UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Coloraciones de nudos y códigos correctores de errores

Autor: Gabriel Lladó Victoria

Director: Dr. Javier Gutiérrez
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 10 de junio de 2024

Abstract

In this work we study a recent connection between knot theory and code theory. Specifically we will see how to build error-correcting codes from the colorations of the knots and the correspondence established between some characteristics of the knots and the parameters of their associated codes.

Resumen

En este trabajo estudiamos una reciente conexión entre la teoría de nudos y la teoría de códigos. Concretamente, veremos cómo construir códigos correctores de errores a partir de coloraciones de los nudos y la correspondencia que se establece entre algunas características de los nudos y los parámetros de los códigos asociados.

2020 Mathematics Subject Classification. 57K10, 94B05

Agradecimientos

En primer lugar, quisiera agradecer a mi tutor del trabajo, el Dr. Javier J. Gutiérrez, su propuesta de trabajo y su ayuda y correcciones durante todos estos meses. Además quiero agradecer también al resto de profesores que me han impartido clases durante todo el grado su tiempo y su disponibilidad.

En segundo lugar, quisiera dedicarlo a mis padres y a mis hermanos, que siempre han sido mi mayor soporte en todo.

Quisiera también agradecer a todos los amigos que he conocido en la carrera y con los que he compartido estos cuatro años, ha sido para mí un regalo compartir este tiempo con ellos, disfrutar de los mejores momentos y apoyarnos en los más difíciles.

Por último quiero dedicar este trabajo a dos de mis grandes referentes: la hermana Clare y el Padre Henry, y a mi madre del Cielo: la Virgen María.

Índice

1. Introducción

La teoría de nudos es una rama de las matemáticas relativamente joven que nace aproximadamente en el siglo XVIII. Dicha rama consiste en abstraer matemáticamente un concepto cotidiano como es un nudo. Los nudos aparecen en muchísimos aspectos de la realidad, desde los nudos en los cordones de los zapatos a nudos en las moléculas de ADN. De hecho, la teoría de nudos es una rama de las matemáticas que, a lo largo de su corta historia, se ha relacionado con distintas ciencias como la química o la biología, entre otras. Una de las cosas que motivó el profundizar en ellos fue la hipótesis de Kelvin ya que, en un contexto en que se creía que el éter era la sustancia que llenaba todo el espacio, el físico y matemático Lord Kelvin decía que los átomos son nudos de este éter y los distintos elementos se deben a distintos nudos. Esto motivó a algunos matemáticos y físicos a empezar a indagar y clasificar estos nudos. A pesar de que esta hipótesis resultó ser incorrecta, se comenzaron a descubrir un montón de nudos y propiedades muy interesantes, no solo a nivel matemático, sino también a nivel aplicado.

Estos nudos pueden ser proyectados en un plano y, una vez allí, pueden ser coloreados de tal manera que, cada vez que haya un cruce de hebras, éstas sean todas del mismo color o todas de diferente color. Si asociamos a cada color un número, podemos luego expresar los colores de cada hebra como un vector de dimensión el número de hebras del nudo proyectado.

Lo que veremos en este trabajo es que podemos asociar al conjunto de vectores que colorean el nudo de la manera descrita un código lineal. He aquí una de las varias aplicaciones que pueden tener los nudos, y es la de generar códigos lineales que pueden ser usados para enviar mensajes con información extra que pueda ayudarnos a detectar y corregir los posibles errores que puedan surgir.

Esto es lo que se conoce como códigos detectores y correctores de errores y son actualmente una importante herramienta para muchas empresas en el tema de la fiabilidad de los datos obtenidos. Los datos aumentan sin cesar y su envío y distribución también. Por eso, se ha convertido en algo prioritario el poder almacenar, enviar y recibir datos de manera segura y fiable, aunque también eficiente. Es decir, necesitamos una manera de asegurar que nuestros datos son correctos sin que esto pueda causar grandes costes de memoria o eficiencia. En este trabajo nos centraremos sobre todo en los códigos lineales porque se usan bastante debido a sus buenos resultados y su sencillez.

Nuestro objetivo es descubrir en que se basa la relación que hay entre los códigos correctores de errores y las coloraciones de un nudo. Es decir, queremos relacionar dos campos como lo son la teoría de nudos y la teoría de códigos que aparentemente no tienen nada que ver y ver si se aportan algo entre ellas. Para ello, trataremos las nociones básicas tanto de la teoría de nudos como de la de códigos para, finalmente, poder explicar y entender la correspondencia entre ambas y cómo algunas propiedades de los nudos se transmiten a las de sus códigos asociados y viceversa.

Estructura de la Memoria

En el primer capítulo introduciremos todos los conceptos que necesitaremos a lo largo del trabajo sobre la teoría de nudos, dotando de especial relevancia a los invariantes y la coloración de Fox junto con la matriz de Alexander.

En el segundo capítulo introduciremos las definiciones y resultados más importantes

sobre la teoría de códigos para este trabajo. Nos centraremos, en especial, en códigos lineales y en algunas de sus características y parámetros en cuanto códigos y en cuanto a su capacidad para detectar y corregir errores.

En el tercer y último capítulo hablaremos de como asociar códigos lineales a nudos, por medio de su coloración. De esta relación surgirán nuevos invariantes y métodos para construir códigos con propiedades que pueden ser de utilidad. Además, terminaremos la sección estudiando si todos los códigos pueden estar asociados a un nudo.

2. Teoría de nudos

En esta sección comenzaremos definiendo qué es un nudo matemático e introduciremos todos los conceptos básicos relacionados que sean necesarios para el objetivo de este trabajo. La mayoría de definiciones y resultados se encuentran en [15], [16] y [11].

2.1. Definiciones y conceptos básicos

La idea de nudo matemático no es muy distinta a la idea de nudo de unos zapatos o de un nudo marinero, pero con los extremos enganchados. Es decir,

Definición 2.1. Un *nudo (matemático)* K es un subespacio topológico del espacio Euclidiano $\mathbb{R}^3$ que es homeomorfo al círculo unidad $\mathbb{S}^1 \subseteq \mathbb{R}^2$, dotado de la topología euclidiana inducida, donde $\mathbb{S}^1 = \{(x, y) \mid x^2 + y^2 = 1\}$.

Veamos tres de los nudos más típicos que nos servirán como ejemplo en varias ocasiones:

Ejemplos 2.2.

Figura 1: Nudo trivial

Figura 2: Nudo trébol

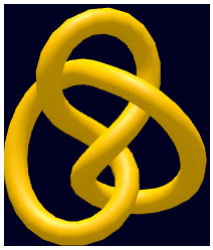


Figura 3: Nudo ocho

Una parte esencial de la teoría de nudos es la equivalencia entre nudos, que desarrollaremos más adelante.

Definición 2.3. Dados dos nudos $K_1, K_2 \subseteq \mathbb{R}^3$, decimos que son *equivalentes* (o del mismo tipo) si existe un homeomorfismo $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ tal que $f(K_1) = K_2$.

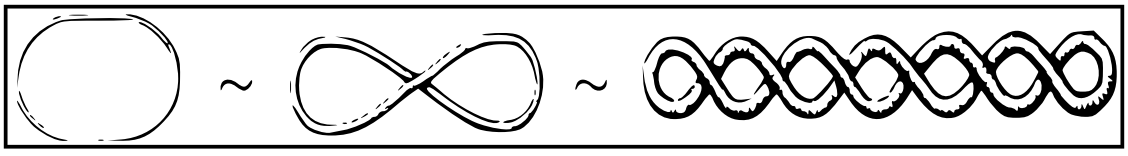


Figura 4: Nudos equivalentes al trivial

Observación 2.4. A la definición de nudo y de equivalencia podríamos añadir el concepto de orientación. Con *orientación* hacemos referencia al sentido en que se recorre el nudo. Si nos situamos en cualquier punto del nudo, tenemos dos orientaciones posibles: derecha e izquierda. La definición de equivalencia para nudos orientados sería la misma pero añadiendo que se tiene que preservar la orientación. En general, no trabajaremos con la orientación.

Para hablar de nudos, durante todo el trabajo, los visualizaremos y estudiaremos usando sus proyecciones en dos dimensiones, a lo que llamaremos diagrama del nudo. Para definir estos diagramas usaremos los siguientes conceptos:

Definición 2.5. Una *curva* es la imagen de una función continua $\gamma : I \longrightarrow \mathbb{R}^3$, donde I es un intervalo de $\mathbb{R}$. Una curva es *cerrada* si $I = [a, b]$ y $\gamma(a) = \gamma(b)$. Si γ es inyectiva en el interior del intervalo, la curva se denomina *simple*. Una curva es un *segmento lineal* si $\gamma(t) = tu + v$ para $u, v \in \mathbb{R}^3$.

Definición 2.6. Un *nudo poligonal* es una curva simple y cerrada en $\mathbb{R}^3$ que consiste en la unión de un número finito de segmentos lineales. Estos segmentos lineales son las *aristas* y sus extremos son los *vértices* del nudo. Cuando un nudo es equivalente a un nudo poligonal lo llamaremos *dócil*. En caso contrario lo llamaremos *salvaje*.

Observación 2.7. Podemos pensar en los nudos salvajes como los que no podemos construir con una cuerda en la vida real mientras que los dóciles son los que sí que podríamos.

En la Figura 5 vemos que el nudo trébol es un nudo dócil y vemos su equivalente nudo poligonal. En la Figura 6 tenemos un ejemplo de nudo salvaje:

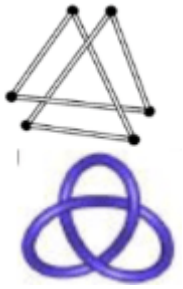


Figura 5: Nudo dócil

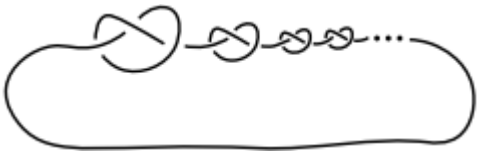


Figura 6: Nudo salvaje

Observación 2.8. En general, si no se dice lo contrario, los nudos que estudiaremos serán los dóciles, entre otras razones porque varios de los invariantes que luego mencionaremos solo se dan en los dóciles.

Definición 2.9. Sea $p : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ definida como $p(x, y, z) = (x, y, 0)$. La proyección de un nudo poligonal K es $p(K)$ junto con la orientación heredada de K, en caso de que hubiera. Diremos que la proyección es *regular* si satisface estas 3 condiciones:

1. $p(K)$ tiene un número finito de puntos de intersección, donde Q es un *punto de intersección* de $p(K)$ si $|p^{-1}(Q)| > 1$. Es decir, no tenemos segmentos enteros que se nos solapen al hacer la proyección.

2. Si Q es un punto de intersección de $p(K)$, entonces $K \cap p^{-1}(Q)$ tiene exactamente 2 puntos. Este punto se denomina *punto doble* de $p(K)$. Es decir, el nudo no puede pasar más de dos veces por el mismo punto en su proyección.

3. Un vértice de K no tiene como imagen un punto doble de $p(K)$. Es decir, un cruce no puede tener lugar en el vértice.

Observación 2.10. Esta definición de proyección regular es válida para todos los nudos dóciles (equivalentes a un poligonal). Podemos pensarlo como si hiciéramos tres pasos. Dado un nudo dócil, lo convierto en su poligonal, lo proyecto y le devuelvo su forma original, respetando las dos primeras condiciones de proyección regular.

Ahora ya podemos definir lo que es un diagrama del nudo (aunque ya los hemos usado sin mencionarlo) y qué partes lo componen:

Definición 2.11. Un *diagrama del nudo* K es una proyección regular de K con una alteración: para distinguir si el nudo pasa por encima o por debajo de sí mismo, dibujaremos la proyección con pequeños cortes para indicar que la parte cortada está pasando por detrás de la que no lo está.

Veamos como ejemplos los diagramas de los nudos del Ejemplo 2.2:

Ejemplos 2.12.

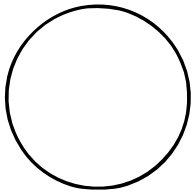


Figura 7: Nudo trivial

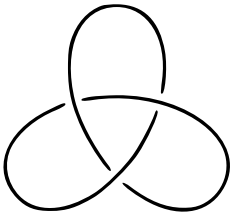


Figura 8: Nudo trébol

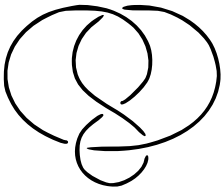


Figura 9: Nudo ocho

Como vemos en el Ejemplo 2.12, nos queda una proyección formada con arcos separados a los cuales llamaremos *hebras*. Al punto doble en lo llamaremos *cruce*. En cada cruce, a las dos hebras que están separadas por el corte les llamaremos *understrands* ("hebras inferiores") y a la otra hebra que va por encima, *overstrand* ("hebras superiores"). Por último, a las áreas delimitadas por las hebras y al área exterior del diagrama se las denomina *regiones*.

Observación 2.13. Observemos que un diagrama de un nudo no es único, puede haber infinitas proyecciones regulares. Para facilitar las cosas, se suele trabajar con un diagrama que contenga el mínimo de cruces posibles, aunque aún así, seguimos sin tener unicidad.

Vemos también que estas partes están relacionadas entre sí:

Lema 2.14. *Sea D un diagrama de nudo con $n \geq 1$ cruces. Entonces hay n hebras y $n+2$ regiones.*

Para demostrar este lema veamos un par de resultados de la teoría de grafos [1] y [8]:

Lema 2.15. (Handshacking) *Dado un grafo simple (es decir, que acepta como mucho una arista por cada dos vértices y no hay aristas que tengan sus dos extremos en el mismo vértice), la suma de los grados (número de aristas incidentes al vértice) de los vértices del grafo es igual al doble del número de aristas del grafo.*

Teorema 2.16. (de Euler) *Dado un grafo plano (que puede ser dibujado en el plano sin que ninguna arista se cruce), se cumple que :*

$$caras + vértices - aristas = 2$$

Y veamos un ejemplo de como convertir un diagrama de un nudo en un grafo, por ejemplo con el nudo trébol:

Ejemplo 2.17. La idea es que cada cruce se convierta en un vértice y cada understrand se convierta en una arista. Las overstrands las representaremos con 2 aristas cortadas, como si no fueran la misma hebra.

Consideramos, por ejemplo, el nudo trébol de la Figura 8. Aplicando los cambios mencionados nos queda el grafo de la Figura 10. Observemos que el resultado es un grafo plano en que cada vértice tiene grado 4.

