EQUALITY ALGEBRAS

Desmond Fearnley-Sander and Tim Stokes

As part of an attempt to capture abstractly the most fundamental properties of algebraic reasoning involving equality, we introduce the notion of an *equality algebra*. It is a universal algebra A endowed with a binary function $=_i A \times A \to L$, where L is a meet-semilattice with top element 1, called *internalised equality*, and satisfying, for all $x, y \in A$,

1. $(x =_i x) = 1$; and
2. $(x =_i y)f(x) = (x =_i y)f(y)$, where f is any function $A \to L$ derived from the operations on A, the semilattice operations, and $=_i$.

We characterise internalised equalities in terms of finitely many identities, give examples, and show that all are equivalent to internalised equalities defined in terms of congruences on the underlying algebra. In the special case in which A is an Abelian group or ring, the internalised equality is shown to be equivalent to the dual of a norm-like mapping taking values in a semilattice.

All semilattices are assumed to be meet-semilattices with top element 1. Denote meet by $\wedge$ or juxtaposition.

Every semilattice L is a partially ordered set with respect to the order defined by setting $a \leqslant_L b$ if and only if $ab = b$ for all $a, b \in L$. Hence any inequality in a semilattice can be expressed as an equation.

1. Equality algebras

We shall say that any universal algebra A equipped with a function $=_i\colon A \times A \to L$ is an *e-algebra* over the semilattice L. Notation: $(A, L, =_i)$.

An e-algebra $(A, L, =_i)$ may be viewed as a many-sorted algebra having two sorts, *semilattice* having carrier L, and *underlying* having carrier A.

A *replacement algebra* over the semilattice L is an e-algebra over L for which, for all $x, y \in A$,

1. $(x =_i x) = 1$; and

2. $(x =_i y)f(x) = (x =_i y)f(y),$

for all functions $f : A \to L$ derived from the operations on A, the semilattice operations and $=_i$.

We call 1 *the reflexivity rule* and 2 *the replacement rule*. We call $=_i$, satisfying both rules, an *L-valued internalised equality* on A. An element of the form $(a =_i b)$ is called an *internalised equation*.

Taking the many-sorted view, a replacement algebra is an e-algebra $(A, L, =_i)$ for which the identity $(x =_i x) = 1$ and the family of identities

$$(x =_i y)f(x, x_1, x_2, \ldots, x_n) = (x =_i y)f(y, x_1, x_2, \ldots, x_n)$$

holds, where f ranges over all sort *semilattice* elements in the free e-algebra on countably many generators of each sort.

The motivation for defining equality algebras is simple enough – it is an attempt to capture abstractly and internalise the most basic kinds of reasoning involving equality: "$x = x$ is always true"; and "if x equals y and $p(x)$, then x equals y and $p(y)$, and conversely". Something formally close to replacement algebras is studied from a computer science point of view by Dijkstra and Scholten in [**2**], although there the semilattice is assumed to be a Boolean algebra. In comparison, our approach is more algebraic, the focus being on particular algebras equipped with semilattice-valued mappings rather than the generalised "Boolean structures" of Dijkstra and Scholten.

Among the many rules satisfied by $=_i$, the following are especially significant.

PROPOSITION 1.1.   *Let $(A, L, =_i)$ be a replacement algebra. For all $a, b, c \in A$,*

1. $(a =_i a) = 1;$
2. $(a =_i b) = (b =_i a);$
3. $(a =_i b)(b =_i c) \leqslant_L (a =_i c).$

For any n-ary operation on A and any $a_1, b_1, \ldots, a_n, b_n \in A$,

$$(a_1 =_i b_1) \cdots (a_n =_i b_n) \leqslant_L (\rho(a_1, \ldots, a_n) =_i \rho(b_1, \ldots, b_n)).$$

PROOF: We prove the parts in order. The first is immediate, and

$$(a =_i b) = (a =_i b)(b =_i b) = (a =_i b)(b =_i a) = (b =_i b)(b =_i a) = (b =_i a)$$

proves the second. For the third,

$$(a =_i b)(b =_i c)(a =_i c) = (a =_i b)(b =_i c)(b =_i c) = (a =_i b)(b =_i c).$$

For the final part,

$$\begin{aligned}
&(a_1 =_i b_1) \cdots (a_n =_i b_n)(\rho(a_1, \ldots, a_n) =_i \rho(b_1, \ldots, b_n)) \\
&= (a_1 =_i b_1) \cdots (a_n =_i b_n)(\rho(b_1, \ldots, b_n) =_i \rho(b_1, \ldots, b_n)) \\
&= (a_1 =_i b_1) \cdots (a_n =_i b_n).
\end{aligned}$$

Thus familiar general properties of equality are internalised. Let us call an e-algebra A over L which satisfies the above four properties an *equality algebra* over L.

It follows easily from the above result that the relation $\rho_{=_i} = \{(a,b) \mid a,b \in A, (a =_i b) = 1\}$ defined on A is a congruence relation. The idea of a *fuzzy relation* is defined over an arbitrary partially ordered set in [**3**]; a fuzzy relation defined on an algebra, taking values in a semilattice and satisfying the conditions of Proposition 1.1 seems a plausible candidate for the title of "fuzzy congruence".

Proposition 1.1 shows that every replacement algebra is an equality algebra. The converse is also true.

THEOREM 1.2. *Every equality algebra is a replacement algebra.*

PROOF: In proving the replacement rule, we may assume that x_1 actually appears in the element of sort *semilattice* $f(x_1, x_2, \ldots, x_n)$ of the free e-algebra, since otherwise there is nothing to prove. We give an inductive argument based on the *depth* of a specific way of writing $f(x_1, x_2, \ldots)$ using the operations of $(A, L, =_i)$ viewed as a two-sorted algebra, that is, the deepest bracketing that occurs in the expression. (For example $y(z(u =_i (v * w))))$ has depth four. One could be more precise in the definition of depth, but it seems unnecessary; obviously depth is not an invariant of f, but consideration of one representative way of writing it suffices.)

Fix n. We shall show for all m that for any sort *semilattice* $f(x_1, x_2, \ldots, x_n)$, of depth m, $(x =_i y) f(x, y_1, y_2, \ldots) = (x =_i y) f(y, y_1, y_2, \ldots)$ is an identity.

