DÍGITOS DE CONTROL Y CÓDIGOS CORRECTORES: ¿TIENEN LUGAR EN LA EDUCACIÓN MATEMÁTICA?

Omar Gil
Instituto de Matemática y Estadística "Prof. Ing. Rafael Laguardia", UdelaR, Uruguay.
omargil@fing.edu.uy

Nivel educativo: Educación primaria, educación secundaria, formación docente.
Palabras clave: información, errores, ingeniería didáctica

Resumen

Una subárea de la Teoría de la Información, desarrollada a partir de la segunda mitad del siglo XX, es la detección y corrección automática de errores. Este trabajo presenta una breve descripción de algunas ideas básicas de esta subárea, prestando especial atención a la identificación de problemas y conceptos que permitan generar actividades útiles para la educación matemática en los niveles primario, secundario y de formación de docentes. Sobre el final se reportan algunos resultados preliminares de un proyecto en curso, enfocado en el nivel escolar y en la formación de maestros, en colaboración con Lucía Brusa y Beatriz Rodríguez Rava. A lo largo de todo el texto se enfatiza la relación de la temática de dígitos de control y códigos correctores con temas bien establecidos del currículo, y con aspectos de la vida moderna.

1. Protección contra errores y teoría de la información. La protección automática de la información contra errores en su transmisión y reproducción asegura la buena calidad de nuestras comunicaciones, a través del tiempo (almacenando y recuperando más tarde registros) o a través del espacio (telefonía móvil, tráfico sobre Internet, etcétera) [3].

Control de paridad y aritmética módulo 2. Un procedimiento básico de protección contra errores es el de forzar a los *bytes*, agrupamientos de ocho bits en los que podemos almacenar los valores 0 o 1, a satisfacer un control de paridad. La idea es poner datos sólo en los primeros siete lugares, reservando el octavo para un *carácter de control*, que se elige de modo tal que el número total de unos en el *byte* sea par. Esta codificación de la información permite detectar el cambio de un 0 por un 1, o viceversa, en algún bit, y también recuperar un caracter perdido.

Dado cualquier número entero *n* se puede construir una *aritmética módulo n*, siguiendo la regla de dividir entre *n* el resultado de cualquier operación y sólo conservar el resto de la división entera. La condición de paridad sobre los *bytes* puede expresarse en términos de la *aritmética módulo 2* por una sencilla ecuación algebraica: los coeficientes del *byte* deben sumar cero módulo 2. La aritmética módulo 2 es conocida por los alumnos de la escuela primaria, porque corresponde a los enunciados

par más par, par,	*Par por par, par,*
par más impar, impar,	*par por impar, par,*
impar más impar, par.	*impar por impar, impar,*

en los que *par* se identifica con el número cero, e *impar* con el uno. La aritmética resultante está construida a partir de la habitual, pero es diferente.

Las matemáticas involucradas en la detección y corrección automática de errores tienen un nivel de dificultad que va desde la aritmética más elemental, como la que acabamos de exponer, hasta la existencia de una activa área de investigación en la que confluyen científicos con diferentes formaciones, fundamentalmente matemáticos e ingenieros. A continuación mostramos un segundo ejemplo que requiere ideas algo más elaboradas, algunas todavía manejables a nivel escolar.

ISBN. La gran mayoría de los libros que existen en la actualidad están identificados con un número de diez cifras, generado por un sistema estándarizado llamado ISBN (International Statistical Book Number) que asigna a cada publicación un número único. Un registro de ISBN puede adulterarse al transmitirlo o almacenarlo, por esa razón el ISBN incorpora a su diseño un dígito de control. De los diez dígitos que forman cada número de ISBN, los nueve primeros portan la información, y el décimo es un carácter de control. Los nueve dígitos que almacenan la información están divididos en tres campos: el primero corresponde al área geográfica, el segundo identifica al editor, y el tercero a la publicación. Por ejemplo, para el primer campo, el número correspondiente a Uruguay es 9974. La receta para determinar el dígito de control es la siguiente: hay que multiplicar la primera cifra del número que identifica al libro por 1, la segunda por 2, la tercera por 3, la cuarta por 4, la quinta por 5, la sexta por 6, la séptima por 7, la octava por 8, la novena por 9, sumar todo y hacer la división entera con el resultado como dividendo y el número 11 como divisor. El resto será el dígito de control. Veamos un ejemplo. El libro Maticuatro [9] está identificado por el ISBN 9974 – 618 – 14, del que sólo hemos copiado los datos que corresponden a la región, editor y número de publicación. Falta calcular el dígito de control. Hacemos la cuenta

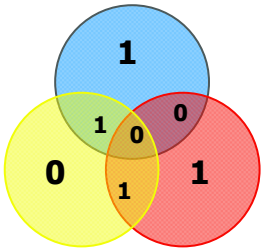
$$9x1 + 9x2 + 7x3 + 4x4 + 6x5 + 1x6 + 8x7 + 1x8 + 4x9 = 200 = 18 \times 11 + 2.$$

El ISBN que estamos buscando es entonces 9974 – 618 – 14 – 2. Para algunos libros al hacer el cálculo la división entre 11 arroja resto 10. En estos casos el carácter de control se representa con una X.

