Randomized Arguments are Transferable

Jeffrey C. Jackson*

July 20, 2009

Abstract

Easwaran has given a definition of transferability and argued that, under this definition, randomized arguments are not transferable. I show that certain aspects of his definition are not suitable for addressing the underlying question of whether or not there is an epistemic distinction between randomized and deductive arguments. Furthermore, I demonstrate that for any suitable definition, randomized arguments are in fact transferable.

Kenny Easwaran [Easwaran2008] has recently given a definition of transferability of mathematical proofs and has attempted to use this notion to epistemically differentiate between traditional deductive proofs and certain inductive arguments based on randomized trials (which I will call *randomized arguments*; more on this below). However, I will show that there are problems with Easwaran's definition and further demonstrate that, for any suitable definition of the term, transferability does not epistemically distinguish between deductive proofs and randomized arguments.

1 Background

It will be helpful to begin by defining a few terms and concepts. First, for consistency with Easwaran's arguments, we define belief using a Bayesian framework. In particular, terms such as "come to believe" and "become convinced" will be used in a Bayesian sense: if a rational person's posterior confidence in the truth of a proposition after observing evidence for that proposition is sufficiently near 1, then that person comes to believe the proposition, or becomes convinced of the truth of the proposition. In this context, if one begins with a prior belief about the truth/falsehood of a proposition and conducts random trials for which the likelihoods can be accurately calculated (or at least bounded) and are sufficiently extreme, then potentially one can rationally become convinced of the truth (or falsehood) of the proposition via a statistical form of inference. Easwaran (as Fallis [Fallis1997, Fallis2002] before him) calls such a statistical inference leading to belief a *probabilistic proof*. However, this term is sometimes used to describe a form of mathematical argument that relies on probabilistic analysis within a deductive proof (see, e.g., [Alon and Spencer2000]), and "proof" denotes to many a deductive argument. I will therefore instead employ the term *randomized argument* for what Easwaran calls probabilistic proof. (See [Easwaran2008] for detailed descriptions of this concept and of Bayesian belief acquisition more generally.)

As a concrete example or a randomized argument, Easwaran uses (and Fallis [Fallis1997, Fallis2000, Fallis2002] earlier used) the Miller-Rabin primality testing algorithm [Rabin1980], which I briefly describe next. Given a positive odd integer $N > 1$, this algorithm proceeds in rounds. In each round, a number between 2 and $N - 2$ is chosen uniformly at random, and a calculation is performed using the chosen number. The calculation can produce one of two results: either clear evidence that N is not a prime (is composite), or no clear evidence for either the primality or compositeness of N. It has been proven that for any odd composite N, the probability (over random choice of numbers) that r rounds of Miller-Rabin will fail to provide evidence of compositeness is at most $1/4^r$, which is of course extremely small for even

*Department of Mathematics and Computer Science, Duquesne University, Pittsburgh PA USA 15282-1754. jacksonj@duq.edu

moderately large values of r. Thus, for essentially any reasonable prior belief about the primality of a given N and essentially any reasonable Bayesian threshold on posterior probability required to achieve belief, if N survives a moderately large number of rounds of Miller-Rabin without definitive evidence of compositeness then one will come to believe that N is prime.

A final term to be considered is *proof sketch*. Easwaran describes a proof sketch for some mathematical proposition as a proof from which certain steps have been removed, leaving gaps that the reader must either fill in or simply accept based on expert familiarity with the domain. The types of gaps allowable in a proof sketch potentially depend on the particular community of mathematicians for whom the sketch is written. But it is assumed that every community will be able to recognize an acceptable level of sketchiness when they see it.

What Easwaran is perhaps not entirely clear about is *how* these gaps are to be filled. At one point, he refers to the reader filling in "the" steps of a proof sketch, and as we will see, this view of sketches is crucial in his later argument concerning transferability. Yet elsewhere he gives as an example of the sort of statement that might appear in a sketch the phrase, "a straightforward application of the Axiom of Choice shows that..." Will such a sketch necessarily lead all competent readers to fill the gaps in exactly the same way, reproducing exactly the same proof, or is it possible that the "straightforward application" by some readers will differ in one or more ways from those of other readers?

