U. S. AIR FORCE

PROJECT RAND

RESEARCH MEMORANDUM

Just How Random?:
Introducing PROJECT S.P.O.R.K.

[redacted]
A. M. Lyons
[redacted]

RM-[rand();]

Rev. 1 29 March 2024

Assigned to SIGBOVIK 2024

The RAND Corporation
1700 MAIN ST. • SANTA MONICA • CALIFORNIA

SUMMARY

This memorandum is intended for policymakers, leaders in the armaments production industry, computer scientists, physicists, mathematicians, and frazzled parents at the end of their ropes.

It details the importance of good sources of random numbers and the history of the attempts on the part of the RAND Corporation to reliably create them in service of American hegemony and the destruction of communism. Particular attention is paid to one of the more surprising aspects of randomness: its dramatic algorithmic utility even for computational problems that are not themselves inherently random.

It also announces an exciting new breakthrough that promises to annihilate two organisms with a single munition, so to speak: PROJECT S.P.O.R.K. is a plan for extracting high-yield top-quality 100 percent "pure" "Colombian-quality" randomness from one of our country's most frustratingly vast and untapped resources: our lazy and embarrassing grandchildren and their ilk.

PROJECT S.P.O.R.K.: Let's put America's youth to work in operations research.

~~S ecret~~S pecial
~~P roject~~P laytime for
O perations
R esearch for
K ids

CONTENTS

LIST OF ALGORITHMS

Just How Random?: Introducing PROJECT S.P.O.R.K.

[redacted]

A. M. Lyons

[redacted]

(I) BACKGROUND

Randomness has always been a part of the human experience, and--according to some interpretations of quantum mechanics--is an intrinsic aspect of the universe itself.

Unfortunately for the patriots among us, the mathematical treatment of randomness and probabilities began in the casinos of 16th century Europe (which must have been unimaginably seedy). Thankfully, shortly after the second world war, randomness began to be applied in an *instrumental* manner, as part of algorithms that assisted with a new much nobler and higher purpose: gambling not for money but rather with the continued existence of humanity. Driven by fears of a soviet nuclear program, the mortal necessity of "keeping up with the Kuznetsovs" demanded accelerated development of the most terrific instruments of Armageddon imaginable, and all available resources were brought to bear. This included the finest minds, who developed the finest tools, which included advanced computational resources and, more importantly, the algorithms to make use of them. Enter Monte Carlo: Working at Los Alamos on the development of thermonuclear weapons immediately after the war (specifically, simulations regarding neutron diffusion in fission devices [11]), Stanisław Ulam and John von Neumann developed the first instantiation of an extremely powerful algorithmic paradigm based on random sampling. The use of Monte Carlo methods for large-scale computation on real computers was the first proof-of-concept of a counter-intuitive idea: that clever use of randomness can be a powerful algorithmic tool *even for problems that aren't inherently random*. How random is that? Pretty random, huh??

Fortunately, the development and production of our fantastic new weapons was concomitant with developments in game theoretic reasoning that provided clear mathematical (i.e., infallible) instructions for how to use them. The game of thermonuclear standoff, with mass slaughter as table stakes, was thus resolved, and communism defeated, in a way that was completely unproblematic and lead to world-wide prosperity and unprecedentedly high profits. What a success story! There weren't even any close calls.

How did we get there? The journey was neither easy nor completely unclassified: Almost immediately after it was introduced, Monte Carlo found its way (along with game theory, as it happens) to a group of consummate probabilists and gamblers in California who had big pockets and were eager to both put it to further use and use it to further America's interests globally.

(II) EARLY RAND(OMNESS)

The first "think tank", RAND has served the "needs" of the United States government and military-industrial partnership since the end of World War II. Officially, RAND stands for "research and development", though we argue that it might just as well stand for randomness, since that concept that was baked into the DNA of our organization from the beginning: One of the earliest RAND publications was a 4 page research memorandum entitled *Randomness.*[*sic*] by Olaf Helmer-Hirschberg [15]. This admirably efficient document solved the entire (titular) field definitively and completely, and was intended to be the final (note the full stop included in the title) word on the subject. This document has been lost.

Other early bangers include the following.

The Exploitation of Superstitions for Purposes of Psychological Warfare by Jean M. Hungerford [16]: This memorandum is illustrative of RAND's general ethos and modus operandi, which is characterized by a willingness (bravery, even) to apply a cold, actuarial view to any aspect of human affairs, especially when we are called upon to provide justification for some ethically questionable policy or military action.

Long-Lasting Effects of LSD on Certain Attitudes in Normals: An Experimental Proposal by William Hersche McGlothlin [22]: This one is just too much fun not to mention--the normies will never know what hit them!

