Contents

1 Equational Unification

In the following let E be a set of identities of the form $\{e_1 \approx f_1, \dots, e_n \approx f_n\}$. Furthermore let $\mathcal{S}ig(E)$ denote the set of all function symbols occurring in E. Let Σ be a finite set of function symbols and a superset of $\mathcal{S}ig(E)$.

Definition 1.1. An E**-unification problem** over Σ is a finite set S of the form $S = \left\{ s_1 \overset{?}{\approx}_E t_1, \dots, s_n \overset{?}{\approx}_E t_n \right\}$ with $s_1, \dots, s_n, t_1, \dots, t_n \in T(\Sigma, V)$, V being a countable set of Variables.
A substitution σ is an E**-unifier** of S iff $\sigma(s_i) \approx_E \sigma(t_i)$ for all $1 \leq i \leq n$. The set of all E-unifiers of S is denoted by $\mathcal{U}_E(S)$. S is E**-unifiable** iff $\mathcal{U}_E(S) \neq \emptyset$.

Definition 1.2. Let S be an E-unification problem over Σ.

- S is an **elementary** E-unification problem iff $\mathcal{S}ig(E) = \Sigma$.
- S is an E-unification problem **with constants** iff $\Sigma - \mathcal{S}ig(E) \subseteq \Sigma^{(0)}$ and $\mathcal{S}ig(E) \subset \Sigma$
- S is an **general** E-unification problem iff $\Sigma - \mathcal{S}ig(E)$ contains an at least unary function symbol.

One *most general unifier* does not always suffice to represent $\mathcal{U}_E(S)$. In this case we need a *minimal complete set of unifiers* but to define this set we first need an order on substitutions.

Definition 1.3. Let X be a set of variables. A substitution σ is **more general** modulo $\approx_E$ than a substitution σ' on X iff there is a substitution δ such that $\delta(\sigma(x)) \approx_E \sigma'(x)$ for all $x \in X$. We denote this by $\sigma \lesssim_E^X \sigma'$.

$\lesssim_E^X$ is a is a quasi order since it obviously is reflexive and transitive. But why do we only demand equality modulo $\approx_E$ on X and not on all Variables like we did in syntactic unification? Note that by the restriction to Variables in X more substitutions are comparable with respect to $\lesssim_E^X$ since we do not demand equality modulo $\approx_E$ on all Variables. Lets denote the Variables occurring in an E-unification problem S by $\mathcal{V}ar(S)$. It is easy to see that if $X = \mathcal{V}ar(S)$, σ' is an E-unifier of S and $\sigma \lesssim_E^X \sigma'$ then σ is also an E-unifier of S. This only shows that restriction to X does not do any damage but the reason it is useful is that there are E-unification problems S for which any *minimal complete set of E-unifiers* has to contain Variables not occurring in S. Lets consider a small example, let $\sigma := \{x \mapsto f(y)\}$ be in $\mathcal{M}$ a *minimal complete set of E-unifiers* of S with $\mathcal{V}ar(S) = \{x\}$ and $\{a \approx x\} \notin E$. Clearly $\sigma' := \{x \mapsto f(a)\}$ is also an E-unifier of S but σ and σ' are incomparable w.r.t. $\lesssim_E^{\{x,y\}}$. The substitution $\delta := \{y \mapsto a\}$ does not work here since $\delta(\sigma(y)) = a \not\approx_E y = \sigma'(y)$ which means there has to be another unifier σ'' in $\mathcal{M}$ with $\sigma'' \lesssim_E^{\{x,y\}} \sigma$. But if we restrict X to $\{x\}$ we only need that $\delta(\sigma(x)) = f(a) \approx_E f(a) = \sigma'(x)$ so $\sigma \lesssim_E^{\{x\}} \sigma'$ holds. We see that *minimal complete sets of E-unifiers* can become unnecessary large if we consider all Variables. Since we have talked about these sets a lot lets define them formally.

Definition 1.4. Let S be an E-unification problem over Σ and let $X := \mathcal{V}ar(S)$. An **E-complete** set of S is a set of substitutions $\mathcal{C}$ that satisfies the following properties.

- each $\sigma \in \mathcal{C}$ is an E-unifier of S
- for all $\theta \in \mathcal{U}_E(S)$ there exists a $\sigma \in \mathcal{C}$ such that $\sigma \lesssim_E^X \theta$

An **E-minimal E-complete** set is an E-complete set $\mathcal{M}$ that satisfies the additional property

- for all $\sigma, \sigma' \in \mathcal{M},\ \sigma \lesssim_E^X \sigma'$ implies $\sigma = \sigma'$.

The substitution σ is a **most general E-unifier** (mgu) of S iff $\{\sigma\}$ is an E-minimal E-complete set of S.

