ON THE ALLEGED SIMPLICITY OF IMPURE PROOF

ANDREW ARANA

Abstract. Roughly, a proof of a theorem, is "pure" if it draws *only* on what is "close" or "intrinsic" to that theorem. This article considers the contention that impure proofs, drawing on means "distant" or "foreign" to what is being proved, are generally simpler than pure proofs. After clarifying this claim, evidence for it from proof theory is assembled. It is shown that this evidence does not support the claim.

Roughly, a proof of a theorem, is "pure" if it draws *only* on what is "close" or "intrinsic" to that theorem. Mathematicians employ a variety of terms to identify pure proofs, saying that a pure proof is one that avoids what is "extrinsic", "extraneous", "distant", "remote", "alien", or "foreign" to the problem or theorem under investigation. In the background of these attributions is the view that there is a distance measure (or a variety of such measures) between mathematical statements and proofs. Mathematicians have paid little attention to specifying such distance measures precisely because in practice certain methods of proof have seemed self-evidently impure by design: think for instance of analytic geometry and analytic number theory. By contrast mathematicians have paid considerable attention to whether such impurities are a good thing or to be avoided, and some have claimed that they are valuable because generally impure proofs are *simpler* than pure proofs. This article is an investigation of this claim, formulated more precisely by proof-theoretic means. After assembling evidence from proof theory that may be thought to support this claim, we will argue that on the contrary this evidence does not support the claim.

1. The purity debate in overview

A purity constraint, restricting proofs of theorems to what is "close" or "intrinsic" to that theorem, requires an account of how the distance between proof and theorem is to be measured. Two such measures of distance are what we have called "elemental" and "topical" distance. A proof is *elementally close* to a theorem if the proof draws only on what is more elementary or simpler than the theorem (cf. [Arang]). A proof is *topically close* to a theorem if the proof draws only on what belongs to the content of the theorem, or what we have called the *topic* of the theorem (cf. [DA11] and [AM12]). Each of these distance metric induces a purity constraint,

Date: June 5, 2016.
Forthcoming in *Simplicity: Ideals of Practice in Mathematics and the Arts*, edited by Roman Kossak and Philip Ording, Springer. Thanks to Walter Dean, Michael Detlefsen, Sébastien Maronne, Mitsuhiro Okada, Marco Panza, and Sean Walsh for helpful discussions on these subjects.

viz. elemental purity and topical purity. In these articles cases from mathematics have been presented that make evident the importance of these constraints in the history of mathematics through the present.

Once a purity constraint has been identified, we can ask why mathematicians value proofs that obey such a constraint. The basic case for preferring elementally pure proofs over elementally impure proofs, made in [Arang], is that elementarily pure proofs make the most efficient use of the information at the disposal of a given investigator (e.g. a student who knows little more than what a problem asks to be done). By contrast, in [DA11] the case is made that pure proofs give better reason to believe that *the* statement whose proof is sought has been proved, rather than some other, perhaps closely related, statement. This analysis takes a "vectorial" conception of mathematical investigation, in which the success of a proof is determined by the extent to which it is directed at exactly the intended statement. A proof may succeed as a proof of some different statement while failing as a proof of the statement towards which it was intended to be directed.

By contrast, impure proofs have been judged valuable on account of their illuminating previously unseen connections. For example, Kreisel has written:

> But also there is the void created by simply not saying out loud what (knowledge) is gained by impure proofs, for example by analytic proofs in number theory: knowledge of *relations between the natural numbers and the complex plane* or, more fully, between arithmetic and geometric properties. It is precisely this knowledge which provides effective new means of checking proofs: if this conflicts with some ideal of rigour, so much the worse for the ideal (which is being tested). (Cf. [Kre80], p. 167)

Additionally, it is a technical feat to use evidently "distant" methods to solve a problem at hand. In a way that is what is so impressive about them. We wonder how it is that, for instance, complex analysis can be brought to bear on arithmetic. and we are struck that this is possible. Whereas when seeking a pure proof, the search space is constrained, and so the strikingly distant connections characteristic of impurity cannot arise.

This constraint of the search space can be thought to be an advantage in proof, since the variety of considerations that can be brought to bear on the directing problem or theorem includes only a fraction of all the possible considerations that might otherwise be tried. Additionally, one might think that the "closeness" of proof to theorem would engender other justificatory efficiencies, since such proofs will avoid what would seem from outside the practice to be extraneous or "roundabout".

However, there is a strand of theorizing on mathematics that emphasizes the opposite, stressing the *simplicity* of impure proof in comparison with pure proof. Such claims have been made, for instance, on behalf of analytic geometry and of complex analysis in real arithmetic and analysis.

Let us consider these claims in further detail now, so that we can more precisely *formulate* and *evaluate* theses concerning the simplicity of impure proof relative to pure proof.

2. Simplicity and impurity in mathematical practice

Since the seventeenth century analytic methods have been viewed by many as a source of impurity in geometry, in contrast to the coordinate-free "synthetic" methods typified by Euclidean geometry. Descartes canonized a procedure for solving geometrical problems as follows: first express the problem by algebraic equations, then solve these equations by algebraic manipulations, and finish by translating these algebraic solutions back into geometrical terms. He lauded this method for making it "easy" [*aisé*] to find constructions, though he noted that sometimes the method requires "dexterity" [*adresse*] in order to find "short and simple" [*courtes et simples*] constructions.[1] Note that this Descartes here distinguishes two types of simplicity: the simplicity of *discovering* a solution to a problem, and the simplicity of the construction itself. This distinction will recur and we will return to it shortly.

In contrast with Descartes, some mathematicians have judged such use of algebra in geometry to be "rather far" from the problems at hand, and thus impure. Consider for example the following passage of Newton:

> Equations are Expressions of Arithmetical Computation, and properly have no Place in Geometry, except as far as Quantities truly Geometrical (that is, Lines, Surfaces, Solids, and Propositions) may be said to be some equal to others. Multiplications, Divisions, and such sort of Computations, are newly received into Geometry, and that unwarily, and contrary to the first Design of this Science.... Therefore these two Sciences ought not to be confounded. The Antients did so industriously distinguish them from one another, that they never introduced Arithmetical Terms into Geometry. And the moderns, by confounding both, have lost the Simplicity in which all the Elegancy of Geometry consists. (Cf. [New20], p. 119–20)

Newton spelled out the type of geometric simplicity he sought in the following passage:

> Men of recent times, eager to add to the discoveries of the ancients, have united specious arithmetic [i.e., algebra] with geometry. Benefitting from that, progress has been broad and far-reaching if your eye is on the profuseness of output but the advance is less of a blessing if you look at the complexity of its conclusions. For these computations, progressing by means of arithmetical operations alone, very often express in an intolerably roundabout way quantities which in geometry

[1] Cf. [Des37], p. 351, though statements of this sort are found throughout *La géométrie*. For more on the simplicity of the Cartesian method in geometry, cf. [Ara16], §2, and [Mar10].

> are designated by the drawing of a single line. (cf. [New71], p. 421; translation from [Gui09], p. 77)

Thus Newton identified the impurity of algebra in geometry as detracting from the simplicity of geometrical reasoning that ancient works had exemplified.