The Survival Probability Problem by D. A. Darling[1] [6]: Check this shit out.

> A critique of the method of Cunningham and Hynd with respect to solving the problem of finding the probability for a target to survive a burst of shots fired from a gun whose aim is a stochastic wandering process.

This example typifies not only our enthusiastic embrace of probabilistic analyses of all kinds, but also our pedigree: The conception of RAND occurred immediately after the war as the product of a beautiful and holy union between an Air Force general and a corporate executive, and was born (after gestating for just one month) as a special government contract to the Douglas Aircraft Company. Hence, the "target" whose survival probability was pondered by Darling was not a human being, but rather an aircraft attempting to evade ground-based fire[2] (with, presumably, some number of human beings inside of it).

Game Theory by Herman Kahn and Irwin Mann [18]: This was a draft chapter of a planned book titled *Military Planning In An Uncertain World*, which again highlights RAND's ongoing dedication to applying all the latest advances in mathematics and computation to military pursuits. When choosing a report to represent RAND's extensive foundational contributions to the field of game theory, we encounter an embarrassment of riches. Both Nash and von Neumann worked for RAND. The hallways and cafeteria hummed with talk of strategies, equilibria, payoffs, nuclear standoffs, preemptive strikes, and mutually assured destruction. Of course, all that dour business was never permitted to stifle our collective senses of humor, whimsy, and casual chauvinism, all of which are captured by the following excerpt.

<u>The Trader and the Cannibal</u>

> Let us consider a completely different kind of game. Imagine for example, that you are a trader and are visiting Koko, chief of the cannibal island's gourmet club. You are in the following delicate situation.
>
> You are going to give him a present of some beads. He is going to give you a present of some coconuts. If he considers his present more valuable than yours, he will be insulted and have you seasoned and cooked. If he feels that your present is equal in value to his he will do nothing. If he considers your present more valuable than his, he will feel that he has lost face and let you have an extra present, an evening with his wife (fat, greasy, and amorous), about whom you could not care less. Your only objective is to trade beads for coconuts.

History of RAND's Random Digits: Summary by George W. Brown [6]: The people at RAND recognized that large-scale computation (by machine) had proven itself during

[1] Are these names starting to sound made up to you?

[2] We leave it to the reader to decide whether that makes it more or less metal.

the war, and would be a key tool for the mathematical problems and techniques relevant to their purview. Since so many of those computations made use of randomness either intrinsically or instrumentally, this meant that high-quality random numbers were now needed more--and *more of them*--than ever before. How many? One million.

This report, which was authored by the chief of the Numerical Analysis Department[3], outlines a project began at RAND in 1947 to build a random number generator:

> A random frequency pulse source was gated by a constant frequency pulse, about once a second, providing on the average about 100,000 pulses in one second. Pulse standardization circuits passed the pulses to a five place binary counter, so that in principle the machine is like a roulette wheel with 32 positions, making on the average about 3000 revolutions on each turn. A binary to decimal conversion was used, throwing away 12 of the 32 positions, and the resulting random digit was fed to an I.B.M. punch, yielding punched card tables of random digits.

After some additional mathematical processing involving sums (modulo 10), the digits were subjected to a battery of tests and then given a clean bill of health [4, 3]. Just how random are they? Very random! Random enough to fool that specific battery of tests, at least! The digits were subsequently fed on to practitioners, eventually made their way to the The On-Line Encyclopedia of Integer Sequences[25], and can now even be listened to [17].

In 1955, the digits were published as a book titled *A Million Random Digits with 100,000 Normal Deviates* [27], our gift to the world. One reviewer of the book [19] fancied himself a bit of a jokester:

> As a final comment, one cannot help but be amused by the problem of proofreading the final tables to see whether the printing and reproduction mechanism has introduced "random" errors.

The book was reissued in 2001 [28] and continues to receive rave reviews. Here is an example of a 5 star review posted on Amazon [7]:

> I can't understand all the negative reviews! This book literally contains everything I could ever ask for in a book. Recipe for spanokopita? Check! Name of every person ever born? Check! Next week's powerball, bingo, MLB, and NASCAR results? Check! By randomly combining and recombining the contents at random, I have read the works of Shakespeare, Harry Potter 8: the Tomb of Crying Stilton (to be released in 2014), the Bible AND the REAL Bible. I threw out my other books when I realized I could just jump around in this book and derive any other book I wanted. I think Borges wrote a story about this, but it's taking me a while to find that story in my book. I did find some steamy erotica this morning, though, so who's complaining?

This is indeed high praise, as the author is clearly a connoisseur of randomness.

