CyTe - Infosec Technology Newsletter

Wordle es uno de los juegos más populares de los últimos meses y se han propuesto una gran cantidad de estrategias para resolver el juego. El objetivo de este texto es el de explorar una estrategia óptima para el juego desde el punto de vista de teoría de información y explicar de dónde vienen algunos de los conceptos más importantes en criptografía como es el de la entropía.

Encontrando una estrategia para wordle utilizando teoría de la información

por José Darío Flórez

La teoría de la información es el área de la informática que se centra en el estudio de la transmisión y cuantificación de la información. La teoría de la información da algunos de los conceptos sobre los cuales se basa la criptografía y se ha utilizado para estudiar cómo cuantificar si un sistema es seguro contra atacantes; un análisis más profundo de cómo se utilizan estos conceptos para definir un cifrario perfectamente seguro y de cómo el concepto de entropía nos permite probar la seguridad de sistemas criptográficos se puede encontrar en (https://www.cyte.co/blog/NL_5-Desciframiento-Forzado).
Como se informó al comienzo, Wordle es un juego que ha ganado mucha popularidad en los últimos meses, alcanzando un número de 3 millones de jugadores diarios (https://www.mcgilltribune.com/a-e/wordles-popularity-is-no-puzzle-02152022/). Para este artículo nos referiremos a el juego de wordle en español encontrado en (https://wordle.danielfrg.com/). El objetivo del juego es descubrir la palabra de 5 letras del día, las reglas del juego son las siguientes:

- Empezamos con una cuadrícula de 6x5 como la de la siguiente imagen:

Figura 1: Cuadricula inicial de wordle

- Escribimos una palabra de cinco letras en la primera fila y como resultado el juego indica por cada letra colocada tres posibilidades: la letra se pondrá en gris si esa letra no aparece en la palabra escondida, la letra tomará un color amarillo si la letra aparece en la palabra pero no en la posición en la que la colocamos, la letra tomará un color verde si está en la palabra oculta en la posición que la colocamos. En un juego al escribir la palabra "pares.[es] posible obtener el siguiente resultado:

Figura 2: Primer palabra

- De acuerdo con estas pistas, el jugador sigue escribiendo palabras hasta que encuentre la palabra escondida o hasta completar seis intentos sin éxito y perder el juego. Por ejemplo:

Figura 3: Juego completo

La idea del juego es encontrar la palabra del día con el menor número de intentos posible. En este artículo presentaremos una solución óptima desde el punto de vista de la teoría de la información y propondremos un programa que aplica esta heurística para resolver el problema.

Teoría de la información

Para poder hablar de la solución óptima del problema de wordle tenemos que definir un concepto fundamental en la teoría de la información que es el de la entropía.
El concepto de la entropía intuitivamente se puede pensar como la cantidad de información que da una observación sobre cierto experimento con diferentes resultados. Para definir este concepto mas formalmente supongamos que tenemos un experimento sobre una variable aleatoria X, en la cual hay n posibles resultados; decimos que si una observación sobre este experimento reduce el espacio de posibles soluciones a la mitad, entonces tenemos 1 bit de información; por otro lado, si reduce este a espacio a la cuarta parte, se tendrán 2 bits de información, si lo reduce a la octava parte se tendrán 3 bits, y así sucesivamente. En el caso específico del wordle, un ejemplo podría ser la observación de que una palabra tiene la letra 'a'; si solo la mitad de las palabras tuvieran la letra a, podríamos decir que esta observación nos da 1 bit de información. De manera que, en este ejemplo, si una letra que es poco probable que aparezca dentro de un palabra de cinco letras en el diccionario español, aparece habríamos ganado mucha información. En ese sentido, el cálculo de la probabilidad p(x), de que una letra aparezca dentro de la palabra, se convierte en una parte de la heurística muy útil para encontrar la solución.
Con está definición intuitiva podemos ver que la información en número de bits $I(x)$ que nos da la observación x está relacionada con la probabilidad de que ocurra de la siguiente manera:

$$(\frac{1}{2})^I = p(x)$$

dónde $p(x)$ es la probabilidad de que el evento x ocurra. Al usar un poco de álgebra y reescribir esta ecuación obtenemos que la información es:

$$I(x) = -log_2(p(x))$$

Ahora bien, algo que nos gustaría poder calcular es el valor esperado de cuánta información ganamos al jugar una palabra específica en wordle. Esta es una expresión estándar de valor esperado dada por:

$$E[Informacion] = \sum_x p(x) * I(x)$$

donde $p(x)$ es la probabilidad de que ocurra el evento x y $I(x)$ es el valor del evento x. Recordando lo que habíamos mencionado antes el valor de una palabra, en este caso el número de información que esperamos obtener, está dado por $I(x) = -log_2(p(x))$. Por lo que obtenemos el siguiente resultado:

$$E[Informacion(x)] = -\sum_x p(x) * log_2(p(x))$$

Este valor es el valor conocido y formalizado por Claude Shannon en 1948 que se conoce como entropía. Este valor se interpreta como la información esperada que obtenemos al identificar el resultado del experimento X.
En nuestro ejemplo, si el experimento es jugar la palabra "Habla", el valor $E[Informacion]$ nos dice cual es la información en promedio que ganaríamos al jugar esta palabra.

