THE PRIME NUMBER THEOREM, OR THE INCOMPRESSIBILITY OF THE PRIMES

Aidan Rocke
aidanrocke@gmail.com

February 16, 2021

ABSTRACT

From an information-theoretic analysis of the prime number theorem, we may deduce that prime number sequences are incompressible. By pushing this analysis further, we may conclude that while a single counter-example may be used to prove that the Riemann Hypothesis is false, we can't prove that the Riemann Hypothesis is true.

1 An information-theoretic derivation of the prime number theorem

If we know nothing about the primes in the worst case we may assume that each prime number less than or equal to N is drawn uniformly from $[1, N]$. So our source of primes is:

$$X \sim U([1, N]) \tag{1}$$

where $H(X) = \ln(N)$ is the Shannon entropy of the uniform distribution.

Now, given a strictly increasing integer sequence of length N, $U_N = \{u_i\}_{i=1}^N \in [1, N]^N$ we may define the *prime encoding* of U_N as the binary sequence $X_N = \{x_i\}_{i=1}^N$ where $x_i = 1$ if u_i is prime and $x_i = 0$ otherwise. With no prior knowledge, given that each integer is either prime or not prime, we have 2^N possible prime encodings(i.e. arrangements of the primes) in $[1, N] \subset \mathbb{N}$.

If there are $\pi(N)$ primes less than or equal to N then the average number of bits per arrangement gives us the average amount of information gained from correctly identifying each prime number in U_N as:

$$S_c = \frac{\log_2(2^N)}{\pi(N)} = \frac{N}{\pi(N)} \tag{2}$$

Furthermore, if we assume a maximum entropy distribution over the primes then we would expect that each prime is drawn from a uniform distribution as in (1) so we would have:

$$S_c = \frac{N}{\pi(N)} \sim \ln(N) \tag{3}$$

and this implies:

$$\pi(N) \sim \frac{N}{\ln(N)} \tag{4}$$

which happens to be equivalent to the prime number theorem.

2 The Shannon source coding theorem, and the compressibility of the primes

By the Shannon source coding theorem, we may also infer that $\pi(N)$ primes can't be compressed into fewer than $\pi(N) \cdot \ln(N)$ bits so this result tells us something about the incompressibility of the primes. Specifically, what we gained from this analysis is the understanding that prime number sequences behave like statistically incompressible sequences.

Now, if $X_N = \{x_i\}_{i=1}^N$ is a prime encoding of length N we must asymptotically obtain:

$$\mathbb{E}[K(X_N)] \sim \pi(N) \cdot \ln(N) \sim N \tag{5}$$

where $K(\cdot)$ is the Kolmogorov Complexity.

We shall now proceed by contradiction. If there is an algorithmic method which may be used to prove that the Riemann Hypothesis is true then we may construct a program of finite length *zeta* which takes as input a strictly increasing integer sequence of length N, U_N, and outputs a prime encoding of length N, X_N, by correctly deciding whether each element in that sequence is prime or not.

By the hypothesis on *zeta* and U_N, an application of the Minimum Description Length principle yields:

$$\mathbb{E}[K(\ \textit{zeta} \circ U_N)] \leq -\ln(P(X_N|\textit{zeta} \circ U_N)) + \text{Cst} = \text{Cst} \tag{6}$$

since $P(X_N|\textit{zeta} \circ U_N) = 1.0$, as there exists a prime encoding $X_N \in \{0,1\}^N$ such that $\textit{zeta} \circ U_N = X_N$. So we must also have:

$$\mathbb{E}[K(\ \textit{zeta} \circ U_N)] = \mathbb{E}[K(X_N)] \tag{7}$$

However, X_N is known to be incompressible due to (5) so we have:

$$\lim_{N\to\infty} \frac{\mathbb{E}[K(\ \textit{zeta} \circ U_N)]}{\mathbb{E}[K(X_N)]} \sim \lim_{N\to\infty} \frac{\text{Cst}}{N} = 0 \tag{8}$$

which is a contradiction.

From this analysis we may conclude that while a single counter-example may be used to prove that the Riemann Hypothesis is false, we can't prove that the Riemann Hypothesis is true.

References

[1] Dániel Schumayer and David A. W. Hutchinson. Physics of the Riemann Hypothesis. Arxiv. 2011.

[2] Doron Zagier. Newman's short proof of the Prime Number Theorem. The American Mathematical Monthly, Vol. 104, No. 8 (Oct., 1997), pp. 705-708

[3] Peter D. Grünwald. The Minimum Description Length Principle . MIT Press. 2007.

[4] M. Li and P. Vit´anyi. An Introduction to Kolmogorov Complexity and Its Applications. Graduate Texts in Computer Science. Springer. 1997.

[5] Peter Shor. Shannon's noiseless coding theorem. lecture notes. 2010.