# Some Applications of MATH 1090 Techniques

## 0.1 A simple problem about Nand gates in relation to And gates and inversion (Not) Gates.

In this subsection the notation "$\vdash A$" means that $A$ is proved from the axioms of first-order logic and also from the specific Axioms (2)–(6) of the Nand/And/Inv theory under discussion.

**Language.**
First-order with two constants, 0 and 1 and three function symbols,

- *inv* (arity one)
- *and* (arity two)
- *nand* (arity two)

**Axioms**.

(1) The first order Logical Axioms are all the *partial generalisations* of certain schemata (See [Tou08] and/or MATH 1090 class notes). We remind ourselves only of the *Two Equality Schemata* below under (1):

- $$\vdash t = t, \text{ for any term } t \qquad (identity)$$
- $$t = s \to (A[x := t] \equiv A[x := s]), \text{ for any terms } t \text{ and } s \text{ and formula } A \qquad (Leib.\ Axiom)$$
- From the equality axioms we obtain (routinely proved in MATH 1090) the following "properties of equality" (**theorems**), for *all* terms $t$ and $s$:
  **Symmetry**: $\vdash t = s \to s = t$
  **Transitivity**: $\vdash t = s \wedge s = t' \to t = t'$ (also, if $\vdash t = s$ and $\vdash s = t'$, then $\vdash t = t'$)

(2) Axioms (2)–(6) describe the theory of Nand/And/Inv. They are nonlogical.

$$\neg 0 = 1$$

(3)

$$(\forall x)\Big(x = 1 \vee x = 0\Big)$$

(4) (Inv)

$$(\forall x)\Big(inv(x) = 1 \equiv x = 0\Big)$$

This can also be used (via specialisation) as

$$\vdash inv(t) = 1 \equiv t = 0 \qquad (4')$$

for any term $t$.

Some exercises from EECS 3342. Retold by George Tourlakis: 2018–19

(5) (And)

$$(\forall x, y)^*\Big(and(x, y) = 1 \equiv x = 1 \wedge y = 1\Big)$$

(6) (Nand)

$$(\forall x, y)\Big(nand(x, y) = 0 \equiv x = 1 \wedge y = 1\Big)$$

We now prove the theorem

$$(\forall x, y)\Big(inv\big(and(x, y)\big) = nand(x, y)\Big) \qquad (thm)$$

First a lemma:

**0.1 Lemma.** *For any terms $t$ and $s$, $\vdash t = s \equiv (t = 0 \equiv s = 0)$.*

*Proof.* Ping-pong proof: ($\rightarrow$) direction. By Leib. Equality Axiom above, taking "$x = 0$" as "$A$".

($\leftarrow$) direction. Along with the assumption (7)

$$t = 0 \equiv s = 0 \qquad (7)$$

we have

$$t = 1 \vee t = 0 \qquad (8)$$

via specialisation on axiom (3). So we do proof by cases $t = 0$ and $t = 1$:

- Case $\vdash t = 0$. (7) and tautological implication yield $\vdash s = 0$. By $\vdash s = 0 \rightarrow 0 = s$ ("symmetry" of "=") we get $\vdash 0 = s$ by modus ponens; and then the assumption of this case and transitivity yield $\vdash t = s$ as required.
- Case $\vdash t = 1$. Thus we can prove $\vdash \neg t = 0$, say, by contradiction, for *assuming* also $\vdash t = 0$ we get $0 = 1$ by the case assumption transitivity contradicting, axiom (2). This, (7) and tautological implication yield $\vdash \neg s = 0$. Since (8) holds for all terms, we have $\vdash s = 1 \vee s = 0$ and by tautological implication $\vdash s = 1$. This, the assumption for this case, and transitivity yield once again $\vdash t = s$.

**Proof of the theorem**. Since the prefix "$(\forall x, y)$" can be introduced to

$$inv\big(and(x, y)\big) = nand(x, y) \qquad (9)$$

as all our nonlogical axioms are *closed*[†], it suffices to prove (9) instead of $(thm)$. In fact, in view of the lemma above, and thinking of $inv\big(and(x, y)\big)$ as $t$ and $nand(x, y)$ as $s$, we prove instead

$$inv\big(and(x, y)\big) = 0 \equiv nand(x, y) = 0 \qquad (10)$$

here it goes

[*] "$(\forall x, y)$" is shorthand for "$(\forall x)(\forall y)$".

