Cifrado con cubos marcados

Moisés Coriat
mcoriat@ugr.es
María C. Cañadas
mconsu@ugr.es
Departamento de Didáctica de la Matemática.
Universidad de Granada

Resumen

Con cuatro de los 8 tetracubos y con la ayuda de la noción de cubo mínimo (cubo formado por dos tetracubos), introducimos los "cubo marcados". A su vez, usamos esta idea para generar claves con las que cabe transmitir mensajes cifrados. Damos ejemplos de claves y mencionamos algunas posibilidades más de cifrado con dichos cubos marcados. En la introducción presentamos algunas facetas del cifrado. Después, describimos algunos policubos y prestamos especial atención a los cuatro tetracubos que permitirán construir los cubos de mínimo tamaño. Con éstos caracterizamos los cubos marcados que, a su vez, son utilizados para presentar algunos códigos alfanuméricos. Termina la comunicación con unas reflexiones sobre la conexión entre geometría y álgebra en el contexto de lo aquí presentado.

Introducción

Si M es un mensaje, C es un procedimiento sistemático y reversible para sustituir las letras de un mensaje por otros símbolos y C(M) el mensaje cifrado, esperamos que al aplicar el procedimiento recíproco (C^{-1}) al mensaje cifrado, volveremos a obtener el mensaje M: $M = C^{-1}(C(M))$. El procedimiento C se basa siempre en una regla de transformación de cada letra de un idioma L en otra letra, letras o números de cualquier otro idioma, generalmente L. Esa regla de transformación recibe el nombre de clave. Es usual el abuso de lenguaje consistente en identificar la clave con el procedimiento C.

Cuando un emisor difunde un mensaje cifrado, C(M), espera que solamente lo descifren quienes estén en posesión de C o que, al menos, cualquier otro receptor tarde mucho tiempo en determinar la clave.

Una solución en la que la clave es fácil de concebir y difícil de obtener, la tenemos en los números que solamente aceptan 4 divisores, como el 10. El emisor difundirá un mensaje con la clave 10, 2 y confía en que solamente un receptor reconocerá esa clave, respondiendo 10, 5. El ejemplo anterior es trivial, pero si consideramos que dos de los divisores son números primos de 30 cifras, el tiempo de respuesta que necesita un tercer receptor para suplantar al destinatario esperado es demasiado largo para que la violación del mensaje (en este caso, el mensaje es un reconocimiento de identidad) tenga éxito.

Los ordenadores son utilizados con frecuencia para descubrir claves y con ello descifrar mensajes. El programa Mathematica ha sido utilizado con este fin y un ejemplo reciente lo encontramos en McLoone (2011).

Coriat, M. y Cañadas, M. C. (junio, 2011). *Cifrado con cubos marcados*. Trabajo presentado en el II Encuentro AprenGeom. CIEM, Castro Urdiales, Santander.

Otra soluciones se basan en la idea de que haya un gran número de posibilidades para elegir la clave. Cuando el número de posibilidades es suficientemente alto, de manera que cualquier ordenador deba dedicar un tiempo prohibitivo a decidir si estamos ante una clave correcta, cabe esperar que sencillas situaciones de combinatoria elemental aporten poderosas técnicas de cifrado. En este trabajo exploramos esta idea.

En el primer apartado presentamos el material con el que proponemos generar códigos, los policubos. En el segundo apartado nos centramos en los dicubos, tricubos y tetracubos. En el tercero exponemos un modo sistemático para producir los cuatro tetracubos que utilizaremos para la generación de claves. En el cuarto presentamos las ideas de "cubos mínimos" y "cubos marcados" para la generación de los elementos de codificación. El quinto apartado inicia la presentación de un código para escribir números con tetracubos.

1. El material utilizado

En este trabajo indagamos en la idea de generar códigos que no sean fáciles de descifrar como consecuencia de que haya gran número de posibilidades para elegir una clave correcta. Para ello, usamos ciertas construcciones hechas con cubos macizos congruentes. A su vez, con algunas de estas construcciones (policubos), generaremos nuevos cubos macizos. Un modelo físico adecuado, pero no único, lo constituyen los "cubos elementales de colores", también conocidos como cubos "multilink" (marca registrada). Cada cubo físico elemental tiene cinco caras con un hueco cilíndrico y una cara con un saliente que permite unir dos cubos encajando por presión el saliente de uno de los cubos en un entrante del otro. Geométricamente, lo que exigimos de la unión de dos cubos es que compartan exactamente una cara. Un cubo puede compartir diferentes caras compartidas con distintos cubos. Mediante la unión de dos cubos en estas condiciones formamos *dicubos*. *Tricubos,* con la unión de tres cubos. *Los tetracubos,* se construyen mediante la unión de cuatro cubos y así, sucesivamente. Cualquier composición de este tipo (en la que lo esencial es que dos cubos contiguos compartan una cara) la denominamos *policubo*.

