Le théorème de Cayley informationnel

Partition des tables par classe d'isomorphisme et poids informationnel des groupes

Hugues Genvrin — Programme du grain

September 7, 2026

Résumé

On enrichit le théorème de Cayley d'une dimension informationnelle. Le nombre de tables de groupe sur n éléments se *partitionne* selon les classes d'isomorphisme, chaque groupe G occupant une orbite de $n!/|\operatorname{Aut}(G)|$ tables sous réétiquetage (Burnside). On définit le *poids informationnel* $w(G) = \log_2\big(\text{tables}(n)\,|\operatorname{Aut}(G)|/n!\big)$: le coût en bits pour désigner une table de G parmi toutes. Résultat central : *plus un groupe est symétrique (grand* Aut*), plus il est rare, plus il est informatif.* Le groupe de Klein V est ainsi plus « riche » que $\mathbb{Z}/4$ (2 bits contre 0,42). On explique enfin la coïncidence $n = 4$ par $\operatorname{Aut}(V) = \mathrm{GL}(2, \mathbb{F}_2) \cong S_3$ — un accident des petits nombres, non une loi en n.

1 La partition des tables

On compte les tables de groupe *étiquetées* sur $E = \{1, \dots, n\}$ (document *Quantification des axiomes*). Le groupe symétrique S_n agit dessus par réétiquetage ; deux tables sont dans la même orbite ssi les groupes sont isomorphes.

Théorème 1 (Cayley informationnel : partition par isomorphisme)**.** *Le nombre de tables de groupe sur n éléments est la somme, sur les classes d'isomorphisme de groupes d'ordre n, des tailles d'orbites sous réétiquetage :*

$$\boxed{\text{tables}(n) = \sum_{[G]\,:\,|G|=n} \frac{n!}{|\operatorname{Aut}(G)|}.}$$

Chaque classe $[G]$ est une orbite de S_n, de stabilisateur Aut(G)*, donc de taille $n!/|\operatorname{Aut}(G)|$ (théorème orbite–stabilisateur).*

Proof. S_n agit sur les structures de groupe étiquetées par permutation des éléments. L'orbite d'une table est l'ensemble de ses réétiquetages ; deux tables sont dans la même orbite ssi elles définissent des groupes isomorphes. Le stabilisateur d'une table est l'ensemble des permutations qui la préservent, soit exactement $\operatorname{Aut}(G)$. Par orbite–stabilisateur, $|\text{orbite}| = |S_n|/|\operatorname{Aut}(G)| = n!/|\operatorname{Aut}(G)|$. Sommer sur les classes d'isomorphisme (les orbites) donne le total. □

Remarque 2 (Le lien avec ton intuition additive). À $n = 4$, il y a *deux* classes ($\mathbb{Z}/4$ et V), d'où

$$\text{tables}(4) = \frac{24}{|\operatorname{Aut}(\mathbb{Z}/4)|} + \frac{24}{|\operatorname{Aut}(V)|} = \frac{24}{2} + \frac{24}{6} = 12 + 4 = 16.$$

C'est la décomposition $16 = 12 + 4$ pressentie — non pas « $\mathbb{Z}/k + V$ » en général, mais « somme sur les classes d'isomorphisme », qui se trouve avoir deux termes à $n = 4$.

2 Le poids informationnel d'un groupe

Définition 3 (Poids informationnel)**.** Pour un groupe G d'ordre n, le *poids informationnel* est le coût en bits pour désigner une table de G parmi toutes les tables de groupe :

$$w(G) = \log_2 \frac{\text{tables}(n)}{n!/|\operatorname{Aut}(G)|} = \log_2 \frac{|\operatorname{Aut}(G)| \cdot \text{tables}(n)}{n!} \geq 0.$$

Proposition 4 (Symétrie interne = richesse informationnelle)**.** *$w(G)$ croît avec $|\operatorname{Aut}(G)|$: plus un groupe est symétrique, plus son orbite est petite, plus son poids informationnel est grand. Le groupe le plus symétrique d'un ordre donné est le plus « rare » en tables, donc le plus informatif.*

Proof. $w(G) = \log_2\big(|\operatorname{Aut}(G)| \cdot \text{tables}(n)/n!\big)$ est croissant en $|\operatorname{Aut}(G)|$ (les autres facteurs sont fixés à n donné). □

Remarque 5 (Klein est plus riche que $\mathbb{Z}/4$). À $n = 4$: $w(\mathbb{Z}/4) = \log_2(16/12) = 0{,}42$ bit, $w(V) = \log_2(16/4) = 2$ bits. Le groupe de Klein, trois fois plus symétrique ($|\operatorname{Aut}(V)| = 6$ contre 2), est quatre fois plus rare (4 tables contre 12), donc porte 2 bits contre 0,42. C'est le sens précis de sa « fécondité » : sa symétrie interne se paie en néguentropie de structure.

3 La table des poids

n	groupe	$\lvert\operatorname{Aut}(G)\rvert$	tables	tables(n)	$w(G)$ (bits)
4	$\mathbb{Z}/4$	2	12	16	0,42
4	$V = (\mathbb{Z}/2)^2$	6	4	16	**2,00**
6	$\mathbb{Z}/6$	2	360	480	0,42
6	S_3	6	120	480	**2,00**
8	$\mathbb{Z}/8$	4	10 080	22 080	1,13
8	$\mathbb{Z}/4 \times \mathbb{Z}/2$	8	5 040	22 080	2,13
8	D_4	8	5 040	22 080	2,13
8	Q_8	24	1 680	22 080	3,72
8	$(\mathbb{Z}/2)^3$	168	240	22 080	**6,52**