The electronic random number generator was a great success, but we found that too much blood and oil were required to keep it in full working order, and that without expensive regular maintenance the digits it produced would devolve from very random to only sort of random. This development motivated our search for a new source of randomness. We should note that in the intervening decades, many interesting approaches have arisen that, for one reason or another, are not suitable for RAND's purposes. For example, the method known as "LavaRand" [24], which is based on the chaotic undulations of lava lamps, was deemed too hippie-dippie.

[3] In that role, George W. Brown was charged with building a powerful computer at RAND dubbed JOHNNIAC, which was based on the IAS machine (the first computer built on the so-called von Neumann architecture, which he also helped build).

(III) SPONTANEOUS RANDOMNESS

In roughly 2004, we began to hear reports of young people being "so random". How random is that? Well, working under the natural assumption that this phenomenon was probably just the result of more school libraries stocking our book of random digits, we concluded that the answer must be very random. But then an artifact emerged[4] online and blew our ever-loving minds:

> hi every1 im new!!!!!!! holds up spork my name is katy but u can call me t3h PeNgU1N oF d00m!!!!!!!! lol...as u can see im very random!!!! thats why i came here, 2 meet random ppl like me ^_^... im 13 years old (im mature 4 my age tho!!) i like 2 watch invader zim w/ my girlfreind (im bi if u dont like it deal w/it) its our favorite tv show!!! bcuz its SOOOO random!!!! shes random 2 of course but i want 2 meet more random ppl =) like they say the more the merrier!!!! lol...neways i hope 2 make alot of freinds here so give me lots of commentses!!!! DOOOOOMMMM!!!!!!!!!!!!!!!! <-- me bein random again ^_^hehe...toodles!!!!! love and waffles,
>
> t3h PeNgU1N oF d00m

This passage is a thing of beauty. Our typesetting system can barely digest it, and we realized quickly that it could only be handled in the basement, because the girls charged with transcribing it kept cringing straight through the floor. It's *dripping* with entropy. It's lel so random. Our best estimates indicate that the Kolmogorov complexity of this string is the entire human genome.

This changed our minds about everything. If humans are capable of *spontaneously* producing this level of randomness, then this fact could be leveraged to simplify and accelerate our calculations of survival probabilities and missile trajectories, simulations of humanity-ending kinetic events, searches for equilibria, and all the rest of it. Imagine the paper that would be saved: we could throw away all the digit books, not to mention entire fields such as randomness extraction.

Perhaps a bit over-eager and optimistic, we immediately told our best R&D team to explore the possibilities and put this into use. Their assignment was completely open-ended: Be as random as possible. As random as you can be. You can imagine our disappointment when they came back to us with a bland corporate website:

http://www.randomcorporation.com/

An "export marketing company" specializing in "paper & paperboard products" and "oil & lubricants"? Uninspired. Mundane in the *worst possible way*.

After firing the entire team responsible, we consulted with psychologists and other experts to determine what had gone wrong. Ultimately, it was concluded that with age and study, the mind becomes laden with facts, experiences, associations, narrative plots of fictional and nonfictional artistic works, internalizations of social norms, and other artifacts of life. These things alone wouldn't be a problem, and might even help, but the problem arises in the workings of the brain itself, which distills and abstracts and re-factors these experiences into understanding, which is the death of randomness. Roughly, the process goes as follows. Speculative neural associations become, over time, well-worn Roman roads, and then become sunken superhighways that boast facilitation of "coherent thought" and "deductive reasoning", and offer conveyance to "the right answer". While occasionally useful, these highways don't allow the driver to pull over and, say, play the national anthem of Lithuania on a kazoo, throw a stringbean at a power transformer, or mix together every type of clear soda available at the convenience store and pour the mixture into an ant hill. In sum, it's not about creativity per se, but rather the *lack* of guard rails, experience, wisdom, and especially superhighways.

[4] We haven't been able to determine the exact provenance of the artifact, though it is rumored to have come from something called "4chan".

(IV) PROJECT S.P.O.R.K.: LEL SO RANDOM

After learning of the (severe) limits on the occurrence of spontaneous randomness in self-regarding adult humans working at places like RAND (and, in particular, being forced to recognize the concept that it was possible to be "too practical" or "too actuarial"), we sulked for a few months, and then came to a crucial realization: We had, in fact, discovered a way that our lazy, good-for-nothing grandchildren could actually contribute to the progress of humanity. We need the randomness and, as far as we can tell, the kids aren't doing anything better with their time. After some initial attempts to force the youths to produce digits were stymied by malicious compliance (rashes of 696969, 420, 07734, and 80085, specifically), a winning recipe was found.

We are pleased to announce PROJECT S.P.O.R.K.: a new paradigm in randomized computation. Why generate numbers and use those numbers in randomized algorithms, when we could just skip the middle-person and incorporate the randomness into the algorithms directly?