Now let us consider an example in which an E-minimal E-complete set contains infinitely many elements. Let $A := \{x + (y + z) \approx (x + y) + z\}$ be a set of identities and $S := \left\{ x + a \overset{?}{\approx}_A a + x \right\}$ an A-unification problem over $\Sigma := \{+, a\}$. For $n > 0$, we define substitutions σ_n inductively as follows:

$$\begin{aligned} \sigma_1 &:= \{x \mapsto a\} \\ \sigma_{n+1} &:= \{x \mapsto a + \sigma_n(x)\} \end{aligned}$$

Since A axiomatizes associativity we can omit the brackets and give an explicit definition of σ_n.

$$\sigma_n := \{\underbrace{a + \cdots + a}_{n \times a}\}$$

Now it is easy to see that all σ_n are A-unifiers of S. Lets consider an arbitrary A-unifier θ of S. $\theta(x)$ has the form $\theta(x) := x_1 + \cdots + x_n$ where the $x_i's$ are either a or a variable. Since θ is an A-unifier of S we have that:

$$\begin{array}{lr} & \theta(x) + a \approx_A a + \theta(x) \\ & x_1 + \cdots + x_n + a \approx_A a + x_1 + \cdots + x_n \\ \Longrightarrow x_1 = a, x_n = a & a + x_2 + \cdots + x_{n-1} + a + a \approx_A a + a + x_2 + \cdots + x_{n-1} + a \\ \Longrightarrow x_2 = a, x_{n-1} = a & a + a + \cdots + a + a + a \approx_A a + a + a + \cdots + a + a \\ \vdots & \vdots \\ \Longrightarrow & \underbrace{a + \cdots + a}_{n+1 \times a} \approx_A \underbrace{a + \cdots + a}_{n+1 \times a} \end{array}$$

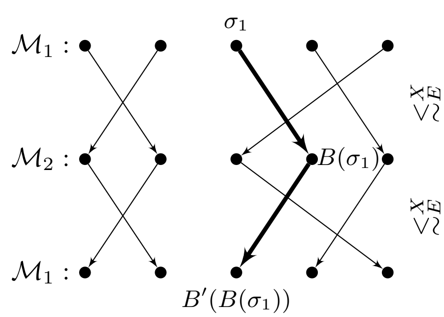
So $\theta(x) = \sigma_n(x)$ which implies $\sigma \lesssim_A^{\{x\}} \theta$. Since we picked θ arbitrarily this yields A-completeness of the set $\mathcal{M} := \bigcup_{n>0} \{\sigma_n\}$. All σ_n are distinct and map x to ground terms. Hence they are pairwise incomparable with respect to $\lesssim_A^{\{x\}}$. This yields A-minimality of $\mathcal{M}$. We see that E-minimal E-complete sets do not need to have finite cardinality.

We denote equivalence class induced by $\lesssim_E^X$ with $\sim_E^X$.

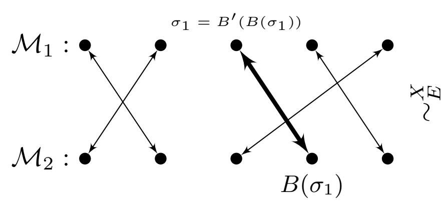
$$\sigma \sim_E^X \sigma' \text{ iff } \sigma \lesssim_E^X \sigma' \text{ and } \sigma' \lesssim_E^X \sigma$$

Lemma 1.5. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be E-minimal E-complete sets of S. Then there exists a bijective mapping $B : \mathcal{M}_1 \mapsto \mathcal{M}_2$ such that $\sigma_1 \sim_E^X B(\sigma_1)$ for all $\sigma_1 \in \mathcal{M}_1$.*

Proof. We define a mapping $B : \mathcal{M}_1 \mapsto \mathcal{M}_2$ such that $B(\sigma_1) \lesssim_E^X \sigma_1$ for all $\sigma_1 \in \mathcal{M}_1$. This is possible since $\mathcal{M}_1 \subseteq \mathcal{U}_E(S)$ and E-completeness of $\mathcal{M}_2$ yields that for every $\sigma_1 \in \mathcal{M}_1$ there exists a $\sigma_2 \in \mathcal{M}_2$ such that $\sigma_2 \lesssim_E^X \sigma_1$. We define $B' : \mathcal{M}_2 \mapsto \mathcal{M}_1$ in a similar way.



Since by definition $B'(B(\sigma_1)) \lesssim_E^X B(\sigma_1) \lesssim_E^X \sigma_1$ E-minimality of $\mathcal{M}_1$ implies that $B'(B(\sigma_1)) = \sigma_1$ for all $\sigma_1 \in \mathcal{M}_1$. Symmetrically, $B(B'(\sigma_2)) = \sigma_2$ for all $\sigma_2 \in \mathcal{M}_2$. It follows that B is a bijection and $B' = B^{-1}$.