[†] Have no free variables.

$$
\begin{aligned}
& nand(x, y) = 0 \\
\Leftrightarrow\ & \langle \text{Spec. of Axiom (6) (Nand)} \rangle \\
& x = 1 \wedge y = 1 \\
\Leftrightarrow\ & \langle \text{Spec. of Axiom (5) (And)} \rangle \\
& and(x, y) = 1 \\
\Leftrightarrow\ & \langle \text{Axiom (4) (Inv) —(4}') \text{ form} \rangle \\
& inv\big(and(x, y)\big) = 0
\end{aligned}
$$

□

## 0.2 $\sqrt{2}$ is *irrational*

In this subsection we prove that $\sqrt{2}$ is irrational, that is, it is impossible to have

$$\sqrt{2} = \frac{m}{n}, \text{ where } m > 0 \text{ and } n > 0 \text{ are natural numbers} \tag{1}$$


Why $m > 0$ and $n > 0$?


We will prove this in Peano Arithmetic (for short "PA", that is, the arithmetic of the *natural numbers* $\mathbb{N}$).

**PA Alphabet; Nonlogical (Mathematical) Part.** The Logical Part is common to ALL first-order Theories.

The *a priori Nonlogical* Alphabet of PA has only the (math) symbols 0 (constant), $S$ (stands for the successor function " + 1"; unary function), the binary functions "plus" +, and "times" ×, and the binary predicate <.

Of course, equality is in all first-order alphabets! The practice of mathematics to introduce *new functions* and *predicates* by definitions is empowered in first-order logic where PA belongs. One such example of a defined predicate is the predicate $O$ in (3) below.


Wait a minute! If the PA symbols list above is complete, then what about symbols for 1, 2, 101, 3333356699? Why are they not in the alphabet? Well, it IS complete! $S0$ —intuitively, "0 + 1"— is denoted by "$\widetilde{1}$" and represents (stands for) 1; $SS0$ stands for 2 (formal abbreviation $\widetilde{2}$) and in general,

$$\overbrace{SS\ldots S}^{n \text{ copies of } S}\ 0$$

stands for the informal $n$ and has the formal abbreviation $\widetilde{n}$.

In any case, in practice, *to preserve our sanity* we will drop the $\widetilde{\ }$ and simply write 1, 2, $n$.


Below we list the PA Axioms ("nonlogical" —i.e., not needed for Logic— or mathematical Axioms). We will quote a few (but not all) of them here. But as I will sometimes say "original PA Axioms" it is fair to know which ones those are. We will also use (without proof usually as it would be far to hard and outside our means and goals) PA Theorems (and lemmata) as "Axioms". Which is fine as long as we do NOT misquote them!! (See MATH 1090 classes or text [Tou08]) where it is shown that a known (proved) theorem can be used exactly as an axiom in a proof).

**0.2 Definition. (Peano Arithmetic Axioms)** The axioms are the universal closures of the formulas in the groups PA-1, PA-2 etc., below. The universal closure of a formula $A$ is the *minimum partial generalisation* (cf. MATH 1090 classes or text [Tou08]) of $A$ that bounds *all* its free variables.

Thus, all Axioms are closed, that is, they have no free variables.

**PA-1.** (*Regarding* $\boldsymbol{S}$)

- $\boldsymbol{S1}$. $0 < Sx$ (for any variable $x$; the Axiom is alternatively given as $\neg 0 = Sx$ which only causes a minor shuffle to early theorems.)
- $\boldsymbol{S2}$. $Sx = Sy \to x = y$ (for any variables $x, y$; as we recognise via MATH 1019, this says that $S$ is 1-1.)