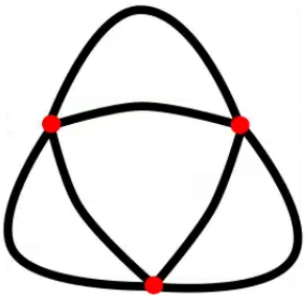


Figura 10: Grafo del nudo trébol

Ahora ya podemos demostrar el lema con ayuda de la demostración que aparece en [15]:

Lema 2.14. Construimos un grafo a partir del diagrama D con el método usado en el Ejemplo 2.17. El resultado es un grafo plano en el que cada vértice tiene grado 4 así que podemos aplicar el Lema 2.15 y el grafo tiene $\frac{1}{2}\sum_{i=1}^{n} grado(v) = \frac{1}{2}\sum_{i=1}^{n} 4 = 2n$ aristas. Teniendo en cuenta que en cada uno de los n vértices hay dos aristas que cuentan como una overstrand, tenemos que el diagrama tiene $2n - n = n$ hebras. Y sustituyendo en la fórmula del Teorema 2.16 obtenemos que hay $n + 2$ regiones. □

Ejemplo 2.18. Veamos algunos ejemplos:

- Si representamos el nudo trivial con $n = 0$ cruces como en la Figura 7, entonces el lema no se cumple porque no se satisface $n \geq 1$.En este caso tenemos 1 hebra y 2 caras.
- Si representamos el nudo trivial con $n = 1$ cruce como en la Figura 4, entonces el lema ya sí que se cumple: tenemos 1 hebra y $1 + 2 = 3$ caras.
- En el caso del nudo trébol como aparece en la Figura 8 tenemos 3 cruces y, por tanto, 3 hebras y 5 caras.
- En el caso del nudo ocho como aparece en la Figura 9 tenemos 4 cruces, 4 hebras y 6 caras.

2.2. Movimientos de Reidemeister y el problema central de la teoría de nudos

El hecho de que podamos transformar un nudo en otro equivalente, siempre y cuando no cortemos ni peguemos, nos induce a pensar que sus diagramas también se pueden ver afectados. De hecho, en 1927, Kurt Reidemeister demostró que todos los movimientos permitidos para pasar de un diagrama de un nudo a un diagrama de un nudo equivalente

se pueden resumir en tres. Estos son conocidos como los *movimientos de Reidemeister* y consisten, básicamente, en enredar una hebra sobre sí misma, mover una hebra por delante o por detrás de otra y mover una hebra por delante o por detrás de dos hebras que se cruzan.

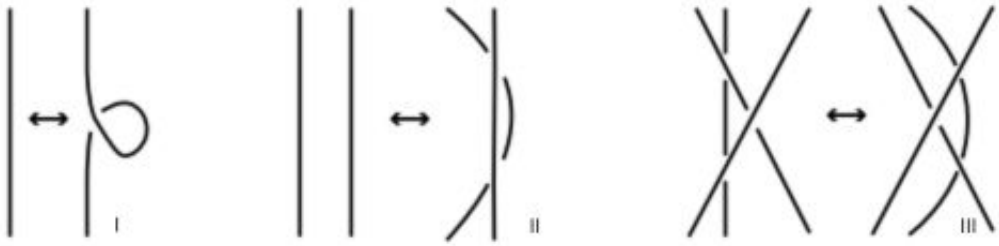


Figura 11: Los movimientos de Reidemeister: I, II y III

Observación 2.19. Como hemos mencionado, los movimientos de Reidemeister II y III incluyen también el mismo movimiento pero de manera que, la hebra que en la Figura 11 va por detrás, vaya por delante, y viceversa.

Estos tres movimientos nos permiten definir la equivalencia entre dos diagramas de nudos y, gracias al Teorema 2.21, demostrado en [17], hablaremos de equivalencia entre nudos y entre sus diagramas indistintamente.

Definición 2.20. Dos diagramas D y D' se denominan *equivalentes*, y se denota $D \sim D'$, si D se puede transformar en D' usando una secuencia finita de movimientos de Reidemeister.

Teorema 2.21. *Sean D y D' diagramas de los nudos K y K' respectivamente. Entonces, $K \sim K'$ si y solo si $D \sim D'$.*

Veamos un ejemplo de uso de los movimientos de Reidemeister para obtener diagramas equivalentes $D1$ y $D2$:

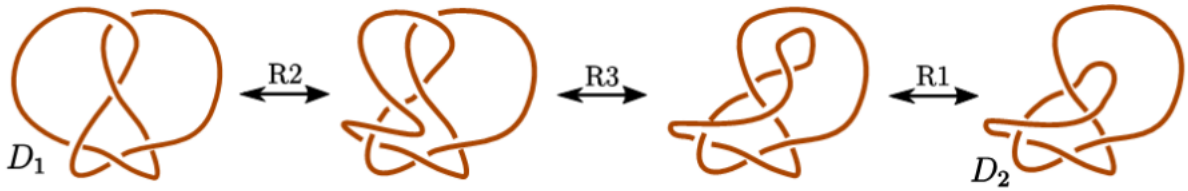


Figura 12: $D1 \sim D2$ por los movimientos de Reidemeister

El *problema central de la teoría de nudos*, sobre el cual giran la mayoría de investigaciones que se llevan a cabo en relación a nudos matemáticos, consiste en saber si, dados dos nudos, estos son equivalentes o no. Tratar de dar una respuesta a esta pregunta, si los nudos son muy sencillos como en la Figura 4, puede ser trivial pero, con nudos complejos, puede ser extremadamente difícil. La Figura 12 nos muestra dos diagramas que son equivalentes pero sin los pasos intermedios no es evidente la equivalencia, y eso que no son nudos muy complicados. Con diagramas con más de 10 cruces necesitamos un método que nos ayude. Por eso, una técnica muy útil para estudiar la equivalencia entre dos nudos es por medio de los invariantes del nudo.

Definición 2.22. Un *invariante del nudo* f es una función que asigna a un nudo K un objeto algebraico $f(K)$ de manera que para dos nudos equivalentes K_1 y K_2, tenemos que $f(K_1) \sim f(K_2)$.

Observación 2.23. De aquí se deduce que, si un invariante de dos nudos no coincide, entonces no son nudos equivalentes. Además, para ver que un objeto algebraico es un invariante basta ver que se conserva por movimientos de Reidemeister.

Más adelante irán saliendo distintos invariantes.

2.3. La suma de nudos

Podemos obtener nuevos nudos mediante la composición de otros nudos gracias a la suma conexa:

Definición 2.24. Dados dos nudos orientados K_1 y K_2, definimos la *suma (conexa)*, que denotamos $K_1 \# K_2$ (o $K_1 + K_2$), como el nudo orientado que se obtiene tomando un arco arbitrario de una hebra arbitraria de los dos nudos y uniendo los extremos de ambos con dos nuevos arcos, de manera que estos dos arcos no se crucen y preserven la orientación.

Ejemplo 2.25. Veamos, por ejemplo, la suma conexa de dos nudos trébol orientados:

Figura 13: Suma de dos nudos trébol

Observación 2.26. La definición la hemos dado con nudos orientados pero se define de igual manera si no hay orientación.

Podemos ver además que el resultado de la suma de un nudo cualquiera con el nudo trivial es el mismo nudo.

Ejemplo 2.27. Lo comprobamos para una hebra cualquiera de un nudo cualquiera:

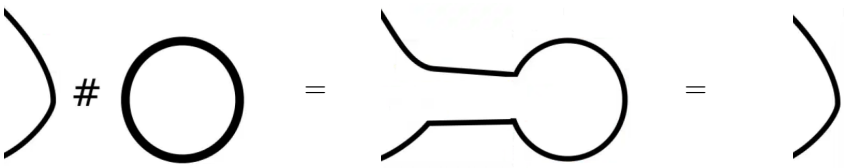


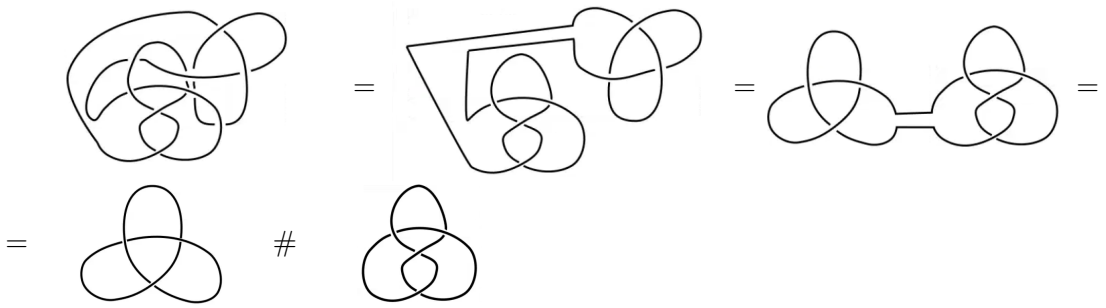
Figura 14: Suma de un nudo cualquiera y el nudo trivial

Observación 2.28. Se puede demostrar que la suma de los nudos no depende de la elección de las hebras.

Gracias al concepto de suma conexa podemos clasificar los nudos de manera análoga a como clasificamos los números en aritmética:

Definición 2.29. Un nudo *primo* es un nudo que no puede escribirse como la suma de dos nudos no triviales. Un nudo *compuesto* es un nudo que no es primo, es decir, que sí puede escribirse como la suma de dos nudos no triviales.

Y de la misma manera que un número compuesto se puede descomponer de manera única como producto de números primos, un nudo compuesto puede ser descompuesto unívocamente en la suma de nudos primos [16].



Observación 2.30. Del problema central de la teoría de nudos podemos deducir que determinar si un nudo es primo o no, no es tarea fácil.

2.4. Primeros invariantes y notación

Veamos ahora dos tipos muy útiles de diagramas y algunos invariantes que se deducen:

Definición 2.31. Decimos que un diagrama del nudo es *alternado* si al recorrer el nudo siguiendo una orientación fijada, en cada cruce nos encontramos con un understrand u overstrand alternadamente, o lo que es lo mismo, nunca pasamos dos cruces seguidos por encima o por debajo. Si un nudo tiene algún diagrama alternado, entonces se denomina *nudo alternado*.

Definición 2.32. Decimos que el diagrama de un nudo es *reducido* si no podemos eliminar ningún cruce. Es decir, es la manera de representar un nudo de la forma más simplificada posible.

Ejemplo 2.33. Los diagramas que hemos visto de los nudos trébol y ocho son alternados y reducidos.

Observemos que para nudos equivalentes, su diagrama reducido consistirá en un diagrama donde aparecerá el mínimo número de cruces que admita el nudo. Puesto que sus diagramas son equivalentes, es natural pensar que dos diagramas reducidos equivalentes tendrán el mismo número de cruces. Tenemos entonces nuestro primer invariante:

Definición 2.34. El *número de cruces* de un nudo es el mínimo número de cruces que puede tener un diagrama que lo represente.

Este valor es utilizado en la *notación de Alexander-Briggs* para organizar los nudos según el número de cruces que tienen. Para clasificar un nudo se pone el número de cruces junto con un subíndice que indica su posición respecto a los demás nudos con el mismo número de cruces. Esta clasificación se hace por clases de nudos, es decir, los nudos equivalentes estarán representados por un único nudo representante. Por establecer

un criterio, usaremos el orden de clasificación del libro [2]. Veamos algunos ejemplos de los nudos que hemos ido viendo tomados directamente del mismo [2], que, aunque aparecen sin especificar los understrands y overstrands de cada cruce en los diagramas, nos sirven para los ejemplos.

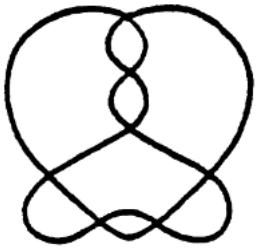


Figura 15: Nudo 7_3

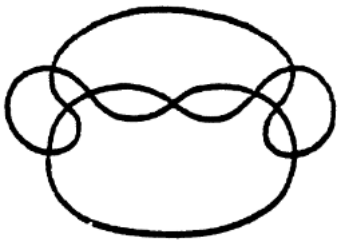


Figura 16: Nudo 9_{17}

Ejemplos 2.35.

- El número de cruces del nudo trivial es 0. Se escribirá como 0_1.
- El número de cruces del nudo trébol es 3. Se escribirá como 3_1.
- El número de cruces del nudo ocho es 4. Se escribirá como 4_1.

A partir $n \geq 5$ cruces, ya empezamos a tener más de un nudo con n cruces:

- El nudo de la Figura 15 tiene 7 cruces. Se escribirá como 7_3.
- El nudo de la Figura 16 tiene 9 cruces. Se escribirá como 9_{17}.

Veamos, para terminar la sección, otro invariante del nudo:

Definición 2.36. Dado un nudo K, decimos que una hebra que es una overstrand en al menos un cruce es un *puente*. El *número puente* $\beta(K)$ de un nudo es el mínimo número de puentes que puede tener un diagrama suyo.

Observación 2.37. En el caso de nudos alternados, todas las hebras son puentes, así que $\beta(K) = n$, siendo n el número de hebras de K.

2.5. Colorabilidad y matriz de Alexander

Como ya hemos visto, un diagrama de nudo con n cruces tiene n hebras y $n + 2$ regiones. Hay diferentes manera de colorear un nudo aunque las más conocidas son la coloración de Fox y la coloración de Dehn. Mientras que la coloración de Fox consiste en pintar las hebras de una manera determinada, la coloración de Dehn colorea por regiones. En este trabajo nos centraremos en la coloración de Fox aunque para la coloración de Dehn muchos de los resultados y propiedades son análogos.

Cuando hablamos de colorear un nudo, nos referimos a la asignación de elementos de un cuerpo finito $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$, donde q es un número primo, a cada una de las hebras.

Definición 2.38. Llamamos *coloración de Fox (o también q-coloración de Fox)* a la forma de colorear un diagrama de nudo asignando como colores elementos de $\mathbb{F}_q$ de manera que en cada cruce, las dos understrands (pongamos x_i y x_j) y la overstrand (pongamos x_k) cumplan la siguiente igualdad:

$$x_i + x_j - 2x_k \equiv 0 \qquad (mod\ \ q). \tag{2.1}$$

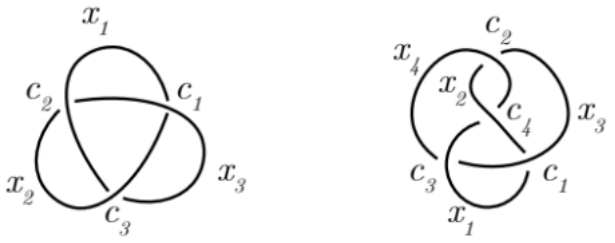


Figura 17: coloración de Fox de los nudos trébol (izquierda) y ocho (derecha)

El nudo trivial tiene un solo color. En el caso de nudos trébol y ocho, la coloración podría ser de la manera representada en la Figura 17, donde cada c_i representa el cruce en que las understrands son x_i y x_{i+1}, salvo el caso c_j con $j \geq i$, para todo i, que será el cruce entre x_j y x_1.

