Problem Set 1 Solutions

Reminder: **QUIZ 1** in class on Monday, 7 October.

Problem 3(a)

We use structural induction on arithmetic expression e, to show that $\vdash$ (f = g) implies

$$\vdash (e[x := f] \texttt{ = } e[x := g])$$

for any arithmetic expressions e, f, g, and variables x.

Base case 1: e is a constant or variable, c, distinct from x. Then by the definition of substitution, $e[x := f]$ is actually the arithmetic expression c. Likewise, $e[x := g]$ is c. Since (c = c) is an instance of the reflexivity axiom, we immediately have $\vdash$ (c = c). In this base case, we did not need to use the hypothesis $\vdash$ (f = g).

Base case 2: e is the variable x. Then by the definition of substitution, $e[x := f]$ is the expression f. Likewise $e[x := g]$ is g. So this base case requires that we show that (f = g) is provable. But this is exactly the hypothesis $\vdash$ (f = g), so we are done.

Structural induction case 1: e is of the form e_1 + e_2. Assume $\vdash$ (f = g). Then by induction, we also have that

$$\vdash (e_1[x := f] \texttt{ = } e_1[x := g]),$$

and

$$\vdash (e_2[x := f] \texttt{ = } e_2[x := g]).$$

We must now show that

$$\vdash \texttt{ (} (e_1 \texttt{ + } e_2)[x := f] \texttt{ = } (e_1 \texttt{ + } e_2)[x := g] \texttt{)}$$

By +-congruence from the first two equations above, we have

$$\vdash \texttt{ (} e_1[x := f] \texttt{ + } e_2[x := f] \texttt{ = } e_1[x := g] \texttt{ + } e_2[x := g] \texttt{)}.$$

But by definition of substitution, the lefthand side of this equation is the same as $(e_1 + e_2)[x := f]$, and the righthand side is $(e_1 + e_2)[x := g]$, so we are done.

Structural induction cases 2 & 3: e is of the form e_1 * e_2 or -e_1. Essentially the same as case 1.

Problem 3(b)

We use induction on the length of the equational proof of (e = g) to show that $\vdash$ (e = g) implies $\vdash$ ($e[x := f]$ = $g[x := f]$).

Base case: The proof of (e = g) is of length 1. This means that (e = g) is an axiom. But then we claim that ($e[x := f]$ = $g[x := f]$) is another instance of the same axiom, and so also has a proof of length 1.

We illustrate why the claim holds for the (commutativity of +) axiom, (e_1 + e_2 = e_2 + e_1). Namely, we claim that the equation

$$((e_1 \texttt{ + } e_2)[x := f] \texttt{ = } (e_2 \texttt{ + } e_1)[x := f])$$

is also an instance of commutativity. To see this, let h_1 be the expression $e_1[x := f]$ and h_2 be $e_2[x := f]$. By the definition of substitution, the lefthand side of the equation displayed above is h_1 + h_2 and the righthand side is h_2 + h_1, so the equation above is of the required form (h_1 + h_2 = h_2 + h_1).

The proofs of the claim for the other axioms follow similarly.

Induction: The proof of (e = g) is of length $n + 1$ for some $n \geq 1$.

In this case we use the fact that the five[1] formal inference rules of Handout 3, Table 1, have a property similar to that claimed for the axioms. Namely, if we perform the same substitution on all the antecedents and the consequent of a rule, we obtain another instance of the same rule. The argument proving this is similar to the argument above for the commutativity axiom. We leave it to the reader to check this fact.

Now, if (e = g) is an axiom, the proof for the Base case shows that $\vdash$ ($e[x := f]$ = $g[x := f]$). Otherwise, (e = g) must follow from an instance of an inference rule whose antecedents are equations earlier in the formal proof. By the claim above, substituting f for x into the antecedents and consequent of this inference rule is another instance of the rule. But the antecedents must have proofs of length at most n, so by induction, we have the result of substituting f for x in any antecedent equation is also provable. Now the equation ($e[x := f]$ = $g[x := f]$) is the consequent of the substituted instance of the inference rule, and the substituted antecedents are provable, so we conclude by Problem 2 that this consequent is also provable.

