

# Le charme *discret* des mathématiques

András SEBŐ\*

Après une brève introduction aux mathématiques discrètes, le lecteur sera invité à suivre la solution simple mais surprenante d'un problème issu des télécommunications qui est resté ouvert pendant plus de vingt ans, et qui l'amènera peut-être à saisir certaines idées discrètes. D'autres exemples confirmeront que les mathématiques discrètes sont ancrées à la fois dans les mathématiques et les applications contemporaines. Nous espérons que les preuves incluses illustreront comment cette jeune discipline se forge ses propres méthodes pour servir à la fois la Beauté et l'Utilité.

## Le monde est-il discret ?

« Discret » est ici le contraire de continu. C'est à peu près tout ce qu'on peut dire du terme lui-même. Avouons-le, ce mot ne correspond à aucune notion mathématique précise. Les nombres réels forment un ensemble « continu ». Les entiers, bien qu'infinis, sont *discrets*, c'est à dire « loins » les uns des autres.

Et le monde, est-il discret ? Oui ! Depuis que l'on sait que la matière est faite d'un nombre fini d'atomes (discrets) . . . Et les mouvements continus peuvent être remplacés par de très petits mouvements discrets . . .

N'est-il pas étonnant, quand on est écolier, que même l'eau soit constituée d'un nombre fini d'atomes ? Et pourtant, la plupart des théories mathématiques classiques traitent seulement « le continu », et sont souvent vues comme les sciences de l'infini. Les mathématiques discrètes veulent traiter de ce qui est discret (fini ?), mais trop complexe pour être traité « à la main », sans outils mathématiques.

On peut arriver au discret par l'approximation du continu d'une part. Mais la science moderne, et en particulier l'industrie automatisée, l'informatique, l'économie etc., produisent des problèmes qui sont dès le départ « discrets ».

Les problèmes à caractère discret peuvent souvent se modéliser d'une manière naturelle en terme de graphes. Mathématiques discrètes, théorie des graphes, ou combinatoire sont des synonymes pour certains, couvrent des notions différentes d'après d'autres, mais la partie commune de ces domaines est certainement très grande : peut-on rédiger un problème combinatoire qui ne peut pas être reformulé en termes de graphes ? Il est vrai aussi qu'il existe des méthodes plus « graphiques » que d'autres.

Rappelons tout d'abord qu'un graphe est une paire d'ensembles  $G = (V, E)$  où  $V$  est un ensemble quelconque, et  $E$  est un sous-ensemble des paires d'éléments de  $V$ . Les éléments de  $V$  s'appellent les *sommets* du graphe et les éléments de  $E$  s'appellent *arêtes*. On dira aussi que  $\{u, v\} \in E$  est une arête *entre*  $u$  et  $v$  : on peut représenter les sommets d'un graphe par des points et ses arêtes par des lignes qui les relie. Deux sommets  $u, v \in V$  sont *voisins* si  $\{u, v\} \in E$ .

Voyons maintenant, à titre d'exemple, un des problèmes les plus classiques : le couplage. Il s'agit de marier (coupler) un nombre maximum de filles et de garçons en respectant leurs sympathies mutuelles, données à l'avance sous

---

\* Laboratoire Leibniz, UMR 5522 CNRS, 46 Avenue Félix Viallet, 38000 Grenoble.  
Andras.Sebo@imag.fr

forme d'un graphe. Quelles peuvent être les raisons pour lesquelles on ne peut pas marier plus de 184 filles lorsqu'il y en a 276 en tout ? Autrement dit, pourquoi peut-on être obligé de renoncer au mariage de 92 filles ? Une des raisons possibles : un sous-ensemble de filles rassemblant par exemple 231 d'entre elles, ne sympathisent en tout qu'avec 139 garçons. Déjà dans un tel sous-ensemble de filles, il y en aura au moins 92 qui ne seront pas mariées !

Appelons *déficit* d'un ensemble de filles la différence entre le nombre de ses éléments et le nombre de ses sympathisants (92 dans l'exemple) ; si ce nombre est négatif, le déficit est défini comme étant 0. Le déficit pourrait être considéré comme une mesure de « difficulté » d'une communauté de filles à se marier.