Notación 2.39. *Cuando hablemos de* colorear *un nudo, nos referiremos a la acción de asignar a cada hebra un elemento de* $\mathbb{F}_q$.

Observemos que la condición de la Definición 2.38 es equivalente a pedir que las tres hebras que se cruzan en cada cruce, tengan o bien las tres el mismo color, o bien las tres colores distintos. Comprobemos que pasa si tenemos el caso en que dos son de igual color y una distinta:

- Supongamos que $x_i = x_j \neq x_k$. Entonces, la condición la podemos escribir como $x_i \equiv x_k \pmod{q}$, contradiciendo la hipótesi.
- Supongamos que $x_i = x_k \neq x_j$. Entonces, la condición la podemos escribir como $x_i \equiv x_j \pmod{q}$, contradiciendo la hipótesi.
- El caso $x_j = x_k \neq x_i$ es análogo al primero.

Si las tres son del mismo color, $x_i = x_j = x_k$ y entonces $x_i + x_i - 2x_i \equiv 0$ siempre. Si las tres son de color distinto, podemos representar los colores como $x_i = 0$, $x_j = 2$ y $x_k = 1$, de manera que la ecuación se cumple. Observemos que en el caso $q = 2$ tenemos solo dos colores y tres hebras, así que no podremos colorear las tres hebras de distinto color.

Observación 2.40. Con esto hemos visto que es equivalente pedir que se cumpla la igualdad (2.1) que que todos los colores en cada cruce sean iguales o distintos. Sin embargo, en la práctica no siempre podremos usar los 3 colores: $0, 1, 2$, puesto que si se usan en un cruce es posible que no se puedan usar en otro. Por eso, hablaremos de como al construir un sistema de ecuaciones formado por esta igualdad en cada uno de los cruces, podremos encontrar qué colores sí que satisfacen la igualdad en cada cruce y obtendremos las $q-$coloraciones del nudo.

Definición 2.41. Decimos que una coloración de Fox es *trivial* si todas las hebras son del mismo color. Decimos que un nudo es *q-coloreable* si admite una coloración no trivial.

Podemos comprobar que la propiedad de la q-colorabilidad de un nudo no depende del diagrama que escojamos ya que es un invariante. Es decir, si un diagrama de un nudo es q-coloreable, todos los diagramas de ese nudo también lo son. Podemos comprobarlo

estudiando como se comporta esta propiedad en los movimientos de Reidemeister, cosa que veremos en la demostración del Teorema 4.6.

Para cada cruce de un nudo se tiene que cumplir la condición (2.1). Si el diagrama tiene n cruces, entonces tenemos un sistema de ecuaciones homogéneo con n ecuaciones y n incógnitas. El espacio de soluciones de este sistema será un subespacio vectorial de $\mathbb{Z}_q^n$ de *dimensión* $dim_q(K)$. Es interesante ver que no solo la q-colorabilidad es un invariante del nudo, sino que también el número de q-colorabilidades lo es. Este segundo invariante es mucho más potente que el primero al ser más concreto ya que, a la hora de distinguir si dos nudos son equivalentes o no, es más preciso conocer el número de q-colorabilidades que solo conocer si es o no $q-$coloreable.

Proposición 2.42. *El número de coloraciones de Fox de un diagrama de nudo es un invariante del nudo.*

La demostración de esta proposición es equivalente a la de la Proposición 4.6, así que la omitiremos.

Denotamos el número de coloraciones de Fox como $col_q(K)$. Del resultado anterior se deduce el siguiente:

Proposición 2.43. *Sea K un nudo y q un número primo. Entonces, $col_q(K) = q^{dim_q(K)}$.*

Demostración. Como acabamos de ver, los colores de una q-coloración de un nudo K son elementos de $\mathbb{Z}_q$, y, todas las formas de colorear un diagrama de K con n hebras, usando máximo q colores, son elementos de $\mathbb{Z}_q^n$, que tiene q^n elementos. Obteniendo las diferentes maneras de colorear por medio del sistema de ecuaciones homogéneo ya mencionado, obtenemos un subespacio vectorial de $\mathbb{Z}_q^n$ de *dimensión* $dim_q(K)$. La fórmula se deduce del hecho de que este subespacio tiene $q^{dim_q(K)}$ elementos diferentes (que son todas las combinaciones posibles de una base). □

Observemos además que el número de coloraciones de Fox está acotado inferiormente por el número de coloraciones triviales y superiormente por el número de coloraciones posibles (todos los elementos de $\mathbb{Z}_q^n$):

$$q \leq col_q(K) = q^{dim_q(K)} \leq q^n. \tag{2.2}$$

Volviendo al sistema de ecuaciones anterior, podemos estudiar su matriz de coeficientes que, como veremos más adelante, tendrá un papel fundamental en la relación con la teoría de códigos.

Definición 2.44. Sea un diagrama de un nudo K con n cruces $c_1, \ldots, c_n$ y sean $x_1, \ldots, x_n$ sus hebras. Definimos la *matriz de Alexander* o *matriz de coloración* o *matriz de cruces* M como la matriz que satisface que, para toda $q-$coloración x de las hebras, $Mx^T = 0$.

En el caso de que el diagrama de K sea reducido, podemos construirla de la siguiente manera:

$$M_{ij} = \begin{cases} -2, & \text{si } x_j \text{ es un overstrand en el cruce } c_i, \\ 1, & \text{si } x_j \text{ es un understrand en el cruce } c_i, \\ 0, & \text{en caso contrario.} \end{cases}$$

Es decir, es la matriz asociada al sistema de ecuaciones visto antes. Cualquier coloración de Fox posible cumplirá que el producto con la matriz de Alexander es el vector nulo.

Observación 2.45. Solamente podemos construir la matriz de esta manera en el caso de que no tengamos, en ningún cruce, una hebra que participe dos veces (una como understrand y otra como overstrand), por ejemplo, al aplicar el primer movimiento de Reidemeister (ver Figura 11), ya que entonces, en una misma casilla, tendríamos que poner el valor 1 y -2. Por eso, hemos puesto la condición de reducido, aunque es necesario recalcar que los movimientos de Reidemeister II y III no siempre tienen porque quedar excluidos.

Observemos que las ecuaciones pueden definirse para los no reducidos también pues, el caso de tener en un cruce solo dos hebras nos obligará a colorear las hebras de ese cruce del mismo color (para que se satisfaga que son todos iguales o todos diferentes) y, por tanto, estaremos en la situación $x + x - 2x = 0$.

En general, los resultados de esta sección, si no se dice lo contrario, usarán la matriz de coloreo construida a partir de un diagrama reducido.

Ejemplos 2.46.

- Una matriz del nudo trébol es $\begin{pmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$.

  Si tomamos una coloración posible, vemos que se cumple lo que acabamos de afirmar:

$$\begin{pmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

  Sin embargo, una coloración que no sea de Fox no anula el producto:

$$\begin{pmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}.$$

- Una matriz del nudo ocho es $\begin{pmatrix} 1 & 1 & -2 & 0 \\ 0 & 1 & 1 & -2 \\ -2 & 0 & 1 & 1 \\ 1 & -2 & 0 & 1 \end{pmatrix}$.

  De igual manera, comprobamos que una coloración de Fox como la trivial sí anula el producto:

$$\begin{pmatrix} 1 & 1 & -2 & 0 \\ 0 & 1 & 1 & -2 \\ -2 & 0 & 1 & 1 \\ 1 & -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

  y una que no lo sea, no:

$$\begin{pmatrix} 1 & 1 & -2 & 0 \\ 0 & 1 & 1 & -2 \\ -2 & 0 & 1 & 1 \\ 1 & -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \end{pmatrix}.$$

Se puede demostrar que si dos diagramas son equivalentes, entonces sus dos matrices de Alexander también lo son [3]. Dos matrices son equivalentes si pueden obtenerse de la otra operando secuencialmente de la siguiente manera [11]:

- Usando las operaciones básicas en filas (intercambiar filas, combinar linealmente filas y multiplicar una fila por un escalar no nulo) y en columnas (similar).
- Añadiendo o eliminando una fila nula.
- Añadiendo o eliminando un pivote. Dada una matriz A $n \times m$ y una matriz B $(n+1) \times (m+1)$, B se obtiene añadiendo un pivote a A si es el resultado de añadir una fila y una columna al final, con todas las entradas 0 excepto un 1 en la posición $(n+1, m+1)$. De la misma manera, A se obtiene eliminando un pivote de B si podemos eliminar la útlima fila y la última columna siendo estas nulas en todas sus entradas excepto en la entrada $(n+1, m+1)$.

Debido a que el sistema de ecuaciones mencionado siempre tiene al menos soluciones triviales (y por tanto soluciones distintas de 0), siempre se cumple $det(M) = 0$. Sin embargo, es más interesante fijarnos en el determinante de uno de los menores $(n-1) \times (n-1)$ de la matriz.

Definición 2.47. El *determinante de un nudo* K, que denotaremos $det(K)$, es el valor absoluto del determinante de un menor cualquiera $(n-1) \times (n-1)$ de la matriz de Alexander.

Ejemplos 2.48.

- El determinante de la matriz Alexander del nudo trébol es:

$$det(\begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix}) = 3$$

- El determinante de la matriz Alexander del nudo ocho es:

$$det(\begin{pmatrix} 1 & 1 & -2 \\ 0 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix}) = -5$$

Observación 2.49. Este determinante no depende ni de la elección del menor, ni de la etiquetación de los cruces y hebras del diagrama, ni de la elección del diagrama [12]. Por eso, el determinante de un nudo es un invariante del nudo [15].

Proposición 2.50. *Dados un nudo K y un número primo p, K es p-coloreable si y solo si $p \mid det(K)$.*

Demostración. Sea M una matriz de cruce $n \times n$ de K. Como resultado de la Proposición 2.43, tenemos que es no trivialmente coloreable si y solo si la dimensión del espacio de soluciones es mayor que 1. Así, el rango de M tiene que ser menor que $n-1$ y por eso, cualquier determinante de un menor $(n-1) \times (n-1)$ de M será 0. Como estamos trabajando módulo p, $det(K) \equiv 0 \mod p$. Es decir, que $p \mid det(K)$. □

Ejemplos 2.51.

- Como el determinante de la matriz de coloreo del nudo trébol es 3, tenemos que el nudo trébol es 3−coloreable.
- Como el determinante de la matriz de coloreo del nudo ocho es -5, tenemos que el nudo ocho es 5−coloreable.

3. Teoría de códigos

En esta sección hemos recopilado la mayoría de información de [6] y [7].

3.1. Ideas generales

La teoría de códigos es una especialidad matemática, muy relacionada con el álgebra, que trata de las leyes de la codificación de la información. La situación que estudia es la siguiente: un *emisor* quiere enviar un *mensaje* mediante un *canal* a un *receptor*. El canal, generalmente, puede presentar dos tipos de problemas: ruido y falta de seguridad. El primer caso consiste en que el mensaje se recibe distorsionado debido a que el canal presenta ciertas condiciones desfavorables a las que llamamos ruido. Por ejemplo, manchas a la hora de leer un CD o señales de satélites que llegan muy debilitadas debido a su lejanía. El segundo caso consiste en que un tercero intercepta el mensaje y lo modifica o se lo queda sin permiso. De este tipo de casos se encarga la criptografía. Nosotros nos centraremos en el primer caso, que es la situación que se pretende solucionar o mejorar mediante los códigos detectores y correctores de errores.

El proceso que se utiliza para transmisión de información, sin tener en cuenta las medidas criptográficas, es el siguiente: hay un mensaje inicial que se codifica (usando un código que tanto el emisor como el receptos conocen) y se transmite por un canal. Durante este canal puede haber interferencias y se recibe un mensaje codificado (que finalmente se descodificará) que puede no ser el enviado. La idea es que de alguna manera se pueda deducir cuál era el mensaje enviado a partir de lo que hemos recibido. Es decir, queremos poder detectar qué errores ha habido y corregirlos a partir del código que se ha utilizado.

La estrategia de codificar consiste en añadir cierta información que luego, el recibir el código, nos permita deducir los errores que se hayan podido cometer y nos ayuden a corregirlos. Una de las cosas más importantes al escoger la codificación que usamos es que sea adecuado al canal. Es decir, si tenemos un canal que comete un error cada 10 dígitos, puede ser muy costoso usar un código que nos permita corregir un dígito de cada 2 y muy poco fiable uno que nos permita corregir solo un dígito de cada 100.

3.2. Códigos

Definición 3.1. Definimos un *alfabeto* como un conjunto $A = \{a_1, \ldots, a_q\}$ de cardinal $q \in \mathbb{N}$, al cual denominaremos *medida del alfabeto*, es decir, $q = |A|$. A los elementos de A los llamaremos *letras* y con un número finito de estas letras se pueden formar *palabras*, concatenándolas y escribiéndolas en forma de vector.

Ejemplo 3.2. Dado un alfabeto $A = \{a_1, a_2, a_3\}$, la medida del alfabeto es $q = 3$. Si tomamos la palabra $(a_3, a_2, a_2, a_1, a_3)$, su longitud es $n = 5$.

Definición 3.3. Un *código* C es un conjunto de palabras sobre un mismo alfabeto. Un *código de bloque* es un código que cumple que todas sus palabras tienen la misma longitud. Así, si n es la longitud, C el código y A el alfabeto, tenemos que $C \subseteq A^n$. Definimos también $M = |C|$ como la *medida del código* C y $k = log_q M$ como la *dimensión*.

Ejemplo 3.4. En el alfabeto A del Ejemplo 3.2, podemos tomar el código

$$C = \{(a_3, a_2, a_1, a_1), (a_2, a_1, a_2, a_1), (a_3, a_3, a_3, a_3)\}$$

que es, de hecho, un código de bloque dado que todas sus palabras tienen longitud $n = 4$, así que $C \subseteq A^4$. La medida del código es $M = 3$ y la dimensión es $k = log_3 3 = 1$.

A partir de ahora, si no se dice lo contrario, al hablar de códigos, nos referimos a códigos de bloque.

En general, codificar un mensaje consiste en sustituir el mensaje por palabras de un código C. La clave para poder detectar y corregir errores, será que las palabras de C sean entre sí lo más distintas posibles para facilitar la detección y corrección, como veremos más adelante. Primero, formalizamos el concepto de palabras distintas entre sí:

Definición 3.5. Dado un código C y dos palabras $x, y \in C$ de longitud n, definimos la *distancia de Hamming* entre $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ como el número de componentes en que difieren ambas. Es decir,

$$d(x, y) = |\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}|.$$

Y podemos demostrar que, efectivamente, es una distancia:

Proposición 3.6. *La distancia Hamming es una distancia en el conjunto de palabras que forman un código.*

Demostración. Solo necesitamos ver que se cumplen las tres condiciones de distancia para todo x, y, z pertenecientes a un código:

1. $d(x, y) = 0 \Leftrightarrow x = y$. Es evidente que son iguales si y solo si no tienen ninguna componente distinta.
2. $d(x, y) = d(y, x)$. Es evidente que tendrán el mismo número de componentes distintas.
3. $d(x, z) \leq d(x, y) + d(y, z)$. Observemos que si tomamos una componente i-ésima cualquiera de cada palabra, tenemos dos situaciones posibles. Si $x_i = z_i$ entonces, o bien $x_i = y_i = z_i$ o bien $x_i \neq y_i$ y $y_i \neq z_i$. Si $x_i \neq z_i$ entonces, $x_i \neq y_i$ y/o $y_i \neq z_i$. En ambos casos se cumple la desigualdad.

