Comptage des sélections de rang plein sur $\mathbb{F}_2$

Une frontière de complexité entre le comptage modulo 2 et modulo 4

Zakaria Gharzouli
Residual Labs, Moissy-Cramayel, France
ORCID : 0009-0005-7604-4709 • contact@residual-labs.fr
Prépublication v1.1 - 26 novembre 2026 - CC BY 4.0
DOI 10.5281/zenodo.24557901

Résumé

Nous comptons les choix d'un vecteur dans chacun de plusieurs ensembles binaires explicites, sous la condition que les vecteurs choisis engendrent tout l'espace. Le premier bit du compte se calcule en temps polynomial par une seule élimination de Gauss. Décider si le deuxième bit vaut un est $\oplus$P-complet, même pour les plans d'arêtes d'un graphe simple sans sommet isolé et à au moins deux arêtes. La preuve relie le compte modulo quatre au nombre de 3-colorations à permutation de couleurs près. Pour des domaines arbitraires, chaque bit d'indice fixé supérieur ou égal à un est $\oplus$P-complet. L'existence d'un algorithme polynomial pour ces bits équivaut à P = $\oplus$P. Des calculs reproductibles et une formule de raccordement complètent ces résultats.

Mots-clés — Comptage modulaire, rang matriciel, 3-coloration, inversion de Möbius, $\oplus$P.

1. Le problème de comptage

Soit $U = \mathbb{F}_2^r$. Une instance fournit m ensembles explicites $A_1,\dots,A_m \subseteq U$. Chaque ensemble décrit les lignes admissibles à une position d'une matrice à m lignes et r colonnes. On compte les tuples ordonnés.

$$N = \#\{(v_1,\dots,v_m) \in A_1 \times \cdots \times A_m : \langle v_1,\dots,v_m\rangle = U\}. \quad (1)$$

Le bit d'indice j est $\lfloor N / 2^j \rfloor \bmod 2$. Les indices commencent à zéro. Un domaine vide donne N = 0. Si m = 0, N vaut 1 pour r = 0 et 0 sinon. Si r = 0 et que tous les domaines sont non vides, chacun vaut {0} et N = 1. Les vecteurs sont donnés en coordonnées binaires denses.

La contribution principale porte sur le passage de la parité à la précision modulo quatre. Une instance dont N est impair possède au moins une sélection de rang plein. Une parité nulle peut aussi correspondre à un compte positif, comme le montrent les exemples de la section 5.

2. La parité par élimination de Gauss

Théorème 1. Posons $a_i = \bigoplus_{v \in A_i} v$ et $b_i = 1 + (|A_i| \bmod 2)$ dans $\mathbb{F}_2$. Le compte N est impair exactement lorsque le système $a_i \cdot u = b_i$, pour $1 \le i \le m$, possède une unique solution $u \in U$.

Preuve. Pour un tuple de rang s, il existe exactement 2^{r-s} vecteurs u orthogonaux à toutes ses lignes. Ce nombre est impair exactement pour s = r. En échangeant les sommes sur les tuples et sur u, il vient

$$N \equiv \Sigma_{u \in U} \prod_{i=1}^{m} |\{v \in A_i : u \cdot v = 0\}| \pmod 2. \quad (2)$$

Dans $\mathbb{F}_2$ l'indicatrice de $u \cdot v = 0$ vaut $1 + u \cdot v$. Le facteur i est donc $(|A_i| \bmod 2) + u \cdot a_i$. Le produit vaut un exactement pour les solutions du système annoncé. Un système affine compatible de rang ρ a $2^{r-\rho}$ solutions. Sa contribution modulo deux vaut un exactement pour $\rho = r$. □

Algorithme. Parcourir chaque ensemble pour calculer son XOR et sa cardinalité modulo deux. Réduire la matrice augmentée [a | b] sur $\mathbb{F}_2$. Renvoyer 1 si le système est compatible et si le rang de la matrice des coefficients vaut r, 0 sinon. Avec des vecteurs denses, le coût naïf est $O(r \Sigma_i |A_i| + mr \min(m,r))$ opérations binaires. Le cas carré admet aussi une preuve par multilinéarité du déterminant.

