ALGORITMO DE SIMS-SCHREIER

Vamos a ver cómo resolver el puzle con un método distinto, el algoritmos de Sims-Schreier. Este método va a ser un poco más lento, pero tiene la ventaja de que funciona siempre y de manera relativamente rápida, en el sentido de que calcula si un elemento de S_n está en un determinado subgrupo G (dado por generadores) en a lo sumo n^5 pasos (compara eso con el tamaño de S_n que es $n!$). Por tanto, podríamos usarlo para resolver cualquier puzle o juego que involucre permutaciones (cubos de Rubik, n-puzles, etc).

En nuestro caso

$$G = \langle r, s\rangle \leq S_6$$

con $r = (13456)$ y $s = (132)$, y queremos ver si $m = (1423)(56)$ está en G. Por Lagrange tendríamos que $15 \mid |G|$. Como G es transitivo, tendríamos que $6 \mid |G|$, luego deducimos que $30 \mid |G| \mid 720$. Vemos que hemos avanzado algo, pero todavía nos queda para saber qué permutaciones están en G.

Si tomamos $x \in X$, hemos visto que $|G/G_x| = |\mathrm{Orb}_G(x)|$. Si calculamos dicha órbita, tendremos el tamaño de $|G/G_x|$. Pero tenemos

$$|G| = |G/G_x||G_x|.$$

Así, para calcular $|G|$ sólo nos faltaría calcular $|G_x|$. Podríamos iterar el proceso, calculando $G_x/(G_x)_y$ para otro $y \in X$. Pero para calcular dicho cociente, o lo que es lo mismo la órbita $\mathrm{Orb}_{G_x}(y)$, necesitamos conocer generadores para G_x. Eso es lo que nos da el siguiente resultado

Lema 0.1 (Generadores de un subgrupo)**.** *Sea $G = \langle r_i\rangle$ finito, $H \leq G$ con $G/H = \{g_k H\}$. Entonces*

$$H = \langle [r_i g_k]^{-1} r_i g_k\rangle$$

con $[w]$ el representante g_j de w en G/H.

Demostración. Por definición tenemos que $J = \langle [r_i g_k]^{-1} r_i g_k\rangle \leq H$. Queremos demostrar que $H \leq J$. Es suficiente ver que $G = CJ$, con $C = \{g_k\}$, ya que entonces $|C||H| = |G| \leq |C||J|$.

Pero ver que $G = CJ$ es equivalente a ver que $r_i CJ \subset CJ$ para todo r_i, ya que r_i genera G. Pero $r_i g_k = [r_i g_k][r_i g_k]^{-1} r_i g_k$, lo que muestra que $r_i C \subset CJ$, luego $r_i CJ \subset CJJ = CJ$, ya que J es subgrupo. □

Una vez hecho esto, veamos además que hemos resuelto el problema de ver si un elemento $m \in S_n$ está en $G \leq S_n$. Si $m \in G$, entonces

$\overline{m} = \overline{g_k}$ con g_k uno de los representantes de $G/G_n = \{g_k G_n\}$. Pero esto es lo mismo que ver si alguno de los g_k lleva $n \mapsto m(n)$. Si esto no es cierto, deducimos que $m \notin G$. Si es cierto, entonces $m_n = g_k^{-1} m$ fijaría n, luego $m \in G \Leftrightarrow m_n \in G_n$. Pero como $G_n \lesssim S_{n-1}$, hemos simplificado el problema. Podríamos seguir iterando dicho procedimiento para ver si $m \in G$, y en caso de que que la respuesta sea afirmativa, el procedimiento nos permite expresar m en términos de generadores de G.

Veamos cómo usar dicho resultado para el caso del puzle

$$G = \langle r, s \rangle \leq S_6$$

$r = (13456)$, $s = (132)$. Comenzamos por ejemplo por la órbita del 6, que queda todo $\{1, 2, 3, 4, 5, 6\}$. Para calcular representantes de G/G_6 basta con ecntrar permutaciones que lleven $6 \mapsto 1$, $6 \mapsto 2$, $6 \mapsto 3$, $6 \mapsto 4$, $6 \mapsto 5$ y $6 \mapsto 6$. En ese orden, podemos tomar $r = (61345)$, $sr^2 = (6214)(35)$, $r^2 = (63514)$, $r^{-2} = (64153)$, $r^{-1} = (65431)$, e. Así

$$G/G_6 = \{\overline{r}, \overline{sr^2}, \overline{r^2}, \overline{r^{-2}}, \overline{r^{-1}}, \overline{e}\}.$$

