Logique & Analyse **179–180** (2002), 373–388

WHAT DO MATHEMATICIANS WANT? PROBABILISTIC PROOFS AND THE EPISTEMIC GOALS OF MATHEMATICIANS

DON FALLIS

Abstract
Several philosophers have used the framework of means/ends reasoning to explain the methodological choices made by scientists and mathematicians (see, e.g., Goldman 1999, Levi 1962, Maddy 1997). In particular, they have tried to identify the epistemic objectives of scientists and mathematicians that will explain these choices. In this paper, the framework of means/ends reasoning is used to study an important methodological choice made by mathematicians. Namely, mathematicians will only use *deductive proofs* to establish the truth of mathematical claims. In this paper, I argue that none of the epistemic objectives of mathematicians that are currently on the table provide a satisfactory explanation of this rejection of probabilistic proofs.

1. *Introduction*

People have objectives that they want to achieve — students want to pass their exams and athletes want to win their races. In order to achieve their objectives, people engage in activities that they believe to be means to achieving those objectives — students study and athletes train. These are examples of people engaging in *means/ends reasoning*.

Unfortunately, in most cases, we cannot directly observe the objectives that other people have.[1] We can only observe the activities that they engage in. As a result, we are sometimes left wondering *why* people choose to engage in the activities that they do. For example, we might wonder why a particular person chooses to spend so much time studying or training. In order to explain why people choose to engage in the activities that they do,

[1] In fact, people (including mathematicians) may not always have a clear idea of what their *own* objectives are (see Maddy 1997, 197–198).

we have to identify the objectives (e.g., passing the exam or winning the race) that they want to achieve.

Several philosophers have used this framework of means/ends reasoning to explain the methodological choices made by scientists and mathematicians. That is, they have tried to identify the objectives that lead scientists and mathematicians to make these choices. For example, Isaac Levi (1962) and Alvin Goldman (1999) have tried to show that the epistemic objectives of acquiring true beliefs and avoiding error can be used to explain many of the methodological choices of scientists.[2] Penelope Maddy (1997) has tried to identify the epistemic objectives that explain why mathematicians have adopted particular set theoretic axioms (e.g., the axiom of choice).

In this paper, I use the framework of means/ends reasoning to study the definitive methodological choice made by mathematicians. Namely, mathematicians will only use *deductive proofs* to establish the truth of mathematical claims. This particular methodological choice is in line with the standard preference (e.g., among philosophers such as Descartes) for deductive arguments over inductive arguments. Thus, an explanation of why mathematicians reject *probabilistic proofs* should help to explain why deductive arguments are considered superior to inductive arguments.

The project of this paper is to identify epistemic objectives that will explain this rejection of probabilistic proofs. Along the way, I identify several important epistemic objectives of mathematicians. Also, I defend using the framework of means/ends reasoning to explain the methodological choices of mathematicians. However, I conclude that none of the epistemic objectives of mathematicians that are currently on the table provide a satisfactory explanation of this rejection of probabilistic proofs. Thus, there may not be a good epistemic reason for this methodological choice.

2. *Deductive Proofs and Probabilistic Proofs*

Mathematicians only use *deductive proofs* to establish the truth of mathematical claims. A deductive proof of a mathematical claim is a procedure which, if carried out correctly, insures that the claim is true.[3] By contrast, a probabilistic proof of a mathematical claim is a procedure which, even if carried

[2] K. Brad Wray (2002, 155) uses this framework to explain why scientists engage in *collaborative research*.

[3] Strictly speaking, a deductive proof of a mathematical claim only insures that this claim is a logical consequence of some other mathematical claims (e.g., the axioms of set theory). However, for the sake of simplicity, I will ignore this complication.

out correctly, does not insure that the claim is true. Even so, a probabilistic proof can provide very good evidence that the claim is true.

Despite the reliability of certain probabilistic proofs, mathematicians will not use them to establish that mathematical claims are true. For example, according to the mathematician David Harel (1989, 295), "as long as we use probabilistic algorithms only for petty, down-to-earth matters such as wealth, health, and survival, we can easily make do with very-likely-to-be-correct answers to our questions. The same, it seems, cannot be said for our quest for absolute mathematical truth."

Of course, as a number of philosophers have argued, deductive proof is not the only way to acquire mathematical knowledge (see, e.g., Steiner 1975, 102–106, Coady 1992, 249–261, Folina 1999, 428).[4] In fact, mathematicians do accept that mathematical claims are likely to be true on the basis of inductive evidence, testimony, picture proofs, etc.[5] However, they do not use any of these methods to definitively *establish* that a mathematical claim is true. For example, as Mark Steiner (1975, 93) himself points out, "journals of mathematics will not publish anything less than a proof of a scholarly result."

