Judge's Commentary: The Outstanding Fingerprints Papers

Michael Tortorella
Dept. of Industrial and Systems Engineering
Rutgers University
Piscataway, NJ
mtortore@rci.rutgers.edu

Introduction

The brief statement of this problem hid many layers of complication. Teams were challenged to find the mathematical kernel of a problem of interest to anthropologists, forensic scientists, attorneys and judges, and just plain folks. In essence, the problem reduces to

> *Estimate the probability that two humans who have ever lived have the same fingerprint.*

After the MCM was over, the *Wall Street Journal* carried an article entitled "Despite its reputation, fingerprint evidence isn't really infallible" [Begley 2004]. The uncritical acceptance of fingerprint evidence that was common in the past is undergoing new scrutiny, and our examination of the question in the MCM was timely indeed, if unplanned.

The Issues

Philosophical Questions

The problem seems innocuous enough; but you get very quickly into some deep—even philosophical—questions that have to be addressed in modeling assumptions. For example, exactly how finely does nature model the

The UMAP Journal 25 (3) (2004) 261–266.

real numbers? In mathematics, between every two real numbers there is another one; if between any two positions in physical space there is another one (distinguishable—by whom?—from the other two), then a homotopy between any two distinct fingerprints—however "fingerprint" is defined—produces an infinite number of distinct fingerprints. So the probability requested could reasonably be asserted to be zero, even if we say translations and rotations of a given fingerprint are not different from the original. Hence, a purely mathematical approach to the problem is not very interesting. On the other hand, the number of people n who have ever lived is finite, so we may find the answer "zero" unsatisfying.

A Simple Model

Here is a simple model that takes a next step: Assume that fingerprints (the actual skin patterns) are assigned at birth, at random from a pool of potential fingerprints. If we assume that the pool contains $N >> n$ elements and selection is made on an equally-likely basis, then the probability that there are no two fingerprints alike is the solution to a birthday problem with n people and N birthdays; namely, the probability of no match (denoted $Q_1 = 1 - P_2$ in Weisstein [2004]) is given by

$$P(\text{no match}) = \frac{N}{N}\frac{N-1}{N}\cdots\frac{N-n+1}{N} = \frac{N!}{n!N^n} \approx e^{-n(n-1)/2N},$$

which for fixed n is asymptotic to 1 as $N \to \infty$[1].

This is about the simplest model that one could devise for this problem, and teams should use these sorts of simple models as a baseline against which to assess other more complicated efforts. One thing that we learn from this model is that in effect, all the additional definitions for "fingerprint" serve essentially to shrink the pool of possible "fingerprints," that is, restrict N so that there is a chance that the probability of no match will be less than 1.

Reinterpreting the Question

In fingerprint analysis, a human being, either with the unaided eye or with some tool(s), judges two fingerprints to be "identical." So a reasonable interpretation of the relevant question could be:

> *Determine the probability that there have never been two identical fingerprints, given the capability of the technology used to determine "different."*

This is a little more interesting a question. Different assumptions can reasonably be made concerning this capability, which lead to different models and, usually, different answers.

[1] The condition that $N >> n$ is not idle: When $N = 2n$, the probability of no match is approximately $e^{-(n-1)/4}$, which is actually quite small for large n. But we already knew this from the "standard" birthday problem learned in Probability 101.

But First You Have to Define . . .

The first step in developing a model based on this question is to *define*:

- "fingerprint,"
- the probability space in which this experiment is conducted, and
- "distinct."

"Distinct" depends on who's looking; or, to put it more conventionally, resolution matters. All this is by way of scope delineation, so that when an answer is arrived at, the domain in which the answer is valid will be clear.

The definition of "fingerprint" is wrapped up in the definition of the probability space, because most teams made assumptions about the minimum spacing between ridges that could possibly occur. This assumption is based on empirical evidence (at least from humans who have been alive in the last century or so) and is the first step down a road leading to consideration of only a finite number of potential fingerprints.

Additional assumptions of this nature included restriction of the mathematical model to the six common types of fingerprint patterns (loops, arches, whorls, etc.) and a few variations.

The Importance of Interpretation

As always, interpretation is the key to success in modeling problems. The first key was to understand that the word "fingerprint," in addition to its usual semantic or prose usage, must be given a *mathematical meaning* in the context of a model. Successful papers began by providing a mathematical definition of "fingerprint," for example, as a rectangular area, 2 cm by 3 cm, containing alternating ridges and valleys arranged in one of 6 global patterns (arch, tented arch, left loop, right loop, whorl, and twin loop). Alternatively, one may distinguish between the fingerprint as a physical or biological entity on the body and a fingerprint as an image made on paper or other surface by a deliberate or accidental process. Any of these can lead to reasonable solutions but the modeler's choice should be made clear.

Once that is accomplished, it begins to be possible to talk in quantitative terms about how two fingerprints may be distinguished. Most papers adopted the FBI criteria concerning the number and location of minutiae as their differentiating method. A minutia is a local feature of the fingerprint, for example, the end of a ridge line or an isolated very short ridge of approximately the same length and width. Again, the standard FBI categorization of minutiae was most often used. A grid of some size (typically 1 mm on a side) is imposed on the fingerprint and the presence or absence of a minutia in a grid square is recorded (at most one minutia per square is permitted). Some papers noted that the size of the grid square should be approximately equal to, or slightly smaller than, the typical size of a minutia so that the possibility of more than one minutia in a grid square is minimized. The feature-resolving capability of the instrument used to view the fingerprint also matters, because if infinite resolution is possible, then all fingerprints will look different. In fact, this observation implies that one can pose this problem

- "theoretically," treating the "fingerprint" as a mathematical construct and using only properties of the real numbers, etc., to form a solution; or
- "practically," where the aspects of detectability of differences by human or machine methods are central.