□

Ahora podemos definir un parámetro que será esencial a la hora de saber cuantos errores se pueden detectar y corregir según la codificación.

Definición 3.7. Dado un código C, definimos la *distancia mínima (Hamming)*, que denotamos por $d(C)$ como la menor de las distancias entre las palabras diferentes de C. Es decir,

$$d(C) = min\{d(x, y) \mid x, y \in C,\ x \neq y\}.$$

Notación 3.8. *Dado un código $C \in \mathbb{F}_q^n$, lo expresaremos como $[n, M, d(C)]_q$-código, siendo n la longitud, M la medida y $d(C)$ la distancia mínima. Si $q = 2$ (es decir, el alfabeto tiene dos letras), no lo especificaremos.*

Por último, usaremos un parámetro que nos medirá qué parte de la información que se transmite a través del canal corresponde al mensaje original. Este parámetro se conoce como *tasa (de transmisión)* y es el resultado de dividir la dimensión entre la longitud: $\frac{k}{n}$. De aquí se deduce que el valor que nos mide la parte que corresponde a la redundancia que hemos escogido es $1 - \frac{k}{n}$, y se denomina *tasa de redundancia*.

Ejemplos 3.9. 1. El *código trivial* es el que solo consta de una palabra y se expresa como $[n, 1, 0]_q$-código. Su tasa de transmisión es 0. Es pues un código inútil porque no nos permite transmitir información.

2. El *código total* es el conjunto total, el formado por todas las palabras con la misma longitud n fijada de un alfabeto de medida q. Se expresa como $[n, q^n, 1]_q$-código y su tasa de transmisión es 1, es decir, que enviamos el mensaje tal cual, sin añadir nada, y, por tanto, no podremos detectar ni corregir ningún error.

3. Dado un alfabeto $A = \mathbb{F}_q^n$, el código

$$R_q(n) = \{(a, \ldots, a) \mid a \in A\}$$

se denomina código de repetición y decimos que es un $[n, q, n]_q$-código. Su tasa de transmisión es $\frac{1}{n}$.

4. Sea $A = \mathbb{F}_2$. Entonces el código

$$C_1 = \{(0,0,0,0,0,0), (1,1,1,1,1,1), (1,0,1,0,1,0), (1,1,1,0,0,0)\}$$

es un $[6, 4, 2]$-código y tiene una tasa de transmisión de $\frac{log_2 4}{6} = \frac{1}{3}$.

5. Con el mismo alfabeto, el código

$$C_2 = \{(0,0,0,0,0,0), (1,1,1,1,1,1), (1,0,0,0,1,1), (0,1,0,1,1,0)\}$$

es un $[6, 4, 3]$-código y tiene tasa de transmisión también $\frac{1}{3}$. Sin embargo es mejor que C_1 porque tiene una distancia mínima más grande, lo que proporcionará un mayor numero de detecciones o incluso correcciones de error (las palabras están más separadas).

6. Con el mismo alfabeto, el código

$$C_3 = C_1 \cup \{(0,0,0,1,1,1), (0,1,0,1,0,1)\}$$

es un $[6, 6, 2]$-código y su tasa de transmisión es $\frac{log_2 6}{6} \approx 0,43 \geq \frac{1}{3}$. Así, C_3 es mejor que C_1 debido a su mayor tasa de transmisión, a pesar de que tienen la misma distancia mínima.

3.3. Detección y corrección de errores

Como hemos dicho anteriormente, por el canal enviamos un mensaje codificado. La estrategia para detectar si un código recibido contiene errores es comprobar si la palabra recibida forma parte del código. Si la palabra no forma parte del código podemos pedir una retransmisión o se marca como errónea la palabra en cuestión. La *capacidad detectora* de un código es el máximo número de errores que esta estrategia es capaz de detectar. Esta capacidad máxima está directamente relacionada con la distancia mínima del código utilizado para codificar:

Proposición 3.10. *Un código C nos permite detectar como mucho $d(C) - 1$ errores.*

Demostración. Supongamos que enviamos un código x y recibimos un código y, y se han producido menos de $d(C)$ errores. Entonces, por definición de distancia mínima, tenemos que $y \notin C$ y por tanto hay un error.
Si se produjeran $d(C)$ errores, entonces podría pasar que recibiéramos una palabra $y \in C$ que estuviera a distancia $d(C)$ de x y por tanto no podríamos detectar el error, puesto que la palabra recibida, aún perteneciendo a nuestro código, no sería la enviada. □

Ejemplos 3.11. Siguiendo con los Ejemplos 3.9,

1. Los códigos trivial y total tienen capacidad detectora 0.
2. El código de repetición detecta $n-1$ errores.
3. Los códigos C_1 y C_3 detectan un error, mientras que C_2, que como hemos visto tiene mayor distancia mínima, detecta 2 errores.

La estrategia para corregir errores consiste en que, enviado un código x, si recibimos un código y que no pertenece a nuestro código, entonces buscamos la palabra del código más cercana a y. En el caso en que la palabra más cercana no fuera x, esto no funcionaría. La *capacidad correctora* de un código es el número máximo de errores que esta estrategia puede corregir correctamente. También esta capacidad correctora está directamente relacionada con la distancia mínima:

Proposición 3.12. *Por medio del descodificador por mínima distancia se pueden corregir un máximo de* $\rho = \left[\frac{d(C)-1}{2}\right]$ *errores.*

Demostración. Sea un código C con distancia mínima $d(C)$. Supongamos que enviamos una palabra x y recibimos una palabra y tal que $d(x,y) \leq \rho$. Para ver que la corrección nos dará como resultado x, supongamos que existe $z \in C$ tal que $d(y,z) \leq \rho$. Entonces, $d(x,z) \leq d(x,y) + d(y,z) \leq 2\rho \leq d(C) - 1$. Tendríamos que la distancia mínima es $d(C)-1$, en contradicción con el enunciado. Entonces, x es la única palabra a distancia como mucho ρ y podríamos corregir la palabra.

Si, por el contrario, se producen $\rho+1$ errores habiendo enviado x y recibido y, entonces tenemos dos casos:

- Si $d(C)$ es par, $d(C) = 2(\rho+1)$. Entonces, si tenemos otra palabra $z \in C$ tal que $d(x,z) = d(C)$, podría ser que $d(z,y) = \rho + 1$ y en ese caso el descodificador no podría decidir si el mensaje correcto era x o z.
- Si $d(C)$ es impar, $d(C) = 2\rho + 1$. Entonces, si tenemos otra palabra $z \in C$ tal que $d(x,z) = d(C)$, podría ser que, dado que $d(x,y) = \rho + 1$, entonces $d(z,y) = \rho$. En este caso, el descodificador interpretaría que la palabra enviada era z, errando en la corrección.

□

Ejemplos 3.13. Siguiendo los Ejemplos 3.9,

- Los códigos trivial, total, C_1 y C_3 no pueden corregir ningún error porque tienen distancia mínima menor o igual que 1.

- El código de repetición es capaz de corregir $\left[\frac{n-1}{2}\right]$ errores, lo cual está bastante bien. Su defecto es que tiene una tasa de transmisión muy baja que disminuirá cuanto más aumente n, y eso significará que por cada mensaje que queramos enviar, tendremos que añadir una gran cantidad de dígitos que nos ayuden a controlar los errores.
- El código C_3 será capaz de corregir $2 - 1 = 1$ error.

Observación 3.14. No entraremos con más detalle en esto pero existen resultados que nos permiten agrupar estas dos proposiciones de manera que se puedan corregir y detectar errores a la vez, siempre y cuando el número de errores que quieras detectar y corregir estén acotados de alguna manera por la distancia mínima. Además existen diversas cotas, como la de Singleton, que veremos más adelante, o la de Gilbert, para lo que se conoce como *códigos óptimos*, que son los que tienen mayor medida de entre todos los códigos con una longitud y distancia mínima fijada.

Observación 3.15. Existe también la posibilidad de que conozcamos la posición de los errores, debido a que el mensaje puede llegar con borrones en posiciones específicas que podemos conocer. En este caso, el saber la posición de los errores aumenta la capacidad correctora hasta $d(C) - 1$, es decir, duplicaríamos esta capacidad respecto a cuando no conocemos la posición de los errores.

3.4. Códigos lineales

A partir de ahora trabajaremos con un tipo de códigos muy concreto, no solo por su sencillez, sino también por la ventaja de que nos permitirán operar con las palabras y letras. Estos serán los códigos lineales y nuestro alfabeto será un cuerpo finito $\mathbb{F}_q$. Una de las desventajas que tiene el restringirse a este tipo de códigos es que limitamos las opciones, pues q tiene que ser una potencia de un número primo . Aún así, su medida puede ser arbitrariamente grande.

Definición 3.16. Un *código lineal* C de longitud n es un subespacio vectorial de $\mathbb{F}_q^n$.

Tenemos pues que los códigos lineales son códigos de bloque dotados con la operación suma de vectores y producto por un escalar. Es decir, son códigos de bloque que nos permiten operar con palabras al tener las operaciones propias de un espacio vectorial.

Observación 3.17. Observemos que la dimensión de un código lineal como subespacio vectorial coincide con la dimensión definida para un código de bloque. Si esta dimensión es k, entonces podemos encontrar una base $v_1, \ldots, v_k$ del código y cada palabra del código se expresa de manera única como combinación lineal de esta base. De aquí que la medida del código sea $M = q^k$ y, por tanto, $k = log_q M$.

Notación 3.18. *En el caso de códigos lineales diremos que C es un $[n, k, d(C)]_q$-código.*

A partir de ahora, todos los códigos serán lineales si no se dice lo contrario. Una de las grandes ventajas de los códigos lineales es una simplificación que podemos hacer a la hora de calcular las distancias entre palabras y, por tanto, el cálculo de la distancia mínima.

Definición 3.19. Definimos el *peso de Hamming* de un elemento $x \in \mathbb{F}^n$ como el número de coordenadas no nulas que tiene y lo denotaremos como $w(x)$. Es decir,

$$w(x) = |\{i \in \{1, \ldots, n\} \mid x_i \neq 0\}|.$$

Proposición 3.20. *Dado $x \in \mathbb{F}_q^n$, $d(x,y) = w(x-y)$.*

Demostración. Usando las definiciones de distancia y peso podemos comprobar que $d(x,y) = |\{i \in \{1,\dots,n\} \mid x_i \neq y_i\}| = |\{i \in \{1,\dots,n\} \mid x_i - y_i \neq 0\}| = w(x-y)$. □

Proposición 3.21. *Dado un $[n,k,d(C)]_q$-código C (sobre $\mathbb{F}_q$), tenemos que*

$$d(C) = min\{w(x) \mid x \in C,\ x \neq 0\}$$

Demostración. $d(C) = min\{d(x,y) \mid x,y \in C,\ x \neq y\} = min\{w(x-y) \mid x,y \in C,\ x-y \neq 0\} = min\{w(z) \mid z \in C,\ z \neq 0\}$, donde en la primera igualdad es por definición, la segunda es por la Proposición 3.21 y la tercera es haciendo un simple cambio de variable $z = x-y$, en el que sabemos que $z \in C$ por ser C subespacio vectorial. □

Observación 3.22. Acabamos de obtener que, para calcular la distancia mínima de un código lineal solo hace falta mirar cual de todas las palabras no nulas tiene menor número de elementos distintos de 0.

Ejemplo 3.23. Sea $C \in \mathbb{F}_2^7$ un código lineal que tiene como base

$$\{(1,0,0,0,1,1,0),(0,1,1,0,1,0,0),(0,0,1,1,0,1,0),(0,0,0,1,1,0,1)\}.$$

Para calcular la distancia mínima necesitamos conocer todas las palabras de C:

$$\begin{aligned} C = \{&(0,0,0,0,0,0,0),(0,1,1,0,1,0,0),(0,0,1,1,0,1,0),(0,0,0,1,1,0,1),\\ &(1,0,0,0,1,1,0),(1,0,0,1,0,1,1),(1,0,1,1,1,0,0),(0,0,1,0,1,1,1),\\ &(1,0,1,0,0,0,1),(1,1,1,0,0,1,0),(0,1,1,1,0,0,1),(1,1,1,1,1,1,1),\\ &(0,1,0,1,1,1,0),(1,1,0,1,0,0,0),(0,1,0,0,0,1,1),(1,1,0,0,1,0,1)\} \end{aligned}$$

Nos llevaría muchísimo tiempo calcular la distancia mínima comparando todas las palabras entre sí. En cambio, gracias a la Proposición 3.21 solo tenemos que hacer 16 comprobaciones casi inmediatas (contar cuantos 1's tiene cada palabra). La distancia mínima resulta que es 3.

Trabajar con códigos lineales nos proporciona también la ventaja de asociarle una matriz. Sea C un $[n,k,d(C)]_q$-código y una base $v_1,\dots,v_k$ del código. Sabemos que toda palabra $c \in C$ se escribe de manera única como

$$c = m_1v_1 + \cdots + m_kv_k, \quad m_i \in \mathbb{F}_q, \text{ para todo } i.$$

Entonces, podemos expresar este sistema de ecuaciones matricialmente:

$$c = (m_1 \cdots m_k) \begin{pmatrix} v_{1,1} \cdots v_{1,n} \\ \vdots \quad\quad \vdots \\ v_{k,1} \cdots v_{k,n} \end{pmatrix} = mG$$

Definición 3.24. Una *matriz generadora* de un código lineal C es una matriz que tiene por filas una base de C.

Observación 3.25. Por como hemos definido la matriz generadora, tenemos que el rango es máximo, es decir, es igual al número de filas (por definición de base, el número de filas será menor o igual al número de columnas). Además, de la propia definición se deduce que $C = \{mG \mid m \in \mathbb{F}_q^k\} \subseteq \mathbb{F}_q^n$. Así, muchas veces que queramos definir un código podemos escribir sencillamente su matriz generadora.

