Journal of Automated Reasoning 4 (1988) 381–396.
© 1988 *by Kluwer Academic Publishers.*

Unification in Boolean Rings

URSULA MARTIN[*] and TOBIAS NIPKOW[**]
Department of Computer Science, University of Manchester, Manchester M13 9PL U.K.

(Received: 24 June 1987)

Abstract. We show that two Boolean terms which are unifiable have a most general unifier, which can be described using the terms themselves and a single unifier. Techniques for finding a single unifier are given.

Key words. Boolean ring, Boolean algebra, unification, string equations.

1. Introduction

Unification, or the solution of equations, in particular algebraic theories has attracted a great deal of attention among computer scientists in recent years, as it is a basic inference mechanism in algebraic manipulation of formulae, automated reasoning and some programming languages. A detailed account is given in survey paper [16].

This paper is concerned with unifying Boolean terms, such as those arising in set theory, and the propositional and predicate calculus. Rather than working with union and intersection we take as our primitive operators on sets symmetric difference, denoted by $+$, and intersection, denoted by $*$ or just by concatenation. This makes the terms we are looking at into a Boolean ring, that is, a commutative ring in which every element x satisfies $x * x = x$ and $x + x = 0$. The empty set corresponds to 0 and the universal set to 1.

This way of dealing with Boolean terms appeared in Boole's book, *The Mathematical Analysis of Logic*, in 1847. A comprehensive account of Boole's work is given in Hailpern [3]. It gives rise to a rather convenient decision procedure for the propositional calculus. For $+$ represents *exclusive or*, $*$ represents *and* and 0 and 1 represent *false* and *true* respectively. Then we can transform any proposition into a polynomial in the Boolean ring by replacing $\neg p$ by $1 + p$ and $p \wedge q$ by $p * q$ and so on, and the proposition will be a tautology if and only if the polynomial is identically equal to 1. For example $(p \to q) \to ((p \vee r) \to (q \vee r))$ becomes

$$1 + (1 + p + pq) + (1 + p + pq)(1 + (p + r + pr) +$$
$$+ (p + r + pr)(q + r + qr)),$$

which reduces to 1 after multiplying up and simplifying using $x * x = x$ and $1 + 1 = 0$. This procedure is also described in Herbrand's thesis [4], and in [19] and [8].

[*] Current address: Department of Computer Science, Royal Holloway & Bedford New College, University of London, Egham Hill, Egham, Surrey, TW20 0EX, U.K.
[**] Current address: Laboratory for Computer Science, MIT, 545 Technology Square, Cambridge, MA 01239, U.S.A.

Boole also investigated solving equatins, or unification. His method involved successive elimination of variables, and leads to a simple test for the existence of a solution.

THEOREM 1 (Boole). *The equation*

$$f(x_1, \ldots, x_n) = 0$$

over the Boolean ring B has a solution if and only if

$$\prod f(a_1, \ldots, a_n) = 0,$$

where the product is taken over all elements $(a_1, \ldots, a_n)$ *of* $\{0, 1\}^n$.

Löwenheim [10] gave a formula for the most general solution of a Boolean equation, expressed in terms of a particular solution. Expressed in Boolean ring terms this is

THEOREM 2 (Löwenheim). *Let* $s = s(x_1, \ldots, x_n)$ *and* $t = t(x_1, \ldots, x_n)$ *be two terms over a Boolean ring B, and let* $b_1, \ldots, b_n$ *be elements of B with*

$$s(b_1, \ldots, b_n) = t(b_1, \ldots, b_n).$$

Then the substitution

$$x_i \to x_i' + (s(x_1', \ldots, x_n') + t(x_1', \ldots, x_n'))(x_i' + b_i)$$

is the most general unifier of s and t.

For example, let $s = ax + by$, $t = a$. One solution to $s = t$ is

$$x \to a, \qquad y \to 0.$$

Thus $ax + by$ and a have the most general unifier

$$x \to x' + (a + ax' + by')(x' + a),$$

$$y \to y' + (a + ax' + by')(y' + 0)$$

which simplifies to

$$x \to x' + ax' + bx'y' + aby' + a,$$

$$y \to y' + ay' + by' + ax'y'.$$

These results, and many others, including techniques for finding a particular solution, can be found in Rudeanu's book [15]. Löwenheim's theorem has been rediscovered many times, for example in [11]. Boole's technique has been used in hardware verification in [2].

We shall build on this work by describing a method for finding particular solutions for any equation over any Boolean ring. Taken with Theorem 2, this gives an algorithm for finding the most general unifier of two Boolean terms. Boolean rings are described in Section 2, and Löwenheim's theorem is proved in Section 3. A normal form for the elements of a Boolean ring is given in Section 4, and the algorithm is in Section 5. In Section 6 we discuss how our method is used for unification in sets and in formulae of the propositional calculus.

2. Boolean Rings

In this section and the next we collect some background material about Boolean rings, in particular two kinds of canonical form and a lemma which leads to a straightforward proof of Löwenheim's theorem.