Problem 4(a)

Show that $\vdash$ ($\texttt{-}e$ = $\texttt{-1 *}\ e$).

[1] We don't need to count (reflexivity), since it is an axiom.

Remember that a *formal proof* of an arithmetic equation, $\mathcal{E}$, is sequence $\mathcal{E}_1, \mathcal{E}_2, \ldots$ of arithmetic equations which fit together according to the inference rules of Handout 3 and which end with $\mathcal{E}$. Formal proofs are generally too long and tedious to write out.

What follows is a real, *mathematical* proof—written in English with mathematical notation—that *there exists a formal proof.* Using the mathematical properties of formal provability from Problems 2 and 3(a), we can conclude that the formal proof exists without writing it out.

Proof: The sequence of two equations

$$\texttt{(0 + (-}e\texttt{) = -}e\texttt{),}$$
$$\texttt{(-}e\texttt{ = 0 + (-}e\texttt{))}$$

is a formal proof because the first equation is an instance of the (identity for +) axiom, and the second equation follows from the first by the (symmetry) rule. Hence,

$$\vdash \texttt{(-}e\texttt{ = 0 + (-}e\texttt{)).}$$

Now observe that the equation $\texttt{(0 + (-}e\texttt{) = (}e\texttt{*0) + (-}e\texttt{))}$ follows from the equations $\texttt{(0 = }e\texttt{*0)}$ and $\texttt{(-}e\texttt{ = -}e\texttt{)}$ by the (+-congruence) rule. From Figure 2 of Handout 3, we know $\vdash \texttt{(0 = }e\texttt{*0)}$, and of course $\vdash \texttt{(-}e\texttt{ = -}e\texttt{)}$ by the (reflexivity) axiom. So by the results of Problem 2, we conclude

$$\vdash \texttt{((0 + (-}e\texttt{) = (}e\texttt{*0) + (-}e\texttt{)).}$$

It will be useful at this point to introduce some new notation:

$$\vdash e_1 = e_2 = \cdots = e_n$$

is an abbreviation for the assertions $\vdash \texttt{(} e_i \texttt{ = } e_j \texttt{)}$ for all $1 \leq i, j \leq n$. Note that if

$$\vdash e_1 = e_2 = \cdots = e_n,$$

and for some $i \leq n$,

$$\vdash \texttt{(} e_i \texttt{ = } e_{n+1} \texttt{),}$$

then by the formal inference rules (transitivity) and (symmetry), and the results of Problem 2, we may conclude

$$\vdash e_1 = e_2 = \cdots = e_{n+1} = e_{n+1}.$$

So we can summarize the two provable equations displayed above by the "three-way" equality

$$\vdash \texttt{-}e\texttt{ = 0 + (-}e\texttt{) = (}e\texttt{*0) + (-}e\texttt{).}$$

Now $\vdash$ `( (1 + (-1)) = 0 )` the (inverse for `+`) axiom and (symmetry). Substituting the two sides of this equation for `x` in the expression $(e$`*x) + (-`e`)`, we conclude from Problem 3(a) that

$$\vdash \texttt{((}e\texttt{*0) + (-}e\texttt{) = (}e\texttt{*(1 + (-1))) + (-}e\texttt{)).}$$

So we can attach `= (`e`*(1 + (-1))) + (-`e`)` to the three-way equality to obtain the four-way equality

$$\vdash \texttt{-}e\texttt{ = 0 + (-}e\texttt{) = (}e\texttt{*0) + (-}e\texttt{) = (}e\texttt{*(1 + (-1))) + (-}e\texttt{).}$$

