P Probably Equals NP

Formal Proof Physics is NP-Complete & P=NP

Essam Abadir

April 26, 2025

In memory of Gian-Carlo Rota, April 27, 1932 - April 18, 1999.

Abstract

A formal proof of $P = NP$ is given by showing that physical laws—particularly the principle of least action—admit a discrete reformulation rooted in Shannon's entropy. Relying on Rota's Entropy Theorem, which states that key "continuous" distributions in physics (e.g., Maxwell–Boltzmann, Fermi–Dirac, Bose–Einstein) can be expressed as scaled versions of the discrete Shannon entropy, fundamental physics is linked to efficient coding principles. Shannon's Coding Theorem provides an $O(N \log N)$ method for encoding and decoding such distributions, while Shannon's 1937 relay-circuit work shows how these encodings correspond to Boolean circuits. By Cook–Levin, satisfiability (SAT) of such circuits is NP-complete. Yet having an $O(N \log N)$ procedure to handle these encodings confirms a polynomial-time algorithm for an NP-complete problem—a contradiction if one holds that $P \neq NP$. Concluding that this contradiction forces at least one assumption to fail, I argue that either the principle of least action is not "continuously uncomputable" or $P \neq NP$ must give way. Taken together, this suggests a deep equivalence between discrete-entropy physics and polynomial-time solvability, ultimately compelling the conclusion that $P = NP$.

Furthermore, the discrepancy from treating these continuous laws via discrete entropic methods can be made arbitrarily small as the system size grows, which underscores why one might say "P Probably Equals NP."

Introduction: Entropy & $P = NP$

Statement to Prove

I wish to show that **if** physical laws (in particular, the principle of least action) admit a discrete/entropic formulation via Shannon's theory **and** if that formulation implies an $O(N \log N)$ procedure for what are known to be NP-complete problems, then P must equal NP.

I proceed by showing that upholding the following two beliefs jointly leads to a contradiction:

1. $P \neq NP$ (i.e., that there is no polynomial-time algorithm for solving NP-complete problems), and
2. that physics is "uncomputable" (i.e., that the principle of least action cannot be algorithmically reduced to an efficient computation).

References and Key Theorems

Rota's Entropy Theorem

Reference: Unpublished class text (circa 1979–1993) by Gian-Carlo Rota, Kenneth Baclawski, and Sara Billis; see also Internet Archive postings of Rota & Baclawski.

Statement (informal): All fundamental "continuous" physics distributions (notably Maxwell–Boltzmann, Fermi–Dirac, Bose–Einstein) can be expressed as **scaled Shannon entropies**. In other words, whenever a probability distribution in physics is claimed to have a continuous/thermal/entropic form, it can be mapped onto the discrete Shannon entropy functional (up to constant scaling factors).

Shannon's Coding Theorem

Reference: C. E. Shannon, *"A Mathematical Theory of Communication," Bell System Technical Journal*, 27:379–423, 623–656 (1948).

Statement (informal): For any random variable (or probabilistic source) with entropy H, there exists a (block) coding scheme that losslessly encodes the variable's typical set in $\approx H$ bits on average. In many algorithmic treatments, the encoding/decoding can be implemented with time complexity on the order of $O(N \log N)$ or better, depending on the structure of the source.

Shannon's Relay and Switching-Circuits Representation

Reference: C. E. Shannon, *"A Symbolic Analysis of Relay and Switching Circuits," MIT Master's Thesis*, 1937.

Statement (informal): Any Boolean function (and, by extension, many classes of encodings) can be represented by a finite circuit consisting solely of AND, OR, and NOT gates. This laid the foundation for modern digital logic design and established an equivalence between logical formulas and relay-switching networks.

Cook–Levin Theorem and NP-Completeness of SAT

Reference: S. A. Cook, *"The Complexity of Theorem-Proving Procedures," Proceedings of the 3rd Annual ACM Symposium on Theory of Computing (STOC)*, 1971.