We begin by proving by induction that any f of the form $(g =_i h)$ satisfies this; we note that if f has such a form, then g, h have sort *underlying*.

Now $f(x_1, x_2, \ldots, x_n)$ cannot have depth zero as then it would not be of *semilattice* sort. If it is of depth one, then it has the form $(x =_i y)$ where x, y are of sort *underlying*, and then we are required to prove the identity $(x =_i y)(x =_i z) = (x =_i y)(y =_i z)$. Now $(a =_i b)(a =_i c) \leqslant_R (b =_i c)$ for all $a, b, c \in A$, so $(a =_i b)(a =_i c) \leqslant_R (a =_i b)(b =_i c)$. Reversing the argument establishes the desired equality.

If f is of depth two, then $f = (\rho(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_v}) =_i \sigma(x_{\delta_1}, x_{\delta_2}, \ldots, x_{\delta_w}))$, where ρ has arity v and σ has arity w and at least one of the $x_{\sigma_i}, x_{\delta_j}$ is x_1. Then, for a fixed substitution of $a_2, a_3, \ldots \in A$ for the variables other than x_1 in f, we can write $f(x_1, a_2, a_3, \ldots) = (g(x_1) =_i h(x_1))$, where g, h are derived operations of depth 1. Then $(g(a) =_i g(b)) \geqslant (a =_i b)$, as follows from the equality algebra axioms; thus $(a =_i b) = (g(a) =_i g(b))(a =_i b)$. Similarly, $(a =_i b) = (h(a) =_i h(b))(a =_i b)$. So from the depth 1 case considered above,

$$
\begin{aligned}
(a =_i b) f(a, a_2, a_3, \ldots) &= (a =_i b)(g(a) =_i h(a)) \\
&= (a =_i b)(g(a) =_i g(b))(h(a) =_i h(b))(g(a) =_i h(a)) \\
&= (a =_i b)(g(a) =_i g(b))(g(a) =_i h(b)) \\
&= (a =_i b)(g(b) =_i h(b))
\end{aligned}
$$

$$= \ (a =_i b) f(b, a_2, a_3, \ldots),$$

as required.

Assume that the result holds if f has depth at most $k - 1$.

For $f = (g =_i h)$ of depth at most k, and for a fixed substitution of $a_2, a_3, \ldots \in A$ for the variables other than x_1 in f, we can write $f(x_1, a_2, a_3, \ldots) = (g(x_1) =_i h(x_1))$, where g, h are derived operations of depth at most $k - 1$; thus (letting $x = x_1$) we may write $g(x) = \rho(g_1(x), g_2(x), \ldots, g_m(x))$, where ρ is an m-ary operation on A and each $g_i(x)$ is a (possibly constant) derived unary operation of depth at most $k - 2$ on A; similarly, $h(x) = \sigma(h_1(x), h_2(x), \ldots, h_p(x))$ for some p-ary σ and derived unaries h_i on A of depth at most $k - 2$. Then define $g_i'(x) = (g_i(x) =_i g_i(a))$, $g_i''(x) = (g_i(x) =_i g_i(b))$, and similarly $h_i'(x) = (h_i(x) =_i h_i(a))$ and $h_i''(x) = (h_i(x) =_i h_i(b))$. Note that $g_i'(a) = g_i''(b) = 1$ for all i, and $h_i'(a) = h_i''(b) = 1$ for all i, and that all the g_i', g_i'', h_i', h_i'' have depth at most $k - 1$. Hence by the inductive assumption,

$$
\begin{aligned}
(a =_i b) &= \ (a =_i b) g_1'(a) g_2'(a) \cdots g_m'(a) h_1'(a) h_2'(a) \cdots h_p'(a) \\
&= \ (a =_i b) g_1'(b) g_2'(b) \cdots g_m'(b) h_1'(b) h_2'(b) \cdots h_p'(b).
\end{aligned}
$$

It follows from this and the equality algebra axioms that

$$
\begin{aligned}
(a =_i b) f(a, a_2, a_3, \ldots) &= \ (a =_i b)(g(a) =_i h(a)) \\
&= \ (a =_i b)(\rho(g_1(a), \ldots, g_m(a))) =_i \sigma(h_1(a), \ldots, h_p(a)) \\
&= \ (a =_i b)(\rho(g_1(b), \ldots, g_m(b))) =_i \sigma(h_1(b), \ldots, h_p(b)) \\
&= \ (a =_i b)(g(b) =_i h(b)) \\
&= \ (a =_i b) f(b, a_2, a_3, \ldots),
\end{aligned}
$$

as required. This intermediate fact now follows: if $f = (g =_i h)$, then general replacement works for f.

We now return to the general problem, which we likewise prove by induction on the depth of f. But we need only consider f not of the form $(g =_i h)$. The depth zero and one cases are trivial. Assume that the result holds if $f(x_1, x_2, \ldots, x_n)$ has depth $k - 1$. If $f(x_1, x_2, \ldots, x_n)$ has depth k, then it must be of the following form: $g(x_1, x_2, \ldots, x_n) h(x_1, x_2, \ldots, x_n)$, where $g(x_1, x_2, \ldots, x_n)$ and $h(x_1, x_2, \ldots, x_n)$ each has depth at most $k - 1$.

But then

$$
\begin{aligned}
&(x =_i y) f(x, y_1, y_2, \ldots, y_{n-1}) \\
&= \ (x =_i y)(g(x, y_1, y_2, \ldots, y_{n-1}) h(x, y_1, y_2, \ldots, y_{n-1})) \\
&= \ ((x =_i y) g(x, y_1, y_2, \ldots, y_{n-1}))((x =_i y) h(x, y_1, y_2, \ldots, y_{n-1})) \\
&= \ ((x =_i y) g(y, y_1, y_2, \ldots, y_{n-1}))((x =_i y) h(y, y_1, y_2, \ldots, y_{n-1}))
\end{aligned}
$$

$$
\begin{aligned}
&= (x =_i y)(g(y, y_1, y_2, \ldots, y_{n-1})h(y, y_1, y_2, \ldots, y_{n-1})) \\
&= (x =_i y)f(y, y_1, y_2, \ldots, y_{n-1}).
\end{aligned}
$$

Thus in every case, $(x =_i y)f(x, y_1, y_2, \ldots, y_{n-1}) = (x =_i y)f(y, y_1, y_2, \ldots, y_{n-1})$, and the result follows in full generality. □

Thus replacement algebras and equality algebras are the same objects, and we adopt the name "equality algebra" exclusively from now on; similarly for the title "internalised equality". For a given variety of universal algebras, the equality algebras definable on members of the variety are essentially the same as the replacement algebras definable on them, a fact which one can phrase in terms of the existence of a term equivalence between varieties of two-sorted algebras in an obvious manner. The terms "group with equality" and "ring with equality" have the obvious meanings.