A good solution to this problem, like that of the paper from the team at University College Cork, treats both aspects and their interplay.

At Last, a Model

Even with these few assumptions, a model is possible: the total number of possible distinct fingerprints implied is $2^{600} \approx 10^{181}$. The number of people who have ever lived is about 1.06×10^{11}; so, assuming that all 2^{600} patterns are equally likely, the probability that no two persons who have ever lived have the same fingerprint is approximately $1 - 10^{-159}/2$ (this latter computed from the "birthday problem" with $1.06 \times 10^1 1$ people and 2^{600} possible "birthdays," a point that many teams missed). The University College Cork team handled this approach about as well as could be.

It is easy to poke holes in this model. Empirically, it is clear that

- not every grid square has the same probability of containing a minutia,
- stochastic independence of the presence or absence of minutiae from grid square to grid square is not reasonable, and
- there are several different types of minutiae.

Many teams overcame these objections by adding to the basic model assumptions comprehending several types of minutiae and various other refinements based on empirical observations of physical characteristics, such as ridge width, interridge distance, and frequency of occurrence of different types of minutiae in a grid square. For example, both the papers from Harvey Mudd College and University College Cork introduced orientation of minutiae as another distinguishing characteristic (although the University College Cork paper does not follow through on this additional detail, giving this the feeling of a dead end). In all cases, though, when such assumptions based on empirical observation are introduced, the modeler should attempt to bound the answers using a range of possible reasonable values for the inputs because sampling error could affect the assumptions. Once could argue that sampling error should be negligible in drawing inferences from a database containing millions of records, like most fingerprint databases, but most teams did not address this issue in any way.

Finally, the problem asks for comparison of the computed probability with the probability of misidentification by DNA evidence, a topic much in the public eye in the last decade. Some teams ignored this requirement. Others quoted popular anecdotes concerning the DNA misidentification probability. In the latter case, teams would be advised to bolster their contentions with at least one legitimate citation.

As Always, Advice

- **Make your paper easy to read.** That means, at least, number the pages and the equations, check your spelling, and double-space the text (or at least use a font size large enough for easy readability). All three Outstanding papers shown here did a good job with this.

- Good organization will not make up for poor results, but poor organization can easily overwhelm good results and make them hard to dig out. **Organize the paper into sections corresponding to the parts of the problem.**

- **Define all terms** that a reader might find ambiguous; in particular, any term used in the model that also has a common prose meaning should be carefully considered. The paper from University College Cork in particular does a very thorough job with this.

- **Complete all the requirements of the problem.** If the problem statement says certain broad topics are required, begin by making an outline based on those requirements.

- **Read the problem statement carefully,** looking for key words implying actions: design, analyze, compare, etc. (imperative verbs). These are keys to the sections your paper ought to contain.

- **Address sensitivity to assumptions as well as the strengths and weaknesses of the model.** That means that these topics should be covered separately in sections of their own.

- When you do strengths and weaknesses, or sensitivity analysis, **go back to your list of assumptions and make sure that each one is addressed.** This is your own built-in checklist aiding completeness; use it.

- **Your summary should state the results that you obtained, not just what you did.** Keeping the reader in suspense is a good technique in a novel, but it simply frustrates judges who typically read dozens of papers in a weekend. The University of Colorado paper has an excellent summary: crisp, concise, and thorough.

- **Use high-quality references.** Papers in peer-reviewed journals, book, and government Websites are preferred to individuals' websites. Note also that it is not sufficient to copy, summarize, or otherwise recast existing literature; judges want to see *your* ideas. It's okay to build on the literature, but there must be an obvious contribution from the team.
- **Verify as much as you can.** For example, the total population of the earth should be readily verifiable. Make whatever sanity checks are possible: is answer you get larger than the number of atoms in the known universe? If it is, should it be?
- **Finally, an outstanding paper usually does more than is asked.** For example, the University of Colorado team created two different models to attack the problem and compared the results from each approach; the reasonably good agreement they obtained showed that either
  - they were on the right track, or
  - they were victims of very bad luck in that both of the methods that they tried gave nearly the same bad answers!

Reference

Begley, Sharon. 2004. Despite its reputation, fingerprint evidence isn't really infallible. *Wall Street Journal* (4 June 2004) B1.

Weisstein, Eric. 2004. Birthday problem. `http://mathworld.wolfram.com/BirthdayProblem.html` .

About the Author

Mike Tortorella is a Research Professor in the Department of Industrial and Systems Engineering at Rutgers, the State University of New Jersey, and the Managing Director of Assured Networks, LLC. He retired from Bell Laboratories as a Distinguished Member of the Technical Staff after 26 years of service. He holds the Ph.D. degree in mathematics from Purdue University. His current research interests include stochastic flow networks, information quality and service reliability, and numerical methods in applied probability. Mike has been a judge at the MCM since 1993 and has particularly enjoyed the MCM problems that have a practical flavor of mathematics and society. Mike enjoys amateur radio, the piano, and cycling; he is a founding member of the Zaftig Guys in Spandex road cycling team.