*A priori*, on pourrait imaginer qu'il y a d'autres raisons que le déficit pour empêcher le mariage des filles. La clef de ce problème est l'un des premiers résultats de la théorie des graphes, et son message est qu'il n'y a pas d'autre raison !

**Théorème 1 [König-Hall, 1931].** *Le nombre minimum de filles non-mariées est égal au maximum du déficit des sous-ensembles de filles.*

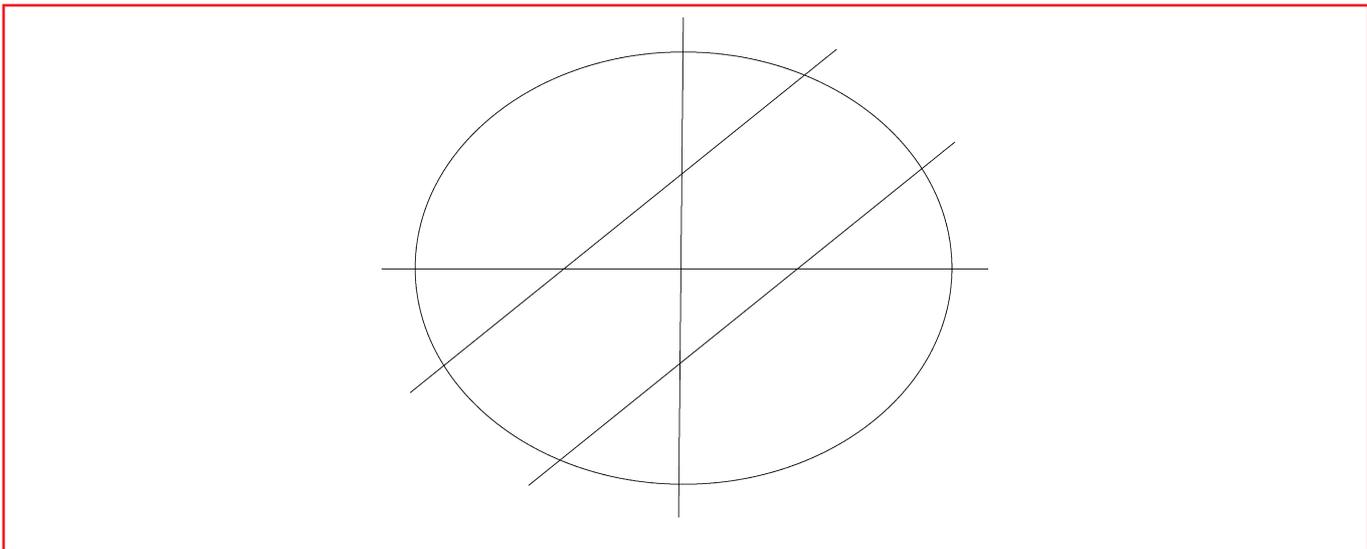
Grâce à ce théorème, on peut facilement certifier à quelqu'un qu'un couplage est le plus grand possible : on lui montre un sous-ensemble de filles dont le déficit est égal au nombre de filles non mariées.

D'après Edmonds, l'existence d'un certificat d'optimalité est un bon indice pour que l'optimalité puisse être décidée d'une manière efficace. Malgré ce pari – dont la formulation précise est «  $NP \cap coNP = P ?$  », similaire à la célèbre question «  $P = NP ?$  » –, certains résultats laissent à penser que *trouver* pourrait être plus difficile que certifier. Par exemple, écrire un entier positif donné comme produit de deux entiers supérieurs à 1 pourrait s'avérer plus difficile que certifier l'existence d'une telle décomposition. En ce qui concerne les couplages max, on peut décider s'ils existent ou non, et on peut même les trouver. Ce théorème et l'algorithme efficace qui le montre (la « méthode hongroise », en train de fêter son 50.-ème anniversaire<sup>1</sup>, s'exécute en temps « polynomial », voir LL, AS) fournissent à la fois le couplage optimal et un ensemble de filles de déficit maximum.