A set B containing an element 0 is a *Boolean Ring* under the operations $+$ and $*$ if for all a, b, $c \in B$ we have

$$\left.\begin{aligned} a + b &= b + a \\ (a + b) + c &= a + (b + c) \\ a + 0 &= a \\ a + (-a) &= 0 \\ (a * b) * c &= a * (b * c) \\ a * (b + c) &= a * b + a * c \\ (a + b) * c &= a * c + b * c \\ a * a &= a \end{aligned}\right\} E,$$

where 0 is the zero element and $-a$ is the additive inverse of a. It then follows that $*$ is commutative and every element is its own additive inverse, that is

$$a * b = b * a$$

and

$$a + a = 0.$$

An element 1 of B with the property that

$$1 * a = a * 1 = a$$

for all a in A is called an identity element. In the sequel we will repeatedly make use of the identities $a * (1 + a) = 0$, and $a^k = a$ for $k \neq 0$. The Boolean ring with two elements, 0 and 1, will be denoted by F. In the sequel we work only with finite Boolean rings, which always have an identity element.

For our purposes there are two important examples. The power set $\mathscr{P}(S)$ of a set S with n elements forms a Boolean ring with 2^n elements under the operations of symmetric difference $(+)$ and intersection $(*)$, where $1 = S$ and $0 = \varnothing$, the empty set. The set of all well-formed formulae of the propositional calculus on set of n symbols for propositions forms a Boolean ring with 2^n elements under the operations of exclusive or $(+)$ and conjunction $(*)$, where 1 is *true* and 0 is *false*.

It is a consequence of the following theorem that these two are isomorphic.

THEOREM 3 (Stone). *Any finite Boolean ring is isomorphic to the power set of a set.*

If C is a set with n elements we may form the free algebra $\mathscr{T}(C, \Sigma)_E$ over C, which is just the term algebra over C with signature $\Sigma = \{+, *, 0, 1\}$, factored by the congruence induced by the equations E above. Any element b of $\mathscr{T}(C, \Sigma)_E$ can be expressed, by repeatedly applying the distributive law, as

$$b = b_0 + b_1 v_1 + \cdots + b_n v_n$$

where $b_i \in F$ and each v_i is a product of elements of C, in which each element of C appears at most once. Thus each v_i is of the form

$$v_U = \prod_{x \in U} x = \prod_{x \in C} x^{e_x},$$

where U is a non-empty finite subset of C, and $e_x = 1$ if $x \in U$ and $e_x = 0$ otherwise. If we define $v_\varnothing$ to be 1, we obtain

$$b = \sum_{U \subseteq C} b_U v_U,$$

where each b_U is an element of F. The 2^n elements v_U form a basis for $\mathscr{T}(C, \Sigma)_E$ as a vector space over F, and $\mathscr{T}(C, \Sigma)_E$ has 2^{2^n} elements.

A Boolean ring B is said to be *generated* over F by a subset C if each element b of B can be written as a sum of products of elements of C, that is

$$b = \sum_{U \subseteq C} b_U v_U$$

where

$$v_U = \prod_{x \in U} x, \qquad v_\varnothing = 1 \quad \text{and} \quad b_U \in F.$$

Thus $\mathscr{T}(C, \Sigma)_E$ is generated by C.

A Boolean ring B is often described in terms of a set of generators $C = \{c_1, \ldots, c_n\}$ and relations $w_1 = 0, \ldots, w_k = 0$ on terms w_i. Formally we write

$$B = \langle c_1, \ldots, c_n | w_1, \ldots, w_k \rangle.$$

This means that B is isomorphic to the quotient of $\mathscr{T}(C, \Sigma)_E$ by the subring of $\mathscr{T}(C, \Sigma)_E$ generated by the elements $w_1, \ldots, w_k$. Thus if ϕ is the natural homomorphism from $\mathscr{T}(C, \Sigma)_E$ onto B, B is generated by $\{\mathrm{c}_1\phi, \ldots, c_n\phi\}$. In practice we often drop all mention of ϕ and refer to the c_i as elements of B.

For example, the Boolean ring Q generated by a and b subject to $ab + a = O$ consists of the 8 elements

$$\{ra\phi b\phi + s(a\phi + 1)b\phi + t(a\phi + 1)(b\phi + 1) | r, s, t \in F\},$$

which are all distinct. It is isomorphic to the quotient of $\mathscr{T}(\{a, b\}, \Sigma)_E$ by the subring $\{ab + a, O\}$.

We now define a subset of a Boolean ring called an orthogonal basis, which gives rise to a normal form for the elements.

A subset $D = \{d_1, \ldots, d_n\}$ of B is called an *orthogonal basis* for B if

(a) D is a *basis* for B as a vector space over F. This means that each $b \in B$ can be expressed as a linear combination of elements of D,

$$b = \sum_{i=1}^{n} b_i d_i$$

where $b_i \in F$, and that the elements of D are linearly independent, that is,

$$0 = \sum_{i=1}^{n} b_i d_i$$

if and only if each $b_i = 0$.

(b) The elements of D are *orthogonal*, that is,

$$d_i d_j = 0 \quad \textit{for } i \neq j.$$

Thus

$$D = \{ab, (a + 1)b, (a + 1)(b + 1)\}$$

is an orthogonal basis for the Boolean ring Q above.