**PA-2.** (*Regarding* $+$)

- $\boldsymbol{+1}$. $x + 0 = x$ (for any variable $x$)
- $\boldsymbol{+2}$. $x + Sy = S(x + y)$ (for any variables $x, y$)

**PA-3.** (*Regarding* $\times$)

- $\boldsymbol{\times 1}$. $x \times 0 = 0$ (for any variable $x$)
- $\boldsymbol{\times 2}$. $x \times Sy = (x \times y) + x$ (for any variables $x, y$)

**PA-4.** (*Regarding* $<$)

- $\boldsymbol{<1}$. $\neg x < 0$ (for any variable $x$)
- $\boldsymbol{<2}$. $x < Sy \equiv x < y \vee x = y$ (for any variables $x, y$)
- $\boldsymbol{<3}$. $x < y \vee x = y \vee y < z$ (for any variables $x, y$)

**PA-5.** (**Induction**.)

This is the schema $A[x := 0] \wedge (\forall x)(A \to A[x := Sx]) \to (\forall x)A$ □

**0.3 Remark. For what follows in this subsection we note**

- We use the simplified "$\vdash A$" for the correct "$PA \vdash A$", that is, "$A$ is proved from the Axioms of PA".

- Since all the PA axioms are closed, we have for all formulas $A$ and variables $x$,
$$\text{If } \vdash A \text{ (i.e., } PA \vdash A\text{), then } \vdash (\forall x)A$$

□ 

We can speak neither of square roots in PA (the symbol "$\sqrt{\ }$" is *not even in the alphabet* of PA) nor can PA speak of fractions $m/n$.

Thus we will prove, instead of the impossibility of (1) on p.3, that the equivalent statement (equivalent over the reals, that is) obtained by squaring both sides of (1) and "distributing" the fraction —that is, (2) below— is *not* a PA theorem.
$$2n^2 = m^2 \tag{2}$$
We will "cheat" by taking a few standard PA theorems as *additional* (to the original Axioms of 0.2) starting points —as Axioms— given that it is extremely tedious to develop PA from scratch (if you don't believe me see chapter 2 here: [Tou03]).

Before we proceed let us state correctly, in a Gentzen-style format ("fraction" like configuration), the "auxiliary variable metatheorem" (covered and used in MATH 1090, albeit in a Hilbert style setting):
$$\text{L}\exists\ \frac{\Gamma, A[x := y] \vdash B}{\Gamma, (\exists x)A \vdash B} \text{ provided } y \text{ is } \textit{fresh} \text{ for the denominator}$$
Here $\Gamma$ is a set of formulae, and $A$ and $B$ are individual formulae. What the "rule" says is that if from the *hypotheses* $\Gamma \cup \{A[x := y]\}$ we can prove $B$, then we can prove $B$ also from the hypotheses $\Gamma \cup \{(\exists x)A\}$ *as long as the restriction on the new variable* (Gentzen called it "*eigenvariable*") *holds*.

The "wordy" elaboration of the "left $\exists$" rule above is the version (meta) proved in MATH1090. In the course we named $y$ the "auxiliary variable" (see also [Tou08]). In use, this rule allows *elimination* of $\exists$, in the sense that instead of proving $\Gamma, (\exists x)A \vdash B$ we prove the *stronger* —and easier[‡]— $\Gamma, A[x := y] \vdash B$ in its place.

Let us apply the idea in proving —within PA— that "if $x$ is odd, then so is $x^2$". We assume all the normal "algebra" over $\mathbb{N}$ as well as the definition (3) below, where $O(x)$ stands, intuitively, for "$x$ is odd"; thus $O$ is a *defined* (unary) predicate.
$$O(x) \overset{Def}{\equiv} (\exists y)x = 2y + 1 \tag{3}$$

 We are working *formally* in $\mathbb{N}$ arithmetic, *without* set theory! Thus expressions like $x \in \mathbb{N}$ *have no place*.

[‡]Why "easier"? Because removing the leading $\exists$ may uncover user-friendly Boolean structure in $A$, and if so, we may be able to use "tautological implications" in our proof.

The only "cheating" we allow is "knowing" a few theorems! But we will state them explicitly, as if they were axioms!

