L'Ordinateur et le Mathématicien

Thomas Fernique

Dubna, 19–29 juillet 2016

1 Le théorème des quatre couleurs

1.1 Coloriage de graphes

Une carte est partition d'une partie du plan en un nombre fini de compacts homéomorphes à des disques (les pays). On lui associe un graphe planaire dual : chaque pays correspond à un sommet, deux sommets étant reliés si les pays correspondants sont adjacents. Un k-coloriage d'une carte/graphe consiste alors à affecter une couleur parmi k à chaque pays/sommet de sorte à ce que deux pays/sommets voisins aient une couleur différente.

Question 1 *Existe-t-il un nombre fini de couleur permettant de colorier n'importe quelle carte ? Si oui, quel est le plus petit tel nombre ?*

L'exemple du Luxembourg montre qu'il faut au moins quatre couleurs. L'exemple de la clique (graphe complet) montre que la planarité est nécessaire. Le théorème de De Bruijn-Erdős (1951) montre que ce nombre est le même pour un graphe infini.

Conjecture 1 (Guthrie, 1852) *Quatre couleurs suffisent.*

Comme remarqué par Cayley (1879), on peut se restreindre aux cartes *cubiques*, c'est-à-dire qui n'ont que des points triples. En effet, les points doubles peuvent être supprimés sans rien changer, et il suffit de rajouter un pays sur chaque point de degré quatre ou plus pour obtenir une carte cubique dont on dérive de tout k-coloriage un k-coloriage de la carte initiale simplement en supprimant le pays ajouté (Fig. 1). En terme de graphe dual, cela revient à étudier la colorabilité des graphes planaires *triangulés*.

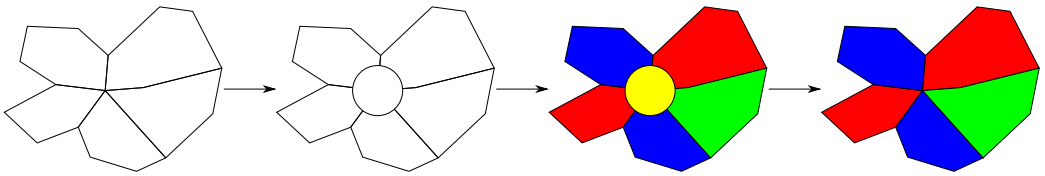

FIGURE 1 – La k-colorabilité des cartes et des cartes cubiques est équivalente.

1.2 Six couleurs

Théorème 1 (Euler, 1752) *Soit un graphe planaire (simple et connexe) avec s sommets, a arêtes et f faces. Alors $s - a + f = 2$.*

Preuve. On réduit pas à pas le graphe en montrant que la quantité $s-a+f$ est conservée. S'il y a un sommet pendant, on l'enlève avec son arête incidente :

$$s \to s - 1, \qquad a \to a - 1, \qquad f \to f.$$

Sinon on enlève une arête entre deux faces (qui sont donc fusionnées) :

$$s \to s, \qquad a \to a - 1, \qquad f \to f - 1.$$

En au plus a étapes on se retrouve avec un unique sommet et on a :

$$s = 1, \qquad a = 0, \qquad f = 1,$$

ce qui donne bien la valeur $s - a + f = 2$. □

Théorème 2 *Tout graphe planaire*[1] *a un sommet de degré au plus cinq.*

Preuve. Considérons un graphe planaire avec s sommets, a arêtes et f faces. Chaque face est délimitée par au moins 3 arêtes et chaque arête est partagée par exactement 2 faces, d'où :

$$2a \geq 3f.$$

Si au moins 6 arêtes partent de chaque sommet, alors comme chaque arête relie exactement 2 sommets, on a

$$2a \geq 6s.$$

1. sans arête multiple

La relation d'Euler donne alors

$$2 = s - a + f \leq \tfrac{1}{3}a - a + \tfrac{2}{3}a = 0.$$

Cette contradiction montre que les sommets ne peuvent pas tous être de degré au moins 6. □

Remarque 1 *Dans [1] la preuve (page* 39*) est similaire mais faite sur les cartes,* i.e.*, duale.*

En particulier, on ne peut pas faire de ballon de foot avec seulement des faces hexagonales. On en déduit aussi facilement :

Théorème 3 *Six couleurs suffisent.*

Preuve. Par l'absurde. Considérons un graphe non 6-coloriable minimal en terme de nombre de sommets. La relation d'Euler assure qu'il a un sommet de degré $k < 6$. En enlevant ce sommet et ses arêtes incidentes on a, par minimalité, un graphe 6-coloriable. On peut alors rajouter ce sommet et ses arêtes et lui affecter une couleur non utilisée par ses $k < 6$ voisins. On a la contradiction recherchée. □

1.3 Recoloriage

Avec moins de six couleurs l'argument précédent ne marche plus car un pays entouré de cinq autres pays n'a plus forcément de couleur "libre". Un outil utile pour libérer une couleur est alors le *recoloriage de Kempe* :

1. Soit un graphe entièrement colorié excepté un sommet v_0.
2. Soit un sommet voisin de v_0, mettons de couleur bleu.
3. Choisir une autre couleur "cible", mettons vert, et considérer la composante connexe bleu-vert qui contient ce sommet (*chaîne de Kempe*).
4. Si elle ne contient pas d'autre voisin de v_0, alors interchanger bleu et vert dans cette composante (*recoloriage de Kempe*).

Si le sommet v_0 n'avait qu'un voisin bleu, alors ce recoloriage de Kempe a permis de libérer cette couleur pour v_0. On parle de *D-réductibilité* (selon la terminologie de Heesch) :

Définition 1 (D-reductibilité) *Une configuration est dite* D-réductible *si tout* 4*-coloriage des pays qui l'entourent peut être complété en un* 4*-coloriage de la configuration après d'éventuels recoloriages de Kempe.*

Théorème 4 (Kempe, 1879) *Un pays avec* $k \leq 5$ *voisins est D-réductible.*

Preuve. Soit v_0 le sommet d'un tel pays. Si ses voisins utilisent au plus trois couleurs, ce qui est en particulier le cas si $\deg(v_0) \leq 3$, alors il en reste une libre et la complétion est immédiate. Il reste donc deux cas :
1. Le sommet v_0 a quatre voisins de couleurs toutes différentes, mettons rouge, vert, bleu et jaune dans le sens des aiguilles d'une montre (Fig. 2). Il ne peut y avoir simultanément une chaîne rouge-bleu qui boucle sur les voisins rouge et bleu et une chaîne vert-jaune qui boucle sur les voisins vert et jaune (obstruction topologique). On peut donc faire un recoloriage de Kempe sur une chaîne qui ne boucle pas et libérer une couleur pour v_0.
2. Le sommet v_0 a cinq voisins utilisant les quatre couleurs, mettons rouge, vert, bleu, jaune et vert dans le sens des aiguilles d'une montre (Fig. 3). S'il n'y a pas de boucle rouge-bleu ou rouge-jaune, on libère une couleur pour v_0 par recoloriage de Kempe. Sinon, alors la boucle rouge-bleu (resp. rouge-jaune) isole en l'entourant une chaîne vert-jaune (resp. vert-bleu). Un recoloriage de Kempe sur ces deux chaînes permet alors de libérer le vert pour v_0. □

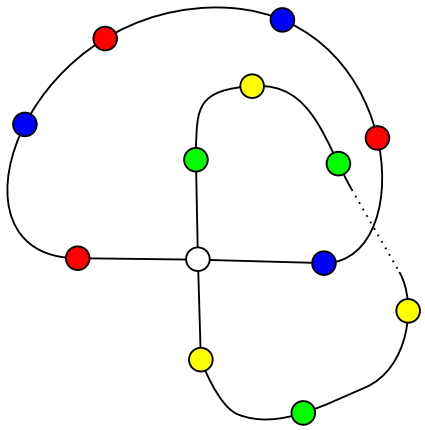

FIGURE 2 – Si la chaîne rouge-bleu boucle, alors la chaîne vert-jaune ne peut pas boucler. Un recoloriage de Kempe peut alors libérer vert (ou jaune).

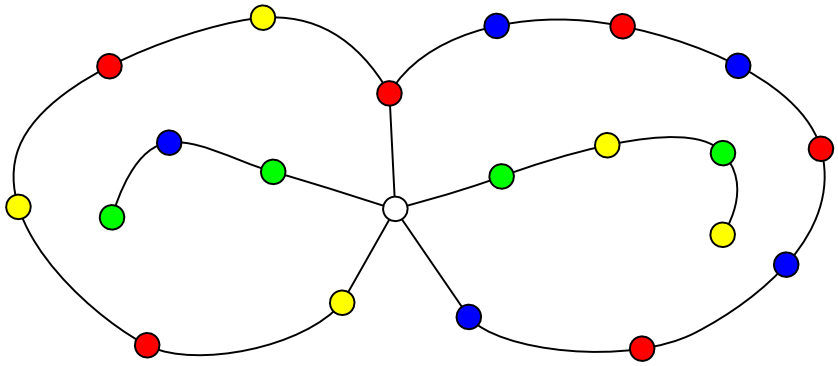

FIGURE 3 – Une boucle rouge-jaune (resp rouge-bleu) isole une chaîne vert-bleu (resp. vert-jaune). Un recoloriage de Kempe sur ces chaînes libère vert.

On adapte alors facilement la preuve du théorème des six couleurs pour montrer que quatre couleurs suffisent !

