# Contents

# 1 Equational Unification

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

**Definition 1.1.** An $E$**-unification problem** over $\Sigma$ is a finite set $S$ of the form $S = \left\{ s_1 \overset{?}{\approx}_E t_1, \ldots, s_n \overset{?}{\approx}_E t_n \right\}$ with $s_1, \ldots, s_n, t_1, \ldots, t_n \in T(\Sigma, V)$, $V$ being a countable set of Variables.
A substitution $\sigma$ 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 $\Sigma$.

- $S$ 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 $\sigma$ is **more general** modulo $\approx_E$ than a substitution $\sigma'$ on $X$ iff there is a substitution $\delta$ 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 $X = \mathcal{V}ar(S)$, $\sigma'$ is an $E$-unifier of $S$ and $\sigma \lesssim_E^X \sigma'$ then $\sigma$ 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 $\sigma$ and $\sigma'$ 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 $\sigma''$ 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 $\Sigma$ 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 $\sigma$ 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 $\sigma_n$ inductively as follows:

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

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

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

Now it is easy to see that all $\sigma_n$ are $A$-unifiers of $S$. Lets consider an arbitrary $A$-unifier $\theta$ 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 $\theta$ is an $A$-unifier of $S$ we have that:

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

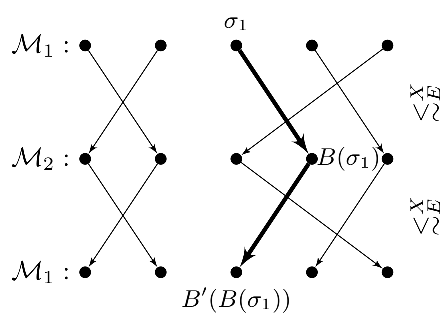
So $\theta(x) = \sigma_n(x)$ which implies $\sigma \lesssim_A^{\{x\}} \theta$. Since we picked $\theta$ arbitrarily this yields $A$-completeness of the set $\mathcal{M} := \bigcup_{n>0} \{\sigma_n\}$. All $\sigma_n$ are distinct and map x to ground terms. Hence they are pairwise incomparable with respect 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 $\sim_E^X$.

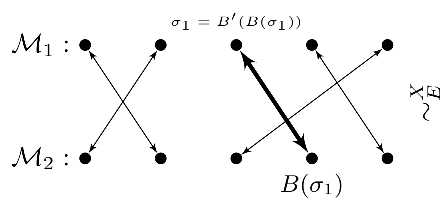
$$\sigma \sim_E^X \sigma' \text{ iff } \sigma \lesssim_E^X \sigma' \text{ and } \sigma' \lesssim_E^X \sigma$$

**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 $B' = B^{-1}$.




$\square$

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 $\leq 1$.

**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

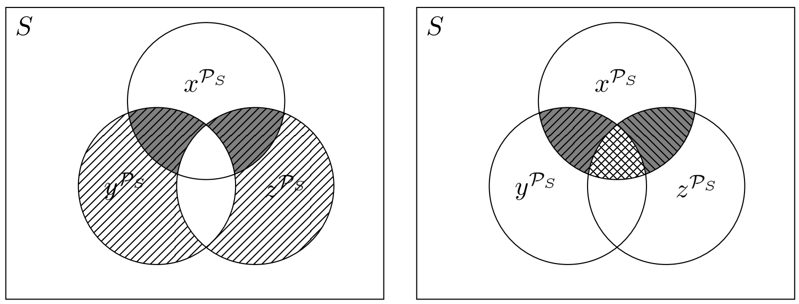
$$B := \left\{ \begin{array}{cc} x+y \approx y+x, & x*y \approx y*x, \\ (x+y)+z \approx x+(y+z), & (x*y)*z \approx x*(y*z), \\ x+x \approx 0, & x*x \approx x, \\ 0+x \approx x, & 0*x \approx 0, \\ x*(y+z) \approx (x*y)+(x*z), & 1*x \approx x \end{array} \right\}$$

Since $+$ and $*$ are associative we can omit most of the brackets. Furthermore we often write $xy$ instead of $x*y$. Lets consider a semantic 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". Lets consider another model of $B$ the powerset interpretation $\mathcal{P}_S$ with the carrier set $2^S$:

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

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.

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




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

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 isomorph.