El ISBN de diez dígitos emplea la *aritmética módulo 11*. El nuevo ISBN13, que llevan los libros impresos a partir de enero de 2007 y que seguramente será el mayoritario en nuestras bibliotecas dentro de poco tiempo, el sistema EAN13, que identifica los productos que encontramos en almacenes y supermercados con un número que aparece representado por medio de un código de barras impreso en el exterior del envase (EAN 13 e ISBN13 son idénticos desde el punto de vista del cálculo de sus dígitos de control) y el dígito de control de la cédula de identidad uruguaya emplean la *aritmética módulo 10* para su construcción. Calcular con la *aritmética módulo 10* es sencillo: consiste en conservar de los números sólo la cifra de las unidades.

La gran simplicidad de la aritmética módulo 10 permite trabajar desde muy temprano sobre ella en las aulas escolares. Las propiedades de un dígito de control basado en una aritmética módulo 11, o, en general, sobre cualquier número primo, son mejores que las de uno que emplea aritmética módulo 10. Esta observación abre el camino para motivar actividades matemática interesantes y adecuadas a niveles más avanzados, incluso en el de formación de docentes.

Un paso más: corrigiendo. Agregar un dígito de control permite detectar un error, pero esto no es suficente para muchas aplicaciones. En su fundamental artículo de 1950, *Error detecting and error correcting codes* [6], Richard Hamming (1915-1998), analiza el problema de cómo conseguir que una computadora pueda corregir los inevitables errores que se producen en el procesamiento de un gran volumen de datos. Hamming relata "*en algunas situaciones la verificación automática no es suficiente ... las máquinas trabajaban sin atención durante las noches y fines de semana, sin embargo, los errores implicaban que los cálculos se detuvieran, aunque las máquinas pudieran dedicar-se a otros problemas, ... la incidencia de fallos aislados, aún cuando sean detectados,*



podría interferir seriamente con el uso normal de estas máquinas. ... parece entonces deseable examinar el proximo paso más allá de la detección de errores, la corrección de errores" [6]. Hamming propone entonces un procedimiento para hacer esto, una familia de códigos, que ilustramos a través de un ejemplo, por medio de una representación gráfica introducida por Robert McEliece. El código que mostraremos codifica una "palabra" de cuatro bits, como (1010) con siete bits, y permite corregir un error. Comenzamos por distribuir los cuatro símbolos 1, 0, 1, y 0 en las intersecciones de los círculos de color que aparecen en el esquema. Los hemos representado con números de pequeño tamaño. Luego agreguemos controles de paridad en cada uno de los círculos, de modo que todos contengan un número par de unos. Para nuestro ejemplo, en el azul y en el rojo hay que colocar un uno, y un cero en el amarillo. Estos dígitos de control, representados en el esquema con un tipo de letra de mayor tamaño, completan una palabra de siete bits (**1 0** 1 **1** 0 1 0), formada por los cuatro dígitos originales (la información que queremos almacenar o transmitir), y los tres dígitos de control de paridad, que hemos intercalado en negrita. Si uno de los siete dígitos se cambia por un valor equivocado, tal como hemos hecho en la segunda figura, tenemos suficiente información para ubicarlo y corregir el "bit dañado". Al examinar el círculo azul del nuevo esquema encontramos que su control de paridad falla, igual que ocurre con el rojo. Pero el del amarillo se satisface. Por lo tanto tenemos que cambiar lo que está en la intersección de los discos rojo y azul, pero no en el amarillo. De esta manera corregimos el uno equivocado, y recuperamos la palabra que habíamos codificado en nuestro primer diagrama.

Shannon y la teoría de la información. La fiabilidad de los procesos de comunicación depende de un análisis estadístico, cuyos fundamentos fueron establecidos por Claude Shannon en el artículo *A Mathematical Theory of Communication* [11], publicado en 1948. Una obra sobre la que en buena parte descansa la sociedad de la información y las telecomunicaciones de nuestra época. Los procesos de protección contra errores y de compresión de la información encuentran en ella un marco natural. Luego de los trabajos de Hamming y Shannon de fines de los años cuarenta, el progreso en esta área se fue acelerando. Un hecho notable para la historia de la ciencia y para la educación matemática es que el

álgebra introducida por el francés Evaristo Galois (1811-1832) encontró en este nueve terreno un espacio riquísimo para su aplicación [10].