It follows from Stone's theorem that the finite Boolean ring B is isomorphic to the power set of a set, and so it must contain a subset of elements which correspond to the singleton sets under this isomorphism. In fact this subset is just the orthogonal basis. In section 4 we shall give a direct proof that an orthogonal basis always exists and is unique.

THE POLYNOMIAL FORM OF AN ELEMENT

To prove Löwenheim's theorem we need to investigate a different normal form, the polynomial form, for certain Boolean rings. Let B be any Boolean ring, V a set of symbols not occurring in B and $B[V]$ the free Boolean ring over V generated by V. In general B will be a homomorphic image of $\mathscr{T}(D, \Sigma)_E$ for some D, and $B[V]$ will be a homomorphic image of $\mathscr{T}(D \cup V, \Sigma)_E$.

Any element b of $B[V]$ can be expressed as

$$b = b_0 + b_1 v_1 + \cdots + b_n v_n$$

where $b_i \in B$ and each v_i is of the form

$$v_U = \prod_{x \in U} x = \prod_{x \in C} x^{e_x},$$

where U is a non-empty finite subset of C, and $e_x = 1$ if $x \in U$ and $e_x = 0$ otherwise.

If we define $v_\varnothing$ to be 1, we obtain

$$b = \sum_{U \subseteq C} b_U v_U,$$

where each b_U is an element of B. We call this form the *polynomial form* of b. Two elements with the same polynomial form are equal. We use the polynomial form in the next section to prove Löwenheim's theorem.

3. Proof of Löwenheim's Theorem

If b is in $B[V]$ and $b_{\varnothing} = 0$ then b is said to be *homogeneous.*

We can consider an element u of $B[V]$ as a function of the elements $x_1, \ldots, x_k$ of C, and as a map from $B[V]^k$ to $B[V]$ and write

$$u = u(x_1, \ldots, x_k) = u(\underline{x}).$$

Similarly $u(a\underline{x} + b\underline{y})$ denotes $u(ax_1 + by_1, \ldots, ax_k + by_k)$ where a, b, x_i, y_i are in $B[V]$. In this notation, $u(\underline{x})$ is homogeneous if and only if $u(\underline{0}) = 0$.

The following lemma gives a useful property of homogeneous terms which we shall use frequently.

LEMMA 1. *Let $u(\underline{x})$ be homogeneous. Then*

1. *if b is in B then $bu(\underline{x}) = u(b\underline{x})$*
2. *if $\underline{x} = b_1\underline{x}_1 + \cdots + b_n\underline{x}_n$ and $b_ib_j = 0$ for $i \neq j$ then*

$$u(\underline{x}) = b_1u(\underline{x}_1) + \cdots + b_nu(\underline{x}_n)$$

Proof

1. We have

$$u(\underline{x}) = \sum_{i=1}^{n} a_i \prod_{x \in V} x^{e_{ix}}$$

where for each i not all the e_{ix} are 0. Then

$$\begin{aligned} bu(\underline{x}) &= \sum_{i=1}^{n} a_i b \prod_{x \in V} x^{e_{ix}} \\ &= \sum_{i=1}^{n} a_i b^{k_i} \prod_{x \in V} (x)^{e_{ix}} \\ &= \sum_{i=1}^{n} a_i \prod_{x \in V} (bx)^{e_{ix}} \\ &= u(b\underline{x}) \end{aligned}$$

since for each value of i we have $b = b^{k_i}$ where $k_i = \Sigma_{x \in V} e_{ix}$.

2. Observe that $b_i\underline{x} = b_i\underline{x}_i$ for each i. Then

$$\begin{aligned} &b_1u(\underline{x}_1) + \cdots + b_nu(\underline{x}_n) \\ &\quad = u(b_1\underline{x}_1) + \cdots + u(b_n\underline{x}_n) \\ &\quad = u(b_1\underline{x}) + \cdots + u(b_n\underline{x}) \\ &\quad = (b_1 + \cdots + b_n)u(\underline{x}) \\ &\quad = u((b_1 + \cdots + b_n)\underline{x}) \\ &\quad = u(b_1\underline{x}_1 + \cdots + b_n\underline{x}_n). \end{aligned}$$ □

We can now prove Löwenheim's theorem rather easily.

THEOREM 4. *Let $s(\underline{x}), t(\underline{x}) \in B, \underline{w} \in B^n$ such that $s(\underline{w}) = t(\underline{w})$. Then the substitution*

$$\underline{y} = \underline{x} + (s(\underline{x}) + t(\underline{x}))(\underline{x} + \underline{w})$$

is a mgu of the two terms $s(\underline{x})$ and $t(\underline{x})$.

Proof. First we show that the above substitution is indeed a unifier. We can write

$$s(\underline{x}) + t(\underline{x}) = u(\underline{x}) + a,$$

where $u(\underline{x})$ is homogeneous and $a \in B$. Then $u(\underline{w}) = a$, since $s(\underline{w}) = t(\underline{w})$.

$$\begin{aligned} s(\underline{y}) + t(\underline{y}) &= u(\underline{y}) + a = u(\underline{x} + (u(\underline{x}) + a)(\underline{x} + \underline{w})) + a \\ &= u((1 + u(\underline{x}) + a)\underline{x} + (u(\underline{x}) + a)\underline{w}) + a \\ &= (1 + u(\underline{x}) + a)\mathrm{u}(\underline{x}) + (u(\underline{x}) + a)u(\underline{w}) + a \quad \text{by lemma 1} \\ &= 0 \end{aligned}$$

It follows that $s(\underline{y}) = t(\underline{y})$.