Seul hic : le raisonnement de Kempe dans son deuxième cas est faux, comme remarqué par Heawood en 1889 (dix ans plus tard). En effet, le problème est que les boucles rouge-bleu ou rouge-jaune ont en commun rouge et peuvent donc se croiser (Fig. 4). Donc même si la boucle rouge-jaune (resp rouge-bleu) isole bien une chaîne vert-bleu (resp. vert-jaune), cette chaîne peut boucler sur le voisin bleu (resp. jaune) de v_0, de sorte que les recoloriage de Kempe ne libéreront pas forcément une couleur...

Néanmoins, si on se donne 5 couleurs, alors le recoloriage de Kempe marche pour un sommet de degré 5 comme il marchait avec 4 couleurs pour un sommet de degré 4. On en déduit :

Théorème 5 *Cinq couleurs suffisent.*

1.4 Réductibilité

Que le pentagone ne soit pas D-réductible ne prouve pas que quatre couleurs ne suffisent pas. On peut en effet imaginer bien d'autres notions de réduction, comme celle due à Birkhoff (ici avec la terminologie de Heesch) :

Définition 2 (A-réductibilité) *Soit $\mathcal{C}$ une configuration et $x_1, \ldots, x_k$ son* bord, i.e., *le cycle formé par ses sommets connectés hors de $\mathcal{C}$. Elle est dite*

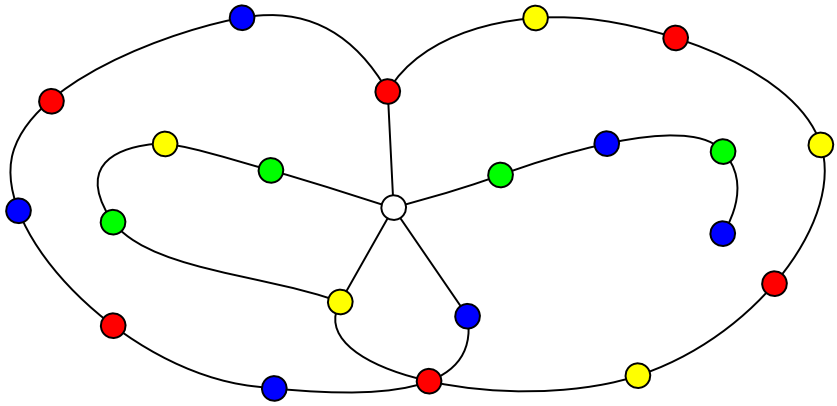

FIGURE 4 – L'erreur de Kempe : les boucles rouge-bleu et rouge-jaune peuvent se croiser, faussant le raisonnement.

A-réductible *s'il existe une configuration $\mathcal{C}'$ plus petite, de bord $y_1, \ldots, y_k$, telle que tout 4-coloriage du bord de $\mathcal{C}$ induit par un 4-coloriage de $\mathcal{C}'$ en donnant à x_i la couleur de y_i se prolonge en un 4-coloriage de $\mathcal{C}$.*

Par exemple, comme le montre la figure 5, le carré est A-réductible.

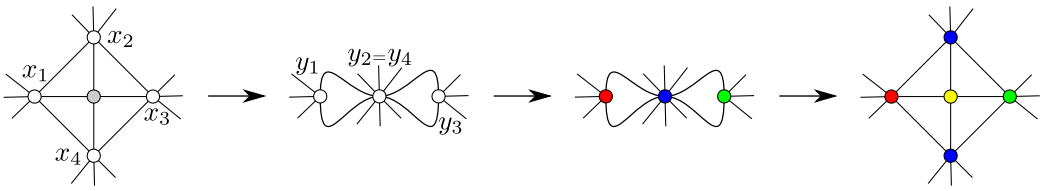

FIGURE 5 – Le carré est A-réductible.

On parle de *B-réductibilité* ou *C-réductibilité* si on autorise en plus un ou plusieurs recoloriages de Kempe sur le bord de $\mathcal{C}'$. On a donc les inclusions suivantes pour la réductibilité des configurations :

$$A \subset B \subset C \qquad \text{et} \qquad D \subset C.$$

Un des premiers exemples est la configuration appelée *diamant de Birkhoff* (Fig. 6). Birkhoff a montré qu'il était B-réductible (Fig. 7 et Fig. 8) et donc qu'il ne pouvait apparaître dans un contre-exemple minimal. On peut montrer qu'il est en fait D-réductible (c'est plus long).

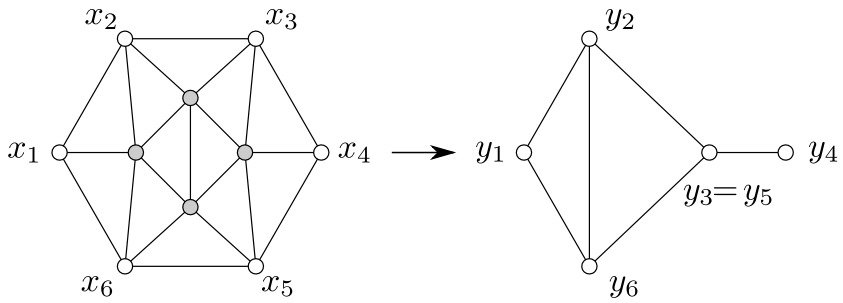

FIGURE 6 – Le diamant de Birkhoff (à gauche) et son réducteur (à droite).

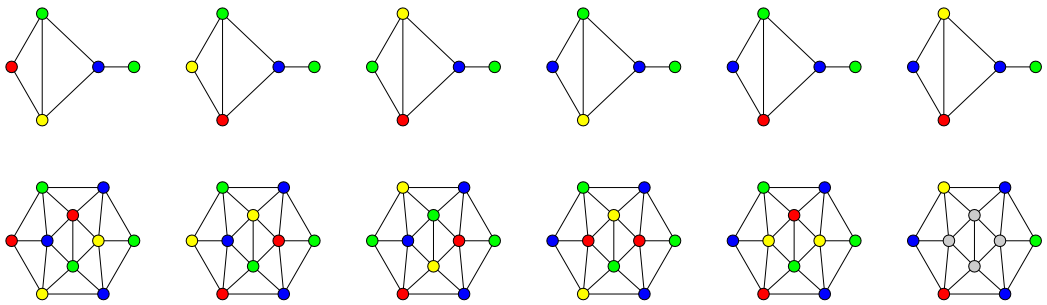

FIGURE 7 – Le diamant réduit admet 6 coloriages différents à permutation des couleurs près. Les coloriages induits sur le bord du diamant se prolongent tous sur son intérieur, sauf un (le dernier).

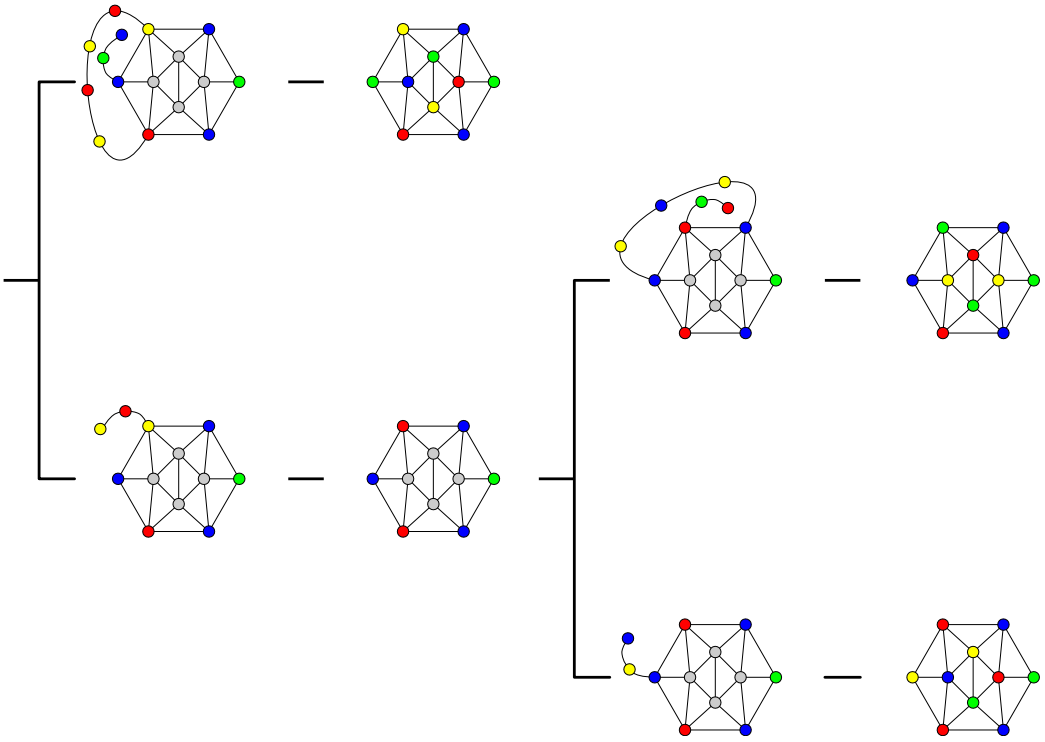

FIGURE 8 – On traite ce dernier bord via un ou deux recoloriage de Kempe.