According to David Sherry (1997, 405), mathematicians distinguish "demonstrative from heuristic reasoning and require demonstrative reasoning for a finished piece of mathematics." This distinction is analogous to that commonly made in medieval courts (see Laudan 2001, 282). Circumstantial evidence (e.g., blood on the clothes of the accused) could be used to determine who is likely to be guilty. However, only the testimony of two eyewitnesses or a confession counted as "full proof of guilt." Such full proof of guilt was required in order to convict an individual of a capital crime. Similarly, according to mathematicians, deductive proof is needed in order to establish the truth of a mathematical claim. Probabilistic proof is not sufficient.

Finally, it should be noted that mathematicians have been making this same methodological choice for centuries.[6] For example, according to the eighteenth-century mathematician Leonhard Euler, "we should take great

[4] Some philosophers do disagree. Bernard Williams (1972, 9), for example, claims that "access to mathematical truth must necessarily lie through proof, and that therefore the notion of non-accidental true belief in mathematics essentially involves the notion of mathematical proof."

[5] There are circumstances (e.g., when establishing that a computer program does what it is supposed to) where inductive evidence is actually preferred to deductive proof (cf. De Millo et al. 1979). In fact, Donald Knuth (1999) famously wrote "beware of bugs in the above code; I have only proved it correct, not tried it."

[6] In the past, mathematicians initially rejected many other methods — such as non-constructive proofs, proofs that appeal to the axiom of choice, and computer proofs — of

care not to accept as true such properties of the numbers which we have discovered by observation and which are supported by induction alone" (quoted in Polya 1954, 3).

3. *Explaining the Rejection of Probabilistic Proofs*

In the framework of means/ends reasoning, there are three possible explanations for why a person (or a group of people) might refuse to engage in a particular activity (e.g., using a probabilistic proof to establish that a mathematical claim is true). First, the activity might not be a means to achieving her objectives.[7] Second, she might not recognize that the activity is a means to achieving her objectives. Third, she might not be rational.

Any of these three options might explain why mathematicians will not use probabilistic proofs to establish that mathematical claims are true. However, the second and third options would — for obvious reasons — be somewhat unsatisfying explanations. It would certainly be preferable to show that probabilistic proofs are simply not a means to the objectives of mathematicians.

Most mathematicians (and philosophers) certainly believe that probabilistic proofs are not a means to the objectives of mathematicians. For example, according to the mathematician Carl Pomerance (1982, 142), there is "a qualitative difference between probabilistic verification and mathematical proof that is important to mathematicians." However, Don Fallis (1997) and Catherine Womack and Martin Farach (2003) have argued that there is no such difference. And, unless there is such a difference, it is difficult to see how deductive proofs could be a means to the objectives of mathematicians while probabilistic proofs are not.

It should be noted, however, that there are actually many possible objectives that might lead mathematicians not to use probabilistic proofs. For example, they might consider deductive proofs more *aesthetically pleasing* than probabilistic proofs. Also, they might only be able to get NSF funding for their research if they use deductive proofs. However, the project of this paper is to determine, in particular, if there are any *epistemic* objectives of mathematicians that will explain the rejection of probabilistic proofs.

Admittedly, there are a few mathematicians who think that probabilistic proofs should be used to establish the truth of mathematical claims (see, e.g.,

establishing that a mathematical claim is true. However, mathematicians now commonly use these methods (cf. Hersh 1997, 54–56).

[7] That is, it might not be a means to achieving her objectives *all things considered*. For example, taking performance enhancing drugs is a means to winning the race. But it may not be a means to achieving an athlete's objectives because she may also want to compete fairly.

Zeilberger 1993, Hersh 1997, 59, Chaitin 1982, 942). These mathematicians point out that it is just not possible to establish the truth of many mathematical claims unless we are willing to use probabilistic proofs.[8] This is because any deductive proof of certain mathematical claims would be far too long for any human being (or computer) to produce whereas a probabilistic proof of the same claim would be considerably shorter.

Zeilberger, Hersh, and Chaitin, however, are clearly arguing that mathematicians should change their practice.[9] But the project of this paper is to identify epistemic objectives that will explain the current practice of rejecting probabilistic proofs. Along the lines suggested by Hilary Kornblith (1999, 166), "what we need to do is look at the knowledge gathering enterprise and see what goals are embedded in it, what goals make sense of [mathematicians' actual] practice."