Our first task is to prove

$$\vdash O(x) \to O(x^2) \tag{4}$$

As we know (MATH 1090) this is *equivalent*[§] to proving the "easier"

$$O(x) \vdash O(x^2) \tag{4'}$$

In view of (3), (4′) translates into the task

$$(\exists y)x = 2y + 1 \vdash O(x^2)$$

and using our L∃ rule it *suffices* to prove

$$x = 2z + 1 \vdash O(x^2), \text{ where } z \text{ is fresh.} \tag{4''}$$

We have a short equational proof

$$\begin{array}{ll} & x = 2z + 1 \\ \Rightarrow & \langle \text{algebra of } \mathbb{N}\text{: squaring both sides of "="} \rangle \\ & x^2 = (2z + 1)^2 \\ \Leftrightarrow & \langle \text{Leib. and algebra of } \mathbb{N}\text{: expand} \rangle \\ & x^2 = 4z^2 + 4z + 1 \\ \Leftrightarrow & \langle \text{Leib. and algebra of } \mathbb{N}\text{: factor} \rangle \\ & x^2 = 2\Big(2z^2 + 2z\Big) + 1 \\ \Rightarrow & \langle \text{Dual Spec. (MATH 1090 or [Tou08])} \rangle \\ & (\exists y)x^2 = 2y + 1 \\ \Leftrightarrow & \langle \text{Def. (3)} \rangle \\ & O(x^2) \end{array}$$

The above proves $\vdash x = 2z + 1 \to O(x^2)$ hence also (4″) as needed.

Next, the definition of an even natural number:

**0.4 Definition.**

$$E(x) \stackrel{Def}{=} (\exists y)x = 2y \tag{6}$$

□

Before our next step, which will be relating $O(x)$ to $E(x)$, we will also profit from the following review:

[§](4) meta implies (4′) by modus ponens; the converse meta implication is by the Deduction Theorem.

**0.5 Definition. (Definition of "$\leq$")**

$$x \leq y \stackrel{Def}{\equiv} \neg y < x$$

□

The formulas in Lemma 0.6 below are hard to prove as most require formalised induction within PA (see [Tou03]) but fortunately are not hard to "believe". All stated formulas are known to us as (informal) theorems of the arithmetic of natural numbers, say from EECS 1019 or even from High School.

Here we take them too as Axioms since we do not offer proof (but someone else does, so we are good; we would *never* take as axiom the first thing that comes to our mind!).

**0.6 Lemma.**

1. $\vdash x < y \wedge y < z \rightarrow x < z$
2. $\vdash \neg x < x$
3. $\vdash x \leq y \equiv x = y \vee x < y$
4. $\vdash x < y \rightarrow Sx < Sx$
5. $\vdash x < y \equiv Sx \leq y$

*Proof.* Proofs can be found in [Tou03] but it is not recommended to look:

1. The proofs are hard.
2. This reference is incompatible with the MATH 1090 approach as it adopts "strong generalisation" *axiomatically*. On the other hand in the MATH 1090 approach we prefer to "hide" generalisation in the axioms and *only take modus ponens axiomatically*. Thus we can prove that we *only* have weak generalisation in the MATH 1090 case! "Only"? Yes! Both in MATH 1090 lectures and in [Tou08] we show that strong generalisation is invalid.

   Then is [Tou03] "wrong"?

   No, they are two different approaches. This reference adopts strong generalisation, so to generalise is easy; unconstrained. But applying the deduction theorem is hard.

   The [Tou08] makes generalisation hard (weak generalisation "$(\forall x)A$" **cannot be applied** if the axioms that proved $A$ have a free $x$). The up side is that applying the deduction theorem is easy!

   A trade off!

