Formal versus semiformal proof in teaching predicate logic

David Gries [1]
Computer Science, Cornell University
Ithaca, NY 14853 [2]

August 1996

In [1], Steve Grantham advocates teaching proof, especially in the context of predicate logic, using "semiformal" methods. He introduces several metaphors and notational conventions intended to help students understand the role of universal and existential quantification and illustrates the ideas with two examples.

Grantham says,

> This [kind of semiformal proof] is difficult to define precisely, but what I have in mind is the type of proof that most mathematicians would consider complete and rigorous, but that is not strictly formal in the sense of a purely syntactic derivation using a very precise and circumscribed formal set of rules of inference. In other words, I have in mind the type of proof found in a typical textbook on algebra, analysis, number theory, etc.

Grantham goes on to say that

> The main problem with formal proof in the setting of pure logic is the length and tedium involved in proofs of even simple and obvious results by these methods. This precludes tackling examples with much intrinsic interest or complexity. ...

The thesis of this note is that, with a calculational predicate logic, teaching students about proof using formal proofs is superior to teaching them using the "semiformal" proofs proposed by Grantham. Formal proofs for the kinds of theorems in which Grantham is interested need not be long or tedious. Indeed, our experience is that the formal approach, with explanations interposed at judicious places, usually makes arguments clearer, shorter, and more memorable.

We butress our arguments for this thesis with formal proofs of two theorems that Grantham [1] proves "semiformally". We use the calculational predicate logic of the text *A Logical Approach to Discrete Math* [2], with a few modifications that will appear in the next edition. To make our discussion self-contained, we repeat one of Grantham's semiformal proofs verbatim.

[1] Supported by NSF grants CDA-9214957 and CCR-9503319.
[2] http://www.cs.cornell.edu/Info/People/gries/gries.html gries@cs.cornell.edu

Problems with a semiformal approach

A major pedagogical problem with the semiformal approach proposed by Grantham is punctuated by his statement "This [kind of proof] is difficult to define precisely". Without a precise definition of *proof*, proofs remain a mystery to students, so naturally students have difficulties developing proofs. If they don't know all the rules, they can't play the game well. If they don't know the rules, they won't *like* the game. On the other hand, we have observed that formal precision, used in a way that discourages complexity and detail from overwhelming, is welcomed by students.

Grantham's [1] metaphors for eliminating quantifications are written in an informal style, and without formal justification. Students are being asked to believe the metaphors without understanding why they should believe them. Just as importantly, "semiformal" proofs are likely to have missing steps, which the students don't see —not all the theorems of predicate logic that are actually needed are mentioned. With parts of proofs missing, it is no wonder that students don't understand proofs.

Moreover the nature of "semiformal" proofs make them longer than necessary, make them harder to follow, and make them less memorable. Finally, the formal (calculational) approach lends itself to more effective discussions of proof strategies.

Tools for dealing with quantification

Grantham [1] organizes his discussion around the following points:

1. How do we *prove* universally quantified conclusions?
2. How do we *use* existentially quantified statements that appear as premises?
3. How do we *use* universally quantified statements that appear as premises?
4. How do we *prove* existentially quantified conclusions?

These are indeed important questions. However, Grantham's answers to these questions suffer from the fact that they are couched in informal reasoning and are not backed up by suitable theorems and metatheorems. Graham's informal reasoning does not provide students with enough understanding for them to really grok predicate logic. In our view, it is far more advantageous to proceed as follows.

1. Introduce suitable axioms for predicate logic and discuss why they are used, why they are relevant.
2. Introduce general theorems for manipulating quantified expressions and prove these theorems formally.
3. Introduce metatheorems for removal and introduction of quantification, prove them, and show some simple examples of how the metatheorems are used.

Of course, a rigorous, formal approach works only if formal proofs are simple enough. We believe that this is the case when using the calculational predicate logic of [2]. For example, the proofs of the theorems and metatheorems presented below, which are most relevant to this discussion, are proved without complexity overwhelming —see [2].

First, let us discuss notation. Our notation for quantification over any binary, symmetric, and associative operator $\star$ is $(\star i \mid R.i : E.i)$. An example is $(+i \mid 0 \leq i < 3 : i^2)$, which equals $0^2 + 1^2 + 2^2$. Range $R.i$ is a boolean expression. If the type of $\star$ is $t \times t \rightarrow t$, then body $E.i$ has type t.