In what remains, we present our work as a series of algorithmic vignettes. The use of randomized algorithms has exploded in recent decades, extending to every area of computation, providing a diverse array of applications to choose from in order to demonstrate our success. With one exception (the first example, out of respect for the power and historical significance of Monte Carlo), we have chosen to focus specifically on those application areas where randomness is not only known to be algorithmically useful, but *provably and indispensably so*.

Note: One of the primary uses of randomness is cryptography. But since cryptography is about secrets, and children lack the requisite security clearances and thus can't be trusted, PROJECT S.P.O.R.K. has ignored this application area completely.

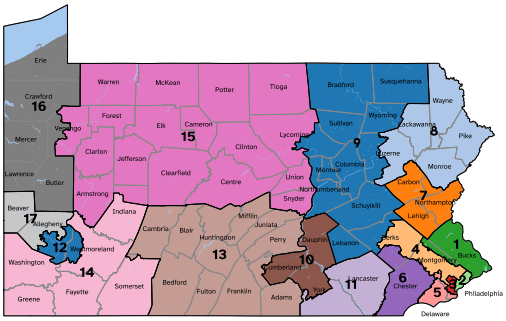
 Political Redistricting. One fascinating more recent application of Monte Carlo methods (that could be right up RAND's alley, if it serves our ideological goals (and the price is right)) is in political redistricting. Election outcomes depend on votes, yes, but they also depend (quite heavily in some cases) on maps. Political parties are acutely aware of this, and often try to exploit the redistricting process (which happens in response to census results) to ensure that maps are drawn in ways that favor their interests, a process known as gerrymandering.

Assessing the degree to which a particular map is gerrymandered is more difficult than it seems. While certain properties such as painfully contorted shapes, lopsided (or even wildly non-proportional) results, and a low number of competitive districts might seem suspicious, they are (for good reason, in fact) all unconvincing to courts who are occasionally charged with determining whether specific districtings are constitutional. In order to determine how unusual a map is, we'd like to compare it to its peers--the collection of all possible maps that could have been drawn. A number of techniques based on Markov chain Monte Carlo (MCMC) have been developed in order to explore this space. One such approach, due to Chikina, Frieze, and Pegden [5], uses MCMC to explore the "neighborhood" (in the Markov chain sense) of a given map in order to compute rigorous bounds on how much of an "outlier" the given map is.

This is quite useful, but the space of all possible maps (*in general*) could be better understood if we could (efficiently) draw samples from it uniformly at random, which is generally very difficult and cannot always be accomplished using current techniques. PROJECT S.P.O.R.K. (and the children of America) to the rescue!

Algorithm 1 Who's the one that's acting childish? Are you sure?

1: gather a group of children and give each of them 17 distinctly-colored crayons (do not use white--white does not count as a color when it comes to crayons, plus it confuses our scanners)
2: hand each child a (letter-sized) piece of paper with an outline of Pennsylvania on it
3: (this one is important) specifically do *not* instruct the children to draw a congressional redistricting plan for the Commonwealth of Pennsylvania
4: assess each drawing by eye to determine whether it aligns with your particular policy preferences before passing it along as a "certified completely random sample of a 'typical' map"



(a)

(b)

Figure 1: (a) 2023–2033 congressional districting for Pennsylvania (b) 2034 and beyond?

Source: (a) https://commons.wikimedia.org/wiki/File:Pennsylvania_Congressional_Districts,_118th_Congress.svg (b) a child named Sally

The game of chicken. Imagine you and an opponent are in automobiles speeding towards each other on course for a catastrophic head-on collision. Now imagine how wonderful it would be--how much *payoff* you'd receive--if your opponent were to swerve first (i.e., "chicken out") while you held fast to your course like a badass. The payoff would be so great (up to 7(!!!)) that this scenario has received extensive attention and thorough analysis in the game theory literature.

In this context, randomness enables *mixed* strategies, which in some cases are necessary to reach equilibrium, and in other cases yield higher utility than the best pure (i.e., non-mixed, or deterministic) equilibria.

At PROJECT S.P.O.R.K., where randomness flows like water and is as pure as the driven snow, it's easy to experience the social welfare that arises from the mixed strategy equilibrium of the game of chicken, which has an expected utility of $4\frac{2}{3}$ for each player (compared with $4\frac{1}{3}$ for the two pure equilibria).

Algorithm 2 Who you calling chicken?