Con tetracubos y tricubos es posible construir un cubo 3x3x3, también conocido como "cubo de Soma" o "cubosoma". Piet Hein descubrió, en 1936, que es posible construir un cubo 3x3x3, usando siete piezas básicas, mostradas en la figura 2 y en las figuras de la 4 a la 9 del siguiente apartado. Este cubo recibe el nombre de "cubo de Soma" o "cubosoma". Diversos trabajos resaltan la importancia de la visualización en diferentes construcciones (Masalski, 1977), indagan sobre el tipo y el número de figuras diferentes que se pueden formar con esas piezas básicas, los niveles de las figuras compuestas que se pueden construir según las piezas empleadas (Spector, 1982) o algunas que no se pueden construir con unas piezas determinadas (Carson, 1973). Las posibilidades didácticas de los policubos han sido utilizadas por diferentes autores en distintos niveles educativos. Su relación con el uso que los niños hacen de los ejes corporales es indicado por Sack y Vázquez (2008).

2. Dicubos, tricubos y tetracubos

Si limitamos las consideraciones a la forma de la unión, observamos que todas las maneras de unir dos cubos generan una sola forma de dos cubos, por eso decimos que solamente existe un dicubo. Análogamente, hay dos tricubos (figuras 1 y 2) y ocho tetracubos (figuras 3 a 9).

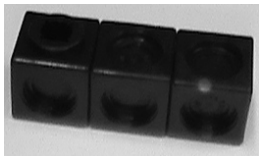


Figura 1: Tricubo "I"

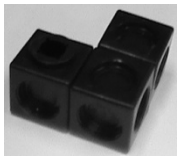


Figura 2: Tricubo "L"

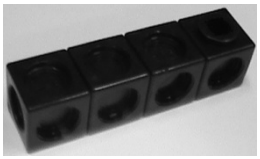


Figura 3: Tetracubo "I"


Figura 4: Tetracubo "L"


Figura 5: Tetracubo "T"

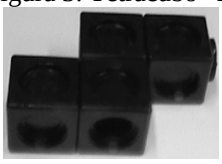


Figura 6: Tetracubo "S" o "Z"


Figura 7: Tetracubo "OO"


Figura 8: Tetracubo "3D"

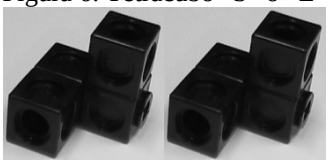


Figura 9: Tetracubos "II" y "DD"

3. Descripción operacional de cuatro tetracubos

Partimos del tricubo "L" (figura 2) y, situando un cuarto cubo en posiciones no equivalentes, generamos los tetracubos de las figuras 4 a 9. Describimos aquí la construcción de los cuatro tetracubos de las figuras 7 a 9 a partir del tricubo "L", dando por supuesto que se conocen los ejes corporales vertical, longitudinal y horizontal[1].

Tetracubo "OO". El cuarto cubo se coloca de manera que se forme un prisma de base cuadrada. (Ver figuras 2 y 7.)

Tetracubo "3D". El cuarto cubo se coloca sobre el cubo que ya compartía dos caras con distintos cubos; el cubo en común soporta 3 dicubos que, conjuntamente, se pueden colocar de manera que sean paralelos a tres ejes mutuamente perpendiculares. (Ver figuras 2 y 8.)

Tetracubo "DD". En el tricubo L, apoyado en un plano horizontal, de manera que un dicubo marca el eje horizontal y el otro el eje longitudinal, colocamos el cuarto cubo encima del cubo no compartido del dicubo que marca el eje longitudinal. (Ver figuras 2 y 9-derecha.)

Tetracubo "II". En el tricubo L, apoyado en un plano horizontal, de manera que un dicubo marca el eje horizontal y el otro el eje longitudinal, colocamos el cuarto cubo

[1] En una primera idea, el eje vertical se identifica con la línea marcada en cada lugar por la plomada; el eje longitudinal, con la línea que corresponde al sentido de la marcha, y el eje horizontal con cualquier línea perpendicular al plano definido por los otros dos.