□

The most interesting consequence from this Lemma is that E-minimal E-complete sets of the same S always have the same cardinality. This allows us to classify equational theories $\approx_E$ by the existence and possible cardinalities of E-minimal E-complete sets of E-unification problems.

Definition 1.6. The equational theory $\approx_E$ is of **unification type**

unitary iff for all E-unification problems S there exists an E-minimal E-complete set of cardinality ≤ 1.

finitary iff for all E-unification problems S there exists an E-minimal E-complete set with finite cardinality.

infinitary iff for all E-unification problems S there exists an E-minimal E-complete set, and there exists an E-unification problem for which this set is infinite.

zero iff there exists an E-unification problem that does not have an E-minimal E-complete set.

Note that if the E-unification problem S has no E-unifiers then the empty set is an E-minimal E-complete set of S. $\emptyset$ is E-complete because there are no $\sigma \in \emptyset$ and $\mathcal{U}_E$ is empty. E-minimality holds trivially. This is the reason we allow the cardinalities 0 and 1 in the *unitary* case. An example for a *finitary* theory that is not *unitary* is $\mathcal{C} := \{f(x,y) \approx f(y,x)\}$ which axiomatizes commutativity. With $\mathcal{A} := \{x + (y + z) \approx (x + y) + z\}$ the theory that axiomatizes associativity we have already seen an example for an *infinitary* equational theory. In the definition of the *unification types* we allowed for arbitrary E-unification problems but if we distinguish between elementary E-unification problems, E-unification problems with constants and general E-unification problems we might end up with different *unification types*. For example

2 Boolean Rings

$$B := \left\{ \begin{array}{cc} x + y \approx y + x, & x * y \approx y * x, \\ (x+y)+z \approx x + (y+z), & (x*y)*z \approx x*(y*z), \\ x + x \approx 0, & x * x \approx x, \\ 0 + x \approx x, & 0 * x \approx 0, \\ x*(y+z) \approx (x*y)+(x*z), & 1 * x \approx x \end{array} \right\}$$

Since $+$ and $*$ are associative we can omit most of the brackets. Furthermore we often write xy instead of $x * y$. Lets consider an interpretation of B the two element boolean ring $\mathcal{B}_2$ with the carrier set $\mathbf{2}$:= $\{0, 1\}$ where $*$ is "and" and $+$ is "exclusive or":

$$\begin{array}{rlrl} (x+y)^{\mathcal{B}_2} & := \left(x^{\mathcal{B}_2} \wedge \neg y^{\mathcal{B}_2}\right) \vee \left(\neg x^{\mathcal{B}_2} \wedge y^{\mathcal{B}_2}\right) & (x*y)^{\mathcal{B}_2} & := x^{\mathcal{B}_2} \wedge y^{\mathcal{B}_2} \\ 0^{\mathcal{B}_2} & := 0 & 1^{\mathcal{B}_2} & := 1 \end{array}$$

It is easy to see that $\mathcal{B}_2$ is indeed a model of B. Furthermore we can transform a term back from an Boolean algebra into Boolean ring theory:

$$\begin{aligned} x \wedge y &\mapsto x * y \\ x \vee y &\mapsto x + y + x * y \\ \neg x &\mapsto x * (x + 1) \end{aligned}$$

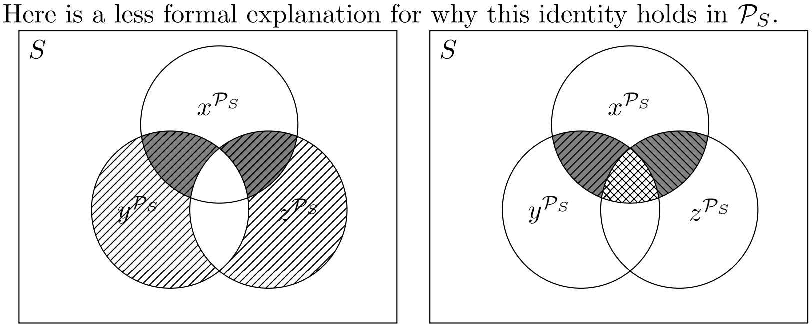
We work with + and * instead of $\vee, \wedge$ and $\neg$ because in Boolean rings we have a very convenient normal form which makes the following proofs easier.
Lets consider another model of B the powerset interpretation $\mathcal{P}_S$ with the carrier set 2^S:

$$(x+y)^{\mathcal{P}_S} := x^{\mathcal{P}_S} \Delta y^{\mathcal{P}_S} \qquad (x*y)^{\mathcal{P}_S} := x^{\mathcal{P}_S} \cap y^{\mathcal{P}_S}$$
$$0^{\mathcal{P}_S} := \emptyset \qquad 1^{\mathcal{P}_S} := S$$