We say $(A, L, =_i)$ is a *strong* equality algebra if $(a =_i b) = 1$ implies $a = b$ for all a, b, and we then call $=_i$ a *strong internalised equality*. Writing $\Delta_A = \{(a, a) \mid a \in A\}$, the trivial congruence on A, it is obvious that $(A, L, =_i)$ is strong if and only if $\rho_{=_i} = \Delta_A$.

PROPOSITION 1.3. *Every equality algebra has a strong equality algebra as a homomorphic image.*

PROOF: Let $(A, L, =_i)$ be an equality algebra. For any $x, y \in A/\rho_{=_i}$, define $(x =_{s'} y) = (a =_i b)$ for any $a \in x, b \in y$; this is well-defined since if $(a =_i a') = (b =_i b') = 1$ then

$$
(a =_i b) = (a =_i b)(a =_i a')(b =_i b') \leqslant (a' =_i b)(b =_i b') \leqslant (a' =_i b'),
$$

and reversing the argument establishes equality. $=_{s'}$ is obviously a strong equality on $A/\rho_{=_i}$. The canonical mapping $f : A \to A/\rho_{=_i}$ together with the identity mapping $L \to L$ constitute a homomorphism $(A, L, =_i) \to (A/\rho_{=_i}, L, =_{s'})$. □

2. EXAMPLES

Let A be a universal algebra and S a set. Define $* : A^S \times A^S \to 2^S$ by setting $f * g = \{x \mid x \in S, f(x) = g(x)\}$. Then $*$ is easily seen to be a 2^S-valued internalised equality on A, (where in 2^S, meet is set intersection). Generalising, if S is a topological space, define $(f =_i g)$ to be the interior of $f * g$, again a 2^S-valued internalised equality on A (and in fact an $\mathcal{O}$-valued internalised equality, where $\mathcal{O}$ is the lattice of open sets of S).

Some important equality algebras are subalgebras of such examples. For instance, let $R = k[x_1, x_2, \ldots, x_n]$ be the polynomial ring in n variables over the field k. Then each $f \in R$ may be viewed as a function $k^n \to k$, and then $f * g = \mathcal{V}(f - g)$, the variety defined by $f - g$.

Another important special case is as follows: if $A = \{0,1\}$, a two-element set without operations, elements of A^S are essentially *characteristic functions* or, equivalently, subsets of S, and for all $U, V \in S$, $(U * V) = (U' \cap V') \cup (U \cap V)$. Indeed if R is any Boolean algebra, define $(a * b) = (a \wedge b) \vee (a' \wedge b') = a + b$ for all $a, b \in R$, the Boolean ring addition on R; then $*$ is an R-valued internalised equality on R.

We generalise to arbitrary direct products: if $X = \Pi_{i \in \mathcal{I}} X_i$, define $((a_i) *_\mathcal{I} (b_i)) = \{i \mid i \in \mathcal{I}, \ a_i = b_i\}$, for all $(a_i), (b_i) \in X$. Clearly $*_\mathcal{I}$ is a $2^\mathcal{I}$-valued internalised equality on X – the *coordinate equality*. This and the previous examples are strong internalised equalities.

Let A be an algebra and E a set of congruences on A (just equivalence relations if A has no operations). For $a, b \in A$, define $a *_E b = \{\rho \mid \rho \in E, \ a\rho b\}$. The coordinate equality on a direct product is a special case of this – hence the notation.

PROPOSITION 2.1. *For a set E of congruences on A, $*_E$ is a 2^E-valued internalised equality on A.*

PROOF: That $a *_E a = 1$ and $a *_E b = b *_E a$ for all $a, b \in A$ is obvious. For any $a, b, c \in A$, if $\rho \in (a *_E b) \cap (b *_E c)$, then $a\rho b$ and $b\rho c$, so $a\rho c$ and so $\rho \in a *_E c$.

For any n-ary operation ρ on A and any $a_1, b_1, \ldots, a_n, b_n \in A$, if $\sigma \in (a_1 *_E b_1) \cap \cdots \cap (a_n *_E b_n)$ then $(a_1, b_1) \in \sigma, \ldots, (a_n, b_n) \in \sigma$, so $(\rho(a_1, \ldots, a_n)), (\rho(b_1, \ldots, b_n)) \in \sigma$, and so $\sigma \in (\rho(a_1, \ldots, a_n)) *_E (\rho(b_1, \ldots, b_n))$.   ☐

If E is not the set of all congruences on A, $*_E$ need not be strong.

PROPOSITION 2.2. *Let $E = \{\rho_i \mid i \in \mathcal{I}\}$ be a collection of congruences on A. Then $*_E$ is strong if and only if $\bigcap_{i \in \mathcal{I}} \rho_i = \Delta_A$, whence there exists an embedding of $\left(A, 2^E, *_E\right)$ in $\left(\Pi_{i \in \mathcal{I}} A/\rho_i, 2^\mathcal{I}, *_\mathcal{I}\right)$.*

PROOF: For all $a, b \in A$, the following are equivalent: $(a *_E b) = E$; $a\rho b$ for all $\rho \in E$; $(a, b) \in \rho$ for all $\rho \in E$; $(a, b) \in \bigcap_{\rho \in E} \rho = \Delta_A$. The existence of the embedding $\phi : A \to \Pi_{i \in \mathcal{I}} A/\rho_i$ follows from a result of Kurosh, [4, p.183]; here, $\phi(a) = (\rho_i a)$, where $\rho_i a$ is the congruence class in A/ρ_i containing a. This embedding, together with the isomorphism $\psi : 2^E \to 2^\mathcal{I}$ defined by setting $\psi(S) = \{i \mid i \in \mathcal{I}, \ \rho_i \in S\}$, constitutes an isomorphism $(\phi, \psi) : \left(A, 2^E, *_E\right) \to \left(Im(\phi), 2^\mathcal{I}, *_\mathcal{I}\right)$.   ☐