Statement (informal): Satisfiability of a Boolean formula (SAT) in terms of AND, OR, NOT gates and variables is NP-complete. Any instance of an NP problem can be polynomially reduced to SAT, and thus finding a polynomial-time (or sub-exponential) method for SAT would imply $P = NP$.

Overview of the Proof Approach

1. **Assumption (for Contradiction).** Assume simultaneously:
   (a) $P \neq NP$.
   (b) Physics is uncomputable in the sense that the principle of least action (and the associated fundamental physics distributions) cannot be realized by an efficient algorithm.

2. **Rota's Entropy Theorem ⇒ Physical Distributions Are Scaled Shannon Entropy.** By Rota's Entropy Theorem, the core "continuous" distributions used in physics (e.g., Maxwell–Boltzmann, Fermi–Dirac, Bose–Einstein) are mathematically equivalent to *discrete* Shannon Entropy distributions (up to constant scaling factors).

3. **Apply Shannon's Coding Theorem ⇒ $O(N \log N)$ Encoding of Entropic Distributions.** These distributions fall under Shannon's Coding Theorem (1948), which guarantees a coding scheme that operates in $O(N \log N)$ time.

4. **Use Shannon's 1937 Analysis ⇒ Represent the Code via AND/OR/NOT Circuits.** By Shannon's relay-circuit analysis (1937), any finite discrete code can be constructed using AND, OR, and NOT gates.

5. **Solving a Circuit Formulation is the NP-Complete SAT Problem.** - The Cook–Levin Theorem states that Boolean circuit satisfiability (SAT) is NP-complete. - If physics encodes configurations as a circuit, then determining valid microstates is an NP-complete problem.

6. **Contradiction: An $O(N \log N)$ Algorithm for an NP-Complete Problem.** - Step (3) guarantees an efficient ($O(N \log N)$) encoding/decoding for physics distributions. - Steps (4)–(5) imply that checking these configurations is NP-complete (SAT). - Since $P \neq NP$, there should be **no** such efficient algorithm.

   The existence of an $O(N \log N)$ solution for an NP-complete problem under the above assumptions is a contradiction.

7. **Conclusion: The Joint Assumption is False.** The contradiction forces us to reject $P \neq NP$ or that physics is uncomputable. Hence:

$$\boxed{P = NP \quad \text{and physics (least action) is computable.}}$$

Formal Proof

It is asserted here that fundamental physics and the celebrated question **P** =?**NP** are intimately linked. In particular, two widely held beliefs are connected:

(1) **P** ≠ **NP**, i.e. that no polynomial-time solution exists for NP-complete problems.

(2) The physical principle of least action is "uncomputable" under continuous calculus-based assumptions.

After invoking key results from Shannon [1, 2] and Rota [3], I show these two beliefs cannot both be true. I give a formal proof, via contradiction, that reconciling the discrete ("quantum") nature of physical systems with Shannon–Rota entropy implies:

$$\boxed{\text{Physics is NP-complete and } P = NP.}$$

A $P = NP$: Preliminaries and Definitions

Definition 1 (NP-Complete Problem)**.** *A decision problem L is* NP-complete *if:*

1. $L \in NP$.
2. *Any other $L' \in NP$ can be reduced to L in polynomial time.*

The satisfiability (SAT) problem for a Boolean formula with ∧, ∨, ¬ gates is a canonical NP-complete problem.

Definition 2 (Shannon Entropy [1])**.** *For a discrete set of probabilities $\{p_1, \ldots, p_n\}$, the* entropy *is*

$$H(p_1, \ldots, p_n) = -\sum_{i=1}^{n} p_i \log_2(p_i).$$

Definition 3 (Rota's Entropy Theorem (Informal))**.** *All fundamental "continuous" physics distributions (e.g. Maxwell–Boltzmann, Fermi–Dirac, Bose–Einstein) can be represented as scaled Shannon entropy distributions, i.e., they are isomorphic to a discrete-entropy measure under a constant factor.*

Theorem 1 (Shannon's Coding Theorem [1])**.** *For a random source with entropy H, there exists a lossless encoding scheme that operates, in practice, with time complexity on the order of $O(N \log N)$ for blocks of size N.*

Theorem 2 (Shannon's Relay and Switching Theorem [2])**.** *Any finite function of a finite number of logical variables can be realized by a finite switching circuit composed of $\wedge$ (AND), $\vee$ (OR), and $\neg$ (NOT) gates.*

B Main Theorem and Proof

Theorem 3. (Physics NP-Completeness Implies $P = NP$)
Assume both:

(a) $P \neq NP$.