In the case that $\star$ is $\wedge$ or $\vee$, we defer to tradition and write the quantifications as $(\forall i \mid R.i : E.i)$ and $(\exists i \mid R.i : E.i)$, respectively. In case range $R.i$ is the constant *true*, we abbreviate the quantifications as $(\forall i \mid\!: E.i)$ and $(\exists i \mid\!: E.i)$. Also, we abbreviate nested quantifications like $(\forall i \mid\!: (\exists j \mid\!: E.i.j))$ as $(\forall i \exists j \mid\!: E.i.j)$.

We always put parentheses around quantifications so that the scope of the dummies is explicit. However, in order to minimize parentheses, which helps facilitate manipulations, we write function applications like $T(x, y)$ —in which the arguments are variables or constants— as $T.x.y$.

The notation $E[x := e]$ denotes (simultaneous) substitution: provided the variables in lists x and e do not contains dummies of quantifications in E, $E[x := e]$ denotes a copy of E in which all free occurrences of variables from list of variables x are replaced by their corresponding expressions in list of expressions e. (If x or e do contain dummies, rename the dummies in the quantification before performing the substitution.)

We now list the axioms and theorems of predicate calculus used later on. For introducing and eliminating a quantification, we have the following three rules. The first one holds for $\star$ being $\forall$ and $\exists$ —and, in fact, for any associative and symmetric operator.

(1) **One-point rule:** Provided x does not ocur free in E, $(\star x \mid x = E : P) \;=\; P[x := E]$

(2) **Instantiation:** $(\forall x \mid\!: P) \;\Rightarrow\; P[x := E]$

(3) **$\exists$-Introduction:** $P[x := E] \;\Rightarrow\; (\exists x \mid\!: P)$

(4) **Quantified freshy:** Provided z does not occur free in P, $(\exists z \mid R : P) \;\Rightarrow\; P$

The next theorem provides guidance for proving a universal quantification.

(5) **Metatheorem.** P is a theorem iff $(\forall x \mid\!: P)$ is a theorem.

Using this Metatheorem, a proof of a theorem $Q : (\forall x \mid\!: P)$ is often done in the form

> For arbitrary x, we prove P
> ... proof of P, where we may have to consider several cases depending on what x ranges over.

The following Metatheorem is a tool for dealing with existentially quantified antecedents.

(6) **Metatheorem Witness.** Suppose $\hat{x}$ does not occur free in P, Q, or R. Then

$(\exists x \mid R : P) \Rightarrow Q$ is a theorem iff
$(R \wedge P)[x := \hat{x}] \Rightarrow Q$ is a theorem.

Identifier $\hat{x}$ is called a *witness* for the existential quantification. [3]

Now, the standard Deduction Theorem says that a proof of C from premises P_0, ..., P_n is really a proof of $P_0 \wedge \ldots \wedge P_n \Rightarrow C$. Therefore, we are able to use (an extended form of) Metatheorem (6) Witness to conclude the following:

(7) **Metatheorem.** Suppose C is being proved using a premise of the form $(\exists x \mid R : P)$. Then, instead, $(R \wedge P)[x := \hat{x}]$ can be used as a premise, where $\hat{x}$ is a "fresh" variable.

Finally, we have the following metatheorem concerning weakening a subexpression of a formula.

(8) **Metatheorem Monotonicity.** Suppose V occurs exactly once in formula E, and not in an operand of $\equiv$ or $\not\equiv$. Define the parity of V in E to be *even* if V occurs in an even number of negations, antecedents, and ranges of universal quantifications and odd otherwise. Then

$E[V := P] \Rightarrow E[V := Q]$ (provided the parity of V in E is even)

$E[V := Q] \Rightarrow E[V := P]$ (provided the parity of V in E is odd)

To the left, below, we indicate a use of monotonicity when the parity is even; to the right, when the parity is odd.

$$\begin{array}{l} E[V := P] \\ \Rightarrow \quad \langle \text{Monotonicity: } P \Rightarrow Q \rangle \\ E[V := Q] \end{array} \qquad \begin{array}{l} E[V := P] \\ \Leftarrow \quad \langle \text{Antimonotonicity: } P \Rightarrow Q \rangle \\ E[V := Q] \end{array}$$

Theorems and metatheorems (1)–(8) are important tools for dealing with quantifications. Most of them come into play in proving Grantham's theorems (in the calculational style), so trying to prove his theorems without having seen these tools does not seem reasonable. It is better to state these tools crisply and formally than to leave them "semiformal". Further, the formal proofs of these tools are simple enough to be understood by freshmen (although the proof of (8) does require induction over the structure of formulas and has to wait until induction is thoroughly explained.)