Le problème des mariages, ou couplages, est l'un des problèmes de base de la théorie des graphes, dont les variantes, spécialisations ou généralisations apparaissent partout en recherche opérationnelle et dans de nombreuses autres disciplines. Voici par exemple comment les couplages apparaissent dans un problème « d'ordonnancement de tâches » classique :

Etant données  $n$  tâches devant être exécutées sur deux machines identiques, déterminer le temps d'exécution minimum, si

- l'exécution de chaque tâche demande une minute ;
- des « contraintes de précédence » sont données entre les tâches.



**Figure 1** – VLSI, lignes aériens, etc.

1. [www.cs.elte.hu/HungarianMethod50](http://www.cs.elte.hu/HungarianMethod50).

Est-ce que des chemins de précédence entre deux tâches forment le seul obstacle, c'est-à-dire la seule raison de ne pas pouvoir exécuter les tâches en moins de temps ?

On peut essayer de coupler le plus possible de tâches exécutables en même temps. Autrement dit « marier » les tâches, mais c'est un peu plus difficile, car on n'a pas une division naturelle en deux ensembles, « garçons » et « filles ». Le maximum  $k$  de paires de tâches exécutables en même temps peut quand même être déterminé (algorithme d'Edmonds). Comme on ne peut pas exécuter plus de 2 tâches en même temps on peut être sûr qu'au moins  $n - k$  minutes sont nécessaires pour exécuter toutes les tâches. Miracle : il est vrai aussi (montré par Fujii, Kasami, Ninomiya en 1969), que  $n - k$  minutes suffisent ! Pour trois machines déjà, ce problème est ouvert.

Encore quelques exemples – qui mènent d'une manière moins évidente aux couplages – juste pour montrer comment l'abstraction mathématique unifie des modèles qui ont l'air d'être très différents à un plus bas niveau. Les lignes (4 lignes droites et une circulaire) que vous voyez sur la Figure 1 peuvent représenter des connexions électriques. Le dessin doit être réalisé avec des fils électriques (en métal) en utilisant les deux côtés d'une plaque (chaque point sur exactement un des deux côtés). On doit faire attention à une et une seule chose : deux lignes ne peuvent pas se toucher, c'est-à-dire que deux fils qui se croisent doivent être sur des côtés différents de la plaque au point d'intersection.

Pour bien arranger correctement les lignes, on peut creuser des trous dans la plaque, et faire passer les fils d'un côté à l'autre, mais bien sûr, pas dans les croisements, car ceci causerait des faux contacts. Il est facile de voir, qu'on peut toujours réaliser un plan de connexion sans croisements en faisant suffisamment de trous. Mais les trous ne sont pas gratuits à faire, et rendent le système plus compliqué . . . Comment trouver le nombre minimum de trous ?

Les lignes peuvent aussi représenter des trajectoires d'avion qui doivent toujours voler à l'un des niveaux possibles parmi deux, leurs itinéraires ne pouvant pas se croiser (pas même à des temps différents). On doit alors minimiser le nombre de changements de niveaux (qui sont coûteux, inconfortables pour les passagers, dangereux pour la marchandise . . .).

Cette même Figure 1 peut encore être interprétée de multiples façons. Toute discipline mathématique essaiera de trouver des modèles généraux qui synthétisent les méthodes et regroupent les problèmes autour de ces méthodes. Les interprétations de la Figure 1 se rejoignent à un niveau plus général : ce sont des cas particuliers du problème de coupe maximum (coupe max) dans un graphe planaire, qui se résout avec des méthodes de la « théorie des couplages ».

« L'univers discret » est structuré, et les mathématiciens ont bien avancé dans la hiérarchie et les interrelations des classes de problèmes. Les résultats théoriques peuvent devenir de bons conseillers pratiques : ils arrivent souvent à cerner où se situent de nouveaux problèmes dans cette jungle ; ce faisant ils orientent les chercheurs vers des méthodes appropriées.

