MATHEMATICS 300 — SPRING 2001

Introduction to Mathematical Reasoning (640 - 300, Section 03)

H. J. Sussmann

HANDOUT NO. 9—REVISED VERSION

(April 12, 2001)

HOMEWORK ASSIGNMENT DUE ON MONDAY, APRIL 16

1. Section No. 12 of the book, Problems 1 (parts (b), (c), (d), (e)); 4; 5 (parts (b), (c), (d), (f)); 9.
2. Section No. 13 of the book; Problems 2 (parts (a), (b), (c), (e)); 7, 8, 9, 10, 16.

HOMEWORK ASSIGNMENT DUE ON MONDAY, APRIL 23—PROBLEM 1.

There will be a few more problems, to be assigned on Monday, April 16

Using the axioms for real number arithmetic (listed in Page 4 of this handout), plus the axioms for equality, and the rules of inference—including Rule SUB—plus the following three definitions:

$$2 = 1 + 1\,, \qquad 3 = 2 + 1\,, \qquad 4 = 3 + 1\,,$$

give a formal proof of the following statement: $\boxed{2.2 = 4}$.

A SPECIAL PRIZE WILL BE GIVEN TO THE STUDENT WHO MANAGES TO DO THE PROOF IN THE SMALLEST NUMBER OF STEPS. (Your proof will probably take somewhere between 30 and 40 steps, but it may also be possible to do it in fewer steps than that.) Naturally, NO CHEATING IS ALLOWED. ("Cheating" means: any step which is not justified according to the rules. Proving theorems is like playing solitaire: one single violation of the rules suffices to enable you to "win," but if you "win" that way then your "victory" is worthless and does not count for anything.) ONE IMPROPERLY JUSTIFIED MOVE INVALIDATES THE WHOLE PROOF.

The prize will be: extra credit for homework equal to the full value of one homework assignment.

If there is a tie, then the prize will be divided among the winners. (For example, if there is a tie involving three students, then each one will get extra credit for homework equal to the one third of the full value of one homework assignment.)

THE SECOND MIDTERM TEST

The test will be on **Thursday, April 19.**

TERMS

A *term* is a formal expression that is supposed to be the name of a *thing*. For example, 3, $3 + 4$, $x - 7$, $3.(x + 6) - 7.u$ are terms, but $x = 3$, $\forall x, (x = 7)$ are *not* terms.

A *constant* term is a term that contains no variables. For example, if in a proof you have introduced constants a, b by saying "let a be arbitrary," "let b be arbitrary," and x is a variable, then 3, a, $a + b$, $a + 3$, $7.(a + 4) - b$, are constant terms, but $x + a$ is not a constant term.

The specialization rule 6.U is also valid to substitute *constant terms* rather than just constants:

EXTENDED RULE 6.U. Suppose that

1. x is a variable,
2. $\mathcal{A}(x)$ is a formula where there is no quantifier involving x,
3. t is a constant term, and $\mathcal{A}(t)$ is what you get from $\mathcal{A}(x)$ by substituting a for x in all the occurrences of x in $\mathcal{A}(x)$.

Then, if you have $\forall x, \mathcal{A}(x)$ in a previous step, you can go to $\mathcal{A}(t)$.

THE AXIOMS FOR EQUALITY

Here are the axioms about equality.

Eq1. $\forall x, (x = x)$.

Eq2. $\forall x, \forall y, (x = y \longrightarrow y = x)$.

Eq3. $\forall x, \forall y, \forall z, ((x = y \wedge y = z) \longrightarrow x = z)$.

In addition, there is also an *inference rule for equality*, called the **substitution rule**:

RULE SUB: Suppose that:

1. x is a variable,
2. p is a formula that has no x-quantifiers,
3. t, s are constant terms,
4. $p(t)$, $p(s)$ are the formulas that result from p by substituting t, s, respectively for x,

Then, if the sentences "$t = s$" and "$p(t)$" appear before in a proof, you can go to "$p(s)$."

AN EXAMPLE: Here is an example showing how to work with the extended specialization rule and with the substitution rule for equality.