Newton's views would come to seem rather peculiar, as the power of the Cartesian method became increasingly evident (cf. [Pyc97] and [Gui09]). This power was characterized by Colin MacLaurin, a contemporary and expositor of Newton, as follows:

> The improvements that have been made by [analytic methods], either in geometry or in philosophy, are in great measure owing to the facility, conciseness, and great extent of the method of computation, or algebraic part. (cf. [Mac42], Book 2, p. 163)

Similarly, Lagrange and Klein emphasized the utility of algebraic methods in geometry. Lagrange wrote:

> As long as algebra and geometry have been separated, their progress has been slow and their usage limited; but when these two sciences are reunited, they lend each other strength and march onward together at a rapid pace toward perfection.[2]

Along the same lines, Klein wrote:

> As a matter of principle, we have always availed ourselves of the aids of analysis, and in particular of the methods of analytic geometry. Hence we shall here again assume a knowledge of analysis, and we shall inquire *how we can go, in the shortest way, from a given system of axioms to the theorems of analytic geometry*. This simple formulation is, unfortunately, rarely employed, because geometricians often have a certain aversion to the use of analysis, and desire, insofar as possible, to get along without the use of numbers. (Cf. [Kle53], p. 160)

While MacLaurin, Lagrange and Klein were clearly promoting the gain in simplicity afforded by algebra in geometry, these passages leave it unclear whether they intended to promote the gain it affords in producing work that is simple to verify once located, or in the discovery of geometric results in the first place. Detlefsen has drawn attention to this distinction, identifying the former type of simplicity as *verificational* simplicity and the latter as *inventional* simplicity (cf. [Det90], p. 376 and [Det96], p. 87). Verificational simplicity measures the simplicity of determining whether a given proof is a proof at all; thus it measures the simplicity of confirming the validity of the deductions of a given proof. By contrast, inventional simplicity measures the simplicity of discovering a proof of a given statement. MacLaurin's remarks on the simplicity of algebraic methods in geometry do not seem to be sensitive to this distinction.

[2]Cf. [Lag76], p. 271. For a detailed historical investigation of Lagrange's views on purity in his algebraic work, cf. [FP11].

By contrast with MacLaurin, Lagrange and Klein, d'Alembert claimed explicitly that algebraic methods in geometry afford both types of simplicity. Firstly, he remarked of ancient geometrical works "that almost no one reads them with the ease [*facilité*] given by algebra in reducing their demonstrations to a few lines of calculation" (cf. [d'A51], p. 551). He thus stressed the gain in verificational simplicity that algebraic considerations can bring to geometrical proof. He went on to remark, though, that these considerations enable us to "arrive nearly automatically at results giving the theorem or the problem that we sought, which otherwise we would not have gotten or would only have gotten with much effort." (*Ibid.*) That is, he also stressed that our ability to discover results in geometry is improved when we make use of algebraic methods (though he also noted exceptions to this, in particular when trigonometric expressions were involved).

We find such claims regarding the simplicity of impure methods also in discussion of the application of complex analysis to real analysis, algebra and arithmetic. One prominent example of such application was in the theory of equations. Algebraists since Cardano had sought exact solutions in finite terms to cubic polynomial equations with rational coefficients having three *real* roots, and were dismayed to discover that this seemed to require using imaginary numbers. This is an apparent impurity for a problem concerning just real algebra. The *casus irreducibilis*, as this is known, spurred numerous, unsuccessful attempts to avoid imaginary numbers, even leading to a prize question in 1781 from the scientific academy in Padua.[3]

Another such example is the prime number theorem, a result concerning the distribution of prime numbers among the natural numbers that gives a precise estimate of the number of primes less than a given natural number.[4] It was proved by Hadamard (cf. [Had96]) and, independently, de la Vallée Poussin (cf. [dlVP96]) using complex analysis in 1896. Their use of imaginary numbers to solve a number-theoretic problem was judged impure by many , spurring work that led to the "elementary" proofs of Selberg and Erdős in 1949 that avoid reference to imaginary numbers (cf. [Sel49] and [Erd49]). The elementary proofs have been viewed as more pure than the complex analytic proofs; as Granville recently put it, "A simple question like 'How many primes are there up to x?' deserves a simple answer, one that uses elementary methods rather than all of these methods of complex analysis, which seem rather far from the question at hand."[5]

As with the application of algebra to geometry, these allegedly impure solutions have been promoted for their alleged efficiency. In a famous remark, Hadamard observed that "the shortest

[3]The prize question is described in [Rid82], p. 4. Otto Hölder showed in 1892 that there is no exact solution in finite terms to cubics in the casus irreducibilis that avoids imaginary numbers; cf. [Höl92]. For a more thorough discussion of the casus irreducibilis in relation to purity, cf. [Ara08].

[4]More precisely, the prime number theorem states that $\frac{\pi(x)}{x/\log(x)}$ approaches 1 in the limit, where $\pi(x)$ is the number of primes less than or equal to x.

[5]Cf. [Gra08], p. 338. For more on purity in arithmetic, cf. [Ara14] and [Arang].

and best way between two truths of the real domain often passes through the imaginary one" (cf. [Had45], p. 123). Palle Jorgensen (cf. [Jor15]) has observed that Hadamard, who prefixes this passage by saying that "it has been written", is referring to the following passage of Painlevé's:

> The natural development of this study soon led geometers to embrace in their research imaginary values of variables as well as real values. The theory of Taylor series, of elliptic functions, the vast doctrine of Cauchy made the fecundity of this generalization erupt. It appeared that between two truths in the real domain, the easiest and shortest path often passes through the complex domain. (Cf. [Pai72], pp. 72–73)

Hadamard and Painlevé presumably had in mind applications of complex analysis in the solution of differential equations, in the evaluation of real integrals using residue theory, and in the solution to arithmetic problems by analytic number theory. Once again, though, there is ambiguity concerning whether they meant that the "easiest" or "shortest" paths engendered by complex analysis are easy or short when it comes to verifying proofs or to discovering them.

None of the authors just surveyed seem to have had sharp measures of the type of simplicity to which they were appealing. Because of their expertise the anecdotal evidence they offer ought to be taken seriously. However, claims of the sort quoted here are typically given as part of a broader polemic in which the author is promoting his or her own favored approach to the topic in question. We thus ought to take their *evidence* with a grain of salt.

However, we should take their *claims* very seriously. If true, they would undermine the value purity has been taken to have by many mathematicians. More precisely, the value of pure proof would be countered by disadvantages if impure proof is *generally* or *systematically* simpler than pure proof. Toward determining if this is so, the tradeoff between the difficulty of discovering impure proofs, and the simplicity impurity allegedly confers, warrants further investigation.

It is thus urgent to formulate claims regarding the simplicity of impure proof relative to pure proof, so that the theses in question can be better evaluated. We have identified the following two theses in the reflections we have surveyed:

> **Thesis 1:** Impure proofs are generally simpler to *verify* than pure proofs of the same statement.

> **Thesis 2:** Impure proofs are generally simpler to *discover* than pure proofs of the same statement.