An even simpler example should make clear that, in fact, proof sketches—and even what we call "proofs"—do not necessarily lead to the exact same proof steps for all readers. Consider the following phrase: "Since $3/10 < 4/13$,..." If such a phrase appeared in a mathematical article (and it very well might, in the context of a larger proof), it would be mathematically gauche to give a justification for the proposition $3/10 < 4/13$, since it is so extremely simple to verify its truth. In fact, if this was the only unproven proposition within a proof, it is almost beyond imagination that any mathematician would demand that the proof be labeled a sketch. Yet, there are several different methods that mathematicians might use to convince themselves of the truth of this proposition: cross-multiplication by the denominators, comparison of the decimal (or other number base) expansions of the fractions, application of a lemma such as that for any positive integers i and j satisfying $i^2 < j$, $i/j < (i+1)/(i+j)$, etc.

2 Transferability and Randomized Arguments

Given the background of the previous section, we are ready to consider the concept of transferability. The first thing to ask is *what* exactly are we interested in transferring between author and readers? Broadly speaking, I believe that Easwaran would agree that we are interested in the transfer of a proposition (call it P) and an argument for P via which a competent reader[1] can become convinced of P's truth without the need for any appeal to authority. But this broad answer allows several distinct possibilities related to what readers will ultimately be expected to know and how readers will be expected to obtain this knowledge. In terms of what readers will know, a definition of transferability might or might not require that all competent readers be able to reconstruct from the author's published work exactly the same argument A for P as the author had in mind. And in terms of how readers obtain knowledge, a definition might or might not require readers to become convinced of the truth of P by merely considering the author's proof (or proof sketch, as the case may be).

Easwaran implicitly assumes the most stringent definition: all readers must be able to reconstruct the same argument A for P, and they must ultimately be convinced of the truth of P based merely on consideration of A (or more precisely, on consideration of what the author has written). Given this definition, Easwaran observes that readers cannot know that an author of a randomized argument actually performed truly randomized trials (as required if such an argument is to be valid), for there is no way for the author to prove that she was not biased in her choice of trials by her choice of problem or vice versa. For example, in an argument for the primality of a number N based on a purported execution of the Miller-Rabin algorithm, readers of the argument cannot be convinced that the author actually chose numbers randomly between 2

[1] Technically, it might require a team of readers with various types of expertise to fully verify the truth of a proposition. We will ignore this fine point; see [Easwaran2008] for a full discussion.

and $N-2$ after—and independently of—choosing N. Thus, a randomized argument based on Miller-Rabin is not transferable according to this strict definition, because the reader cannot become convinced of the primality of N by merely considering what the author has written.

However, recalling the earlier discussion of proof sketches, it should be clear that sketches also do not qualify as transferable under this strict definition. This stands in contradiction to Easwaran's explicitly stated understanding that sketches should be transferable (although, as noted above, his article is a bit hazy about exactly what a proof sketch is). What's more, Easwaran's purpose in considering transferability is to shed light on the question of whether or not there is an epistemic reason for mathematicians to accept knowledge obtained deductively while rejecting any and all knowledge purportedly obtained via randomized arguments such as Miller-Rabin [Easwaran2008]. Since mathematicians clearly accept the use of proof sketches to transfer mathematical knowledge, and since sketches are not transferable under the strict definition of transferability, this definition is not suitable for discerning epistemic reasons for rejecting the use of randomized arguments while accepting traditional arguments, including proof sketches.

Thus, the strongest definition that might be suitable for shedding light on the underlying epistemic question is this: a proof of a proposition P is transferable if and only if all competent readers can become convinced of P merely by considering what the author has written. In particular, this definition does not allow readers to employ any randomized arguments in order to become convinced of P, because that would involve performing randomized trials, which goes beyond mere consideration of the author's argument.

It appears that Easwaran's argument would hold under this definition of transferability as well, so it might seem that his argument can be salvaged even if his definition of transferability is slightly flawed. However, the reader has perhaps already noticed that this weakened definition is unsatisfactory for a different reason: if we are interested in differentiating between randomized and deductive arguments, and if we are allowing that authors might make use of randomized arguments, then why would we require that readers use only deductive reasoning? In point of fact, we should not: such a definition would be begging the question by implicitly giving deductive reasoning a privileged position over randomized argumentation.

