|}[\|A\|] \overset{\text{BDR}}{=} {}_{\lambda_{\vec{y}}}[0] \overset{\text{BDR}}{=} 0$$

which with Lemma 57 as well as Theorem 59 further gives us:

$${}_{\|\tau\|}[\|A\|] \overset{\text{BR}}{=} \|{}_{\eta_{\vec{y}}\,\|\tau\|}[\|A\|]\| \overset{\text{BR}}{=} 0$$

Similarly, we get that ${}_{\|\tau\|}[\|B\|] \overset{\text{BR}}{=} 0$, i. e. $\|\tau\|$ is a BR-unifier of $\{\|A\| = 0, \|B\| = 0\}$.

To show that $\tau \overset{\text{BDR}}{=} \overline{\|\tau\|}$, first, define the substitution ψ for all i by ${}_{\psi}[\hat{w}_i] \coloneqq {}_{\tau\lambda_{\vec{x}}}[w_i](z+1)$. Then, consider, by Lemma 41:

$$\begin{aligned}
{}_{\tau\lambda_{\vec{x}}}[w_i] &\overset{\text{BDR}}{=} \delta\Big({}_{\tau\lambda_{\vec{x}}}[w_i]\Big)z + \delta\Big({}_{\tau\lambda_{\vec{x}}}[w_i](z+1)\Big) \\
&\overset{\text{BDR}}{=} {}_{\tau\lambda_{\vec{x}}\eta_{\vec{w}}}[w_i]z + \delta\big({}_{\psi}[\hat{w}_i]\big) \\
&\overset{\text{BDR}}{=} {}_{\eta_{\vec{y}}\|\tau\|}[w_i]z + {}_{\psi}[\delta(\hat{w}_i)] \\
&\overset{\text{BDR}}{=} {}_{\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}}[w_i] + {}_{\psi}[\delta(\hat{w}_i)] \\
&\overset{\text{BDR}}{=} {}_{\psi\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}}[w_i] + {}_{\psi\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}}[\delta(\hat{w}_i)] \\
&\overset{\text{BDR}}{=} {}_{\psi\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}}[w_i + \delta(\hat{w}_i)] \\
&\overset{\text{BDR}}{=} {}_{\psi\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}\nu_{\vec{x}}}[w_i]
\end{aligned}$$

i. e. we have that $\tau\lambda_{\vec{x}} \overset{\text{BDR}}{=} \psi\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}\nu_{\vec{x}}$. Therefore, by the definitions as well as Lemma 70 and Lemma 71, we have that:

$$\tau \overset{\text{BDR}}{=} \tau\lambda_{\vec{x}}\kappa_{\vec{x}} \overset{\text{BDR}}{=} \psi\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}\nu_{\vec{x}}\kappa_{\vec{x}} \overset{\text{BDR}}{=} \psi\eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}\kappa_{\vec{x}} \overset{\text{BDR}}{=} \eta_{\vec{y}}\|\tau\|\varepsilon_{\vec{w}}\kappa_{\vec{x}} \overset{\text{BDR}}{=} \overline{\|\tau\|}$$

which concludes the proof. ∎

THEOREM 77. Let $T(\vec{x})$ be any BDR-term. The equation $T = 0$ has either no or exactly one most general unifier.

PROOF. Let $A(\vec{a}, \vec{b})$ and $B(\vec{a}, \vec{b})$ be benign such that ${}_{\kappa}[T] \overset{\text{BDR}}{=} Az + B$ and define $\vec{w} \coloneqq (\vec{a}, \vec{b})$. Suppose $T = 0$ is BDR-unifiable. Then, by Theorem 76, it holds that $\{\|A\| = 0, \|B\| = 0\}$ is BR-unifiable. Since unification of Boolean rings is unitary, there exists a BR-mgu σ. If $\vec{y}$ is such that ${}_{\sigma}[\|A\|]$ and ${}_{\sigma}[\|B\|]$ are terms in $\vec{y}$, then, by Theorem 75, it holds that $\overline{\sigma} = \eta_{\vec{y}}\sigma\varepsilon_{\vec{w}}\kappa_{\vec{x}}$. We claim that $\overline{\sigma}$ is in fact the BDR-mgu of $T = 0$.