If E is a collection of congruences on A such that the intersection of any subset of the relations in E is also in E, then we shall say that E is $\cap$-*closed*; for example, suppose E is all congruences on A. In such a case E constitutes a complete lattice in which meet is intersection, the join $\rho_1 \vee \rho_2$ is the intersection of all congruences in E containing both ρ_1 and ρ_2, and the bottom element is $0 = \bigcap_{\rho \in E} \rho$. There is a smallest congruence in E containing each $(a, b) \in A \times A$, namely the intersection of all congruences in E that contain (a, b); denote this by $\rho_{a,b}$. We adopt the convention of using the opposite of the usual inclusion ordering on E: we say $\rho_1 \leqslant \rho_2$ if and only if $\rho_2 \subseteq \rho_1$. Thus

semilattice meet (which we denote by juxtaposition to avoid confusion with intersection) is not intersection but rather the join of congruences in E as described above; further, the top element is the intersection of all congruences in E, which we refer to as 1. Now define $\circ_E : A \times A \to E$ by setting $(a \circ_E b) = \rho_{a,b}$ for all $a, b \in A$. Again, the coordinate equality on a direct product has essentially this form.

PROPOSITION 2.3.   *If E is a $\cap$-closed collection of congruences on A, then $\circ_E$ is an E-valued internalised equality on A, where E is given the opposite order to set inclusion.*

PROOF: For all $a, b, c \in A$, $\rho_{a,a} = \bigcap_{\rho \in E} \rho = 1$; $\rho_{a,b} = \rho_{b,a}$ is clear; and because $(a, b), (b, c) \in \rho_{a,b}\rho_{b,c}$, it follows that $(a, c) \in \rho_{a,b}\rho_{b,c}$, and so $\rho_{a,c} \subseteq \rho_{a,b}\rho_{b,c}$, that is, $\rho_{a,c} \geqslant \rho_{a,b}\rho_{b,c}$. Finally if σ is an operation on A of arity n, then $(a_1, b_1), \ldots, (a_n, b_n) \in \rho_{a_1,b_1} \cdots \rho_{a_n,b_n}$, so $(\sigma(a_1, \ldots, a_n), \sigma(b_1, \ldots, b_n)) \in \rho_{a_1,b_1} \cdots \rho_{a_n,b_n}$, and so $\rho_{\sigma(a_1,\ldots,a_n),\sigma(b_1,\ldots,b_n)} \geqslant \rho_{a_1,b_1} \cdots \rho_{a_n,b_n}$. $\square$

The internalised equality $\circ_E$ is strong if and only if the same condition holds on E as was required in Proposition 2.2. If E is the collection of all congruences on A, we call $\circ_E$ the *full congruence equality* on A; obviously it is strong.

Recall that an *ultrametric space* (X, d) is a metric space which satisfies $d(x, y) \leqslant max(d(x, z), d(y, z))$ for all $x, y, z \in X$ – the generalisation to pseudo-ultrametric spaces is obvious. Let $\leqslant^*$ be the reverse of the usual ordering on the non-negative reals $[0, \infty)$; then $L = ([0, \infty), \leqslant^*)$ is a $\wedge$-semilattice with top element zero and $a \wedge b = max(a, b)$ for all $a, b \in [0, \infty)$.

Then $=_d$ defined by setting $(a =_d b) = d(a, b)$ for all $a, b \in X$ is an L-valued internalised equality on X.

3. EQUIVALENCE

In an equality algebra $(A, L, =_i)$, all of the interesting behaviour occurs in the two-sorted subalgebra generated by A, that is, the equality algebra $(A, L_{=_i}, =_i)$, where $L_{=_i}$ is the subsemilattice of L generated by the internalised equations – elements of the form $(a =_i b)$ for some $a, b \in A$; the rest of L has no interaction with A. We say that equality algebras $(A_1, L_1, =_1)$ and $(A_2, L_2, =_2)$ are *equivalent* if their respective two-sorted subalgebras $\left(A_1, (L_1)_{=_1}, =_1\right)$ and $\left(A_2, (L_2)_{=_2}, =_2\right)$ are isomorphic. Equivalence is obviously an equivalence relation on equality algebras.

Let us say that the internalised equality $=_2$ on A taking values in L_2 is a *quotient* of the internalised equality $=_1$ on A taking values in L_1 if there is a mapping $\psi : L_1 \to L_2$ for which $\psi((a =_1 b)) = (a =_2 b)$ for all $a, b \in A$ and for which the restriction of ψ to $(L_1)_{=_1}$ is a homomorphism; in such a case it is clear that ψ maps $(L_1)_{=_1}$ onto $(L_2)_{=_2}$. We call such ψ a *quotient map*. If such a ψ exists with the additional property that its restriction to $(L_1)_{=_1}$ is an isomorphism, then we say $=_1$ and $=_2$ are *equivalent*, and ψ is an

equivalence map. The notion of equivalence is an equivalence relation on the collection of internalised equalities defined on A. Indeed this collection defines a category in which the objects are pairs $(L, =_i)$ where $=_i$ is an L-valued internalised equality on A and arrows are quotient maps; in this category, isomorphism is equivalence as defined above.

Clearly, $=_2$ is a quotient of $=_1$ if and only if there exists $\psi : L_1 \to L_2$ for which the two-sorted mapping $(I, \psi) : \left(A, (L_1)_{=_1}, =_1\right) \to \left(A, (L_2)_{=_2}, =_2\right)$, where $I : A \to A$ is the identity map, is a two-sorted homomorphism; $=_2$ and $=_1$ are equivalent if and only if this homomorphism is an isomorphism for some ψ. If $=_1, =_2$ defined on A are equivalent, then $(A, L_1, =_1)$ and $(A, L_2, =_2)$ are equivalent. More generally, $(A_1, L_1, =_1)$ and $(A_2, L_2, =_2)$ are equivalent if and only if there exists an isomorphism $\phi : A_1 \to A_2$ for which $=_{1'}$ given by $(a =_{1'} b) = (\phi(a) =_2 \phi(b))$ is an L_2-valued internalised equality on A_1 equivalent to $=_1$.