One way to evaluate these theses would be to undertake a detailed case study of a mathematical sub-discipline, as Avigad does for number theory in [Avi06], and to evaluate simplicity claims on the basis of this investigation. An alternate way would be to consider the theses in light

of work in proof theory.[6] In this paper we will undertake the latter kind of evaluation. Each approach brings different information and is valuable for different reasons. The chief advantage of the formal approach is that it permits the theses to be formulated exactly and for those theses to be evaluated systematically. Its chief disadvantage is that proof-theoretic formulations may distort the phenomena being measured. We will address this disadvantage as they come to light in the ensuing discussion. In general we believe that this investigation should be carried out side-by-side by case study investigations; such investigations may lead to new formal measures of proof complexity.

As we have explained, these theses, if true, would give reason to discount the value of purity. This would not be the case if *some* impure proofs are simpler than pure proofs of the same theorems; rather, what needs to be investigated is whether there is a *general* pattern of improvement of simplicity when moving from pure to impure proof. This article focuses on Thesis 1; Thesis 2 will be addressed in another article. Our main finding in this article is that work in proof theory provides little evidence for thinking that there is a general pattern of improvement of verificational simplicity when moving from pure to impure proof.

3. A formal evaluation of simplicity of impure proof

In order to investigate Thesis 1, we will focus on the verificational simplicity of theorems in these theories. We will use as a measure of verificational simplicity the length of proofs in formal theories. This measure is well-known in proof theory, and accordingly we will be able to employ theorems of proof theory to evaluate Thesis 1.

Our approach will be to investigate extensions of a given formal theory (which we will call the "base theory') by elements that yield, we will argue, *impure* proofs for theorems of that base theory. We will consider extensions that are "conservative" in the following rough sense: anything provable in the extended theory that can be expressed in the language of the base theory is already provable in the base theory. Thus we can compare the verificational simplicity of proofs of theorems of the base theory with proofs of those same theorems in an extended theory. We can thus compare the verificational simplicity of pure and impure proofs of theorems of the base theory.

Our strategy for this evaluation is as follows. In Section 3.1, we will introduce the formal theories to be studied here. In Section 3.2, we will argue that the extensions of the base theory permit impure proofs of theorems of the base theory. In Section 3.3, we will state what is known concerning the conservativity of these extensions over the base theory. In Section 3.4 we will introduce the aforementioned measure of verificational simplicity, proof length, and an apparatus for comparing the verificational simplicity of proofs known as "speed-up". In Section

[6]Note that in [Avi06] Avigad draws on work from automated reasoning, which is closely allied with proof theory; thus these approaches are not exclusive.

3.5 we will state what is known concerning the speed-up of proofs in the extended theory over proofs of the same theorems in the base theory. Finally, in Section 3.6, we will explain how this evidence bears on Thesis 1. Since proofs in the extended theories will be seen to be impure in general for theorems in the base theory, our case will be that the evidence tells against Thesis 1.

3.1. **The theories.** Our investigations will focus on formal theories of arithmetic. For starters, first-order Peano Arithmetic (PA) has axioms that define addition, multiplication, and an ordering of integers, as well as induction axioms given by the familiar induction schema. Its language $\mathscr{L}_{\mathrm{PA}}$ consists of constants 0, 1, function symbols +, ×, and relation symbol <. At the center of our investigations here, however, is the first-order arithmetic theory known as Primitive Recursive Arithmetic (PRA). PRA is obtained from first-order PA by adding to PA symbols and defining equations for all primitive recursive functions, and restricting the induction scheme to quantifier-free formulas.

PRA will serve as our "base theory" in the sense described above: our proof-theoretic observations will compare proofs of theorems in PRA with proofs of the same theorems in extensions of PRA. We will consider extensions of PRA of two different types, adopting a helpful classificatory scheme due to Ignjatović (cf. [Ign90] and [CI05]): "arithmetical" and "conceptual" extensions. These types of theories give proofs of theorems of PRA that are, as we will argue, *impure*.

Arithmetical extensions of PRA add new arithmetical principles, specifically induction schemas for more inclusive classes of arithmetical formulas. We will focus on the arithmetical extension $\mathrm{I}\Sigma_1$ of PRA, which is obtained from PA by restricting the induction schema to Σ^0_1-formulas. It is not obvious that $\mathrm{I}\Sigma_1$ is an extension of PRA, since PRA contains function symbols and defining equations for all the primitive recursive functions, and $\mathrm{I}\Sigma_1$ doesn't. But it can be shown that PRA is "essentially" included in $\mathrm{I}\Sigma_1$, as follows (cf. [Sim99], pp. 374–5, for the details). The language of $\mathrm{I}\Sigma_1$ (i.e. $\mathscr{L}_{\mathrm{PA}}$) can be interpreted in the language of PRA by what Simpson calls the "canonical interpretation", which (a) interprets 0 and 1 as 0 and 1 in the language of PRA; (b) interprets addition and multiplication as primitive recursive functions defined in the expected way; and (c) interprets < by defining predecessor and truncated subtraction as primitive recursive functions from which < can be straightforwardly defined. It can then be shown that any first-order formula that is provable in PRA is provable in $\mathrm{I}\Sigma_1$ when given the canonical interpretation. Moreover, any model of $\mathrm{I}\Sigma_1$ can be expanded to a model of PRA by interpreting the symbols for the primitive recursive functions according the their definitions. Since Σ^0_1 induction suffices to prove the totality of these functions, the language $\mathscr{L}_{\mathrm{PA}}$ can be extended to include these extra symbols while remaining conservative over $\mathrm{I}\Sigma_1$ (cf. [Sim99], §II.3, pp. 69–73, and [Kay91], Chapter 4).

By contrast, *conceptual* extensions add to PRA a new type of element, sets, and principles for using sets. We will focus on three conceptual extensions of PRA: RCA_0, WKL_0 and

WKL_0^+, each a subsystem of second-order arithmetic. Firstly, the theory RCA_0 is obtained by adding to PRA a comprehension schema for Δ_1^0-definable sets of numbers—that is, a *recursive* comprehension schema, hence the name—and replacing PRA's induction scheme with an induction schema for Σ_1^0 formulas, possibly with set parameters.[7] Secondly, WKL_0 is the theory RCA_0 augmented by weak König's lemma, which yields paths through infinite $\{0,1\}$-trees. Thirdly, WKL_0^+ is the theory WKL_0 augmented by a form of the Baire category theorem saying that every arithmetically defined sequence of dense open sets of Cantor space has non-empty intersection.

3.2. **Impurity.** Next, we will argue that each of these extensions of PRA yields impure proofs of theorems of PRA. Firstly, proofs of theorems of PRA in conceptual extensions of PRA are, in general, *topically* impure, because they draw on set-theoretic resources rather than just resources concerning natural numbers. Theorems of PRA, a first-order theory of arithmetic, are theorems about natural numbers and not sets: in particular, its quantifiers range over objects of arithmetic rather than set-theoretic type. While PRA also uses functions and relations on numbers, these functions can be understood algorithmically, without appeal to set theory. We see no good reason to think that a set-theoretic understanding of functions takes precedence, particularly in the case of PRA where the functions are merely used for computations on natural numbers.

