OCW
OpenCourseWare

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

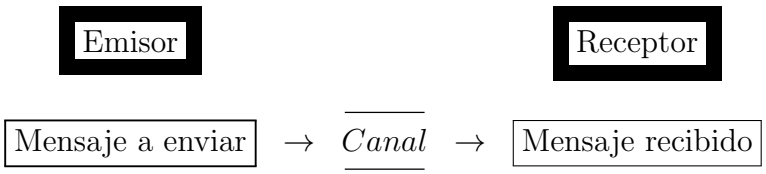
Facultad de Ciencia y Tecnología. UPV/EHU

Resumen Teórico
Apartado 1 del Tema 2:
Introducción: El problema de la codificación

Mayo de 2017

1 Introducción: El problema de la transmisión de la información

En la transmisión de la información nos encontramos con que un emisor manda un mensaje a través de un canal para que le llegue al receptor. Esto es, podemos representar los elementos que tenemos en el proceso de transmisión de una información mediante el siguiente esquema:



Sin embargo, durante la transmisión de la información puede haber problemas debido a interferencias que se produzcan en el canal. Estas interferencias pueden traducirse en dos situaciones diferentes:

1. Al receptor no le llega el mensaje que le ha enviado el emisor, sino que reciba un mensaje diferente del original por haber habido una mala transmisión.
2. El mensaje enviado ha sido interceptado por alguien que no es el destinatario final y este usurpador ha manipulado o ha hecho un uso indebido del mensaje captado.

Así, estas situaciones diferentes que se pueden darse sobre el canal usado nos llevan a realizar una clasificación del canal en dos tipos diferenciados:

1. Canal poco fiable: Hay "ruido" en el canal que dificulta la transmisión. Un ejemplo de este tipo de canal se tiene cuando intentamos leer un CD que presenta huellas de dedos que obstaculizan el acceso a la información grabada en él o cuando recibimos la señal de un satétite muy alejado de la Tierra, por lo que ésta llega muy debilitada, y no sabemos el valor exacto que se ha emitido.
2. Canal poco seguro: El canal que transmite la información soporta el ataque de espías que pueden manipular la información que transcurre por él o hacerse con ella sin ser el destinatario final. Por ejemplo, estaríamos ante un canal poco seguro cuando al hacer una compra por Internet con VISA, el ordenador que utilizamos para enviar la información de nuestra tarjeta tiene instalado un programa espía que captura los datos de nuestra tarjeta y se los pasa a otra persona para que haga otras compras que no hemos autorizado con nuestros datos, ó cuando el que intercepta el mensaje lo manipula antes de que continúe viajando por la red alterando el significado del mismo (p.e., hemos autorizado un pago de 30 euros a un vendedor X y el que lo altera indica al banco que autorizamos un cargo a nuestra cuenta de 300 euros, 30 para el vendedor X y 270 para abonar a Y).

CC BY NC SA

En cualquiera de los dos casos, es necesario disponer de herramientas que nos ayuden a solventar, en la medida de lo posible, este problema de interferencias en el canal. De hecho, las Matemáticas nos permiten solucionar en muchos casos esta dificultad y, tras un proceso más o menos complejo que debe aplicarse a la información que va a ser enviada por el canal, es posible "recuperar" el mensaje inicial (en el caso de canales poco fiables) o "esconder" la información que viaja por el canal, de forma que cualquiera que la intercepte no sepa de qué se trata (cuando el canal es poco seguro). Obviamente, según el tipo de interferencias que podamos sufir en el canal deberemos adoptar acciones diferentes. Así,