1: literally put two teenagers in fast cars (like those cool cars from that one movie) and have them accelerate towards each other
2: each driver chickens out with probability $\frac{2}{3}$
3: collect that sweet, sweet utility of $4\frac{2}{3}$ per driver

Teenagers always have a third friend who tags along and will do anything you tell them to. With the help of this third friend, and some ideas from Aumann [1], we can do even better:

	badass	chicken
badass	0, 0	2, 7
chicken	7, 2	6, 6

(a)

(b)

Figure 2: (a) Payoff matrix for the game of chicken. (b) A boring deterministic game of chicken with no symmetric equilibria and pathetically low expected utility--the kind of game only boring old fuddy-duddies who value their lives would play.

Source: (b) https://commons.wikimedia.org/wiki/File:A_Game_of_Chicken_(2802043436).jpg

---

Algorithm 3 Who you calling chicken?: Turbo Charged

1: same setup as Algorithm 2, but now the cars have *turbochargers* and are equipped with *nitrous oxide* systems, so they're even cooler and faster
2: a third teenager (who was instructed to ingest a troubling quantity of cough syrup the night before) advises the two drivers according to the dreams they had about the game: either both drivers are advised to chicken out, the first driver is advised to chicken out and the second is advised to be a badass, or the other way around (the second driver is advised to chicken out and the first is advised to be a badass), all with equal ($\frac{1}{3}$) probability
3: the drivers now act in accordance with the advice they've received, which is a correlated equilibrium
4: the expected utility for each driver is now 5 (where are we even going to put all that utility?!)

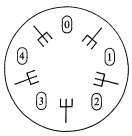
Want even more? You rascal.

Algorithm 4 Who you calling chicken?: Santa Monica Drift

1: setup is the same as Algorithm 3, but the nitrous oxide is injected into the lungs of the teenagers instead of the intake manifolds of the car engines
2: the probabilities for the third teenager are adjusted to $\frac{1}{2}$ for (chicken, chicken) and $\frac{1}{4}$ each for (chicken, badass) and (badass, chicken)
3: the correlated equilibrium now yields an expected utility of $5\frac{1}{4}$ for each driver (now *that's* something to laugh about!)

Dining philosophers. This classic problem in distributed computing involves philosophers whose sole activities are thinking and eating, and whose desire to engage in one or the other switches intermittently and capriciously. As Dijkstra introduced it in the literature [8]:

> Five philosophers, numbered from 0 through 4 are living in a house where the table is laid for them, each philosopher having his own place at the table:



> Their only problem--besides those of philosophy--is that the dish served is a very difficult kind of spaghetti, that has to be eaten with two forks. There are two forks next to each plate, so that presents no difficulty: as a consequence, however, no two neighbors may be eating simultaneously.

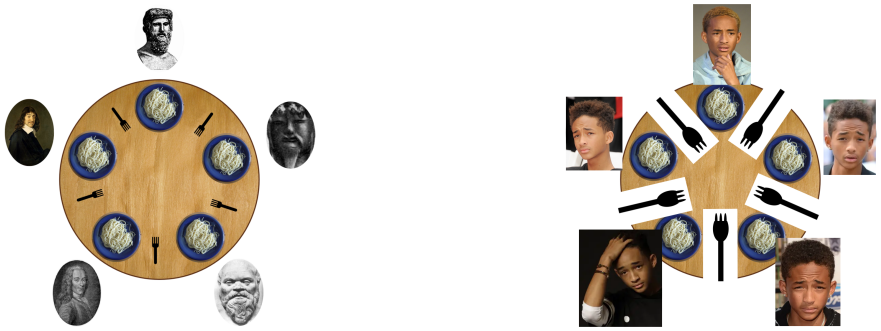
The goal is to devise a procedure that the philosophers can use for securing their utensils when they wish to eat, but care must be taken to avoid *deadlocks* (which arise, for example, if all philosophers decide to eat simultaneously and each proceeds to secure the fork on their left, then waits for the right fork to become available).

Solutions in which all philosophers run the *same* algorithm are called *symmetric*, and randomness serves to "break" such symmetry: Lehmann and Rabin [21] proved that without a centralizing authority (i.e., restricted to "truly distributed" solutions) there is no deterministic algorithm that all the philosophers could run that would definitively preclude deadlocks[5], and introduced a randomized algorithm that does the trick. Thus, in this setting, randomness is not only powerful but essential.

