

DEL BIT A LA REVOLUCION INFORMATICA

Un homenaje a Claude Shannon
Diego Pareja Heredia. *Universidad del Quindío*



Claude E. Shannon (1.916 - 2.001)

Introducción.

Hace poco más de cincuenta años, Claude Elwood Shannon inició, posiblemente sin proponérselo, la más grande revolución que la humanidad haya podido experimentar en toda su historia. Nos referimos a la *Revolución de la Información*. No hay prácticamente ningún campo del conocimiento o de la vida práctica, en el que no se sienta el influjo del manejo constante de la información: desde el compact disc y el horno de microondas hasta las redes informáticas de los teléfonos celulares y de la Internet. Esta revolución que nos está cambiando las formas tradicionales de vivir y hasta de morir, tiene su origen en una pieza muy pequeña de tecnología, el microprocesador (Chip) y en el modo de procesar la información que la aprendimos de Claude Shannon.

Fue Shannon, quien entendió por primera vez el potencial que encerraba el poder procesar la información codificada en un lenguaje binario (ceros y unos), información que podía ser numérica, textual(en forma de texto) o inclusive de contenido lógico-simbólico. En su tesis de Master "*A Symbolic Analysis of Relay and Switching Circuits*," mostró cómo la lógica booleana (inventada por George Boole, el siglo XIX), puede simularse automáticamente con el recurso de circuitos eléctricos. Aquí el símbolo 1 puede representar el paso de la corriente en el circuito y el símbolo 0, lo contrario. Sencillamente 0 para apagado (off) y 1 para encendido (on).

Su tesis tuvo una motivación práctica. Por los años de 1940 la demanda del servicio telefónico era cada vez mayor y así mismo la complejidad y el tamaño de las redes. Se hacía necesario encontrar un lenguaje matemático para describir y formular los problemas del comportamiento de circuitos de gran complejidad, pues su manejo requería cada vez mayor número de personas que hicieran manualmente los enlaces en los nodos dispuestos para tal fin. Este propósito de reemplazar al ser humano por procesos automáticos de conmutación dio como origen, en los trabajos de Shannon, toda una técnica que vendría a ser estándar en el diseño posterior de todos los computadores.

En 1948 Shannon publicó en el *Bell System Technical Journal* su hoy famoso artículo "*A Mathematical Theory of Communication*", republicado en forma de libro en 1949 con la coautoría de Warren Weaver y con título ligeramente cambiado *The Mathematical Theory of Communication*. Hoy, después de cincuenta años, este libro aún sigue en circulación (publicado por University of Illinois Press). La aparición de esta obra es un hito histórico, pues con ella se dio origen a la teoría de la información. Es además, considerada en sí misma toda una obra maestra en el tema. Su aparición nuevamente, estuvo motivada por la necesidad de simplificar la transmisión de información en forma más eficiente a través de distintos canales..

Shannon fue quien, por primera vez encasilló el concepto de información en términos del tamaño del contenido informático del mensaje, sin tener en cuenta el significado que el mensaje conlleva. Según la teoría de la información, una poesía tiene el mismo contenido de información que un chiste, siempre que los dos textos se puedan codificar con el mismo número de bits. En forma precisa, él definió información, en términos del número de bits requerido para transmitir un determinado mensaje. En cuanto tiene que ver con la transmisión de la información, ya sea alfanumérica (palabras, números), música, video o archivos en general, lo que importa en últimas, es el número de 0's y 1's necesarios para codificar la información y transmitirla. Esta idea fue acogida y adoptada gradualmente por los ingenieros de comunicaciones, y propició la tecnología que vino a desembocar en lo que ha dado en llamarse hoy la *era de la información* y en la que hoy todos estamos inmersos.

Shannon fue un matemático de formación. Sus estudios de postgrado los hizo en el MIT (Massachusetts Institute of Technology), después de haber recibido títulos de matemáticas y de ingeniería en la Universidad de Michigan. En el MIT entró en contacto con la élite de científicos que pusieron, en buena parte, las bases para la revolución informática que empezó a gestarse después de la Segunda Guerra Mundial. Entre ellos Norbert Wiener (1894-1964), el renombrado matemático, quien acuñara el término *cibernética*, que él, Shannon y otros usarían en ciertos trabajos de teoría de la información, y Vannevar Bush, por ese entonces decano de la Facultad de Ingeniería. Vannevar Bush, era ya conocido por el diseño y construcción del *Differential Analyzer* (Analizador Diferencial), uno de los primeros computadores analógicos. Fue Bush también uno de los creadores de la National Science Foundation de Estados Unidos, y precursor, de la World Wide Web (WWW) al proponer la creación de la máquina de hipertexto llamada *Memex* en su artículo *As We May Think*. En 1940, Shannon estuvo como becario en el Instituto de

Estudios Avanzados de Princeton trabajando con el matemático Hermann Weyl, el famoso discípulo de David Hilbert y propulsor de la teoría de grupos aplicada a la mecánica cuántica.