Another way of seeing the problem with this definition is to consider again in somewhat more detail the question of what exactly mathematical authors are attempting to transfer to their readers. If I were to write in a paper, "I first proved Lemma 4 in a different way," this sentence would not be transferring mathematical knowledge, because it conveys historical, not mathematical, information. In particular, there is no way for me to argue for the truth of this claim mathematically because it is a claim about an event that physically occurred at a point in time and not a claim about mathematical knowledge. Some readers might accept this claim on authority and find it interesting, but it would be absurd for a definition of transferability to require that readers be able to validate such claims by merely considering what I have written.

Now suppose that I write, "$2^{6,972,593}-1$ is a prime, as the reader can verify by, for example, running Miller-Rabin for a convincing-to-the-reader number of rounds (I used 100 rounds with the random numbers ...)." The parenthetical portion of this statement is no more mathematical knowledge than is a claim about how an author first proved a lemma. Specifically, a claim about what I did is a historical claim, and a list of numbers (presumably) obtained via some physical process that is believed to produce random numbers—but since it is a physical process, there is and can be no convincing mathematical argument for this belief—is not mathematical knowledge, either. So it would again be absurd for a definition of transferability to require readers to validate the parenthetical claims by mere consideration. The mathematical knowledge that *is* being transferred here is clearly the proposition that $2^{6,972,593}-1$ is prime along with the sketch of an argument that competent readers can use, without undue effort, to convince themselves that the proposition is true without relying on authority.

In short, it appears to me that any definition of transferability suitable for examining the epistemic differences between deductive and randomized arguments must allow readers to construct their own arguments for an author's proposition P and to employ randomized arguments if they so choose. And as should be apparent from the previous discussion, given any such definition, randomized arguments are indeed transferable. More precisely, the *essence* of such an argument (*e.g.*, "Miller-Rabin can be used to verify") can be transferred from author to readers, much as the essence of a deductive argument can be transferred via a proof sketch. Given this essence, competent readers can convince themselves of the truth of the underlying

proposition P. In the case of a proof sketch, this convincing takes the form of "fleshing out" the sketch into a fuller argument and becoming convinced of P by consideration of this argument. In the case of a randomized argument, this convincing takes the form of readers fleshing out the argument by performing their own randomized trials. Because their Bayesian prior beliefs about P and threshold for being convinced of the truth of a proposition might differ from the author's, they might need more or fewer trials than the author needed in order to become convinced. But, if P is true, become convinced they can, without resorting to authority.

3 Concluding Remarks

In summary, transferability has been offered as epistemically differentiating between deductive and randomized arguments. However, the definition of transferability used to obtain this result is not suitable given the underlying epistemic purpose. Under any more suitable definition, randomized arguments are in fact transferable. Thus, the only formal attempt to date to explicate a mathematically-significant epistemic difference between randomized and deductive arguments, while raising some interesting issues, does not in fact demonstrate such a difference. This adds credence to Fallis's observation that there is apparently no epistemic reason for mathematicians to reject randomized arguments such as Miller-Rabin.

4 Funding

This material is based upon work supported by the National Science Foundation under Grant No. CCF-0728939.

5 Acknowledgments

I thank Kenny Easwaran and Don Fallis for their insightful comments and encouragement.

References

[Alon and Spencer2000] Alon, N. and Spencer, J. H. (2000). *The Probabilistic Method*. Wiley-Interscience, 2 edition.

[Easwaran2008] Easwaran, K. (2008). Probabilistic Proofs and Transferability. *Philosophia Mathematica*. Advance Access article available at `http://philmat.oxfordjournals.org/cgi/content/abstract/nkn032v1`.

[Fallis1997] Fallis, D. (1997). The epistemic status of probabilistic proof. *The Journal of Philosophy*, 94(4):165–186.

[Fallis2000] Fallis, D. (2000). The reliability of randomized algorithms. *Br J Philos Sci*, 51(2):255–271.

[Fallis2002] Fallis, D. (2002). What do mathematicians want?: Probabilistic proofs and the epistemic goals of mathematicians. *Logique et Analyse*, 45(179–180):373–388.

[Rabin1980] Rabin, M. O. (1980). Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12(1):128–138.