Notes on Proving Arithmetic Equations

1 Expressions and Values

In these notes we describe a formal system for proving arithmetic equations. Our objective is to explain what it means to have a completely formal, automatically verifiable proof system, and to clarify the basic properties of such proof systems. Our objective is *not* to clarify the basic properties of numbers—we need to know these beforehand in order to understand and justify the proof system. For example, it will take some effort in our system to prove that $e \cdot 0 = 0$; the formal proof certainly does not make this equation any more or less obvious.

Definition 1.1. *Arithmetic expressions* (ae's) are defined inductively as follows:

- The numerals `0` and `1` are ae's.
- Any variable, x, is an ae.
- If e is an ae, then there is an ae called "*minus* e" which is abbreviated as $-e$.
- If e, f are ae's, then there is an ae called the "*sum* of e and f" which is abbreviated as $e + f$, and there is also an ae called the "*product* of e and f" which is abbreviated as $e \cdot f$ or ef.
- That's all.

We use the symbol $\mathbb{R}$ for the set of real numbers and $\mathbb{Z}$ for the set of all integers $\{0, 1, -1, 2, -2, \dots\}$.

In order to evaluate an ae, we need to know the values of the variables – what a Computer Scientist would call an *environment*. The kind of environments needed for ae's simply map each variable to a real number; these simple environments are called *valuations*.

Definition 1.2. A *valuation*, V, is a mapping from the set, *Var*, of variable symbols which may appear in ae's, into $\mathbb{R}$. The *value*, $val\,(e, V)$, of an ae, e, at a valuation, V, is defined by structural induction on ae's as follows:

- $val\,(\mathtt{0}, V) ::= 0$ and $val\,(\mathtt{1}, V) ::= 1$.
- $val\,(x, V) ::= V(x)$ for any variable, x.
- $val\,(-e, V) ::= -\,val\,(e, V)$.
- $val\,(e + f, V) ::= val\,(e, V) + val\,(f, V)$, and

- $val\,(e \cdot f, V) ::= val\,(e, V) \cdot val\,(f, V)$.

The *meaning*, $[\![e]\!]$, of an ae, e, is the function from valuations to $\mathbb{R}$ defined by:

$$[\![e]\!](V) ::= val\,(e, V)\,.$$

It is conventional to omit parentheses around the arguments of meaning functions, writing "$[\![e]\!]V$" instead of "$[\![e]\!](V)$."

Definition 1.3. An *arithmetic equation (aeq)* consists of two ae's called its *lefthand side* and its *righthand side*. The aeq with lefthand side e and righthand side f is abbreviated as "$e = f$". The aeq $e = f$ is *true* at valuation V, written

$$V \models (e = f),$$

iff $[\![e]\!]V = [\![f]\!]V$. The equation is *valid*, written

$$\models (e = f),$$

iff it is true at all valuations, that is, iff $[\![e]\!] = [\![f]\!]$.

Example 1.4. Let e_0, f_0 be the ae's

$$\begin{array}{lcl} e_0 & ::= & ((1 + (1 + 1)) \cdot (x + y)), \\ f_0 & ::= & ((y \cdot (x \cdot y)) + (-((1 + 1) + 1))). \end{array}$$

Let V_1 be a valuation such that $V_1(x) = 2$, and $V_1(y) = 3$. Then $val\,(e_0, V_1) = 15$ and $val\,(f_0, V_1) = 15$, so $V_1 \models (e_0 = f_0)$. Let V_2 be the valuation such that $V_2(v) = 0$ for all variables v. Then $val\,(e_0, V_2) = 0 \neq -3 = val\,(f_0, V_2)$, so $V_2 \not\models (e_0 = f_0)$. Thus, the aeq $e_0 = f_0$ is *not* valid.

As another example, note that equations of the following form are valid:

Lemma 1.5.

$$\models ((e \cdot (f + g)) = ((e \cdot f) + (e \cdot g)))$$

for all ae's e, f, g.

Proof. Let V be any valuation and l, m, n be the values of e, f, g at V. Then

$$[\![(e \cdot (f + g))]\!]V = l(m + n)$$

by definition of the meaning of ae's. Likewise,

$$[\![((e \cdot f) + (e \cdot g))]\!]V = lm + ln.$$

But $l(m + n) = lm + ln$ by the distributive law of arithmetic, so

$$[\![(e \cdot (f + g))]\!]V = [\![((e \cdot f) + (e \cdot g))]\!]V.$$

But V was arbitrary, so this equation must hold for all V, *i.e.*, the equation is valid. □

2 Equational Proofs

Definition 2.1. An aeq, C, is said to *follow by the transitivity rule* from the pair of aeq's A_1 and A_2 iff A_1 is of the form $e = f$, A_2 is of the form $f = g$, and C is of the form $e = g$.

