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 $e \times 0 = 0$; 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 $\mathtt{0}$, $\mathtt{1}$ are ae's.
- Any variable, x, is an ae.
- If e is an ae, then so is $\mathtt{(-}e\mathtt{)}$.
- If e, f are ae's, then so are $\mathtt{(}e\ \mathtt{+}\ f\mathtt{)}$ and $\mathtt{(}e\ \mathtt{*}\ f\mathtt{)}$.
- That's all.

Definition 1.2 A *valuation*, V, is a mapping from the set, *Var*, of variable symbols which may appear in ae's, into the integers, $\mathbb{Z}$. 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.
- $val(\mathtt{(-}e\mathtt{)}, V) = -val(e, V)$.
- $val(\mathtt{(}e\ \mathtt{+}\ f\mathtt{)}, V) = val(e, V) + val(f, V)$, and
- $val(\mathtt{(}e\ \mathtt{*}\ f\mathtt{)}, V) = val(e, V) \times val(f, V)$.

The *meaning*, $[\![e]\!]$, of an ae, e, is the function from valuations to $\mathbb{Z}$ 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) is an expression of the form $(e\ \texttt{=}\ f)$ where e, f are ae's. The aeq is *true* at valuation V, written

$$V \models (e\ \texttt{=}\ f),$$

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

$$\models (e\ \texttt{=}\ f)$$

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

Example 1 Let e_0, f_0 be the ae's

$$\begin{aligned} e_0 &::= \texttt{((1 + (1 + 1)) * (x + y))},\\ f_0 &::= \texttt{((y * (x * y)) + (-((1 + 1) + 1)))}. \end{aligned}$$

Let V_1 be a valuation such that $V_1(\texttt{x}) = 2$, and $V_1(\texttt{y}) = 3$. Then $val(e_0, V_1) = 15$ and $val(f_0, V_1) = 15$, so $V_1 \models (e_0\ \texttt{=}\ f_0)$. 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 $(e_0\ \texttt{=}\ f_0)$ is *not* valid.

Here is an example of a set of valid equations:

Lemma 1.4

$$\models (\ (e\ \texttt{*}\ (f\ \texttt{+}\ g))\ \texttt{=}\ ((e\ \texttt{*}\ f)\ \texttt{+}\ (e\ \texttt{*}\ g))\ )$$

for all ae's e, f, g.

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

$$[\![(e\ \texttt{*}\ (f\ \texttt{+}\ g))]\!]V = l(m+n)$$

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

$$[\![((e\ \texttt{*}\ f)\ \texttt{+}\ (e\ \texttt{*}\ g))]\!]V = lm + ln.$$

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

$$[\![(e\ \texttt{*}\ (f\ \texttt{+}\ g))]\!]V = [\![((e\ \texttt{*}\ f)\ \texttt{+}\ (e\ \texttt{*}\ g))]\!]V.$$

■

2 Equational Proofs

We've been careful so far to distinguish the actual symbols "), $*$,"... in ae's from the mathematical symbols "*)*, x, e, f" used to describe ae's. To keep our notation uncluttered, from now on we will use less formal descriptions when there is no danger of ambiguity—in particular, we often will omit parentheses and use one font throughout expressions. For example, the valid equations of Lemma 1.4 above will now be written as

$$e * (f + g) = (e * f) + (e * g).$$

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

$$\frac{e = f, \quad f = g}{e = g} \text{ (transitivity)}$$

as a shorthand description of this rule. The aeq's above the horizontal line are called the *antecedents* of the rule, and the aeq below the line is called its *consequent.*

The *symmetry rule* is similarly described by:

$$\frac{e = f}{f = e} \text{ (symmetry)}$$

The *congruence rule* has one case for each arithmetic operator:

$$\frac{e = f}{-e = -f} \qquad \frac{e_1 = f_1, \quad e_2 = f_2}{e_1 + e_2 = f_1 + f_2} \qquad \frac{e_1 = f_1, \quad e_2 = f_2}{e_1 * e_2 = f_1 * f_2} \text{ (congruence)}$$

The *reflexive* rule is

$$\frac{}{e = e} \text{ (reflexivity)}$$

The rules above are called the *standard equational inference rules.*

Note that the reflexive rule has no antecedents. Such rules without antecedents are usually called *axioms* and are simply written as equations, omitting the horizontal line.