Ejemplo 3.26. La matriz del código lineal del Ejemplo 3.23 es

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Observemos que si tenemos un mensaje cualquiera $m = (1, 1, 0, 1)$, entonces su codificación será $c = mG = (1, 1, 1, 1, 1, 1, 1)$. Una de las ventajas de tener la matriz generadora es que podemos obtener todas las palabras de C sin tener que ir comprobando todas las combinaciones lineales de la base. Simplemente se pueden coger todos los elementos de $\mathbb{F}_q^k$ y calcular su producto con G. Esto puede venir bien por ejemplo para cuando necesitas calcular la distancia mínima y quieres visualizar todas las palabras para luego poder contar cuantas letras de cada palabra son distintas de 0.

Podemos efectuar las transformaciones básicas de matrices: permutar filas, multiplicar filas por un escalar no nulo y sumar a una fila la combinación lineal de otras. No podemos sin embargo intercambiar columnas puesto que se pueden generar códigos distintos. En este caso, hablaremos de códigos equivalentes:

Definición 3.27. Decimos que dos códigos $C_1, C_2 \in \mathbb{F}^n$ de dimensión k son *equivalentes* si las palabras de uno se pueden obtener mediante las palabras del otro usando las siguientes operaciones:

- Permutar las coordenadas de las palabras (es decir, intercambiar columnas de la matriz generadora);
- Multiplicar por un escalar distinto de 0 las coordenadas de una posición dada (es decir, multiplicar por un escalar no nulo una columna de la matriz generadora).

3.5. Matriz de control

En este capítulo veremos otra matriz que podemos definir para un código y su relación con otros conceptos ya vistos. Esta matriz será muy importante a la hora de relacionar códigos y nudos.

Podemos definir un subespacio C de $\mathbb{F}_q^n$ por medio de un sistema de ecuaciones lineales homogéneo (y linealmente independiente, siendo $r = n - k$, donde k es la dimensión del código):

$$\begin{cases} h_{1,1}x_1 + \cdots + h_{1,n}x_n = 0 \\ \vdots \\ h_{r,1}x_1 + \cdots + h_{r,n}x_n = 0 \end{cases}$$

de manera que cualquier elemento $x \in C$ tiene que ser solución de este sistema, que matricialmente se puede expresar, siendo $x = (x_1, \ldots, x_n)$ un elemento de C y

$$H = \begin{pmatrix} h_{1,1} \cdots h_{1,n} \\ \vdots \quad \vdots \\ h_{r,1} \cdots h_{r,n} \end{pmatrix}$$

la matriz de coeficientes del sistema, como:

$$Hx^t = 0. \tag{3.1}$$

Dado que la matriz es de rango máximo, podemos decir que $r = rank(H)$ y lo llamaremos *codimensión.*

Definición 3.28. Una *matriz de control* o *matriz de chequeo de paridad* de un código lineal $C \subseteq \mathbb{F}_q^n$ es una matriz H de dimensión $r \times n$ que cumple que $x \in C$ si y solo si $Hx^t = 0$.

Existe una relación entre la matriz generadora y la matriz de control de un código [6]:

Proposición 3.29. *Sean $C_1, C_2 \subseteq \mathbb{F}_q^n$ códigos lineales de dimensión $k \geq 1$. Supongamos que G es una matriz generadora de C_1 y H una matriz de control de C_2. Entonces, $C_1 = C_2$ si y solo si $HG^t = 0$.*

Demostración. Supongamos que $HG^t = 0$ y sea $m \in \mathbb{F}_q^k$ un vector cualquiera tal que, como hemos visto en la Observación 3.25, $mG \in C_1$. Entonces,

$$H(mG)^t = HG^t m^t = 0 \cdot m = 0,$$

de lo que se deduce que $C_1 \subseteq C_2$. Esto, junto con el hecho de que $dim(C_1) = dim(C_2)$, implica que $C_1 = C_2$.

Recíprocamente, supongamos que $C_1 = C_2$ y sea $m \in \mathbb{F}_q^k$ arbitraria. Tenemos que $mG \in C_1$ y, por tanto, $mG \in C_2$. De esta inclusión se deduce la segunda igualdad:

$$HG^t m^t = H(mG)^t = 0$$

De la arbitrariedad de m, deducimos que $HG^t = 0$. □

De este resultado se puede deducir una manera de calcular la matriz de control a partir de la generadora [13]:

Proposición 3.30. *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión $k \geq 1$. Entonces C tiene una matriz generadora de la forma $G = (I_k|A)$ si y solo si C tiene una matriz de control de la forma $H = (-A^t|I_r)$, donde I_m es la matriz identidad de dimensión $m \times m$.*

Ejemplo 3.31. Siguiendo el Ejemplo 3.26, tratamos de darle a G la forma que exige la Proposición 3.30:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \underset{F_3 = F_3 - F_4}{\overset{F_2 = F_2 - F_3}{=}} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \overset{F_2 = F_2 - F_4}{=} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Tenemos ya la matriz identidad 4×4 y a la derecha la matriz

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Por la mencionada proposición, la matriz de control de este código tendrá la forma $H = (-A^t|I_r)$, donde $r = n - k$. Entonces, sabiendo que $q = 2$,

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Otro resultado interesante es ver como la distancia mínima de un código se puede calcular a partir de su matriz de control, cosa que puede simplificar muchos cálculos.

Proposición 3.32. *Sea C un código lineal con matriz de control H. La distancia mínima $d(C)$ es igual al mínimo número de columnas de H que son linealmente dependientes.*

Demostración. Denotamos $H_1, \ldots, H_n$ las columnas de H, $x = (x_1, \ldots, x_n) \in C \subseteq \mathbb{F}^n$ y w el peso mínimo del código. Entonces,

$$Hx^t = x_1H_1 + \cdots + x_nH_n = 0.$$

Si x tiene peso w, renombrando índices (en las primeras posiciones los $x_i \neq 0$), obtenemos que $x_1H_1 + \cdots + x_wH_w = 0$, así que hay w columnas linealmente dependientes. Y este número es mínimo pues, si hubiera $w-1$ columnas linealmente dependientes, existiría una palabra y de C tal que, nuevamente renombrando índices, $y_1H_1 + \cdots + y_{w-1}H_{w-1} = 0$ y $y_i = 0$ para todo $i \in \{w, \ldots, n\}$. Y esto implicaría que el peso mínimo no es w.

Recíprocamente, si sabemos que hay w columnas linealmente dependientes y que este número es mínimo, entonces $x_1H_1+\cdots+x_wH_w = 0$ y, como es mínimo, $(x_1, \ldots, x_w, 0, \ldots, 0)$ es el elemento con peso mínimo, es decir, la distancia mínima es w. □

Ejemplo 3.33. Veamos el caso de la matriz de control del Ejemplo 3.31

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

que ya hemos visto que pertenece a un código que tiene distancia mínima 3. Lo podemos comprobar viendo que ninguna de las columnas es nula ni hay dos columnas iguales y que las tres primeras columnas son linealmente dependientes pues suman cero. Así que, efectivamente, las distancia mínima es 3.

Por último vamos a dar una cota muy útil, que nos servirá para más adelante. Se conoce como la *cota de Singleton* y la demostraremos solo para códigos lineales [9]:

Teorema 3.34. *Sea C un $[n, k, d(C)]$-código. Entonces,*

$$d(C) \leq n - k + 1.$$

Demostración. Sabemos que la matriz de control tiene rango $n - k$, así que $n - k + 1$ columnas serán linealmente dependientes. De la Proposición 3.32 se deduce la desigualdad ya que la distancia mínima es el mínimo número de columnas linealmente dependientes. □

4. Relación entre nudos y códigos

4.1. Códigos asociados a nudos

El principal objetivo de esta sección es presentar la idea de definir códigos a partir de nudos y viceversa, con la idea de poder luego profundizar en esta relación entre nudos y códigos. Básicamente consideramos la posibilidad de que un código lineal sea una posible coloración de un diagrama de un nudo.

Dado un diagrama de un nudo con n hebras y una q-coloración de Fox (siendo q un número primo) de las hebras dada por el vector $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_q^n$, entonces se tiene que cumplir que, si M es la matriz de cruce del diagrama, $Mx^T = 0$. La idea es usar esto tratando x no solo como una coloración, sino también como una palabra de un código, y que, de esta manera, la matriz de control del código que contiene x venga dada por la matriz de coloreo de la coloración x de un diagrama de nudo.

Definición 4.1. Sea D un diagrama de un nudo, M su matriz de cruce. El *código asociado al nudo* del diagrama D (o el código asociado a D) es:

$$C_D = \{x \in \mathbb{F}_q^n \mid Mx^T = 0\}.$$

Ejemplos 4.2. A partir de las coloraciones de los nudos trébol y ocho que hemos visto en el Ejemplo 2.46, tenemos que sus códigos asociados son:

$$\begin{aligned} C_{D_{trébol}} &= \{x \in \mathbb{F}_3^3 \mid \begin{pmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix} x^T = 0\} \\ &=< (1,0,2), (0,1,2) > . \end{aligned}$$

y

$$\begin{aligned} C_{D_{ocho}} &= \{x \in \mathbb{F}_5^4 \mid \begin{pmatrix} 1 & 1 & -2 & 0 \\ 0 & 1 & 1 & -2 \\ -2 & 0 & 1 & 1 \\ 1 & -2 & 0 & 1 \end{pmatrix} x^T = 0\} \\ &=< (1,0,3,4), (0,1,3,2) > . \end{aligned}$$

Dos códigos asociados a dos diagramas de nudos equivalentes pueden ser equivalentes pero no es necesario que lo sean. Veamos un ejemplo en que no lo son:

Ejemplo 4.3. Sean el nudo ocho en su representación habitual y sea un nudo equivalente al nudo ocho, coloreados como en las Figuras 18 y 19.

Sus matrices de coloración son, respectivamente:

$$M = \begin{pmatrix} 1 & 1 & 0 & -2 \\ 0 & -2 & 1 & 1 \\ -2 & 1 & 1 & 0 \\ 1 & 0 & -2 & 1 \end{pmatrix} \qquad \text{y} \qquad M' = \begin{pmatrix} 1 & 1 & -2 & 0 \\ 1 & -2 & 0 & 1 \\ 0 & 1 & 1 & -2 \\ -2 & 0 & 1 & 1 \end{pmatrix}.$$

Sabemos que con esto podemos obtener las matrices de control de sus respectivos códigos asociados tomando el mayor número de filas linealmente independientes. Usamos

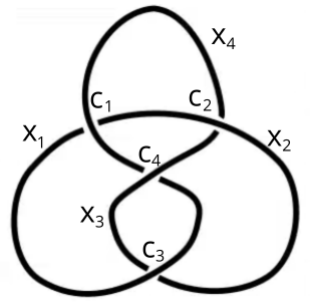


Figura 18: Nudo ocho etiquetado

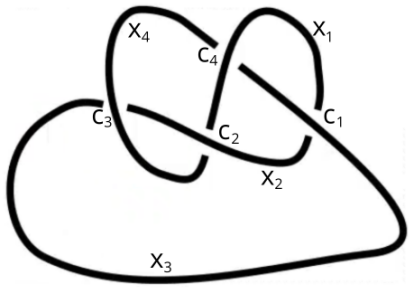


Figura 19: Nudo equivalente al nudo ocho etiquetado

la Proposición 3.30 para obtener la matriz generadora de cada código.

$$M = \begin{pmatrix} 1 & 1 & 0 & -2 \\ 0 & -2 & 1 & 1 \\ -2 & 1 & 1 & 0 \\ 1 & 0 & -2 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 3 & 1 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}.$$

La matriz de control corresponde a la matriz que tiene como filas las dos últimas filas de M. Como $-A^t = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}$, entonces, la matriz generadora del primero será:

$$G = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 4 & 3 \end{pmatrix}.$$

De la misma manera,

$$M' = \begin{pmatrix} 1 & 1 & -2 & 0 \\ 1 & -2 & 0 & 1 \\ 0 & 1 & 1 & -2 \\ -2 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 2 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{pmatrix}.$$

De nuevo, la matriz de control corresponde a la matriz que tiene como filas las dos últimas filas de M'. Como $-A'^t = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$, entonces, la matriz generadora del segundo será:

$$G' = \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 1 & 3 & 2 \end{pmatrix}.$$

Hay 3 columnas que son iguales. Si se cumpliera

$$\begin{pmatrix} 2 \\ 4 \end{pmatrix} \cdot x = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

para algún $x \in \mathbb{F}_5$ no nulo, entonces serían equivalentes, por la misma definición de códigos equivalentes. Los elementos no nulos de $\mathbb{F}_5$ son $\{1, 2, 3, 4\}$. Los comprobamos los cuatro:

$$\begin{pmatrix} 2 \\ 4 \end{pmatrix} \cdot 1 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 4 \end{pmatrix} \cdot 2 = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

$$\begin{pmatrix}2\\4\end{pmatrix}\cdot 3=\begin{pmatrix}1\\2\end{pmatrix}$$

$$\begin{pmatrix}2\\4\end{pmatrix}\cdot 4=\begin{pmatrix}3\\1\end{pmatrix}$$

obteniendo que, dado que la ecuación propuesta no tiene solución, entonces los códigos no son equivalentes, a pesar de estar asociados a nudos equivalentes.

Aunque vemos que los códigos asociados a los diagramas de nudos no tienen porque ser equivalentes entre ellos, y por tanto, no pueden ser invariantes del nudo, en la sección siguiente veremos algún invariante que se puede deducir de estos códigos.

Para terminar la sección, enunciaremos la conjetura de Kauffman y Harary, ya demostrada por Mattmann y Solis [14], para luego demostrar un resultado muy interesante sobre los códigos asociados a nudos [11]:

Teorema 4.4. *Sea D un diagrama de nudo reducido y alternado de un nudo K con determinante un primo p. Entonces, toda p-coloración de Fox no trivial de D asigna colores diferentes a hebras diferentes del diagrama.*

Proposición 4.5. *Sea D un diagrama de nudo reducido y alternado de un nudo K con n hebras y determinante p primo. Entonces, el código asociado a D es un $[n, 2, n-1]_p$-código sobre $\mathbb{F}_p$.*

Demostración. Por el Teorema 4.4, tenemos que cada coloración no trivial de D asigna colores distintos a hebras distintas. De esta manera, la distancia mínima será $n-1$ y vendrá dada por la distancia entre una coloración no trivial y una coloración trivial (pueden coincidir como mucho en un color). Así pues, como tenemos al menos una coloración no trivial y la trivial, la dimensión del código será mínimo 2. Por la cota de Singleton, $k \leq 2$. Entonces, los únicos posibles parámetros son dimensión 2 y distancia mínima $n-1$, obteniendo así un $[n, 2, n-1]$-código. □

De aquí podemos deducir que los diagramas alternados y reducidos cuando el determinante es primo (que, para números de cruce bajos, es lo habitual), entonces la capacidad correctora es $\left[\frac{n-1}{2}\right]$ y su tasa es $\frac{2}{n}$. Cuanto más grande es n, más crece la capacidad correctora pero más decrece la tasa. Para que sea útil, hay que enconctrar un equilibrio, según el caso. Hablaremos de esto también más adelante.