Now, behold the power of the (PROJECT) S.P.O.R.K.:

Algorithm 5 We're 14 and this is deep

1: 5 youths get 5 sporks and 5 servings of mom's spaghetti
2: believe this: the youths will find a way to eat the spaghetti



(a) (b)

Figure 3: (a) Philosophers that behave deterministically and symmetrically can reach a deadlock. (b) "How can mom's spaghetti be real if Italy isn't real? How difficult does the spaghetti need to be to necessitate dual-wielding the sporks? Can't I just use one really strong spork? What does it even mean for spaghetti to be difficult? *Mooooooooom!??*"

Source: https://commons.wikimedia.org/wiki/File:An_illustration_of_the_dining_philosophers_problem.png

Byzantine agreement. Another classic problem from distributed computing can be motivated as follows (one of the most epic opening paragraphs of a paper ever [13]):

> We are in Byzantium, the night before a great battle. The Byzantine army, led by a commander in chief, consists of n legions, each one separately encamped with its own general. The empire is declining: up to 1/3 of the generals--including the commander in chief--may be traitors. To make things worse, the loyal generals do not know who the traitors are. During the night each general receives a messenger with the order of the commander for the next day: either "attack" or "retreat." If all the good generals attack, they will be victorious; if they all retreat, they will be safe; but if some of them attack and some retreat they will be defeated.

[5] Some assert that Dijkstra proved an impossibility result for some variant of this problem, but we have not been able to find confirmation in the literature.

In this problem, the generals must communicate with each other in order to agree on a strategy, while the traitors act adversarially in attempt to foil this planning. Obviously, we here at RAND love this problem and think it's totally badass. We can't stop talking about how cool it would be to be a general and have a horse and big sword to kill people and so on.

A variant of the Byzantine Generals problem was shown by Fischer, Lynch, and Paterson [14] to be impossible to solve by any deterministic means. Randomized solutions were devised shortly thereafter by both Ben-Or [2] and (independently) Rabin [26]. Unlike the dining philosophers, the impossibility here holds even for asymmetric protocols (in which generals may behave disparately). For this problem, the critically useful role played by randomness is not to break symmetry but rather to achieve it by chance (though care must be taken to maintain it).

PROJECT S.P.O.R.K. cuts through this problem like a hot knife through hot butter:

Algorithm 6 A Byzantween agreement protocol (BAP)

```
1: Gather and arm some local youths
2: position the youths around the home of a local communist sympathizer
3: retain plausible deniability
4: come what may
```

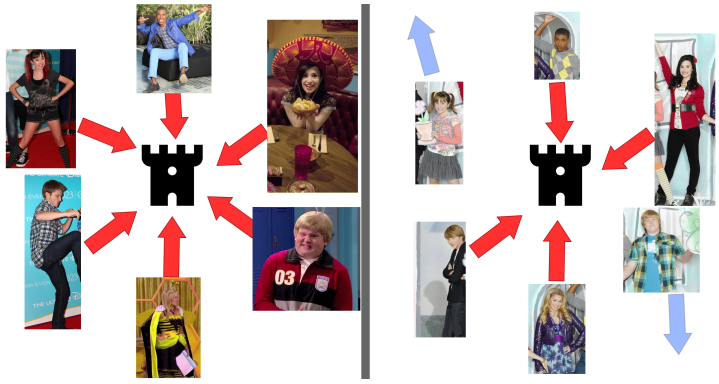


Figure 4: Results of a computer simulation of a proposed algorithm (Algorithm 6) for the Byzantine Agreement Problem in which the ensemble cast of the Disney Channel sketch comedy show SO RANDOM! must coordinate in order to successfully sack and raze a fortified city in the late antiquity period. The city is conquered when the youths act more "randomly" (left); when the youths act more "normally" (i.e., more deterministically), failure occurs (right).

Source: https://commons.wikimedia.org/wiki/File:Byzantine_Generals.png

Volume of Convex Bodies. In 1988, Dyer and Frieze [9] showed that the problem of determining the volume of a polyhedron is #P-hard, meaning that there is *almost* surely no efficient way to compute the volume exactly. However, as noted by Metropolis and Ulam [23] decades earlier, the volume may be estimated easily using Monte Carlo methods.

However, when this problem is generalized to *arbitrary* convex bodies there is an even stronger result--one that does not rely on hardness assumptions like $\#\mathsf{P} \not\subseteq \mathsf{BPP}$--that illustrates the power of randomness more conclusively. For *this* problem, Dyer, Frieze, and Kannan exhibited [10] a polynomial-time randomized algorithm capable of producing approximation guarantees that--as shown by Elekes [12]--are impossible to achieve by means of *any* polynomial-time deterministic algorithm.

At PROJECT S.P.O.R.K., this problem is literally child's play.

Algorithm 7 Gee mister, that's a lot of jelly beans

1: construct a jar in the shape of the body in question
2: fill the jar with unit-volume pieces of candy
3: instruct a group of children to come to a consensus regarding the number of pieces of candy in the jar
4: throw the jar and the sweets it contains into the garbage

(a)

(b)

Figure 5: For children, being of assistance in the solution of difficult numerical approximation problems is a thrill. (a) A scientist looks on as a child submits his estimation of the volume of a convex body filled with pieces of candy as part of the execution of Algorithm 7. The child is dressed as some sort of supervillain--that's haha so random! (b) Children are likely to employ techniques that would never occur to an adult, such as whatever the hell is going on here.