To capture the properties of arithmetic expressions, we will need some additional axioms. These *equational axioms for arithmetic* are all the aeq's of the forms given in Table 1.

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.

Table 1: Equational Axioms for Arithmetic

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

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,

$$\vdash 0 = 0 * e.$$

Proof. Figure 2 exhibits a formal proof along with rule name comments. ∎

Problem 1. 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.

Figure 2: A proof of $0 = e * 0$.

$0+1$	$=$	1	(identity for $+$)
e	$=$	e	(reflexivity)
$e*(0+1)$	$=$	$e*1$	(congruence)
$e*1$	$=$	$e*(0+1)$	(symmetry)
$e*(0+1)$	$=$	$(e*0)+(e*1)$	(distributivity)
$e*1$	$=$	$(e*0)+(e*1)$	(transitivity)
$-(e*1)$	$=$	$-(e*1)$	(reflexivity)
$(e*1)+-(e*1)$	$=$	$((e*0)+(e*1))+-(e*1)$	(congruence)
$\vdots$			
(Insert proof	from	Figure 1 with $e*0, e*1$ for f, g).	
$\vdots$			
$(e*1)+-(e*1)$	$=$	$e*0$	(transitivity)
$(e*1)+-(e*1)$	$=$	0	(inverse for $+$)
0	$=$	$(e*1)+-(e*1)$	(symmetry)
0	$=$	$e*0$	(transitivity)

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

Problem 2. **(a)** Show that $\vdash -e = -1 * e$.
(b) Show that $\vdash 1 = -1 * -1$.

In Lemma 1.4, we saw that the validity of the distributivity axiom followed directly from the distributivity of the integers and definition of the value of an ae. It is easy to see that all the other equational axioms of arithmetic 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. It is equally easy to see that all the standard equational inference rules above are validity-preserving. Thus,

Theorem 2.4 (*Soundness*)

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

Proof. Immediate by induction on the definition of arithmetic equational theorems given in Problem 1, using the fact that the inference rules are validity-preserving. ∎

3 Canonical Forms

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

- $\hat{0} = \texttt{0}$,
- $\widehat{n+1} = \texttt{(1 + } \hat{n}\texttt{)}$,
- $\widehat{-(n+1)} = \texttt{((-1) + } \widehat{-n}\texttt{)}$

For example,

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

Problem 3. Prove that $[\![\hat{n}]\!]V = n$ for all $n \in \mathbb{Z}$ and valuations V.

Problem 4. **(a)** Show that $\vdash \texttt{(1 + } \hat{n}\texttt{)} = \widehat{n+1}$ for all $n \in \mathbb{Z}$.

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

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

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

(e) Show that $\vdash \texttt{(-}\hat{n}\texttt{)} = \widehat{-n}$ 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

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

Proof. Choose some fixed valuation V. From $\models e = f$, we have $[\![e]\!]V = [\![f]\!]V = n$ for some $n \in \mathbb{Z}$. By Problem 4, part (f), $\vdash e = \hat{n}$ and $\vdash f = \hat{n}$, so $\vdash e = f$ by symmetry and transitivity. ■

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

Let L be a sequence of distinct variables. An *L-canonical arithmetic expression of degree $d \geq 0$* 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 (no matter what their degrees).

– The L-canonical ae's of degree $d+1$ are those ae's of the form

$$\texttt{((}a \texttt{ * } x^{d+1}\texttt{) + }c\texttt{)}$$

where $a \neq \texttt{0}$ is an L'-canonical form (of any degree) and c is an L-canonical form of degree $\leq d$.

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,

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

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 5. **(a)** 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 $\vdash e = c$.

(b) Describe the x, y, z-canonical form of $((x + (\widehat{-3} * y^2)) + z^3)^2$.

Problem 6. The development above extends easily to arithmetic expressions over the *real numbers* simply by allowing valuations in which the values of variables may be real numbers. (For uniformity, we keep the syntax unaltered, so the only numbers definable by variable-free ae's are still the integers.) We say an aeq $e = f$ is *valid over the reals*,

$$\models_{\mathbb{R}} e = f,$$

iff it holds for all real-valued valuations. Prove that

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

4 Arithmetic Inequalities

We can extend our formal proof system to include arithmetic *in*equalities.