1.5 Inévitabilité

Définition 3 *Un ensemble de configurations est dit* inévitable *si toute carte contient au moins une de ces configurations.*

Pour montrer que quatre couleurs suffisent, il suffirait de trouver un ensemble inévitable de configurations toutes réductibles. On a déjà montré, grâce à la relation d'Euler, que l'ensemble constitué des sommets de degré 5 ou moins était inévitable. Malheureusement le pentagone n'est pas réductible. Parmi les mathématiciens qui ont cherché des ensembles inévitable on peut par exemple citer Lebesgue. On va ici exposer une méthode due à Heesch, dite de *déchargement*. D'abord, on raffine la relation d'Euler :

Proposition 1 *Soit une carte cubique avec s_i pays ayant i voisins. Alors*

$$4s_2 + 3s_3 + 2s_4 + s_5 - s_7 - 2s_8 - 3s_9 - \ldots = 12.$$

Preuve. Considérons un graphe triangulé avec f faces, a arêtes et s sommets, dont s_i de degré i. On a

$$s = s_2 + s_3 + s_4 + \ldots$$

Chaque arête étant commune à deux sommets, on a aussi

$$2a = 2s_2 + 3s_3 + 4s_4 + \ldots$$

Enfin, le graphe étant triangulé, chaque face a trois arêtes, chacune comptant pour deux faces, d'où

$$3f = 2a.$$

On injecte alors dans la relation d'Euler :

$$f - a + s = 2 \;\Leftrightarrow\; -\frac{a}{3} + s = 2 \;\Leftrightarrow\; 6s - 2a = 12 \;\Leftrightarrow\; \sum_{i\geq 2}(6-i)s_i = 12.$$

C'est bien la formule annoncée. □

Par exemple, un ballon de foot étant fait de pentagones et hexagones, la formule ci-dessus montre qu'il y a forcément 12 pentagones. Mais on peut aller plus loin :

Proposition 2 (Wernicke, 1903) *Une carte cubique contient soit un pays avec au plus quatre voisins, soit deux pentagones adjacents, soit un pentagone adjacent à un hexagone.*

Preuve. Associons à chaque sommet de degré i le nombre $6 - i$, appelé sa *charge*. La formule précédente assure que la charge totale du graphe vaut 12. Supposons maintenant que la carte n'a aucune des configurations annoncée et appliquons la règle de *déchargement* suivante : chaque pentagone (s'il y en a), qui a une charge $6 - 5 = 1$, donne $\frac{1}{5}$ à chacun de ses voisins. La charge totale est évidemment inchangée, pourtant tous les pays ont une charge négative ! En effet

- il n'y a pas de pays avec au plus quatre voisins ;
- deux pentagones n'étant jamais voisins, ils se retrouvent à 0 ;
- un hexagone n'étant jamais voisin d'un pentagone, il reste à 0.
- un pays avec $k \geq 7$ voisins en ayant au plus $\lfloor k/2 \rfloor$ qui sont des pentagones (sinon deux seraient adjacents), sa nouvelle charge est au plus

$$6 - k + \left\lfloor \frac{k}{2} \right\rfloor \times \frac{1}{5} \leq -\frac{2}{5}.$$

Cette contradiction prouve la proposition. □

Malheureusement, personne ne sait prouver directement la réductibilité d'un pentagone adjacent à un pentagone ou un hexagone (qui est cependant un corollaire du théorème des quatre couleurs). D'autres règles de déchargement permettent d'obtenir divers ensembles inévitables de plus en plus complexes, comme celui de la proposition ci-dessous (dû à Franklin en 1920) ou celui de la figure 9 (dû à Chojnacki et Hanani en 1942).

Proposition 3 (Franklin, 1920) *Une carte cubique contient soit un pays avec au plus quatre voisins, soit un pentagone adjacent à deux pays ayant chacun cinq ou six voisins.*

1.6 L'ordinateur à la rescousse

La piste est maintenant tracée : il faut trouver un ensemble de configurations inévitables dont on puisse prouver la réductibilité… mais l'un comme l'autre deviennent des tâches de plus en plus calculatoires. Or c'est à cette

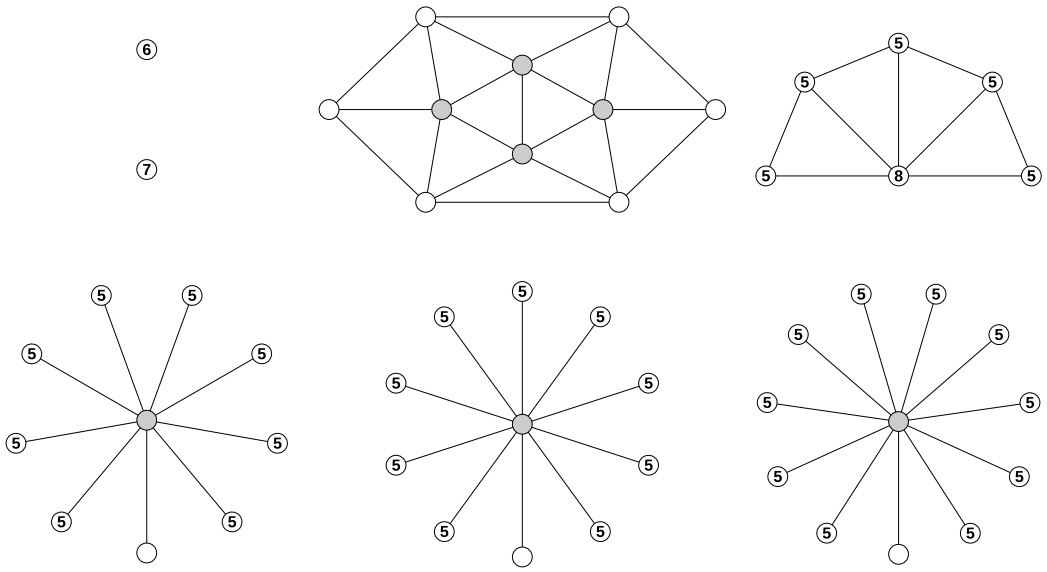

FIGURE 9 – Un ensemble inévitable de 7 configurations (les sommets dont tous les voisins sont représentés sont grisés, et une étiquette indique un degré prescrit). Toutes sont prouvées réductibles sauf l'hexagone et l'heptagone.

époque, vers le début des années 60, que les premiers calculateurs, apparus dans les années 50, commencent à devenir raisonnablement accessibles. Cependant, même pour un ordinateur (surtout à cette époque), les calculs sont vite trop long (en particulier vérifier la réductibilité) et il faut ruser en utilisant des *heuristiques*, c'est-à-dire des règles empiriques qui permettent d'éviter des cas dont on pense qu'ils ne donneront rien, comme par exemple :

Heuristique 1 (Appel-Haken-Heesch) *Une configuration formée de n pays* externes *entourant m autres pays* internes *est "sans doute facilement réductible" si $m \geq \frac{3}{2}n - 6$ et si elle ne contient*

- *ni un pays interne adjacent à quatre pays externes consécutifs ;*
- *ni un pays interne adjacent à trois pays externes non consécutifs.*

Le diamant de Birkhoff vérifie cela, mais pas les autres configurations de la figure 9 (pourtant prouvées réductibles à la main sauf l'hexagone et l'heptagone).

Après une course contre la montre face à des concurrents menaçants, Appel et Haken arrivent à prouver fin juin 1976 la réductibilité d'un ensemble

de 1482 configurations, qu'ils avaient auparavant montrées être inévitables via 487 règles de déchargement. Le théorème des quatre couleurs était prouvé !

Théorème 6 (Appel-Hakken, 1976) *Quatre couleurs suffisent.*

Remarque 2 *Bien qu'ayant apporté les principales idées de cette preuve, Heesch a dû se retirer car l'université de Göttingen lui a refusé sa puissance de calcul, contrairement à l'université d'Illinois pour Appel et Haken.*

1.7 Exercices

1. 4-colorier la carte Fig. 10, à gauche (poisson d'avril 1975 de Gardner).
2. 3-colorier les gadgets Fig. 10, à droite.

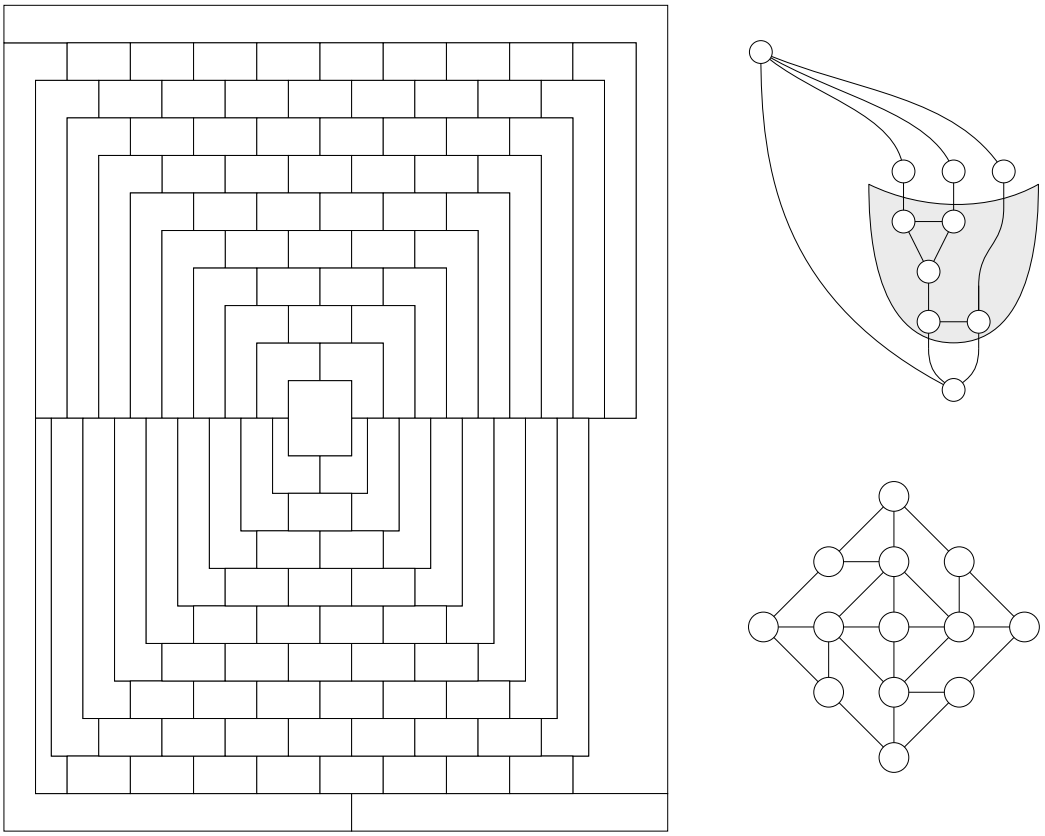

FIGURE 10 – Coloriages.