2. Todo esto, ¿tiene un lugar en la escuela? Las matemáticas que el procesamiento y trasmisión de la información utiliza son muy ricas y variadas, y pueden llevarse a todos los niveles del sistema educativo. Las primeras actividades que se pueden proponer a un nivel muy lúdico, sólo requieren sumar e identificar la cifra de las unidades de un número natural. Las codificaciones según los estándares EAN13 e ISBN13 son aplicaciones realistas que pueden trabajarse a partir de estas mismas ideas y la multiplicación por tres. A partir de aquí, se extiende un continuo de posibilidades, con un nivel de dificultad que va creciendo hasta alcanzar cuestiones de investigación en la frontera misma del conocimiento. El estudio de los dígitos de control y los códigos correctores de errores permite integrar en forma natural temas de aritmética, geometría, combinatoria, probabilidad, estadística y álgebra lineal. También contribuye a mostrar que el conocimiento matemático es el resultado de una obra humana inacabada, que continúa y a la que nuestra sociedad uruguay contribuye, porque hay académicos trabajando en este tema en nuestro país. Habilita a presentar situaciones en las que se opera con objetos usuales siguiendo reglas diferentes, e ilustra sobre la variedad de formas que toma la Matemática para adaptarse a distintas situaciones [7]. Todo esto puede hacerse poniendo en juego competencias y contenidos tradicionales que es pertinente conservar, al tiempo que se propone una mirada actualizada de ellos, y se promueve en contextos simples el acercamiento a un aspecto crucial de la ciencia contemporánea, como es la construcción y el análisis de algoritmos.

Actividades en el aula. El área permite generar actividades muy diversas para el aula, desde el nivel escolar que sucintamente analizaremos en esta sección, hasta la formación de Profesores de Matemática [4], pasando por ejercicios con estudiantes liceales que permiten trabajar conceptos básicos de la teoría de funciones al tiempo que se juega con "transmisiones" de datos codificadas con alfabetos telefónicos de uso corriente. En el nivel escolar se pretende desarrollar sistemáticamente una secuencia de actividades, que atienda a los aspectos algorítmicos del tema, implementables sobre las computadoras XO del plan CEIBAL, y acompañarla de material de apoyo para maestros [2]. Con el propósito de acceder a la observación y al control de fenómenos de enseñanza propios de nociones matemáticas de esta área, se utiliza la estructura básica de la Ingeniería Didáctica [1,8]. A continuación esbozamos el análisis de una propuesta de trabajo en el aula, que hemos ensayado con niños desde el primer año escolar. Los resultados que aquí se presentan corresponden a su puesta en práctica con alumnos de sexto año [5].

En esta actividad se presenta a los alumnos una caja conteniendo las 10.000 posibles listas de cinco números números de una cifra cuya suma es múltiplo de diez, o, equivalentemente, es cero módulo 10.

Objetivo: identificar una regularidad en un conjunto de datos.

Consigna: en esta caja hay muchísimas listas de números de una sola cifra. Cada equipo sacará dos listas y las copiará en una hoja. Al copiar una de ellas el equipo debe cambiar una cifra por otra que elija, sin que ningún otro equipo se entere. La otra lista la deben copiar sin realizar ningún cambio. Cada equipo nos mostrará sus listas y descubriremos cuál es la lista que ha sido modificada.

Se pretende que los alumnos busquen una posible explicación a la "magia". Nuestra hipótesis inicial era que podía resultar difícil el reconocimiento de la regularidad por lo que previmos algunas intervenciones

posibles. El docente puede proponer sumar los números de cada lista y observar alguna regularidad. Los alumnos deben extraer una "regla" para discutir colectivamente. Previamente pensamos que era posible que los niños intentaran probar con otros números el cumplimiento de la regla. Los alumnos inmediatamente comenzaron a buscar la regularidad y la identifican de la siguiente manera:

- "Da justo, 20, 30, 40…pero la que cambia, no."
- "En realidad tiene que dar un número terminado en cero."
- "¡Son múltiplos de 10!"

Se genera luego una discusión sobre qué múltiplos de 10 son posibles.

- B - Sí, son múltiplos de 10.
- R - Pero no todos, porque 100 no te puede dar.
- B – Claro, porque no llegas.
- A – Sí, puede ser 10, 20 o 30.
- R – Te puede dar 40, si pones 9,9,9,9,4 da 40.
- A – Pero vos repetiste el 9.
- R – y pongo 8,9,7,7,9 y también me da 40
- B – pero sin repetir ninguno solo podes llegar a 30.

Otras actividades estimularon la consideración de otros aspectos de la aritmética [5].