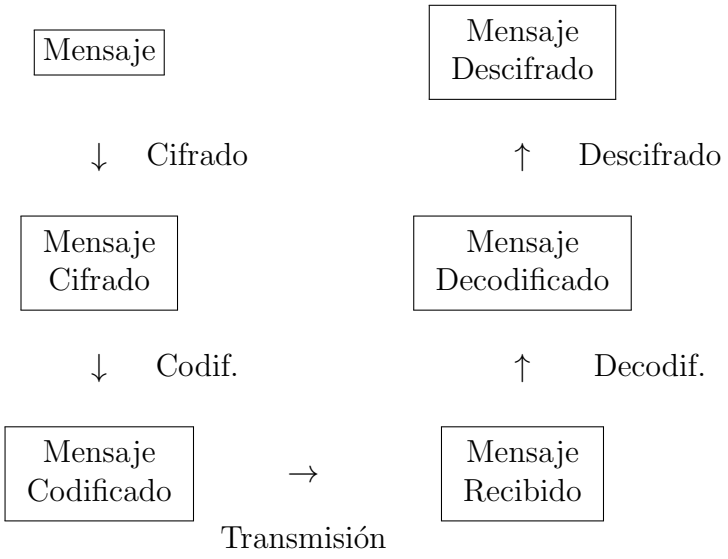
1. Si el canal es poco fiable, usaremos los llamados **códigos detectores y correctores de errores** que nos permiten al recibir un mensaje conocer si se ha producido algún fallo en la transmisión (esto es, detecta los errores producidos) y, en ciertos casos, incluso puede saberse cuál fue el mensaje inicial enviado. En esencia, los códigos detectores y correctores añaden información a la inicial, conociendose este proceso como codificación del mensaje, de forma que con la información extra añadida sepamos si se ha producido algún error en el mensaje recibido y, si es así, aplicarle un proceso llamado de decodificación, que permite recuperar (si es posible) el mensaje enviado.

2. Si el canal es poco seguro, la herramienta matemática de la que disponemos es el uso de los conocidos como **sistemas criptográficos**, que antes de enviar la información, la transforman en otra sin sentido para el que pretende hacerse con ella de forma ilegal y al ser recibida por el receptor la información transformada, éste revierte la transformación realizada para obtener el mensaje real que le quería mandar el emisor. El proceso de modificar la información para que carezca de sentido para el que escucha sin ser el receptor se conoce como proceso de encriptado o cifrado y la acción de revertir el mismo, que lo hace el receptor, es el proceso de desencriptado o descifrado.

Hay veces que por las características de la información a enviar y del canal a utilizar será preciso realizar una combinación de ambas herramientas: en primer lugar se esconde la información, esto es, se cifra. Luego se le añade información extra, es decir, se codifica. A continuación se pasa por el canal y el receptor aplica primero un proceso de decodificación y al mensaje resultante uno de descifrado para llegar al mensaje original que deseaba hacerle llegar el emisor. Si queremos resumir

CC BY NC SA

esquemáticamente de este proceso, podemos usar el siguiente diagrama:



En cualquier caso, tanto al usar códigos detectores y correctores de errores como sistemas criptográficos, debemos ser especialmente cuidadosos en la elección del tipo de código o sistema a utilizar: debe ser acorde a las posibles interferencias que soporte el canal. Por ejemplo, si queremos mandar una información a través de un canal no muy fiable del que sabemos que cada 10 dígitos que pasamos por él se produce un error y queremos solventar este problema, de entre los códigos correctores de errores deberemos elegir uno que se ajuste a lo que nosotros necesitamos. Así, sería factible elegir uno que nos permita corregir uno o dos errores en cada bloque de 10 dígitos, pero no uno que permita corregir un error producido cada 100 datos (sería escaso) u otro que nos permita corregir uno de cada dos (podría ser demasiado costoso). Del mismo modo, cuando debamos trabajar con un canal poco seguro, deberemos valorar el tiempo y coste necesarios de los procesos de cifrado /descifrado de mensaje para adecuarlos al canal que usamos.

En este curso nos centraremos en estudiar algunos de los códigos detectores y correctores de errores, que son estudiados por la parte de las Matemáticas conocida como Teoría de Códigos, mientras que el estudio de los sistemas criptográficos, de los que se ocupa la Criptografía, se dejará para cursos posteriores. Asimismo, dentro del estudio de los códigos detectores y correctores de errores nos centraremos en analizar las propiedades y manejo de los llamados códigos lineales, que son los más sencillos de trabajar. El estudio de otros tipos de códigos correctores de errores, como por ejemplo, los algebro-geométricos que usan curvas elípticas en sus definiciones, transciende el objetivo de este curso que lo que pretende es exponer de forma rigurosa, desde el punto de vista matemático, las características fundamentales de los códigos lineales, proporcionando de este modo una primera aproximación a la matemática más sencilla que está detrás de la Teoría de Códigos. No obstante, en este capítulo nos preocupamos por formalizar los conceptos más importantes sin restringirnos, en muchos del ellos, al marco exclusivo de los códigos lineales, sino que estas definiciones son válidas para los códigos detectores y correctores en general.

CC BY NC SA