A. Einstein, "Erklärung der Perihelbewegung des Merkur aus der allgemeinen Relativitätstheorie", *K. Preußische Akademie der Wissenschaften. Sitzungsbe-richte*, 1915c, pp. 831-839.

A. Einstein, "Die Feldgleichungen der Gravitation", *K. Preußische Akademie der Wissenschaften. Sitzungsbericht*, 1915d, pp. 844-847.

Galileo Galilei (EN): *Le opere*, Nuova ristampa della Edizione Nazionale, 20 vols. G. Barbera, Firenze 1964-1966.

C. Glymour, "Indistinguishable space-times and the fundamental group", in Earman et al. *Foundations of Space-Time Theories*, University of Minnesota Press, Minneapolis 1977, pp. 50-59.

S. W. Hawking, "Black hole explosions?", *Nature*, **248**, 1974, 30-31.

S. W. Hawking, "Black holes and thermodynamics", *Physical Review* **D. 13**, 1976, 191-197.

S. W. Hawking, "Particle creation by black holes", *Communications in Mathematical Physics* **43**, 1975, 199-220.

S. W. Hawking, "The quantum mechanics of black holes", *Scientific American* **236** 1, 1977, 34-40.

S. W. Hawking and W. Israel, eds. *General Relativity: An Einstein Centenary Survey*, Cambridge University Press, Cambridge, 1979.

P. Kitcher, *The Advancement of Science: Science without Legend, Objectivity without Illusions*, Oxford University Press, New York 1993.

L. Laudan, "A confutation of convergent realism", *Philosophy of Science* **48**, 1981, 19-48.

D. Malament, "Observationally indistinguishable spacetimes: Comments on Glymour's paper", in Earman et al. *Foundations of Space-Time Theories*, University of Minnesota Press, Minneapolis 1977, pp. 61-80 (Minnesota Studies in the Philosophy of Science **8**).

G. Maltese and L. Orlando, "The definition of rigidity in the special theory of relativity and the genesis of the general theory of relativity", *Studies in the History and Philosophy of Modern Physics* **26B**, 1995, 263-306.

S. Psillos, "Theories and models in scientific processes", *Studies in the History and Philosophy of Science* **25**, 1994, 159-190.

S. Psillos, "A philosophical study of the transition from the caloric theory of heat to thermodynamics: Resisting the pessimistic meta-induction", *Poznan Studies in the Philosophy of the Sciences and the Humanities* **44**, 1995, 105-133.

H. Putnam, *The Many Faces of Realism*, The Paul Carus Lectures, Open Court, LaSalle, IL, 1987.

K. Schwarzschild, "Über das Gravitationsfeld eines Massenpunktes nach der Einsteinschen Theorie", *K. Preußische Akademie der Wissenschaften. Sitzungsberichte*, 1916, pp. 189-196.

C. M. Will, *Theory and Experiment in Gravitational Physics*, Cambridge University Press, Cambridge 1981.

PETER GALISON

RANDOM PHILOSOPHY

1. INTRODUCTION

Somewhere, in any computer-based Monte Carlo simulation, is a line of code that produces random numbers. With names like RANDU, RANDOM, RANF, or RNDM, the command is innocuous, a single, practically invisible step in a program that could run to hundreds of lines. Indeed, in the 1960s, the then-standard IBM 709 came oufitted with a random generator that was used around the world to produce simulations of phenomena ranging from nuclear weapons and airplane wings to the impact of pions on protons, from weather modelling to the analysis of number theory. In this brief paper, I want to take out the philosophical magnifying glass and peer into the epistemological and metaphysical changes at work behind the code.

The idea of a Monte Carlo is not complicated: by sampling randomly from a set of points one can often approximate a volume. Throw darts at a circle inscribed in a square and count the ratio of points in the circle to the number of hits inside the square (including both those in the circle and those between the circle and the perimeter of the square). That ratio gives an approximation of the ratio of the circle area to that of the square ($\pi/4$). Similarly, one could take a function $f(x)$ and rough out its integral $\int_a^b f(x)dx$ by "throwing darts" at the rectangular region defined from $x = a$ to $x = b$ and by an interval of values of $y = f(x)$ from some point below the minimum of f(x) in [a,b] and the maximum of $f(x)$ in [a,b]. The ratio of hits below the curve $f(x)$ to the number of hits not below the curve then approximates the ratio of the area $\int_a^b f(x)dx$ to the area of the whole rectangle. In other words one uses random points to fill out a series of pairs (x_i, y_i) counting as hit points such that $y_i < f(x_i)$ and divides by the total number of pairs tried—this approximates $\int_a^b f(x)dx$.