Now suppose there exists some solution $\underline{z}$, i.e. $s(\underline{z}) = t(\underline{z})$. We need to show that $\underline{z}$ is an instantiation of $\underline{y}$. Fortunately $\underline{x} = \underline{z}$ will do: $\underline{z} + (s(\underline{z}) + t(\underline{z}))(\underline{z} + \underline{w}) = \underline{z}$ because $s(\underline{z}) + t(\underline{z}) = 0$. Therefore $\underline{y}$ is indeed a most general solution. □

REMARK. It is usually necessary to introduce new variables in the unification step of a unification algorithm, but in this case we do not need to do this as the mgu substitutes all variables present in the original two terms.

4. The Orthogonal Normal Form

In this section we consider the structure of the arbitrary Boolean ring, and show that we can always find a canonical form for the elements in terms of an orthogonal basis.

We shall show that every Boolean ring has a unique orthogonal basis, which can be described in terms of a set of generators.

THEOREM 5. *Let B be a Boolean ring. Then*

1. *If $C = \{c_1, \ldots, c_n\}$ is a set of generators of B and $U \subseteq C$ let*

$$v^U = \prod_{u \in U} u \prod_{w \in C \setminus U} (1 + w).$$

Then the non-zero v^U are all distinct, and form an orthogonal basis of B. This orthogonal basis is unique.

2. *If B has a presentation as*

$$B = \langle c_1, \ldots, c_n | w_1, \ldots, w_k \rangle$$

then

$$\{(v^U)\phi \mid (1 + w_1) \cdots (1 + w_k)v^U \neq 0 \text{ in } \mathcal{T}(C, \Sigma)_E\}$$

forms an orthogonal basis of B.

EXAMPLE. Let R be the Boolean ring on a, b, c subject to $ab + bc + ca = 0$. There are eight elements v^U, of the form $\tilde{a}\tilde{b}\tilde{c}$, where $\tilde{x}$ represents x or $\bar{x} = 1 + x$. Of these,

$$abc = \bar{a}bc = a\bar{b}c = ab\bar{c} = 0,$$

and the rest

$$\bar{a}\bar{b}c,\ \bar{a}b\bar{c},\ a\bar{b}\bar{c} \text{ and } \bar{a}\bar{b}\bar{c}$$

are non-zero and distinct, and form an orthogonal basis for B.

The easiest way to determine this is to apply part 2 of the theorem to determine which v^U satisfy

$$(ab + bc + ca)v^U = 0$$

in $\mathcal{T}(\{a, b, c\}, \Sigma)_E$.

Notice that although we may choose many other generating sets for R, for example $\{a, a + b, a + b + c\}$, they will all give rise, by theorem 5, to the same orthogonal basis.

Experts can deduce this theorem from standard results about semisimple Artinian rings – see [5] for example. We will present a direct proof.

We first collect some properties of the v^U.

LEMMA 2. *Let C be a finite subset of the Boolean ring B, and for any $U \subseteq C$ let*

$$v_U = \prod_{x \in U} x$$

and

$$v^U = \prod_{x \in U} x \prod_{y \in C \setminus U} (1 + y).$$

Then

1. $v^U v^W = 0$ for $U \neq W$.
2. $v^U v_W = v^U$ *if* $W \subseteq U$ *and* 0 *otherwise.*
3. $1 = \Sigma_{U \subseteq C} v^U$.
4. *If* $p = \Sigma_{U \subseteq C} b^U v^U$ *with* $b^U \in F$ *then* $pv^U = b^U v^U \in \{O, v^U\}$.

Proof.

1. If U and W are different then there will be some element y which contributes y to one term and $1 + y$ to the other, so that the product is zero.
2. If there is an element y in W but not in U then $y(1 + y)$ appears in the product $v^U v_W$, which is then zero. Otherwise $v^U v_W = v^u$.
3. The proof is by induction on $|C|$. If $C = \{c\}$, then $1 = c + (1 + c)$ as required. Suppose $C = D \cup \{c\}$, where D is non empty. By induction $1 = \Sigma_{U \subseteq D} v^U = [(1 + c) + c]\Sigma_{U \subseteq D} v^U = \Sigma_{W \subseteq C} v^W$.
4. By (1), $pv^U = b^U v^U$, and since $b^U \in F$, we have $pv^U \in \{O, v^U\}$.

Proof of Theorem, Part 1. We show first the non-zero v^U are distinct. For suppose $U \neq W$ and $0 \neq v^U = v^W$. Multiplying both sides by v^U and applying Lemma 2 gives $v^U = 0$, which is a contradiction.