We use the notation

$$e = f,\ f = g \quad \Longrightarrow \quad e = g$$

as a shorthand description of this rule. The aeq's to the left of $\Longrightarrow$ are called the *antecedents* of the rule, and the aeq to the right is called its *consequent*.

Along with transitivity, the *reflexivity, symmetry*, and *congruence rules* together are called the *standard equational inference rules*. They are described in Table 1. Note that the reflexive rule has no antecedents. Such rules without antecedents are usually called *axioms* and are just written as equations, omitting the symbol $\Longrightarrow$.

Table 1: Standard Equational Inference Rules.

	$\Longrightarrow$	$e = e$	(reflexivity)
$e = f$	$\Longrightarrow$	$f = e$	(symmetry)
$e = f,\ f = g$	$\Longrightarrow$	$e = g$	(transitivity)
$e_1 = e_2,\ f_1 = f_2$	$\Longrightarrow$	$e_1 + f_1 = e_2 + f_2$	($+$-congruence)
$e_1 = e_2,\ f_1 = f_2$	$\Longrightarrow$	$e_1 * f_1 = e_2 * f_2$	($*$-congruence)
$e = f$	$\Longrightarrow$	$-e = -f$	($-$-congruence)

To capture the properties of arithmetic, we will need some additional axioms. These *equational axioms for arithmetic* are all the aeq's of the forms given in Table 2.

Table 2: Equational Axioms for Arithmetic

$(e + f) + g$	$=$	$e + (f + g)$	(associativity of $+$)
$(e \cdot f) \cdot g$	$=$	$e \cdot (f \cdot g)$	(associativity of $\cdot$)
$e + f$	$=$	$f + e$	(commutativity of $+$)
$e \cdot f$	$=$	$f \cdot e$	(commutativity of $\cdot$)
$0 + e$	$=$	e	(identity for $+$)
$1 \cdot e$	$=$	e	(identity for $\cdot$)
$e + (-e)$	$=$	0	(inverse for $+$)
$e \cdot (f + g)$	$=$	$(e \cdot f) + (e \cdot g)$	(distributivity)

Definition 2.2. An *arithmetic equational proof* is a finite sequence of aeq's such that every aeq in the sequence follows from aeq's earlier in the sequence by one of the standard equational inference rules or axioms of arithmetic. An aeq, $e = f$, is *equationally provable*, written

$$\vdash e = f,$$

iff it is the last equation of some proof.

A crucial property of formal proofs is that they can be checked automatically, *i.e.*, by a program, without any need for "understanding" of the subject matter by the checker. Adding comments to an equational proof can make proof checking easier, but it is not strictly necessary, since it is not hard to program a checker for uncommented proofs.

Figure 1 contains a formal proof of the equation $(f + g) + -g = f$. For the reader's convenience, the names of the rules from which each equation follows have been included as a comment after the equation.

Figure 1: An arithmetic equational proof.

$g + -g$	$=$	0	(inverse for $+$)
f	$=$	f	(reflexivity)
$f + (g + -g)$	$=$	$f + 0$	(congruence)
$(f + g) + -g$	$=$	$f + (g + -g)$	(associativity of $+$)
$(f + g) + -g$	$=$	$f + 0$	(transitivity)
$f + 0$	$=$	$0 + f$	(symmetry)
$(f + g) + -g$	$=$	$0 + f$	(transitivity)
$0 + f$	$=$	f	(identity for $+$)
$(f + g) + -g$	$=$	f	(transitivity)

Using this formal proof, we can show:

Lemma 2.3. *For all ae's e,*

$$\vdash 0 = 0 \cdot e.$$

Proof. Figure 2 exhibits a formal proof with rule names as comments. □

Figure 2: A proof of $0 = e \cdot 0$.

$0 + 1$	$=$	1	(identity for $+$)
e	$=$	e	(reflexivity)
$e \cdot (0 + 1)$	$=$	$e \cdot 1$	(congruence)
$e \cdot 1$	$=$	$e \cdot (0 + 1)$	(symmetry)
$e \cdot (0 + 1)$	$=$	$(e \cdot 0) + (e \cdot 1)$	(distributivity)
$e \cdot 1$	$=$	$(e \cdot 0) + (e \cdot 1)$	(transitivity)
$-(e \cdot 1)$	$=$	$-(e \cdot 1)$	(reflexivity)
$(e \cdot 1) + -(e \cdot 1)$	$=$	$((e \cdot 0) + (e \cdot 1)) + -(e \cdot 1)$	(congruence)
$\vdots$			
(Insert proof from	Fig. 1	with f, g replaced by $e \cdot 0, e \cdot 1$, respectively).	
$\vdots$			
$(e \cdot 1) + -(e \cdot 1)$	$=$	$e \cdot 0$	(transitivity)
$(e \cdot 1) + -(e \cdot 1)$	$=$	0	(inverse for $+$)
0	$=$	$(e \cdot 1) + -(e \cdot 1)$	(symmetry)
0	$=$	$e \cdot 0$	(transitivity)