For any collection of congruences E on the algebra A, let

$$E^\cap = \{\rho \mid \rho \text{ is an intersection of elements of } E\}.$$

$E^\cap$ is a $\cap$-closed collection of congruences on E.

THEOREM 3.1. *Let E be a collection of congruences on an algebra A. Then the internalised equalities $*_E$ and $*_{E^\cap}$ on A are equivalent.*

PROOF: Define $\phi : 2^E \to 2^{(E^\cap)}$ by setting $\phi(\alpha) = \alpha^\cap$ for all $\alpha \subseteq E$. Now for any $a, b \in A$,

$$
\begin{aligned}
\phi(a *_E b) &= \{\rho \mid \rho \in E, (a, b) \in \rho\}^\cap \\
&= \{\rho \mid \rho \in E^\cap, (a, b) \in \rho\} \\
&= (a *_{E^\cap} b),
\end{aligned}
$$

so ϕ respects internalised equality.

For a finite intersection $\bigcap_i (a_i * b_i) \in 2^E{}_{*_E}$, where i ranges from 1 to n,

$$
\begin{aligned}
\phi\left(\bigcap_i (a_i *_{E^\cap} b_i)\right) &= \{\rho \mid \rho \in E, (a_i, b_i) \in \rho, i = 1, \dots, n\}^\cap \\
&= \{\rho \mid \rho \in E^\cap, (a_i, b_i) \in \rho, i = 1, \dots, n\} \\
&= \bigcap_i \{\rho \mid \rho \in E^\cap, (a_i, b_i) \in \rho\} \\
&= \bigcap_i \{\rho \mid \rho \in E, (a_i, b_i) \in \rho\}^\cap \\
&= \bigcap_i \phi(a_i *_E b_i),
\end{aligned}
$$

so ϕ is a $\cap$-homomorphism $\left(2^E\right)_{*_E} \to \left(2^{E^\cap}\right)_{*_{E^\cap}}$.

For finite intersections $\bigcap_i (a_i *_E b_i), \bigcap_j (c_j *_E d_j) \in 2^E{}_{*_E}$, suppose $\phi\left(\bigcap_i (a_i *_E b_i)\right) = \phi\left(\bigcap_j (c_j *_E d_j)\right)$. Now if $\rho \in \bigcap_i (a_i *_E b_i)$, then $(a_i, b_i) \in \rho$ for all i, and $\rho \in \left(\bigcap_i (a_i *_E b_i)\right)^\cap$

$= \left(\bigcap_j (c_j *_E d_j)\right)^{\cap}$, so ρ is an intersection of things in $\bigcap_j (c_j *_E d_j)$, say $\rho = \bigcap_k \rho_k$, where, for all j, $(c_j, d_j) \in \rho_k$ for all k. So $(c_j, d_j) \in \rho$ for all j, and so $\rho \in \left(\bigcap_j (c_j *_E d_j)\right)$, and so $\bigcap_i (a_i *_E b_i) \subseteq \bigcap_j (c_j *_E d_j)$. Reversing the argument gives equality, establishing that $\phi : 2^E{}_{*_E} \to 2^{(E^{\cap})}{}_{*_{E^{\cap}}}$ is one-to-one.

Surjectivity of $\phi : 2^E{}_{*_E} \to 2^{(E^{\cap})}{}_{*_{E^{\cap}}}$ now follows easily:

$$\phi\left(\bigcap_i a_i *_E b_i\right) = \bigcap_i \phi(a_i *_E b_i) = \bigcap_i (a_i *_{E^{\cap}} b_i).$$

Hence the map $\phi : 2^E{}_{*_E} \to 2^{(E^{\cap})}{}_{*_{E^{\cap}}}$ is an isomorphism which respects internalised equality, and so is an equivalence map.   ◻

4. Equality algebras and congruences

Let $(A, L, =_i)$ be a fixed equality algebra throughout this section. For all $\alpha \in L$, define

$$\rho_\alpha = \{(a, b) \mid a, b \in A, \alpha \leqslant (a =_i b)\},$$

and let $\mathcal{C}_{=_i} = \{\rho_\alpha \mid \alpha \in L\}$.

Lemma 4.1.   *For every $\alpha \in L$, ρ_α is a congruence on the underlying sort A.*

Proof: Let $\alpha \in L$. Then for all $a \in A$, $(a =_i a) = 1$, so $a\rho_\alpha a$. For all $a, b \in A$, if $a\rho_\alpha b$ then $(a =_i b) \geqslant \alpha$, so also $(b =_i a) = (a =_i b) \geqslant \alpha$, so $b\rho_\alpha a$. Finally, for $a, b, c \in A$, if $a\rho_\alpha b$ and $b\rho_\alpha c$, then $(a =_i b) \geqslant \alpha$ and $(b =_i c) \geqslant \alpha$, so $(a =_i c) \geqslant (a =_i b)(b =_i c) \geqslant \alpha$, and so $a\rho_\alpha c$. Hence ρ_α is an equivalence relation.

Now let σ be n-ary on A, with $a_1, b_1, \ldots, a_n, b_n \in A$. If $a_i \rho_\alpha b_i$ for each $i = 1, 2, \ldots, n$ then $(a_i =_i b_i) \geqslant \alpha$ for all i, so $\alpha \leqslant \wedge_i (a_i =_i b_i) \leqslant (\sigma(a_1, \ldots, a_n) =_i \sigma(b_1, \ldots, b_n))$, and so by definition, $\sigma(a_1, \ldots, a_n)\rho_\alpha\sigma(b_1, \ldots, b_n)$.   ◻

4.1. Sets of congruences characterisation   We showed in Proposition 2.1 that for any collection E of congruences on A, $*_E$ is a 2^E-valued internalised equality. Up to equivalence, every equality algebra arises in this way.