2 Le problème des trois couleurs

2.1 Algorithme et complexité

On déduit facilement de la preuve du théorème des six couleurs un *algorithme*, *i.e.*, un procédé automatique (comme une recette de cuisine), pour colorier effectivement en six couleurs une carte donnée :

```
colore(c: carte)
 si c n'a qu'un seul pays
 - le colorier en rouge (par exemple)
 - renvoyer la carte c coloriée
 sinon
 - trouver un pays avec au plus 5 voisins
 - contracter ce pays en un point pour obtenir une carte c'
 - colorier la carte c' par un appel récursif à colore(c')
 - redilater le pays
 - lui choisir une couleur non utilisée par ses voisins
 - renvoyer la carte c coloriée
```

L'algorithme termine car à chaque appel récursif il y a un pays de moins. On montre par induction sur le nombre de pays qu'il renvoit une carte bien coloriée. Mais comment croît le *temps d'exécution* avec le nombre n de pays ? On parle de la *complexité* de l'algorithme, qu'on cherche à *anayser*.

L'exemple emblématique est celui du *tri* d'une séquence de nombres :

insertion : insérer un à un dans une nouvelle liste initialement vide chaque nombre à sa place : $O(n^2)$;

bulle : échanger deux nombres consécutifs mal ordonnés (tant qu'il y en a) : $O(n^2)$;

fusion : trier récursivement chaque moitié puis les fusionner : $O(\log_2(n))$ ($c(n) = 2 * c(n/2) + n$) ;

rapide : idem mais couper selon le premier élément (*pivot*) : $O(\log_2(n))$.

Dans le cas du coloriage avec six couleurs (ci-dessus), il y a n boucles, chacune parcourant les n pays pour en trouver un avec au plus 5 voisins. Ceci va donner une complexité en $O(n^2)$ (ou linéaire en étant un peu malin). C'est un peu plus délicat pour quatre couleurs, mais Appel et Haken ont dérivé

un algorithme en $O(n^4)$, ce qui reste très raisonnable en pratique. Et s'il n'y a que trois couleurs ? Les cartes ne sont certes pas toutes 3-coloriables, mais certaines le sont... est-ce facile à déterminer algorithmiquement ?

2.2 NP-complétude

Une solution stupide mais qui marche : essayer tous les coloriages possibles (*brute force/perebor*). Pour n pays, ça fait 3^n coloriages à vérifier... On peut raffiner, par exemple choisir à chaque fois le pays qui a le moins de couleurs possibles, mais il y aura toujours des cas où ça ne changera pas grand chose. Pire, on va voir qu'il n'y a sans doute pas moyen de faire mieux car décider si un graphe planaire est 3-coloriable ou pas est un problème *NP-complet*.

Définition 4 (NP) *Un problème de décision est dit* NP *s'il existe une* machine de Turing non-déterministe *qui le décide en temps polynomial.*

Une *machine de Turing* est un modèle d'ordinateur (Turing, 1936). Il consiste en une tête qui se déplace sur un ruban infini (la mémoire) et qui, à chaque pas, selon ce qu'elle lit dans la case courante et son état courant, écrit quelque chose dans la case, se déplace à gauche ou à droite et passe dans un autre état (nombre fini d'états, nombre fini de symboles différents). En gros c'est un programme (l'ordinateur étant une machine de Turing *universelle*).

Une machine de Turing est dite *non-déterministe* s'il y a plusieurs actions possibles à chaque pas, la machine choisissant l'une d'elles ("la bonne"). Évidemment c'est un modèle totalement irréaliste, qui peut même paraître stupide, mais il se trouve que savoir si on peut toujours trouver une machine de Turing déterministe qui joue ce rôle est sans doute la principale question ouverte de l'informatique théorique, connu sous le nom de problème "P=NP" et un des septs *problèmes du millénaire*.

Définition 5 (NP-complet) *Un problème $\mathcal{D} \in NP$ est dit* NP-complet *si tout autre problème $\mathcal{D}' \in NP$ s'y ramène via une* réduction polynomiale*, c'est-à-dire un algorithme polynomial qui transforme toute instance de $\mathcal{D}'$ en une instance de $\mathcal{D}$ en préservant l'existence (ou pas) d'une solution.*

Si un problème de décision est NP-complet, le problème associé consistant à *calculer* une solution est dit *NP-difficile*.

Le problème de décision qui nous intéresse est 3-*colorabilité planaire* : un graphe planaire donné est-il 3-colorable ? C'est clairement un problème NP : il suffit de colorier les pays un à un en choisissant la bonne couleur ! Quid de la complétude ? Il suffirait de le réduire à autre problème déjà prouvé NP-complet...

2.3 Le théorème de Cook-Levin

Beaucoup des problèmes "intéressants" sont en fait NP-complets : sac-à-dos, voyageur de commerce, vertex-cover, partition d'entiers, arbre de Steiner, colorabilité de graphe, mariages à trois, Super Mario Bros...

On peut montrer qu'un problème NP est NP-complet en le réduisant à un autre problème NP-complet déjà connu, mais comment faire pour le premier ? Historiquement, c'est le problème SAT qui a joué ce rôle :

Définition 6 (SAT) *Étant donnée une formule de la logique propositionnelle, existe-t-il une instanciation de ses variables qui la satisfasse ?*

Théorème 7 (Cook-Levin, 1971) *SAT est NP-complet.*

Preuve. Considérons un problème dans NP et une machine non-déterministe $(Q, \Sigma, s, F, \delta)$ qui le décide en temps polynomial $p(|I|)$ sur une instance I, où
- Q est l'ensemble (fini) des états ;
- Σ est l'alphabet (fini) ;
- $s \in Q$ est l'état initial ;
- $F \subset Q$ est l'ensemble des états finaux ;
- $\delta \subset (Q \times \Sigma) \times (Q \times \Sigma \times \pm 1)$ est la fonction de transition.

On construit comme suit une formule de taille $O(p(|I|)^3)$ satisfiable ssi une des exécutions de la machine s'arrête en temps $p(|I|)$ sur l'instance I.

Les variables et leur interprétation sont
- Q_{qk} : la machine est dans l'état q au k-ème pas du calcul ;
- H_{ik} : la tête est sur la i-ème case du ruban au k-ème pas ;
- T_{ijk} : la i-ème case contient le symbole j au k-ème pas ;

où $q \in Q$, $j \in \Sigma$, $|i| \leq p(|I|)$ et $k \leq p(|I|)$.

La formule est la conjonction des quatre formules suivantes.
1. La conjonction des clauses suivantes, qui traduisent le fonctionnement de base de toute machine :

— $T_{ijk} \Rightarrow \neg T_{ij'k}$ pour $j \neq j'$: un seul symbole par case ;
— $Q_{qk} \Rightarrow\neq Q_{q'k}$ pour $q \neq q'$: un seul état à la fois ;
— $H_{ik} \Rightarrow \neg H_{i'k}$ pour $i \neq i'$: une seule tête sur le ruban :
— $T_{ijk} = T_{ij(k+1)} \vee H_{ik}$: on ne peut écrire que là où est la tête .

2. La conjonction des clauses suivantes, qui traduisent l'état initial du ruban et de la machine :

— Q_{s0} : la machine est dans l'état initial ;
— T_{iI_i0} : le ruban contient I ;
— H_{00} : la tête est en position en 0.

3. La disjonction des clauses suivantes, qui traduisent le fonctionnement non-déterministe de la machine. Pour chaque transition $(q, j, q', j', d) \in \delta$, chaque case i du ruban et chaque pas k du calcul :

$$(H_{ik} \wedge Q_{qk} \wedge T_{ijk}) \;\Rightarrow\; (H_{(i+d)(k+1)} \wedge Q_{q'(k+1)} \wedge T_{ij'(k+1)}).$$

4. La disjonction des $Q_{f,p(|I|)}$ pour $f \in F$, qui traduit que l'arrêt de la machine dans un état final. □

2.4 De SAT à CNF-SAT

Une formule de la logique propositionnelle en *forme normale conjonctive* est une une conjonction ($\wedge$) de disjonction ($\vee$) de littéraux (x ou $\neg x$). Soit F une formule de la logique propositionnelle quelconque, par exemple

$$F = \neg(x \vee y) \vee (z \wedge t).$$

On va la transformer en une formule en forme normale conjonctive. Tout d'abord, on utilise $P \Rightarrow Q \equiv \neg P \vee Q$ et les lois de De Morgan $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ et $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ pour obtenir une formule (au plus deux fois plus grande) formée de littéraux et des seuls connecteurs $\vee$ et $\wedge$.

$$F = (\neg x \wedge \neg y) \vee (z \wedge t).$$

On applique alors la fonction ϕ définie inductivement par les règles suivantes. Il y a trois règles naturelles, qui préservent l'équivalence logique :

$$\phi(x) = x, \qquad \phi(\neg x) = \neg x, \qquad \phi(P \wedge Q) = \phi(P) \wedge \phi(Q).$$