The axioms of Table 2 are so fundamental that they have a special mathematical name: *the commutative ring axioms*. Any set of elements with $+, \cdot, -$ operations satisfying these axioms is called a *commutative ring*. In addition to $\mathbb{R}$, other examples of commutative rings are the integers, $\mathbb{Z}$, the rational numbers, $\mathbb{Q}$, the complex numbers, $\mathbb{C}$, and $\mathbb{Z}_n$, the integers modulo n.

Problem 1. **(a)** Show that $\vdash -e = -1 \cdot e$.

(b) Show that $\vdash\ 1 = -1 \cdot -1$.

Problem 2. Define the set of *Arithmetic Equational Theorems* (aet's) inductively as follows:

- every equational axiom of arithmetic is an aet.
- if all the antecedents of a standard equational inference rule are aet's, then so is the consequent.

Prove that the set of equationally provable aeq's equals the set of aet's.

Problem 3. For arithmetic expressions e, f and variable x, the *substitution*, $e[x := f]$, of f for x in e is defined by induction on e:

$$\begin{array}{rcl} x[x := f] & ::= & f, \\ c[x := f] & ::= & c \quad \text{for any constant or variable, } c, \text{ distinct from } x, \\ (-e_0)[x := f] & ::= & -(e_0[x := f]), \\ (e_0\ op\ e_1)[x := f] & ::= & e_0[x := f]\ op\ e_1[x := f], \quad \text{where } op\ \in \{+, \cdot\} \end{array}$$

(a) Prove that

$$\vdash f = g \text{ implies } \vdash\ e[x := f] = e[x := g].$$

(b) Prove that

$$\vdash e = g \text{ implies } \vdash\ e[x := f] = g[x := f].$$

Problem 4. Repeat 1, using the results of the previous two problems to simplify the argument.

The validity of the distributivity axiom—Lemma 1.5—followed directly from the distributivity of the integers and definition of the value of an ae. It is equally easy to see that all the other equational axioms of arithmetic of Table 2 are valid as well.

A rule of inference is *validity-preserving* if the consequent of the rule is valid whenever all its antecedents are valid. For example, it follows directly from the symmetry of mathematical equality, that the (symmetry) inference rule of our formal equational proof system is validity-preserving. Clearly all the standard equational inference rules of Table 1 are also validity-preserving. As a consequence, we have:

Theorem 2.4. *(*Soundness*)*

$$\vdash e = f \quad \textit{implies} \quad \models e = f.$$

Proof. Immediate by induction on the definition of arithmetic equational theorems given in Problem 2, using the fact that the inference rules are validity-preserving. □

3 Canonical Forms

The only numerals defined to occur in aeq's are `0` and `1`—not `2`, `3`, ... We don't need these other numerals since there are expressions for them, *e.g.*, `1 + 1` is an expression whose meaning is the integer two. It *is* useful to have a standard expression, or *canonical form*, for every integer:

Definition 3.1. For integers $n \geq 0$ define ae's $\hat{n}$ and $\widehat{-n}$ inductively:

- $\hat{0} ::= \mathtt{0}$,
- $\widehat{n+1} ::= \mathtt{1} + \hat{n}$,
- $\widehat{-(n+1)} ::= (-1) + \widehat{-n}$.

For example,

$$\begin{array}{rcl} \hat{3} & \text{is} & 1 + (1 + (1 + 0)), \\ \widehat{-2} & \text{is} & (-1) + ((-1) + 0). \end{array}$$

Problem 5. Prove that $[\![\hat{n}]\!]V = n$ for all $n \in \mathbb{Z}$ and valuations V.

Problem 6. **(a)** Show that $\vdash (\mathtt{1} + \hat{n}) = \widehat{n+1}$ for all $n \in \mathbb{Z}$.

(b) Show that $\vdash (\mathtt{-1}) + \hat{n} = \widehat{n-1}$ for all $n \in \mathbb{Z}$.

(c) Show that $\vdash (\hat{n} + \hat{m}) = \widehat{n+m}$ for all $m, n \in \mathbb{Z}$. (hint: Induction on magnitude of n.)

(d) Show that $\vdash (\hat{n} \cdot \hat{m}) = \widehat{n \cdot m}$ for all $m, n \in \mathbb{Z}$.

(e) Show that $\vdash -\hat{n} = \widehat{-n}$ for all $n. \in \mathbb{Z}$.

