Proof P = NP // Corrected Oversights

Jamell Ivan Samuels
N/A

doi: 10.20944/preprints202007.0588.v1

Proof P $\neq$ NP

J. I. Samuels

jamellsamuels13@imperial.ac.uk

Abstract

The P vs NP problem is a well known open problem in mathematics. In this paper I attempt to prove that $P \neq NP$ by establishing a basic groundwork from which I derive my proof.

1. *Counting*

In mathematics the two basic operations are counting and totalling.

Definition 1. Counting is the acting out of a method using a unit measure. Example there are a hive of bees, I count the bees using my unit measure | as ||||||.

Definition 2. Totalling is the explicit use of number to sum a count, I sum my count |||||| using the numerical system $1, 2, 3....$ as 6.

Counting and Totalling inhabit a region I shall call the Method Space M, which is an area used to categorise and derive operations.

Definition 3. A Method M is any operation or process used to solve a problem. In the Method Space, methods are represented as M(current operation, next variable), where $n \ \forall \ \mathbb{R}$ and $i \ \forall \ \mathbb{R}$.

Definition 4 Limit of Counting to 0.
The limit of counting to 0 $M(n, i) \lim_{i \to 0} M(1, 0)$
The limit of totalling to 0 $M(n + i_i, i_{i+1}) \lim_{i \to 0} M(n, 0)$

Definition 5 Limit of Counting to ∞.
The limit of counting to infinity $M(n, i) \lim_{i \to \infty} M(1, 1)$
The limit of totalling to infinity $M(n + i_i, i_{i+1}) \lim_{i \to \infty} M(\infty, \infty)$

Using slopes to measure the difference between counting and totalling .

$$\frac{d\Delta T}{d\Delta C} = \frac{M(\infty, \infty) - M(n, 0)}{M(1, 1) - M(1, 0)} = \frac{M(\infty, \infty)}{M(0, 1)} \equiv \frac{(\infty, \infty)}{(0, 1)} \tag{1.1}$$

And dividing to resolve the equation you obtain.

$$(1, \infty) \tag{1.2}$$

2000 *Mathematics Subject Classification* 68W01, 68Q01 (primary), 68Q17 (secondary).

Thereby establishing 0 as a non countable number.

2. *Checking and Solving*

Definition 6. Checking is the process where you assure that the solution you have gained is valid.

Definition 7. Solving is the process used to acquire a solution.

Lemma 2.1. *Your best solving method can not run faster than your best checking method therefore, Solving* $\lim \xrightarrow{Method}$ *Checking.*

3. *Probability*

Probability can be stated as the likelihood that an event will occur. It is counted as the number of times an event will occur out of the total number of possible events. Any probability outside the boundaries of [0,1] does not exist on the plane of probability and therefore can only be interpreted for it's meaning rather than stated as an absolute definition of chance.

3.1. *Planes and Cylinders of Probability*

Probabilities must remain on the same plane and in truth they can only be added or subtracted. The use of multiplication can be considered the resolution of a stack of probabilities (and therefore multiple events) that exist on separate planes which you have resolved to one. Therefore we define a probability plane and cylinder as.

Definition 8. A probability plane is the area in which a probability exists or acts upon. Probabilities may exist on separate planes, but they must be resolved to act on one.

Definition 9. A probability cylinder is a stack of multiple planes, a cylinder must be resolved to act on one plane.

3.2. *The Fundamental Probability - Derivation of Given*

The most fundamental probability to calculate is the probability that event(B) is not going to happen given that event(A) has or is going to happen. All other probabilities that can be calculated fundamentally rely on this and although can be calculated in other ways, risk losing the information contained within. Henceforth we are going to state the probabilities in the order that they are calculated.

$$P(!B|A) = P(A) - P(B) \tag{3.1}$$

$$P(B|A) = P(A) - P(!B|A) \tag{3.2}$$

3.3. *Simultaneous Occurrences*

Probabilities must exist on a single plane and as a single event. Any event with more than one possible outcome can be considered a simultaneous event. When resolving multiple events to a single plane or events in a single plane, the probabilities must be fully counted to not lose or create inconsistencies in the information contained.