Notre pari est maintenant d'expliquer la solution complète d'un problème difficile.

## La pluie

Que peut-on demander à des enveloppes mouillées ? Peut-on éviter, sinon avec des parapluies, que l'information qu'elles contiennent ne soit perdue ?

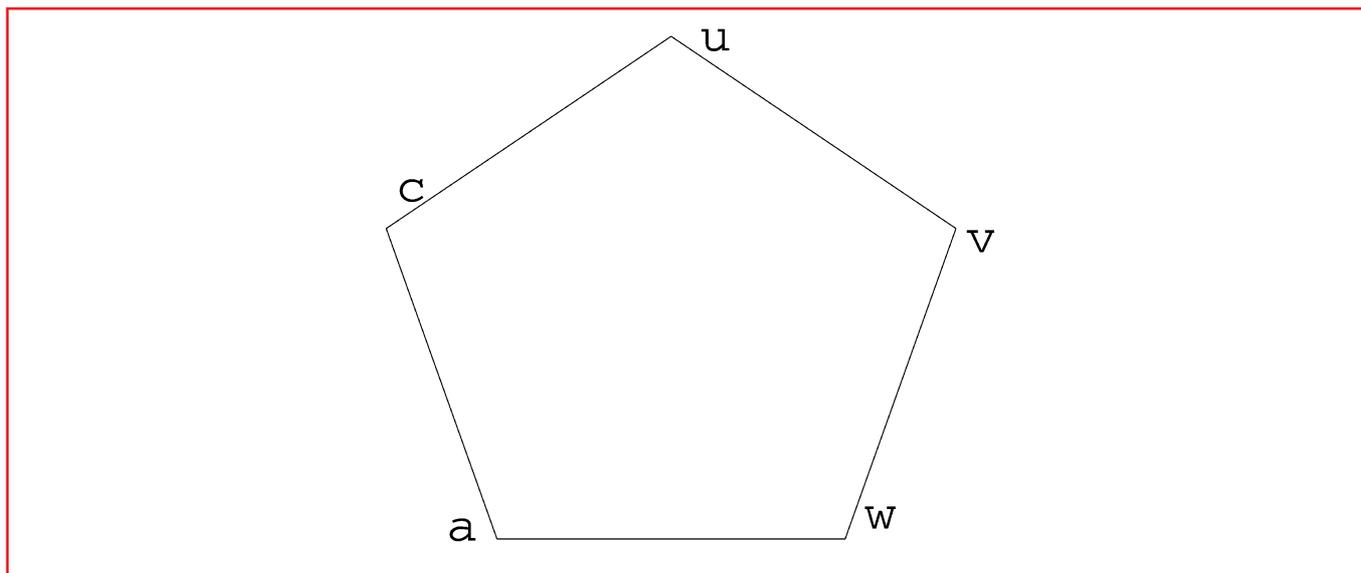
Il s'agit du problème de Shannon : trouver un code pour transmettre des messages sans ambiguïté, bien que certaines paires de lettres puissent être confondues.

Imaginez que vous deviez envoyer un message par l'intermédiaire d'un médium qui connaît seulement les lettres («  $a$  », «  $c$  », «  $u$  », «  $v$  », «  $w$  »). Quand les enveloppes sont mouillées, chaque lettre peut être confondue avec son prédécesseur et successeur dans cet ordre cyclique (le  $a$  avec le  $c$  et le  $w$ , le  $c$  avec le  $a$  et le  $u$ , etc.). Que devraient faire les facteurs sous la pluie ?

Juste ouvrir leur parapluie !

Les paires de lettres qu'on peut confondre sont représentées par les arêtes d'un graphe (Figure 2), qu'on va appeler *graphe des confusions*.

On supposera qu'on envoie des messages ayant tous la même longueur  $k$  fixée (nombre de caractères). Si par exemple «  $a$  » est l'espace, on peut toujours compléter à  $k$  caractères les messages plus courts. Deux messages peuvent être confondus, si toutes les paires de lettres qui sont à la même position dans les deux se confondent. On ne peut pas les confondre, *s'il existe deux lettres aux mêmes positions qui ne peuvent pas être confondues*.