Ensuite, si $\phi(P) = P_1 \wedge \ldots \wedge P_n$ et $\phi(Q) = Q_1 \wedge \ldots \wedge Q_m$, alors on peut utiliser la distributivité pour obtenir une expression logiquement équivalente :

$$\phi(P \vee Q) = \bigwedge_{i,j} (P_i \vee Q_j).$$

Malheureusement ceci peut augmenter beaucoup la taille de la formule. En particulier, la formule de taille linéaire

$$(X_1 \wedge Y_1) \vee (X_2 \wedge Y_2) \vee \ldots \vee (X_n \wedge Y_n)$$

sera transformée en la formule de taille exponentielle

$$\bigwedge_{Z_i \in \{X_i, Y_i\}} (Z_1 \vee \ldots \vee Z_n).$$

C'est pour cela qu'on n'utilise la distributivité sur $P \vee Q$ que lorsque P ou Q est un littéral. Sinon, on introduit une variable z "fraîche" (*i.e.*, non utilisée par ailleurs) et on transforme $P \vee Q$ en une formule qui n'est pas logiquement équivalente mais seulement *équisatisfiable* (et c'est ce qui nous importe) :

$$\phi(P \vee Q) = \phi(z \vee P) \wedge \phi(\neg z \vee Q).$$

On montre alors que la taille de la formule finalement obtenue est au plus quadratique en celle de la formule initiale (on peut faire linéaire en utilisant la transformation de Tseytin), les deux étant equisatisfiable. On en déduit :

Théorème 8 *CNF-SAT est NP-complet.*

Sur notre exemple :

$$\begin{aligned} \phi((\neg x \wedge \neg y) \vee (z \wedge t)) &= \phi(u \vee (\neg x \wedge \neg y)) \wedge \phi(\neg u \vee (z \wedge t)) \\ &= (u \vee \neg x) \wedge (u \vee \neg y) \wedge (\neg u \vee z) \wedge (\neg u \vee t). \end{aligned}$$

Ici la distributivité aurait en fait conduit à une formule de la même taille :

$$(\neg x \vee z) \wedge (\neg x \vee t) \wedge (\neg y \vee z) \wedge (\neg y \vee t).$$

2.5 De CNF-SAT à 3-SAT

Étant donnée une formule de CNF-SAT, on remplace chaque clause

$$X_1 \vee \ldots \vee X_k$$

par une conjonction de $k-2$ clauses avec des variables fraîches $Y_1, \ldots, Y_{k-1}$:

$$(X_1 \vee X_2 \vee Y_1) \wedge (\neg Y_1 \vee X_3 \vee Y_2) \wedge \ldots \wedge (\neg Y_{k-1} \vee X_{k-1} \vee X_k).$$

Si la clause originale est vrai, il y a alors un X_i vrai et il suffit de poser
— $Y_{i-1}, \ldots Y_{k-2}$ faux pour satisfaire les clauses après celle contenant X_i ;
— $Y_1, \ldots, Y_{i-2}$ vrai pour satisfaire les clauses avant celle contenant X_i ;
de sorte que la conjonction de $k-2$ clauses est satisfaites.

Inversement, si la clause originale est fausse, alors tous les X_i sont faux. Pour satisfaire la première clause $(X_1 \vee X_2 \vee Y_1)$ il faut alors poser Y_1 vrai. Puis pour satisfaire la clause $(\neg Y_1, X_3, Y_2)$ il faut encore poser Y_2 vrai. De proche en proche on doit donc poser Y_i vrai pour tout i, jusqu'à la dernière clause $(\neg Y_{k-2} \vee X_{k-1} \vee X_k)$ qui est alors fausse.

La formule originale et sa transformée sont donc bien équisatisfiables. Cette dernière étant de taille linéaire en la taille de la première, on a prouvé

Théorème 9 *3-SAT est NP-complet.*

2.6 De 3-SAT à 3-colorabilité

On introduit ce qu'on appelle un *gadget*, en l'occurence un petit graphe appelé "porte ou" qui a une propriété spéciale, voir Figure 11. Puis, étant donnée une instance de 3-SAT, on utilise ce gadget pour définir un "graphe circuit" de taille polynomiale en cette instance et qui est 3-coloriable si et seulement si l'instance dest satisfiable (exemple Fig. 12) :

1. créer un somme "masse" ;
2. créer un sommet pour chaque littéral et un pour sa négation ;
3. les relier ensemble pour qu'ils n'aient pas la même valeur ;
4. relier tous ces sommets à la masse pour n'autoriser que deux couleurs qui seront interprétées comme "vrai" et "faux" ;

5. créer une porte *ou* par clause ;
6. relier les entrées de chaque "porte-clause" à ses littéraux ;
7. relier toutes les sorties en un unique sommet, qui sera aussi relié à la masse et dont la couleur sera interprétée comme "vrai".

On en déduit :

Théorème 10 *3-colorabilité est NP-complet.*

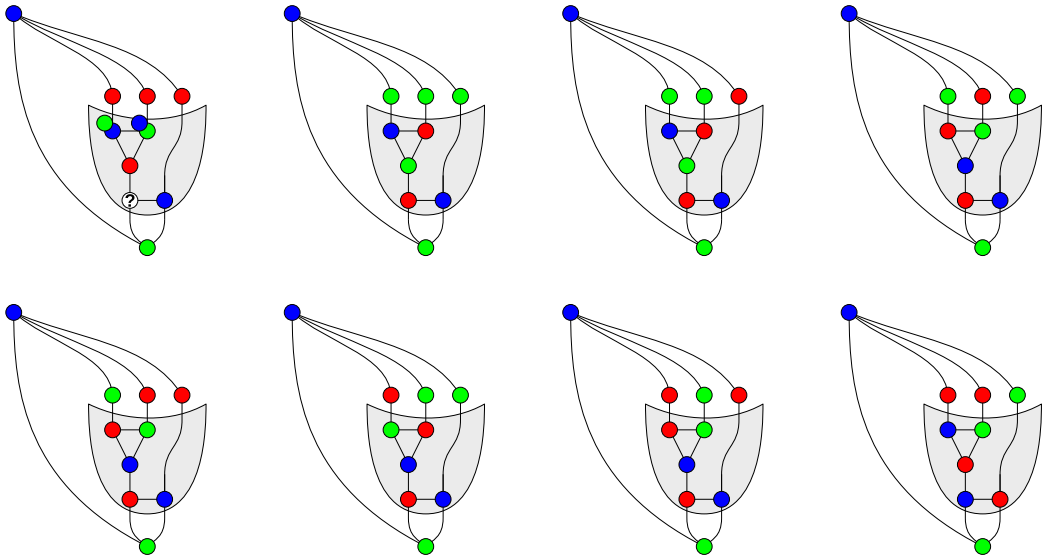

FIGURE 11 – Des "portes ou", reliées à la masse (en bleu en haut à gauche). La sortie est en vert, en bas. Il n'y a pas de 3-coloriage avec trois entrées rouges (porte de gauche). Par contre, toute autre coloriage des entrées se complète en un 3-coloriage (portes suivantes). En interprétant vert/rouge en vrai/faux, cette porte réalise donc la disjonction des trois entrées.

2.7 De 3-colorabilité à 3-colorabilité planaire

La transformation précédente donne un graphe G à 3-colorier qui n'est *a priori* pas planaire. On va ici le transformer en un graphe planaire G', de taille polynomiale en celle de G, et tel que l'un est 3-coloriable ssi l'autre l'est.

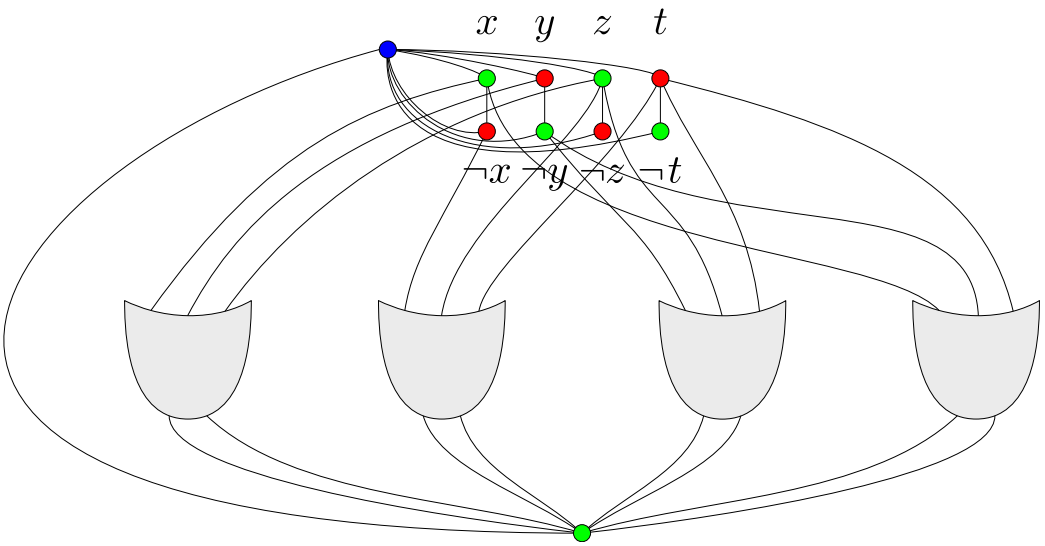

FIGURE 12 – Le graphe de $(x \vee y \vee z) \wedge (\neg x \vee z \vee t) \wedge (\neg y \vee z \vee t) \wedge (x \vee \neg y \vee t)$.

Ici encore on va utiliser un gadget. Il s'agit d'un graphe planaire obtenu en subdivisant un carré et dont les 3-coloriages donnent tous une même couleur à deux coins diagonalement opposés, en permettant toutes les combinaisons possibles, voir Figure 13.

On définit alors le graphe G' comme suit (exemple Figure. 14) :

1. le long d'une arête, on remplace tous les segments créés par les intersections - sauf un - par un *propagateur de couleur* ;
2. on remplace chaque intersection par le gadget précédent, en connectant deux coins opposés aux deux segments d'une même arête.