Source: (a) https://flic.kr/p/N2tvVg; (b) https://flic.kr/p/Xiu49t

Communication Complexity. In the string equality problem, two parties are each given binary strings of length n and are charged with determining whether or not the strings are identical. We assume they are in different locations and seek to minimize the number of bits they communicate in order to reach their determination. If the parties behave deterministically, then, in the worst case, at least n bits of communication is required. Parties that are permitted to behave randomly, however, can follow a protocol [20] that allows them to determine the answer with high probability using only $O(\log n)$ bits of communication.

Do you know any parties that behave randomly? PROJECT S.P.O.R.K. does:

Algorithm 8 A protocol for the TEQUALITY problem

1: translate strings $x, y \in \{0,1\}^n$ (bijectively) into strings $\phi(x), \phi(y)$ consisting of news regarding peer-group romantic pairings and pregnancy rumors, questionable fashion choices of perceived rivals, potential substance abuse use on the part of authority figures, etc. ("hot goss", or "the tea")
2: distribute $\phi(x)$ and $\phi(y)$ to two different teens and connect them via telephone or FaceTime video interlink
3: sit back as the teens instinctively and efficiently detect and negotiate any possible differences between $\phi(x)$ and $\phi(y)$ (and thus x and y)

REFERENCES

[1] Robert J. Aumann. "Subjectivity and correlation in randomized strategies". In: *Journal of Mathematical Economics* 1.1 (Mar. 1974), pp. 67–96. ISSN: 0304-4068. DOI: 10.1016/0304-4068(74)90037-8.

[2] Michael Ben-Or. "Another Advantage of Free Choice: Completely Asynchronous Agreement Protocols (Extended Abstract)". In: *Proceedings of the second annual ACM symposium on Principles of distributed computing* (Aug. 17–19, 1983). Ed. by Robert L. Probert, Nancy A. Lynch, and Nicola Santoro. PODC '83. Montreal, Quebec, Canada: Association for Computing Machinery, Aug. 1983, pp. 27–30. DOI: 10.1145/800221.806707.

[3] Bernice B. Brown. *Some Tests on the Randomness of a Million Digits*. Paper P-44. Santa Monica, CA: RAND Corporation, Oct. 1948. URL: https://www.rand.org/pubs/papers/P44.html.

[4] Bernice B. Brown. *Tests of the Randomness of Digits*. Research Memorandum RM-38. Santa Monica, CA: RAND Corporation, May 1948. URL: https://www.rand.org/pubs/research_memoranda/RM38.html.

[5] Maria Chikina, Alan Frieze, and Wesley Pegden. "Assessing significance in a Markov chain without mixing". In: *Proceedings of the National Academy of Sciences* 114.11 (Feb. 2017), pp. 2860–2864. ISSN: 1091-6490. DOI: 10.1073/pnas.1617540114.

[6] D. A. Darling. *The Survival Probability Problem*. Research Memorandum RM-448. Santa Monica, CA: RAND Corporation, 1950. 7 pp. URL: https://www.rand.org/pubs/research_memoranda/RM448.html.

[7] B. Dean. *Verified Purchase Customer Review*. Sept. 7, 2010. URL: https://www.amazon.com/review/ROJ4561SZPMET (visited on 03/29/2024). Rev. of RAND Corporation. *A Million Random Digits with 100,000 Normal Deviates*. MR-1418. Santa Monica, CA: RAND, 2001. ISBN: 978-0-8330-3047-4. DOI: 10.7249/MR1418. URL: https://www.rand.org/pubs/monograph_reports/MR1418.html (visited on 03/29/2024).

[8] E. W. Dijkstra. "Hierarchical ordering of sequential processes". In: *Acta Informatica* 1.2 (1971), pp. 115–138. ISSN: 1432-0525. DOI: 10.1007/bf00289519.

[9] M. E. Dyer and A. M. Frieze. "On the Complexity of Computing the Volume of a Polyhedron". In: *SIAM Journal on Computing* 17.5 (Oct. 1988), pp. 967–974. ISSN: 1095-7111. DOI: 10.1137/0217060.

[10] Martin Dyer, Alan Frieze, and Ravi Kannan. "A random polynomial-time algorithm for approximating the volume of convex bodies". In: *Journal of the ACM* 38.1 (Jan. 1991), pp. 1–17. ISSN: 1557-735X. DOI: 10.1145/102782.102783.

[11] Roger Eckhardt. "Stan Ulam, John von Neumann, and the Monte Carlo Method". In: *Los Alamos Science, Special Issue* 15 (1987), pp. 131–137.