4. *Probabilistic Proofs of Primality*

In order to focus the discussion, this paper will look at why mathematicians refuse to use probabilistic proofs to establish the truth of a particular type of mathematical claim: viz., that a number is *prime*. Admittedly, the fact that a particular number is prime is not a terribly exciting mathematical claim.[10] Even so, it is a legitimate mathematical claim. For example, mathematicians keep track of the largest numbers whose primality has been established (see, e.g., Ribenboim 1996, 158).[11] Of course, in order for a number to get on this list of largest known primes, its primality must be established with a deductive proof (see, e.g., Pomerance 1982).

There are a number of procedures that yield deductive proofs of primality (see, e.g., Pomerance 1981, Ribenboim 1996, 19–178). For example, we can try dividing n by all of the numbers less than or equal to $\sqrt{n}$. If none of these numbers divide evenly into n, we conclude that n is prime. I will refer to

[8] The argument is reminiscent of William James' (1979, 31–32) claim that "a rule of thinking which would absolutely prevent me from acknowledging certain kinds of truth if those kinds of truth were really there, would be an irrational rule."

[9] It is not completely clear whether Zeilberger, Hersh, and Chaitin think that this change in practice should occur simply because mathematicians have not realized that probabilistic proofs are a means to their epistemic objectives or because mathematicians currently have the wrong epistemic objectives.

[10] It is not even a claim about an *infinite* number of cases.

[11] See http://www.utm.edu/research/primes/largest.html for the latest news on large primes.

this particular procedure as the *trial division test*. If this procedure is carried out correctly, n must be prime.

There are also a number of procedures that yield probabilistic proofs of primality. For example, Michael Rabin (1980) developed the following procedure: We pick a whole bunch of numbers less than n at random and test to see if any of them are *witnesses to the compositeness of* n.[12] A witness to the compositeness of n is a number that has a special property that implies that n is *composite* (i.e., that n is not prime). This property can be tested for very quickly. Also, if n is composite, then over three-quarters of the numbers less than n have this property. Thus, if none of the numbers that we test are witnesses, we conclude that n is prime. I will refer to this particular procedure as the *Rabin test*. Even if this procedure is carried out correctly, n might not be prime. In particular, we might have gotten very unlucky and missed all the witnesses when we picked numbers at random. However, if this procedure is carried out correctly, the overwhelming odds are that n is prime.[13]

I have claimed that mathematicians will not use probabilistic proofs to *establish* that a number is prime. However, mathematicians are willing to use probabilistic proofs of primality for other purposes. Mathematicians do recognize that a number is very likely to be prime if there is a probabilistic proof of its primality. As a result, they are happy to use such *probable primes* for practical applications that require prime numbers (e.g., secure encryption schemes, see Rivest et al. 1978). In addition, probabilistic proofs can be used to identify likely candidates whose primality can then be established using deductive proofs.[14]

[12] Robert Solovay and V. Strassen (1977) developed a similar procedure that differs only with respect to the precise definition of a witness.

[13] Another inductive procedure for identifying prime numbers uses the fact that certain species such as cicadas always reappear after a prime number of years (see Markus and Goles 2002). Additionally, it is not yet known how certain autistic savants are able to quickly identify large primes. However, given their inability to perform simple arithmetic calculations, it seems unlikely that their procedure is purely deductive (cf. Welling 1994, 203–205).

[14] Analogously, circumstantial evidence in medieval courts was used to determine who should be investigated and tried. George Polya (1954) has famously promoted this kind of use of inductive evidence in mathematics. Even so, Polya (1954, 50) is careful to point out that "verification in many well-chosen instances may be very helpful as an encouragement, but can never prove a conjectural law in the mathematical sciences."

5. *Epistemic Objectives that Do Not Explain*

The two epistemic objectives most commonly discussed by epistemologists are *(a)* the objective of acquiring more true beliefs and *(b)* the objective of avoiding error (see, e.g., Levi 1962). Mathematicians certainly have both of these objectives. Unfortunately, that fact alone is not sufficient to explain their rejection of probabilistic proofs. After all, all scientists have both of these objectives. However, most scientists are happy to use inductive arguments in their inquiries.

Of course, mathematicians are different from other scientists with regard to the relative importance that they assign to these two epistemic objectives. As Levi (1962, 64) points out, there are "differences in the degrees of caution normally exercised in different [scientific] disciplines." In particular, the Harel quote above suggests that, for mathematicians, the objective of avoiding error trumps the objective of acquiring new true beliefs. In other words, mathematicians are much more (epistemically) risk averse in their inquiries than other scientists.