Le poids maximal va toujours au groupe *élémentaire abélien* $(\mathbb{Z}/2)^m$ (le plus symétrique) : à $n = 8$, $(\mathbb{Z}/2)^3$ avec $|\operatorname{Aut}| = 168$ pèse 6,52 bits, loin devant les autres. Code :

```
import math
from math import factorial
log2 = math.log2
groups = { # ordre n : [(nom, |Aut(G)|), ...]
  4: [("Z/4",2), ("V",6)],
  6: [("Z/6",2), ("S_3",6)],
  8: [("Z/8",4),("Z/4xZ/2",8),("D_4",8),("Q_8",24),("(Z/2)^3",168)],
}
for n, gs in groups.items():
    fn = factorial(n)
    tabs = [(name, a, fn//a) for name,a in gs]
    total = sum(t for _,_,t in tabs)
    for name,a,t in tabs:
        print(n, name, "|Aut|=",a, "tables=",t, "w=",round(log2(total/t),2))
# n=4 : V pese 2.00 bits contre 0.42 pour Z/4
```

4 Le cas $n = 4$ expliqué : $\mathrm{Aut}(V) = \mathrm{GL}(2, \mathbb{F}_2)$

Pourquoi le dénominateur 6 pour V, et pourquoi la coïncidence $6 = |S_3|$?

Proposition 6 (La source du 6)**.** *Le groupe de Klein est l'espace vectoriel $V = \mathbb{F}_2^2$. Ses automorphismes de* groupe *sont exactement ses automorphismes* linéaires *:*

$$\mathrm{Aut}(V) = \mathrm{GL}(2, \mathbb{F}_2), \qquad |\,\mathrm{GL}(2, \mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 3 \cdot 2 = 6.$$

Et $\mathrm{GL}(2, \mathbb{F}_2) \cong S_3$: les 6 transformations linéaires permutent les 3 vecteurs non nuls de $\mathbb{F}_2^2$ de toutes les façons possibles.

Proof. Sur $(\mathbb{Z}/2)^m$, tout endomorphisme de groupe est $\mathbb{F}_2$-linéaire (car $2x = 0$ force l'additivité à être linéaire sur $\mathbb{F}_2$), donc $\mathrm{Aut}((\mathbb{Z}/2)^m) = \mathrm{GL}(m, \mathbb{F}_2)$. Pour $m = 2$, les 3 vecteurs non nuls sont librement permutables par $\mathrm{GL}(2, \mathbb{F}_2)$, d'où l'isomorphisme avec S_3 (comptage : $|\,\mathrm{GL}(2, \mathbb{F}_2)| = 6 = |S_3|$, et l'action sur 3 points est fidèle). □

Pourquoi ta formule ne valait qu'à $k = 4$. L'égalité proposée $|\,\mathrm{Aut}(V)| = |S_{k-1}|$ n'est vraie qu'à $k = 4$, et c'est un *accident* : $\mathrm{Aut}(V) = \mathrm{GL}(2, \mathbb{F}_2)$ *coïncide* avec S_3 seulement parce que $\mathrm{GL}(2, \mathbb{F}_2) \cong S_3$. Pour $(\mathbb{Z}/2)^m$ général, $|\,\mathrm{Aut}\,| = |\,\mathrm{GL}(m, \mathbb{F}_2)| = \prod_{i=0}^{m-1}(2^m - 2^i)$:

$$m = 1 : 1, \quad m = 2 : 6, \quad m = 3 : 168, \quad m = 4 : 20\,160, \ldots$$

Seul $m = 2$ donne $6 = |S_3|$. Il n'y a donc pas de loi en « S_{k-1} » : la bonne généralisation est $\mathrm{GL}(m, \mathbb{F}_2)$, pas le symétrique. La coïncidence est isolée.

5 Lien avec le programme

Remarque 7 (Deux comptages d'orbites emboîtés). Ce théorème complète la quantification des axiomes (document précédent) et le théorème de Klein (chapitre *Matière*) : tous trois comptent des orbites sous une action de groupe, en bits. *Klein* : orbites d'un groupe agissant sur des configurations. *Axiomes* : orbites contraintes par les axiomes. *Ici* : orbites des tables de groupe sous réétiquetage. Le poids informationnel $w(G)$ est à la classe d'isomorphisme ce que la néguentropie d'orbite est à la structure : une mesure de rareté, donc d'ordre.

Remarque 8 (Cayley enrichi). Cayley plonge tout groupe d'ordre n dans S_n. Le *Cayley informationnel* ajoute : ce plongement occupe une orbite de taille $n!/|\,\mathrm{Aut}(G)|$, et le coût de l'y désigner est $w(G)$. La place d'un groupe dans S_n n'est plus seulement qualitative (il s'y plonge) mais *quantitative* (il y occupe tant de bits).

6 Portée et limites

Remarque 9 (Acquis). Le nombre de tables se partitionne par classe d'isomorphisme (théorème 1) ; le poids informationnel $w(G)$ croît avec la symétrie interne (proposition 4) ; le cas $n = 4$ s'explique par $\mathrm{Aut}(V) = \mathrm{GL}(2, \mathbb{F}_2) \cong S_3$ (proposition 6), coïncidence isolée.

Limites. *(i)* Comptage *étiqueté* (tables sur $\{1, \ldots, n\}$), non à isomorphisme près. *(ii)* $|\,\mathrm{Aut}(G)|$ doit être connu pour chaque groupe : facile aux petits ordres, plus lourd ensuite (mais tabulé). *(iii)* Le poids $w(G)$ mesure une rareté *combinatoire* (informationnelle), non une richesse *algébrique* intrinsèque : un groupe « lourd » en bits est celui dont beaucoup de réétiquetages coïncident, ce qui est une propriété de son Aut, à ne pas confondre avec sa complexité de structure.