3. Reflexiones finales. El siglo XX fue muy rico en avances de la ciencia, en particular de la Matemática, en direcciones muy diversas. Las implicaciones de este desarrollo en el currículo escolar todavía están lejos de agotarse. Incluso en lo que tiene que ver con grandes ejes temáticos clásicos que atraviesan el currículo educativo y que seguramente deberán mantenerse en futuros programas de estudio. Por ejemplo, para la escuela tienen vigencia los ejes de número, operaciones, geometría y mediciones. Son temas tradicionales, bien establecidos, que tienen significado para la vida moderna. Son antiguos, pero no obsoletos. Sin embargo, los avances del siglo XX muchas veces significan cambios en la aproximación a viejas cuestiones, o la introducción de ideas simples con consecuencias profundas. Es falsa la creencia de que las matemáticas contemporáneas son necesariamente más complejas que las antiguas, y que a nivel del sistema educativo sólo pueden tener lugar a niveles de posgrado, pero son poco importantes para la formación de docentes, mucho menos aún para el currículo del bachillerato o la enseñanza media, y completamente irrelevantes para el nivel escolar. En muchos casos la diferencia entre tenerlas presentes o no es más una cuestión de orientación general del sistema, que de profundidad de los conocimientos que se pretenden compartir y comunicar. En particular, algunas de estas cuestiones permiten visitar con una nueva mirada antiguas cuestiones, o simplemente proponer actividades que ayudan a explicar aspectos de la vida cotidiana que han aparecido gracias al avance científico y tecnológico. Los ejemplos provenientes de los códigos correctores de errores implican un contexto en el que realizar operaciones aritméticas, permiten resignificar algunas operaciones y aproximarse a ellas desde nuevos ángulos (por ejemplo, el resto de una división pasa a tener una importancia de la que carece en otros problemas), y hacen referencia a cuestiones de la vida diaria, contribuyendo a explicarlas.

Nuestra hipótesis de trabajo, que motiva la presentación de estos materiales, es que los problemas relacionados con dígitos de control permiten generar un conjunto de actividades que, por su valor cultural, su capacidad de movilizar otros contenidos matemáticos, y el lugar que en la ciencia contemporánea ocupa todo lo que tiene que ver con el procesamiento de la información, justifican el tratamiento del tema en todos los niveles del sistema educativo. Intuimos que muchos otros temas de la matemática del siglo XX, en particular otros relativos a la transmisión de información, como son la compresión de datos y la criptografía, son susceptibles de un tratamiento similar, aunque no hemos avanzado en esta dirección, ni siquiera para formular las primeras conjeturas y borradores de propuestas.

4. Referencias

[1] ARTIGUE, Michèle; DOUADY, Régine; MORENO, Luis (1995) *Ingeniería didáctica en educación matemática*, Bogotá: Grupo Editorial Iberoamérica.

[2] BRUSA, Lucía; GIL, Omar; RODRIGUEZ RAVA, Beatriz (2010) *La enseñanza de aspectos de la Teoría de la Información en la escuela,* proyecto presentado a la convocatoria 2009 del Fondo María Viñas, ANII (Agencia Nacional de Investigación e Innovación).

[3] FERNÁNDEZ GALLARDO, Pablo; GIL ÁLVAREZ, Omar (2002) *Una introducción a los códigos detectores y correctores de errores*. Disponible en http://www.matematicaparatodos.com/varios/Codigos.pdf.

[4] GIL, Omar (2009) *Excursiones por el Álgebra lineal y sus aplicaciones*. Santiago de Chile. J.C. Sáez.

[5] GIL, Omar; RODRÍGUEZ RAVA, Beatriz (2007) *Códigos detectores y correctores de errores: ¿tienen lugar en la escuela?* Inspección de Educación Privada. CEP. Uruguay.

[6] HAMMING, Richard (1950) *Error Detecting and Error Correcting Codes*, The Bell System Technical Journal **29**, páginas 147-160.

[7] HAMMING, Richard (1980) *The unreasonable effectiveness of mathematics*, American Mathematical Monthly **87**, páginas 81-90.

[8] RODRÍGUEZ RAVA, Beatriz (2005) *La Ingeniería didáctica,* en B. Rodríguez Rava; A. Xavier de Mello, El Quehacer Matemático. Montevideo. Edit. Queduca. FUM – TEP

[9] PENA, Mónica; GADINO, Alfredo; VARELA, Carlos (1999) *Maticuatro. Libro para el alumno*, Aula.

[10] REED, Irving; SOLOMON, Gustave (1960) *Polynomial Codes over certain Finite Fields,* Journal of the Society for Industrial and Applied Mathematics **8**, páginas 300-304.

[11] SHANNON, Claude (1948) *A Mathematical Theory of Communication*, The Bell System Technical Journal **27**, páginas 379-423, 623-656.