One might object to this on the following grounds, following a suggestion of Sean Walsh. By the same reasoning, proofs of theorems of $\mathrm{I}\Sigma_1$ in RCA_0 are also topically impure, since they too deploy set-theoretic resources for proving arithmetic theorems. But $\mathrm{I}\Sigma_1$ and RCA_0 are mutually interpretable. Thus, we can translate any proof in RCA_0 into a proof in $\mathrm{I}\Sigma_1$, and thus into a proof that avoids set-theoretic resources; and this translations is line-by-line, as straightforward as it gets. Thus, one might maintain, the impurity of proofs in RCA_0 of theorems of $\mathrm{I}\Sigma_1$ is a mirage; proofs in RCA_0 use set-theoretic resources only in a superficial way, that can easily be expressed in non-set-theoretic ways, without any significant gain in length of proof.

This objection can be expressed more sharply, taking a cue from Wright in a slightly-different context:

> Well, I imagine it will be granted that to define the distinctively arithmetical concepts is so to define a range of expressions that the use thereby laid down for those expressions is indistinguishable from that of expressions which do indeed express those concepts. The interpretability of Peano arithmetic within Fregean arithmetic ensures that has already been accomplished as far as all pure arithmetical uses are concerned. (Cf. [Wri99], pp. 17–18; [HW01], p. 322)

[7] In [Sim99], Simpson defines RCA_0 (on p. 24) in a slightly different but equivalent way, using Σ_1^0-induction (with set parameters) but not primitive recursion. As he notes on p. 73, Friedman originally defined RCA_0 in the way we have done here; cf. [Fri76], pp. 557–8.

A topically pure proof of a theorem draws only on what belongs to the content of the theorem; following Wright, one could maintain that this includes concepts whose use is *indistinguishable* from that of concepts that feature in the statement of the theorem. Since the mutual interpretability of $I\Sigma_1$ and RCA_0 entails that the use of set-theoretic concepts in an RCA_0-proof of a $I\Sigma_1$-theorem is indistinguishable, in a precise sense, from the use of purely arithmetical resources, the objection asserts that an RCA_0-proof of a $I\Sigma_1$-theorem is in fact topically pure.

In reply, let's consider an agent P, a relative logical novice who is familiar with $I\Sigma_1$ but not RCA_0, because she does not know any set theory. She can understand theorems of $I\Sigma_1$ and $I\Sigma_1$-proofs of these theorems, but not RCA_0-proofs of them. The objector maintains that he can translate any $I\Sigma_1$-proof into an RCA_0-proof, but P does not understand the translated versions. The objector may reply that P "implicitly" understands the parts (terms, sentences) of the RCA_0-proof she purports not to understand, since she understands the parts of the $I\Sigma_1$-proof from which they have been translated. But P does not understand this translatability, since she does not know RCA_0. The objector may then reply that the type of "implicit" understanding of RCA_0-proofs intended here is not psychological, but rather *semantic*: that the meanings of the parts of RCA_0-proofs are the same as the meanings of the parts of $I\Sigma_1$-proofs. By virtue of mutual interpretability, parts of RCA_0-proofs play the same inferential role in proofs of $I\Sigma_1$-theorems as parts of $I\Sigma_1$-proofs. They thus have the same use, and hence the same meaning. Call this *Wright's thesis*. It follows, the objection goes, that agent P does in fact understand the parts of RCA_0-proofs she purports not to understand, since she understands their translations into $I\Sigma_1$.

Whatever the virtues of Wright's thesis otherwise, its application to mathematics dissolves important aspects of mathematical practice, and thus impairs our ability to understand this practice. For suppose we admit Wright's thesis, maintaining that if two theories T_1 and T_2 are mutually interpretable, then their semantic parts (terms, statements) have identical meanings. Hilbert showed that the theory of fields is mutually interpretable (with parameters) with the theory of Pappian projective planes (cf. [Hil99]). Thus purely geometric talk of projective planes can be term-by-term translated back and forth with purely algebraic talk of fields. Wright's thesis entails that this purely geometric talk and this purely algebraic talk have the same meaning. This goes against five hundred years of thinking in mathematics, where algebraic thinking and geometric thinking have been thought to be distinct (as discussed in Section 2). If the semantic boundary between algebra and geometry is dissolved, then topical purity for algebra and geometry is also dissolved, since topical purity is a semantic view as well. But topical purity has been and remains today important to mathematical practice, as we explained earlier and in several other referenced articles as well. Dissolving the semantic boundary between algebra and geometry would dissolve topical purity as a genuine constraint of mathematical practice, and would thus impair our ability to understand mathematical practice. That is too high a price

to pay for a controversial semantic view like Wright's thesis. Thus we reject Wright's thesis and maintain, against the objection, that RCA_0-proofs of $I\Sigma_1$-theorem are in general topically impure.

We next turn to the impurity of arithmetical extensions of PRA. This case is different than for conceptual extensions of PRA, because arithmetical extensions do not add set-theoretic resources to PRA. Thus they do not engender proofs that are obviously topically impure for PRA. Instead, these extensions add stronger induction principles than PRA. These principles are, as we will argue, less elementary than the quantifier-free induction of PRA, and thus proofs of theorems of PRA in conceptual extensions of PRA are, in general, *elementally* impure.

We focus on proofs of theorems of PRA using Σ_1-induction rather than just PRA's quantifier-free induction; that's to say, proofs that may apply the induction schema of PRA to Σ^0_1-formulas rather than just to quantifier-free formulas. Tait has argued that the finitist accepts quantifier-free induction, on constructive grounds, while not accepting Σ_1-induction (cf. [Tai81]). That's because there need be no way of constructing the existential witness of the conclusion of Σ_1-induction from the witnesses for the existential formulas in the antecedent clauses.

As a result, the finitist maintains that proofs using quantifier-free induction are (all else being equal) more *secure* than proofs using Σ_1-induction. Taking epistemic security as a criterion of elementarity, it follows that Σ_1-inductive proofs of theorems of PRA are elementally impure. Proofs of theorems of PRA using Σ_1-induction involve a redeployment of PRA's conceptual resources that does not meet the epistemic standards that the principles of PRA are taken to meet, and hence are elementally impure.

As the reference to finitism suggests, Hilbert arguably held a view of purity like this, at least in his later years (for discussions of Hilbert's earlier views on purity, see [Halo8], [AM12] and [Arao8]). As Kreisel described it, Hilbert's "famous consistency programme is also a particular case of this search for pure methods: so-called finitist theorems should have finitist proofs" (cf. [Kre80], p. 163). Hilbert characterized the "real" propositions of "ordinary finite number theory" as those that can be "developed through the construction of numbers by means solely of intuitive contentual considerations" that are basic "for mathematics and, in general, for all scientific thinking, understanding, and communication." (cf. [Hil25], p. 376). As he saw it, such "real" propositions, being "immediately intuitive and directly intelligible", were more securely knowable than "ideal" propositions which are non-contentual and are "merely things that are governed by our rules" (cf. [Hil25], p. 380). Hence, he judged, real propositions are best proved by real rather than ideal methods. Thus, we agree with Kreisel that Hilbert's program is a program for purity, in particular for elemental purity.[8]

[8]A significant remaining question is whether $I\Sigma_1$ is especially significant, as an arithmetical extension of PRA, for the thesis that impurity generally offers gains of efficiency; or whether a study of $I\Sigma_2$, for instance, would offer key additional insights. Toward this, Ignjatović has conjectured that further inductive strengthenings of PRA