Coriat, M. y Cañadas, M. C. (junio, 2011). *Cifrado con cubos marcados*. Trabajo presentado en el II Encuentro AprenGeom. CIEM, Castro Urdiales, Santander.

encima del cubo no compartido del dicubo que marca el eje horizontal. (Ver figuras 2 y 9-izquierda.)

4. Cubos mínimos y cubos marcados

Los cubos de mínimo tamaño (o "cubos mínimos") que se pueden construir con tetracubos son cubos 2x2x2 y se obtienen por empaquetamiento de dos tetracubos OO, 3D, DD ó II, respectivamente. Consideramos que este resultado no necesita más desarrollo. Se observa que el resto de los tetracubos (figuras 3 a 6) no permite construir un cubo 2x2x2 usando dos tetracubos.

Una proposición recíproca también se cumple: dado un cubo C generado con dos tetracubos, solamente pueden haberse usado dos OO, dos 3D, dos DD o dos II (Rupérez y García, 2009).

Este resultado habilita el enunciado de los siguientes convenios: designaremos con las letras OO, 3D, DD e II el correspondiente tetracubo y el único cubo generado con dos de dichos tetracubos. Sabremos distinguir el objeto al que nos referimos según el contexto. Los modelos físicos correspondientes los designaremos, globalmente, como "cubos marcados". Para conocer su "marca" u "origen" hay que desmontarlos y ver los tetracubos que los componen. En las figuras 10 a 13 mostramos la construcción de los cuatro cubos marcados. No tendría sentido mostrar los cubos terminados, serían indistinguibles. Con cubos marcados construiremos dicubos y tricubos marcados.


Figura 10: Cubo OO


Figura 11: Cubo 3D


Figura 12: Cubo DD


Figura 13: Cubo II

Otro resultado obvio es el siguiente: DD e II se transforman uno en otro de dos maneras: la primera, por reflexión con respecto a un plano (por eso son enantiomorfos[2]) y la segunda, girando un ángulo llano, con respecto al eje AB, uno de los dos dicubos que no yacen totalmente en ese eje. (Ver figura 14.) Estos resultados permiten cambiar la caracterización operacional dada para estos tetracubos en un apartado anterior. Si, en lugar de "encima", escribimos "debajo", volveremos a obtener ambos tetracubos, pero en distinto orden.

[2]El resultado de que los tetracubos DD e II son imágenes especulares el uno del otro o enantiomorfos, puede verse, por ejemplo en Rupérez y García (2010)., pero es bien conocido desde mucho tiempo atrás.

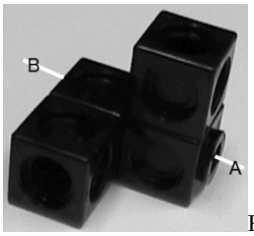


Figura 14

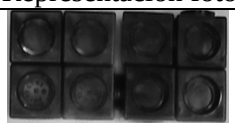
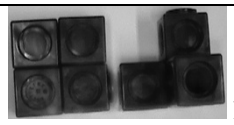
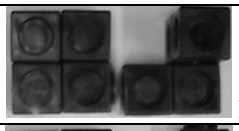
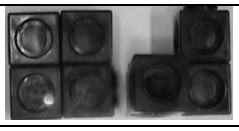
No estudiamos la generalización de lo dicho hasta ahora. Por ejemplo, el siguiente policubo que podría dar un cubo (macizo) por adición de dos policubos congruentes sería el 32-cubo; en general, habría que estudiar los policubos de orden 2^{3n-1}. Otra generalización posible, que tampoco hemos estudiado, se refiere al uso del cubo de Soma u otras configuraciones.

5. Códigos con diez caracteres

Si se usan los 4 cubos marcados para construir dicubos, se obtienen *varios* dicubos, en lugar de uno solo. Enunciaremos por ello un nuevo convenio: al usar cubos marcados, consideraremos diferentes dos dicubos si difieren al menos en un cubo marcado. En particular, el orden en que se coloquen dos cubos marcados no es relevante. Este convenio negativo es esencial para aplicar movimientos a los dicubos sin por ello cambiar el código asociado. Por ejemplo, solamente hay un dicubo formado con los cubos OO y 3D. Este dicubo lo simbolizamos así: OO+3D

Los tetracubos OO, DD, 3D e II constituyen un alfabeto básico que permite inventar claves para representar números usando los cubos indicados.