Unfortunately, their higher degree of caution is not sufficient to explain their rejection of probabilistic proofs (and only probabilistic proofs). As I will argue below, some probabilistic proofs of primality (e.g., the Rabin test) are more reliable than some deductive proofs of primality (e.g., the trial division test). Thus, even if mathematicians are extremely risk averse, they should still prefer using certain probabilistic proofs to using certain deductive proofs.

In order to see this, we need to look at the reasons why a mathematician might mistakenly conclude that a number is prime in both cases. First of all, even though they use only deductive proofs, mathematicians sometimes make mistakes.[15] As David Hume (1967, Book I, Part IV, Section I) has pointed out, "in all demonstrative sciences the rules are certain and infallible; but when we apply them, our fallible and uncertain faculties are very apt to depart from them, and fall into error." In the trial division test, for example, a mistake might be made when we test to see if a particular number divides evenly into n. A mathematician might mistakenly conclude that n is prime because of such a mistake.

Of course, probabilistic proofs are also subject to mistakes. In the Rabin test, for example, a mistake might be made when we test to see if a particular number is a witness to the compositeness of n. A mathematician might mistakenly conclude that n is prime because of such a mistake. However,

[15] The mathematician Philip Davis (1972, 260–262) has compiled an entertaining list of deductive proofs that have turned out to be incorrect. In fact, Davis (1972, 260) concludes that "the authenticity of a mathematical proof is not absolute, but only *probabilistic*" (emphasis added).

there is another reason why a mathematician might mistakenly conclude that a number is prime on the basis of the Rabin test. Even if the test is carried out correctly, n might not be prime. In particular, we might have gotten very unlucky and missed all the witnesses when we picked numbers at random.[16]

Even so, since the Rabin test requires significantly fewer calculations than the trial division test, the probability of making a mistake in a calculation is significantly smaller with the Rabin test. In addition, the probability of getting unlucky and missing all the witnesses can be made arbitrarily small simply by picking more numbers at random (and testing to see if any of them are witnesses). Thus, the *overall* probability of mistakenly concluding that n is prime on the basis of the Rabin test can be less than the overall probability of mistakenly concluding that n is prime on the basis of the trial division test (cf. Pomerance 1981, 100).[17]

It should be noted that this argument that the Rabin test is more reliable than the trial division test relies on the fact that the trial division test takes exponential time while the Rabin test takes only polynomial time. Interestingly, Agarwal et al. (2002) have just recently discovered the first polynomial time procedure that yields a deductive proof of primality.[18] It is possible that this procedure, unlike the trial division test, will always be more reliable than the Rabin test. However, even if this turns out to be the case, mathematicians' concern for reliability still cannot be used to explain their rejection of probabilistic proofs. Even if faster (and, thus, more reliable) procedures are available, as Pomerance (1981, 97) notes, the trial division test still provides a "proof of primality for prime n." Thus, an explanation of the rejection of probabilistic proofs must be consistent with the acceptability of the trial division test.[19]

So far, I have been discussing the reliability of the trial division test and the Rabin test when they are initially performed. However, mathematicians

[16] There is also a very slim chance that there is a mistake in Rabin's proof that over three-quarters of the numbers less than a composite n are witnesses to its compositeness.

[17] An important reason why deductive proofs are so reliable is that mathematicians are extensively trained in using deductive proofs to establish that mathematical claims are true. Probabilistic proofs might be less reliable *in actual practice* simply because mathematicians do not have nearly as much experience with using probabilistic proofs. However, this concern could presumably be eliminated by giving mathematicians appropriate training.

[18] Vaughan Pratt (1975) had already shown that it is always possible to deductively prove that a number is prime in polynomial time. However, until now, we were not always able to *find* the proof in polynomial time.

[19] This is so even if no one outside of elementary school ever uses the trial division test to establish that a number is prime (because it takes too long).

are not only concerned with getting to the truth right off the bat (cf. Azzouni 2000, 136). It might be suggested that the objective of avoiding errors *in the long run* explains the rejection of probabilistic proofs. After all, if we are worried that a mistake may have crept into a deductive proof, we know just what to do. We carefully survey the proof. By contrast, if we are worried that we have mistakenly concluded that a number is prime on the basis of the Rabin test, we have no proof to survey. We just know that several randomly chosen numbers are not witnesses.