3.3.1. *Probability of* $\wedge$

If you recall the standard probability definition of "and" is $P(A \wedge B) = P(A) \times P(B)$.

$$P(A) = 1;\ P(B) = \frac{1}{9}$$

$$1 \times \frac{1}{9} = \frac{1}{9}$$

Therefore.

$$P(A \wedge B) = P(B)$$

And although the example given is very simple, you can henceforth state that the event $P(A \wedge B)$ is not dependent on $P(A)$. And ergo $P(A \wedge B)$ is fundamentally contradictory. This can be stated because the use of multiplication is the loss of information. For example. $[5 + 5 + 5 + 5 + 5]$ contains more information than 5×5. It is therefore better to state that $P(A \wedge B) = P(A|B) \times P(B|A)$. And to treat all "and" statements as a matrix containing the possible events.

$$P(A{\wedge}B) = \begin{bmatrix} P(A|B) \\ P(B|A) \end{bmatrix} \tag{3.3}$$

3.3.2. *Probability of* $\vee$

Although the probability of $(A \vee B)$ can be considered a fundamental probability as it can be calculated as $P(A) + P(B)$, it is actually one of the derived probabilities as it has more than one possible outcome and therefore must be resolved as a single event.

$$P(!A{\vee}!B) = \begin{bmatrix} P(!A|B) \\ P(!B|A) \end{bmatrix} \tag{3.4}$$

$$P(!A{\vee}!B) = P(A \wedge B) + P(!A{\wedge}!B) \tag{3.5}$$

$$P(A \vee B) = 1 - P(!A{\vee}!B) \tag{3.6}$$

4. *Non-Polynomial Time Problems*

Any Non-Polynomial problem is the result of two distinct and independent variables. Which I shall refer to as the value and the order.

- Value v is the property of a variable that makes it distinct.
- Order o is the particular arrangement of properties in manner that is transferable to a base 1 count.

An example of this is Sudoku, where the values are placed in a particular order to solve the problem. Any problem S which can be described in this manner is what we shall consider a Non-Polynomial problem for the sake of this argument.

Definition 10. Polynomial Problems

$$\begin{aligned} S &= f(v, o) \\ o &= f(v) \\ S &= f(v) \\ P(S) &= P(A) \end{aligned}$$

Definition 11. Non-Polynomial Problems

$$\begin{aligned} S &= f(v, o) \\ o &\neq f(v) \\ S &\neq f(v) \\ P(S) &= P(B|A) \end{aligned}$$

4.1. *Proof the Problem is exponential*

It was previously stated that non-polynomial problems are dependent on v and o. When solving a non-polynomial problem it is typical to say a solution is found when both events A and B occur, $P(A \wedge B)$. However in truth, a solution is found when given event A, B has occurred which can only be written as $P(B|A)$. However, when deriving a solution $P(!B|A)$ must be used.

4.1.1. $P(!B|A)$ We are now going to derive the algorithm as given event A has occurred, event B will not happen. Where A is the probability that the order is correct B is the probability the value was correct and n is length of the problem i.e. the number of possible solutions .

$$P(A) = 1 \tag{4.1}$$

$$P(B) = \frac{1}{n^2}$$

$$P(!B|A)_{Algorithm} = P(A) - P(B)$$

– For an algorithm to be correct the probability of finding a solution must equal 1.

$$P(S)_{Algorithm} = 1. \tag{4.2}$$

– For $n^2 \times n^2$ required solutions the probability of finding the correct solution is.

$$P(S)_{Algorithm} = (P(A) - P(B))^{n^2 \times n^2} = 1^{n^2 \times n^2} \tag{4.3}$$

Using the binomial identity

$$\sum_{k}^{n^4} \binom{n^4}{k} A^{n^4-k} B^k = 1. \tag{4.4}$$

– Where k represents a single step
– This can be expanded as

$$\binom{n^4}{0} A^{n^4} B^0 - \binom{n^4}{k} A^{n^4-k} B^k + \binom{n^4}{2k} A^{n^4-2k} B^{2k} ... + \binom{n^4}{n^4} A^0 B^{n^4} = 1 \tag{4.5}$$

- As B is negative, every $(k+1)th$ step is impossible and therefore incalculable. We therefore square every step.

$$\binom{n^4}{0}^2 A^{2n^4}B^0 + \binom{n^4}{2k}^2 A^{2n^4-2k}B^{2k} + ...\binom{n^4}{n^4}^2 A^0B^{2n^4} = 1 \tag{4.6}$$