Con los cubos marcados se obtienen diez dicubos (ver figuras 15 a 24[3]), a los que haremos corresponder las diez cifras del sistema de numeración habitual, como muestra la tabla 1. Si necesitamos una base mayor que diez, resulta fácil y posible cambiar la representación.

Cifra	Dicubo	Representación fotográfica
0	OO+OO	 Figura 15
1	OO+3D	 Figura 16
2	OO+DD	 Figura 17
3	OO+II	 Figura 18

[3]En las figuras 15 a 24 se han usado tetracubos, no cubos marcados, ya que éstos son indistinguibles en foto plana. Coriat, M. y Cañadas, M. C. (junio, 2011). *Cifrado con cubos marcados*. Trabajo presentado en el II Encuentro AprenGeom. CIEM, Castro Urdiales, Santander.

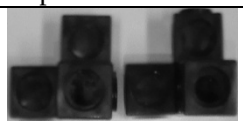
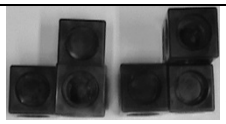
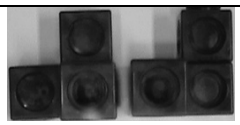
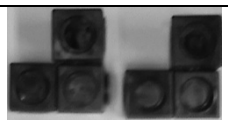
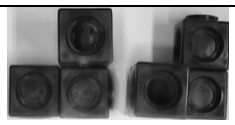
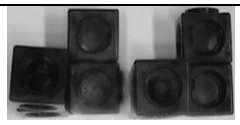
Cifra	Dicubo	Representación fotográfica
4	3D+3D	 Figura 19
5	3D+DD	 Figura 20
6	3D+II	 Figura 21
7	DD+DD	 Figura 22
8	DD+II	 Figura 23
9	II+II	 Figura 24

Tabla 1: Emparejamiento de dicubos marcados y códigos para las cifras de la base diez.

La clave establecida en la tabla 1 es arbitraria, cualquier permutación de la primera columna de esa tabla genera *otra* clave. Hay, por tanto, 10! maneras de codificar los números en base diez. Si alguien intenta adivinar la clave que otro haya establecido a partir de los elementos existentes, calculando cada una de las permutaciones, es necesario determinar una de 3628800 posibilidades. Por ejemplo, si un banco decidiera usar esta clave para cambiar cada día, internamente, el código de emparejamiento de las tarjetas de crédito, intentando así evitar pirateos aleatorios, dispone de unos diez mil años para que se repita un emparejamiento.

A partir de la tabla 1, la tabla 2 muestra dos representaciones del número 18, una simbólica, otra gráfica.

18	OO+3D,DD+II	 Figura 25

Tabla 2: Varias representaciones de un número de dos cifras

En la figura 25 se muestran, sucesivamente, los tetracubos OO, 3D, II y DD. Los correspondientes dicubos, hechos con cubos marcados, son OO+3D y DD+II. Finalmente, el convenio relativo a la irrelevancia de la permutación de cubos marcados en un dicubo, lleva a concluir la cantidad que representa (18). Así, en la fotografía, no es necesario presentar en grupos más de dos cubos. La Figura 26 también representa el número 18.

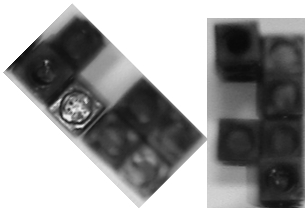


Figura 26. Otra representación del número 18. La decena se reconoce aquí por impregnación de la lectura de números, es decir, por el dicubo que está más a la izquierda. Para tener completa libertad de colocación de los dicubos, sería necesario añadir un código indicador de las decenas y las unidades.

6. Escritura alfanumérica con tricubos

Usando los 4 cubos marcados para construir tricubos, se obtienen *varios* de ellos.

Consideramos idénticos dos tricubos si, estando formados por los mismos tricubos, hay una isometría directa que transforma el uno en el otro. Por ejemplo, OO+OO+3D es igual que 3D+OO+OO porque hay una rotación que transforma el uno en el otro.

Además, sabemos que existen dos tricubos distintos el "I" y el "L" (ver figuras 1 y 2). Por tanto, cuando expresamos OO+OO+3D, podemos estar haciendo referencia a cualquiera de los dos tricubos. Centraremos nuestra atención en el tricubo "I" porque va a facilitar la expresión de las ideas y después extenderemos nuestro análisis al "L".