Continuing, we can attach

$$\texttt{= (}e\texttt{*1 + }e\texttt{*(-1)) + (-}e\texttt{)}$$

by the (distributivity) axiom and substitution. Next we attach

$$\texttt{= (1*}e\texttt{ + }e\texttt{*(-1)) + (-}e\texttt{)}$$

by (commutativity of `*`) and substitution, and

$$\texttt{= (}e\texttt{ + }e\texttt{*(-1)) + (-}e\texttt{)}$$

by (identity for `*`) and substitution,

$$\texttt{= (-}e\texttt{) + (}e\texttt{ + }e\texttt{*(-1))}$$

by (commutativity of `+`),

$$\texttt{= ((-}e\texttt{) + }e\texttt{) + }e\texttt{*(-1)}$$

by (associativity of `+`),

$$\texttt{= (}e\texttt{ + (-}e\texttt{)) + }e\texttt{*(-1)}$$

by (commutativity of `+`) and substitution,

$$\texttt{= 0 + }e\texttt{*(-1)}$$

by (inverse for `+`) and substitution,

$$\texttt{= }e\texttt{ * (-1)}$$

by (identity for `+`),

$$\texttt{= -1 * }e$$

by (commutativity of `*`).

Hence,

$$\vdash \texttt{(-}e\texttt{ = -1 * }e\texttt{).}$$

■

Problem 4(b)

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

Proof:

$\vdash$ `1 = 0+1 = 1+0 = 1+(-1 + (-(-1))) = (1+(-1)) + (-(-1)) = 0 + (-(-1)) = -(-1)`

where the successive equalities follow by (identity for `+`) & (symmetry), (commutativity for `+`), (inverse for `+`) & substitution, (associativity), (inverse for `+`) & substitution, and (identity for `+`). So

$\vdash$ `( 1 = -(-1) )`.

But letting e be `-1` in 4(a), we have

$\vdash$ `( -(-1) = -1 * (-1) )`,

so by transitivity and Problem 2,

$\vdash$ `( 1 = -1 * (-1) )`.

■

Problem 5

Since $\widehat{n}$ and $\widehat{-n}$ were defined inductively for $n \geq 0$, we use induction on $n \geq 0$ to show that $[\![\widehat{n}]\!]V = n$ and $[\![\widehat{-n}]\!]V = -n$ for all valuations V.

Base case: $[\![\widehat{0}]\!]V = [\![0]\!]V = 0$.

Induction case 1: Assume $[\![\widehat{n}]\!]V = n$ for $n \geq 0$. Then

$$\begin{aligned} [\![\widehat{n+1}]\!]V &= [\![(\mathtt{1} + \widehat{n})]\!]V \\ &= [\![\mathtt{1}]\!]V + [\![\widehat{n}]\!]V \\ &= 1 + n \\ &= n + 1 \end{aligned}$$

Induction case 2: Assume $[\![\widehat{-n}]\!]V = -n$ for $n \geq 0$. Then

$$\begin{aligned} [\![\widehat{-(n+1)}]\!]V &= [\![(\mathtt{(-1)} + \widehat{-n})]\!]V \\ &= [\![\mathtt{(-1)}]\!]V + [\![\widehat{-n}]\!]V \\ &= -[\![\mathtt{1}]\!] + (-n) \\ &= -1 + (-n) \\ &= -(n+1) \end{aligned}$$

Problem 6(c)

We use induction on the magnitude of n to show that $\vdash$ `(` $\widehat{n}$ `+` $\widehat{m}$ `=` $\widehat{n+m}$ `)` for all $m, n \in \mathbb{Z}$.

Base case: $n = 0$. We must show that

$$\vdash \texttt{(}\ \widehat{0}\ \texttt{+}\ \widehat{m}\ \texttt{=}\ \widehat{0+m}\ \texttt{)}.$$

Since $\widehat{0}$ is `0`, the arithmetic expression on the lefthand side of the equation is actually `(0 +` $\widehat{m}$`)`, and the righthand side is of course $\widehat{m}$. So the equation is simply an instance of the (identity for `+`) axiom, and so is provable.

