



Nervous System: The Entropy of Wordle

BY DAVID KALAT

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have been with us longer than we remember.

Nervous System is a monthly series that approaches issues of data privacy and cyber security from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.

Thanks to Josh Wardle's viral wordgame Wordle, millions of people now start (or end) their day by actively engaging in a gamified version of Information Theory. 70-odd years ago, an eccentric genius named Claude Shannon set out to solve the ancient problem of signal versus noise. Shannon rethought the entire problem from a novel direction, embracing noise fearlessly with the confidence that a new approach to encoding information would be largely impervious to it. He invented the "bit," the raw atom of modern information science, and thereby launched the modern era of computing. And, as Wordle fans will appreciate, his 1948 paper *A Mathematical Theory of Communication* makes for a highly satisfying game.

Generations of engineers had been tackling the conundrum of signal versus noise for ages. At one end of a chain of communication was a sender, who sent a message. Various forms of interference corrupted that message on its path, until a degraded version was received at the other end. Throughout history, the common assumption had been that the solution lay, somehow, in the right way of boosting the signal or filtering the noise, to cause the received message to be as close to the original as possible. This approach never really worked, however, because methods of amplification tended to amplify the noise as well, while methods of filtration tended to filter out the signal.

There are many ways in which Shannon's 1948 paper *A Mathematical Theory of Communication* was revolutionary. Among its groundbreaking insights was his realization that some degree of noisy interference will always be a factor in communication. Rather than attempting a quixotic effort to prevent this inevitability, Shannon proceeded to measure it, quantify it, and address it.

To this end he turned his attention to the smallest possible message—a single coin flip. It either comes up heads or tails. He called this irreducible atom of information a binary unit, or "bit" (Shannon credited the term to mathematician John Tukey).

Two things arose from his concept of the bit as the fundamental building block of information. The first is that the influence of noise on a single bit is only significant to the degree that the interference risks causing the wrong value for the bit to be received. Noisy interference that does not risk “flipping the bit” to the wrong value is therefore irrelevant (a discovery that rendered much of the fight over signal versus noise moot).

Secondly, the informational *value* of a given bit varies, depending on how much of the message can be known or guessed without it. For example, if a bit can be likened to a coin flip, not every coin is equally weighted between heads and tails. If the coin is a trick coin that always turns up heads, or turns up heads more frequently than tails, then the informational “surprise” that comes from each coin flip is less than would be true for a fair coin.

Another innovation in Shannon’s theory of communication was the notion that the first step is the *selection* of a message—that is, the selection of a message out of all possible messages represents a probabilistic act that can be quantified mathematically. And, when that message is a form of human communication, not every utterance is equally likely. Language and meaning impose rules and customs that greatly constrain what messages are possible, much less probable.

The ability to probabilistically guess some messages over others means that there is a quantifiable way of measuring the “surprise” factor of any given message. Shannon called this “entropy,” inspired by the use of the term in physics. Entropy is a measurement of the amount of information in a variable. The less easy it is to probabilistically deduce that information, the more entropy the variable has—or put another way, the more surprising the information is, the more its entropy.

Consider Wordle, an online word-guessing game created by programmer Josh Wardle as a gift to his girlfriend. Each day, the Wordle algorithm selects a five-letter English word as the secret word for that day’s game, and players have six guesses to figure it out. Each guess must itself be a valid English word, and the system informs players which if any of the letters in their guesses are correct (these are highlighted in green), which appear in the answer word but in a different position (these are highlighted in yellow), and which do not appear at all (these are grayed out). In this way the game is like a cross between Hangman and Mastermind.

Importantly, the letters that constitute the English alphabet are not distributed equally in the language. Some occur more frequently, some letter combinations occur more frequently, some letter combinations are known to cluster in particular places in a word, and so on. These limitations mean that even when the Wordle game begins and no guesses have yet been made, the player already knows some essential facts that greatly reduce its entropy. Each successive guess further reduces the entropy. Part of the game’s appeal lies in the pleasurable “eureka” feeling when a player can sense the range of possible guesses collapse down to a select few, and the solution to the puzzle emerges.

Wordle players experience this process intuitively, but information scientists can quantify informational entropy to precisely calculate the bandwidth needed to transmit a given signal, how densely a given piece of information can be compressed, or how resilient a certain message will be to interference.

This article was originally published in Legaltech News on April 4, 2022. The opinions expressed in this publication are those of the individual author and do not represent the opinions of BRG or its other employees and affiliates. The information provided in the publication is not intended to and does not render legal, accounting, tax, or other professional advice or services, and no client relationship is established with BRG by making any information available in this publication, or from you transmitting an email or other message to us. None of the information contained herein should be used as a substitute for consultation with competent advisors.