Tricubo "I"

Con los tres cubos marcados iguales, podemos construir 4 tricubos diferentes (OO+OO+OO, 3D+3D+3D, DD+DD+DD e II+II+II). Son combinaciones de 4 elementos tomados de 3 en 3 (C_3^4).

Con dos cubos iguales y uno diferente, podemos construir 24 tricubos. Teniendo en cuenta que para el primero podemos elegir uno cualquiera de los cuatro cubos marcados, ese tendría que ser el mismo para el segundo, y para el tercero podría ser cualquiera de los otros tres cubos marcados: esto aporta 12 posibilidades. Si el cubo diferente se coloca entre los dos cubos iguales, obtenemos un nuevo tricubo, por lo que las posibilidades de construcción anteriores se duplican, obteniendo 24 posibilidades. Por ejemplo, para el caso de un tricubo formado por dos "OO" y un "3D", tendremos las seis posibilidades indicadas en la tabla 3:

OO+OO+3D	OO+OO+DD	OO+OO+II
OO+3D+OO	OO+DD+OO	OO+II+OO

Tabla 3: Seis posibilidades con dos cubos iguales y uno distinto

Si esto se repite para cada uno de los cubos, multiplicaríamos por 4 las 6 opciones y obtendríamos 24 tricubos.

Son variaciones de cuatro elementos tomados de 2 en 2 y multiplicadas por 2 ($2V_2^4$)

Con tres cubos marcados diferentes se pueden construir tantos tricubos como permutaciones de cuatro elementos tomados de 3 en 3 dividido entre dos, es decir, 12 tricubos diferentes ($P_4 / 2$).

Así, tenemos 4+24+12=40 tricubos del tipo "I" diferentes. Análogamente, obtendríamos 40 tricubos del tipo "L". Finalmente, obtendríamos que se pueden construir 80 tricubos distintos. Expresándolo en lenguaje combinatorio, para los tricubos tenemos $2(C_3^4 + 2V_2^4 + P_4 / 2)$ posibilidades de generar códigos diferentes.

Si asignáramos un código arbitrario para dar significado a los 80 tricubos, podríamos conseguir un sistema de numeración en base 80 y habría 80! maneras de establecer un código.

Por ejemplo, podríamos asignar las 27 letras del alfabeto (A, B, C, etc.), los 10 elementos del sistema de numeración decimal (del 0 al 9) y 3 símbolos más. Así tendría 40 elementos a los que debería asignar un significado. Por tanto, tendríamos V_{40}^{80} claves diferentes para generar un código.

Por ejemplo, nos podríamos encontrar con la palabra HOLA. Tratándose de un código generado por medio de tricubos, cada carácter es un tricubo diferente. Dado que hay 80 tricubos diferentes, habría 80x79x78x77 posibles significados para esta palabra. Un posible significado sería: 3D+OO+OO, 3D+II+OO, DD+DD+II, II+II+II, pero esa sería una entre muchas.

7. Comentarios finales

Para construir un cubo 2x2x2 con tetracubos, es necesario contar con dos tetracubos iguales. Sólo con cuatro de los tetracubos se puede llegar a tener este cubo. Una vez construidos los cubos, es imposible saber con qué tetracubos se han construido, pues están encajados y son indistinguibles. La idea de "cubos marcados" permite diferenciar el tetraedro a partir del cual se obtiene el cubo. Recurrir a fotos cuando se está construyendo el cubo puede ayudar a la distinción pero no es operativo y por ello hemos recurrido a la nomenclatura OO, DD, II y 3D para diferenciar los cuatro cubos marcados diferentes que se pueden conseguir.

Uniendo dos cubos marcados 2x2x2, como los anteriores, obtenemos dicubos marcados. Con los cuatro cubos, podemos obtener 10 dicubos diferentes. Utilizando los elementos de la secuencia numérica (del 0 al 9) obtenemos 10! códigos posibles, en función del significado que demos a cada uno de los elementos de la secuencia numérica. Esto hace que utilizar esta forma de codificar dificulte la lectura de un mensaje cifrado mediante el código que elijamos de entre los 10! códigos posibles. El número de posibles códigos aumenta de forma considerable si, en lugar de dicubos, consideramos tricubos, ya que hay 80 tricubos marcados diferentes. Si aumentáramos el número de cubos que unimos,

tenemos una fuente inagotable de formas distintas de generar códigos que serían cada vez más difíciles de descifrar.