Even so, it is not clear that we are really in a better position with regard to avoiding errors in the long run if we only use deductive proofs. First of all, if we are worried that a mistake may have crept into a deductive proof, there is no guarantee we will be able to find it. For example, Richard De Millo, Richard Lipton, and Alan Perlis (1979, 272) describe a case where two groups of topologists claimed to have proved results that turned out to be contradictory. In order to resolve the situation, both proofs were carefully surveyed, but mathematicians were not able to find a mistake in either proof. Also, even when mathematicians do find the mistake in a deductive proof, it can take a very long time (see, e.g., Davis 1972, 262, Anglin 1997, 87–88). For example, it took eleven years for mathematicians to discover the error in Kempe's "proof" of the four-color conjecture (see Sipka 2002, 21).

Furthermore, if we are worried that we have mistakenly concluded that a number is prime on the basis of the Rabin test, we do know what to do. We simply pick more numbers at random and test to see if any of them are witnesses. If the number really is composite, then — even though we got unlucky with the initial test — we are very likely to find a witness very quickly.

So far, I have been discussing the probability of mistakenly concluding that a single mathematical claim is true. However, mathematicians typically use mathematical results to derive further results. It might be suggested that this consideration explains the rejection of probabilistic proofs. As Ivars Peterson (1990, 15) notes, "mathematics is constructed like a giant house of cards: one theorem piled on top of another ... if one element were faulty, then the whole structure could come tumbling down." In fact, even if several results that are highly probable are used to derive a further result (e.g., their conjunction), this further result may not be highly probable. As a result, mathematicians might like to have a method of establishing that mathematical claims are true that provides absolute certainty. However, since deductive proofs do not provide absolute certainty either, it is not clear that this consideration explains the rejection of probabilistic proofs.[20]

[20] Of course, whether mathematicians use deductive proofs or probabilistic proofs, they can gather independent corroborating evidence to try to insure that things will not "come tumbling down." For example, the fact that no more finite simple groups have been discovered

Finally, as Michael Detlefsen and Mark Luker (1980, 819) note in their brief discussion of the Rabin test, "there may be reasons other than the desire for a high degree of certitude for restricting the methods of proof to purely deductive techniques." For example, mathematicians clearly prefer proofs that do not just establish that a mathematical claim is true, but that allow them to *understand why* this claim is true (see, e.g., Rota 1997). If mathematicians required that proofs provide understanding, this epistemic objective might explain the rejection of probabilistic proofs. After all, the Rabin test does not provide us with much understanding of why a number is prime.

However, many deductive proofs (e.g., the trial division test) do not provide us with much understanding of why the mathematical claim in question is true either. Understanding is an example (along with simplicity, clarity, beauty, fruitfulness, etc.) of something that is valuable to mathematicians, but it is not something that they require of a proof technique.[21] Thus, it is not an epistemic objective that will explain the rejection of probabilistic proofs.[22]

6. *Epistemic Objectives that Do Explain but that are Not Satisfying*

Even so, there are at least a few possible epistemic objectives of mathematicians that might explain the rejection of probabilistic proofs. Unfortunately, the available explanations are, for a variety of reasons, somewhat unsatisfying.

First, using deductive proofs might be something that is simply *intrinsically* valuable to mathematicians. After all, mathematics is, almost by definition, a deductive science (cf. Steiner 1975, 93, Tymoczko 1979, 63). Such an epistemic objective would clearly explain the rejection of probabilistic proofs. However, deductive proof simply being an end in itself is a somewhat unsatisfying explanation. We might have hoped that mathematicians restrict themselves to using deductive proofs because doing so is the most effective

since the proof of the classification theorem suggests that the proof is correct (cf. Peterson 1990, 280).

[21] W. S. Anglin (1997, 85–127) provides a fairly comprehensive list of mathematical values. However, all of these values arguably fall into this category.

[22] Fallis (1997) argues that several other epistemic objectives (e.g., having an a priori justification) also fail to explain the rejection of probabilistic proofs.

means to achieving some further epistemic objective (such as avoiding errors and finding errors that have already been made).[23]

Second, even though mathematicians will sometimes be mistaken about the truth of mathematical claims — even when they use deductive proofs, they might not want to be mistaken simply because they got unlucky (i.e., mistaken through no fault of their own). Since we might simply get unlucky if we choose to use probabilistic proofs, such an epistemic objective would explain the rejection of probabilistic proofs. However, it is not clear why it would be so important for mathematicians to avoid being mistaken for this particular reason. It is especially unclear given that the overall probability of being mistaken can be less if a mathematician uses a probabilistic proof such as the Rabin test.