4.2. Dimensión y distancia mínima

Como ya hemos visto, los códigos de diagramas equivalentes no tienen porque ser equivalentes. Sin embargo, la dimensión nos podrá dar un poco más de juego, pues sí es un invariante del nudo:

Teorema 4.6. *La dimensión del código asociado a un diagrama de un nudo es un invariante del nudo.*

Usaremos la coloración de los movimientos de Reidemeister de la Figura 20 para la demostración:

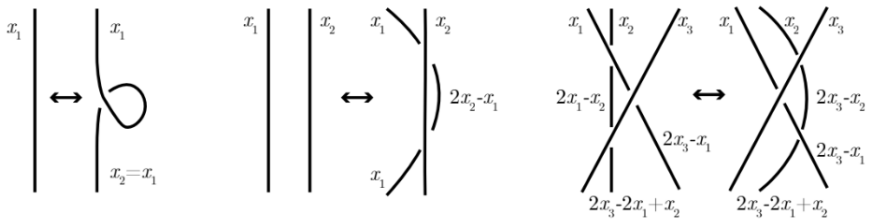


Figura 20: Coloración de los movimientos de Reidemeister

Demostración. Sean D y D' dos diagramas de nudos equivalentes y sean C_D y $C_{D'}$ sus respectivos códigos asociados. Supongamos que D tiene n hebras. Veremos qué pasa localmente con cada movimiento de Reidemeister, tal y como aparecen en la Figura 20. Supondremos, sin pérdida de generalidad, que sus partes abiertas no pertenecen a la misma hebra.

- Supongamos que D' se obtiene al aplicar una vez el primer movimiento de Reidemeister a D en la hebra x_1. Obtenemos dos hebras que serán understrands y una de ellas será también overstrand. El color asignado a ambas es necesariamente el mismo (sino, no habría coloración de Fox), así que si la $k \times n$ matriz generadora de C_D de rango máximo es

$$G = \begin{pmatrix} | & | & | \\ \cdots & x_1 & \cdots \\ | & | & | \end{pmatrix}$$

  entonces la matriz generadora de $C_{D'}$ será

$$G' = \begin{pmatrix} | & | & | & | \\ \cdots & x_1 & x_1 & \cdots \\ | & | & | & | \end{pmatrix}.$$

  Lo que estamos afirmando es que si aplico una vez el primer movimiento de Reidemeister en x_1, la nueva hebra que se forma tiene el mismo color siempre. Así, todas las coloraciones que haya para este nuevo nudo serán las mismas que para el anterior pero con un nuevo valor (que aumenta la longitud de las palabras del código asociado en 1) que siempre será igual que x_1.

- Supongamos que D' se obtiene al aplicar una vez el segundo movimiento de Reidemeister a D en las hebras x_1 y x_2. Sea

$$G = \begin{pmatrix} | & | & | & | \\ \cdots & x_1 & x_2 & \cdots \\ | & | & | & | \end{pmatrix}$$

  la matriz $k \times n$ de rango máximo de C_D. Entonces,

$$G' = \begin{pmatrix} | & | & | & | & | & | \\ \cdots & x_1 & x_2 & x_1 & 2x_2 - x_1 & \cdots \\ | & | & | & | & | & | \end{pmatrix}$$

es la matriz $k \times (n+2)$ generadora de $C_{D'}$.
Igual que en el caso anterior, aplicar el segundo movimiento de Reidemeister es, en coloraciones, añadir a todas las coloraciones del nudo inicial dos colores: uno que sea siempre el mismo que x_1 y otro cuyo valor sea siempre $2x_2 - x_1$

- Supongamos que D' se obtiene al aplicar una vez el tercer movimiento de Reidemeister a D. Sea

$$G = \begin{pmatrix} | & | & | & | & | & | & | & | \\ \cdots & x_1 & x_2 & x_3 & 2x_1 - x_2 & 2x_3 - x_1 & 2x_3 - 2x_1 + x_2 & \cdots \\ | & | & | & | & | & | & | & | \end{pmatrix}$$

la matriz $k \times n$ de rango máximo de C_D. Entonces,

$$G' = \begin{pmatrix} | & | & | & | & | & | & | & | \\ \cdots & x_1 & x_2 & x_3 & 2x_1 - x_2 & 2x_3 - x_2 & 2x_3 - 2x_1 + x_2 & \cdots \\ | & | & | & | & | & | & | & | \end{pmatrix}$$

es la matriz $k \times n$ generadora de $C_{D'}$.

En los tres casos, la matriz G' tiene el mismo rango que la matriz G ya que las columnas añadidas o cambiadas son combinación lineal de las columnas de G. Estas transformaciones las podemos aplicar el número de veces necesarias cada una. Así, como por la equivalencia de diagramas del nudo podemos transformar uno en el otro mediante movimientos de Reidemeister, deducimos que sus dos códigos asociados tienen la misma dimensión. □

También podemos obtener cierta información sobre la dimensión de estos códigos usando invariantes del nudo. Este resultado no lo demostraremos porque requiere de conceptos que no hemos introducido como, por ejemplo, un invariante llamado el *número de Wirtinger*.

Proposición 4.7. *Sea C_D el código asociado a un diagrama D de un nudo K sobre $\mathbb{F}_q$ y sea $\beta(K)$ el número puente del nudo. Entonces,*

$$dim(C_D) \leq \beta(K).$$

Y podemos acotar también como se demuestra en [11]:

Proposición 4.8. *Sea D un diagrama de un nudo con n hebras y sea C_D su código asociado sobre $\mathbb{F}_q$. Tenemos la siguiente cota:*

$$1 \leq dim(C_D) \leq \frac{n+1}{2}.$$

Por otro lado, tenemos la distancia mínima. En este caso, podemos ver que la distancia mínima de dos códigos asociados a dos diagramas de nudos equivalentes no es un invariante del nudo.

Observación 4.9. La demostración de la Proposición 4.6 nos puede dar la idea para encontrar ejemplos de la afirmación anterior. La clave está en que aplicando los movimientos de Reidemeister, de manera sencilla puedo conseguir nudos equivalentes que, por el hecho de haber añadido columnas, podremos tener una distancia mínima distinta si tenemos un peso de Hamming distino.

Ejemplo 4.10.

- Sean el nudo trivial representado con su diagrama habitual y el nudo trivial aplicando el segundo movimiento de Reidemeister, tal y como aparece en la Figura 20. El diagrama del nudo trivial representado sin cruces se puede colorear solo de un color. Por eso, su distancia mínima es 1, porque cualquier color no nulo cumple que tiene peso Hamming 1. En este caso, el diagrama del nudo trivial habiendo aplicado el segundo movimiento de Reidemeister también tiene distancia mínima 1.

- El diagrama del nudo ocho de la Figura 17, tiene distancia mínima 3 dado que, como todas las hebras participan con todas las demás en algún cruce, solo una de ellas puede tener el color 0 y las otras 3 tendrán color no nulo.

- El diagrama del nudo ocho de la Figura 21 puede aceptar hasta dos hebras coloreadas de color 0, por ejemplo, podemos tener $x_1 = 0$ y $x_3 = 0$. Es relativamente fácil de comprobar que no hay manera de colorear 3 hebras del mismo color (por medio del prueba y error), así que tenemos que la distancia mínima será 4, por la Proposición 3.21.

Vemos que, a pesar de que los dos últimos ejemplos son nudos equivalentes, tienen distancia mínima diferente, en el primero es 3 y en el segundo es mínimo 4.

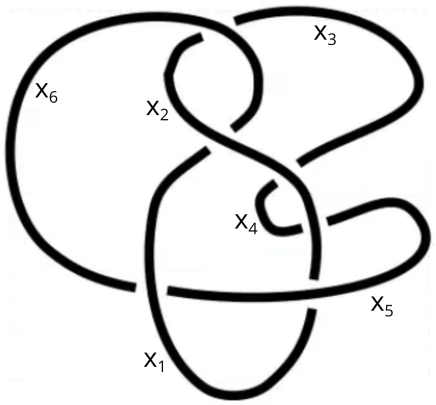


Figura 21: Nudo ocho con distancia mínima 4

Sin embargo, sí que existen un par de resultados interesantes. Uno muy sencillo lo demostraremos a continuación y el otro más adelante, pues está relacionado con los nudo pretzel, que definiremos en la siguiente sección.

Proposición 4.11. *Un código asociado a un diagrama de un nudo no trivial sobre $\mathbb{F}_q$ tiene mínima distancia mayor o igual que 2.*

Demostración. Procederemos por reducción al absurdo. Supongamos que existe un código asociado a un diagrama de un nudo con mínima distancia 1. Necesariamente, el código contiene una palabra de peso 1 (por la Proposición 3.21), que corresponde a una coloración en la que todas las hebras están coloreadas con 0 menos una que tiene color c distinto de 0. Para cada cruce en la que esta hebra participe, tendremos o bien $c + 0 - 2 \cdot 0 = 0$ o bien $0 + 0 + 2c = 0$, según sea understrand u overstrand. En cualquier caso, $c = 0$ y contradicción. □

Concluimos por este resultado que si nuestro código es un código asociado a un nudo no trivial entonces tenemos la certeza de que al menos podremos detectar un error.

4.3. Los nudos pretzel

En esta sección estudiaremos uno de los tipos de nudos que más juego nos dan: los nudos pretzel. Gran parte de su importancia radica en que nos permiten construir códigos de cualquier dimensión, lo cual puede resultar muy útil dado que, como hemos visto, la tasa de transmisión depende de la dimensión y es uno de los factores importantes a la hora de determinar la utilidad de un código. Además del hecho de que, cuanto mayor sea la dimensión, es más fácil conseguir una distancia mínima mayor.

Nos fijaremos también en su capacidad correctora de errores gracias a un resultado que veremos relacionado con la distancia mínima que, en general, su cálculo puede ser tarea complicada. La distancia mínima es el otro de los factores más importantes a la hora de estudiar esta capacidad correctora.

Definición 4.12. Sea $n \geq 1$. Un *enlace* $L = \{K_1, K_2, \cdots, K_n\}$ es una colección finita de nudos de manera que $K_i \cap K_j = \emptyset$, para todo $i, j \in \{1, \cdots, n\}$, con $i \neq j$. A cada uno de estos n nudos lo llamaremos *componente* del enlace. En particular, un *enlace poligonal* es un enlace cuyos componentes son nudos poligonales.

Observación 4.13. En este trabajo solo hemos trabajado con nudos poligonales así que también solo trataremos enlaces poligonales, a los cuales llamaremos simplemente enlaces.

Observación 4.14. Los enlaces son uniones disjuntas de nudos y, dos enlaces L_1, L_2 son equivalentes si tienen el mismo número de componentes y existe un homeomorfismo $h : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ tal que $h(L_1) = L_2$. Podemos observar que un nudo no es más que un enlace con un solo componente y que todas las definiciones que hemos visto son válidas para enlaces.

Ejemplos 4.15. En la Figura 22 y en la Figura 23 tenemos un par de ejemplos de enlaces con dos componentes [19] y en la Figura 24 tenemos el logo de las Olimpiadas, que es un ejemplo de enlace con 5 componentes.

Figura 22: Enlace 2_1^2

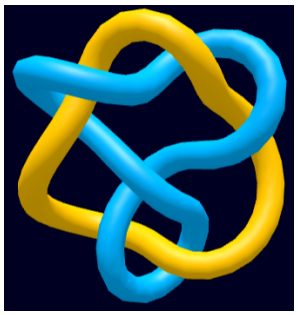


Figura 23: Enlace 7_2^1

Definición 4.16. Un *tangle* (se traduce literalmente como *giro*) es una parte de un diagrama de nudo que componen dos hebras y al menos un cruce entre ellas. En general, para que sea visual y aprovechando la equivalencia entre diagramas, los dibujaremos como en el Ejemplo 4.17. Un tangle con $b \in \mathbb{N}$ cruces lo llamaremos un *b-tangle* cuando la hebra de arriba a la derecha sea una overstrand, y lo llamaremos *(−b)-tangle* cuando sea una understrand.

Figura 24: Logo Olimpiadas

Ejemplos 4.17. Tenemos, en la Figura 25 un 3-tangle a la izquierda y un (-4)-tangle a la derecha.

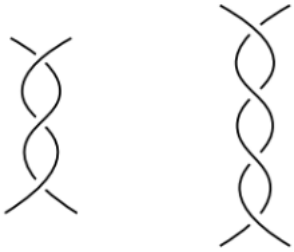


Figura 25: 3-tangle y (-4)-tangle

Definición 4.18. Sean $p_1, \cdots, p_m$ enteros no nulos para un $m \geq 1$. Un *enlace pretzel* (cuyo nombre viene por las galletas saladas que parecen nudos) es un enlace que se obtiene cuando múltiples tangles se ponen uno al lado de otro de manera que, para cada par de hebras vecinas, las hebras superior e inferior de la derecha del tangle situado en la izquierda están conectadas con con las hebras superior e inferior de la izquierda del tangle en la derecha. En el caso del primer y del último tangle, se conectan las hebras superior en inferior de la izquierda del primer tangle y las hebras superior en inferior de la derecha del último tangle. Lo denotaremos como $P(p_1, \cdots, p_m)$.

Veamos como ejemplos los enlaces de las Figuras 26, 27 y 28.

No todos los enlaces pretzel son nudos, enunciaremos una condición necesaria y suficiente para que lo sea, cuya demostración se encuentra en [10].

Proposición 4.19. *Un enlace pretzel $P(p_1, \ldots, p_m)$ es un nudo si y solo si m y p_i son enteros impares para todo $i \in \{1, \ldots, m\}$ o si $m \geq 1$ y exactamente uno de los p_i es par.*

Veamos algunos ejemplos de aplicación de esta proposición:

Ejemplos 4.20.

- El enlace de la Figura 26 es un nudo pretzel dado que $m, p_1, p_2, p_3 = 3$ son todos impares.
- El enlace de la Figura 27 es un nudo pretzel dado que $m = 2 \geq 1$ y de $p_1 = 3$ y $p_2 = 4$, solo p_2 es par.

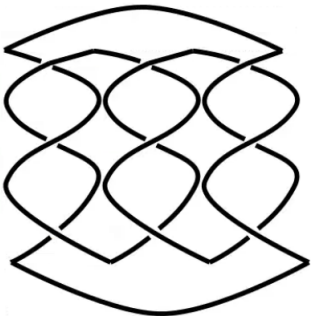


Figura 26: $P(3,3,3)$

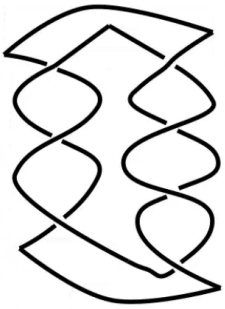


Figura 27: $P(3,4)$

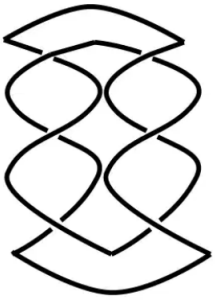


Figura 28: $P(3,3)$

- El enlace de la Figura 28 no es un nudo pretzel dado que $m = 2$ no es par y ninguno de los p_i tampoco lo es.