Generalizing from such considerations, the Monte Carlo can be used to sample-estimate the definite integral of a high-dimensional definite integral, a feature valuable in all manner of problems from hydrodynamic flow to the intricacies of thermonuclear weapons design in which radiation transport, fusion, Compton effects, and a myriad of other processes are at work. Strikingly—amazingly it has seemed to some—these approximations could, with increasing numbers of sample points, converge to the "true" value of the definite integral at a rate far exceeding any previously-known method of numerical integration.

The Monte Carlo Method, invented by mathematician Stanislaw Ulam and mathematician/physicist John von Neumann towards the end of World War II, was

E. Agazzi and M. Pauri (eds.), The Reality of the Unobservable, 123-128.

initially used to calculate the physics of fission weapons, especially the physics of neutrons in the chain reaction. Such tasks gobbled random numbers at an alarming rate, and without a ready and reliable supply, the process of launching trial "throws" such as the choice of (x_i, y_i) would come to a screeching halt. Generated from electrical noise, from the alpha decay of radioactive minerals, and from the arrival times of cosmic rays, these "true randoms" were compiled and published in books. Putting aside the conceptual difficulty of taking a published hardbound volume of true random numbers off the shelf (how often could people begin their series 947826 and still consider it random?) the pedigree of these digits was impeccable. "True randoms", physically-generated random numbers, could be thought of as truly standing for the world: what could be more natural than using alpha-decay-produced randoms to model the diffusion of neutrons inside a reactor core? Even when the process to be modelled was not itself random—as in the evaluation of a finite integral—numbers were needed fast and plentifully.

To accelerate the early simulations to the point where they could be useful, von Neumann introduced the notion of pseudo-random numbers. Instead of plucking digits off a list of the true randoms, von Neumann proposed that a suitably chosen algorithm could generate a series of digits that "for practical purposes" could serve more or less as well. For example, one could take an eight-digit number (from a "true random" book, if one so wished) square it and excise the middle eight digits. This new group became the seed for the next one: square the eight digits and extract the central eight digits of the result. The computer itself could continue in this way, *ad libitum.*

Now from the instant of von Neumann's proposal, it was manifest to him that this sequence of pseudo-randoms was not and could never be "random." There are, after all, only 10^8 eight-digit numbers. So in at most 10^8 repetitions of this game, an eight-digit sequence will repeat. When it does, as sure as the sun rises in the east (more surely, actually) the algorithm will repeat the exact sequence of numbers it got the first time around. So the sequence is not random—much worse, it is an eternal, precisely repeating cycle. We are living in a state of sin, von Neumann confessed to a colleague, when we use Monte Carlos. Still, the sequences and their owners worked with a pragmatic confidence. If the sequence passed its tests all was fine. Or was it?

To certify the pseudo-random generators, physicists and their mathematical colleagues developed a series of tests. Were the digits equitably distributed—that is, were there roughly the same number of 0s, 1's, 2's, ... and 9's? Were there correlations between the i^{th} and $(i+k)^{th}$ digit, where k was 1, 2, 3, . . . up to some reasonable value of k? One author somewhat cynically captured the philosophy of the idea this way: "if a pseudo-random number has passed a certain number of tests, then it will pass the next one where the next one is the answer to our problem."[1] It was, nonetheless, hoped that generators could be designed such that repetitions and correlations could be excluded at least for a long-enough sequence for the simulation to run. "Tests of randomness" would vouchsafe the "approximate randomness" of the series.