Third, mathematicians might value using proof techniques that *in principle* (i.e., if they are carried out correctly) insure that they will not be mistaken about the truth of mathematical claims.[24] In practice, neither deductive proofs nor probabilistic proofs provide a guarantee that mathematicians will not be mistaken. However, in principle, deductive proofs, unlike probabilistic proofs, do guarantee that mathematicians will not be mistaken about the truth of mathematical claims. Thus, such an epistemic objective would explain the rejection of probabilistic proofs. However, we would have hoped that mathematicians use deductive proofs exclusively because of some *actual* epistemic benefit that they derive.

Fourth, mathematicians might only want to use proof techniques that are widely applicable. For example, deductive proofs can be used to (reliably) establish the truth of facts in all areas of mathematics. By contrast, most of the probabilistic proof techniques *that are known to be reliable* can only be used to establish the truth of simple combinatorial facts (e.g., that a number is prime).[25] Thus, such an epistemic objective would explain the rejection of probabilistic proofs. However, it is not clear why mathematicians should refuse to use probabilistic proofs in those areas of mathematics where they are available (and are known to be reliable).

Finally, mathematicians might only want to use proof techniques that are means to *at least one* of several possible epistemic objectives (e.g., a proof

[23] Jonathan Kvanvig (1998, 433–434) critiques the view that justification is intrinsically valuable along similar lines. Also, Goldman (1999, 78) critiques Helen Longino for assigning "fundamental epistemic value to impartiality and nonarbitrariness" in science when we would have thought that they were valuable only because they "foster accuracy and truth."

[24] This is essentially just another way of expressing the epistemic objective discussed in the previous paragraph.

[25] Of course, it should be noted that the proofs of a number of important mathematical theorems utilize simple combinatorial facts (see, e.g., Tymoczko 1979).

technique might have to be very reliable *or* be very explanatory). In this paper, I have been considering epistemic objectives one at a time. However, it is conceivable that some disjunction of these epistemic objectives might explain the rejection of probabilistic proofs.[26] Unfortunately, it is not immediately clear what this disjunction could be or that such a disjunction would provide a satisfying explanation. After all, the Pomerance quote above suggests that we are looking for a *single* qualitative difference between deductive proofs and probabilistic proofs.

7. *Rejecting Epistemic Consequentialism*

So far, we have not been able to find an epistemic objective of mathematicians that explains the rejection of probabilistic proofs in a satisfying way. It might be suggested that our failure to find a satisfying explanation is simply a result of the theoretical framework that we are using. The framework of means/ends reasoning is essentially a consequentialist framework. According to consequentialism, the right action is solely determined by what has the best consequences (cf. Smart and Williams 1973, 4). Epistemic consequentialism, in particular, says that the right action is solely determined by what has the best *epistemic* consequences (cf. Goldman 1999, 87). However, many theorists claim that consequences are not all that matter.[27]

In many contexts, it is also important how those consequences are brought about. For example, according to virtue ethics, the right action is one that is performed in a virtuous way or with good motives (cf. Oakley 1996, 129–130). This sort of idea has recently been applied to epistemology (see, e.g., Zagzebski 2003, 17–18). Along these lines, it might be suggested that only by using a deductive proof can we come to know that a mathematical claim is true in an intellectually virtuous way. This would arguably explain the rejection of probabilistic proofs.

However, there are a couple of problems with this sort of non-consequentialist strategy. First, it requires that we reject "the deeply plausible-sounding feature [of consequentialist theories] that one may always do what would lead to the best available outcome overall" (Scheffler 1982, 4). It is very

[26] It is very unlikely that a *conjunction* of these epistemic objectives could explain the rejection of probabilistic proofs. Since a proof technique is not required to be a means to any of the epistemic objectives discussed in the last section, it follows that a proof technique is not required to be a means to a conjunction of these objectives.

[27] Of course, even if non-consequentialist considerations can explain the rejection of probabilistic proofs, it is still interesting to determine if anything can be said to defend the rejection on consequentialist grounds.

strange that mathematicians should not be able to use probabilistic proofs when doing so would have the best epistemic consequences (e.g., in those areas where they are known to be reliable).

Second, traditionally non-consequentialist considerations are not actually excluded from the framework of means/ends reasoning (cf. Dreier 1993, 23). People often have objectives with respect to how desirable consequences are brought about (cf. the athlete that wants to win fairly). In fact, we have already countenanced such an objective by considering the possibility that using deductive proofs is intrinsically valuable. However, as noted above, it is mysterious *exactly why* using deductive proofs is intrinsically valuable. In other words, it is not clear why using probabilistic proofs does not also count as being intellectually virtuous.