Now let T be the set of non-zero v^U. It follows from Lemma 2 that the elements of T are orthogonal. To show that they are a basis, we first show they are linearly independent. Suppose that

$$\sum_{t \in T} b_t t \;=\; 0,$$

for some $b_t \in F$, and that $s \in T$ with $b_s \neq 0$. Now

$$O \;=\; s \sum_{t \in T} b_t t \;=\; sb_s \;=\; 1 * s \;=\; s,$$

which is a contradiction, and so the elements of T are linearly independent. We also need to show that if $b \in B$ then b is a linear combination of elements of T. Now $b = \Sigma_{U \subseteq C} b_U v_U$ with each $b_U \in F$. We have

$$v_U \;=\; v_U 1 \;=\; v_U \sum_{W \subseteq C} v^W,$$

which, by Lemma 2, is a linear combination of elements of T, since each $v_U v^W$ is either 0 or v^W. Thus b is a linear combination of elements of T.

To show that T is unique, we must show that if P is another orthogonal basis then $P = T$. So suppose that $p \in P$. We have

$$p \;=\; 1p \;=\; \sum_{U \subseteq C} pv^U,$$

and so there must be a subset U of C with $pv^U \neq 0$. Now since T is an orthogonal basis it follows from lemma 2 that $pv^U = v^U$, and since P is an orthogonal basis that $pv^U = p$. Thus $p \in T$, and hence $P \subseteq T$, and, by applying the above argument with P and T interchanged, $T = P$.

Part 2. We know from *Part 1* that $v^U \phi$ is a basis element if and only if it is non-zero. Now if $v^U \phi = O$ then

$$v^U \;=\; \sum_{i=1}^{i=k} w_i a_i$$

for some $a_1, \ldots a_k \in \mathscr{T}(C, \Sigma)_E$ and so

$$v^U(1 + w_1) \cdots (1 + w_k) \;=\; 0.$$

Conversely if

$$v^U(1 + w_1) \cdots (1 + w_k) \;=\; 0$$

then $v^U \phi = \dot{0}\phi = 0$ as required.

5. Finding Particular Solutions

In this section we describe how to find a particular solution to a Boolean equation by using an orthogonal basis.

If we want to test if an equation has a solution we can use Boole's criterion of theorem 1. This involves testing whether a certain Boolean expression which depends only on the equation is zero or not. Thus an equation over some Boolean ring B' has a solution in B' if and only if it has a solution in B, the subring of B' generated by the coefficients appearing in the equation, and so when looking for a particular solution we need only consider B.

Since B is finite and enumerable, there is a trivial way to find a particular solution. All one needs to do is to test all possible valuations. The problem itself is NP-complete since it also covers the special case where $C = \{\ \}$, i.e. propositional formulae: finding a particular solution to $p = 1$ is equivalent to determining the satisfiability of p. Therefore it is unlikely that we can find a sub-exponential solution. However our method is significantly better than this.

We shall describe a technique for determining whether or not an equation has a solution, and producing one if it has. We shall then describe a more efficient modification which can be used when we already know, for example by applying Boole's criterion, that the equation has a solution.

We begin with an example. We want to find a solution in $B = T(\{a, b\}, \Sigma)_E$ to

$$axy + by = a.$$

Let $u(\underline{x}) = axy + by$, where $\underline{x} = (x, y)$. Now using the orthogonal normal form we see that B is a vector space over $F = \{0, 1\}$ with basis $\mathrm{D} = \{ab = d_1, a\bar{b} = d_2, \bar{a}b = d_3, \bar{a}\bar{b} = d_4\}$ where $\bar{c} = (1 + c)$. This means that each $c \in B$ can be expressed uniquely as

$$c = \sum_{i=1}^{4} c_i d_i \quad \text{with} \quad c_i \in F$$

We have $d_i d_j = 0$ for $i \neq j$ and, by lemma 2, $cd_i = c_i d_i \in \{d_i, 0\}$ for any $c \in B$.

Now suppose that

$$\begin{aligned} x &= x_1 d_1 + x_2 d_2 + x_3 d_3 + x_4 d_4 \quad \text{and} \\ y &= y_1 d_1 + y_2 d_2 + y_3 d_3 + y_4 d_4 \quad \text{and thus} \\ \underline{x} &= d_1 \underline{x}_1 + d_2 \underline{x}_2 + d_3 \underline{x}_3 + d_4 \underline{x}_4 \quad \text{where } \underline{x}_i = (x_i, y_i). \end{aligned}$$

We have

$$\begin{aligned} u(\underline{x}) &= u(d_1\underline{x}_1 + d_2\underline{x}_2 + d_3\underline{x}_3 + d_4\underline{x}_4) \\ &= d_1 u(\underline{x}_1) + d_2 u(\underline{x}_2) + d_3 u(\underline{x}_3) + d_4 u(\underline{x}_4) \quad \text{by Lemma 1} \\ &= d_1(ax_1y_1 + by_1) + d_2(ax_2y_2 + by_2) + d_3(ax_3y_3 + by_3) + \\ &\quad + d_4(ax_4y_4 + by_4) \\ &= d_1(x_1y_1 + y_1) + d_2(x_2y_2) + d_3(y_3) + d_4(0) \end{aligned}$$

So $u(\underline{x}) = d_1 u_1(\underline{x}_1) + \cdots + d_4 u_4(\underline{x}_4)$ where $u_i(\underline{x}_i)$ is a polynomial in x_i, y_i with coefficients in F.

