Notes prepared by
Stanley Burris
February 10, 1997

# 1 Quasi-Identity Logic

| | |
|---|---|
| SYMBOLS | $\approx$ |
| | function symbols |
| | constant symbols |
| | variables |

In Chapter III of **LMCS** we looked at Birkhoff's study of equational logic. The next larger interesting fragment of first-order logic with equality is the logic of quasi-identities.

Quasi-identities are universal Horn formulas of the form

$$\forall \vec{x}\,[p_1 \approx q_1 \wedge \cdots p_n \approx q_n \to p \approx q],$$

including the possibility that $n = 0$ and we simply have an equation. As with identities, we usually omit writing the universal quantifiers. The study of quasi-identities, and the corresponding model classes called quasi-varieties, has been pursued mainly in Eastern Europe, following the lead of Mal'cev. In Western Europe and North America the focus has been on identities and varieties, a direction initiated by Birkhoff. The rules for working with quasi-identities are not as simple, or standardized, as the rules of Birkhoff. Of course the usual rules of first-order logic suffice to derive all the quasi-identity consequences of a set of quasi-identities, but one might prefer to have a logical system which only produces quasi-identities from quasi-identities. One such was given by Selman [5] in 1972 with four axiom schemes and six rules of inference. By considering a conjunction $p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n$ as a set of equations, rather than an abbreviation for some particular way of inserting parentheses, we can omit his fifth rule (which handles rearranging the parentheses and repeat copies of equations):

AXIOMS:

**(a)** $p \approx q \wedge r \approx s \rightarrow r \approx s$

**(b)** $p \approx p$

**(c)** $p \approx q \wedge q \approx r \rightarrow r \approx p$

**(d)** $p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \rightarrow f(p_1, \ldots, p_n) \approx f(q_1, \ldots, q_n)$.

RULES:

**(a)** $$\frac{r \approx s}{p \approx q \rightarrow r \approx s}$$

**(b)** $$\frac{p \approx q,\ p \approx q \rightarrow r \approx s}{r \approx s}$$

**(c)** $$\frac{p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \rightarrow p \approx q,\ p \approx q \rightarrow r \approx s}{p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \rightarrow p \approx q, \rightarrow r \approx s}$$

**(d)** $$\frac{p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \rightarrow p \approx q,\ p \approx q \wedge r_1 \approx s_1 \wedge \cdots \wedge r_n \approx s_n \rightarrow r \approx s}{p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \wedge r_1 \approx s_1 \wedge \cdots \wedge r_n \approx s_n \rightarrow r \approx s}$$

**(e)** $$\frac{p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \rightarrow p \approx q}{\sigma(p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \rightarrow p \approx q) \qquad (\sigma \text{ a substitution})}$$

We will not go into quasi-identity logic except to make some remarks on the complexity of quasi-identity theories. We note that the quasi-identity theory of a class $K$ of algebras is the same as that of the quasi-variety $Q(K)$ generated by $K$, as well as of the variety $V(K)$ generated by $K$. In the latter context the study of quasi-identity theory is better known as *the uniform word problem* for the variety.

## 1.1 Presentations and word problems

Word problems were one of the first places in mathematics where mathematicians were able to apply the concepts of algorithm (developed in the mid 1930's) to obtain undecidability results. Let $\Sigma$ be a set of equations in the language $\mathcal{F} \cup \mathcal{C}$.

**DEFINITION 1** A *presentation* $\Pi$ with respect to $\Sigma$ is an ordered pair $(\mathrm{G}, \mathrm{R})$ where G is a set of constant symbols disjoint from $\mathcal{C}$, called the set of *generators*, and R is a set of ground equations over G called the *defining relations.*

Presentations of groups came early in the century in the study of algebraic topology. Of course associated with the presentation one had a group.

**LEMMA 2** Given a presentation $\Pi = (\mathrm{G}, \mathrm{R})$ with respect to $\Sigma$, the relation $\theta_\Pi = \{(t_1, t_2) \in \mathrm{T}_{\mathrm{G}\cup\mathcal{C}} \times \mathrm{T}_{\mathrm{G}\cup\mathcal{C}} : \Sigma \cup \mathrm{R} \vdash t_1 \approx t_2\}$ is a congruence on $\mathbf{T}_{\mathrm{G}\cup\mathcal{C}}$.

PROOF. We observed this fact in the proof of the Birkhoff completeness theorem. ■.

**DEFINITION 3** Given a presentation $\Pi$ over $\Sigma$, let $\mathbf{A}_\Pi$ be the algebra $\mathbf{T}_{\mathrm{G}\cup\mathcal{C}}/\theta_\Pi$, *the algebra defined by the presentation.*

**EXAMPLE 4** Up to isomorphism we have

**(a)** $(\{a, b\}, \{ab \approx ba\})$ over groups[1] defines $\mathbf{Z} \times \mathbf{Z}$

**(b)** $(X, \emptyset)$ over $\Sigma$ defines the *free algebra* $\mathbf{F}_\Sigma(X)$ in the equational class determined by $\Sigma$

**(c)** $(X, \emptyset)$ over rings[2] defines the *polynomial ring* $\mathbf{Z}[X]$

**(d)** $(\emptyset, \{\underbrace{1 + \cdots + 1}_{n} \approx 0\})$ over rings defines $\mathbf{Z}_n$, the integers modulo $n$.

