

Boletín del IMI, Nº 66 (3 de noviembre de 2022) <https://doi.org/10.57037/b-imi.00066>

5) 1+400. Divulgación con 1 imagen y 400 palabras

Roberto Santos Bueno, Matemáticas detrás de una llave,
Boletín del IMI, Nº 66 (3 Nov 2022), Sección "1+400. Divulgación con 1 imagen y 400 palabras."
<https://doi.org/10.57037/b-imi.00066.1mas400>

En esta sección se publican artículos cortos de divulgación, con una imagen y un máximo de 400 palabras (sin tener en cuenta en estas restricciones los datos de los autores). Las personas que quieran publicar un artículo pueden enviarlo a secreadm.imi@mat.ucm.es

La colección de todos los artículos publicados en esta sección se puede ver en www.ucm.es/imi/1mas400

Roberto Santos Bueno, autor de este artículo, es Doctor Ingeniero Industrial por la Universidad Pontificia Comillas. Tras varios años en consultoría estratégica, trabaja en la actualidad en una entidad financiera. Divulga Matemáticas, Física e Ingeniería en su cuenta de Twitter [@rober_fun](https://twitter.com/rober_fun)

Matemáticas detrás de una llave

Roberto Santos Bueno



La imagen es la llave de mi casa. Esconde muchas matemáticas, más allá de que el elemento de la cerradura en el que se inserta se llame cilindro.



Gracias al sistema llamado amaestramiento, además de la entrada a mi piso, puedo abrir las puertas exteriores de acceso a la urbanización, el portal y la rampa del garaje. Mi vecino también, pero ninguno puede abrir la casa del otro. Los vecinos del portal de al lado también abren el acceso al garaje que compartimos, pero los de un portal no podemos abrir los otros portales. En cambio, la llave del personal de mantenimiento abre todos los portales y, además, otros cuartos (instalaciones) que no abre la llave de ningún vecino.

Todo ello requiere una adecuada codificación de las llaves y los cilindros. Una solución sencilla, aunque ineficiente, sería usar un bit para cada cilindro y escribir en la llave un 1 si lo abre o un 0 en caso contrario; sin embargo, las llaves y cilindros imponen ciertas restricciones físicas que hacen inviable un sistema así: códigos con todo 0 o todo 1 no valen porque la llave resultante sería una pletina lisa, hay restricciones en los saltos que pueden darse de un “dígito” a otro y nadie quiere llaves enormes o carísimas que permitan los muchísimos códigos necesarios.

Veamos un ejemplo sencillo para ver la dificultad. Hay 2 portales con 5 viviendas cada uno y codificamos las llaves como número de portal-vivienda. Así, la llave 2-4 corresponde a la vivienda 4 del portal 2. Podemos poner entonces un cilindro en el portal 1 que se abra con cualquier llave que empiece por 1 y otro cilindro en el portal 2 que haga lo mismo para llaves que empiecen por 2 y así las llaves de las viviendas de cada portal podrán abrir el suyo y sólo el suyo. Pero con esta solución no hay forma de generar una llave que abra ambos portales.

En general es un problema de partición (cada cilindro divide el conjunto de llaves en aquéllas que lo abren y aquéllas que no) con jerarquía/ordenación (llaves que abren varios cilindros) que puede plasmarse en un grafo. Está clasificado como NP-complejo y requiere el uso de ordenadores. De hecho, los algoritmos empleados son considerados material confidencial por los fabricantes de estas cerraduras.

Instituto de Matemática Interdisciplinar
Universidad Complutense de Madrid
Plaza de Ciencias 3, 28040, Madrid
<https://www.ucm.es/imi>

Haga click aquí para recibir el Boletín del IMI / Click here to receive the Boletín del IMI
Para dejar de recibir el Boletín del IMI escriba a secreadm.imi@mat.ucm.es / To unsubscribe send an email to secreadm.imi@mat.ucm.es
Los anteriores boletines se pueden encontrar en / Previous bulletins can be found at <https://www.ucm.es/imi/boletín-del-imi>