- Substituting $B^k = \frac{1}{n^2}^k$ and $A = 1$

$$\binom{n^4}{0}^2 \left(\frac{1}{n^2}\right)^0 + \binom{n^4}{2k}^2 \left(\frac{1}{n^2}\right)^{2k} + ...\binom{n^4}{n^4}^2 \left(\frac{1}{n^2}\right)^{n^4} = 1 \tag{4.7}$$

- 0 can not be counted. And therefore the expression for the algorithm becomes

$$\binom{n^4}{2k}^2 \left(\frac{1}{n^2}\right)^{2k} + \binom{n^4}{4k}^2 \left(\frac{1}{n^2}\right)^{4k} + ...\binom{n^4}{n^4}^2 \left(\frac{1}{n^2}\right)^{2n^4} = 1. \tag{4.8}$$

4.1.2. *Limit Of Probability* If we are to assume that the solution we are checking is correct, the probability that the value and the order are correct are both 1.

$$P(A)_{Check} = 1 \tag{4.9}$$

$$P(B)_{Check} = 1 \tag{4.10}$$

$$P(A \wedge B)_{Check} = 1 \tag{4.11}$$

$$P(A|B)_{Check} = 1 \tag{4.12}$$

A property of a check is that it is self proving. Given the nature of the problem, the probability of the check can be defined as $P(B|A)$. The probability of a check can also be stated as $P(A \wedge B)$, as an efficient polynomial checking algorithm will only total. Removing the co-efficients from the previously stated algorithm as these represent a non-determinacy and taking just the pure calculation.

$$P(!B|A)_{Algorithm} = \left(\frac{1}{n^2}\right)^2 + \left(\frac{1}{n^2}\right)^4 + \left(\frac{1}{n^2}\right)^6 + ...\left(\frac{1}{n^2}\right)^{2n^4} = 1 \tag{4.13}$$

The limit of the sum is.

$$\Sigma P(!B|A)_{Algorithm} \rightarrow \lim 1. \tag{4.14}$$

And therefore for non-polynomial problems, as the probability that any polynomial algorithm can correctly solve the problem can never equal 1, there is no deterministic algorithm that can solve the problem in P time.

4.1.3. *Proof of Exponential Nature*

Proof. Recalling that the relationship between $P(A)$,$P(B)$ and n is

$$\Pi_{k=0}^{n^4} P(A)^{n^4-k}P(B)^k = \frac{1}{n^2}^{\Sigma_{k=0}^{n^4} 2k}$$

Let the left side be checking and let it be said that $P(A) = P(B) = 1$

$$1 = \left(\tfrac{1}{n^2}\right)^{\sum_0^{n^4} 2k}$$

$$ln|1| = -\sum_0^{n^4} 4kln|n|$$

$$0 = -\sum_0^{n^2} 4kln|n|$$

$$0 = \frac{-\sum_0^{n^4} 4k}{n}$$

$$e^0 = e^{\frac{-\Sigma_0^{n^4} 4k}{n}}$$
$$1 = e^{\frac{-\Sigma_0^{n^4} 4k}{n}}$$

Thereby proving that the problem is naturally exponential. This can than be calculated as,

The exponential series formula is given as

$$\Sigma_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + ...$$

The sum of the exponential term 4k where the region of k is $= (0, n^4)$

$$\Sigma_{k=0}^{n^4} 4k = 2n^4(n^4+1) = 2n^8 + 2n^4$$
$$e^{-\Sigma_{k=0}^{n^4} 4k . \frac{1}{n}} = e^{-2n^7-2n^3}$$
$$\Sigma_{k=0}^{\infty} \frac{-2n^7-2n^3}{k!} = 0 \text{ for } n \geq 2$$

As previously proven the natural limits for k are $(1, \infty)$, (1.2).

$$\Sigma_{k=0}^{\infty} \frac{-2n^7-2n^3}{k!} = 1 + \Sigma_{k=1}^{\infty} \frac{-2n^7-2n^3}{k!}$$
$$\Sigma_{k=1}^{\infty} \frac{-2n^7-2n^3}{k!} = -1 \text{ for } n \geq 2$$

$$1 = -1.$$

As the modulus of $|-1| = 1$ we can conclude the problem is correctly solved, however, as $-1 \neq 1$ we can also conclude that $NP \neq P$ as it does not exist on the same plane. This is true for all problems of length greater or equal to 2 i.e 3SAT, Sudoku etc. Note if we were to disregard 1.2 and state that the region of k is $(0, \infty)$ we would arrive at

$$1 = 0.$$

Which shows every exponential solution as wrong, however still proves that $NP \neq P$. □