Grantham's first example

Grantham [1] poses the following problem: Determine whether

$C : (\exists a \forall b \mid : T.b.a)$

[3] Identifier x itself can be used for $\hat{x}$ if x does not occur free in Q.

follows from the following four premises.

$$P0: \ (\forall x \,|\!:\, (\forall y \,|\!:\, T.x.y) \ \vee \ (\exists z \,|\!:\, R.x.z))$$
$$P1: \ (\exists x \forall y \forall z \,|\!:\, R.y.z \ \Rightarrow \ P.x.y)$$
$$P2: \ (\forall x \exists y \,|\!:\, Q.x.y)$$
$$P3: \ (\forall x, y, z \,|\!:\, P.x.z \ \wedge \ Q.x.y \ \Rightarrow \ T.z.x)$$

Our proof (development) proceeds as follows. C is an existential quantification, and of the premises, only $P1$ is an existential quantification, so a witness for x of $P1$ is likely to be used in the proof of C. Accordingly, we use Metatheorem (7) to introduce the premise

$$P1': \ (\forall y \forall z \,|\!:\, R.y.z \ \Rightarrow \ P.\hat{x}.y) \quad ,$$

for a fresh identifier $\hat{x}$. We now attempt to prove $(\forall b \,|\!:\, T.b.\hat{x})$, since application of $\exists$-Introduction (3) will then prove C.

Hence, for arbitrary b, we attempt to prove $T.b.\hat{x}$.

Now, T occurs only in $P0$ and $P3$, so it makes sense to investigate the use of these two in proving $T.b.\hat{x}$. An instantiation of $P0$ looks promising, because the goal $T.b.\hat{x}$ can be reached easily from at least the first disjunct of its body. This would yield a proof that started from a premise and ended with the goal.

On the other hand, we could begin with the goal $T.b.\hat{x}$ and immediately use an instantiation of $P3$ to weaken it to $(\forall y \,|\!:\, P.\hat{x}.b \ \wedge \ Q.\hat{x}.y)$. This would yield a proof that started with the goal.

Let us pursue the first alternative and write the following.

$$\begin{array}{ll} & (\forall y \,|\!:\, T.b.y) \ \vee \ (\exists z \,|\!:\, R.b.z) \quad \text{— } P0\text{, with instantiation } x := b \\ \Rightarrow & \quad \langle \text{Monotonicity: Instantiation (2)} \rangle \\ & T.b.\hat{x} \ \vee \ (\exists z \,|\!:\, R.b.z) \\ \Rightarrow & \quad \langle \text{Monotonicity: A possible lemma, see below} \rangle \\ & T.b.\hat{x} \ \vee \ T.b.\hat{x} \\ = & \quad \langle \text{Idempotency of } \vee \rangle \\ & T.b.\hat{x} \end{array}$$

Hence, it remains to prove a lemma: $(\exists z \,|\!:\, R.b.z) \ \Rightarrow \ T.b.\hat{x}$.

As an aside, we perform a step the reason for which is seen only later in the proof[4]. Instantiate $P2$ with $x := \hat{x}$ to yield the premise $(\exists y \,|\!:\, Q.\hat{x}.y)$. Then use Metatheorem (7) with a fresh variable $\hat{y}$ to arrive at

$$P2': \ Q.\hat{x}.\hat{y} \quad .$$

We now prove $(\exists z \,|\!:\, R.b.z) \ \Rightarrow \ T.b.\hat{x}$.

[4] Were we to develop this proof in a lecture, we would wait to introduce $P2'$ until the place where it was needed; then we would backtrack to introduce it at this point. It is needed here because $\hat{y}$ needs to be a fresh variable —one that does not appear thus far in the proof.