Here too one could raise an objection. Friedman has conjectured that every arithmetical theorem already proved in the *Annals of Mathematics* can be proved in the theory known as elementary function arithmetic (EFA), which is proof-theoretically weaker than PRA (cf. [Avi03]). If true, one might infer that elemental purity is a trivial constraint: every arithmetic theorem has an elementally pure proof, indeed a *very* elementally pure proof. In reply, we observe firstly that Friedman's "grand" conjecture is far from certain. At the moment an active research program is aimed at showing that Fermat's Last Theorem is provable in EFA (cf. [McL10]), but even this modest step toward Friedman's conjecture is a long way from being settled. Secondly, even if true, the conjecture says nothing about the length of proofs of arithmetic theorems in EFA. One would expect them to be much longer in general. There are thus two notions of elementarity at play here: on the one hand, inductive strength, and on the other hand, length of proof. These seem to be in conflict with one another: if the conjecture is correct, then every arithmetic theorem has an elementally pure proof in the sense of inductive strength, but not necessarily in the sense of length of proof. Thus the conjecture, if true, would lead to an investigation of the length of proof of arithmetic theorems in EFA versus in inductively stronger arithmetic theories. This is precisely the sort of investigation to be carried out in this article for other theories, so the conjecture would simply necessitate a sequel to this article, rather than refuting its points.

3.3. **Conservativity.** Having argued that arithmetic and conceptual extensions of PRA are in general impure, we now turn to the question of their conservativity over PRA. Recall that a theory T_2 is *conservative* over a theory T_1 iff for every sentence φ in the language of T_1 that is provable in T_2, φ is also provable in T_1. Each of these extensions of PRA are conservative over PRA. The arithmetic extension $\mathrm{I}\Sigma_1$ is conservative over PRA for Π^0_2 sentences, as shown by Parsons (cf. [Par70]). Since RCA_0 and $\mathrm{I}\Sigma_1$ prove the same first-order sentences (cf. [Sim99], pp. 25, 369), it follows again from Parsons' result that RCA_0 is conservative over PRA for Π^0_2 sentences. Friedman observed that WKL_0 is conservative over PRA for Π^0_2 sentences, and Harrington has shown that WKL_0 is conservative over RCA_0 for Π^1_1 sentences, and hence for all arithmetical sentences (cf. [Sim99], pp. 369–372). Finally, Brown and Simpson have shown that WKL^+_0 is conservative over RCA_0 for Π^1_1 sentences (cf. [BS93]).

3.4. **Speed-up.** To compare the efficiency of proofs of theorems of PRA with proofs of these *same* theorems in conservative extensions of PRA, we consider the "speed-up" of proofs in extensions of PRA. Proof theorists measure the complexity of a system of proof by the "speed-up" that one system of proof offers over another. By calling a theory T_2 a "speed-up" of a theory T_1, we mean that all the theorems of T_1, perhaps restricted to those of a given type, have significantly more efficient proofs in T_2, measured in terms of length of proof.

with respect to the quantifier-free theorems of PRA will yield a *significant* gain of efficiency, but to the best of our knowledge this is still open.

Proof theorists distinguish between two types of speed-ups—*polynomial* and *super-polynomial*—the former being regarded as relatively insignificant, the latter as relatively significant. Suppose T_1, T_2 are two theories such that $T_2 \subset T_1$. We say that T_1 is at most a *polynomial speed-up* of T_2 when for every φ provable in T_2, the length of the shortest proof (measured in terms of total number of symbol occurrences) of φ in T_2 is less than some fixed polynomial multiple of the length of the shortest proof of φ in T_1. This notion can be relativized as follows. Let Φ be a set of formulas provable in T_2. We say that T_1 is at most a polynomial speed-up of T_2 *with respect to* Φ when for every $\varphi \in \Phi$, the length of the shortest proof of φ in T_2 is less than some fixed polynomial multiple of the length of the shortest proof of φ in T_1.[9]

Polynomial speed-up is distinguished from a particular type of non-polynomial speed-up called *roughly super-exponential speed-up*. This is speed-up by a function that grows much more rapidly than a polynomial function.[10] T_1 is said to have a *roughly super-exponential speed-up* over T_2 when for every φ provable in T_2, the length of the shortest proof in T_2 of φ is a "roughly super-exponential multiple" of the length of the shortest proof of φ in T_1. This notion can also be relativized as follows. For a set Φ of formulas provable in T_2, T_1 is a super-exponential speed-up of T_2 *with respect to* Φ when the lengths of the shortest T_2-proofs of the various φ_i in Φ are "roughly super-exponential multiples" of the shortest T_1-proofs of those same φ_i.[11]

[9]Polynomial speed-up may be more carefully defined as follows (cf. [CI05], pp. 4–5). Let the *length* $\ell(\pi)$ of a proof π be the number of symbol occurrences in π. For any formula φ, let $\pi^{<}_{T_i}(\varphi)$ be the *shortest proof* (in terms of number of symbol occurrences) of φ in T_i. We say that T_1 is *at most a polynomial speed-up of* T_2 with respect to Φ if there is a polynomial $p(x)$ with natural number coefficients such that for every φ provable in T_2

$$\ell(\pi^{<}_{T_2}(\varphi)) < p(\ell(\pi^{<}_{T_1}(\varphi))).$$

[10]This can be defined precisely as follows. Firstly, a function $f(x)$ *eventually dominates* a function $g(x)$ if there is an m such that for all $n > m$, $f(n) \geq g(n)$. Secondly, let 2^x_m be the function defined by: $2^n_0 = n, 2^n_{m+1} = 2^{2^n_m}$. For example, $2^n_1 = 2^{2^n_0} = 2^n$, $2^n_2 = 2^{2^n_1} = 2^{2^n}$, $2^n_3 = 2^{2^n_2} = 2^{2^{2^n}}$, and so on. A function $f(x)$ has *Kalmar elementary growth rate* if there is an m such that 2^x_m eventually dominates $f(x)$. It turns out that 2^x_x is the first function that dominates all Kalmar elementary functions. A function $f(x)$ has *roughly super-exponential growth rate* if and only if (i) it does not have Kalmar elementary growth rate, but (ii) there is a polynomial $p(x)$ with natural number coefficients such that $p(2^x_x)$ eventually dominates it.

[11]Roughly super-exponential speed-up may be more carefully defined as follows (cf. [CI05], pp. 4–5). T_1 has *roughly super-exponential speed-up over* T_2 if and only if

(1) there is no function $f(x)$ with Kalmar elementary growth rate such that for every φ provable in T_2, $\ell(\pi^{<}_{T_2}(\varphi)) < f(\ell(\pi^{<}_{T_1}(\varphi)))$; and
(2) there is a function $g(x)$ with roughly super-exponential growth rate such that for every φ provable in T_2, $\ell(\pi^{<}_{T_2}(\varphi)) < g(\ell(\pi^{<}_{T_1}(\varphi)))$.

For Φ a set of formulas provable in T_2, T_1 has roughly super-exponential speed-up over T_2 *with respect to* Φ if and only if there is a sequence $\{\varphi_i : i \in \omega\}$ of formulas from Φ such that

(1) there is no function $f(x)$ with Kalmar elementary growth rate such that for every $\varphi_n \in \Phi$, $\ell(\pi^{<}_{T_2}(\varphi_n)) < f(\ell(\pi^{<}_{T_1}(\varphi_n)))$; and
(2) there is a function $g(x)$ with roughly super-exponential growth rate such that for every $\varphi_n \in \Phi$, $\ell(\pi^{<}_{T_2}(\varphi_n)) < g(\ell(\pi^{<}_{T_1}(\varphi_n)))$.