No estuvo Shannon alejado de los albores de lo que hoy llamamos *inteligencia artificial*. Con John McCarthy y Marvin Minski participaron en la Conferencia sobre Máquinas Inteligentes y Temas Afines celebrada en el Dartmouth College de New Hampshire en 1956. El origen de la inteligencia artificial está ligado a los nombres de McCarthy y Minski, entre otros, mientras que la teoría de la información y la comunicación, tiene a Claude Shannon como su máximo gestor. Por esta época otra figura cimera de las matemáticas estaba abriendo brecha en áreas afines a la inteligencia artificial. El matemático John von Neumann (1903-1957), entre los años 1.945 y 1.955 venía trabajando en la teoría de autómatas y en la analogía entre el cerebro y el computador. La teoría de autómatas es un área interdisciplinaria que linda, con las matemáticas en el campo de la lógica simbólica y la teoría de las máquinas de Turing; con la ingeniería en lo tocante a la construcción de computadores de propósitos múltiples y con la neurofisiología en lo relacionado con redes y complejos neuronales.

La Teoría de la Información

Como decíamos arriba, en la teoría de la información, no se tiene en cuenta el contenido semántico del mensaje, objeto de la información. Información aquí es centralmente una medida, una cantidad discreta, igual que lo es la densidad o la masa, medibles en el sentido físico.

Son cinco los elementos básicos en la descripción teórica de todo sistema general de información, de acuerdo al modelo propuesto por Shannon y Bush.

- ❖ 1 – Una *fuentes* de información o un dispositivo que transforma la información o mensaje en algo apropiado para ser transmitido por un medio particular. Esta fuente, para el modelo que Shannon creó, codificará el mensaje en 0's y 1's.
- ❖ 2 – El *medio o canal* a través del cual se transmite el mensaje. En la tecnología moderna estos canales pueden ser los cableados de las redes telefónicas, las redes de microondas, las mismas ondas de radio y la tan útil red de la Internet.
- ❖ 3 – Un *dispositivo decodificador*, entendido como el proceso de convertir la serie de 1's y 0's en un mensaje inteligible para quien recibe el mensaje.
- ❖ 4– El *destinatario o receptor* del mensaje.
- ❖ 5 – Una *fuentes de ruido*, llamada también interferencia o distorsión, que podría afectar el mensaje, en forma impredecible. durante la transmisión.

Presentemos algunos ejemplos que se acomodan al modelo descrito arriba:

La transmisión de mensajes por Fax. La fuente o el emisor es aquí el mensaje a ser enviado junto al aparato que codifica el mensaje en forma apropiada para poder enviarse. El canal sería la línea telefónica, sea ella cableado de cobre, fibra óptica u ondas electromagnéticas de alta frecuencia. El dispositivo decodificador en este caso es el aparato a cuyo número va dirigido el mensaje. El receptor es la persona o entidad quien lee o interpreta el mensaje. Finalmente la fuente de ruido podría ser las interferencias que usualmente se presentan por deficiencias en las líneas de transmisión.

Los órganos de los sentidos. Cada órgano sensorial en el ser humano en concordancia con el cerebro y la consciencia puede tomarse como un sistema de información. Pongamos por caso la visión. La imagen y los ojos corresponden al emisor o fuente. El ojo, a través de la retina, convertirá la imagen (conjunto de señales lumínicas) en puntos claros y puntos oscuros. Estos puntos se transmiten al cerebro por el nervio óptico. El cerebro decodifica estos datos que recibe pasándolos a nuestra consciencia que es en últimas la que recibe el mensaje. En este ejemplo una fuente de ruido podría ser la deficiencia en la visión o inclusive las redes neuronales que procesan la información que llega al cerebro. Este es el caso en pacientes de la enfermedad de Alzheimer que ven las luces de la ciudad como un pavoroso incendio que les produce terrible angustia. El olfato, el gusto y el oído son ejemplos similares. El tacto merece tratamiento aparte en razón a un efecto que vale la pena destacarse, por cuanto el autor de estas líneas, no lo ha visto descrito en la literatura consultada.