Exemple calculé. Avec r = 2, $A_1 = \{e_1\}$, $A_2 = \{e_2\}$, $A_3 = \{e_1, e_2, e_1+e_2\}$, les XOR sont e_1, e_2, 0. Toutes les cardinalités sont impaires. Les équations sont $u_1 = 0$, $u_2 = 0$, $0 = 0$. La solution unique donne N mod 2 = 1. Les deux premières lignes engendrent déjà U, donc N = 3.

Formule de comptage exact. Pour $W \le U$, le nombre de tuples dont toutes les lignes appartiennent à W est le produit des $|A_i \cap W|$. L'inversion de Möbius sur les sous-espaces isole les tuples qui engendrent U [1].

$$N = \Sigma_{W \le U} (-1)^c \, 2^{c(c-1)/2} \prod_{i=1}^{m} |A_i \cap W|, \; c = r - \dim W. \quad (3)$$

Le coefficient de Möbius de l'intervalle [W,U] est celui du treillis des sous-espaces d'un quotient de dimension c. Dans le produit des c facteurs $(1 + z\,2^j)$ pour $j = 0,\dots,c-1$, le coefficient de z^k est le nombre de sous-espaces de dimension k multiplié par $2^{k(k-1)/2}$. C'est l'identité du binôme gaussien, obtenue par récurrence en c. En $z = -1$ le produit vaut zéro pour $c > 0$, comme l'exige la relation de Möbius. Pour c = 0, le coefficient vaut un.

3. Le deuxième bit et les colorations

Théorème 2. Soit $G = (V,E)$ un graphe simple sans sommet isolé, avec au moins deux arêtes. Associons à chaque arête uv le domaine $A_{uv} = \langle e_u, e_v \rangle = \{0, e_u, e_v, e_u+e_v\}$ dans $U = \mathbb{F}_2^{|V|}$. Si $\chi_G(3)$ désigne le nombre de 3-colorations propres à couleurs étiquetées, alors

$$N(G) \equiv 2 \cdot ((\chi_G(3) / 6) \bmod 2) \pmod 4. \quad (4)$$

La division par six est entière et précède la réduction modulo deux. Le nombre de colorations étiquetées est toujours pair sur cette famille.

Preuve. Dans (3), les termes de codimension au moins trois s'annulent modulo quatre par leur coefficient. Pour $W = U$, tous les facteurs valent quatre. En codimension un, chaque plan A_{uv} rencontre W en dimension au moins un. Comme il y a au moins deux arêtes, le produit est multiple de quatre. Restent les sous-espaces de codimension deux, de coefficient $+2$. Leur produit est impair exactement lorsque $W \cap A_{uv} = \{0\}$ pour chaque arête.

Pour un tel W, un isomorphisme $U/W \to \mathbb{F}_2^2$ associe à chaque sommet la classe de son vecteur de base. Sur une arête, les deux classes sont indépendantes, donc distinctes et non nulles. Chaque sommet appartient à une arête. Les trois vecteurs non nuls deviennent les trois couleurs. Réciproquement, une coloration propre définit une application linéaire en fixant l'image des vecteurs de base. Elle est surjective, car une arête fournit deux images indépendantes. Les applications surjectives de même noyau se déduisent les unes des autres par $GL(2,2)$, qui permute les trois vecteurs non nuls de toutes les manières. Chaque noyau admissible correspond donc exactement à six colorations. □

Avec une seule arête et deux sommets, $N = 0$ et $\chi_G(3)/6 = 1$. Un sommet isolé impose une colonne nulle et empêche le rang plein.

Exemple calculé. Pour le triangle, les ensembles sont les trois plans de coordonnées dans $\mathbb{F}_2^3$. Un noyau de codimension deux est une droite. Pour éviter les trois plans, son unique vecteur non nul doit être $(1,1,1)$. Il existe donc un seul noyau admissible, et (4) donne 2 modulo 4. Pour le compte exact, les codimensions 0, 1, 2 et 3 contribuent respectivement 64, $-(3\cdot16+4\cdot8)$, $2\cdot(3\cdot4+3\cdot2+1)$, -8. Leur somme vaut 14, également obtenu en énumérant les 64 sélections.