Definition 4.1 An *arithmetic inequality* (aineq) is an expression of the form $(e \texttt{ <= } f)$ where e, f are ae's. The aineq is *true* at valuation V, written

$$V \models (e \texttt{ <= } f)$$

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

$$\models (e \texttt{ <= } f)$$

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

We add some additional inference rules for inequalities:

$$\frac{e = f}{e \leq f}\ (\leq\text{-reflexivity})$$

$$\frac{e \leq f, \quad f \leq e}{f = e}\ (\leq\text{-antisymmetry})$$

$$\frac{e \leq f, \quad f \leq g}{e \leq g}\ (\leq\text{-transitivity})$$

$$\frac{e \leq f}{e + g \leq f + g} \qquad \frac{e \leq f, \quad 0 \leq g}{e * g \leq f * g} \qquad \frac{e \leq f}{-f \leq -e} \quad (\leq\text{-congruence})$$

$$0 \leq 1 \quad \text{(01-axiom)}$$

Problem 7. (Completeness for constant inequalities)

(a) Show that $n \leq m$ iff $\vdash (\hat{n} \texttt{ <= } \hat{m})$.

(b) Conclude that if e, f are ae's with no occurrences of variables, then

$$\models e \leq f \quad \text{implies} \quad \vdash e \leq f.$$

Since we are now considering two notions of validity—over the reals and over the integers—we'll use the notation $\models_{\mathbb{Z}}$ for $\models$ when it is helpful to emphasize our original notion of validity. We also have two proof systems, the original one for just equality and the system extended with the rules for inequalities. We'll use the notations $\vdash_{=}$ and $\vdash_{\leq}$ when it's useful to emphasize the relevant proof system.

In contrast to the situation for equalities, cf. Problem 6, validity of inequalities over the integers does not agree with validity over the reals. For example,

$$\begin{aligned} \models_{\mathbb{Z}} 0 &\leq x * (x + -1), \\ \not\models_{\mathbb{R}} 0 &\leq x * (x + -1). \end{aligned}$$

Lemma 4.2 (Incompleteness for $\vdash_{\leq}$) There is an arithmetic inequality which is valid over the integers but not provable in the system above, namely,

$$\begin{aligned} \models_{\mathbb{Z}} 0 &\leq x * (x + -1), \\ \not\vdash_{\leq} 0 &\leq x * (x + -1). \end{aligned}$$

Proof. All the rules in our proof system are validity-preserving over the reals, so an inequality which is not valid over the reals cannot be provable. ∎

This particular discrepancy between validity and provability can be regarded an oversight in the design of our proof system. We could try to repair it simply by adding the "missing" inequality as an axiom. That is, if we define $\vdash_{xx-1}$ to have the rules of $\vdash_{\leq}$ along with the axiom $0 \leq x * (x + -1)$, then the resulting proof system remains sound over the integers (though not over the reals any more). Now, of course, the formerly missing inequality is immediately $\vdash_{xx-1}$ provable. This is an *ad hoc* repair, and it would not be surprising if $\vdash_{xx-1}$ was itself still incomplete over the integers.

However, given our success in finding a complete proof system for arithmetic equalities over the integers, we might hope to achieve the same thing for inequalities. One of the great mathematical results of the Twentieth Century is that **there is *no* sound, complete proof system for arithmetic inequalities over the integers**. In fact, given a proof checking program for any sound proof system for integer inequalities, it is possible to construct, from the text of the checking program, a valid inequality which has no proof recognizable by the checker! This is a consequence of the Undecidability of the Halting Problem for programs and Matijasevich's negative solution to Hilbert's Tenth Problem, topics which are taken up in more advanced courses in Theory of Computation such as 6.044 or 6.045.

Problem 8. (For discussion) We have explained that, given any proof checking program for a sound proof system for arithmetic inequalities over the integers, we can construct a valid inequality which has no proof in the system. But if the inequality has no proof, how can we possibly know it is valid?