El tacto y el *Efecto Pareja*. Cuando el apóstol Tomás puso en duda la resurrección de Jesús, negándose a creer lo que sus ojos veían, se dice que Jesucristo lo increpó para que tocara sus heridas y así disipar la duda. La información que llega al cerebro transmitida por el sentido del tacto siempre se ha creído fidedigna a tal punto de decirse de algo incontrovertible, como una verdad palpable. Aquí la fuente son las terminales nerviosas diseminadas en todo el cuerpo, pero particularmente en las manos donde está más concentrado el sentido del tacto. El medio o canal es el sistema nervioso encargado de llevar los impulsos nerviosos provenientes de las manos, digamos, al cerebro. Como en los otros sentidos el órgano decodificador de las señales provenientes del tacto es el cerebro(o una parte de él) y el destinatario final o receptor es la consciencia, cualquiera sea su definición.

No es nada nuevo saber que los sentidos mienten. Corrientes filosóficas respetables así lo pregonan. Los ejemplos abundan en el caso de la vista (el dicho popular de que *la vista engaña* solo confirma lo que aquí se dice). Quién no confunde un perfume con otro o un sabor con otro. ¿Quién no ha oído una palabra cuando le dijeron otra? Pero en el *tacto*, ¿alguien se ha equivocado diciendo que algo es duro cuando en realidad es blando o que algo está frío, cuando en realidad quema?. O que está tocando dos cosas, cuando en realidad está tocando una sola. Bueno, este último caso no es tan evidente, como lo muestra el siguiente experimento, que me fue comunicado por el médico *Fernando Pareja Binder*. Lo he denominado *Efecto Pareja* por razones que se desprenden del mismo experimento, como se verá en seguida.

El experimento, inicialmente se hizo al palpar una esfera pequeña, una canica, digamos. El experimentador debe cruzar el dedo del centro por encima del dedo índice, como quien está deseando buena suerte. Se coloca la esfera encima de una superficie plana y con los dedos cruzados se hace rodar en círculos de tal manera que los dos dedos hagan contacto con la superficie de la esfera. A la pregunta de cuantas esferas el experimentador toca, honestamente, el tiene que responder que dos. En lugar de una esfera, tendrá una *pareja*. Al observar la esfera, no ve sino una. Conclusión tampoco el tacto es tan fiable como se pensaba. Mas sencillo aún, Cierre los ojos, cruce los dedos, como se describió arriba, y deslice los dedos por una arista de su silla (siempre que la tenga, obviamente) cuidando que las yemas de los dedos cruzados toquen la arista. ¿Cuántas aristas está tocando? Dos, por supuesto. Al mirar descubre que solamente hay una.

Bueno y ¿qué hay aquí que relacione este efecto con la teoría de la información?. ¿Por qué llegó a la consciencia un mensaje equivocado?. La única explicación que tengo es la teoría de la información en lo que respecta a un factor de ruido o distorsión que actúa al enviarse el mensaje al cerebro a través de la red neuronal de nuestro cuerpo. Posiblemente esa distorsión ocurre por efecto del cruce de los dedos. Este efecto parece tan cercano e inmediato, que sería realmente extraño que no haya sido descrito y explicado en los tratados de Psicología o Neurofisiología.

En épocas anteriores a Shannon, tanto matemáticos como ingenieros que trabajaban en tecnología de la comunicación, entendieron su actividad como la búsqueda de procesos que pudieran mantener la integridad de las señales analógicas enviadas a través de cable de cobre sujeta a los riesgos de la fluctuación de la corriente eléctrica o a través del aire convertidas en ondas de frecuencia modulada. El enfoque de Shannon se encaminó hacia la codificación de la información como señales en forma completamente digital como sucesiones de 0's y 1's, a las que se referiría de allí en adelante como *bits (binary digits)*, acogiendo la sugerencia de su colega de la Universidad de Princeton John Tukey. Después de Shannon, el problema del manejo de la información se encaminó a buscar la forma más eficiente de enviar secuencias discretas de pulsos eléctricos o electromagnéticos de un punto a otro.