Theorem 4.2.   *The internalised equality $=_i$ on A is equivalent to $*_C$, where $C = \mathcal{C}_{=_i}$.*

Proof: Let $C = \mathcal{C}_{=_i}$. Define $\phi : L \to \left(2^C, \cap\right)$ by setting $\phi(\alpha) = \{\rho_\beta \mid \alpha \geqslant \beta\}$. Then ϕ is a semilattice homomorphism:

$$\begin{aligned}
\phi(\alpha\beta) &= \{\rho_\gamma \mid \alpha\beta \geqslant \gamma\} \\
&= \{\rho_\gamma \mid \alpha \geqslant \gamma \text{ and } \beta \geqslant \gamma\} \\
&= \{\rho_\gamma \mid \alpha \geqslant \gamma\} \cap \{\rho_\gamma \mid \beta \geqslant \gamma\} \\
&= \phi(\alpha) \cap \phi(\beta).
\end{aligned}$$

Restricted to $L_{=_i}$, ϕ is injective. For suppose $\phi(\wedge_j(a_j =_i b_j)) = \phi(\wedge_j(p_j =_i q_j))$, where the meets are finite. In particular this implies that if $\beta \leqslant \wedge_i(a_j =_i b_j)$, then there exists $\gamma \in L$ such that $\beta \leqslant (c =_i d)$ if and only if $\gamma \leqslant (c =_i d)$ and $\gamma \leqslant \wedge_j(p_j =_i q_j)$. Let $\beta = \wedge_j(a_j =_i b_j)$; it follows that there exists $\gamma \in L$ for which $\wedge_j(a_j =_i b_j) \leqslant (c =_i d)$ if and only if $\gamma \leqslant (c =_i d)$ and $\gamma \leqslant \wedge_j(p_j =_i q_j)$. So for all j, $(p_j =_i q_j) \geqslant \gamma$, so $\wedge_j(a_j =_i b_j) \leqslant (p_j =_i q_j)$ for all j and so $\wedge_j(a_j =_i b_j) \leqslant \wedge_j(p_j =_i q_j)$. Reversing the argument establishes equality.

It is also easy to see that ϕ maps onto $\left(2^C_{*_C}, \cap\right)$.

Finally, ϕ respects internalised equality:

$$\phi(a =_i b) = \{\rho_\beta \mid (a =_i b) \geqslant \beta\} = \{\rho_\beta \mid (a, b) \in \rho_\beta\} = a *_C b.$$

Thus ϕ is an equivalence map.   ☐

There are a number of immediate corollaries to this result. From Theorem 3.1, we have

COROLLARY 4.3. *The equality algebra $(A, L, =_i)$ is equivalent to an equality algebra $\left(A, 2^E, *_E\right)$ where E is a $\cap$-closed collection of congruences on A.*

From Propositions 2.2 and 1.3 we have

COROLLARY 4.4. *Let $(A, L, =_i)$ be a strong equality algebra. Then $(A, L, =_i)$ is equivalent to an equality subalgebra of $\left(\Pi_{i \in \mathcal{I}} A_i, 2^{\mathcal{I}}, =_{\mathcal{I}}\right)$, where the A_i are homomorphic images of A.*

COROLLARY 4.5. *Let $(A, L, =_i)$ be an equality algebra. Then $(A, L, =_i)$ has a homomorphic image in $\left(\Pi_{i \in \mathcal{I}} A_i, 2^{\mathcal{I}}, =_{\mathcal{I}}\right)$, where the A_i are homomorphic images of A.*

4.2. LATTICE OF CONGRUENCES CHARACTERISATION There is a characterisation following Proposition 2.3 also.

THEOREM 4.6. *The internalised equality $=_i$ on A is equivalent to $\circ_C$, where $C = \mathcal{C}_{=_i}$.*

PROOF: Let $C = \mathcal{C}_{=_i}$. Define $\psi : L \to C^\cap$ by setting $\psi(\alpha) = \rho_\alpha$. First note that for all $a, b \in A$,

$$\begin{aligned}
(a \circ_C b) &= \rho_{a,b} \\
&= \cap\{\rho_\alpha \mid \alpha \in L, (a, b) \in \rho_\alpha\} \\
&= \cap\{\rho_\alpha \mid \alpha \in L, (a =_i b) \geqslant \alpha\} \\
&= \rho_{(a =_i b)} \\
&= \psi(a =_i b).
\end{aligned}$$

Let ψ^* denote the restriction of ψ to $L_{=_i}$. Now for finitely many internalised equations $(a_j =_i b_j)$,

$$\wedge_j \psi((a_j =_i b_j)) = \cap\{\rho_\gamma \mid \gamma \in L, \psi(a_j =_i b_j) \subseteq \rho_\gamma \text{ for all } j\}$$

$$
\begin{aligned}
&= \cap\{\rho_\gamma \mid \gamma \in L, \rho_{(a_j =_i b_j)} \subseteq \rho_\gamma \text{ for all } j\} \\
&= \cap\{\rho_\gamma \mid \gamma \in L, (a_j =_i b_j) \geqslant \gamma \text{ for all } j\} \\
&= \cap\{\rho_\gamma \mid \gamma \in L, \wedge_j(a_j =_i b_j) \geqslant \gamma\} \\
&= \rho_{\wedge_j(a_j =_i b_j)} \\
&= \psi(\wedge_j(a_j =_i b_j)),
\end{aligned}
$$

so ψ^* is a homomorphism $L_{=_i} \to (C^\cap)_{\circ_C}$.

ψ^* has image $(C^\cap)_{\circ_C}$ since for any finite meet $\wedge_i(a_j \circ_C b_j) \in (C^\cap)_{\circ_C}$,

$$
\wedge_i(a_j \circ_C b_j) = \wedge_j \rho_{a_j, b_j} = \wedge_i \psi(a_j =_i b_j) = \psi(\wedge_i(a_j =_i b_j)).
$$

Finally, ψ^* is injective. For suppose $\psi(\wedge_j(a_j =_i b_j)) = \psi(\wedge_j(p_j =_i q_j))$ where the meets are finite. Now $(a_j =_i b_j) \geqslant \wedge_j(a_j =_i b_j)$, so $(a_j, b_j) \in \rho_{\wedge_j(a_j =_i b_j)} = \rho_{\wedge_j(p_j =_i q_j)}$, so by definition $(a_j =_i b_j) \geqslant \wedge_j(p_j =_i q_j)$, and so $\wedge_j(a_j =_i b_j) \geqslant \wedge_j(p_j =_i q_j)$. Reversing the argument proves equality. Thus ψ is an equivalence map.   ☐

This result allows us to show that, given an algebra A, the "free-est possible" internalised equality on A is the full congruence equality: the unique free object in the category of equality algebras defined on A.