**Figure 2** – Graphe de confusion  $C_5$ .

Si l'on pouvait confondre toutes les lettres les unes avec les autres, alors on ne pourrait pas envoyer plus d'un seul message quelle que soit sa longueur fixée. Ce ne serait même pas la peine de l'envoyer ! La « capacité de Shannon » vaudra 0. Quand on aura deux lettres qu'on ne peut pas confondre elle vaudra 1. Dans un alphabet de 32 lettres (comme l'alphabet hongrois) si aucune paire ne peut jamais être confondue (le graphe des confusions n'a pas d'arêtes), la « capacité de Shannon » vaudra 5. Ceci voudra dire que cet alphabet a la même capacité que les mots binaires de longueur 5. Pour coder  $n$  messages différents avec des mots binaires de longueur  $k$ , il faut avoir  $2^k \geq n$ , c'est-à-dire  $k \geq \log_2 n$ . En général, quand le graphe  $G$  des confusions est donné, la capacité de Shannon<sup>2</sup> va mesurer le nombre de caractères binaires (bits) équivalents à un de nos caractères ; autrement dit, c'est la longueur du mot binaire équivalent, divisé par la longueur de notre mot. La définition formelle :

La *capacité de Shannon*  $cs(G)$  d'un graphe  $G$  est définie comme la limite ( $k$  tend vers l'infini) du *logarithme en base de 2 du nombre maximum de messages de longueur  $k$  qu'on peut envoyer sans confusions, divisé par  $k$* . La limite existe, car la série est (essentiellement) non-décroissante et bornée.

Dans notre premier exemple (Figure 2) le nombre de messages différents de longueur 1 parmi lesquels il n'y a pas de confusion est 2. Comme si on avait l'alphabet binaire à deux lettres, 0 et 1, sans confusion. Un « bit utile » par lettre. Mais on peut faire mieux avec des mots de deux lettres : en les représentant par un tableau  $5 \times 5$  (Figure 3) on peut confondre deux mots si et seulement si leur représentation sur cet échiquier torique  $5 \times 5$  est voisine par un côté ou par une diagonale. (La première et la dernière lignes sont voisines, idem pour les colonnes.)

Peut-on faire encore mieux (en moyenne) en augmentant la longueur des mots ? C'était la question posée par Shannon dans un article de 1956. Il a fallu attendre vingt deux ans, jusqu'en 1978 pour une réponse. (Par Lovász, [RR]). La question a beaucoup contribué au développement d'une portion très riche de la théorie des graphes.

## Le parapluie

En d'autres termes, les deux lettres – par exemple  $a$  et  $v$  – qu'on ne peut pas confondre nous donnent  $2^k$  mots de longueur  $k$  sans aucun risque de confusion, ce qui nous offre seulement 1 bit utile par lettre. D'après Figure 3 on a mieux :  $5^k$  mots de longueur  $2k$  (à la place de  $4^k$ ). En effet, pour  $k = 1$  on a 5 mots (de longueur  $2k$ ), et avec  $k$  répétitions on aura  $5^k$  mots de longueur  $2k$ , ce qui équivaut à un message binaire de longueur  $k \log_2 5$ . En moyenne une de nos lettres équivaudra donc à  $1/2 \log_2 5 > 1$  lettres binaires (bits) ! Si on démontre qu'on ne peut pas faire mieux on aura :

2. La définition habituelle appelle « capacité de Shannon »  $2^x$  où  $x$  est la capacité de Shannon d'après notre définition. Nous nous permettons cet abus ici car nous trouvons que cette terminologie plus logique rend les explications plus agréables.