Shannon pronto observó que, mientras pequeñas variaciones en la señal analógica, pueden distorsionar un mensaje y así la información contenida en él, la naturaleza discreta de una señal digital es menos propensa a la contaminación por el ruido en el sistema. Más aún, al adicionar extra bits a la señal, podía adicionarse un proceso automático de detección y corrección en el sistema. La codificación digital de la información y sus códigos auto correctores son hechos tan cotidianos, que ya no nos preguntamos, si podría ser de otra manera. Este es el caso cuando bajamos música de Internet usando Napster, por ejemplo. Los archivos llegan a nuestros computadores con una fidelidad sólo sujeta a la calidad del sistema de sonido instalado en nuestro computador.

Como mencionamos antes, el enfoque de Shannon permite medir el tamaño de la información, en el sentido de saber cuánta información lleva una determinada señal. El proceso se reduce a contar el número mínimo de bits necesarios para codificar la

información. Basado en esta simple idea, Shannon fue capaz de desarrollar una teoría cuantitativa del contenido de la información, muy útil sobre todo para los ingenieros quienes tienen que decidir sobre la capacidad de los canales, en las redes de comunicación. En la teoría de Shannon lo que se mide es el tamaño, en el sentido binario, de la señal, no importa qué, esta señal pueda representar. Según esta teoría dos libros, independientemente de lo que traten, tienen el mismo contenido de información, siempre que ellos se dejen codificar en igual número de bits. Esto es demasiado útil en la actualidad cuanto se trata de transmitir digitalmente estos mismos libros a través de Internet. Todas las comunicaciones hoy se miden en bits por segundo, la misma noción que Shannon hizo precisa cuando habló sobre la capacidad de un canal de comunicación. También fue su teoría la que permitió usar los bits cuando se trata de almacenar en el computador, imágenes, sonido y datos de diferentes formas. El Internet no habría sido posible sin la teoría de la información de Shannon. Los usuarios de la red nos beneficiamos enormemente por la facilidad con que accedemos a la información que allí aparece. Muchas cosas no habrían sido posibles, incluyendo este artículo, sin la ayuda de la información encontrada en bases de datos que uno puede visitar. Este artículo se ha escrito casi en su totalidad con información bajada de la red y cuyas fuentes se especifican al final. Nuestro pequeño aporte está, básicamente en el beneficio de la traducción y su adaptación pedagógica. Cada vez que bajamos un paquete de actualización o enviamos un archivo comprimido en formatos como .gif o .jpg, estamos usando algo o mucho de la teoría de la información creada por Shannon.

ENTROPIA Y TEORIA DE LA INFORMACION

La teoría de la información de Shannon tiene una característica muy importante: el concepto de *entropía*. La entropía se define como carencia de contenido de información en un mensaje. Estamos acostumbrados a pensar en información, como hechos, datos o evidencia en tal o cual asunto, pero en teoría de la información *información es incertidumbre*, así que entre más bits de información se tenga más incertidumbre se tiene. Dicho en pocos términos, información es lo que uno no conoce. Si el receptor ya tiene la información, no podemos decir que una comunicación haya tenido lugar. Uno recibe un mensaje del cual desconoce su contenido. La teoría de la información habla precisamente acerca de los posibles mensajes que se pueden recibir o el número de mensajes entre los que se puede escoger, o en general, la teoría de la información habla de las propiedades estadísticas de un mensaje, comparado frente a la totalidad de los mensajes, sin tener en cuenta lo que el mensaje dice.

Un beneficio inmediato de la teoría de la información es que ofrece a los ingenieros las herramientas matemáticas necesarias para estimar la capacidad de los canales de comunicación, más exactamente, cuanta información, sin errores, puede ir de un punto A a otro B. La información que se quiere es la *señal*, la información que **no** se desea es *ruido*. El número M de posibles mensajes que uno puede formar con un número x de bits, será de 2 elevado a la x, puesto que cada lugar en el mensaje de tamaño x puede llenarse ó con 0 ó con 1. A la inversa el número x de bits necesarios para transmitir un mensaje entre los M posibles es logaritmo en base 2 de M. Simbólicamente,

$$2^x = M$$

$$\log_{\text{base } 2} M = x.$$

El valor de x en las fórmulas anteriores, se conoce como *entropía* en la teoría de Shannon. Usualmente la entropía se mide en “bits por símbolo” o en una relación similar, si se está usando un conjunto de símbolos para transmitir el mensaje, la entropía es el número de bits necesarios para representar un símbolo. Por ejemplo, el conjunto extendido de caracteres ASCII tiene 256 caracteres. El logaritmo base 2 de 256 es 8, así que hay 8 bits de entropía por símbolo.