A pesar de que no todos los enlaces pretzel sean nudos pretzel, muchos de los resultados podrán demostrarse también para enlaces que no sean nudos.

Enunciamos ahora un par de resultados que, aunque no demostraremos, nos ayudan a hacernos una idea de como funcionan los nudos pretzel:

Proposición 4.21. *Un enlace pretzel $P(p_1, \ldots, p_n)$ tiene determinante*

$$\left| p_1 p_2 \cdots p_n \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} \right) \right|.$$

Lema 4.22. *Si $(p'_1, \ldots, p'_n)$ es una permutación cíclica de $(p_1, \ldots, p_n)$ entonces $P(p'_1, \ldots, p'_n)$ es equivalente a $P(p_1, \ldots, p_n)$.*

Observación 4.23. De la misma fórmula de la Proposición 4.21, se deduce que todas los enlaces equivalentes por permutaciones cíclicas tienen el mismo determinante.

Siguiendo con los ejemplos de las Figuras 26, 27 y 28 podemos calcular sus determinantes y algunas permutaciones cíclicas:

Ejemplos 4.24.

- $P(3,3,3)$ tiene determinante $3 \cdot 3 \cdot 3 \left(\frac{1}{3} + \frac{1}{3} + \frac{1}{3}\right) = 27$.
- $P(3,4) = P(4,3)$ y tienen determinante $3 \cdot 4 \left(\frac{1}{3} + \frac{1}{4}\right) = 7$.
- $P(3,3)$ tiene determinante $3 \cdot 3 \left(\frac{1}{3} + \frac{1}{3}\right) = 6$.

Como hemos dicho al principio, los nudos pretzel tienen interés en tanto en cuanto nos permiten construir códigos de cualquier dimensión. Esto aumenta en interés sobre todo al observar en la clasificación de nudos según sus números de cruces: de los que tienen entre 3 y 12 (más de 80), solo 7 de ellos tienen códigos asociados con dimensión mayor que 3 [16]. Es decir, con estos nudos no se podría construir prácticamente ningún código que pudiera ser útil en la práctica para valores de n muy grandes ya que la tasa disminuirá sin remedio. Veamos el siguiente Teorema [16]:

Teorema 4.25. *Sea D un diagrama del nudo pretzel $P(p_1, \ldots, p_m)$. Sea q una potencia de un primo p.*

1. *Si p_i y q son coprimos para todo $i \in \{1, \ldots, m\}$, la dimensión del código C_D asociado al nudo pretzel sobre $\mathbb{F}_q$ viene dada por*

$$\begin{cases} 2, & si\ p \mid det(P), \\ 1, & en\ caso\ contrario. \end{cases}$$

2. *Si existe algún p_i que no es coprimo con q para algún $i \in \{1, \ldots, m\}$, entonces la dimensión de C_D sobre $\mathbb{F}_q$ es*

$$dim(C_D) = |\{i \mid gcd(p_i, q) \neq 1,\ \ i \in \{1, \ldots, m\}\}|$$

La parte que nos interesa del Teorema 4.25 es la segunda. Tenemos que, escogiendo los p_i y q con astucia, podemos obtener códigos con dimensiones arbitrarias. Una buena manera puede ser fijar q y luego escoger la cantidad de p_i tal que $gcd(p_i, q) \neq 1$ en función de la dimensión que deseemos obtener. Tendremos que tener cuidado porque la elección de estos p_i no puede hacerse de cualquier manera, tiene que cumplir también una de las dos condiciones vistas en la Proposición 4.19 para que sea un nudo. Veamos un ejemplo de construcción de un código de dimensión 7:

Ejemplo 4.26. Si queremos que la dimensión sea 7, es necesario que $m \geq 7$. Pongamos $m = 7$ para hacerlo más sencillo. Supongamos que queremos trabajar en $\mathbb{F}_{13}$, es decir, $q = 13$. Ahora debemos escoger los cruces de cada giro que forma el enlace con astucia, de manera que todos sean coprimos con $q = 13$. Lo más sencillo es coger $p_1, \cdots, p_7 = 13$, y obtenemos el enlace pretzel

$$P(13, 13, 13, 13, 13, 13, 13).$$

Para poder aplicar el Teorema 4.25 necesitamos que este enlace sea un nudo. Por la Proposición 4.19, como tanto m como todos los p_i son impares, podemos afirmar que es un nudo pretzel. Aplicando la segunda parte del Teorema 4.25 obtenemos que la dimensión es 7, como queríamos.

Para un tipo muy especial de nudos pretzel, como los del ejemplo anterior, podemos determinar los parámetros exactos de su código correspondiente, cosa que es muy útil sobre todo en tanto en cuanto nos da la distancia mínima que, como hemos mencionado al principio de esta sección, puede llegar a ser muy aparatoso calcularla.

Proposición 4.27. ([11]) *Sean p un primo impar, m un impar y D un diagrama de $P(p_1, \ldots, p_m)$, con $p_i = p$ para todo $i \in \{1, \ldots, m\}$. Entonces, C_D es un $[pm, m, 2p-2]$-código.*

Observemos que, como ya vimos en la sección de códigos, al aumentar la distancia mínima, disminuye la tasa de transmisión y viceversa, pues son inversamente proporcionales. En este caso, cuanto más grande sea p, mayor será su distancia mínima y por tanto, su capacidad detectora y correctora. Sin embargo, su tasa de transmisión disminuirá. La clave radicará en ver en cada situación que nos sale más a cuenta y tratar de maximizar al máximo ambos valores sin empequeñecer uno demasiado.

Supongamos que tenemos un canal que es muy ruidoso, entonces necesitaremos corregir bastantes errores. En este caso, priorizamos tener una distancia mínima suficientemente alta como para corregir, por ejemplo, 8 errores por palabra. En este caso, necesitaremos que la distancia mínima sea 16 y, como $2p - 2 = 16$, entonces $p = 9$, y tendremos un nudo pretzel formado por 9-giros. La dimensión no tendrá mucha relevancia en este caso ya que, a la hora de calcular la tasa de transmisión, la m se cancela: $\frac{m}{pm} = \frac{1}{p} = \frac{1}{9}$. Esto significa que, sin importar la dimensión que tengamos, solo $\frac{1}{9}$ parte del código corresponde

al mensaje original y el resto es lo que añadimos para poder corregir errores. Lo único que habrá que tener en cuenta para escoger la m es que, junto con los p_i, cumpla tanto la condición de ser nudo pretzel de la Proposición 4.19 como las condiciones de la segunda parte del Teorema 4.25.

Supongamos que queremos un código que nos permita corregir algunos errores, pero priorizamos que no sea muy largo dado que no podemos contener tanta información. Lo que estamos pidiendo aquí es que no añadamos mucha información extra, es decir, que la tasa de transmisión no sea muy grande. Podemos coger, por ejemplo, la dimensión $m = 3$ y el nudo pretzel $P(3, 3, 3)$. De esta manera, la tasa de trasmisión es $\frac{1}{3}$ y, por tanto, el mensaje que realmente estamos enviando ocupa una tercera parte del código. El precio a pagar de esto es que tendremos una distancia mínima menor que antes: $2 \cdot 3 - 2 = 4$, y esto solo nos permitirá corregir 1 solo error, por la Proposición 3.12.

En la vida real, como hemos dicho, constantemente enviamos y recibimos información. Por eso, a la hora de transmitir un mensaje tendremos que escoger entre un código demasiado repetitivo (que hará el proceso de recibir y descodificar el mensaje mucho más lento) pero más seguro, o un proceso rápido pero con menos fiabilidad. Por ejemplo, si estamos recibiendo datos de un satélite podemos no tener tanta prisa en descodificar y preferimos asegurarnos de que la información que nos está dando es correcta. En cambio, en el caso de que necesitemos tener una comunicación a tiempo real, puede ser demasiado fatigoso usar códigos demasiado redundantes.

4.4. La suma de nudos

En esta sección vamos a profundizar un poco más en la suma (conexa) de nudos. Por la suma de dos nudos veremos que sus respectivos diagramas de nudos generan un nuevo diagrama de nudo. La ventaja de esto es que tanto los sumandos como el resultado tendrán códigos asociados y esto nos permitirá construir códigos de dimensiones arbitrarias. Veremos pues qué relación existe entre los códigos de dos diagramas de nudos y el código asociado a su suma conexa. Además, este estudio nos dará otro método para construir códigos de dimensiones arbitrarias.

Ya hemos visto que dados dos nudos K y L, denotamos $K\#L$ su suma (conexa). Denotaremos durante la sección D_K y D_L sus respectivos diagramas de nudo. Supondremos que los nudos son orientados y poligonales, y notaremos $x_1, \ldots, x_n$ y $y_1, \ldots, y_m$ como sus hebras en sus diagramas D_K y D_L respectivamente. Denotaremos por C y D como sus códigos respectivos sobre $\mathbb{F}_q^n$ y $\mathbb{F}_q^m$, siendo q una potencia de un primo p.

Veamos ahora un resultado para ver como se suman los códigos asociados a dos diagramas de nudos que se suman:

Lema 4.28. *El código de la suma $K\#L$ tomando la conexión de los diagramas D_K y D_L por las hebras x_n y y_m es*

$$C\#D = \{(c, d) \mid c \in C,\ d \in D,\ c_n = d_m\}.$$

Demostración. Una coloración de Fox para el diagrama $D_{K\#L}$ consiste en una coloración de Fox de D_K y una coloración de Fox de D_L de manera que los colores de las hebras que conectamos, en este caso x_n y y_m, tengan el mismo color. □

Una conclusión de este lema es que, si denotamos H_C y H_L las matrices de control de C y D, la matriz de control de $C\#D$ será:

$$H_{C\#D} = \left(\begin{array}{ccc|ccc} & H_C & & & 0_{(n-dim(C))\times m} & \\ & 0_{(m-dim(D))\times n} & & & H_D & \\ 0 & \cdots & 0\ \ 1 & 0 & \cdots & 0\ \ -1 \end{array}\right).$$

Recordemos que H_C tiene dimensión $(n - dim(C)) \times n$ y H_D tiene dimensión $(m - dim(D)) \times m$. La última linea de la matriz consiste en todo los valores 0 menos el de la posición n, que es 1, y el de la posición $n + m$, que es -1. Observemos que el cambio de signo se debe a que, para que se cumpla que una coloración vista como un código sea una coloración válida, por el lema anterior, se tiene que cumplir que $c_n = d_m$ (es decir, que los colores de las hebras que conectamos sean iguales) y, por tanto, la matriz de control tendrá que anular esta coloración, para lo cual necesita de un mismo valor con los signos contrarios. Digamos que es la condición que nos asegura que la suma se puede hacer, pues sin ella, la matriz también me anularía pares (c, d), con $c \in C$ y $d \in D$ tal que $c_n \neq d_m$.

Veamos ahora como se relacionan las dimensiones de los códigos con estas matrices de control. Esta relación que demostraremos es justamente la que nos permite obtener códigos de dimensión arbitraria:

Proposición 4.29. *La dimensión del código $C\#D$ satisface:*

$$dim(C\#D) = dim(C) + dim(D) - 1.$$

Recordemos el siguiente resultado de álgebra lineal [5] que usaremos para la demostración de la Proposición 4.29:

Teorema 4.30. *Sea $f : E \longrightarrow F$ una aplicación lineal, con E, F espacios vectoriales. Entonces,*

$$dim(E) = dimKer(f) + dimIm(f).$$

Proposición 4.29. Como ya sabemos, H_C tiene dimensión $(n - dim(C)) \times n$ y H_D tiene dimensión $(m-dim(D)) \times m$. Por construcción, la matriz $H_{C\#D}$ tiene dimensión $(n+m-(dim(C) + dim(D) - 1)) \times (n + m)$. Como H_C y H_D son matrices de control de paridad, tienen rango máximo, es decir, sus filas son linealmente independientes, así que podemos asegurar que las primeras $n + m - (dim(C) + dim(D))$ también lo son.

Veamos ahora que la última también lo es por contradicción. Asumimos que la última fila se puede escribir como combinación lineal de las anteriores. Particularmente, esto implica que existe una combinación lineal de las filas de H_C que resulta $(0, \ldots, 0, 1) \in \mathbb{F}^n$. Esto quiere decir que $(0, \ldots, 0, 1)$ podría ser una fila de H_C y, por tanto, tendría que satisfacer que $(0, \ldots, 0, 1) \cdot (x_1, \ldots, x_n) = 0$. Así pues, necesariamente $x_n = 0$ siempre y esto es contradictorio con la existencia segura de coloraciones triviales en las que el color no es 0. Así pues, la última fila de $H_{K\#L}$ es independiente a todas las demás y por tanto, por el Teorema 4.30, $dim(C\#D) = dim(C) + dim(D) - 1$. □

Para construir códigos de dimensión arbitraria con la Proposición 4.29 simplemente tendremos que coger dos códigos con cierta astucia. Es decir, si yo quiero construir un código de dimensión 5, puedo simplemente coger un nudo que tenga un código asociado de dimensión 3 y sumarlo consigo mismo. De esta manera, puedo siempre construir códigos de la dimensión que quiera, me basta con conocer códigos de dimensión inferior y combinarlos como más me convenga.

Siguiendo la observación hecha en [11], si sumamos el nudo trébol m veces obtenemos un código sobre $\mathbb{F}_3$ de longitud $3m$ y dimensión $m + 1$, por lo que su tasa de transmisión

sería $\frac{m+1}{3m} \approx \frac{1}{3}$. Es cierto que, en el caso del trébol y su código asociado C, si $d(C) = 2$, el código asociado a la suma de m nudos trébol tiene $d(C) = m$. No puedo generalizar seguramente, el caso del trébol se debe a su sencillez

4.5. De códigos a nudos

Hasta ahora nos hemos centrado en cómo la teoría de nudos puede aportar a la teoría de códigos y en la manera de pasar de un nudo dado a un código. En esta sección queremos mostrar que la razón de centrar nuestro estudio en esta dirección es que, a la inversa, esta relación no suele funcionar bien. Dado un código, quiero asociarle una coloración de un nudo, respetando los resultados y criterios vistos hasta ahora. Esto no va a dar resultado debido a que, fácilmente, un código cualquiera no cumple que sea una coloración de Fox. Veamos algún ejemplo que nos deje claro que todo nudo puede generar un código asociado, pero no todos los códigos tienen un nudo asociado según la coloración que puedan representar, ya que puede no ser una coloración de Fox.