This distinction between types of speed-ups is important because, as we said earlier, polynomial speed-up is generally regarded as relatively insignificant, while super-exponential speed-up is regarded as relatively significant. The case for the significance of polynomial-time computability as a measure of efficiency seems to have been first made by Edmonds in [Edm65], and was quickly adopted as the standard view in computer science and proof theory (cf. [FH03] and [Dea15], §2.2). Edmonds writes that its significance is clear in practice; he cites the graph-theoretic work of organic chemists as a case where polynomial-time complexity is obviously superior to super-polynomial-time complexity (p. 451). Similarly, Parikh writes of "feasible" proofs and proofs of "reasonable length" as being intuitive notions that he identifies with non-super-polynomial complexity, appealing to "common sense" (cf. [Par71], p. 494). We follow this practice here.

3.5. **The evidence.** The following is known regarding speed-up with respect to the theories we have considered.

(1) $I\Sigma_1$ has a roughly super-exponential speed-up over PRA with respect to the Π^0_1 theorems of PRA. This was shown by Ignjatović [CI05].
(2) RCA_0 has at most a polynomial speed-up over $I\Sigma_1$ with respect to first-order arithmetical formulas. This is folklore, following from the existence of the "canonical interpretation" of RCA_0 into $I\Sigma_1$ that we gave earlier.
(3) WKL_0 has at most a polynomial speed-up over RCA_0 with respect to Π^1_1 sentences, and hence for first-order arithmetical formulas. This was shown by Hájek [Háj93] and, by other means, Avigad [Avi96].
(4) WKL_0^+ has at most a polynomial speed-up over WKL_0 with respect to Π^1_1 sentences, and hence for first-order arithmetical formulas. This was shown by Avigad [Avi96].

Thus the arithmetic extension $I\Sigma_1$ has significant speed-up over PRA, but the conceptual extensions RCA_0, WKL_0 and WKL_0^+ do not yield further significant speed-up.

It is reasonable to wonder whether, as we move further up this chain of theories from RCA_0 through WKL_0^+ and beyond, we will find another conceptual extension of PRA that yields a significant speed-up. Yokoyama has proved that there is a maximal such conceptual extension of RCA_0 (cf. [Yok10]), though his proof does not yield the identity of this theory, only its existence[12] ; and has conjectured that no such conceptual extension of RCA_0 offers more than polynomial speed-up. By "such" a conceptual extension of RCA_0, and by "this chain of theories", we mean Π^1_2-axiomatizable theories, like WKL_0 and WKL_0^+.[13] By a "maximal" such theory,

[12]He suggests as a possibility WKL_0^+ + COH, where COH asserts the existence of a cohesive set, having shown that WKL_0^+ + COH is a Π^1_2-axiomatizable Π^1_1-conservative extension of RCA_0 (Corollary 2.5).

[13]That WKL_0 and WKL_0^+ are Π^1_2-axiomatizable can be seen by inspecting the logical form of their axioms. That they are *not* Π^1_1-axiomatizable follows, respectively, from Harrington's result that WKL_0 is Π^1_1-conservative over RCA_0 and from Brown and Simpson's result that WKL_0^+ is Π^1_1-conservative over RCA_0. To see why for the case of WKL_0, note that we can write WKL_0 as $RCA_0 + \varphi$. If WKL_0 were Π^1_1-axiomatizable, then there would be a

we mean a theory that logically implies any other Π^1_2-axiomatizable Π^1_1-conservative extension of RCA_0. At present, all our known methods of producing conservative extensions of RCA_0 rely on the Π^1_2-axiomatizability of the extension. Unless new methods of finding conservative extensions of RCA_0 were to be located, a positive answer to Yokoyama's conjecture would indicate that no other conceptual extension of PRA should be expected to yield significant gains in efficiency of proof length.

3.6. **Evaluating the evidence.** What, if anything, do these findings mean concerning the relative advantages of pure and impure proof? The only clear message is that they do *not* provide evidence of a general pattern of improvement in efficiency in moving from pure to impure proof. The move from $\mathrm{I}\Sigma_1$ to RCA_0, for example, is a move in the direction of topical impurity, we have argued. It does not correspond, however, to significant shortenings of proofs.

This is neither to deny nor to ignore $\mathrm{I}\Sigma_1$'s roughly super-exponential speed-up over PRA. Rather, it is to say, firstly, that the impurity of proofs in $\mathrm{I}\Sigma_1$ of theorems of PRA is a matter of elemental impurity rather than topical impurity; and secondly, that it does not imply a *general pattern* of speed-up in moving from pure to impure proof.

Furthermore, one may reasonably question the relevance of these formal results to the types of gains of simplicity described by MacLaurin, d'Alembert and Painlevé, as discussed in Section 2. No one has ever said, "Proving things in PRA is hard, but is made so much easier by working in $\mathrm{I}\Sigma_1$." But the claims about purity and simplicity from mathematical practice do make claims like this. Thus, whatever kinds of gains in simplicity may be afforded by moving from purity to impurity, the speed-up of proofs in $\mathrm{I}\Sigma_1$ for theorems of PRA does not seem to shed light on those gains.

4. Conclusions

Length of proof is a familiar measure of simplicity in proof theory, though one must be sensitive to what exactly this measure *is not* measuring. As has been frequently observed, proof length is a crude and possibly misleading measure of proof complexity. For instance, Potter has pointed out that proof length is highly dependent on choices of means of expression (cf. [Pot04], pp. 234–236). He notes a recent result showing that the term expressing the cardinal number 1 in Bourbaki's 1954 formal system has approximately 10^{12} characters, when fully expanded; and that when in the fourth edition of the same book ordered pairs (a, b) are defined in Kuratowski's way as $\{\{a\}, \{a, b\}\}$, instead of taken as a primitive as in the earlier editions, the term for 1 has approximately 10^{54} characters (cf. [Mat02]). Intuitively, the introduction

Π^1_1 theory T such that T is equivalent to WKL_0. Since RCA_0 is finitely axiomatizable, $\mathrm{RCA}_0 + \varphi$ is equivalent to a single sentence that, by compactness, is provable in a finite subtheory of T that can be conjoined into a single sentence ψ. Hence RCA_0 proves the equivalence of ψ and φ. Since WKL_0 proves ψ, it follows by Harrington's conservation result that RCA_0 proves ψ, and thus that RCA_0 proves φ, contradicting the fact that WKL_0 is properly stronger than RCA_0. For WKL^+_0 the argument is similar, using Brown and Simpson's result instead.

of a single instance of an ordered pair should not make a proof significantly more complex, but this result suggests that it may. As a result Potter councils caution in using proof length as a measure of proof complexity. He recommends using, in addition to length, "elegance and perspicuity" to judge the improvement in complexity of a proof using higher-order methods, noting that these "are of course much less objective than mere length and hence less amenable to formal study."