Induction case $n \geq 0$: We must show that

$$\vdash \texttt{(}\ \widehat{(n+1)}\ \texttt{+}\ \widehat{m}\ \texttt{=}\ \widehat{(n+1)+m}\ \texttt{)}$$

and

$$\vdash \texttt{(}\ \widehat{-(n+1)}\ \texttt{+}\ \widehat{m}\ \texttt{=}\ \widehat{-(n+1)+m}\ \texttt{)}.$$

We'll work on the second equation.

The lefthand side of the second equation is of the form `(-1 +` $\widehat{-n}$`) +` $\widehat{m}$ because $\widehat{-(n+1)}$ is `-1 +` $\widehat{-n}$ by definition. In this form, we can see that the lefthand side is provably equal to the expression $\widehat{-n}$ `+ (-1 +` $\widehat{m}$`)` by (commutativity), (associativity) and substitution (cf., Problem 3(a)). The previous expression is in turn provably equal to $\widehat{-n}$ `+` $\widehat{m-1}$ by **Problem 6(b)** and substitution. Now *by induction*, this expression is itself provably equal to $\widehat{-n+(m-1)}$ which is of course the same as the righthand side of the second equation.

The argument for the first equation is similar.

Problem 6(f)

We use structural induction to show that $\vdash$ `(`e `=` $\widehat{[\![e]\!]V}$`)` for all valuations V and all variable-fee arithmetic expressions e.

Base case 1: e is `0`. We must show

$$\vdash \texttt{(}\ \texttt{0}\ \texttt{=}\ \widehat{[\![\texttt{0}]\!]V}\ \texttt{)}$$

for every valuation V.

By the definition of values of arithmetic expressions, $[\![\texttt{0}]\!]V = 0$ for any V. So the righthand side of the equation above is $\hat{0}$, which is `0` by definition of $\hat{\ }$. Hence this equation is actually the axiom `( 0 = 0 )`, and so is immediately provable.

Base case 2: e is `1`. Similarly.

Induction case 1: e is e_1 `+` e_2 for variable-free e_1, e_2.

By induction, we have

$$\vdash \texttt{(}\ e_1\ \texttt{=}\ \widehat{[\![e_1]\!]V}\ \texttt{)}$$

and

$$\vdash \texttt{(}\ e_2\ \texttt{=}\ \widehat{[\![e_2]\!]V}\ \texttt{)}.$$

So by `+`-congruence

$$\vdash \texttt{(}\ e_1\ \texttt{+}\ e_2\ \texttt{=}\ \widehat{[\![e_1]\!]V}\ \texttt{+}\ \widehat{[\![e_2]\!]V}\ \texttt{)}.$$

Using Problem 6(c), the righthand side of this equation is provably equal to $\widehat{[\![e_1]\!]V + [\![e_2]\!]V}$. So by transitivity,

$$\vdash \texttt{(}\ e_1\ \texttt{+}\ e_2\ \texttt{=}\ \widehat{[\![e_1]\!]V + [\![e_2]\!]V}\ \texttt{)}.$$

But the righthand side of this equation above is $\widehat{[\![\texttt{(}e_1\ \texttt{+}\ e_2\texttt{)}]\!]V}$ by definition of $[\![\cdot]\!]$. That is,

$$\vdash \texttt{(}\ e_1\ \texttt{+}\ e_2\ \texttt{=}\ \widehat{[\![\texttt{(}e_1\ \texttt{+}\ e_2\texttt{)}]\!]V}\ \texttt{)}$$

as required for this case.

Induction case 2 & 3: e is e_1 `*` e_2 or `-`e_1. Similarly.

Problem 10(a)

To show that $n \leq m$ iff $\vdash_{\leq} \texttt{(}\widehat{n}\ \texttt{<=}\ \widehat{m}\texttt{)}$, we prove the two directions separately.

If $\vdash_{\leq} \texttt{(}\widehat{n}\ \texttt{<=}\ \widehat{m}\texttt{)}$, then $n \leq m$:

The proof system for inequalities is sound, so $\vdash_{\leq} \texttt{(}\widehat{n}\ \texttt{<=}\ \widehat{m}\texttt{)}$ implies this inequality is valid . That is, $[\![\widehat{n}]\!]V \leq [\![\widehat{m}]\!]V$ for any valuation V. From problem 5, we have that $[\![\widehat{n}]\!]V = n$. Therefore, $n \leq m$.