But as James's wry motto made clear, it was not at all clear *which* tests, of the infinite number that could be made, would actually be most useful as guardians of the true random faith. Just how fragile the whole apparatus was became manifest in 1963 when high energy physicist Joseph Lach became suspicious of the generators he and everyone else had been using.[2] Instead of asking after the equidistribution and k-correlations (correlations between the i^{th} and $(i+k)^{th}$ term), Lach pursued the correlations of triplets on at least a fraction of their range.

More specifically, he called up the Fortran number generator RANNO (which produced pseudo-randoms between 0 and 1.0), and had the computer sequentially hunt down the first number less than 0.1. He then programmed the computer to plot the next two numbers, designated x_1 and y_1, as a point on an xy plot on his CRT. Then the computer hunted down the next number that was less than 0.1 and once again made a pair out of the next two numbers, designating them (x_2, y_2) and popping them onto his screen. Continuing in this way, the computer "ought" to have filled its screen with (x_i, y_i) equitably splashed over the screen like the gray static of a TV set. It didn't. Instead of "randomness" Lach saw sharp black diagonal lines—bands of no points at all. The message was as disturbing as it was clear: the black bands announced that RANNO, having passed its other tests with flying colors, had failed the triplet correlation test in the region $0 < z_i < 0.1$. Even if one cooked up a pseudo-random generator that did pass the triplet test, the question lurked: would it do so for quadruplets, quintuplets, and higher multiplets? Virtually every computer in the world was producing manifestly unrandom randoms. The source of the difficulty was, as George Marsaglia of Boeing Scientific Laboratories showed, in the very nature of the so-called multiplicative congruential generators of the form

$$r_i = [a\, r_{i-1} + b]\ (mod\ m)$$

where m was 2 raised to the word size of the computer in use. For example for a 5-bit word one held $m = 32$, and (for example) choosing arbitrarily $a = 21$, $b = 1$, $r_0 = 13$, yields

$$r_1 = [(21)(13) + 1]\ mod\ (32) = 274/32,$$

which has a remainder of 18. Now set $r_1 = 18$ where r_0 was, and we get $r_2 = 27$. In this way we obtain

$$\{r_i\} = 13, 18, 27, 24, 25, 14, \ldots$$

Using an elegant result from Minkowski's *Geometry of Numbers*, Marsaglia demonstrated that the hyperplanes would always occur, no matter what the choices of the parameters were in the algorithm. "For the past 20 years," Marsaglia sadly concluded, "such regularity might have produced bad, but recognized, results in Monte Carlo studies," as multiplicative congruential generators quietly spewed regular hyperplane bands into models of baryons, bombs, and biology.[3]

Even without the Lach-Marsaglia result, pseudo-randoms were in trouble. S.K. Zaremba, for one, denounced the belief that there are a set of properties, exhibited by a test or set of tests, that single out stochastic processes.[4] Furthermore, he argued, the deterministic aspect of the pseudo-random generator made a mockery of the very category of a calculation of variance within a Monte Carlo. For these and other reasons, he turned to replace pseudo-randoms with a new kind of generator, one known as a quasi-random generator. This shift I consider to be of greater epistemic import even than the shift from the true to the pseudo. The idea is this: instead of attempting in ever fancier ways to capture some essential feature of the random, the very ideal of random is taken down a notch, out of the exalted position as a privileged epistemic and metaphysical category. Do not look to secure the randomness of the pseudo-randoms say the quasi-ists, look for the most efficient and powerful distribution of numbers to solve the problem—whatever distribution that may demand. Indeed randomness is taken on the quasi scheme to be just a certain degree of "clumpiness"; and the question becomes (quantitatively) not how to achieve that specific amount and type of clumpiness, but rather the precise degree of clumpiness of sampling that is best at estimating (for example) an integral.