Shannon empleó pruebas matemáticas para mostrar que se puede usar la medida de entropía para medir la capacidad exacta de determinado canal. Más aún, él probó que para cada canal se puede definir una capacidad tal que, si se permanece en él, se puede tener una transmisión tan libre de errores como se quiera. No está descartada la posibilidad de errores (ruido), por supuesto, pero su probabilidad se puede hacer muy pequeña con el uso de códigos auto correctores. Shannon tomó las observaciones que la gente había hecho sobre el intercambio de información y las puso sobre bases sólidas, usando las matemáticas y la estadística. La teoría de la información no es que elimine ruido, si no que nos permite convivir con él y hasta convertirlo en un elemento útil, por ejemplo podemos usar la entropía de la teoría de la información para encontrar la capacidad de un canal para transmitir información útil (la señal).

En 1949, Claude Shannon publicó en el **Bell System Technical Journal**, un artículo vital para la criptografía moderna. Su título fue : "*Communication Theory of Secrecy Systems*". En él, el concepto de entropía permite medir en cierto sentido el número de decodificaciones posibles de un mensaje. Si alguien está interesado en diseñar un programa para encriptar mensajes secretos, lo que se busca es tener la mayor entropía posible con el objeto de hacer que quien quiera quebrar la encriptación tenga que trabajar sobre más posibles mensajes. Operaciones binarias fáciles de hacer en un sentido pero difíciles de reversar, como la multiplicación y su inversa, la factorización, están en el corazón de los más modernos y mejores sistemas de encriptación. Tratar de descifrar un mensaje encriptado con un sistema de estos es similar a tratar de volver al café y a la leche después de tener un café en leche. Son procesos simples en un sentido, pero inimaginablemente compleja su reversa; en la práctica imposibles de deshacer.

Reseña Biográfica de Claude Shannon

Claude Elwood Shannon nació en Gaylor, Michigan en Abril 30 de 1916 en el seno de una familia de tradición cultural bien afincada. Su madre fue rectora del colegio local, su padre el juez de Gaylor y su abuelo un inventor nato con muchas patentes registradas.

Después de obtener títulos de pregrado en matemáticas e ingeniería en la Universidad de Michigan fue al MIT donde trabajó con Vannevar Bush en el Analizador Diferencial y obtuvo su Ph. D. en Matemáticas en 1940. Para optar el título de máster presentó como

tesis la aplicación de las leyes de Boole a la teoría de circuitos y su tesis doctoral versó sobre la aplicación de las matemáticas a la genética.

A partir de 1.941 se vinculó a Laboratorios Bell, donde permaneció por 31 años. Desde allí contribuyó con mucho a lo que vendría a ser la gran revolución de las comunicaciones.

A partir de 1.958 se desempeñó como profesor de ciencias del MIT hasta su retiro como profesor emérito, dos décadas después.

Entre sus aficiones tuvo el malabarismo al que contribuyó extensivamente. En su casa pueden observarse algunos de los aparatos y simuladores de malabarismo, creados por él.

Entre los muchos honores y distinciones a las que se hizo acreedor figuran:

Morris Liebmann Memorial Award, 1.949,

Medalla Ballantine, 1.955

Merin J. Kelly Award of the American Institute of Electrical Engineers, 1.962

National Medal of Science, 1.966

Medal of Honor from the Institute of Electrical and Electronics Engineers, 1.966

Jacquard Award, 1.978

John Fritz Medal, 1.983

Kyoto Prize in Basic Science, 1.985

Fue además galardonado con títulos honoríficos en más de una docena de instituciones alrededor del mundo.

Fue miembro de las siguientes academias

American Academy of Arts and Sciences,

National Academy of Sciences,

National Academy of Engineering,

American Philosophical Society,

Royal Society of London.

Claude Shannon murió el sábado 22 de Febrero de 2.001, en Medford, Mass. a la edad de 84 años, después de una prolongada lucha con la enfermedad de Alzheimer.

Fuentes de Internet consultadas

http://canyon.ucsd.edu/infoville/schoolhouse/class_html/duy.html

<http://math.washington.edu/~hillman/entropy.html>

<http://www.cs.unm.edu/~saia/infotheory.html>

<http://www.clas.ufl.edu/anthro/noetics/flesh-made-word.html>

<http://www-lmmb.ncifcrf.gov/~toms/>

http://www.maa.org/devlin/devlin_5_01.html

La IEEE tiene una página web sobre teoría de la información en:
<http://it.ucsd.edu/>

Las ideas de Shannon sobre malabarismo se encuentran en:
<http://www.juggling.org/papers/science-1/>