Calcul modulo quatre. Pour tout ensemble explicite, (3) ne demande à cette précision que les sous-espaces de codimensions 0, 1 et 2. En codimension deux on peut énumérer les couples indépendants du dual et retenir une seule base réduite par sous-espace dual. Le nombre de sous-espaces candidats en codimension deux est $(2^r-1)(2^r-2)/6$. Cette méthode reste exponentielle en r. Plus généralement, pour un calcul modulo 2^s, un terme de (3) peut être supprimé si $c(c-1)/2 \geq s$. Pour les domaines d'arêtes, la formule (4) permet un contrôle indépendant par énumération des colorations.

4. Classification de complexité

Théorème 3. Décider si le bit d'indice 1 de N vaut un est $\oplus$P-complet sous les réductions déterministes polynomiales many-one, y compris pour les plans d'arêtes du théorème 2.

Difficulté. La classe $\oplus$P décide la parité du nombre de témoins acceptés par un vérificateur polynomial. La version parité de 3-SAT y est complète. On code un circuit à portes ET, OU et NON par une équivalence pour chaque porte, puis on fixe la sortie à vrai. Chaque équivalence se met en CNF de largeur au plus trois, avec clauses unitaires et binaires autorisées. Chaque témoin détermine les variables de portes de façon unique et le compte est conservé.

Partons d'une 3-CNF Φ. Construisons un triangle distingué T, F, B et fixons les couleurs de ses trois sommets. Pour chaque variable x, créons deux sommets x et ¬x, adjacents entre eux et tous deux voisins de B. Ils prennent les couleurs de T et F dans un ordre qui code une affectation. Pour chaque clause, ajoutons un sommet auxiliaire adjacent à F et aux sommets des littéraux de la clause. Si la clause est vraie, l'auxiliaire a des voisins de deux couleurs et un seul choix. Si elle est fausse, ses voisins ont tous la couleur de F et il a deux choix. Les sommets auxiliaires sont indépendants les uns des autres. Une affectation qui viole t clauses donne exactement 2^t extensions. La parité du compte des colorations normalisées est donc celle de #3SAT(Φ).

Une clause vide donne deux choix et une tautologie un choix. Les répétitions ne modifient pas les couleurs vues par l'auxiliaire. Le triangle normalise les orbites. Après suppression des doublons, le graphe est simple, sans sommet isolé et contient au moins trois arêtes. La représentation dense des domaines a taille polynomiale. Par (4), le deuxième bit donne la parité recherchée.

Appartenance. Le deuxième bit de N vaut C(N,2) mod 2. Le vérificateur lit deux sélections en ordre lexicographique strict. Il utilise un index binaire de largeur fixée par domaine, rejette les codes hors domaine et vérifie chaque rang. Chaque paire non ordonnée a un seul témoin accepté. □

Bits supérieurs. Dans $\mathbb{F}_2[z]$, décomposer N en binaire factorise $(1+z)^N$. Le facteur pour chaque bit j à un est $1+z^{2^j}$. Le coefficient de z^{2^j} donne le bit j. Pour j fixé, le vérificateur lit 2^j sélections distinctes en ordre canonique. Pour $j \geq 2$, ajouter $j-1$ dimensions disjointes avec deux domaines {e} et {0,e} sur chacune. Le premier force la dimension, le second double le compte. Le facteur total 2^{j-1} transfère la dureté du bit 1. Ceci porte sur les domaines arbitraires et les indices fixés.

Compte exact. Le vérificateur de rang donne l'appartenance à #P. En carré, limiter chaque domaine aux vecteurs de base permis par une matrice 0–1 réalise son permanent, car les indices choisis doivent être distincts. Valiant établit la #P-complétude sous réductions de Turing et un algorithme polynomial pour le permanent modulo 2^k à k fixé [2].

Existence. Si tous les domaines sont non vides, l'intersection du matroïde linéaire des paires (i,v) et du matroïde de partition imposant au plus un choix par i donne en temps polynomial une famille indépendante de taille maximale [3,14]. Si elle a taille r, on complète les positions restantes arbitrairement.