**(e)** $(\{a\}, \{a^2 + a + 1 \approx 0, 1 + 1 \approx 0\})$ over rings defines $\mathbf{GF}(4)$, the 4-element Galois field.

**DEFINITION 5** The problem of determining which ground equations over G follow from $\Sigma \cup \mathrm{R}$ is called the *word problem for* $\Pi$. If there is an algorithm for this problem then the word problem for $\Pi$ is *solvable*) (or *decidable*); otherwise it is *unsolvable* (or *undecidable*).

[1] In groups one can write all the defining relations in the form $w \approx e$, $e$ the identity element, and thus one can consider the set R (of defining *relators*) as a set of *words* (i.e., terms) $w$.

[2] In rings one can write all the defining relations in the form $w \approx 0$, and thus one can consider R as a set of *words* $w$ (i.e., terms) from $\mathrm{T}_{\mathrm{G}\cup\mathcal{C}}$.

**DEFINITION 6** If there is a single algorithm for solving the word problem for any presentation $\Pi$ over $\Sigma$ we say the word problem for $\Sigma$ is *(uniformly) solvable* (or *decidable*); otherwise it is *unsolvable*[3] (or *undecidable*).

A simple example of a semigroup presentation with unsolvable word problem was found by Tsentin:

| generators | relations | |
|---|---|---|
| $a\ b\ c\ d\ e$ | $ac \approx ca$ | $ad \approx da$ |
| | $bc \approx cb$ | $bd \approx db$ |
| | $abac \approx abacc$ | |
| | $eca \approx ae$ | $edb \approx be$ |

A. Mekler, E. Nelson, and S. Shelah [4] have proved that there is a finite $\Sigma$ such that the word problem for $\Sigma$ is unsolvable, but for each presentation $\Pi$ over $\Sigma$ the word problem is solvable.

The use of finite partial algebras is popular in methods for showing the word problem is solvable; in particular the following are equivalent for a variety $V$:

- The uniform word problem for $V$ is solvable.
- There is an algorithm to determine which finite partial algebras can be embedded into some member of $V$.
- One has an algorithm to find the smallest congruence $\theta$ of a finite partial algebra $\mathbf{P}$ such that $\mathbf{P}/\theta$ embeds into some member of $V$.

One can also show that the uniform word problem for $V$ is polynomial time solvable iff one can find the congruence $\theta$ in the last item above in polynomial time. And if the universal theory of $V^\star$, the relational version of $V$, is finitely axiomatizable then the uniform word problem is solvable in polynomial time. (See Burris [1].)

An interesting example is that of commutative semigroups, where each finite presentation $\Pi$ has a word problem solvable in polynomial time, but the uniform word problem for commutative semigroups is exponential space complete (due to Mayr & Meyer [3]; see also Kharlampovich & Sapir [2]).

[3]Warning: this eminently sensible definition has not been commonly used — the word problem for $\Sigma$ has been called unsolvable provided there is a single presentation with unsolvable word problem

In the table below we give a few examples concerning the solvability of the word problem for *finite* presentations. Rather than give a defining set of equations $\Sigma$ it is simpler to specify the class determined by the intended $\Sigma$.

| $\Sigma$ | | discovered by |
|---|---|---|
| semigroups | undecidable | Post/Markov 1947 |
| groups | undecidable | Novikov 1955 |
| lattices | decidable | Skolem 1920 |
| modular lattices | undecidable | Hutchinson 1973 |
| quasigroups | decidable | Evans 1953 |
| loops | decidable | Evans 1953 |

EXERCISES

**Problem 1** Show that Example 4 (a) has a solvable word problem.

**Problem 2** Show that Example 4 (c) has a solvable word problem.

**Problem 3** If $\mathbf{A}_\Pi$ is finite, show $\Pi$ has a solvable word problem.

**Problem 4** If $\mathbf{A}_\Pi$ is residually finite, show $\Pi$ has a solvable word problem.

**Problem 5** If $\mathbf{A}_\Pi$ is simple, show $\Pi$ has a solvable word problem.

# References


[1] S. Burris, Polynomial time uniform word problems. Math. Logic Quarterly **41** (1995), 173–182.

[2] O.G. Kharlampovich and M.V. Sapir, Algorithmic problems in varieties. Internat. J. Algebra Comput. 5 (1995), no. 4-5, 379–602.

[3] E.W. Mayr and A.R. Meyer, The complexity of the word problem for commutative semigroups and polynomial ideals. Adv. in Math. **46** (1982), 305–329.

[4] A.H. Mekler, E. Nelson, and S. Shelah, A variety with solvable, but not uniformly solvable, word problem. Proc. London Math. Soc. **66** (1993), 225–256.

[5] A. Selman, Calculii for axiomatically defined algebras. Algebra Universalis **2** (1972), 20–32.