□

**0.7 Lemma.**

- $\vdash 0 < 1$
- $\vdash 1 < 2$
- $\vdash 0 < 2$

*Proof.*

- $\vdash 0 < 1$; The first PA axiom is $\vdash (\forall x)0 < Sx$, hence (specialization) $\vdash 0 < St$ for any term $t$. In particular, $\vdash 0 < S0$, that is, $\vdash 0 < 1$
- $\vdash 1 < 2$; we know that the function $S$ ("$+1$") is strictly increasing (4 in 0.6). Thus, from the previous bullet we get $\vdash S0 < S1$. But $S1 = SS0 = 2$ thus we are done.
- $\vdash 0 < 2$; bullets one and two and transitivity of $<$ (1 in 0.6). □

**0.8 Remark.** We immediately have $\vdash (\forall x)0 \leq y$. By Remark 0.3, it suffices to see that $\vdash 0 \leq y$. To this end, note that Axiom PA-4 (2) states $\vdash (\forall x, y)(x < Sy \equiv x = y \vee x < y)$ or, using 3 of Lemma 0.6 and rule Leibniz[¶], we have $\vdash (\forall x, y)(x < Sy \equiv x \leq y)$. Specialising we get

$$\vdash 0 < Sy \equiv 0 \leq y$$

Since $\vdash 0 < Sy$ is an Axiom, we obtain $\vdash 0 \leq y$ by tautological implication. We may add "$(\forall y)$" in front now, by Remark 0.3. □

**0.9 Theorem. (Euclid)** *For all $x, y$, where $y > 0$, there are $z$ and $w$, with $0 \leq w < y$ (conjunctionally), such that $x = yz^{\|} + w$. Informally, this theorem, due to Euclid,[**] says that dividing $x$ by $y$ there will be a* quotient $z$ *and a* remainder $w$ *satisfying the inequality $0 \leq w < y$.*

*Formally,*

$$(\forall x, y)\Big(0 < y \to (\exists z, w)(w < y \wedge x = y \times z + w)\Big)$$

One specialisation instance of the directly above is

$$\vdash 0 < 2 \to (\exists z, w)(w < 2 \wedge x = 2z + w) \tag{7}$$

By Lemma 0.7 (3rd bullet) and tautological implication, we get from (7)

$$\vdash (\exists z, w)(w < 2 \wedge x = 2z + w) \tag{8}$$

[¶] In fact the "weak Leibniz with unrestricted substitution" —acronym WL; see [Tou08], and/or MATH1090 class notes.

[‖] *Proper* notation in PA is $x = y \times z + w$. However we normally employ the common *argot* of "implied multiplication symbol".

[**] The Euclid Theorem also states that for a given $x$ and $y$ the quotient and the remainder are unique, but we will not quote this fact here.

and applying the auxiliary variable metatheorem we may "eliminate" $\exists$ from (8) and add the *assumption* $(*)$ below in our subsequent reasoning, where the variables $r$ and $q$ are fresh:

$$r < 2 \wedge x = 2q + r \qquad (*)$$

Note that we did not forget the conjunct $0 \leq w$ above, from the formal theorem onwards. In Remark 0.8 we proved $\vdash 0 \leq y$. But as we know from MATH 1090, every such theorem can be replaced (is equivalent to)[††] by $\top$, which as a *member of a conjunction is redundant*!

Next let us ponder the question: What can we conclude from $r < 2$ where $r$ is (*as it is throughout this subsection*) an $\mathbb{N}$-variable?

We can conclude that $r = 0$ or $r = 1$!

Let us see if we can *prove* this "easy" and taken for granted fact!

**0.10 Lemma.** $\vdash r < 2 \equiv r = 0 \vee r = 1$.

*Proof.*

$$\begin{aligned}
& r < 2 \\
\Leftrightarrow\ & \langle \text{Def. of } 2 \rangle \\
& r < S1 \\
\Leftrightarrow\ & \langle \text{Axiom PA-4 (2)} \rangle \\
& r = 1 \vee r < 1 \\
\Leftrightarrow\ & \langle \text{Def. of 1 and Leib.} \rangle \\
& r = 1 \vee r < S0 \\
\Leftrightarrow\ & \langle \text{Axiom PA-4 (2) and Leib.} \rangle \\
& r = 1 \vee r = 0 \vee r < 0 \\
\Leftrightarrow\ & \langle \text{ Leib. and } \neg\neg \text{ theorem} \rangle \\
& r = 1 \vee r = 0 \vee \neg\neg r < 0 \\
\Leftrightarrow\ & \langle \text{Leib. and Axiom PA-4 (1)} \rangle \\
& r = 1 \vee r = 0 \vee \neg\top \\
\Leftrightarrow\ & \langle \text{tautological equivalence} \rangle \\
& r = 1 \vee r = 0
\end{aligned}$$

□

Is every number even *or* odd? Can a number be *both* even and odd? We know the answers as "yes" and "no".