To prove this, let τ be another BDR-unifier of $T = 0$. Then it holds by Theorem 76 that $\|\tau\|$ is a unifier of $\{\|A\| = 0, \|B\| = 0\}$ and $\tau \overset{\text{BDR}}{=} \overline{\|\tau\|}$. Since σ is an mgu, it holds that there is a BR-substitution φ such that $\|\tau\| \overset{\text{BR}}{=} \varphi\sigma$. If $\vec{u}$ are such that ${}_{\tau}[T]$ is a term in $\vec{u}$, then It follows by Lemma 74 that

$$\begin{aligned}
\tau &\overset{\text{BDR}}{=} \overline{\|\tau\|} \\
&\overset{\text{BDR}}{=} \eta_{\vec{u}}\|\tau\|\varepsilon_{\vec{w}}\kappa_{\vec{x}} \\
&\overset{\text{BDR}}{=} \eta_{\vec{u}}\varphi\sigma\varepsilon_{\vec{w}}\kappa_{\vec{x}} \\
&\overset{\text{BDR}}{=} \eta_{\vec{u}}\varphi\varepsilon_{\vec{y}}\eta_{\vec{y}}\sigma\varepsilon_{\vec{w}}\kappa_{\vec{x}} \\
&\overset{\text{BDR}}{=} \eta_{\vec{u}}\varphi\varepsilon_{\vec{y}}\overline{\sigma}
\end{aligned}$$

and therefore $\overline{\sigma}$ is at least as general as τ, i. e. together $\overline{\sigma}$ is the mgu of $T = 0$. ∎

COROLLARY 78. Unification of Boolean differential rings is unitary.

PROOF. Using Theorem 15 this is now an immediate consequence of Theorem 77. ∎

The construction of $\overline{\sigma}$ in Theorem 75 provides a straightforward way to specify a unification algorithm for Boolean differential rings.

ALGORITHM 79. Let $T(\vec{x})$ be a BDR-term. Suppose that split is a function that, using Proposition 54, returns, for every BDR term with all variables immediately enclosed by δ, a tuple (A, B) of benign terms such that $T \overset{\text{BDR}}{=} Az + B$. Suppose that $\mathsf{unify}_{\text{BR}}$ is a function returning for every BR-term t a BR-mgu of $t = 0$ in case it is unifiable and $\bot$ otherwise. Then consider the function $\mathsf{unify}^2_{\text{BR}}$, defined using Algorithm 16 and the base case $\mathsf{unify}_{\text{BR}}$. Then we specify the function $\mathsf{unify}_{\text{BDR}}$ that returns for T a BDR-unifier of $T = 0$ in case that it is unifiable, and $\bot$ otherwise by

$$
\begin{array}{l}
\mathsf{unify}_{\text{BDR}}(T) := \\
\quad \textbf{let } (A, B) := \mathsf{split}({}_{\kappa_{\vec{x}}}[T]) \\
\quad \textbf{in let } \sigma := \mathsf{unify}^2_{\text{BR}}(\|A\|, \|B\|) \\
\quad\quad \textbf{in } \eta_{(\vec{a},\vec{b})}\sigma\varepsilon_{(\vec{a},\vec{b})}\kappa_{\vec{x}}
\end{array}
$$

Lastly, the function $\mathsf{unify}^n_{\text{BDR}}$, specified in Algorithm 16 using $\mathsf{unify}_{\text{BDR}}$ from Algorithm 79 as the base case, provides, for $A_1, \ldots, A_n$ BDR-terms, either a BDR-mgu of the system of equations $\{A_1 = 0, \ldots, A_n = 0\}$ in case it is BDR-unifiable, and $\bot$ otherwise.

Example

As an example, consider the equation $\delta(x) = y$. The equation is clearly unifiable and we expect the mgu to be $\tilde{\tau} := \{y \mapsto \delta(x)\}$. To calculate the mgu according to Algorithm 79, let $T := \delta(x) + y$ be a term of $\vec{x} := (x, y)$. First we see that:

$$
{}_{\kappa_{\vec{x}}}[\delta(x) + y] = \delta(\delta(a)z + \delta(b)) + (\delta(c)z + \delta(d)) \overset{\text{BDR}}{=} \delta(a) + \delta(c)z + \delta(d)
$$

with $\kappa_{\vec{x}} = \{x \mapsto \delta(a)z + \delta(b), y \mapsto \delta(c)z + \delta(d)\}$. Then $A := \delta(c)$ and $B := \delta(a) + \delta(d)$ are benign terms of $\vec{w} := (a, b, c, d)$ such that ${}_{\kappa_{\vec{x}}}[T] \overset{\text{BDR}}{=} Az + B$. Now it holds that $\tau_1 := \{c \mapsto 0\}$ is the BR-mgu of $\|A\| = 0$, and further $\sigma := \tau_2 := \{c \mapsto 0, a \mapsto d\}$ the BR-mgu of $\{\|A\| = 0, \|B\| = 0\}$. Then it holds that

$$
\begin{aligned}
\tau &:= \eta_{\vec{w}}\sigma\varepsilon_{\vec{w}}\kappa_{\vec{x}} \\
&= \eta_{\vec{w}}\sigma\varepsilon_{\vec{w}}\{x \mapsto \delta(a)z + \delta(b), y \mapsto \delta(c)z + \delta(d)\} \\
&= \eta_{\vec{w}}\sigma\{x \mapsto \delta(az)z + \delta(bz), y \mapsto \delta(cz)z + \delta(dz)\} \\
&= \eta_{\vec{w}}\{x \mapsto \delta(dz)z + \delta(bz), y \mapsto \delta(0z) + \delta(dz)\} \\
&= \{x \mapsto \delta(\delta(d)z)z + \delta(\delta(b)z), y \mapsto \delta(0z) + \delta(\delta(d)z)\} \\
&\overset{\text{BDR}}{=} \{x \mapsto \delta(d)z + \delta(b), y \mapsto \delta(d)\} =: \tau'
\end{aligned}
$$