Avigad remarks, similarly:

> [L]ength has something to do with explaining how infinitary methods can make a proof simpler and more comprehensible. But the advantages of working in a conservative extension seem to have as much to do with the perspicuity and naturality of the notions involved, and using the number of symbols in an uninterpreted derivation as the sole measure of complexity is unlikely to provide useful insight. (cf. [Avi03], p. 276n18)

Relevant to this is Caldon and Ignjatović's suggestion that moving up the chain of theories we have been discussing, from PRA through RCA_0 to WKL_0 and WKL_0^+, may result in what he calls "conceptual speed-up". That is, it may produce proofs that are generally clearer and easier to grasp than those of their predecessors. If this were correct (and though it may be plausible, Caldon and Ignjatović provide no reason to think it is), then this hierarchy of theories would be a reasonable basis for a formal investigation of perspicuity in mathematical proof. On the other hand, proofs in these formal systems are not necessarily all that simple. As Simpson has remarked (cf. [Sim88], p. 361), proofs in WKL_0, or WKL_0^+ are "sometimes much more complicated than the standard proof."

Avigad also stresses a different but closely related matter. In [Avi03] he notes that a great deal of mathematics can be formalized in the theories $\mathrm{I}\Sigma_1$, PRA, RCA_0, etc. that we have been discussing, as well as in yet weaker theories. Avigad notes that Takeuti was able to formalize enough complex analysis in a conservative extension of PA to permit the formalization of the complex-analytic proofs of the prime number theorem of Hadamard and de la Vallée Poussin. Indeed it was later shown that $\mathrm{I}\Sigma_1$ suffices for this (cf. [Sud01]). Also, Cornaros and Dimitracopoulos were able to formalize Selberg's "elementary" proof in a subtheory of $\mathrm{I}\Sigma_1$ (cf. [CD94]).

Yet, as Avigad notes, both the classical and the elementary proofs are formalizable in the same weak theory, $\mathrm{I}\Sigma_1$. This indicates, he suggests, that whatever difference in complexity there is between the two proofs is not detectable merely by determining how much logical strength is needed to prove it. As he puts it (p. 274), "it is a mistake to confuse mathematical difficulty with logical strength; in other words…there is a difference between saying that a proof is hard, and saying that it requires strong axioms."

We agree with this point, though it runs somewhat orthogonally to our narrative in this paper. Our formal investigation has centered on the gains of general proof efficiency, measured in terms of length, in moving from logically weaker to stronger formal theories of arithmetic. Avigad's point is that the weaker/stronger distinction does not map very well onto the pure/impure distinction as realized in ordinary mathematics. We agree, but our goal in this paper has been to see how far we can get in our investigation of purity and complexity using just the means available in proof theory as it presently exists. Hence, we have considered various set-theoretic extensions of PRA that can be viewed as having added some additional impurity, and tried to say to what extent that additional impurity purchases a gain of simplicity. Our conclusion has been that there is no *general* gain in simplicity purchased by this move, at least for simplicity measured in terms of proof length.

Returning, finally, to the issues raised in Section 2, our conclusion concerns only what we have called Thesis 1, that impure proofs are generally simpler to *verify* than pure proofs of the same statement. The results from proof theory discussed here do not bear on Thesis 2, that impure proofs are generally simpler to *discover* than pure proofs of the same statement. Thesis 2 may seem to be more pertinent to understanding mathematical practice than Thesis 1; it is arguably a better expression of the types of gains of simplicity described earlier by MacLaurin, d'Alembert and Painlevé. We agree with this point. Proof theory is a flawed measure of proof complexity, particularly so for analyzing proofs in mathematical practice. However, at the moment it is the best we have, and these results at least give us *some* data for philosophical reflexion. A measure of *inventional simplicity* would be great to have, in order to analyze more fully the simplicity of impurity in practice, but at the moment we do not have such a measure. Thus, the results of this article are but a start, and we hope they may stimulate further work.

References

[AM12] Andrew Arana and Paolo Mancosu. On the relationship between plane and solid geometry. *Review of Symbolic Logic*, 5(2):294–353, June 2012.

[Ara08] Andrew Arana. Logical and semantic purity. *Protosociology*, 25:36–48, 2008. Reprinted in *Philosophy of Mathematics: Set Theory, Measuring Theories, and Nominalism*, Gerhard Preyer and Georg Peter (eds.), Ontos, 2008.

[Ara14] Andrew Arana. Purity in arithmetic: Some formal and informal issues. In Godehard Link, editor, *Formalism and Beyond. On the Nature of Mathematical Discourse*, pages 315–335. de Gryuter, Boston, 2014.

[Ara16] Andrew Arana. Imagination in mathematics. In Amy Kind, editor, *The Routledge Handbook of Philosophy of Imagination*, chapter 34, pages 463–477. Routledge, London and New York, 2016.

[Arang] Andrew Arana. Elementarity and purity. In Andrew Arana and Carlos Alvarez, editors, *Analytic Philosophy and the Foundations of Mathematics*. Palgrave/Macmillan, Forthcoming.

[Avi96] Jeremy Avigad. Formalizing forcing arguments in subsystems of second-order arithmetic. *Annals of Pure and Applied Logic*, 82:165–191, 1996.

[Avi03] Jeremy Avigad. Number theory and elementary arithmetic. *Philosophia Mathematica*, 11:257–284, 2003.

[Avi06] Jeremy Avigad. Mathematical method and proof. *Synthese*, 153(1):105–159, 2006.

[BS93] Douglas K. Brown and Stephen G. Simpson. The Baire category theorem in weak subsystems of second-order arithmetic. *Journal of Symbolic Logic*, 58(2):557–578, 1993.

[CD94] Charalampos Cornaros and Costas Dimitracopoulos. The prime number theorem and fragments of PA. *Archive for Mathematical Logic*, 33(4):265–281, 1994.

[CI05] Patrick Caldon and Aleksandar Ignjatovic. On mathematical instrumentalism. *Journal of Symbolic Logic*, 70(3):778–794, 2005.

[d'A51] Jean Le Rond d'Alembert. Application de l'algebre ou de l'analyse à la géométrie. In Denis Diderot and Jean Le Rond d'Alembert, editors, *Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers*, volume 1. Briasson, David, Le Breton, and Durand, Paris, 1751.

[DA11] Michael Detlefsen and Andrew Arana. Purity of methods. *Philosophers' Imprint*, 11(2):1–20, January 2011.

[Dea15] Walter Dean. Computational Complexity Theory. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Fall 2015 edition, 2015.

[Des37] René Descartes. La géométrie. In *Discours de la méthode pour bien conduire sa raison et chercher la vérité dans les sciences*, pages 297–413. Jan Maire, Leiden, 1637.

[Det90] Michael Detlefsen. On an alleged refutation of Hilbert's program using Gödel's first incompleteness theorem. *Journal of Philosophical Logic*, 19(4):343–377, November 1990.

[Det96] Michael Detlefsen. Philosophy of mathematics in the twentieth century. In *Philosophy of Science, Logic, and Mathematics*, volume 9 of *Routledge History of Philosophy*, pages 50–123. Routledge, London and New York, 1996. Edited by Stuart G. Shanker.