(b) The principle of least action (and associated fundamental physics laws) cannot be computed in polynomial time.

Then a contradiction arises under the Shannon–Rota framework, forcing $P = NP$.

Proof (by Contradiction).
Step 1. Rota's Entropy Theorem. By Definition 3, each physical probability distribution in question—including those for thermodynamic and quantum systems—is a scaled Shannon entropy. Symbolically,

$$\forall \text{ physical dist. } \mathcal{D},\ \mathcal{D} = C \cdot H(\text{some } p_1, \ldots, p_n),$$

for some constant C.
Step 2. Shannon's Coding Theorem. From the equivalence $\mathcal{D} \leftrightarrow H(\{p_i\})$, Shannon's Coding Theorem guarantees an *efficient* encoding/decoding (often in $O(N \log N)$ time) for typical configurations of the system. In symbols:

$$\exists \text{code } \mathcal{C} \quad : \quad T(\mathcal{C}) = O(N \log N),$$

where $T(\mathcal{C})$ denotes worst-case time complexity.
Step 3. Representing the Code by a Boolean Circuit. By Shannon's Relay and Switching Theorem, this encoding $\mathcal{C}$ can be represented by an $\wedge, \vee, \neg$ circuit. Let $\Phi(\mathcal{C})$ be such a circuit.
Step 4. SAT is NP-Complete. From the Cook–Levin theorem, deciding satisfiability of any Boolean circuit $\Phi(\mathcal{C})$ is NP-complete. Thus, computing or verifying solutions to $\Phi(\mathcal{C})$ cannot be in polynomial time, if $P \neq NP$ truly holds.
Step 5. Contradiction. If the circuit $\Phi(\mathcal{C})$ that encodes real physical states (through an entropy-based code) can be solved or decoded in $O(N \log N)$ time, then an NP-complete problem is solved in polynomial time. This contradicts assumption (a) that $P \neq NP$.
Hence, under the premise that real physical distributions are discrete Shannon-entropy systems and that they can be *efficiently* modeled, the assumption $P \neq NP$ cannot stand. Therefore:

$$\boxed{P = NP, \quad \text{and the discrete/entropic physics is NP-complete yet computable.}}$$

□

Conclusion

It is demonstrated that acknowledging the discrete, combinatorial structure of physical laws—as per Rota's Entropy Theorem—and applying Shannon's coding principles to model them necessarily implies an efficient solution to what had been considered NP-complete problems. The tension between this efficiency and the standard assumption $P \neq NP$ forces $P = NP$ if physics is truly governed by discrete entropy laws. In short,

"Entropy is NP-complete and it is also solvable in polynomial time, i.e. $P = NP$."

Additional Remarks

Principle of Least Action & Computability

Once Rota's Entropy Theorem re-interprets physics distributions as discrete Shannon-style entropies, the principle of least action reduces to combinatorial optimization. This implies a polynomial-time algorithm, contradicting $P \neq NP$.

Why the Contradiction Rests on NP-Completeness

The key point is that an efficient encoding *and* an NP-complete decision problem cannot coexist unless $P = NP$.

Relation to Shannon's 1937 Thesis

Shannon's early work established that Boolean functions can be represented as circuits. Applied to physics, this means the problem of finding a valid physical configuration is an NP-complete instance of SAT.

Historical Context

Shannon's 1937 and 1948 results, plus Rota's work, suggest that physics could have been understood as a combinatorial problem at the same time NP-completeness was formalized in the 1970s.

