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

- The numerals `0`, `1` are ae's.
- Any variable, x, is an ae.
- If e is an ae, then so is $\texttt{(-}e\texttt{)}$.
- If e, f are ae's, then so are $\texttt{(}e \texttt{ + } f\texttt{)}$ and $\texttt{(}e \texttt{ * } f\texttt{)}$.
- That's all.

We use the symbol $\mathbb{Z}$ for the set of all integers $\{0, 1, -1, 2, -2, \ldots\}$.

Definition 2. A *valuation*, V, is a mapping from the set, *Var*, of variable symbols which may appear in ae's, into $\mathbb{Z}$. The *value*, $val(e, V)$, of an ae, e, at a valuation, V, is defined by structural induction on ae's as follows:

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

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

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

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

Example. Let e_0, f_0 be the ae's

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

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 $V_2 \not\models (e_0\ \texttt{=}\ f_0)$. Thus, $(e_0\ \texttt{=}\ f_0)$ is *not* valid.

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

Lemma 1.

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

for all ae's e, f, g.

Proof: Let V be any 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

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

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

2 Equational Proofs

We've been careful so far to use a special "teletype" font for the *actual* symbols "`)`, `*`," ... occurring in ae's, to distinguish them from the italic font mathematical symbols "*)*, x, e, f" used to *describe* ae's. To keep our notation uncluttered, from now on we stop being so careful when there is no danger of ambiguity. In particular, we often will omit parentheses and just use mathematical font throughout expressions. For example, the valid equations of Lemma 1 above will now be written as

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

Definition 4. 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

$$\frac{e = f, \quad f = g}{e = g}$$

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.*

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 horizontal line.

Table 1: Standard Equational Inference Rules.

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

Definition 5. 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. For all ae's e,

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

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

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	Fig. 1	with f, g replaced by $e*0, e*1$, respectively).	
$\vdots$			
$(e*1)+-(e*1)$	$=$	$e*0$	(transitivity)
$(e*1)+-(e*1)$	$=$	0	(inverse for $+$)
0	$=$	$(e*1)+-(e*1)$	(symmetry)
0	$=$	$e*0$	(transitivity)

The axioms of Table 2 are so fundamental that they have a special mathematical name: *the commutative ring axioms.* Any set of elements with $+, *, -$ operations satisfying these axioms is called a *commutative ring.* In addition to $\mathbb{Z}$, other examples of commutative rings are the real numbers, $\mathbb{R}$, the complex numbers, $\mathbb{C}$, and the integers modulo n (for $n > 1$).

Problem 1.

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

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

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:

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

3(a) Prove that

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

3(b) Prove that

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

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

The validity of the distributivity axiom—Lemma 1—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 1. (*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 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 6. 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,

$$\hat{3} \text{ is } \texttt{(1 + (1 + (1 + 0)))},$$
$$\widehat{-2} \text{ is } \texttt{((-1) + ((-1) + 0))}.$$

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

Problem 6.

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

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

6(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.)

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

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

6(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. (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 6(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 7. 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 $\leq d$.

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

Theorem 2. 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 4. 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. (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 2, $\vdash e = c$ 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 4, 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 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. 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.

Problem 9. Prove that

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

4 Arithmetic Inequalities

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

Definition 8. 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 $[\![e]\!] \leq [\![f]\!]$.

As we did with equations, we will stop using teletype font for formal symbols like `<=` which appear in aineq's, writing them instead as ordinary mathematical symbols, e.g., "$\leq$." Some additional formal inference rules for proving inequalities are given in Table 3.

Table 3: Inference Rules for Inequalities.

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

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

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

We now have two proof systems, the original one for equality with the rules in Tables 1 and 2, and the extension of this system by the rules for inequalities in Table 3. We'll use the notations $\vdash_=$ and $\vdash_\leq$ when it's useful to emphasize the relevant proof system.

Problem 10. Completeness for constant inequalities.

10(a) Show that $n \leq m$ iff $\vdash_{\leq}$ ($\hat{n}$ **<=** $\hat{m}$).

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

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

By Problem 10, we know that $\vdash_{\leq}$ is complete for inequalities between aeq's without variables. Given our success in finding a complete proof system for arithmetic equalities over the integers even if variables do occur, we might hope to achieve the same thing for inequalities.

However, there are some notable contrasts between equations and inequations. For example, Problem 9 reveals that the same equations are valid whether we consider meanings over the integers, $\mathbb{Z}$, or the real numbers, $\mathbb{R}$. In fact, exactly the same equations are valid over the complex numbers, $\mathbb{C}$. Not so for inequations. For example, let $\mathbb{R}^+$ denote the positive real numbers. The complex numbers can be partially ordered by the relation, $\sqsubseteq$, where $c \sqsubseteq d$ iff $d - c \in \mathbb{R}^+ \cup \{0\}$. If we interpret the symbol $\leq$ to mean the relation $\sqsubseteq$, then we have:

$$\begin{aligned} &\models_{\mathbb{Z}} 0 \leq e * e, \\ &\models_{\mathbb{R}} 0 \leq e * e, \text{ but} \\ &\not\models_{\mathbb{C}} 0 \leq e * e. \end{aligned}$$

This remark implies a limitation of the proof rules for $\vdash_{\leq}$, namely:

Lemma 5. (Incompleteness for $\vdash_{\leq}$) There is an arithmetic inequality which is valid over the integers but not $\vdash_{\leq}$-provable, namely,

$$\begin{aligned} &\models_{\mathbb{Z}} 0 \leq x * x, \\ &\not\vdash_{\leq} 0 \leq x * x. \end{aligned}$$

Proof: All the rules of $\vdash_{\leq}$ are validity-preserving over the complex numbers with $\leq$ interpreted as $\sqsubseteq$, so an inequality which is not valid over the complexes cannot be provable. ■

This particular discrepancy between validity and provability can be regarded an oversight in the design of our proof system. We could repair it simply by adding the "missing" inequality as an axiom. That is, if we define $\vdash_2$ to have the rules of $\vdash_{\leq}$ along with the axiom $0 \leq e * e$, then the resulting proof system remains sound over the integers (though not any more over the complexes partially ordered by $\sqsubseteq$). Now, of course, the formerly missing inequality is immediately $\vdash_2$-provable.

But $\vdash_2$ is also incomplete over the integers.

Lemma 6. (Incompleteness for $\vdash_2$) There is an arithmetic inequality which is valid over the integers but not $\vdash_2$ provable, namely,

$$\models_{\mathbb{Z}} e \leq e * e,$$
$$\not\vdash_2 x \leq x * x.$$

Proof: All the rules of $\vdash_2$ are validity-preserving over the real numbers, so the inequality $x \leq x * x$, which is not valid over the reals, cannot be provable. ■

Now we might similarly define $\vdash_3$ to have the rules of $\vdash_2$ along with the further rule $e \leq e * e$. At this point, it is no longer so easy to show incompleteness for $\vdash_3$. On the other hand, neither is there an apparent reason to expect $\vdash_3$ to be complete for integer inequalities.

Nevertheless, we can be sure that $\vdash_3$ is *not* complete. One of the great mathematical results of the Twentieth Century implies 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 one of the consequences of Gödel's Incompleteness Theorem and Matiyasevich's negative solution to Hilbert's Tenth Problem[1], topics which we take up later.

Problem 11. 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?

[1] cf. *Hilbert's Tenth Problem*, Yuri V. Matiyasevich, MIT Press, c. 1993, 264 pp.