[dlVP96] Charles de la Vallée Poussin. Recherches analytiques sur la théorie des nombres premiers. *Ann. Soc. Sci. Bruxelles*, 20:183–256, 1896. Reprinted in Collected Works Volume 1, edited by P. Butzer, J. Mawhin, and P. Vetro, Académie Royale de Belgique and Circolo Matematico di Palermo, 2000.

[Edm65] Jack Edmonds. Paths, trees, and flowers. *Canadian Journal of Mathematics*, 17:449–467, 1965.

[Erd49] Paul Erdős. On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proceedings of the National Academy of Sciences, USA*, 35:374–384, 1949.

[FH03] Lance Fortnow and Steve Homer. A short history of computational complexity. *Bull. Eur. Assoc. Theor. Comput. Sci.*, 80:95–133, 2003.

[FP11] Giovanni Ferraro and Marco Panza. Lagrange's theory of analytical functions and his ideal of purity of method. *Archive for History of Exact Sciences*, 65(4), 2011.

[Fri76] Harvey M. Friedman. Systems of second order arithmetic with restricted induction. I. *Journal of Symbolic Logic*, 41(2):557–8, June 1976.

[Gra08] Andrew Granville. Analytic Number Theory. In Timothy Gowers, June Barrow-Green, and Imre Leader, editors, *The Princeton Companion to Mathematics*. Princeton University Press, Princeton, 2008.

[Gui09] Niccolò Guicciardini. *Isaac Newton on Mathematical Certainty and Method*. MIT Press, Cambridge, MA, 2009.

[Had96] Jacques Hadamard. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France*, 24:199–220, 1896.

[Had45] Jacques Hadamard. *The Psychology of Invention in the Mathematical Field*. Princeton University Press, Princeton, 1945.

[Háj93] Petr Hájek. Interpretability and fragments of arithmetic. In Peter Clote and Jan Krajícek, editors, *Arithmetic, proof theory, and computational complexity*, pages 185–196. Oxford University Press, 1993.

[Hal08] Michael Hallett. Reflections on the purity of method in Hilbert's *Grundlagen der Geometrie*. In Paolo Mancosu, editor, *The Philosophy of Mathematical Practice*, pages 198–255. Oxford University Press, 2008.

[Hil99] David Hilbert. *Grundlagen der Geometrie*. B.G. Teubner, Leipzig, 1899.

[Hil25] David Hilbert. On the infinite. In Jean van Heijenoort, editor, *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931*, pages 369–392. Harvard University Press, 1925.

[Höl92] Otto Hölder. Über den Casus Irreducibilis bei der Gleichung dritten Grades. *Mathematische Annalen.*, 38:307–312, 1892.

[HW01] Bob Hale and Crispin Wright. *The Reason's Proper Study: Essays towards a Neo-Fregean Philosophy of Mathematics*. Clarendon Press, Oxford, 2001.

[Ign90] Aleksandar Ignjatovic. *Fragments of First and Second Order Arithmetic and Length of Proofs*. PhD thesis, University of California, Berkeley, 1990.

[Jor15] Palle Jorgensen. Source of Jacques Hadamard quote. http://www.cs.uiowa.edu/~ jorgen/hadamardquotesource.html, December 2015.

[Kay91] Richard Kaye. *Models of Peano Arithmetic*. Oxford University Press, Oxford, 1991.

[Kle53] Felix Klein. *Elementary Mathematics from an Advanced Standpoint. Geometry*. Dover, New York, 1953. Translated from the third German edition by E. R. Hedrick and C. A. Noble, Macmillan, New York, 1939.

[Kre80] Georg Kreisel. Kurt Gödel. *Biographical Memoirs of Fellows of the Royal Society*, 26:149–224, 1980.

[Lag76] Joseph-Louis Lagrange. Leçons sur mathematiques elementaires. In *Oeuvres de Lagrange*, volume VII. Gauthier-Villars, Paris, 1876. Edited by Joseph-Alfred Serret.

[Mac42] Colin MacLaurin. *A Treatise of Fluxions*. Ruddimans, 1742.

[Mar10] Sébastien Maronne. Pascal versus Descartes on geometrical problem solving and the Sluse-Pascal correspondence. *Early Science and Medicine*, 15:537–565, 2010.

[Mat02] A.R.D. Mathias. A term of length 4,523,659,424,929. *Synthese*, pages 75–86, 2002.

[McL10] Colin McLarty. What Does It Take To Prove Fermat's Last Theorem? Grothendieck and the Logic of Number Theory. *The Bulletin of Symbolic Logic*, 16(3):359–377, 2010.

[New20] Isaac Newton. *Universal arithmetick*. J. Senex, W. Taylor, T. Warner, and J. Osborn, London, 1720. Reprinted in *The mathematical works of Isaac Newton*, Vol. II. Edited by Derek T. Whiteside, Johnson Reprint Corp., New York, 1967.

[New71] Isaac Newton. Geometria curvilinea. In D.T. Whiteside, editor, *The Mathematical Papers of Isaac Newton. Vol. IV: 1664–1666*, pages 420–484. Cambridge University Press, Cambridge, 1971.

[Pai72] Paul Painlevé. Analyse des travaux scientifiques. In *Oeuvres de Paul Painlevé*, volume 1. CNRS, 1972. Originally published by Gauthier-Villars, 1900.

[Par70] Charles Parsons. On a number-theoretic choice scheme and its relation to induction. In A. Kino, J. Myhill, and R.E. Vesley, editors, *Intuitionism and Proof Theory*, pages 459–473. North-Holland, 1970.

[Par71] Rohit Parikh. Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494–508, 1971.

[Pot04] Michael Potter. *Set theory and its philosophy*. Oxford University Press, New York, 2004.

[Pyc97] Helena M. Pycior. *Symbols, impossible numbers, and geometric entanglements*. Cambridge University Press, Cambridge, 1997.

[Rid82] Robin E. Rider. *A Bibliography of Early Modern Algebra, 1500–1800*, volume VII of *Berkeley Papers in History of Science*. Office for History of Science and Technology, University of California, Berkeley, 1982.

[Sel49] Atle Selberg. An elementary proof of the prime-number theorem. *Annals of Mathematics*, 50:305–313, 1949.

[Sim88] Stephen G. Simpson. Partial realizations of Hilbert's Program. *The Journal of Symbolic Logic*, 53(2):349–363, 1988.

[Sim99] Stephen G. Simpson. *Subsystems of Second Order Arithmetic*. Perspectives in Mathematical Logic. Springer, 1999.

[Sud01] Olivier Sudac. The prime number theorem is PRA-provable. *Theoretical Computer Science*, 257:185–239, 2001.

[Tai81] William W. Tait. Finitism. *The Journal of Philosophy*, 78(9):524–546, 1981.

[Wri99] Crispin Wright. Is Hume's Principle Analytic? *Notre Dame Journal of Formal Logic*, 40(1):6–30, 1999.

[Yok10] Keita Yokoyama. On Π^1_1 conservativity for Π^1_2 theories in second order arithmetic. In Toshiyasu Arai and et. al., editors, *Proceedings of the 10th Asian logic conference, Kobe, Japan, September 1–6, 2008*, pages 375–386, Hackensack, NJ, 2010. World Scientific.

U.F.R. de philosophie, Université Paris 1 Panthéon-Sorbonne, and IHPST, 13 rue de Four, 75006 Paris, France

E-mail address: andrew.arana@univ-paris1.fr