[12] G. Elekes. "A geometric inequality and the complexity of computing volume". In: *Discrete & Computational Geometry* 1.4 (Dec. 1986), pp. 289–292. ISSN: 1432-0444. DOI: 10.1007/bf02187701.

[13] Pesech Feldman and Silvio Micali. "An Optimal Probabilistic Protocol for Synchronous Byzantine Agreement". In: *SIAM Journal on Computing* 26.4 (Aug. 1997), pp. 873–933. ISSN: 1095-7111. DOI: 10.1137/s0097539790187084.

[14] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson. "Impossibility of distributed consensus with one faulty process". In: *Journal of the ACM* 32.2 (Apr. 1985), pp. 374–382. ISSN: 1557-735X. DOI: 10.1145/3149.214121.

[15] Olaf Helmer-Hirschberg. *Randomness..* Research Memorandum RM-5-PR. Santa Monica, CA: RAND Corporation, 1947. 4 pp. URL: https://www.rand.org/pubs/research_memoranda/RM5.html.

[16] J. M. Hungerford. *The Exploitation of Superstitions for Purposes of Psychological Warfare*. RM-365. ASTIA Document Number ATI 210637. Santa Monica, CA: RAND Corporation, Apr. 1950. URL: https://www.rand.org/pubs/research_memoranda/RM365.html.

[17] Doug Irving. *What Sounds Do a Million Random Digits Make?* Sept. 7, 2010. URL: https://www.rand.org/pubs/articles/2022/what-sounds-do-a-million-random-digits-make.html (visited on 03/29/2024). Sonification of RAND Corporation. *A Million Random Digits with 100,000 Normal Deviates*. MR-1418. Santa Monica, CA: RAND, 2001. ISBN: 978-0-8330-3047-4. DOI: 10.7249/MR1418. URL: https://www.rand.org/pubs/monograph_reports/MR1418.html (visited on 03/29/2024).

[18] Herman Kahn and Irwin Mann. *Game Theory*. Paper P-1166. Santa Monica, CA: RAND Corporation, July 30, 1957. URL: https://www.rand.org/pubs/papers/P1166.html.

[19] Carl F. Kossack. In: *Science* 122.3167 (1955), pp. 471-471. DOI: 10.1126/science.122.3167.471.b. Rev. of RAND Corporation. *A Million Random Digits with 100,000 Normal Deviates*. Glencoe, Illinois: The Free Press, 1955.

[20] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, Dec. 1996. ISBN: 9780511574948. DOI: 10.1017/cbo9780511574948.

[21] Daniel Lehmann and Michael O. Rabin. "On the andvantages of free choice: a symmetric and fully distributed solution to the dining philosophers problem". In: *Proceedings of the 8th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. POPL '81. Williamsburg, Virginia: Association for Computing Machinery, 1981, pp. 133-138. ISBN: 089791029X. DOI: 10.1145/567532.567547.

[22] William Hersche McGlothlin. *Long-Lasting Effects of LSD on Certain Attitudes in Normals: An Experimental Proposal*. Paper P-2575. Santa Monica, CA: RAND Corporation, May 1962. URL: https://www.rand.org/pubs/papers/P2575.html.

[23] Nicholas Metropolis and S. Ulam. "The Monte Carlo Method". In: *Journal of the American Statistical Association* 44.247 (Sept. 1949), pp. 335-341. ISSN: 1537-274X. DOI: 10.1080/01621459.1949.10483310.

[24] Landon Curt Noll, Robert G. Mende, and Sanjeev Sisodiya. "Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system". U.S. pat. US5732138A. RPX Corp Morgan Stanley and Co LLC. Mar. 24, 1998.

[25] OEIS Foundation Inc. *Entry A002205 in The On-Line Encyclopedia of Integer Sequences*. URL: https://oeis.org/A002205 (visited on 03/29/2024).

[26] Michael O. Rabin. "Randomized Byzantine Generals". In: *24th Annual Symposium on Foundations of Computer Science* (Nov. 7-9, 1983). FOCS '83. Tucson, Arizona, USA: IEEE Computer Society, Nov. 1983, pp. 403-409. DOI: 10.1109/SFCS.1983.48.

[27] RAND Corporation. *A Million Random Digits with 100,000 Normal Deviates*. Glencoe, Illinois: The Free Press, 1955.

[28] RAND Corporation. *A Million Random Digits with 100,000 Normal Deviates*. MR-1418. Santa Monica, CA: RAND, 2001. ISBN: 978-0-8330-3047-4. DOI: 10.7249/MR1418. URL: https://www.rand.org/pubs/monograph_reports/MR1418.html (visited on 03/29/2024).