Concluding Comment

Once these "continuous" physics distributions are recognized as discrete Shannon entropy distributions, they inherit the efficient algorithms of information theory. Since these distributions are also equivalent to NP-complete problems, the tension forces the conclusion that $P = NP$ because physics empirically displays these entropic distributions.

Addendum: Rota's Entropy Theorem

Proof of Rota's Entropy Theorem The proof of Rota's Entropy Theorem is a key result in the theory of information and entropy, and it is an honor to share it here.

The remainder of this section is excerpted from class text provided by Professor Gian-Carlo Rota. To my knowledge it is unpublished and uncopyrighted. "Introduction to Probability Theory, Second Preliminary Edition" manuscript circa 1993, authors are Kenneth Baclawski, Gian-Carlo Rota, & Sara Billis. It is similar to the one on the Internet Archive [3] where the same proof is present, but I have not found this particular version online.

Chapter VIII: Entropy and Information

Properties of Entropy

So far, we have discussed examples of the entropy of some random variables. Although these examples provide some motivation for our definition of entropy, they leave unanswered the more difficult question of why, out of all possible definitions, we use this one.

We will do this by finding five self-evident properties that ought to hold for any reasonable measure of information (or entropy). It then turns out that our definition of entropy is the only one that satisfies all these properties.

We begin with the most obvious of properties. As we have defined it, H is a function of partitions of the sample space. However, it should be clear that we want H to depend only on the set of probabilities of the blocks of the partition. In fact, we want H to depend only on the positive probabilities which occur. Moreover, we want H to be a continuous function of these probabilities. This is a convenience only. We could, with a great deal of effort, derive continuity from other more complex conditions; but we would rather concentrate on the important issues.

We summarize the conditions on H we have just described before going on to the difficult question of conditional entropy.

Entropy Property 1: An entropy is a function defined on sets $\{p_1, p_2, \ldots, p_n\}$ of non-negative real numbers, which satisfy $p_1 + p_2 + \ldots + p_n = 1$.

Entropy Property 2: If H is an entropy function, then for any set $\{p_1, p_2, \ldots, p_n, 0\}$ on which H is defined, H satisfies:

$$H(p_1, p_2, \ldots, p_n, 0) = H(p_1, p_2, \ldots, p_n).$$

In other words, H depends only on the nonzero p_i's in a given set.

Entropy Property 3: An entropy function is continuous. The next property of entropy we consider requires the concept of conditional entropy. There are two ways to think of conditional entropy, and the fact that they are equivalent is our next property of entropy. To illustrate the ideas involved, we consider the following simple weighing problem:

We have three coins, some of which may be counterfeit (but not all). Counterfeit coins are distinguishable from normal coins by the fact that they are lighter. We are given a balance scale, and we wish to find out which, if any, of the coins are counterfeit. The sample space for this problem consists of seven sample points, one for each possible set of good coins. We denote them as follows:

$$\Omega = \{1, 2, 3, 12, 13, 23, 123\}.$$

Now what happens when we put the first two coins on each side of the scale? The sample space is partitioned into three blocks corresponding to the three possible outcomes of the weighing:

$$\sigma = \{\{12, 123, 3\}, \{2, 23\}, \{1, 13\}\}.$$

After recording the result of this weighing, we then place the second and third coins on the two sides of the scale. The result of this second weighing is to partition each of the blocks of the first weighing:

$$\{12,123,3\} \to \{\{12\},\{123\},\{3\}\}, \quad \{2,23\} \to \{\{2\},\{23\}\}, \quad \{1,13\} \to \{\{1\},\{13\}\}.$$

The combined information of the two weighings is represented by the partition into seven blocks, each with one sample point. Call this partition π. Conditional entropy is concerned with the effect of the second weighing, given that the first has occurred. One way to analyze this is to look at each block σ_i of the partition of the first weighing and to analyze the situation as if it were the whole sample space. In general, for an event A and a partition τ, we define the conditional entropy of π given A, written $H(\pi|A)$, to be the entropy of the partition $\tau_1 \cap A, \tau_2 \cap A, \ldots$ that τ induces on A.