Suppose you have the axioms

A1. $\forall x, \forall y, (x.y = y.x)$.

A2. $\forall x, \forall y, \forall z, ((x + y).z = x.z + y.z)$.

Let us give a completely formal proof of:

THEOREM: $\forall x, \forall y, \forall z, (z.(x + y) = z.x + z.y)$.

PROOF:

(1) $\forall x, \forall y, \forall z, ((x + y).z = x.z + y.z)$. [Axiom A2]

(2) Let a be arbitrary. [Preparation to apply Rule 6.P]

(3) Let b be arbitrary. [Preparation to apply Rule 6.P]

(4) Let c be arbitrary. [Preparation to apply Rule 6.P]

(5) $\forall y \forall z\, ((a + y).z = a.z + y.z)$. [Rule 6.U, from (1), plugging in a for x]

(6) $\forall z\, ((a + b).z = a.z + b.z)$. [Rule 6.U, from (5), plugging in b for y]

(7) $(a + b).c = a.c + b.c$. [Rule 6.U, from (6), plugging in c for z]

(8) $\forall x, \forall y, (x.y = y.x)$. [Axiom A1]

(9) $\forall y, ((a + b).y = y.(a + b))$. [Extended Rule 6.U, from (8), plugging in $a + b$ for x]

(10) $(a + b).c = c.(a + b)$. [Rule 6.U, from (9), plugging in c for y]

(11) $\forall y, (a.y = y.a)$. [Rule 6.U, from (8), plugging in a for x]

(12) $a.c = c.a$. [Rule 6.U, from (11), plugging in c for y]

(13) $\forall y, (b.y = y.b)$. [Rule 6.U, from (8), plugging in b for x]

(14) $b.c = c.b$. [Rule 6.U, from (13), plugging in c for y]

(15) $c.(a + b) = a.c + b.c$. [Rule SUB, from (7) and (10), with "$x = a.c + b.c$" in the role of p, "$(a + b).c$" in the role of t, and "$c.(a + b)$" in the role of s]

(16) $c.(a + b) = c.a + b.c$. [Rule SUB, from (12) and (15), with "$c.(a + b) = x + b.c$" in the role of p, "$a.c$" in the role of t, and "$c.a$" in the role of s]

(17) $c.(a+b) = c.a + c.b.$ [Rule SUB, from (16) and (16), with "$c.(a+b) = c.a + x$" in the role of p, "$b.c$" in the role of t, and "$c.b$" in the role of s]

(18) $\forall z, (z.(a+b) = z.a + z.b).$ [Rule 6.P, from (4) and (17),

(19) $\forall y, \forall z, (z.(a+y) = z.a + z.y).$ [Rule 6.P, from (3) and (18),

(20) $\forall x, \forall y, \forall z, (z.(x+y) = z.x + z.y).$ [Rule 6.P, from (2) and (19),

END OF PROOF

THE AXIOMS OF REAL NUMBER ARITHMETIC AND OTHER NUMBER SYSTEMS

A1. $\forall x, \forall y, (x + y = y + x).$

A2. $\forall x, \forall y, \forall z, ((x + y) + z = x + (y + z)).$

A3. $\forall x, \forall y, (x.y = y.x).$

A4. $\forall x, \forall y, \forall z, ((x.y).z = x.(y.z)).$

A5. $\forall x, \forall y, \forall z\, ((x + y).z = x.z + y.z).$

A6. $\forall x, (x + 0 = x).$

A7. $\forall x, (x.1 = x).$

A8. $\forall x, (x + (-x) = 0).$

A9. $\forall x, (x \neq 0 \rightarrow (x.x^{-1} = 1)).$

A10. $0 \neq 1.$

A11. $\forall x, (\neg\, x < x).$

A12. $\forall x, \forall y, \forall z, ((x < y \wedge y < z) \longrightarrow x < z).$

A13. $\forall x, \forall y, (x < y \vee y < x \vee x = y).$

A14. $\forall x, \forall y, \forall z, (x < y \longrightarrow x + z < y + z).$

A15. $\forall x, \forall y, \forall z, ((x < y \wedge 0 < z) \longrightarrow x.z < y.z).$