Of course, even if a purely non-consequentialist strategy is not successful, there is room for a more modest rejection of consequentialism. In particular, several philosophers have pointed out that an individual who tries to bring about the best consequences on every occasion will often fail to do so (see, e.g., Railton 1984, 154). As a result, an individual can often do better by deciding once and for all to simply follow a rule that has good consequences overall. Along these lines, it might be suggested that, while using probabilistic proofs might have better epistemic consequences in a few cases, following the rule of using only deductive proofs will have better epistemic consequences overall.

However, this suggestion is open to one of the standard objections to rule consequentialism (cf. Smart and Williams 1973, 10–12). Namely, we can always bring about better consequences overall by following a more elaborate rule. For example, instead of following the rule of using only deductive proofs, why not follow the rule of using deductive proofs except when using probabilistic proofs would have better epistemic consequences? In fact, why not just follow the rule of doing whatever has the best epistemic consequences (which would arguably mean using probabilistic proofs where they are known to be reliable)?

Of course, there are limits to the degree that humans can build exceptions into their rules. In particular, we typically have to make decisions about what to do under fairly tight time constraints (cf. Smart and Williams 1973, 42, Railton 1984, 153). As a result, we have to follow relatively simple rules (e.g., without extensive exceptions) that can be applied quickly to particular cases. However, it is not clear that we are under such tight time constraints when deciding how to establish that a mathematical claim is true. Mathematicians can just wait until they know that they have a reliable method, such as the trial division test *or* the Rabin test.

8. *Conclusion*

The framework of means/ends reasoning can be used to explain the methodological choices of mathematicians. In particular, we can identify epistemic objectives that might have led them to reject probabilistic proofs. For a variety of reasons, however, the explanations that are currently available are unsatisfying. If there really is an important epistemic "difference between probabilistic verification and mathematical proof," more work certainly needs to be done to clarify exactly what this difference is. However, if it turns out that there is no such difference, this finding will have great significance well beyond mathematics. In particular, it will suggest that deductive arguments in general do not have any (actual) epistemic advantage that is not shared by at least some inductive arguments.[28]

School of Information Resources
University of Arizona, Tucson
E-mail: fallis@email.arizona.edu

REFERENCES

Agarwal, Manindra, Neeraj Kayal, and Nitin Saxena (2002), "PRIMES is in P." http://www.cse.iitk.ac.in/news/primality.pdf.

Anglin, W. S. (1997), *The Philosophy of Mathematics: The Invisible Art.* Lewiston, New York: Edwin Mellen.

Azzouni, Jody (2000), *Knowledge and Reference in Empirical Science.* New York: Routledge.

Chaitin, Gregory J. (1982), "Gödel's Theorem and Information." *International Journal of Theoretical Physics* 21:941–54.

Coady, C. A. J. (1992), *Testimony.* New York: Oxford.

Davis, Philip J. (1972), "Fidelity in Mathematical Discourse: Is One and One Really Two?" *American Mathematical Monthly* 79:252–63.

[28] Earlier versions of this paper were presented at the International Conference on "Perspectives on Mathematical Practices" in Brussels, at the 2002 Meeting of the Eastern Division of the American Philosophical Association, at the 2001 Meeting of the Canadian Society for History and Philosophy of Mathematics, and to the Departments of Philosophy and Mathematics of the Massachusetts College of Liberal Arts. This paper benefited greatly from feedback that I received at an NEH summer seminar on "Proofs and Refutations in Mathematics Today" directed by Colin McLarty and David Corfield at Case Western Reserve University. Finally, I would like to thank Jody Azzouni, David Christensen, Peter Lewis, Penelope Maddy, Kay Mathiesen, Gregory Taylor, Paul Weirich, and Catherine Womack for many helpful comments and suggestions.

De Millo, Richard, Richard Lipton, and Alan Perlis (1979), "Social Processes and Proofs of Theorems and Programs." *Communications of the ACM* 22:271–80.

Detlefsen, Michael and Mark Luker (1980), "The Four-Color Theorem and Mathematical Proof." *Journal of Philosophy* 76:803–20.

Dreier, James. 1993. "Structures of Normative Theories." *Monist* 76:22–40.

Fallis, Don (1997), "The Epistemic Status of Probabilistic Proof." *Journal of Philosophy* 94:165–86.

Folina, Janet (1999), "Pictures, Proofs, and 'Mathematical Practice': Reply to James Robert Brown." *British Journal for the Philosophy of Science* 50:425–29.