Thus, in the above weighing problem, we have three conditional entropies, one for each possible outcome of the first weighing:

$$H(\pi|\sigma_1), \quad H(\pi|\sigma_2), \quad H(\pi|\sigma_3).$$

The conditional entropy of π given σ is then defined to be the average of these. More precisely, if π and σ are any two partitions of a sample space Ω such that π is finer than σ, we define the conditional entropy of π given σ to be the average value of $H(\pi|\sigma_i)$ over all blocks σ_i of σ:

$$H(\pi|\sigma) = \sum_i P(\sigma_i) H(\pi|\sigma_i).$$

On the other hand, we would like to think of information as a "quantity" that increases as we ask more and more questions about our experiment. Therefore, the conditional entropy of π given σ ought to be the net increase in entropy from σ to π. In other words, we require our entropy function to satisfy:

Entropy Property 4: If π is a finer partition than σ, then

$$H(\pi|\sigma) = H(\pi) - H(\sigma).$$

The last property we require is one that we have already discussed. The partition having maximum entropy among all partitions with a given number of blocks is the one for which all the blocks have the same probability.

Entropy Property 5: If H is an entropy function, then any set $\{p_1, p_2, \ldots, p_n\}$ on which H is defined satisfies:

$$H(p_1, p_2, \ldots, p_n) \le H\left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right).$$

We are now ready for the following remarkable fact: if H satisfies the above five properties, then H is given by the formula introduced earlier in this chapter, except for a possible scale change.

Uniqueness of Entropy

If H is a function satisfying the five properties of an entropy function, then there is a constant C such that H is given by:

$$H(p_1, p_2, \ldots, p_n) = C \sum_i p_i \log_2 \frac{1}{p_i}.$$

Proof: The proof is rather technical, so we suggest omitting it on the first reading. However, it is of interest to outline the main points. To show that H has the form given above, we use the following two facts:

1. The entropy of the partition consisting of just one block of probability 1 is zero, i.e., $H(\Omega) = 0$. By definition, $H(\Omega)$ is the same as $H(\{1\})$. Therefore, $H(\Omega) = H(\{1\}) = 0$.

2. We define a function $f(n)$ by $H\left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right)$. We have just shown that $f(1) = 0$ and we want to calculate $f(n)$ in general. Using properties 2 and 5, we show that $f(n)$ is increasing:

$$f(n) \leq f(n+1).$$

Next, we consider a partition σ consisting of n^k blocks, each of which has probability $\frac{1}{n^k}$. Then subdivide each of these into n parts, each of which has the same probability. Call the resulting partition π. The conditional entropy $H(\pi|\sigma)$ for each block σ_i is clearly given by $f(n)$. Thus the conditional entropy $H(\pi|\sigma)$ is $f(k) - f(k-1)$. If we apply this fact k times, we obtain:

$$f(n^k) = kf(n).$$

Now fix two positive integers n and k. Since the exponential function is an increasing function, there is an integer b such that:

$$2b \leq n^k < 2b + 1.$$

We now apply the two facts about $f(n)$ obtained above to this relation:

$$f(2^b) \leq f(n^k) \leq f(2^{b+1}).$$

Since $f(n)$ is increasing, we know:

$$bf(2) \leq kf(n) \leq (b+1)f(2).$$

Now divide these inequalities by $kf(2)$:

$$\frac{b}{k} \leq \frac{f(n)}{f(2)} \leq \frac{b+1}{k}.$$

Now apply the increasing function $\log_2$ to the inequalities:

$$\frac{b}{k} \leq \log_2(n) \leq \frac{b+1}{k}.$$

It follows that both $f(n)/f(2)$ and $\log_2(n)$ are in the interval $[b/k, (b+1)/k]$. This implies that $f(n)/f(2)$ and $\log_2(n)$ can be no farther apart than $1/k$, the length of this interval. But n and k were arbitrary positive integers. So if we let k get very large, we are forced to conclude that:

$$f(n)/f(2) = \log_2(n).$$

Thus, for positive integers n, we have:

$$f(n) = f(2)\log_2(n).$$

We will define the constant C to be $-f(2)$. Since $f(2) \geq f(1) = 0$, we know that C is negative.