Now since $a = d_1 + d_2$, we may equate coefficients of the d_i in $u(\underline{x}) = a$ to deduce that this has a solution in B if and only if the four equations

$$\begin{array}{lllll} u_1(\underline{x}_1) & = & x_1y_1 + y_1 & = & 1 \\ u_2(\underline{x}_2) & = & x_2y_2 & = & 1 \\ u_3(\underline{x}_3) & = & y_3 & = & 0 \\ u_4(\underline{x}_4) & = & 0 & = & 0 \end{array} \tag{1}$$

have a solution. It is easy to find solutions to these equations. For the third and fourth one, just set

$$x_3 = y_3 = x_4 = y_4 = 0.$$

For the first, find the shortest word on the left hand side, y_1, and set the variables appearing in it to 1 and the other variables to 0, to get the solution

$$x_1 = 0, y_1 = 1.$$

Similarly for the second: $x_2 = y_2 = 1$.
Thus we have a solution

$$\begin{array}{lllllll} x & = & d_2 & = & a\bar{b} & = & a + ab, \\ y & = & d_1 + d_2 & = & ab + a\bar{b} & = & a. \end{array}$$

The equations (1) were so easy to solve because they were independent, i.e. each variable appeared only in one of them. This is not an accident – it always happens, as can be seen by generalizing the argument of the above example. We do this below.

However first we consider an example of two terms which cannot be unified. Let $u(\underline{x}) = ax = b$. We have

$$x = d_1x_1 + d_2x_2 + d_3x_3 + d_4x_4,$$

hence

$$ad_1x_1 + ad_2x_2 + ad_3x_3 + ad_4x_4 = d_1 + d_3,$$

that is

$$x_1d_1 + x_2d_2 = d_1 + d_3,$$

which gives, on equating coefficients,

$$x_1 = 1, x_2 = 0, 0 = 1, 0 = 0$$

which clearly has no solution. Thus ax and b cannot be unified. Of course we could show this more directly by using Boole's test.

In general then, this is our algorithm. Let B' be a Boolean ring, and let $s(\underline{x}) = t(\underline{x})$ be an equation over B'. The algorithm to determine if the equation $s(\underline{x}) = t(\underline{x})$ has a solution in B' and to compute one if it has can be broken up as follows.

1. Normalize $s(\underline{x}) + t(\underline{x})$ as $u(\underline{x}) + a_0$ where $u(\underline{x}) = a_1 v_1(\underline{x}) + \cdots + a_r v_r(\underline{x})$ is homogeneous, $a_i \in B'$ and the $v_i(\underline{x})$ are pairwise distinct strings of variables in $\underline{x}$ as described above. Let B be the subring of B' generated by the a_i, and let $D = \{d_1, \ldots, d_m\}$ be an orthogonal basis for B, which exists by Theorem 5.
2. For each x_i in $\underline{x} = (x_1, \ldots, x_n)$ write $x_i = d_1 x_{i1} + \cdots + d_m x_{im}$ where the x_{ij} lie in F. Substituting this back into u we get

$$\begin{aligned} u(\underline{x}) &= u(d_1 \underline{x}_1 + \cdots + d_m \underline{x}_m) \\ &= d_1 u(\underline{x}_1) + \cdots + d_m u(\underline{x}_m) \end{aligned}$$

where $\underline{x}_j = (x_{1j}, \ldots, x_{nj})$. For each j we have

$$\begin{aligned} d_j u(\underline{x}_j) &= d_j \Sigma_{i=1}^{r} a_i v_i(\underline{x}_j) \\ &= \Sigma_{i=1}^{r} d_j a_i v_i(\underline{x}_j) \\ &= d_j \Sigma_{i \in N_j} v_i(\underline{x}_j) \\ &= d_j u_j \end{aligned}$$

where $N_j = \{i \in \{1\,..\,r\} \mid d_j a_i \neq 0\}$ and each $v_i(\underline{x}_j)$ is just $v_i(\underline{x})$ with x_{ij} substituted for x_i. Thus u_j is a homogeneous polynomial in the variables $x_{1j}, \ldots, x_{nj}$.
3. Express a_0 in terms of the d_i and equate coefficients:
Let

$$a_0 = \sum_{i=1}^{m} p_i d_i$$

where $p_i \in F$. Now $u(\underline{x}) = a_0$ becomes

$$\sum_{j=1}^{m} u_j d_j = \sum_{j=1}^{m} p_j d_j.$$

Since the distinct d_j are linearly independent, this equation is satisfied if and only if for each j we have $u_j = p_j$, that is if and only if each equation

$$\sum_{i \in N_j} v_i(\underline{x}_j) = p_j$$

has a solution, There are three possibilities for each equation:

3.1. $p_j = 0$: then $\underline{x}_j = \underline{0}$, i.e. $x_{ij} = 0$ for all i, is a solution.

3.2. $p_j = 1$:

3.2.1. $N_j = \{\ \}$: then there is no solution because $1 = \Sigma_{i \in \{\}} \cdot = 0$ has no solution. Hence s and t are not unifiable.