[††] $\Gamma \vdash A$ iff $\Gamma \vdash A \equiv \top$.

How do we *know*?

Let $x$ be a variable. We proceed from $(*)$, p.9.

As the hypothesis $(*)$ is equivalent to two

$$x = 2q + r, \qquad r < 2 \tag{9}$$

we do a proof by cases, since $r < 2$ yields two cases by Lemma 0.10:

- Case $r = 0$. Then the other hypothesis yields $\vdash x = 2q$ and we get $\vdash (\exists y)x = 2y$ that is $\vdash E(x)$.
- Case $r = 1$. Then the other hypothesis yields $\vdash x = 2q + 1$ and we get $\vdash (\exists y)x = 2y + 1$ that is $\vdash O(x)$.

By the proof by cases metatheorem we have proved

$$\vdash E(x) \vee O(x) \tag{$\dagger$}$$

Next we show that there is *no* number that is *both* even and odd.

**0.11 Theorem.** $\vdash \neg(\exists u)\Big(O(u) \wedge E(u)\Big)$.

*Proof.* Arguing by contradiction[‡‡]

$$\text{Let us assume } (\exists u)\Big(O(u) \wedge E(u)\Big)$$

We argue by the method of the auxiliary variable, that is, we now

$$\textit{assume } O(x) \wedge E(x), \text{ where } x \text{ is fresh}$$

So, by splitting the "$\wedge$" as we have learnt in MATH 1090, we have two hypotheses: $O(x)$, that is

$$(\exists y)x = 2y + 1 \tag{$h1$}$$

and $E(x)$, that is

$$(\exists y)x = 2y \tag{$h2$}$$

$(h1)$ allows us to assume

$$x = 2z + 1 \tag{10}$$

while $(h2)$ allows us to assume

$$x = 2w \tag{11}$$

where $z$ and $w$ are fresh. So, ((10) and (11) and transitivity of $=$) *we start with*

$$2z + 1 = 2w$$

[‡‡]From MATH 1090: $\Gamma \vdash A$ iff $\Gamma, \neg A \vdash \perp$.

or equivalently (algebra)

$$1 = 2(w - z)^{\S\S} \tag{12}$$

We have two cases on $w - z$ —since $\vdash 0 \leq w - z$ by 0.8 and $\vdash 0 \leq w - z \equiv 0 = w - z \vee 0 < w - z$ by 0.6 (3):

Case $0 = w - z$: Then

$$\begin{aligned}
& 1 \\
= & \langle (12) \rangle \\
& 2(w - z) \\
< & \langle \text{algebra: multiplying two sides of } < \text{ by } 2 \rangle \\
& 2 \times 0 \\
= & \langle \text{Axiom PA-3 (1)} \rangle \\
& 0 \\
< & \langle \text{Lemma 0.7} \rangle \\
& S0 \\
= & \langle \text{translate} \rangle \\
& 1
\end{aligned}$$

I.e., we have $\vdash 1 < 1$ contradicting 2 of 0.6.

Case $0 < w - z$: This is equivalent to $\vdash 1 \leq w - z$ by 5 of Lemma 0.6: We have the calculation

$$\begin{aligned}
& 1 \\
= & \langle (12) \rangle \\
& 2(w - z) \\
\geq & \langle \text{algebra: multiplying two sides of } \geq \text{ by } 2 \rangle \\
& 2 \times 1 \\
= & \langle \text{algebra} \rangle \\
& 2
\end{aligned}$$

§§ "–"? In PA?! OK, ok. This was *argot*. But now that you noticed, one *can* **define** in PA $x \dot{-} y$, which means "if $x < y$ then 0, else $x - y$". Here: Imitating the recursive definitions PA-2 and PA-3, define first a new function "$p(x)$" (predecessor) by the equations

$$\begin{aligned}
p(0) &= 0 \\
p(Sx) &= x
\end{aligned}$$

and then

$$\begin{aligned}
x \dot{-} 0 &= x \\
x \dot{-} Sy &= p(x \dot{-} x)
\end{aligned}$$

Thus we proved $\vdash 1 \geq 2$ under this case. By Definition 0.5 we have proved $\vdash \neg 1 < 2$. On the other hand, Lemma 0.7 (2) also proves $\vdash 1 < 2$. We got our contradiction!