4.2. *The Argument of Intent*

Although we have mathematically proven that $NP \neq P$ we are going to present a slightly allegorical argument to demonstrate the practical implications of our proof. $P(!B|A)$ represents an algorithm with the intention of getting it wrong. It does however, manage to get it right. $P(B|A)$ however, which is equal to $(1 - \frac{8}{9})$ can never get it right as although it is correct (it equals $\frac{1}{9}$) it is incorrect as it's expansion is in respect to $\frac{8}{9}$. As the algorithm that intends to get it right, can not get it right, and the algorithm that intends to get it wrong can, we can therefore state that there is no single intentional method that can solve this problem and can therefore conclude that no efficient polynomial solution exists.

4.3. *Lower Bound*

In the Clay Mathematics Article [**1**] it was stated that a counting argument gave no clues as to what the lower bound for solving an exponential problem is.

Proof.

The general expression for an algorithm is

$$\int \frac{1}{n^2}^{2k} dk$$
$$\frac{e^{2kln|\frac{1}{n^2}|}}{2ln|\frac{1}{n^2}|} = P$$

Where P is an arbitrary constant representing probability

$$\frac{-4k}{n}e^{2kln|\frac{1}{n^2}|} = 2P \times \frac{-2}{n}$$

$$\frac{-4k}{n}e^{-4kln|n|} = \frac{-4P}{n}$$

$$k = Pe^{4kln|n|}$$

$$k = P\left(e^{4n^4ln|n|} - e^{4ln|n|}\right)$$

$$k = P\left(n^{4n^4} - n^4\right)$$

$$k = \mathcal{O}(n^{4n^4})$$

Taking the integral in the form of

$$\frac{\frac{1}{n^2}^{2k}}{2log(\frac{1}{n^2})} = C$$

$$n^{-4k} = 2Clog(\frac{1}{n^2})$$

$$-4kn^{-4k-1} = \frac{-4C}{n}$$

$$k = Cn^{-1}n^{4k+1}$$

$$k = Cn^{4k}$$

$$k = C\left(n^{4n^4}\right)$$

$$k = \mathcal{O}(n^{4n^4})$$

The following derivations were established as multi-step limits i.e taking k as n^4.
If we were to apply a single step limit i.e $k = 1$ we would establish the lower bound as.

$$k = \mathcal{O}(n^4)$$

□

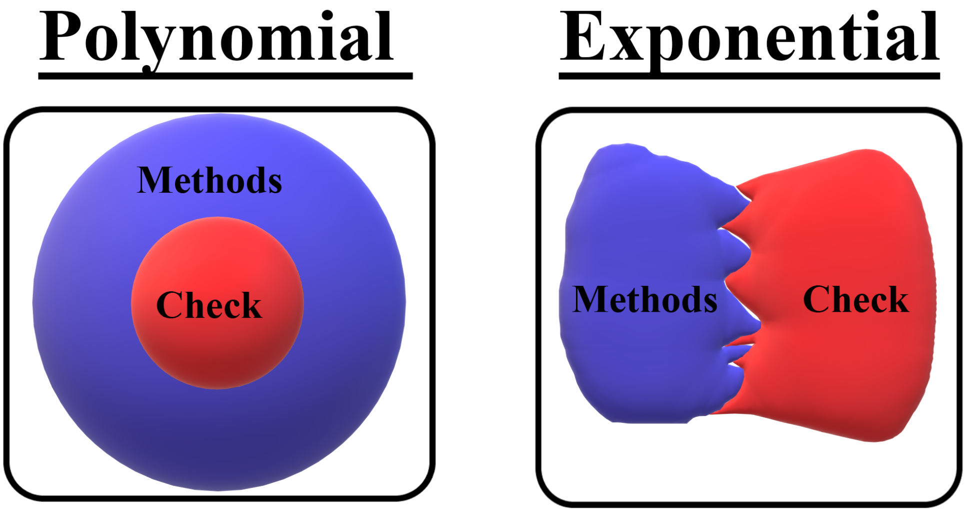

FIGURE 1. *'Method Space' for polynomial and non-polynomial problems.*

References

1. Cook. A.S, "The P versus NP Problem" *Clay Mathematics*,
2. Stewart. I, "The Great Mathematical Problems" page 203-214 *Profile Books*,