If $n \leq m$, then $\vdash_{\leq} \texttt{(}\widehat{n}\ \texttt{<=}\ \widehat{m}\texttt{)}$:

We prove this by induction on $m - n$.

Base case $m - n = 0$: We must show that

$$\vdash_{\leq} \texttt{(}\widehat{n}\ \texttt{<=}\ \widehat{n}\texttt{)}$$

But this follows immediately from (reflexivity) and ($\leq$-reflexivity).

Induction case $m - n > 0$: . We first note that $\vdash_{\leq}$ `( (-1 +` e`) <=` e `)`. Here is a formal proof, beginning with the `+` identity and inverse axioms:

```
( 0 + (-0) = -0 )
( 0 + (-0) = 0 )
( -0 = 0 + (-0) )
( -0 = 0 )
( -0 <= 0 )
( 0 <= 1 )
( -1 <= -0 )
( -1 <= 0 )
( -1 + e <= 0 + e )
( 0 + e = e )
( 0 + e <= e )
( -1 + e <= e )
```

Now $\vdash_{\leq}$ `(` $\hat{n}$ `<=` $\widehat{m-1}$ `)` by induction, and $\vdash$ `(` $\widehat{m-1}$ `= -1 +` $\hat{m}$ `)` by 6(b), so $\vdash_{\leq}$ `(` $\hat{n}$ `<= -1 +` $\hat{m}$ `)` by ($\leq$-reflexivity) and ($\leq$-transitivity). But $\vdash_{\leq}$ `( -1 +` $\hat{m}$ `<=` $\hat{m}$ `)` by the formal proof above, so $\vdash_{\leq}$ `(` $\hat{n}$ `<=` $\hat{m}$ `)` by ($\leq$-transitivity).

Problem 10(b)

We must show for all variable-free e, f, that if $\models$ `(` e `<=` f `)`, then $\vdash_{\leq}$ `(` e `<=` f `)`.

So assume $\models$ `(` e `<=` f `)`. This means that $[\![e]\!]V \leq [\![f]\!]V$ for any valuation V. From 10(a), we have

$$\vdash_{\leq} (\widehat{[\![e]\!]V} \texttt{ <= } \widehat{[\![f]\!]V}).$$

From 6(f) we have

$$\vdash \texttt{(} \ e \texttt{ = } \widehat{[\![e]\!]V} \ \texttt{)}$$

and $\vdash$ `(` f `=` $\widehat{[\![f]\!]V}$ `)`. So by ($\leq$-reflexivity) and ($\leq$-transitivity), we conclude that $\vdash_{\leq}$ `(` e `<=` f `)`.

Problem 11

It was claimed in the Handout 3 that

Theorem. Given any proof checking program for a sound proof system with arithmetic inequalities as formal theorems, we can construct an inequality which is valid over the integers but which has no proof in the system.

But if the inequality has no proof, how can we possibly know it is valid?

Answer: Wait a minute! Nobody said the inequality has no formal proof at all. In fact, as soon as you show me an inequality which can't be proved in some *particular* formal proof system, I can show you *another* formal proof system in which the inequality *can* be proved—namely the original system augmented with the unprovable inequality as an axiom! So there is no such thing as an *inherently unprovable* inequality.

OK, so given a sound formal proof system, how can we find an inequality which is not provable in that particular system and at the same time be sure that the inequality is valid? We'll show how later in the course. When we do so, we will also present an elegant short argument explaining why the inequality is both unprovable and valid. The argument will be short because it begins with the powerful hypothesis that the given formal proof system is *sound*, i.e., that all the inequalities formally provable in the system are themselves valid.

So how we can know that a given proof system is sound? That is a much harder question in general, and it will bear further discussion later in the course.