5. Calculs et reproduction

Graphe	Sommets	Arêtes	$\chi(3)$	Orbites	N exact	N mod 4
Triangle	3	3	6	1	14	2
Cycle C_4	4	4	18	3	30	2
Graphe complet K_4	4	6	0	0	1 960	0

Le tableau compare trois calculs. Le premier énumère les choix et vérifie leur rang. Le deuxième applique (3) sur les sous-espaces. Le troisième énumère les colorations et applique (4). Pour la clause unitaire (x), le gadget a une affectation vraie et donne trois colorations avec le triangle fixé, soit 1 + 2. Il produit bien $N \equiv 2$ modulo quatre.

Rang 256. Fixons $\{e_1\}$ et $\{e_2\}$, puis $A_i = \{e_i, e_i+e_1, e_i+e_2\}$, pour $3 \le i \le 256$. Tout choix est triangulaire avec une diagonale de 1. Le compte est donc 3^{254}. Le XOR du domaine $i \ge 3$ est $e_i+e_1+e_2$. Les 256 équations homogènes ont rang 256. Gauss retrouve la parité sans parcourir les 3^{254} choix.

Protocole. Les scripts Python utilisent la bibliothèque standard, des graines fixes et des entiers exacts. Lancer python -B -S code/reproduire.py calculs, puis python -B -S code/verifier_raccordement.py depuis le dossier du préprint. Le journal couvre 210 modèles de lignes, 45 graphes étiquetés sur trois ou quatre sommets, 160 formules pour le gadget et 5 réductions complètes. Il comprend aussi les contrôles du raccordement de l'annexe. Les fichiers JSON et CSV contiennent les nombres calculés. Les tests comparent des méthodes et des cas finis. Les théorèmes suivent des preuves ci-dessus.

6. À quoi sert le modèle

Codes et communications. Pour une matrice binaire de codage à lignes sélectionnables, N compte les configurations qui conservent r directions indépendantes. Sous des choix indépendants et uniformes dans chaque A_i non vide, $N / \prod_i |A_i|$ est la probabilité exacte de rang plein. Des pertes corrélées ou une distribution non uniforme demandent un modèle de probabilités adapté.

Capteurs et contrôle. Si des mesures sont des formes binaires, le rang plein garantit l'identification de l'état binaire à partir des mesures exactes. Le petit exemple de la section 2 est déjà un modèle avec deux mesures fixes et une mesure sélectionnable. Pour des capteurs réels, la géométrie, le bruit et la stabilité numérique nécessitent une analyse propre.

Calcul distribué et validation combinatoire. Le raccordement de l'annexe dénombre les complétions compatibles entre deux blocs d'observations. Les identités modulo deux et quatre donnent des contrôles de cohérence pour des solveurs de comptage et des générateurs de matrices structurées. Ces transferts sont des usages du modèle binaire. Les expériences rapportées portent sur des instances construites.

Annexe A. Raccordement de deux blocs

Soit $T \le U$ l’espace engendré par les lignes communes fixées. Les blocs gauche et droit sont pondérés par des messages $m_L(R)$ et $m_R(S)$ sur les espaces d’images R,S contenant T. Chaque poids compte les configurations locales d’image donnée. Supposons que les choix locaux soient indépendants une fois les données communes fixées. Il reste h lignes cachées libres dans U. Posons $d = \dim(R+S)$ et $q = 2^h$.

$$M(R,S) = q^{d} \prod_{i=0}^{r-d-1} (q - 2^{i}). \tag{5}$$

Les h lignes projetées dans $U/(R+S)$ forment une matrice $h \times (r-d)$. Pour être de rang plein, ses colonnes doivent être indépendantes. Les choix successifs ont $q - 2^i$ possibilités. Chaque ligne projetée a 2^d relèvements. Si $h < r-d$, un facteur vaut zéro. Le produit vide vaut un. Le compte complet est $\Sigma_{R,S}\, m_L(R)\, M(R,S)\, m_R(S)$.