$T.b.\hat{x}$

$\Leftarrow$ $\langle P3$ seems most appropriate, since $T.z.x$ is the consequent of the body. Use $P3$ instantiated with $x, z, y := \hat{x}, b, \hat{y}$.$\rangle$

$P.\hat{x}.b \wedge Q.\hat{x}.\hat{y}$

$\Leftarrow$ $\langle$ $P2'$, so $Q.\hat{x}.\hat{y} \equiv true$ —this is why $P2'$ was developed$\rangle$

$P.\hat{x}.b \wedge true$

$=$ $\langle$Identity of $\wedge\rangle$

$P.\hat{x}.b$

$\Leftarrow$ $\langle$Quantified freshy (4) —so that $P1'$ can be used$\rangle$

$(\exists z \,|\!|: P.\hat{x}.b)$

$\Leftarrow$ $\langle P1'$, with $y, z := b, z$, i.e. $R.b.z \Rightarrow P.\hat{x}.b \rangle$

$(\exists z \,|\!|: R.b.z)$

Our development is quite similar to Grantham's; the difference is that his is "semiformal" while ours is far more formal and rigorous. Note that our proof references every theorem that it uses, but complexity does not overhwelm at all. Indeed, we believe that the presentation is more easily understood than Graham's. Note that the proof is annotated with comments that explain how it was (or could have been) developed.

Grantham's second example

Prove that

$$C: \ (\forall x \exists y \,|\!|: R.x.y)$$

follows from the following five premises.

$$P0: \ (\exists x \forall y \,|\!|: T.y.x)$$
$$P1: \ (\forall x \,|\!|: A.x \ \Rightarrow \ R.x.x)$$
$$P2: \ (\forall x \,|\!|: B.x \ \Rightarrow \ (\exists y \,|\!|: S.y.x))$$
$$P3: \ (\forall x, y \,|\!|: S.x.y \wedge \neg A.y \ \Rightarrow \ R.y.x)$$
$$P4: \ (\forall x, y \,|\!|: T.x.y \ \Rightarrow \ A.x \vee B.x \vee R.x.y)$$

For arbitrary x , we prove $(\exists y \,|\!|: R.x.y)$. We first use Metatheorem (7) to introduce the premise

$$P0': \ (\forall y \,|\!|: T.y.\hat{x}) \quad .$$

$P0'$ together with the shape of $P4$ encourages us to begin as follows. For arbitrary x , we have

$T.x.\hat{x}$ — $P0'$, instantiated with $y := x$

$\Rightarrow$ $\langle$ $P4$, instantiated with $x, y := x, \hat{x} \rangle$

$A.x \vee B.x \vee R.x.\hat{x}$

$\Rightarrow$ $\langle$Absorption, $X \vee (Y \wedge \neg X) \equiv X \vee Y$ —It looks like case analysis can be used, based on the three disjuncts. The form of $P2$ and $P3$ encourages this step first.$\rangle$
$A.x \vee (B.x \wedge \neg A.x) \vee R.x.\hat{x}$

We now prove $(\exists y \,|\!:\, R.x.y)$ by case analysis, using the three cases indicated in the last formula, which is a consequence of the premises.

Case $A.x$.
$A.x$
$\Rightarrow$ $\langle\, P1$, instantiated with $x := x \,\rangle$
$R.x.x$
$\Rightarrow$ $\langle\, \exists$-Introduction (3)$\rangle$
$(\exists y \,|\!:\, R.x.y)$

Case $B.x \wedge \neg A.x$.
$B.x \wedge \neg A.x$
$\Rightarrow$ $\langle$Monotonicity: $P2$, instantiated with $x := x \,\rangle$
$(\exists y \,|\!:\, S.y.x) \wedge \neg A.x$
$=$ $\langle$Distributivity of $\wedge$ over $\exists$ — y does not occur free in $\neg A.x \,\rangle$
$(\exists y \,|\!:\, S.y.x \wedge \neg A.x)$
$\Rightarrow$ $\langle\, P3$, instantiated with $x, y := y, x \,\rangle$
$(\exists y \,|\!:\, R.x.y)$

Case $R.x.\hat{x}$. $(\exists y \,|\!:\, R.x.y)$ follows by $\exists$-Introduction (3).

References

[1] Grantham, Steve. Semiformal proof in logic, Greek knuckleballs and lucky charms: some metaphors and notation for dealing with quantifiers. Presented at the DIMACS Symposium on Teaching Logic in an Illogical World, 26-27 July 1996. Accessible from the home page for the symposium papers, http://www.cs.cornell.edu/Info/People/gries/symposium/symp.htm.

[2] Gries, D., and F.B. Schneider. *A Logical Approach to Discrete Math*. Springer Verlag, NY, 1993.

Appendix: Grantham's semiformal proof of the second theorem

We present Graham's proof of the second example. Keep in mind that we have not explained Grantham's metaphors for dealing with quantification, and the development of the proof does read better once the metaphors are known. Neverthless, we find our proof much crisper, clearer, and easier to present.