3.2.2. $N_j \neq \{\ \}$: the equation always has a solution. From among the $v_i(\underline{x}_j)$ select one with non-zero coefficient, i.e. $i \in N_j$, such that there is no smaller set of variables in u_j, i.e. there is no $k \in N_j$ with $v_k(\underline{x}_j)$ containing fewer variables than $v_i(\underline{x}_j)$. Set all x_{lj} in $v_i(\underline{x}_j)$ to 1 and all other x_{lj} to

0. Then $v_i(\underline{x}_j)$ is 1 and all other $v_k(\underline{x}_j)$ are either larger or of the same size but different from $v_i(\underline{x}_j)$. In both cases they must contain some x_{lj} not in $v_i(\underline{x}_j)$ which means they evaluate to 0.

The complete algorithm for finding a special solution is given below in a more formal and concise notation. Since all sets involved are finite, even the quantified expressions are in principle executable. The nondeterministic choice of shortest strings of variables is embodied in the **let** *min* ∈ . . . construct.

```
sol(s,t) =
    let $a_0 + a_1v_1 + \cdots + a_rv_r = s + t$ in
    let $p_1d_1 + \cdots + p_md_m = a_0$ in
    let $A = \{i \in \{1..m\} \mid p_i = 1\}$ in
    let $N(i \in A) = \{j \in \{1..r\} \mid d_ia_j \neq 0\}$ in
        if $\exists i \in A : N(i) = \{\}$ then fail
        else let $min \in \{f : A \to \{1..r\} \mid f(i) \in N(i) \wedge \forall j \in N(i) : |v_{f(i)}| \leq |v_j|\}$ in
             let $I(i \in \{1..n\}) = \{j \in A \mid x_i \in v_{min(j)}\}$ in
                 $\{x_i \to \sum_{j \in I(i)} d_j \mid i \in \{1..n\}\}$
```

Computing a special solution is the only algorithmic part in our unification algorithm. Once a particular solution has been derived, it just has to be substituted into the formula for the general solution.

If we already know that our equation has a solution we can refine the algorithm as follows. Step 3.2.1 can never occur, and if step 3.1 occurs we just set $\underline{x}_j = 0$. Thus we only need to consider case 3.2.2, that is those j for which $p_j = 1$, which are just those for which $d_ja_0 \neq 0$.

In some circumstances we can use the above method to find the general solution of an equation, by finding the most general solution to each equation in 3.1 and 3.2, which gives us a solution of the form

$$u = f_1d_1 + \cdots + f_md_m,$$

where each d_i is some function of parameters taking values in F. Notice that in this case we cannot restrict attention to the subring B od B' generated by the coefficients of the equation; we must work with an orthogonal basis for B'. An example is given in section 6.

6. Applications in Set Theory and the Propositional Calculus

UNIFICATION IN SET THEORY

We have seen that the power set of any set $S = \{s_1, \ldots, s_n\}$ forms a Boolean ring $B(S)$ under the operations of symmetric difference (+) and intersection. To apply our methods we need to find an orthogonal basis of $B(S)$.

LEMMA 3. *The elements of S form an orthogonal basis for* $B(S)$.

Proof. The elements of S are orthogonal, since $s_i s_j = 0$ for $i \neq j$. Any element of $B(S)$ can be written as a linear combination of elements of S; the sum of the elements it contains. If

$$\sum_{i=1}^{i=n} b_i s_i = 0$$

with the $b_i \in F$ then, for each j multiplying by s_j gives $b_j s_j = 0$, and so $b_j = 0$. Thus the s_i are linearly independent, and so form an orthogonal basis for $B(S)$.

REMARK. We could also prove this lemma by noting that $B(S)$ is isomorphic to

$$\langle t_1, \ldots, t_n \,|\, t_1 + \cdots + t_n + 1,\ t_i t_j \text{ (for } i \neq j)\rangle,$$

and applying theorem 5 part 2 to get an orthogonal basis, which simplifies to $\{t_1, \ldots, t_n\}$.

EXAMPLE. Suppose we want to solve the equation

$$cxy + xa + yb + c = 0 \tag{2}$$

in $B(\{a, b, c, q_1, \ldots, q_n\})$. Since a, b and c are the only constants appearing in the equation we look for a solution in $B(\{a, b, c\})$. Applying Boole's test (Theorem 1) gives us

$$(1 + c)(1 + a)(1 + b)c = 0$$

so that the equation has a solution. Let a particular solution be

$$x = ra + sb + tc,$$

$$y = r'a + s'b + t'c.$$

The equation has constant term c, and $ac = bc = 0$, so that we apply step 3.1 for the basis vectors a and b and set $r = r' = s = s' = 0$. Since $cc = c \neq 0$, we equate coefficients of c, which gives $tt' = 1$, so $t = t' = 1$ completes our particular solution, $x = y = c$. Thus a most general unifier for (2) is

$$x \rightarrow c + x(1 + a + c) + xyb,$$

$$y \rightarrow c + y(1 + b + c) + xya.$$

We could also do this example by finding the most general solutions to the equations obtained by equating coefficients. If we do this we must work in the ring $B(\{a, b, c, q_1, \ldots, q_n\})$. Substituting for x and y in (2) and equating coefficients gives us