THEOREM 4.7. *The internalised equality $=_i$ on A is a quotient of $\circ_E$, where E is the set of all congruences on A.*

PROOF: By Theorems 3.1 and 4.6, it suffices to show that $\circ_{D^\cap}$ is a quotient of $\circ_E$, where $D = \mathcal{C}_{=_i}$ and E is the set of all congruences on A. Let $C = D^\cap$. Define $\psi : E \to C$ by setting $\psi(\rho) = \cap\{\sigma \mid \sigma \in C, \rho \subseteq \sigma\}$. Then for any $\rho_1, \rho_2 \in E$,

$$
\begin{aligned}
\psi(\rho_1 \rho_2) &= \psi(\cap\{\rho \mid \rho \in E, \rho_1 \cup \rho_2 \subseteq \rho\}) \\
&= \cap\{\sigma \mid \sigma \in C, \rho_1 \cup \rho_2 \subseteq \sigma\} \\
&= \cap\{\sigma \mid \sigma \in C, \psi(\rho_1) \cup \psi(\rho_2) \subseteq \sigma\} \\
&= \psi(\rho_1)\psi(\rho_2).
\end{aligned}
$$

So ψ is a homomorphism, and is surjective: for all $\rho \in C$, $\psi(\rho) = \rho$. Finally, for all $a, b \in A$, letting $\rho^E_{a,b}$ denote the smallest congruence in E containing (a, b) and $\rho^C_{a,b}$ the smallest in C containing (a, b), we have that

$$
\psi(a \circ_E b) = \psi\left(\rho^E_{a,b}\right) = \cap\{\rho \mid \rho \in C, (a, b) \in \rho\} = \rho^C_{a,b} = (a \circ_C b),
$$

so ψ is a quotient mapping.   ☐

In the above proof we have actually shown that the two-sorted mapping $(I, \psi) : (A, E, \circ_E) \to (A, C, \circ_C)$, where I is the identity map $A \to A$ and $C = (\mathcal{C}_{=_i})^\cap$, is a surjective homomorphism.

5. SPECIAL CASES: ABELIAN GROUPS AND RINGS

For groups, congruences are in one-to-one correspondence with normal subgroups; more generally, for multi-operator groups, congruences are in one-to-one correspondence with ideals (see [**4**]), and congruence reduces to ideal membership. Correspondingly, an internalised equality on a (multi-operator) Abelian group can be expressed in terms of a unary operator.

Let L be a semilattice and G an Abelian group, the operation written additively. An *L-valued modal map* [ ] on G is a function $[\cdot] : G \to L$ for which the following conditions are satisfied for all $a, b \in G$:

1. $[0] = 1$;
2. $[-a] = [a]$; and
3. $[a][b] \leqslant [a + b]$.

If also $[a] = 1$ implies $a = 0$, we say $[\cdot]$ is *strong*.

If a modal map is defined on the Abelian group G, we say G is a *modal Abelian group*. If the opposite semilattice L' of L is used, the result is something akin to a pre-norm on G, but taking values in the join-semilattice with zero L' – this connection is explored in an example to follow.

The significance of modal Abelian groups for the current work lies in the following fact.

PROPOSITION 5.1. *The variety of modal Abelian groups is term equivalent to the variety of Abelian groups with equality.*

PROOF: Let G be an Abelian group and L a semilattice. If $[\cdot]$ is a (strong) L-valued modal map on G then $=_i$ given by $(a =_i b) = [a - b]$ for all $a, b \in A$ is a (strong) L-valued internalised equality on G for which $[a] = (a =_i 0)$: $(a =_i a) = [a - a] = 1$ (and in the strong case $(a =_i b) = 1$ implies $[a - b] = 1$ so $a - b = 0$); $(a =_i b) = [a - b] = [b - a] = (b =_i a)$; $(a =_i b)(b =_i c) = [a - b][b - c] \leqslant [a - b + b - c] = [a - c] = (a =_i c)$; $(a =_i b)(c =_i d) = [a - b][c - d] \leqslant [a - b + c - d] = [(a + c) - (b + d)] = (a + c =_i b + d)$; and finally, $[a] = [a - 0] = (a =_i 0)$.

Conversely, suppose $=_i$ is a (strong) L-valued internalised equality on G. Note first that

$$
\begin{aligned}
(a =_i b) &= (a =_i b)(-b =_i -b) \\
&= (a - b =_i b - b) \\
&\leqslant (a - b =_i 0) \\
&= (a - b =_i 0)(b =_i b) \\
&= (a - b + b =_i 0 + b) \\
&\leqslant (a =_i b),
\end{aligned}
$$

so $(a =_i b) = (a - b =_i 0)$ for all $a, b \in G$. Then $[\cdot]$ given by $[a] = (a =_i 0)$ is a (strong) L-valued modal map on G for which $(a =_i b) = [a - b]$: $[0] = (0 =_i 0) = 1$ (and in the strong case $[a] = 1$ implies $(a =_i 0) = 1$, so $a = 0$); $[-a] = (-a =_i 0) = (0 =_i a) = (a =_i 0) = [a]$; $[a][b] = (a =_i 0)(b =_i 0) = (a =_i 0)(0 =_i -b) \leqslant (a =_i -b) = [a + b]$; and finally, $(a =_i b) = (a - b =_i 0) = [a - b]$.   □

The above proof does not generalise to groups in general: a "modal map" on a non-Abelian group G induces an internalised equality on the underlying set of G, but not generally one which is compatible with the group operation.

It follows from Proposition 5.1 that the various notions and theorems for equality algebras and internalised equalities have analogs for modal Abelian groups and modal maps. In particular the notion of equivalence makes sense and we have the following corollaries of Theorems 4.2 and 4.6.

COROLLARY 5.2. *Let C be a collection of subgroups of the Abelian group G. Then $[\ ]_C$ defined by $[a]_C = \{S \mid S \in C, a \in S\}$ for all $a \in G$ is a 2^C-valued modal map on G, and every modal map on G is equivalent to one of this form. If C is $\cap$-closed, then $[\ ]_C'$ defined by $[a]_C' = \cap\{S \mid S \in C, a \in S\}$ for all $a \in G$ is a C-valued modal map on G (where C ordered by the opposite of set inclusion), and every modal map on G is equivalent to one of this form.*

The same analysis can be carried out for any variety of Ω-groups; we here single out (possibly non-associative) rings for special attention but the process is similar in other cases. A ring R is a *modal ring* if it has an additive L-valued modal map $[\ ]$ which additionally satisfies $[ab] \geqslant [a]$ and $[ab] \geqslant [b]$ for all $a, b \in R$; in this case we say $[\ ]$ is a *ring modal map*. Again, the notion of equivalence carries over to modal rings and ring modal maps.