BTW, after all this, the proof by contradiction metatheorem establishes that

$$\vdash \neg(\exists u)\Big(O(u) \wedge E(u)\Big)$$

and hence

$$\vdash (\forall u)\Big(\neg O(u) \vee \neg E(u)\Big)$$

or, using specialisation,

$$\vdash \neg O(u) \vee \neg E(u)$$

Now, rewrite the above as the tautologically equivalent

$$\vdash E(u) \to \neg O(u) \tag{13}$$

On the other hand, (†) on p.10 is tautologically equivalent to

$$\vdash \neg O(u) \to E(u) \tag{14}$$

We thus have (tautological implication from (13) and (14), or ping-pong principle)

$$\vdash E(u) \equiv \neg O(u) \tag{$**$}$$

We are ready for

**0.12 Theorem.** *$\sqrt{2}$ is irrational. That is, for no integers $m > 0, n > 0$ can we have $\sqrt{2} = m/n$*

*Proof.* We prove this by formal contradiction, but as already noted, the **assumption** that we will contradict is the expressible within PA equivalent statement:

$$2n^2 = m^2 \tag{‡}$$

We add for free the assumption that

$$m \text{ and } n \text{ have 1 as the only common factor.} \tag{$\|$}$$

since if we had $\sqrt{2} = m/n$ we could always make $m/n$ *irreducible* by dividing both numerator and denominator by $gcd(m, n)$, that is the *greatest* (read "largest") *common factor* of $m, n$. □

We have the calculation

$$
\begin{array}{ll}
 & 2n^2 = m^2 \\
\Rightarrow & \langle \text{Dual Spec.} \rangle \\
 & (\exists y) 2y = m^2 \\
\Leftrightarrow & \langle \text{Def. 0.4} \rangle \\
 & E(m^2) \qquad \blacktriangleleft \\
\Leftrightarrow & \langle (**) \text{ above} \rangle \\
 & \neg O(m^2) \\
\Rightarrow & \langle \text{contrapositive of (4), p.0.2} \rangle \\
 & \neg O(m) \\
\Leftrightarrow & \langle (**) \text{ above and the tautology } A \equiv \neg B \equiv \neg A \equiv B \rangle \\
 & E(m)
\end{array}
$$

Thus, by (‡) we have proved $\vdash E(m)$ and hence $(\exists y) 2y = m$. Pick a fresh $w$ then, and add the assumption $2w = m$. We now calculate as follows:

$$
\begin{array}{ll}
 & 2w = m \\
\Rightarrow & \langle \text{squaring both sides of } = \rangle \\
 & 4w^2 = m^2 \\
\Rightarrow & \langle \text{Def. transitivity of } = \text{ and } (\ddagger) \rangle \\
 & 4w^2 = 2n^2 \\
\Leftrightarrow & \langle \text{simplify by 2} \rangle \\
 & 2w^2 = n^2 \\
\Rightarrow & \langle \text{Dual Spec.} \rangle \\
 & (\exists y) 2y = n^2 \\
\Leftrightarrow & \langle \text{Def. 0.4} \rangle \\
 & E(n^2) \\
\Rightarrow & \langle \text{by the proof segment, in the previous proof, from the mark } \blacktriangleleft \text{ onwards} \rangle \\
 & E(n)
\end{array}
$$

We have just concluded that $m$ and $n$ have 2 as a common factor contrary to the assumption ($\|$). We are done! □

# References


[Tou03] G. Tourlakis, *Lectures in Logic and Set Theory; Volume 1: Mathematical Logic*, Cambridge University Press, Cambridge, 2003.

[Tou08] ———, *Mathematical Logic*, John Wiley & Sons, Hoboken, NJ, 2008.