**Théorème 2 [Lovász, 1978].**  $cs(C_5) = 1/2 \log_2 5$ .

La méthode utilisée par Lovász a été à l'origine de méthodes fondamentales en optimisation combinatoire, et a eu des rebondissements récents. C'était la première application importante de la « programmation semidéfinie » en combinatoire :

La *représentation orthonormale* des sommets d'un graphe  $G$ , est une affectation de vecteurs unité de dimension  $d$  ( $d$  arbitraire) aux sommets, de façon à ce que pour toute paire de sommets non-adjacents de  $G$ , les vecteurs correspondants aux deux sommets soient perpendiculaires (produit scalaire égal à 0). On dit d'un sous-ensemble  $S \subseteq V(G)$  des sommets d'un graphe qu'il est *stable*, si aucune paire d'éléments de  $S$  n'est une arête ;  $\alpha(G)$  est la cardinalité d'un stable maximum de  $G$ .

**Lemme 1.** *Etant donnée une représentation orthonormale  $r : V(G) \rightarrow \mathbb{R}^d$  ( $r = (r_1, \dots, r_d)$ ) d'un graphe  $G$  (où  $d$  est un entier quelconque), on a pour tout stable  $S \subseteq V(G)$  :*

$$\sum_{s \in S} r_1^2(s) \leq 1$$

En effet, les vecteurs associés aux sommets de  $S$  sont orthonormaux, donc on peut les compléter en une base orthonormale.

Dans cette base orthonormale, la somme des carrés des  $i$ -ièmes coordonnées des vecteurs pour tout  $i = 1, \dots, d$  est égal à 1 (la transposée d'une matrice orthonormale est aussi orthonormale). Si on restreint la somme à  $S$  on a l'inégalité voulue.

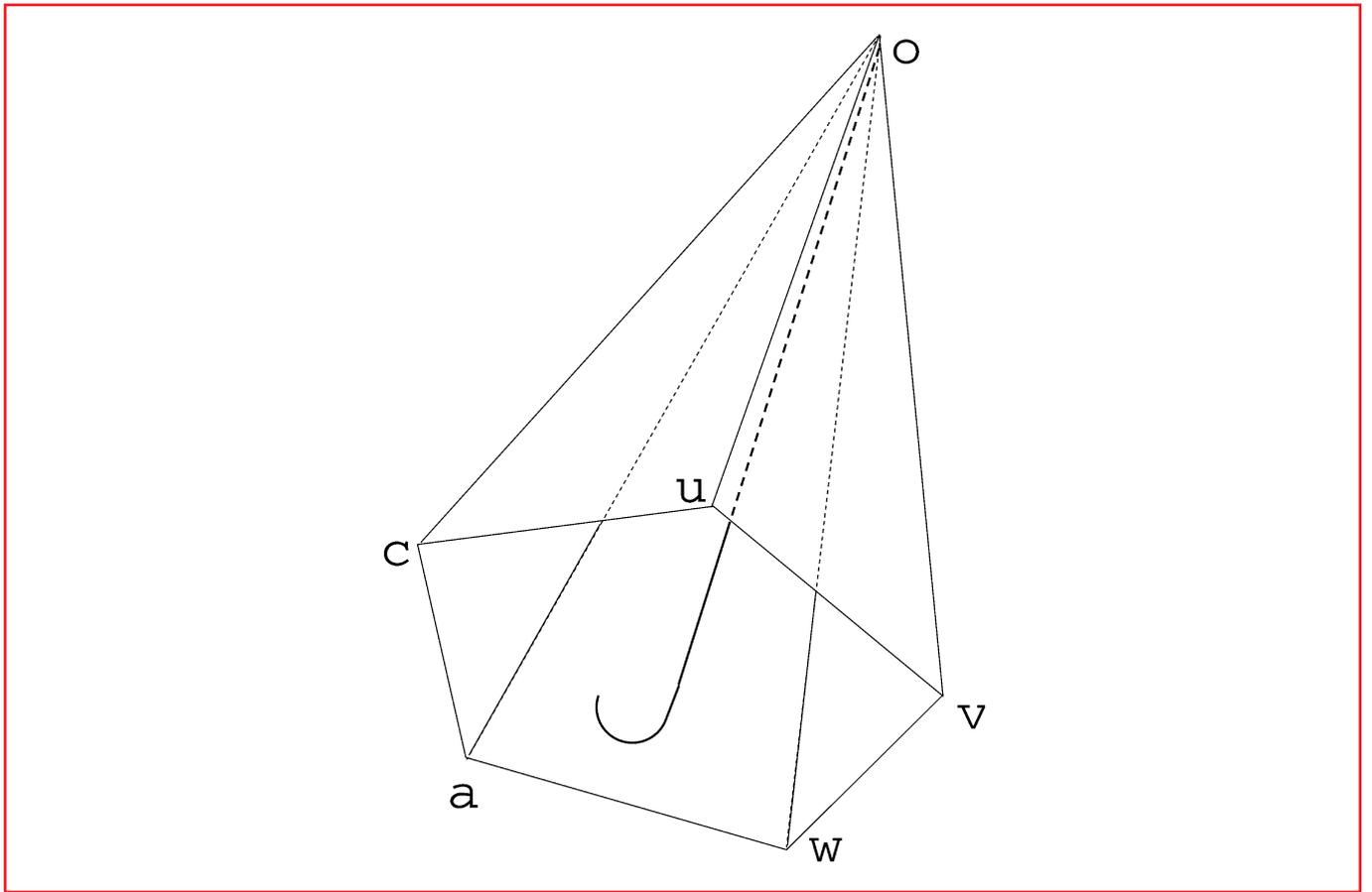
La Figure 4 montre la représentation 3-dimensionnelle de  $C_5$  qui s'avérera optimale pour le Lemme.