Factorisation entière. Dans l’intervalle $[T,U]$, posons $Z_{R,W} = 1$ si $R \le W$, et 0 sinon. L’inversion de Möbius donne une factorisation de matrice de jointure [4].

$$M = Z\, \mathrm{diag}_{W \in [T,U]}(\mu(W,U) \cdot 2^{h \dim W})\, Z^{\top}. \tag{6}$$

En effet, le nombre de choix des h lignes toutes dans W vaut $2^{h \dim W}$ pour W contenant $R+S$. Le tri par dimension rend Z triangulaire de diagonale un, donc inversible sur $\mathbb{Z}$. Les facteurs de Smith sont les $2^{h \dim W + c(c-1)/2}$, rangés par exposant croissant, avec $c = r - \dim W$. Sur $\mathbb{Q}$, M a rang plein. Pour $h = 0$, seules les codimensions 0 et 1 donnent un facteur impair et le rang modulo deux vaut $2^{r - \dim T}$.

Calcul à 256 positions privées. À gauche, 128 lignes ont la première coordonnée nulle. À droite, 128 lignes ont la deuxième coordonnée nulle. Le rang cible est 6. Chacune des deux premières colonnes a 2^{128+h} possibilités, dont une nulle. Parmi les couples non nuls, exactement $2^h - 1$ couples ont deux colonnes égales, puisque leur support commun est caché. Choisir ensuite les quatre colonnes restantes par extension du rang donne

$$((2^{128+h}-1)^2 - (2^h-1)) \prod_{i=2}^{5} (2^{256+h} - 2^{i}). \tag{7}$$

Cette formule indépendante concorde avec le raccordement et avec (3) pour $h = 0$ et $h = 2$. Les deux comptes ont respectivement 1 280 et 1 292 bits. Le vérificateur contrôle 45 matrices de raccordement, 36 formes de Smith obtenues par les mineurs, ainsi que quatre valeurs communes pour des observations non coordonnées.

7. Positionnement et conclusion

Support prescrit. Le compte du théorème 2 est un cas du modèle de Lewis et al. [5, §5]. Le motif autorise deux entrées par ligne, aux extrémités de l'arête, toutes les autres étant nulles. Leur proposition 5.1 donne une congruence en puissances de q−1, dont le module vaut 1 pour q = 2. Leurs formules de la section 2 portent sur des zéros diagonaux. La congruence (4) porte sur les plans d'arêtes à q = 2, modulo quatre.

Problème critique. Les noyaux de (4) évitent l'ensemble formé des e_v et des e_u+e_v pour $uv \in E$. C'est une instance du problème critique de Crapo et Rota [8,9]. La représentation est celle du matroïde graphique du cône sur G. Son polynôme caractéristique évalué en 4 compte les 4-colorations propres du cône dont le sommet ajouté a une couleur fixée, soit $\chi_G(3)$. Le lien entre noyaux et colorations est donc classique. Le théorème 2 le relie au compte entier de rang plein réduit modulo quatre.

Comptage modulaire. Les classifications de CSP et d'homomorphismes modulaires [10–12,18] donnent le cadre général. Le théorème 90 de la version arXiv de Focke et al. [13] implique déjà la $\oplus$P-complétude des 3-colorations à listes modulo deux. Groenland et al. [17, §4.3 de la version longue] étudient les mêmes orbites de colorations et codent les listes par des cliques de référence. Ici, un seul triangle fixé suffit en reliant chaque sommet aux couleurs interdites. On traite les listes vides et les sommets isolés par leurs facteurs de parité. Ces antécédents donnent une voie vers la difficulté des colorations normalisées, puis, via (4), du bit 1. La section 4 en donne une preuve directe.

Matroïdes et parité. En carré, les sélections de rang plein sont exactement les bases communes d'un matroïde linéaire et d'un matroïde de partition [3,14]. Le cadre de Cauchy–Binet pour les bases communes [15] couvre la parité binaire de ce cas. En rectangulaire, plusieurs bases communes peuvent contribuer au même tuple. Le théorème 1 compte les tuples complets.

La complétude caractérise la complexité du second bit. Un algorithme polynomial pour ce bit équivaut à P = $\oplus$P. Aucune séparation de classes n'est établie ici et P contre NP demeure ouvert [7]. La recherche bibliographique ciblée n'établit aucune priorité.