Prove that $C:\ (\forall x \exists y \,|\!:\, R.x.y)$ follows from the following five premises.

$P0:\ (\exists x \forall y \,|\!:\, T.y.x)$

$P1:\ (\forall x \,|\!:\, A.x \ \Rightarrow\ R.x.x)$

$P2:\ (\forall x \,|\!:\, B.x \ \Rightarrow\ (\exists y \,|\!:\, S.y.x))$

$P3:\ (\forall x, y \,|\!:\, S.x.y \wedge \neg A.y \ \Rightarrow\ R.y.x)$

$P4:\ (\forall x, y \,|\!:\, T.x.y \ \Rightarrow\ A.x \vee B.x \vee R.x.y)$

Keeping in mind the theme of working both backwards and forwards, we might start working backwards and observing that C begins with a universal quantifier. Hence it is reasonable to introduce a name for an arbitrary object, say α, hence reducing the problem of proving C to proving the statement

Goal: $(\exists y \,|\!:\, R.\alpha.y)$

At this point we have two choices: ... continue working somewhat backwards, ... [or] first look for some additional "toeholds" among the premises that might help us "work forwards". ... In the example under consideration, probably the cleanest approach is to work forwards by choosing a witness, say $\clubsuit$, for the existential quantifier $\exists x$ in premise $P0$, so that we have

$P0':\ (\forall y \,|\!:\, T.y.\clubsuit)$

... Once we have chosen the witness $\clubsuit$, we have two objects at our disposal, and both of them are reasonable candidates for substitution into the many universally quantified statements we know are true. Instantiating any of the universal quantifiers in premises $P1$, $P2$, or $P3$ with either $\clubsuit$ or α is of questionable value, since we have no guarantee that any of the hypotheses of the implications thus obtained would be true. The same observation is also true for $P4$, except that finding an instantiation that makes the resulting $T(.,.)$ hypothesis true seems much more promising, in view of $P0'$.

These considerations suggest that a reasonable next step would be to instantiate the universal quantifier $\forall y$ in statement $P0'$ with either α or $\clubsuit$ (why not both?), obtaining the statements

$T.\alpha.\clubsuit$ and $T.\clubsuit.\clubsuit$

Of these two statements, the former looks more useful. Specifically, it now seems reasonable to instantiate the universal quantifiers $\forall x$ and $\forall y$ in premise $P4$ with α and $\clubsuit$, respectively, obtaining the statement

$P4':\ T.\alpha.\clubsuit \ \Rightarrow\ A.\alpha \vee B.\alpha \vee R.\alpha.\clubsuit$

Since the hypothesis of this implication is true, we can deduce that the conclusion must be also. That is, we have

$P4'':\ A.\alpha \vee B.\alpha \vee R.\alpha.\clubsuit$

Now if the third of these three disjuncts holds, we are at least moderately happy: we will have shown that $(\exists y \mid\colon R.\alpha.y)$ is true in this case. So we now need to consider the case where $R.\alpha.\clubsuit$ fails and hence either $A.\alpha$ or $B.\alpha$ (or both) is true.

If $A.\alpha$ holds, then premise $P1$ (with the obvious instantiation) immediately gives us

$$R.\alpha.\alpha \quad ,$$

so $(\exists y \mid\colon R.\alpha.y)$ is true in this case as well.

If $A.\alpha$ fails, then $B.\alpha$ must hold, so premise $P2$ (again with the obvious instantiation) gives us

$$(\exists y \mid\colon S.y.\alpha) \quad .$$

The obvious next step is to choose a witness, say $\heartsuit = \heartsuit.\alpha$, for this statement, so that we have

$$S.\heartsuit.\alpha \quad .$$

And now premise $P3$ is perfectly poised to come to our aid: instantiating the universal quantifiers $\forall x$ and $\forall y$ in that premise with $\heartsuit$ and α , respectively, we get

$$P3' : S.\heartsuit.\alpha \wedge \neg A.\alpha \Rightarrow R.\alpha.\heartsuit$$

Since the hypothesis of this implication is true, we may conclude that $R.\alpha.\heartsuit$, so $(\exists y \mid\colon R.\alpha.y)$ is true in this third case as well.

In summary, we have shown that, given an arbitrary object α , we will find ourselves in one of three cases, and in each such case the statement $(\exists y \mid\colon R.\alpha.y)$ is true. Hence, we have indeed shown that conclusion C follows from the premises.