Le parapluie du dessin est ouvert de façon à ce que les paires de baleines non-voisines soient perpendiculaires. Le lecteur se convaincra facilement que ceci est possible. On choisit la longueur des cinq arêtes égale à 1 chacun. Il est clair, que les 5 vecteurs  $oc$ ,  $ou$ ,  $ov$ ,  $ow$ ,  $oa$  fournissent une représentation orthonormale de  $C_5$ .

En substituant le résultat de l'encadré dans le lemme, on obtient que la somme sur un stable quelconque de  $C_5$  de la fonction constante  $1/\sqrt{5}$  est inférieure ou égale à 1, et par conséquent,  $\alpha(C_5) \leq \sqrt{5}$ .

	a	c	u	v	w
a	•				
c			•		
u					•
v		•			
w				•	

**Figure 3** – Cinq mots de deux lettres qu'on ne peut pas confondre.



**Figure 4** – *Le parapluie magique de Lovász.*

Pourquoi avoir travaillé tant pour aussi peu ? On sait très bien, que dans cette inégalité là, on pourrait remplacer  $\sqrt{5}$  par 2 ! Parce que cette borne, même si inexacte pour 2, s'étendra facilement à des messages *arbitrairement longs*, et il se trouve qu'elle donnera la meilleure borne supérieure pour la moyenne du nombre de bits !

Définissons le graphe  $G^k$  dont les sommets sont les mots de longueur  $k$  construits à partir des sommets du graphe des confusions  $G$ , et avec une arête entre deux mots si on peut les confondre. Les stables de ce graphe sont donc les ensembles de  $k$ -tuples qui ne peuvent pas être confondus. On va utiliser le lemme pour démontrer que

$$\alpha(C_5^{2k}) \leq 5^k \quad (*)$$

et ceci finit évidemment la preuve du théorème. On va définir une représentation orthonormale de  $C_5^k$  pour tout  $k$ . On en a déjà une pour  $C_5$ , et pour passer de  $C_5^k$  à  $C_5^{k+1}$ , on va appliquer la méthode suivante :

Si on a déjà une représentation de  $G^r$  et  $G^s$ , on représentera l'ensemble de leurs concaténations (les mots qu'on obtient en mettant l'un à côté de l'autre) – exactement  $G^{r+s}$  –, par le produit tensoriel des vecteurs associés. Le produit tensoriel  $x \otimes y$  de  $x \in \mathbb{R}^r$ ,  $y \in \mathbb{R}^s$  n'est rien d'autre qu'une table de multiplication  $r \times s$  : une matrice  $r \times s$  dont l'élément  $ij$  est  $x_i y_j$ , et que l'on regarde comme un vecteur, pour que par exemple le produit scalaire de deux produits tensoriels soit bien défini (comme la somme des produits des éléments correspondants).