Le projet a été motivé par la démarche assistée par IA d'Alpöge et de Claude, qui a donné lieu à une annonce de preuve de l'hypothèse de Riemann [6,16]. Les théorèmes du présent article reposent sur des arguments d'algèbre et de combinatoire finies.

Déclarations

Auteur. Zakaria Gharzouli a conçu le programme de recherche et mandaté la révision. OpenAI Codex a assisté la formalisation des arguments, les calculs, le code et la rédaction. Les scripts sont fournis et les contrôles croisés ont été réexécutés. L'auteur a personnellement validé le manuscrit. Il déclare n'avoir reçu aucun financement et n'avoir aucun conflit d'intérêts.

Statut et licence. Prépublication non évaluée par les pairs. L'audit assisté par IA et les tests ne constituent pas une relecture humaine indépendante. Licence CC BY 4.0.

Références

[1] G.-C. Rota (1964). On the foundations of combinatorial theory I. Theory of Möbius functions. *Z. Wahrscheinlichkeitstheorie verw. Geb.* 2, 340–368. DOI · Texte

[2] L. G. Valiant (1979). The complexity of computing the permanent. *Theoretical Computer Science* 8(2), 189–201. DOI

[3] J. Edmonds (1979). Matroid intersection. *Annals of Discrete Mathematics* 4, 39–49. DOI

[4] M. Mattila et P. Haukkanen (2013). Determinant and inverse of join matrices on two sets. *Linear Algebra and its Applications* 438(10), 3891–3904. DOI · arXiv:1110.4953

[5] J. B. Lewis, R. I. Liu, A. H. Morales, G. Panova, S. V. Sam et Y. X. Zhang (2011). Matrices with restricted entries and q-analogues of permutations. *Journal of Combinatorics* 2(3), 355–395. DOI · arXiv:1011.4539

[6] L. Alpöge (20 novembre 2026). *Remark*, note accompagnant la diffusion du travail réalisé avec Claude sur l'hypothèse de Riemann. Note de l'auteur

[7] Clay Mathematics Institute. *P vs NP*. Consulté le 26 novembre 2026. Page du problème

[8] H. H. Crapo et G.-C. Rota (1970). *On the Foundations of Combinatorial Theory: Combinatorial Geometries*. MIT Press, chapitre 16. Éditeur

[9] J. P. S. Kung (1996). Critical problems. Dans *Matroid Theory*, Contemp. Math. 197, AMS, 1–127. Texte

[10] J. Faben (2008). The complexity of counting solutions to Generalised Satisfiability Problems modulo k. arXiv:0809.1836

[11] J. Faben et M. Jerrum (2015). The Complexity of Parity Graph Homomorphism: An Initial Investigation. *Theory of Computing* 11(2), 35–57. DOI

[12] A. A. Bulatov et A. Kazeminia (2024). Complexity Classification of Counting Graph Homomorphisms Modulo a Prime Number. *SIAM Journal on Computing*, STOC22-182–223. DOI · arXiv:2106.04086

[13] J. Focke, L. A. Goldberg, M. Roth et S. Živný (2021). Counting Homomorphisms to K_4-Minor-Free Graphs, Modulo 2. *SIAM Journal on Discrete Mathematics* 35(4), 2749–2814. DOI · arXiv:2006.16632

[14] R. Rado (1942). A theorem on independence relations. *Quarterly Journal of Mathematics* os-13(1), 83–89. DOI

[15] K. Matoya et T. Oki (2022). Pfaffian Pairs and Parities: Counting on Linear Matroid Intersection and Parity Problems. *SIAM Journal on Discrete Mathematics* 36(3), 2121–2158. DOI

[16] M. Rubinstein (2026). Alpöge/Claude proof of the Generalized Riemann Hypothesis. Consulté le 26 novembre 2026. Note et vérifications

[17] C. Groenland, I. Mannens, J. Nederlof et K. Szilágyi (2022). Tight Bounds for Counting Colorings and Connected Edge Sets Parameterized by Cutwidth. *STACS*, 36:1–36:20. DOI · arXiv:2110.02730

[18] A. A. Bulatov et A. Kazeminia (2026). Modular Counting over 3-Element and Conservative Domains. *STACS*, 22:1–22:20. DOI