(f) Let e be an arbitrary ae in which there are no occurrences of variables. Conclude that for all valuations V,

$$\vdash e = \widehat{[\![e]\!]V}.$$

(hint: Structural induction on e.)

Lemma 3.2. *(Completeness for Constant Expressions) Let e, f be ae's in which there are no occurrences of variables. Then*

$$\models e = f \quad \textit{implies} \quad \vdash e = f.$$

Proof. Choose some fixed valuation V. From $\models e = f$, we have $[\![e]\!]V = [\![f]\!]V = n$ for some $n \in \mathbb{Z}$. By f, part (f), $\vdash e = \hat{n}$ and $\vdash f = \hat{n}$, so $\vdash e = f$ by symmetry and transitivity. □

The usual canonical form for a polynomial in x is

$$c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$$

where the leading coefficient c_n is nonzero. We use instead the "sparse" canonical form

$$c_{n_1} x^{n_1} + c_{n_2} x^{n_2} + \ldots + c_{n_k} x^{n_k}$$

where $n_1 > n_2 > \ldots$ and *all* coefficients are nonzero. We generalize to more than one variable by treating, for example, a polynomial in variables y and x as a polynomial in y with coefficients which are polynomials in x. Here is the precise definition:

Definition 3.3. For any ae e and integer $n \geq 1$, let $e^1 ::= e$ and $e^{n+1} ::= (e \cdot e^n)$.

Let L be a sequence of distinct variables. An *L-canonical arithmetic expression of degree $d \in \mathbb{N}$* is defined by induction on the length of L:

- If L is empty, then the L-canonical ae's of degree 0 are precisely the ae's of the form $\hat{n}$ for $n \in \mathbb{Z}$. In this case, there are no L-canonical ae's of positive degree.
- If L begins with the variable x, and L' is the rest of L, then the L-canonical ae's of degree d are defined by induction on d:
  - the L-canonical ae's of degree 0 are the L'-canonical ae's (of any degree),
  - the L-canonical ae's of degree $d > 0$ are those ae's of the form

    $$(a \cdot x^d) + c,$$

    or

    $$a \cdot x^d,$$

    where a is a nonzero L'-canonical form, and c is a nonzero L-canonical form of degree $< d$.

Problem 7. Describe an x, y, z-canonical form with the same meaning as $((x + (\widehat{-3} \cdot y^2)) + z^3)^2$.

Theorem 3.4. *Let e be an arithmetic expression and L a sequence of distinct variables including all the variables occurring in e. Then there is an L-canonical form c such that $\vdash e = c$.*

Proof. (Sketch) First prove by induction on d that the sum of an L-canonical form of degree d and any L-canonical form is provably equal to an L-canonical form. Use this to prove that a product of two L-canonical forms, as well as the negative of an L-canonical form, is provably equal to an L-canonical form. Then proceed by structural induction on e. □

Lemma 3.5. *If c and d are syntactically distinct L-canonical forms for some L, then $[\![c]\!] \neq [\![d]\!]$.*

Proof. (Sketch) By induction on the length of L. The induction step uses the fact that if p, q are polynomials in the same variable, x, with real number coefficients, then if the degree of p is greater than that of q, or they have the same degree and the absolute value of the leading coefficient of p is greater than that of q, then the absolute value of p is greater that the absolute value of q for all large enough values of x. □

Theorem 3.6. *(Completeness) For all ae's e, f,*

$$\models e = f \quad \textit{implies} \quad \vdash e = f.$$

Proof. Let L be a sequence of distinct variables including all the variables occurring in either of e or f. By Theorem 3.4, $\vdash e = c$ and $\vdash f = d$ for some L-canonical forms c, d. By Soundness, we have $[\![e]\!] = [\![c]\!]$ and $[\![f]\!] = [\![d]\!]$. Now if $\models e = f$, then $[\![e]\!] = [\![f]\!]$, so $[\![c]\!] = [\![d]\!]$. Then by Lemma 3.5, c and d must be syntactically identical, so we really have $\vdash e = c$ and $\vdash f = c$, from which $\vdash e = f$ follows by symmetry and transitivity. □

Problem 8. Let e be an ae and L a sequence of distinct variables including all the variables in e. Show that there is a *unique* L-canonical form c such that $\vdash e = c$.

The development above extends easily to arithmetic expressions that are to be evaluated over subsets, A, of the real numbers that are closed under the arithmetic operations. We'll use the notation $\models_A e = f$ to indicate that $V \models e = f$ for all valuations, V, in which all variables have values in A. For example, $\models_{\mathbb{Z}}$ indicates validity when all variables must be integer-valued. In particular, the notion of validity considered above is $\models_{\mathbb{R}}$.

Problem 9. Prove that

$$\models_{\mathbb{R}} e = f \quad \text{iff} \quad \models_{\mathbb{Z}} e = f.$$