Note that if L is a lattice, the latter condition is equivalent to $[ab] \geqslant [a] \vee [b]$, and if the opposite lattice to L is used, we obtain something reminiscent of a normed ring.

PROPOSITION 5.3. *The variety of modal rings is term equivalent to the variety of rings with equality.*

PROOF: The term equivalence is the same as that in Proposition 5.1.

Let $(R, L, =_i)$ be a ring with equality. Then $[\ ]$ defined by $[a] = (a =_i 0)$ for all $a \in R$ is an L-valued modal map on the additive group of R for which $(a =_i b) = [a - b]$; moreover, for all $a, b, c, d \in R$,

$$[ab - cd] = (ab =_i cd) \geqslant (a =_i c)(b =_i d) = [a - c][b - d].$$

The fact that $[ab] \geqslant [a]$ follows by putting $c = 0, d = b$; similarly for $[ab] \geqslant [b]$. So $[\ ]$ is a ring modal map.

Conversely, if $(R, L, [\cdot])$ is a modal ring, then $=_R$ defined by $(a =_R b) = [a - b]$ for all

$a, b \in R$ is an L-valued internalised equality on the Abelian group $(R, +)$, satisfying also

$$
\begin{aligned}
(ab =_i cd) & = [ab - cd] \\
& = [(a - c)b + c(b - d)] \\
& \geqslant [(a - c)b][c(b - d)] \\
& \geqslant [a - c][b - d] \\
& = (a =_i c)(b =_i d),
\end{aligned}
$$

so $(R, L, =_i)$ is a ring with equality. $\qquad\square$

COROLLARY 5.4. *Let C be a collection of ideals of the ring R. Then $[\ ]_C$ defined by $[a]_C = \{S \mid S \in C, a \in S\}$ for all $a \in R$ is a 2^C-valued ring modal map on R, and every ring modal map on R is equivalent to one of this form. If C is $\cap$-closed, then $[\ ]'_C$ defined by $[a]'_C = \cap\{S \mid S \in C, a \in S\}$ for all $a \in R$ is a ring modal map on R, and every ring modal map on R is equivalent to one of this form.*

Note that two different $\cap$-closed collections of ideals on a ring R can give rise to equivalent ring modal maps. For instance, let A be the polynomial ring over the field k in infinitely many variables, $k[x_1, x_2, \ldots]$. Let E be the collection of finitely generated ideals in A, C the collection of all ideals of A; then E is a subsemilattice of C, closed under ideal sums (that is, ideal meets with respect to the partial order of interest here), and moreover $[a]_E = [a]_C$ is the ideal generated by $a - b$, so the ring modal maps are equivalent. This shows more generally that two distinct $\cap$-closed collections of congruences on an algebra can give rise to equivalent equality algebras.

Recall the earlier example of a ring with equality: the polynomial ring in n variables over the field k, $R = k[x_1, x_2, \ldots, x_n]$. The 2^{k^n}-valued internalised equality $*$ on R defined by $f * g = \mathcal{V}(f - g)$ arises from the ring modal map $[\ ]$ defined by $[f] = \mathcal{V}(f)$, which equivalently arises from the $\cap$-closed lattice of ideals of the form $\mathcal{I}(S) = \{f \mid f \in R, f(a) = 0 \text{ for all } a \in S\}$ for S a subset of k^n (with order the reverse of set inclusion, as discussed earlier), reflecting the familiar Galois correspondence of algebraic geometry.

We conclude with a class of examples of importance in number theory. Let K be a field on which is defined a *non-Archimedian valuation* $|\cdot|$, taking values in an ordered group G. (See [1].) Thus for all $a, b \in K$,

1. $|a| \geqslant 0$ and $|a| = 0$ if and only if $a = 0$;
2. $|a + b| \leqslant max(|a|, |b|)$;
3. $|ab| = |a| \cdot |b|$.

The standard example is the field of rationals with the usual p-adic valuation (p prime), taking values in the non-negative reals and defined by $|0| = 0$, and $|x|_p = c^k$ for fixed $c \in (0, 1)$, where $x = p^k(a/b)$, $a \neq 0$, $gcd(a, b) = 1$, and p divides neither a nor b.

Let V be the *valuation ring* determined by $|\cdot|$: $V = \{a \mid a \in K, |a| \leqslant 1\}$. Now G is a $\vee$-semilattice satisfying $a \vee b = max(a, b)$, so $|a + b| \leqslant |a| \vee |b|$. $G' = \{a \mid a \in G,$

$0 \leqslant a \leqslant 1\}$ is a subsemilattice of G, and for all $a \in V$, $|a| \in G'$. Finally, for all $a, b \in V$, $|ab| \leqslant |a|$, $|ab| \leqslant |b|$, because $|a|$, $|b| \leqslant 1$. Dualising the order on G' and defining $[a] = |a|$, it follows immediately that $[\ ]$ is a G'-valued ring modal map on V.

The p-adic valuation is of course a pre-norm with respect to which both addition and multiplication are uniformly continuous. This analytic structure on V is typical of modal groups and rings: the modal map behaves like the dual of a pre-norm, and the resulting uniform structure is compatible with the operations and is often non-trivial. These remarks extend to equality algebras in general – one may view the dual of an internalised equality as something like a metric on the underlying algebra with respect to which all its operations are uniformly continuous. We shall explore these matters elsewhere.

REFERENCES

[1]   G. Bachman, *Introduction to p-adic numbers and valuation theory* (Academic Press, New York, 1964).

[2]   E.W. Dijkstra and C.S. Scholten, *Predicate calculus and program semantics* (Springer-Verlag, Berlin, Heidelberg, New York, 1989).

[3]   J.A. Goguen, '*L*-fuzzy sets', *J. Math. Anal. Appl.* **18** (1967), 145–174.

[4]   A.G. Kurosh, *Lectures on general algebra* (Chelsea Publishing Company, New York, 1965).

Department of Mathematics   Department of Mathematics and Statistics
University of Tasmania   Murdoch University
Hobart Tas 7000   Murdoch Wa 6150