Como se ha mostrado para los casos de los dicubos y los tricubos, existe una relación entre la manipulación de los cubos mínimos y los códigos que se pueden establecer mediante la combinación de los mismos. Esta relación se puede expresar en términos de combinatoria elemental. El número de formas diferentes de establecer un código depende del número de cubos que se unan para formar los elementos del código (*n* para un *n*-cubo) y de los diferentes *n*-cubos que se pueden construir. Para el caso de los tetracubos, el número de posibles elementos para el código puede obtenerse mediante la aplicación de la combinatoria, involucrando permutaciones, variaciones y combinaciones. Esperamos avanzar en el trabajo con los tetracubos y obtener más resultados.

Desde el punto de vista educativo, el cifrado permite generar jugosos temas de conversación matemática; esto, unido a las oportunidades de visualización asociadas a las modelos geométricos de algunos policubos sencillos, aporta a la vez situaciones problemáticas para el trabajo conjunto de geometría y álgebra y deja abierta la puerta a indagaciones de los propios alumnos de Secundaria.

Consideremos como ejemplo el caso del álgebra escolar, tradicionalmente asociada con la resolución de ecuaciones y la manipulación de expresiones simbólicas. Los profesores se consideran muy satisfechos cuando los alumnos son capaces de seleccionar una buena representación de una situación; un profesor no solamente quiere que sus alumnos sepan pasar de $ax+b=0$, con a no nulo, a $x=-b/a$; también espera, poco a poco, que aprendan a interpretar el punto de corte de la recta $y=ax+b$ con el eje de abscisas, e incluso a discutir el posible cero del binomio $ax+b$. En todos estos casos, se trata de cambios en la manera de considerar una idea y todos ellos están orientados hacia una mayor abstracción, que choca con la tendencia mayoritaria de los alumnos a asociar siempre una letra con un número desconocido. En el apartado 5, usando la permutación de la tabla 1, caben discusiones sobre la representación de los órdenes de magnitud, o potencias de diez, asociados con cada dicubo: Si suponemos elegido el sentido de izquierda a derecha para representar el número 348, tendremos que mostrar la secuencia OO+II, 3D+3D, DD+II. Ahora tenemos la posibilidad de comparar esta representación del número con la escritura polinómica: $3 \times 10^2 + 4 \times 10^1 + 8 \times 10^0$ o incluso, 3centenas + 4decenas + 8unidades. Aquí no solamente hay símbolos nuevos para el 3, el 4 y el 8, también se han de establecer acuerdos sobre la colocación relativa de los dicubos correspondientes: ¿de izquierda a derecha?, ¿de arriba abajo? ¿criterios de lectura ordenada de tricubos? Comparaciones como la indicada, y muchas otras posibles, ayudan a desarrollar la capacidad de abstracción de los alumnos, tan necesaria para el álgebra elemental.

Agradecimientos

Nuestro agradecimiento a los participantes en el II AprenGeom que hicieron comentarios y sugerencias a la presentación, que se tendrán en cuenta para mejorar el trabajo en un futuro.

Referencias

Carson, G. S. (1973). Soma cubes. *Mathematics Teacher, 66*(7), 583-592.

Masalski, W. J. (1977). Polycubes. *Mathematics Teacher, 70*(1), 46-50.

McLoone, J. (26 de enero de 2011). Breaking secret codes with Mathematica. International Business & Strategic Development. http://blog.wolfram.com/2011/01/26/breaking-secret-codes-with-mathematica/

Rupérez, J. A. y García, M. García (2009). Las disecciones de cubos. Secuenciación en tamaños y dificultad como una propuesta didáctica. Estudio del cubo 2x2x2. Algunas presentaciones de cubos 3x3x3 y 4x4x4, y un reto. *Números, 72*, 129-139.

Rupérez, J. A. y García, M. García (2010). Graduación de la dificultad en el Cubo Soma (I). *Números, 75*, 165-173.

Sack, J. y Vázquez, I. (2008). Three-dimensional visualization: children's non-conventional verbal representations. En O. Figueras, J. L. Cortina, S. Alatorre, T. Rojano y A. Sepúlveda (Eds.), *Proceedings of the Joint Meeting of PME 32 and PME-NA XXX* (Vol. 4, pp. 217-224). Morelia, México: PME.

Spector, D. (1982). Soma: A unique object for mathematical study. *Mathematics Teacher, 75*(5), 404-407.