La transformation étant polynomiale, on a prouvé :

Théorème 11 *3-colorabilité planaire est NP-complet.*

2.8 Exercices

1. Que pensez-vous de 2-SAT ?
2. Que pensez-vous de l'égalité

$$\left\lceil \frac{2}{\sqrt[n]{2}-1} \right\rceil = \left\lfloor \frac{2n}{\log(2)} \right\rfloor$$

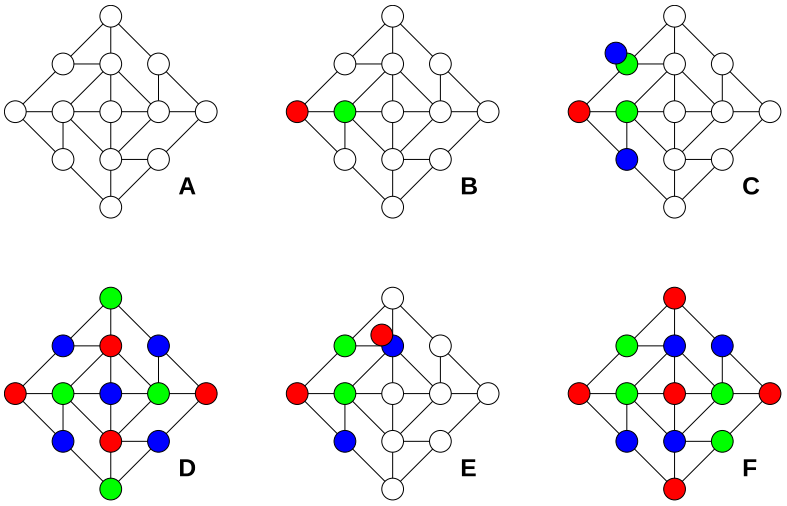

FIGURE 13 – **A.** Un gadget. **B.** Quitte à renommer les couleurs, on peut toujours colorier un coin en rouge et son voisin central en vert. **C.** La propagation des contraintes colorie en bleu un voisin du coin mais laisse un choix bleu/vert à l'autre. **D.** Un choix bleu donne, après propagation des contraintes, un 3-coloriage "croisement de fils différents". **E.** Un choix vert donne un nouveau choix bleu/rouge. **F.** Le choix bleu donne, après propagation des contraintes, un 3-coloriage "croisement de fils égaux", tandis qu'on vérifie que le choix rouge ne peut pas être prolongé en un 3-coloriage.

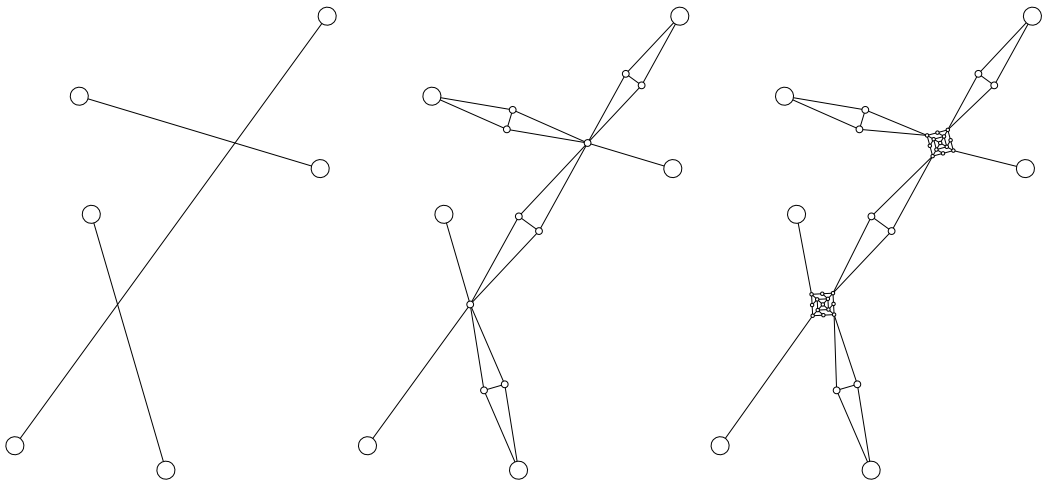

FIGURE 14 – Transformation d'un graphe G en un graphe planaire G' tel que l'un est 3-coloriable ssi l'autre l'est.

3 Du rôle de l'ordinateur

3.1 Vue d'ensemble

La figure 15 propose un schéma articulant les principales tâches occupant la vie du mathématicien. Le but de cette partie est d'illustrer chacune des transitions (sauf la première et la dernière, plutôt méta-mathématiques) par des exemples concrets souvent célèbres. Quelques excellentes revues dédiées :

Mathematics of Computation (1943) : *articles must be of significant computational interest and contain original and substantial mathematical analysis or development of computational methodology.*

Journal of Automated Reasoning (1983) : *focus on several aspects of automated reasoning, a field whose objective is the design and implementation of a computer program that serves as an assistant in solving problems and in answering questions that require reasoning.*

Experimental Mathematics (1992) : *publishes original papers featuring formal results inspired by experimentation, conjectures suggested by experiments, and data supporting significant hypotheses.*

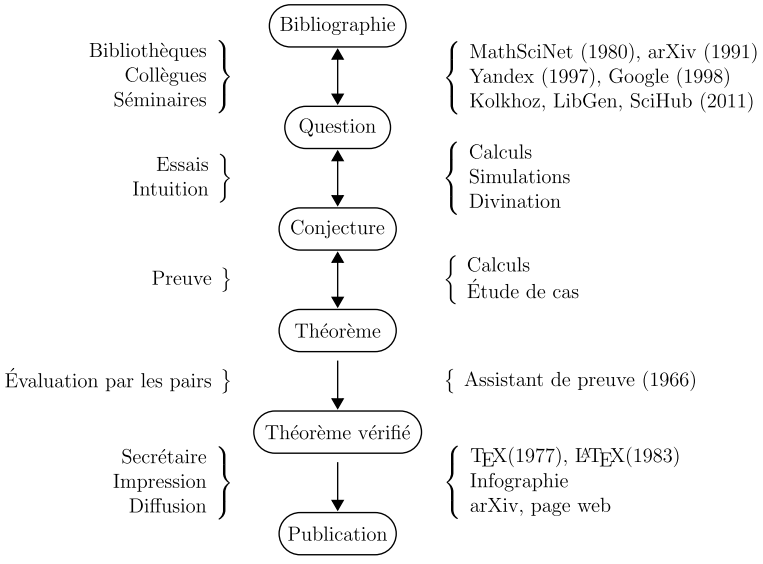

FIGURE 15 – Ce que l'ordinateur change dans la vie du mathématicien.

3.2 Conjecturer sans, prouver avec

Le théorème des quatre couleurs.
Conjecturé en 1852, prouvé en 1976 par une étude de cas sur ordinateur. Réception mitigée : doute sur le fond (erreurs de programmation ?) et rejet de la forme (ce n'est pas une *preuve*, voir paragraphe 3.6). En 1994, nouvelle preuve, due à Robertson & Cie et aussi informatique : ils ont trouvé via 32 règles de déchargement un ensemble inévitable de 933 configurations toutes réductibles (lien). En 2008, encore une preuve, due à Steinberger et toujours informatique : il a trouvé via 42 règles de déchargement un ensemble inévitable de 2832 configurations toutes D-réductibles (plus simple à tester). Les doutes sur le fond sont levés, mais toujours pas de preuve "classique"...

La conjecture de Kepler.
Un *plan compact* est formé de cercles de diamètre 1 disposés sur le réseau triangulaire de côté 1 (les cercles sont donc tangents).

- En 1611, Kepler conjecture que l'empilement le plus dense de sphères dans l'espace est une superposition de plans compacts, chaque sphère venant se loger dans le creux formé par trois sphères du plan dessous.
- En 1773, Lagrange prouve que le plan compact est le plus dense des empilements réguliers.
- En 1831, Gauss prouve la conjecture de Kepler dans le cas des empilements réguliers.
- En 1940, Tóth étend le résultat de Lagrange à tout empilement.
- En 1998, Hales étend le résultat de Gauss à tout empilement.

La preuve de Hales fait un usage très important de l'ordinateur. Un groupe de douze experts [2] l'a vérifiée pendant quatre ans. La partie théorique a finalement été publié dans *Annals of Mathematics*, ce qui a conduit cette revue à adopter une déclaration au sujet des preuves assistées par ordinateur.

Empilements de sphères.
Quid des plus denses empilements de sphères en dimension $d > 3$? Il existe de nombreux encadrements, notamment asymptotiques. Les empilements optimaux *réguliers* sont connus jusqu'à $d = 10$, ainsi que pour $d = 24$. Pour $d = 10$ ou d suffisamment grand, on sait (sans les connaître) que les empilements optimaux ne sont pas réguliers. En 2004, une preuve utilisant l'ordinateur pour vérifier de très nombreux cas a montré que pour $d = 8$ (resp.

2. Chapeauté par Tóth fils !

$d = 24$), sans hypothèse de régularité, l'empilement sur le réseau E_8 (resp. réseau de Leech) était optimal à un facteur au plus $1+10^{-14}$ (resp. $1+10^{-29}$) près. En 2016 est annoncée une preuve "humaine" (avec quand même de bon gros calculs à l'ordinateur à l'intérieur) qu'ils sont en fait optimaux.