Como $\overline{rr^i} = \overline{r^{i+1}}$,, tenemos que $[rr^i]^{-1}(rr^i) = e$; de igual forma $[sr^2]^{-1} sr^2 = e$. Aplicando el resultado anterior con el resto de multiplicaciónes, y observando que $[x]$ es el representante de G/G_6 que lleva $6 \mapsto x(6)$ vemos que

$$G_6 = \langle (sr^2)^{-1} r (sr^2), r^{-1} s (sr^2), (r^2)^{-1} s(r), e^{-1} s(e), (r^{-2})^{-1} s(r^{-2}), (r^{-1})^{-1} s(r^{-1}) \rangle$$

Tenemos que

$$(sr^2)^{-1} r (sr^2) = (25134)$$

$$r^{-1} s s r^2 = (65431)(123)(14635) = (13452),$$

$$r^{-2} sr = (15364)(132)(13456) = (12543)$$

$$r^2 s r^{-2} = (46351)(132)(46351)^{-1} = (452).$$

$$r s r^{-1} = (13456)(132)(13456)^{-1} = (342).$$

luego

$$G_6 = \langle (321), (423), (524), (52134) \rangle \leq S_5.$$

Como dos de ellas envían el 5 al 2, podemos quitar dicha redundancia escribiendo

$$G_6 = \langle (321), (423), (524), (524)^{-1} (52134) \rangle$$

y como $(425)(52134) = (132)$, tenemos que

$$G_6 = \langle (321), (423), (524) \rangle.$$

Así, si queremos ver si $m \in G$, como $m(6) = 5$, quiere decir que $\overline{m} = \overline{r^{-1}}$ en G/G_6, luego $\tilde{m} = rm \in G_6$. Pero

$$m_6 = rm = (13456)(1423)(56) = (51)(24).$$

Así, habríamos reducido el problema a ve si $m_6 \in G_6$. De nuevo G_6 es transitivo visto en S_5 y podemos encontrar representantes

$$G_6/G_{65} = \{\overline{(321)(524)}, \overline{(524)}, \overline{(423)(524)}, \overline{(524)^2}, \overline{e}\}$$

que llevan $5 \mapsto 1$, $5 \mapsto 2$, $5 \mapsto 3$, $5 \mapsto 4$ y $5 \mapsto 5$. Así, vemos que como m_6 lleva $5 \mapsto 1$, entonces $\overline{m_6} = \overline{(321)(524)}$, luego

$$m_{65} = ((321)(524))^{-1} m_6 = (425)(123)(51)(24) = (431)$$

fija el 5. Por tanto, es equivalente ver que $m_6 \in G_6$ a que $m_{65} \in G_{65}$.

Ahora habría que calcular G_{65} a partir de G_6 y representantes de G_6/G_{65}, pero vamos a ver que en este caso podemos calcularlo directamente. Como $G_{65} \geq J = \langle (321), (423) \rangle$ y J es transitivo en S_4 tenemos que $4 \mid |J|$, y como $3 \mid |J|$ vemos que $12 \mid |J|$. Pero además $G_6 \leq A_5$ porque sus generadores son todos pares, luego $G_{65} \leq A_4$, luego $G_{65} = J = A_4$, y en particular

$$G_{65} = \langle (321), (423) \rangle.$$

Por tanto $|G_6| = 5|A_4| = 5!/2$, y de nuevo como $G_6 \leq A_5$ tenemos que $G_6 = A_5$. De la misma forma vemos que $|G| = 6!/2$ y $G = A_6$.

Volvamos ahora a ver si $m_{65} = (431) \in G_{65}$. Como $G_{65} = A_4$, tenemos que $G_{654} = A_3$ y de hecho vemos que en términos de los generadores de G_{65} podemos escribir

$$G_{654} = \langle (321) \rangle, \qquad G_{65}/G_{654} = \{\overline{(321)(423)}, \overline{(423)}, \overline{(423)^2}, \overline{e}\}.$$

Ahora buscamos un representante que lleve el 4 al 3, que es $(423)^2$. Así

$$m_{654} = ((423)^2)^{-1} m_{65} = (423)(431) = (312)$$

está en G_{654}. Ahora buscamos un representante de $G_{654}/G_{6543} = G_{654}$ que lleve $3 \mapsto 1$, que sería $s^2 = (132)^2 = (312)$. Es decir

$$m_{6543} = (s^2)^{-1} m_{654} = e$$

está en $G_{6543} = \{e\}$, luego hemos acabado. Si reescribimos los pasos que hemos dado vemos que

$$m = r^{-1}(321)(524)(423)^2 s^2.$$

Pero todos esos factores sabemos expresarlos en términos de r, s:

$$m = r^{-1} s (r^2 s r^{-2})(r s r^{-1})^2 s^2$$

o como $s^3 = e$

$$m = r^{-1} s r^2 s (r^{-1} s^{-1})^2$$

luego ya sabemos ir de la posición m a la inicial en el puzle de antes.

Observa que una vez calculados representantes de todos esos cocientes, podemos comprobar rápidamente si cualquier otro $m' \in S_6$ está en G y expresarlo en términos de r y s.