Where $x \Delta y := (x \setminus y) \cup (y \setminus x)$ is the symmetric difference of x and y. It is easy to see why $\mathcal{P}_S$ is a model of B. Lets just consider distributivity in detail.

$$\begin{aligned}
(x*(y+z))^{\mathcal{P}_S} &= x^{\mathcal{P}_S} \cap \left(y^{\mathcal{P}_S} \Delta z^{\mathcal{P}_S}\right) \\
&= x^{\mathcal{P}_S} \cap \left(\left(y^{\mathcal{P}_S} \setminus z^{\mathcal{P}_S}\right) \cup \left(z^{\mathcal{P}_S} \setminus y^{\mathcal{P}_S}\right)\right) \\
&= \left(\left(x^{\mathcal{P}_S} \cap y^{\mathcal{P}_S}\right) \setminus z^{\mathcal{P}_S}\right) \cup \left(\left(x^{\mathcal{P}_S} \cap z^{\mathcal{P}_S}\right) \setminus y^{\mathcal{P}_S}\right) \\
&= \left(\left(x^{\mathcal{P}_S} \cap y^{\mathcal{P}_S}\right) \setminus \left(x^{\mathcal{P}_S} \cap z^{\mathcal{P}_S}\right)\right) \cup \left(\left(x^{\mathcal{P}_S} \cap z^{\mathcal{P}_S}\right) \setminus \left(x^{\mathcal{P}_S} \cap y^{\mathcal{P}_S}\right)\right) \\
&= \left(x^{\mathcal{P}_S} \cap y^{\mathcal{P}_S}\right) \Delta \left(x^{\mathcal{P}_S} \cap z^{\mathcal{P}_S}\right) \\
&= ((x*y)+(x*z))^{\mathcal{P}_S}
\end{aligned}$$

Here is a less formal explanation for why this identity holds in $\mathcal{P}_S$.



$(x*(y+z))^{\mathcal{P}_S}$ $\qquad$ $((x*y)+(x*z))^{\mathcal{P}_S}$

This small example should just show that there are other models of B with rather common interpretations of + and * apart from $\mathcal{B}_2$. Note that if $|S| = 1$ then $\mathcal{P}_S$ and $\mathcal{B}_2$ are isomorphic.

2.1 Polynomials

Definition 2.1. A product of distinct variables is a **monomial** (e.g. xyz). And a sum of distinct monomials is a **polynomial** (e.g. $x + xy + yz$).

We compare monomials and polynomials modulo commutativity and associativity. So two monomials are distinct iff the sets of variables occurring in them are distinct and two polynomials are distinct iff the sets of their monomials are distinct. Here are some examples for clarification:

$$yxz = zyx \qquad xy + yz = zy + xy$$
$$yx \neq yxz \qquad xy + yz \neq xy$$

Note that we did not introduce a new symbol for equality of polynomials and just use the same as for syntactic equality since it will be clear from the context which one we mean. Now we can transform every term over $\{0, 1, +, *\}$ into a (w.r.t. equality of polynomials) unique $\approx_B$-equivalent polynomial, its **polynomial form**. Since 1 is the neutral element of * we write 1 for the polynomial containing only the empty monomial correspondingly we identify 0 with the empty polynomial. Now the polynomial form can be computed recursively as follows:

$x, 0, 1$: This is the base case, variables and the constants 0 and 1 are already polynomials.

$t_1 + t_2$: Let p_1 and p_2 be the polynomial forms of t_1 and t_2 the polynomial form of $t_1 + t_2$ is obtained by removing all pairs of equivalent monomials from $p_1 + p_2$. Since we have $\{0 + x \approx x, x + x \approx 0\} \in B$ this rule preserves $\approx_E$-equivalence.

$t_1 * t_2$: Let $p_1 = m_1 + \cdots + m_k$ and $p_2 = n_1 + \cdots + n_l$ be the polynomial forms of t_1 and t_2. The polynomial form of $t_1 * t_2$ is obtained by removing all pairs of equivalent monomials from $p_1 * p_2$ which when multiplied out is the sum

$$m_1 * n_1 + \cdots + m_1 * n_l + \cdots + m_k * n_1 + \cdots + m_k * n_l$$

where the product of two monomials $m = x_1 \ldots x_r$ and $n = y_1 \ldots y_s$ is the monomial obtained by removing repeated occurrences of the same variable from $x_1 \ldots x_r y_1 \ldots y_s$. Since we have $\{x * x \approx x\} \in B$ this rule preserves $\approx_E$-equivalence. Note that if $t_1 = 1$ then we multiply every monomial in p_2 with the empty monomial which does not change anything so the result is as expected just p_2.