3.3 Conjecturer avec, prouver sans

Percolation
Sur la grille $\mathbb{Z}^2$, chaque arête est *ouverte* avec probabilité p, fermée sinon. Il y a *percolation* si la composante connexe (par arêtes ouvertes) qui contient l'origine, C_0, est infinie. Ce modèle fut introduit en 1957, et des simulations conduisirent rapidement à conjecturer qu'il y avait (presque sûrement) percolation pour $p > 1/2$ et pas pour $p < 1/2$. Ce résultat fut démontré en 1982. Plus précisément :

- pour $p < 1/2$ (régime sous-critique) : la probabilité que C_0 soit de taille n décroît exponentiellement avec n (la taille moyenne des composantes connexes est donc finie) ;
- pour $p > 1/2$ (régime sur-critique) : C_0 est (presque sûrement) infinie, unique, et contient une proportion $\Theta(p) > 0$ des points ;
- pour $p = 1/2$ (régime critique) : la probabilité que C_0 soit de taille n décroît en $n^{-5/48}$ (il n'y a donc pas percolation) et la figure est invariante par changement d'échelle (et même invariante conforme).

L'existence d'une *valeur critique* est générale (autres graphes, autres dimensions) mais rarement connue, sans parler de ce qui se passe pour cette valeur.

Percolation amorcée.
Le modèle est proche mais différent. Soit une grille carrée de taille $n \times n$ dont chaque sommet est initialement *infecté* avec une probabilité p. On itère alors un processus de *contagion* : un sommet infecté le reste et un sommet qui a au moins deux voisins infectés le devient à son tour. En 1989, des simulations informatiques poussées jusqu'à $n = 28800$ conduisent à conjecturer que si une proportion $c/\ln(n)$ des sites sont initialement infectés, alors la probabilité que tout le monde devienne infecté tend (avec n) vers 1 si $c > \lambda$ et 0 si $c < \lambda$, où

$$\lambda = 0,245 \pm 0,015.$$

En 2003, Holroyd démontre (à la main)

$$\lambda = \pi^2/18.$$

Problème : $\pi^2/18 = 0.548311\ldots$ Holroyd montre que la convergence est en fait très lente et qu'il aurait fallu pousser les simulations jusqu'à $n = 10^{20}$.

Un jeu apériodique de 11 dominos.
Étant donné un nombre fini de carrés unités au bords colorés, appelés *dominos*, on se demande s'il est possible de *paver* le plan, *i.e.*, le recouvrir par des copies de ces dominos, translatées de sorte à ne pas s'intersecter et telles que deux copies adjacentes le soit tout le long d'une arête de la même couleur. Posé dans les années 60, ce problème s'est avéré indécidable, notamment à cause de l'existence de jeux *apériodiques*, *i.e.*, des ensembles de dominos qui pave le plan mais jamais de manière périodique. Le premier jeu, trouvé en 1966, comportait 104 dominos. Au fil des années des ensembles de plus en plus petits ont été trouvés : 56 dominos en 1969, 16 en 1978, 13 en 1996 et enfin 11 en 2015. Ce dernier jeu a été trouvé par Jeandel et Rao [3] via une recherche intensive sur ordinateur (plusieurs mois de calcul). Le problème de déterminer si un jeu donnée pave étant indécidable, le principe fut de d'abord chercher des *candidats*, *i.e.*, des dominos qui *semblaient* paver (dans la limite de la puissance de calcul disponible) sans qu'on puisse trouver une période, puis d'examiner ces candidats à la main. Ainsi fut trouvé un jeu apériodique de 11 dominos (utilisant 4 couleurs).

3.4 Conjecturer avec, prouver avec

Pas de jeu apériodique avec moins de 11 dominos.
Le jeu apériodique de 11 dominos sur 4 couleurs n'est pas seulement le plus petit connu : c'est le plus petit possible. Parallèlement à leur recherche d'un jeu apériodique, Jeandel et Rao ont effet vérifié que tout jeu avec moins de 11 dominos ou moins de 4 couleurs pavait le plan périodiquement ou ne le pavait pas du tout. Ceci par un programme informatique de recherche exhaustive qui a tourné plusieurs années.

L'attracteur de Lorenz.
En 1963, le météorologue Lorenz étudie numériquement le système dynamique défini, pour des paramètres réels σ, ρ et β donnés, par

$$\dot{x} = \sigma(y - x), \qquad \dot{y} = \rho x - y - xz, \qquad \dot{z} = xy - \beta z.$$

Ses simulations le conduisent à conjecturer pour certains paramètres [3] l'exis-

3. Le célèbre attracteur en forme de papillon correspond à $\sigma = 10$, $\rho = 28$ et $\beta = 8/3$.

tence d'un *attracteur*, *i.e.*, un ensemble A et un voisinage U de A tels que

$$A = \bigcap_{t \geq 0} f_t(U),$$

où f_t est solution du système dynamique précédent. Ses simulations suggèrent également qu'une petite différence sur la position initiale (typiquement, une erreur d'arrondi) conduisent à des trajectoires totalement différentes au bout d'un certain temps. Cette notion de sensibilité aux conditions initiales est à la base de la *théorie du chaos*, qui qualifie d'*étrange* un tel attracteur. Il fallut attendre Tucker en 2002 pour que la réalité de cet attracteur étrange soit prouvée – informatiquement grâce à de l'arithmétique d'intervalle !

3.5 Conjecturer avec, chercher comme on peut

D'autres jeux apériodiques de 11 dominos ?
Si Jeandel et Rao ont pu montrer que 10 dominos ne suffisaient pas et montrer qu'il existait un ensemble de 11 dominos apériodique, ce dernier n'est pas le seul candidat désigné par leurs programmes. Ils ont en effet trouvé 25 autres candidats, dont 2 avec sans doute la même structure, 9 qui ne pavent sans doute pas, et 14 qui restent incompris et pourrait éventuellement conduire à une nouvelle méthode pour définir des jeux apériodiques.

La conjecture de Collatz.
Formulée en 1937 et connue sous différents noms, cette conjecture peut être comprise par un enfant de 8 ans... mais a résisté à tant de mathématiciens qu'elle a fait dire à Erdős que "les mathématiques n'étaient sans doute pas assez mûres" pour la résoudre (il a cependant promis 500$ à qui la résoudrait). Considérons la suite définie pour $n \geq 0$ par

$$u_{n+1} = \begin{cases} 3n+1 & \text{si } n \text{ est impair,} \\ n/2 & \text{sinon.} \end{cases}.$$

La conjecture est que pour tout u_0, il existe n tel que $u_n = 1$. Essayez, par exemple, $u_0 = 27$. Elle est vérifiée jusqu'à $u_0 = 2^{60}$ (mai 2015)...

La conjecture de Birch et Swinnerton-Dyer.
Une *courbe elliptique* rationnelle est une courbe plane E sans point de rebroussement ni point double décrite par une équation à coefficients entiers :

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

L'intérêt est que toute droite qui coupe E en deux points P et Q la coupe en un troisième point R (théorème de Bezout). Ceci permet de définir une *addition* sur les points de E (l'associativité se vérifie par le calcul) :

— 0 est par convention le point à l'infini sur l'axe des ordonnées ;
— le symétrique de R par rapport à l'axe des abscisse est $-R$;
— $P + Q := -R$, en prenant la tangente à E si jamais $P = Q$.

L'ensemble des points rationnels de E forme alors un groupe finiment engendré (théorème de Mordell). Son rang r (cardinal du plus petit ensemble générateur) est appelé *rang de Mordell-Weil* de E. La conjecture de Birch et Swinnerton-Dyer relie le relie au nombre N_p de points sur E réduite modulo p (*i.e.*, coefficients de l'équation et coordonnées des points pris modulo p) :

$$\prod_{\substack{p \text{ premier} \\ p \leq x}} \frac{N_p}{p} \asymp C \log(x)^r.$$

Elle a été conjecturée en 1965 sur la base d'expérimentations numériques et reste toujours ouverte malgré quelques résultats partiels. C'est un des sept *problème du millénaire* (comme $P = NP$).

3.6 Vérifier avec

La preuve du théorème des quatre couleurs a été plutôt froidement accueillie. Non seulement elle n'était pas *vérifiable* à la main par tout un chacun, mais pire : elle n'était pas *explicative*. Sans compter qu'elle était bien loin de figurer dans *Le Livre*[4].

Mais, formellement, une preuve est juste un énoncé obtenu à partir d'axiomes en appliquant des règles de déduction logique. Et s'il n'est pas clair qu'un ordinateur puisse *trouver* une telle preuve (voir paragraphe suivant), il semble par contre tout à fait possible qu'il *vérifie* une preuve formelle proposée par un humain. On parle d'*assistant de preuve*, un concept qui remonte à Automath (de Bruijn) en 1966.

4. Concept mystique dû à Erdős d'un livre qui contiendrait tous les théorèmes avec leur "plus belle" preuve. Le but du mathématicien est d'en découvrir des pages... Malheureusement le ratio des longueurs d'un théorème et de sa plus courte preuve n'est pas uniformément borné, donc certaines pages risquent d'être assez moches...

En outre, on sait depuis les années 60 que les programmes sont des preuves comme les autres (correspondance de Curry-Howard, les types étant des théorèmes). Un assistant de preuve a donc aussi vocation à vérifier des programmes (comme celui utilisé dans la preuve du théorème des quatre couleurs, par exemple).

S'il fallait convaincre de l'utilité de vérifier formellement un programme, on pourrait citer le Vol 501 d'Ariane 5 : le 4 juin 1996, la fusée s'écrase après moins de 40s de vol à cause d'un bête *dépassement d'entier* (370 millions de dollars en fumée, soit 370 prix du millénaire...).