Clearly, $\tau' \neq \tilde{\tau}$, but we have that $\tau' \leq \tilde{\tau}$, since for the substitution $\lambda' \coloneqq \{d \mapsto x, b \mapsto (x + \delta(x)z)z\}$ we have that:

$$\begin{aligned}
\lambda'\tau' &= \lambda'\{x \mapsto \delta(d)z + \delta(b), y \mapsto \delta(d)\} \\
&= \{x \mapsto \delta(x)z + \delta((x + \delta(x)z)z), y \mapsto \delta(x)\} \\
&\overset{\text{BDR}}{=} \{x \mapsto \delta(x)z + x + \delta(x)z, y \mapsto \delta(x)\} \\
&\overset{\text{BDR}}{=} \{x \mapsto x, y \mapsto \delta(x)\} \\
&= \{y \mapsto \delta(x)\}
\end{aligned}$$

Conversely, it also holds that $\tilde{\tau} \leq \tau'$, since for the substitution $\kappa' \coloneqq \{x \mapsto \delta(d)z + \delta(b)\}$ it holds that:

$$\begin{aligned}
\kappa'\tilde{\tau} &= \kappa'\{y \mapsto \delta(x)\} \\
&= \{x \mapsto \delta(d)z + \delta(b), y \mapsto \delta(\delta(d)z + \delta(b)) \\
&\overset{\text{BDR}}{=} \{x \mapsto \delta(d)z + \delta(b), y \mapsto \delta(d)\}
\end{aligned}$$

Since $\tau \overset{\text{BDR}}{=} \tau'$, this shows that in our example Algorithm 79 indeed produces the expected mgu.

Conclusion

In this thesis we have shown that the unification theory of Boolean differential rings and Boolean differential algebras can be reduced to the unification theory of Boolean rings and Boolean algebras. While the possibility of such a reduction was expected by the way Boolean differential rings are defined via Boolean rings, finding the reduction and proving the relationship turned out to be non-trivial. The fact that the unification of Boolean differential rings is unitary means practically that for every unifiable system of equations there is a most general unifier that will generate all possible solutions.

Due to how the above reduction to Boolean rings works, we were able to provided algorithms for finding the mgu of single BDR-equations as well as systems of BDR-equations. These algorithms are based on the respective algorithms of Boolean differential rings. Having such a unification algorithm significantly simplifies the search for possible solutions.

In addition to this, we have also shown that, in fact, terms of Boolean differential rings and Boolean rings are more closely related than it seems. We showed that, like terms of Boolean rings have a unique polynomial form, terms of Boolean differential rings have a unique flat form that coincides with the polynomial form on z-free and δ-free terms. Moreover, we showed that terms of Boolean differential rings relate to terms of Boolean rings by means of $\|\cdot\|$ in a way that respects the equalities of either theory.

A topic that has not been covered by this thesis is the theory of Boolean rings with (finitely) many derivatives. Such a theory has been completely axiomatized by F. Weitkämper [3], and also B. Steinbach and C. Posthoff [1] cover switching algebras with multiple vectorial derivatives. Since they are defined via Boolean rings in a similar way to Boolean differential rings, it would be natural, if the unification theory of such a theory would behave in a similar way. However, this shall be the content of some future work.

Bibliography

[1] B. Steinbach and C. Posthoff, *Logic Functions and Equations*, 3rd ed. Springer, Cham, 2022. doi: 10.1007/978-3-030-88945-6.

[2] B. Steinbach and C. Posthoff, *Boolean Differential Equations*. Morgan & Claypool Publishers, 2013. doi: 10.2200/S00511ED1V01Y201305DCS042.

[3] F. Weitkämper, "Axiomatizing Boolean Differentiation," 2021, *Springer International Publishing*. doi: 10.1007/978-3-030-68071-8_4.

[4] U. Martin and T. Nipkow, "Boolean Unification – The Story So Far," *Journal of Symbolic Computation*, vol. 7, pp. 275–293, 1989.

[5] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical Logic*, 3rd ed. Springer, Cham, 2021. doi: 10.1007/978-3-030-73839-6.

[6] F. Baader and T. Nipkow, *Term Rewriting and All That*. Cambridge University Press, 1998.

[7] U. Martin and T. Nipkow, "Unification in Boolean Rings," *Journal of Automated Reasoning*, vol. 4, pp. 381–396, 1988.