"Local discrepancy" was a term introduced by Hermann Weyl in the early 20th century to quantify the clumpiness of a distribution of points in space.[5] It is defined as

$$g(x) = v(x)/N - x_1 x_2 x_3 \ldots x_d$$

where d is the dimension of the unit cube. So for example in a three-dimensional unit cube we imagine a set of N points distributed in some manner. $v(x)$ is the fraction of those N points contained in a subvolume defined by the origin and the points of intersection of the perpendiculars dropped from x to the walls of the unit cube. $g(x)$ therefore gives the deviation from equidistribution, and it can be postive or negative. Many norms can be defined for $g(x)$ including the extreme global discrepancy defined on a set of points S as

$$D(S) = sup \{|g(x)|\} \textit{ for } x \textit{ in } S$$

where sup is the supremum of the set. The result — the crucial result of the new method of quasi-randoms — was that for $D(S)$ less than that of randoms (less clumpiness than that characteristic of randomness) the approximation of an integral could be better than random, and in some cases much better convergence of this error term

$$E = |\int f(x)dx - 1/N \, \Sigma_k f(x_k)|$$

occurred not with $1/\sqrt{N}$ as in a random Monte Carlo, but rather as $1/N$; and even the $1/\sqrt{N}$ was an enormous improvement over the many regular quadrature schemes in play since the time of Archimedes.

I take three philosophical lessons from this piece of buried Fortran code: an end to the epistemic and metaphysical dominance of randoms in simulations, a sharp blow to the picture of simulation as a literal re-presentation of a natural process, and finally a challenge to our deeply held notions of typicality. In order:

2. DESACRALIZATION OF THE RANDOM

The great discovery and proliferation of computer-based Monte Carlos in the 1940s was that random sampling took $E \rightarrow O$ faster than ordinary numerical quadrature. And somehow, I suspect, that virtue was laid at the door of the random. In a certain way, this no doubt seemed reasonable. Wouldn't it in some sense be best to close one's eyes (so to speak) and then pluck a ball from an urn—wasn't randomness just the notion of studied abstinence from intervention when sampling—justice blindfolded? And at the *metaphysical* level wasn't there something special about a random process, something picked out as a natural kind by nature itself? Here the move from pseudo to quasi Monte Carlo is brusquely pragmatic and utterly deflationary. Randomness becomes no more than the choice of the sample support $\{x_i\}$ yielding a particular value of the clumpiness, $D(S)$. But other schemes were also possible, and the quasi view became simply that $D(S)$ would be chosen to speed the convergence of E to zero, even if it meant taking a value of $D(S)$ that did not resemble the clumpiness of a truly random set. Forget the epistemology of blind justice, forget the metaphysics of a special natural kind corresponding to randomness. Efficiency of convergence matters, and $D(S)$ would be found to suit the problem at hand.

3. THE END OF SIMULATION AS RE-PRESENTATION

For some years after the introduction of Monte Carlos, and even in the 1990s in certain cases, authors frequently emphasized the particular value of Monte Carlos when modelling processes were themselves thought to be random. In this sense the metaphysical correspondence between model and physical system was grounded in the circumstance that both were random. The model was a true Monte Carlo because both it and the phenomenon modelled were of the same natural kind. Such a view was problematic from early on—after all Ulam knew perfectly well that the Monte Carlo could be used to track deterministic processes and even nonphysical mathematical formulae. And with the introduction of pseudo- randoms the "natural kind" correspondence ought to have faded that much more. Still, the view survived. Quasi Monte Carlos, on my reading, ought to eliminate that view for good—the choice of the support set $\{x_i\}$ is made to minimize error fast; random $\{x_i\}$ were useful for a few decades because they beat out the regular $\{x_i\}$ of quadrature, and that is all. Now it was the turn of the randoms and their pseudo cousins to be left behind.

4. THE NEW TYPICALITY

Finally, and this must here remain only a suggestive remark, it seems to me that we have the opportunity to examine the notion of typicality up close. When we choose the support set $\{x_i\}$ in order to estimate an integral, we want above all to choose typical points. For a smooth periodic function it may well be that steady Archimedean footsteps from $x = a$ *to* $x = b$ are perfectly good. The problem comes when those steady footsteps fall in resonance with the behavior of the function—the nice regular sampling of $\sin^2\theta$ from 0 to 10π at intervals of π shows us that the integral of sine squared over that region is exactly zero. Bad job. Random selection aims to find typicality by avoiding all and any possible resonance between function and sample. But what we have learned from Monte Carlo is that even the random has a less than maximally efficient characteristic in extracting information from the integral: it is too bunched. It seems that typicality lies somewhere between Archimedes and Chaos, between, so to speak, the ideals of systematicity and blindness. I conclude these comments with what amounts to a double twist. Some years ago, the authors of a book of random numbers started with a set of true randoms and recoiled in horror as they found certain repetitive strings. To "improve" their set, they stuck in new digits, breaking up the unrandom look of the subsequence.[6] For years this circumstance has been regaled by statisticians as the height of perversity, illustrating how foolish it was to expect random numbers not to occasionally spew out a train of 7's. But the joke is now reversed: breaking up the strings of 7's might have been not a bad idea at all, as it probably served to lower the global discrepancy and might well have improved the convergence of Monte Carlos that made use of the doctored set. Now I don't recommend preparing the $\{x_i\}$ this way, but it reveals to us the twisting path of a random philosophy.