$$r = 0,$$

$$s' = 0,$$

and

$$tt' = 1.$$

The most general solutions for x and y are thus $r = 0, s' = 0$ and $t = t' = 1$, giving

$$x = sb + c + u_1 q_1 + \cdots + u_n q_n,$$

$$y = ra + c + v_1 q_1 + \cdots + v_n q_n.$$

UNIFICATION IN THE PROPOSITIONAL CALCULUS

The set of well formed formulae of the propositional calculus on propositional symbols $P = \{p_1 \ldots, p_n\}$ forms a Boolean ring which is isomorphic to $T(P, \Sigma)_E$. We do not need unification to test if a proposition is a tautology or unsatisfiable – we merely simplify it and see if we get 1 or 0. Unifying a term involving variables with 1 or 0 corresponds to finding the most general values of those variables which makes the corresponding proposition a tautology, or unsatisfiable.

One application is in the construction of derived proof rules. Suppose for example that we want to find the most general value of x which will make

$$\frac{(p \rightarrow q) \wedge x}{q \vee r}$$

into a derived rule. This means we must find the most general solution of

$$((p \rightarrow q) \wedge x) \rightarrow (q \vee r) = 1,$$

or, in Boolean ring notation,

$$1 + (1 + p + pq)x(1 + q + r + qr) = 1,$$

that is

$$(1 + p)(1 + q)(1 + r)x = 0.$$

The most general solution is

$$x \rightarrow x + x(1 + p)(1 + q)(1 + r),$$

that is,

$$x \rightarrow x \wedge (p \vee q \vee r).$$

Thus we have shown that for any x,

$$\frac{(p \rightarrow q) \wedge (p \vee q \vee r) \wedge x}{q \vee r}$$

is a derived rule. Putting $x = p \vee r$, this reduces to the resolution rule.

7. Concluding Remark

The subject of the present paper is a detailed exposition of unification in Boolean rings using Löwenheim's method. However there is at least one other important algorithm for Boolean unification, the 'successive variable elimination' technique due to Boole, which is used in [2] and is also discussed in detail in [15]. A comparison of both methods can be found in a forthcoming survey paper [12].

Acknowledgements

The authors acknowledge partial support of the U.K. SERC under grants GR/D/58514 and GR/D/81718, respectively.

References

1. Boole, G., *The Mathematical Analysis of Logic*, Macmillan 1847. Reprinted B. Blackwell (1948).
2. Büttner, W., Simonis, H., 'Embedding Boolean expressions into Logic Programming', preprint, to appear in *Journal of Symbolic Computation* (1987).
3. Hailpern, T., *Boole's Logic and Probability*, North-Holland (1986).
4. Herbrand, J., 'Investigations in Proof Theory', [*Herbrand's thesis*] *in Jacques Herbrand Logical Writings*, ed. W. Goldfarb, pp. 44–202. D. Reidel (1971).
5. Herstein, I. N., 'Non-commutative rings', *Carus Mathematical Monograph*, Wiley (1968).
6. Herold, A., 'Combination of Unification Algorithms', in 8th International Conference on Automated Deduction, *Lecture Notes in Computer Science* 230, pp. 450–469. Springer (1986).
7. Hsiang, J., 'Rewrite rules for clausal and non-clausal theorem proving', in Proc. 10th ICALP, LNCS 154 (1983).
8. Hsiang, J., 'Refutational Theorem Proving using Term-Rewriting Systems', *Artificial Intelligence* **25** (1985).
9. Kapur, D., Narendran, P., 'An equational approach to theorem proving in the first order predicate calculus', Proc. IJCAI 85, Los Angeles (1985).
10. Löwenheim, L., Über das Auflösungproblem im logischen Klassenkalkül', *Sitzungber. Berl. Math. Gesell.* **7**, 89–94 (1908).
11. Martin, U., Nipkow, T., 'Unification in Boolean Rings', in 8th International Conference on Automated Deduction, *Lecture Notes in Computer Science* **230**, pp. 506–513. Springer (1986).
12. Martin, U., Nipkow, T., 'Boolean Unification – A Survey', to appear in *Journal of Symbolic Computation.*
13. Monk, J. D., *Mathematical Logic*, Springer (1976).
14. Robinson, J. A., 'A machine oriented logic based on the resolution principle', *J.ACM* **12**, 23–41 (1974).
15. Rudeanu, S., *Boolean functions and equations*, North Holland (1974).
16. Siekmann, J. H., 'Universal Unification', in Proceedings of European Conference on Artificial Intelligence, Brighton (1986).
17. Schröder, E., '*Vorlesungen über die Algebra der Logic*, (Leipzig, Vol. 1, 1890; Vol. 2, 1891, 1905; Vol. 3, 1895). Reprint Chelsea, Bronx, NY. (1966).
18. Vitter, J. S., Simons, R. A., 'New Classes for Parallel Complexity: A Study of Unification and Other Complete Problems for *P*', *IEEE Transactions on Computers*, 403–418 (1986).
19. Watts, D. E., Cohen, J. K., 'Computer-Implemented Set Theory', *Amer. Math. Month.* **87** (1980).