Goldman, Alvin I. (1999), *Knowledge in a Social World.* New York: Oxford.

Harel, David (1989), *The Science of Computing.* Reading, Massachusetts: Addison-Wesley.

Hersh, Reuben (1997), *What Is Mathematics, Really?* New York: Oxford.

Hume, David (1967), *A Treatise of Human Nature.* ed. L. A. Selby-Bigge. London: Oxford.

James, William (1979), *The Will to Believe.* Cambridge: Harvard.

Kornblith, Hilary (1999), "In Defense of a Naturalized Epistemology." Pp. 158–69 in *The Blackwell Guide to Epistemology*, eds. John Greco and Ernest Sosa. Malden, Massachusetts: Blackwell.

Knuth, Donald E. (1999), "Frequently Asked Questions." http://www-cs-staff.stanford.edu/ knuth/faq.html.

Kvanvig, Jonathan L. (1998), "Why Should Inquiring Minds Want to Know?: *Meno* Problems and Epistemological Axiology." *Monist* 81:426–51.

Laudan, Larry (2001), "Epistemic Crises and Justification Rules." *Philosophical Topics* 29:271–317.

Levi, Isaac (1962), "On the Seriousness of Mistakes." *Philosophy of Science* 29:47–65.

Maddy, Penelope (1997), *Naturalism in Mathematics.* New York: Oxford.

Markus, Mario and Eric Goles (2002), "Cicadas Showing Up After a Prime Number of Years." *Mathematical Intelligencer* 24:30–32.

Oakley, Justin (1996), "Varieties of Virtue Ethics." *Ratio* 9:128–52.

Peterson, Ivars (1990), *Islands of Truth.* New York: W. H. Freeman and Company.

Polya, George (1954), *Mathematics and Plausible Reasoning.* Princeton: Princeton.

Pomerance, Carl (1981), "Recent Developments in Primality Testing." *Mathematical Intelligencer* 3:97–105.

Pomerance, Carl (1982), "The Search for Prime Numbers." *Scientific American* (December):136–47.

Pratt, Vaughan R. (1975), "Every Prime Has a Succinct Certificate." *SIAM Journal on Computing* 4:214–20.

Rabin, M. O. (1980), "Probabilistic Algorithm for Testing Primality." *Journal of Number Theory* 12:128–38.

Railton, Peter (1984), "Alienation, Consequentialism, and the Demands of Morality." *Philosophy and Public Affairs* 13:134–71.

Ribenboim, Paulo (1996), *The New Book of Prime Number Records.* New York: Springer-Verlag.

Rivest, R., A. Shamir, and L. Adleman (1978), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM* 21:120–126.

Rota, Gian-Carlo (1997), *Indiscrete Thoughts.* Boston: Birkhäuser.

Scheffler, Samuel (1982), *The Rejection of Consequentialism.* Oxford: Oxford.

Sherry, David (1997), "On Mathematical Error." *Studies in History and Philosophy of Science* 28:393–416.

Sipka, Timothy (2002), "Alfred Bray Kempe's "Proof" of the Four-Color Theorem." *Math Horizons* (November):21–23, 26.

Smart, J. C. C. and Bernard Williams (1973), *Utilitarianism: For and Against.* Cambridge: Cambridge.

Solovay, R. and V. Strassen (1977), "A Fast Monte-Carlo Test for Primality." *SIAM Journal on Computing* 6:84–85.

Steiner, Mark (1975), *Mathematical Knowledge.* Ithaca: Cornell.

Tymoczko, Thomas (1979), "The Four-Color Problem and Its Philosophical Significance." *Journal of Philosophy* 76:57–83.

Welling, Hans (1994), "Prime Number Identification in Idiot-Savants: Can They Calculate Them?" *Journal of Autism and Developmental Disorders* 24:199–207.

Williams, B. A. O. (1972), "Knowledge and Reasons." Pp. 1–11 in *Problems in the Theory of Knowledge*, ed. G. H. von Wright. The Hague: Martinus Nijhoff.

Womach, Catherine and Matrin Farach (2003), "Randomization, Persuasiveness and Rigor in Proofs." *Synthese* 134:71–84.

Wray, K. B. (2002), "The Epistemic Significance of Collaborative Research." *Philosophy of Science* 69:150–168.

Zagzebski, Linda (2003), "The Search for the Source of Epistemic Good." *Metaphilosophy* 34:12–28.

Zeilberger, Doron (1993), "Theorems for a Price: Tomorrow's Semi-Rigorous Mathematical Culture." *Notices of the American Mathematical Society* 40:978–81.