Harvard University - U.S.A.

NOTES

1 See James 1987.
2 See Lach 1963.
3 See Marsaglia 1968.
4 See Zaremba 1969.
5 See Weyl 1916.
6 See Lopes 1982.

REFERENCES

F. James, "Monte Carlo Theory and Practice", in Ferbel, *Experimental Techniques in High Energy Physics,* Menlo Park, Addisqā-Wesley, 1987, pp.627-77, on 656.

J. Lach, *Memorandum no. 27, Random Number Generators*, Yale Computer Center, 29 October 1963.

L. L. Lopes, Doing the Impossible: A Note on Induction and the Experience of Randomness, *Journal of Experimental Psychology* **8**, 1982, pp.626-636, on p.629.

G. Marsaglia, "Random Numbers Fall Mainly in the Planes", *Proceedings of the National Academy* **61**, 1968, pp.25-28, on p. 25.

H. Weyl, "Gleichverteilung", *Mathematische Annalen* 77, 1916, 313-352.

S. K. Zaremba, *The Mathematical Basis of Monte Carlo and Quasi-Monte Carlo Methods, Studies in Applied Mathematics* **3**, Philadelphia, Society for Industrial and Applied Mathematics, 1969, pp. 1-11.

MARIO CASARI...

FORMAL REPRESENTATION AND THE SUBJECTIVE SIDE OF SCIENTIFIC REALISM

Key words in my talk will be "way of representation", "way of notation", "symbolical formalization", and similar ones. These concepts, deserving many distinctions in principle, are grouped here on the basis of an elementary observation: experience and common sense testify indeed that, in all scientific disciplines, the perspective on certain problems and the possibility of solving them can be drastically modified by the introduction of a new way of representation. In this notion, besides high level formalizations, I shall consider therefore also the concrete embodiment in signs, figures, graphical devices, methods for writing, short cuts to symbolization, etc. A desordered list of examples may include:

- figures in elementary geometry;
- positional notation for numbers;
- structure formulas in chemistry;
- algebraic notation for calculus;
- all kind of diagrams, from Descartes to Feynman;
- Argand-Gauss plane for complex numbers;
- Boolean algebra;
- Symbolical Dynamics;
- Turing machines;
- nonstandard notation for infinitesimals, etc.

Before going into the argument, some factual remarks are opportune. It is a truism that every problem, before being solved, must be thought. Besides making easier the solution of an existing problem, a new way of representation can open a whole range of previously *unthinkable* themes, independently of the particular argument in relation to which it has been introduced. As if in the notation there were much more than the inventors could suspect, previously invisible objects become visible. A standard example is the Argand-Gauss representation for complex numbers: as a visualization of the roots of an algebraic equation it seems almost trivial; but only through this representation, otherwise inconceivable arguments, such as the geometry of the Riemann surfaces, or the strange properties of the Zeta function, came out from pure virtuality. I don't insist on other classical examples, such as the positional notation for integers, or the habit of representing points through coordinates. Nowadays, as frequently pointed out, a great notational expansion is due to the programming languages: besides the brute computational power, the habit of looking at certain problems in terms of "steps of program" is going to change the point of view and the sensitivity about old arguments, and to introduce, in addition, a variety of new concepts. Chaitin and Kolmogorov ideas on the algorithmic complexity, for instance, and in general the rich development of

E. Agazzi and M. Pauri (eds.), The Reality of the Unobservable, 129-135.