S'il fallait convaincre de l'utilité de vérifier formellement une preuve, on pourrait citer l'histoire de Vladimir Voevodsky, brillant mathématicien russe qui s'est rendu compte quelques temps après avoir reçu la médaille Fields qu'il y avait des fautes dans le travail qu'elle récompensait. Ceci parce que le degré de spécialisation est aujourd'hui tel que la vérification par les pairs atteint ses limites. Voevodsky s'est depuis lors complètement reconverti à la vérification de preuves formelles [5].

Voici deux exemples remarquables combinant vérification de preuve et de programme :

Le théorème des quatre couleurs.
Formalisé en *Coq* en 2005 par Gonthier et Werner.

La conjecture de Kepler.
Formalisée en *HOL-light* en 2014 par Hales et son équipe (projet *Flyspeck*).

Ces preuves ont mobilisé toute une équipe sur plusieurs années, ce qui semble rédhibitoire. Mais c'est aussi parce qu'elles ont nécessité de formaliser une quantité énorme de résultats "classiques", travail qui sera réutilisable. Voici un autre projet toujours en cours :

La classification des groupes finis simples.
Un sous-groupe H de G est *distingué* si

$$\forall g \in G, \qquad gHg^{-1} \subset H.$$

5. Et il ne s'en tire pas trop mal...

Ceci permet de ramener l'étude de G à celle de H et du groupe quotient G/H (les classes d'équivalences modulo H). En particulier, un groupe est *simple* s'il n'a pas d'autre sous-groupe distingué que lui-même et le groupe trivial réduit à l'élément neutre. C'est en quelque sorte une brique de base de la théorie des groupes, comme un nombre premier en théorie des nombres. La classification des groupes finis simples est une tâche qui a occupé une centaine de mathématiciens d'environ 1955 à 2004. La classification finale est répartie en 500 articles totalisant plusieurs milliers de pages [6]. Est-on toujours dans la preuve *vérifiable* et *explicative* ? Une preuve formelle ne serait-elle pas la bienvenue ? Un premier pas dans cette direction a été fait en 2012 :

Le théorème de Feit-Thomson.
Conjecturé en 1911 par Burnside et démontré en 1963 en 250 pages. Une preuve formelle a été obtenue en 2012 par Gonthier et son équipe. Ce théorème stipule que tout groupe fini simple non commutatif est d'ordre (cardinal) pair.

3.7 Et sans mathématicien ?

Si un théorème est juste un énoncé démontré à partir d'axiomes en appliquant des règles de déduction logique, qu'est qui empêche un ordinateur d'explorer l'ensemble (dénombrable) des possibilités ? *A priori* rien... Cependant le nombre de possibilités est exponentiel. Par ailleurs on sait que sauf pour des logiques très simples (sans l'arithmétique de Peano) il y a des théorèmes ni démontrables ni réfutables (Gödel). Certains ont essayé. Quelques théorèmes ont été trouvés (notamment en géométrie plane) ainsi que, par exemple, la conjecture (*i.e.*, l'ordinateur n'a réussi ni à la prouver ni à la réfuter) :

Conjecture 2 (Graffiti.pc, 2007) *Soit G un graphe avec au moins deux sommets qui soit simple, connexe et régulier. Soit d la taille du plus petit ensemble de sommets tel que chaque sommet de G est adjacent à cet ensemble. Soit p la taille de la plus petite partition des sommets de G tel que chaque sous-graphe induit admettent un chemin hamiltonien. Alors $d \geq 2p$.*

Ceci dit les mathématiciens font généralement des théorèmes en cherchant à *comprendre* quelque chose d'autre. Quel serait l'intérêt d'un théorème isolé, rattaché à aucun autre résultat, théorique ou pratique ? L'intuition et le bon sens du mathématicien semble donc pour l'instant irremplaçables...

6. L'ordinateur a été utilisé mais seulement pour découvrir des groupes, notamment les derniers groupes *sporadiques* (qui sont ceux ne faisant pas partie d'une famille infinie).

Références

[1] Robin Wilson, *Four colors suffice*, Princeton University Press, 2002.

[2] Thomas Hales, *Mathematics in the age of the Turing machine*, in Turing's Legacy, Cambridge University Press, 2014, pp. 253–298.

[3] Emmanuel Jeandel et Michael Rao, *An aperiodic set of 11 Wang tiles*, arXiv:1506.06492 (2015)

A Lexique

théorème des quatre couleurs ..... теор**е**ма о четыр**ё**х кр**а**сках
couleur ..... кр**а**ска
rouge, vert, bleu, jaune ..... кр**а**сный, зел**ё**ный, с**и**ний, ж**ё**лтый
pays simplement connexe ..... односв**я**зная стран**а**
ordinateur ..... компь**ю**тер
mathématicien ..... матем**а**тик
proposition, définition ..... ппредлож**е**ние, определ**е**ние
preuve, conjecture ..... доказ**а**тельство, гип**о**теза
colori-er/é/age ..... раскр**а**-сить/шенный/ска
graphe planaire/connexe ..... план**а**рный/св**я**зный граф
sommet, arête, face ..... верш**и**на, ребр**о** (pl. р**ё**бра), грань (f)
degré, sommet de degré x ..... ст**е**пень (f), верш**и**на ст**е**пени x
sommet pendant/voisin ..... вис**я**чая/сос**е**дняя верш**и**на
sommet relié à ..... верш**и**на соединен**а** с
triangulation/carte cubique ..... триангул**я**ция/куб**и**ческая карта
relation d'Euler ..... теор**е**ма **Э**йлера
induction ..... инд**у**кция
carré, pentagone, hexagone ..... квадр**а**т, пятиуг**о**льник, шестиуг**о**льник
réductible, réductibilité ..... приводимый, приводимость
configuration ..... конфигур**а**ция
recolorier ..... перекр**а**сить
boucle, chaîne ..... п**е**тля, путь
bord, intérieur ..... гран**и**ца, вн**у**тренность
inévitable, inévitabilité ..... неизб**е**жный, неизб**е**жность
déchargement ..... разгр**у**зка
heuristique ..... эвр**и**стика

problème des trois couleurs ..... пробл**е**ма о трёх кр**а**сках
algorithme ..... алгор**и**тм
recette de cuisine ..... кулин**а**рный рец**е**пт
temps d'exécution ..... объ**ё**м (вр**е**мя) раб**о**ты
complexité algorithmique ..... вычисл**и**тельная сл**о**жность
tri par insertion, fusion ..... сортир**о**вка вст**а**вками, сли**я**нием
polynomial, exponentiel ..... п**о**линоми**а**льный, экспоненци**а**льный
NP-complet, NP-complétude ..... NP-п**о**лная, NP-полнат**а**
force brute ..... п**о**лный переб**о**р

problème de décision ..... проблема разрешимости
instance ..... входные данные
réduire à, réduction ..... свести к, редукция
(non) déterministe ..... (не)детерминированный
machine de Turing ..... машина Тьюринга
ruban, tête, alphabet, lettre ..... лента, головка, алфавит, символ
état initial/final ..... начальное/терминальное состояние
règle de transition ..... правило перехода
proposition ..... пропозициональная формула
logique propositionnelle ..... пропозициональная логика
variable, littéral ..... переменная, литерал
implication, négation ..... импликация, отрицание
conjonction, disjonction ..... конъюнкция, дизъюнкция
satisfaire, satisfiabilité ..... выполнить, выполнимость
forme normale conjonctive ..... конъюнктивная нормальная форма
distributivité ..... дистрибутивность
lois de De Morgan ..... законы де Моргана
gadget ..... виджет, штук
circuit électrique ..... электрическая цепь

journal scientifique ..... научный журнал
évaluation par les pairs ..... рецензирование
infographie, visualisation ..... визуализация
calcul, simulations ..... вычисление, компьютерное моделирование
assistant de preuve ..... программное средство доказательства теорем
conjecturer, prouver ..... сформулировать гипотезу, доказать
régulier, réseau ..... регулярный, решётка
percolation ..... перколяция
composante connexe, cluster ..... компонента связности, кластер
valeur critique ..... критическое значение
percolation amorcée ..... бутстрапная перколяция
être infecter, contaminer ..... болеть, заразить
valeur approchée ..... приближённое значение
apériodique ..... непериодический
paver, pavage ..... замостить, замощение
trou/superposition ..... дырка/перекрытие
candidat ..... кандидат
attracteur de Lorenz ..... аттрактор Лоренца

attracteur étrange ..... стр**а**нный аттр**а**ктор
système dynamique ..... динам**и**ческая сист**е**ма
sensibil. aux cond. init. ..... чувств**и**тельность к нач**а**льными усл**о**виями
théorie du chaos ..... те**о**рия х**а**оса
arithmétique d'intervalles ..... интерв**а**льная арифм**е**тика
courbe elliptique rationnelle ..... рациональная эллипт**и**ческая крив**а**я
point de rebroussement/double .... касп, точка возврата / двойная точка
groupe finiment engendré ..... конечно порожденная группа
rang, cardinal ..... м**о**щность мн**о**жества
modulo, produit ..... по м**о**дулю, умнож**е**ние
vérification ..... верифик**а**ция/пров**е**рка
expliquer ..... объясн**и**ть
axiome, règles de déduction ..... акси**о**ма
preuve formelle ..... формальное доказ**а**тельство
dépassement d'entier ..... ц**е**лоч**и**сленное переполн**е**ние
classif. gr. finis simples ..... классифик**а**ция простых конечных групп
sous-groupe distingué ..... норм**а**льная подгр**у**ппа
conjugaison ..... сопряж**е**ние
groupe quotient ..... факторгр**у**ппа
groupe simple ..... прост**а**я гр**у**ппа
élément neutre ..... нейтр**а**льный элем**е**нт
classification ..... классифик**а**ция
commutatif ..... коммутат**и**вный
Th. incomplétude Gödel ..... Т. Гёделя о неполноте