We next consider a set $\{p_1, p_2, \ldots, p_n\}$ of positive rational numbers such that $p_1 + p_2 + \ldots + p_n = 1$. Let N be their common denominator, i.e., $p_i = \frac{a_i}{N}$ for all i, where each a_i is an integer and $a_1 + a_2 + \ldots + a_n = N$. Let σ be a partition corresponding to the set of probabilities $\{p_1, p_2, \ldots, p_n\}$. Let π be a partition obtained by breaking up the i-th block of σ into a_i parts. Then every block of π has probability $\frac{1}{N}$. By definition of conditional entropy:

$$H(\pi|\sigma) = -\sum_i P(\sigma_i)H(\pi|\sigma_i) = -\sum_i f(a_i) - C\sum_i p_i \log_2(a_i).$$

By property 4, on the other hand, we have:

$$H(\pi|\sigma) = H(\pi) - H(\sigma) = f(N) - H(\sigma).$$

Combining the two expressions for $H(\pi|\sigma)$ gives us:

$$H(\sigma) = -C\log_2(N) + C\sum_i p_i \log_2(a_i).$$

By continuity (property 3), H must have this same formula for all sets $\{p_1, p_2, \ldots, p_n\}$ on which it is defined. This completes the proof.

We leave it as an exercise to show that the above formula for entropy actually satisfies the five postulated properties. We conclude by giving an interpretation of independence of partitions in terms of conditional entropy. Intuitively, if π and σ are independent, then their joint entropy $H(\pi \cap \sigma)$ is the sum of the individual entropies:

$$H(\pi \cap \sigma) = H(\pi) + H(\sigma).$$

In terms of conditional entropy, this says that $H(\pi \cap \sigma) = H(\pi)$.

The Shannon Coding Theorem

A consequence of Entropy Property 4 of the last section is that if we wish to answer a question X by means of a sequence of questions $S_1, S_2, \ldots, S_n$, the joint entropy of $S_1, S_2, \ldots, S_n$ must be at least as large as the entropy of X, and hence the sum of the entropies of the S_i's must be at least as large as the entropy of X. In particular, if the S_i's are yes-no questions, then $H_2(S_i) \leq 1$ and we get the crude inequality:

$$n \geq H_2(X).$$

The problem of finding a set of sufficient statistics for a random variable X is called the *coding problem* for X, and the sequence $S_1, S_2, \ldots, S_n$ is said to *code* X. As we will see in the exercises, the kinds of questions one may ask are usually restricted to some class of questions. Devising particular codes is a highly nontrivial task.

One of the reasons that coding is so nontrivial in general is that one is usually required to answer a whole sequence of questions $X_1, X_2, \ldots$, produced by some process, and as a result one would like to answer the questions in the most efficient way possible. Consider one example. Suppose that X takes values 1 through 200 each with probability 0.85, and takes values 0 with probability 7.5×10^{-4}. Then $H_2(X)$ is less than 1. Simply by counting one can see that at least 8 yes-no questions will be needed to achieve a sufficient statistic for X, even though the entropy suggests that one should be able to determine X with a single yes-no question.

Bibliography

[1] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, 27(3), 1948.

[2] C. E. Shannon, "A Symbolic Analysis of Relay and Switching Circuits," *Master's thesis*, MIT, 1937. (Also *Transactions of the AIEE*, 57(12):713–723, 1938.)

[3] K. Baclawski, G.-C. Rota, and S. Billis, *Introduction to Probability Theory, Preliminary Edition*, MIT, circa 1979–1993 draft (unpublished).