Algoritmo para jugar wordle.

Ahora que hemos visto el concepto de entropía y vimos que se puede interpretar como el número promedio de información que se obtiene al jugar esta palabra podemos proponer

un algoritmo que informe cuál es la mejor palabra inicial y a partir de ahí dependiendo del resultado de esta palabra, dé pistas para saber con palabra deberíamos continuar.

Primer paso, encontrar la mejor palabra para iniciar

Lo primero por hacer es obtener una lista completa de todas las palabras de 5 letras en español; en este caso vamos a utilizar la lista tomada de (https://www.listasdepalabras.es/palabras5letras.html). Ahora recordemos nuestra ecuación de entropía al jugar una palabra en específico:

$$E[Informacion] = -\sum_{x} p(x) * log_2(p(x))$$

Lo primero que tenemos que ver es cuál es el espacio de resultados posibles de el experimento, es decir todas las maneras diferentes en las que puede resultar jugar una palabra. Esto serán las 3^5 posibilidades diferentes de combinaciones de gris, amarillo y verde para cada una de las letras. Para cada una de estas posibilidades tendremos que $p(x)$ será $\frac{\text{Numero de palabras restantes después de descartar}}{\text{Numero de palabras totales}}$. Por ejemplo si jugamos la palabra "comer " y revisamos el posible resultado del experimento:

Figura 4: Ejemplo de posibilidad

La probabilidad $p(x)$ de esta posibilidad estará dada por el número de palabras que quedan después de descartar todas las que no empiezan por C, no tienen como quinta letra la R o tienen las letras O, M, E dividido por el número total de palabras de 5 letras. Para esta palabra calculamos el valor esperado de información como la suma de $-p(x) * log(p(x))$ donde x va variando entre todas las combinaciones de colores de la palabra.

Ahora que sabemos calcular la entropía, o el valor esperado de información de una palabra calculamos la entropía de cada una de las palabras de 5 letras y nuestra mejor jugada inicial será la palabra con el mayor valor de entropía. Al programar este algoritmo y calcular la palabra con mayor entropía obtuvimos que la mejor palabra de inicio es: "PARES".

Siguiente paso: dar la mejor respuesta para cada nueva palabra

Ahora que sabemos cuál es la mejor palabra para iniciar el juego podemos determinar cuál es la mejor palabra a jugar dependiendo del resultado de la palabra que jugamos anteriormente. Lo siguiente que haríamos sería eliminar de la lista de todas las palabras aquellas que no siguen con el resultado de la palabra inicial. Después de esto volvemos a buscar el elemento de mayor entropía sobre la nueva lista de palabras. Seguimos de esta manera sucesivamente hasta encontrar la palabra que estamos buscando.

En la práctica

Al utilizar el algoritmo para jugar el día 16 de Marzo obtuvimos el siguiente resultado:

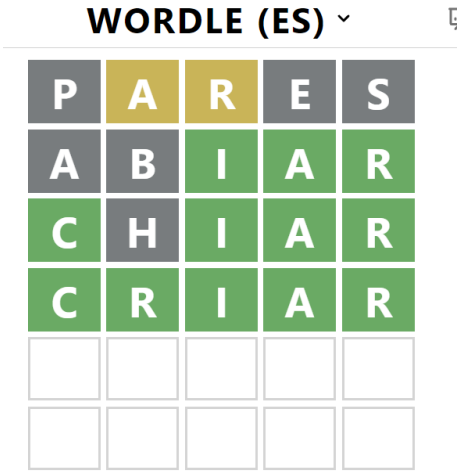

Figura 5: Ejemplo de posibilidad

¿Quiere decir esto que esta es la manera mas rápida de ganar el juego?. No necesariamente, como vemos este algoritmo tardo 4 intentos en encontrar una palabra que se podría haber encontrado en menos intentos, esto es porque hay muchas palabras que aunque tengan una mayor entropía no son palabras que sean muy comunes en el español, por lo que es poco probable que sean la solución para la palabra del día. Una manera de mejorar este resultado sería el de agregarle un peso a cada una de las palabras dependiendo en su frecuencia en textos en español. De esta manera la probabilidad de las palabras mas comunes tendrá un mayor peso y el algoritmo será mas propenso a jugarlas.

El código de toda la implementación lo pueden encontrar en: https://github.com/Enguenye/WordleBotES.

Conclusión

En este texto vimos como se define el concepto entropía, que es uno de los conceptos mas importantes de la criptografía, y cómo podemos entender la definición de este concepto desde un juego como wordle. Además, propusimos un algoritmo utilizando estos conceptos, para hallar una solución óptima al juego de wordle.

Fuentes

[1] Desciframiento forzado

[2] Wordle popularity
[3] Wordle popularity
[4] Solving wordle using information theory

Consúltenos en ✉ info@cyte.co acerca de las preguntas que pueda tener acerca de cómo puede adquirir la herramienta Crypto-Vault® para cifrado y descifrado de documentos sensibles de su organización. Para más artículos similares síganos en nuestro blog en https://www.cyte.co/blog

La imagen inicial usada en esta nota fue tomada de tomada de https://wordle.danielfrg.com/.