Ejemplos 4.31. Veamos algunos ejemplos en los que un código tiene un nudo al que está asociado:

- Sea $C =< (1,0,2),(0,1,2) > \mathbb{F}_3^3$ un código. Es un código de dimensión 2 que, dado que las coordenadas de los vectores son elementos de $\mathbb{F}_3$, tenemos que es posible que sea un código asociado a un nudo trébol ya que puede tratarse de una $3-$coloración y el nudo trébol tiene determinante 3. Tenemos una base de este subespacio, así que podemos construir la matriz generadora del código:

$$G = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

  Usando la Proposición 3.30, con I_2 y $A = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$, podemos construir nuestra matriz de control: $H = (-A^t \mid I_1) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$. Observemos que esta matriz H es la misma que hemos encontrado cuando estudiábamos la matriz de chequeo del nudo trébol y, podemos construir M añadiendo dos filas linealmente dependientes a H:

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

  y, como estamos en F_3, la podemos representar así:

$$M = \begin{pmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix},$$

  que es la del nudo trébol, como ya hemos visto.

- Sea $C \subseteq \mathbb{F}_{11}^6$ dado por su matriz generadora:

$$G = \begin{pmatrix} 1 & 0 & 7 & 6 & 9 & 2 \\ 0 & 1 & 5 & 6 & 3 & 10 \end{pmatrix}.$$

Como $n = 6$, podemos asegurar que, si se trata de una coloración de Fox, tendrá que ser de algún nudo que tenga 6 cruces o menos. Además, tendrá que cumplir que, como $q = 11$, para que sea una $11-$coloración, $11 \mid det(K)$. Para todos los nudos con 6 cruces o menos tenemos [18]: $det(0_1) = 1$, $det(3_1) = 3$, $det(4_1) = 5$, $det(5_1) = 5$, $det(5_2) = 7$, $det(6_1) = 3$, $det(6_2) = 11$ y $det(6_3) = 13$.

El único que satisface la condición mencionada para que sea una $11-$coloración es 6_2. En general, no tendríamos porqué poder determinar el diagrama, pero en este caso, probaremos con el diagrama que aparece en [2] y [19]. Si no funciona, no querrá decir que no sea una coloración de alguno de los diagramas del nudo 6_2, sino que no sabemos cuál.

Tenemos el diagrama del nudo 6_2 etiquetado en la Figura 29 y podemos construir su matriz de Alexander:

$$M = \begin{pmatrix} 1 & 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 1 & 0 & -2 & 0 \\ -2 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & -2 \\ 0 & -2 & 0 & 0 & 1 & 1 \\ 1 & 0 & -2 & 0 & 0 & 1 \end{pmatrix}.$$

Una de las cosas que tienen que cumplir las palabras del código para ser coloraciones es que, si x es una palabra, $Mx^t = 0$. Vamos a hacer la prueba con los dos elementos que generan el código, es decir, veremos si $MG^t = 0$:

$$M = \begin{pmatrix} 1 & 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 1 & 0 & -2 & 0 \\ -2 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & -2 \\ 0 & -2 & 0 & 0 & 1 & 1 \\ 1 & 0 & -2 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 7 & 5 \\ 6 & 6 \\ 9 & 3 \\ 2 & 10 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \pmod{11}.$$

La segunda comprobación que haremos es que la dimensión de G sea la adecuada, ni más ni menos. Si calculamos el rango de M, vemos que, módulo 11, es 4. Entonces, la matriz de control del código asociado a 6_2 tendrá dimensión $(n-k) \times n = 4 \times 6$. Entonces, la matriz generadora tendrá dimensión $k \times n = 2 \times 6$, que es la dimensión de G.

Concluimos que el código dado por G es, efectivamente, el código asociado a un nudo: el nudo 6_2.

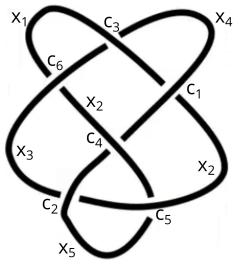


Figura 29: Diagrama del nudo 6_2

Sin embargo, como hemos comentado ya, esto no se cumple para códigos cualesquiera. Para ello veremos un par de ejemplos, para los cuales nos irá bien el siguiente lema:

Lema 4.32. *Sea un nudo K primo y alternado, con D un diagrama alternado y reducido suyo. Entonces, cada hebra del diagrama D participa en exactamente 3 cruces diferentes.*

Demostración. La demostración se deduce a partir de dos sencillas premisas:

- Dado que las hebras tienen dos extremos, podemos afirmar que, al menos, las hebras participarán en dos cruces como understrands. Y estos dos cruces no serán el mismo porque, sino, ya no tendremos un nudo primo sino un enlace.
- Al ser un diagrama alternado, entre dos understrands siempre tiene que haber una sola overstrand.

Así pues, una hebra siempre actuará como understrand 2 veces (en los extremos) y no más (sino, al partir una hebra, tendríamos dos hebras distintas). Si el diagrama es alternado tendrá exactamente una understrand. Concluimos que participa en 3 cruces. □

Observación 4.33. La razón por la cual pedimos que el nudo sea primo es evitar enlaces y nudos compuestos, pues para nuestro objetivo no nos interesan. Y el motivo de pedir la alternancia es que todos los nudos con menos de 10 cruces son alternados menos 3 (ver [19]): $8_{19}, 8_{20}$ y 8_{21}. Este resultado lo usaré para probar en que un código no puede asociarse a la coloración de un nudo en un caso concreto y lo he generalizado por si puede ayudarme en otras ocasiones. La alternancia es imprescindible, pues sino un nudo puede participar en dos o más cruces, sin ningún límite.

Observación 4.34. Observemos que la condición de reducido es necesaria para no tener cruces que se pueden deshacer por el algún movimiento de Reidemeister y que nos puedan llevar a tener en un mismo cruce una participación doble de una hebra. Veamos un ejemplo en la Figura 30.

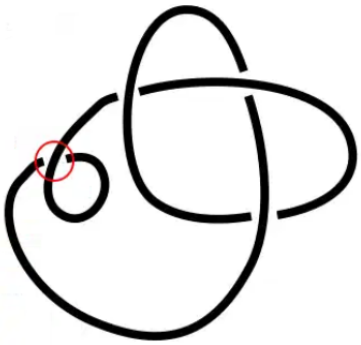


Figura 30: Nudo trébol con primer movimiento de Reidemeister

Vamos a ver ahora un par de ejemplos en que, dado un código, no podremos asociarlo a la coloración de ningún nudo.

Ejemplos 4.35.

- Veamos primero un caso bastante general. Sea $C \subseteq \mathbb{F}_q^n$, con $n \geq 3$ generado por la base compuesta por los dos primeros elementos de la base canónica:

$(1, 0, 0, \cdots)$ y $(0, 1, 0, \cdots)$. Tenemos pues que los elementos de este código serán de la forma:

$$C = \{(x, y, 0, \cdots) \mid x, y \in \mathbb{F}_q\}.$$

Observando la forma que tienen los elementos que forman parte de este código, nos damos cuenta de que C no contiene los elementos de la forma $(a, ..., a)$ para cualquier $a \in \mathbb{F}_q$ y, por tanto, no puede estar asociado a una coloración de un nudo, dado que ninguna de las palabras podrá interpretarse como una coloración trivial no nula. Recordemos que, como mínimo, podremos colorear un nudo de q maneras distintas (ver cota 2.2), todas las triviales asociadas a un valor distinto de $\mathbb{F}_q$.

- Sea un código $C \subseteq \mathbb{F}_5^4$ definido como:

$$C =< (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 1) >= \{(x, y, z, z) \mid x, y, z \in \mathbb{F}_5\}.$$

Como $n = 4$ y $q = 5$, entonces C solo puede ser código asociado del nudo ocho. Observamos que, esta vez, todas las coloraciones triviales sí que están en el código, solo hace falta que $x = y = z$.

Por el Lema 4.32, como el nudo ocho es reducido, tomando un diagrama suyo alternado y reducido, sabemos que cada hebra participa en 3 cruces diferentes. Esto significa, en el caso del nudo ocho (su diagrama reducido tiene 4 hebras y 4 cruces), que todas las hebras se juntan dos veces con las otras hebras. Tomamos ahora una palabra cualquiera que no pueda corresponder a una coloración trivial, es decir, que no se cumpla que $x = y = z$. El hecho de que las últimas coordenadas siempre tengan que ser iguales, nos impone que haya dos hebras que siempre tengan el mismo color. Y eso, si la coloración no es trivial, hace que en dos cruces tengamos dos colores iguales y uno distinto, así que no puede ser una coloración de Fox.

- Curiosamente, este mismo código sí que es una coloración del nudo trébol (si lo pensamos en $\mathbb{F}_3$) si en el tercer cruce aplicamos el primer movimiento de Reidemeister, para tener 4 hebras.

Observación 4.36. Observemos que, en general, ver que un código no puede estar asociado a una coloración de Fox de un nudo puede ser bastante complicado, en especial cuando más alto sea el número de cruces.

Podríamos pensar que lo único que hace falta para comprobar si un código está asociado a un nudo es: multiplicar una base por la matriz de coloreo de uno de los diagramas posibles y ver si se anula y ver que la dimensión es la adecuada (viendo que la matriz de chequeo obtenida por la de coloreo tiene rango $r = n - k$), como hemos hecho en el Ejemplo 4.31, obteniendo el nudo 6_2. Pero esto no funciona debido a que, en la sección anterior, ya vimos que dos diagramas equivalentes no resultan siempre en nudos equivalentes. Esto quiere decir que lo que acabamos de ver no sería suficiente hacerlo con la matriz de uno de los posibles diagramas de uno de los nudos posibles, sino que habría que hacerlo para cada diagrama equivalente de cada uno de los nudos candidatos, y eso es imposible.

5. Conclusiones

Entre la teoría de nudos y la teoría de códigos se puede establecer una relación basada en la obtención de códigos a partir de las coloraciones de un nudo, concretamente, la coloración de Fox. Por medio de esta coloración relacionamos un posible diagrama de un nudo con un código lineal, al que llamamos código asociado.

Hemos visto que los códigos asociados a diagramas de nudo equivalentes, no tienen porqué ser equivalentes. Sin embargo, gracias a esta relación, podemos definir el invariante de la dimensión del código asociado. Como hemos dicho, la obtención de invariantes puede ser una valiosa aportación al problema central de la teoría de nudos, en especial, si el invariante en cuestión es relativamente sencillo de calcular. Tampoco permanece invariante la distancia mínima, aunque hemos visto que, si el nudo no es trivial, al menos podremos detectar siempre un error.

Por medio de los nudos pretzel y la suma de nudos hemos encontrado diferentes resultados que nos permiten construir códigos de dimensiones arbitrarias. Podemos entender la relevancia de este hecho al ver que, de todos los nudos con menos de 12 cruces, solo 7 tienen códigos asociados con dimensión mayor que 3. El problema de que la dimensión sea pequeña es que, en consecuencia, la distancia mínima no será muy grande y eso limita las posibilidades tanto de detección como de corrección de errores. Así, la ventaja de poder construir códigos de dimensión arbitraria es poder contruir códigos correctores que tengan también distancias mínimas lo suficientemente grandes.

Los nudos pretzel también nos permiten también construir códigos con distancia mínima conocida ya de antemano, para una serie de nudos pretzel con unas características muy concretas. Esto nos permite conocer exactamente y sin cálculos, cuantos errores puede detectar y corregir nuestro código.

En un futuro podrá ser interesante estudiar si hay algún tipo de nudos con unas características particulares que permitan la obtención de códigos óptimos, es decir, cuyas capacidades de detección y corrección sean óptimas.

La obtención de nudos a partir de códigos lineales no es tan sencilla. Generalmente, un código no tiene porque estar asociado a un nudo por su coloración de Fox. Aunque hay ocasiones en que sí que se cumple, hemos visto que la comprobación de que corresponde a una coloración, puede ser muy fatigosa, como consecuencia del hecho de que diagramas distintos de un mismo nudo pueden tener asociados códigos que no sean equivalentes. Por esta razón podemos concluir que la relación de momento es más bien unidireccional: parece aportar más la teoría de nudos a la teoría de códigos que a la inversa. Aún así, puede ser interesante estudiar si hay algún tipo de códigos que estén asociados a nudos por sus características particulares.

Referencias

[1] Acosta Carvajal, B.E.; Montoya Conde, L.M.: *Elementos de la teoría de grafos y la conjetura de evasividad*, 2018.

[2] Alexander, J. W.; Briggs, G. B.: *On Types of Knotted Curves* Annals of Mathematics, vol. 28, no. 1/4, pp. 562-86, 1926.

[3] Alexander, J.W: *Topological invariants of knots and links.* Transactions of the American Mathematical Society 30.2: pp. 275-306, 1928.

[4] Cantero López, E.: *Una introducción a los códigos correctores de errores*, TFG Universitat Jaume I, 2023.

[5] Cirici, J.: *Apunts Àlgebra lineal*, Universitat de Barcelona, 2021.

[6] Farré i Cirera, R.: *Apunts de Tractament i Codificació de la Informació*, 2023.

[7] García, M.A.; Martínez, L.; Ramírez, T.: *Introducción a la Teoría de Códigos*, Facultad de Ciencia y Tecnología UPV, 2017.

[8] Gottlieb, E.: *La fórmula de Euler: poliedros, grafos planares y topología.* Revista del instituto de matemática y física, 2005.

[9] Hernández Sanz, J.: *Códigos localmente recuperables*, TFG Universidad de Valladolid, 2022.

[10] Kawauchi, A.: *Survey on knot theory*, Springer Science and Business Media, 1996.

[11] Kiliç, A.B.; Nijsten, A.I.O.; Pellikaan, R.; Ravagnani, A.: *Knot theory and Error-Correcting Codes*, 2023.

[12] Livingston, C.: *Knot theory.* Vol. 24. Cambridge University Press, 1993.

[13] MacWilliams, F.; Sloane, N.: *The Theory of Error-Correcting Codes.* 2nd. North-Holland Publishing Company, 1977.

[14] Mattman, T.W.; Solis, P.: *A proof of the Kauffman-Harary conjecture.* Algebraic and Geometric Topology 9.4: pp. 2027-2039, 2009.

[15] Nijsten, A.I.O.: *Knot and codes*, (Bachelor en Eindoven University of Technology), 2019.

[16] Nijsten, A.I.O.: *Properties of codes of knot diagrams*, (Master en Eindoven University of Technology), 2022.

[17] Reidemeister, K.: *Elementare begr ündung der knotentheorie.* Abhandlungen aus dem Mathematischen Seminar der Universit ät Hamburg, 5:24-32, 1927.

[18] Vendramin, L.: *Teoría combinatoria de nudos*, p. 12, 2014.

[19] *Zoo*, Knotplot, https://knotplot.com/zoo/