Alors l'équation élémentaire

$$(x \otimes y)^T (w \otimes z) = (x^T w)(y^T z).$$

est vraie pour tout  $x, w \in \mathbb{R}^r$ ,  $y, z \in \mathbb{R}^s$ . En effet, les deux côtés somment tous les termes de la forme  $x_i y_j w_i z_j$   $i = 1, \dots, r, j = 1, \dots, s$ .

**Encadré 1**

**Calcul pour le parapluie**

Calculons la représentation orthonormale de  $C_5$  (Figure 4), pour la substituer dans le Lemme, afin d'obtenir la borne supérieure de la capacité de Shannon d'une manière élémentaire.

On fait ce calcul de lycée (il y a plus court, mais y a-t-il plus élémentaire) pour aller au bout de l'expérience : un calcul élémentaire avec un petit peu d'algèbre linéaire et de réflexion combinatoire peuvent collaborer d'une manière originale dans la solution d'un problème difficile ! Faites vérifier les calculs par vos enfants lycéens !

On effectue d'abord des calculs sur le pentagone régulier dont le côté est de longueur 1.

Le losange en gras de la Figure 5 a.) nous permet de trouver la longueur de la diagonale qui vaut  $1 + x$  où  $x$  vérifie l'équation en dessous de la figure, d'où  $x = \frac{-1 + \sqrt{5}}{2}$  ; la longueur de la diagonale est donc  $\frac{1 + \sqrt{5}}{2}$ , et on va noter la

longueur de la demi-diagonale par  $d = \frac{1 + \sqrt{5}}{4}$ . La Figure 5 b.) montre que le rayon  $r$  peut aussi être calculé en appliquant à nouveau le théorème de Pythagore :  $m = \sqrt{1 - d^2} = 1/4\sqrt{10 - 2\sqrt{5}}$ . Donc  $r = 1/(2m) = \frac{2}{\sqrt{10 - 2\sqrt{5}}} =$

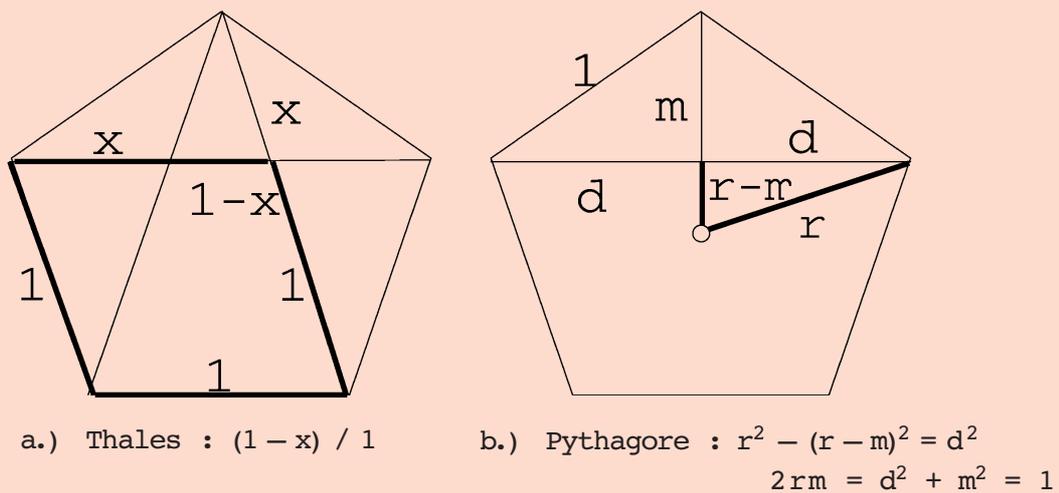
$$\frac{\sqrt{2}}{\sqrt{\sqrt{5}\sqrt{\sqrt{5}-1}}}$$

Et maintenant passons au parapluie dont les baleines sont de longueur 1, et qui est ouvert de façon à ce que chaque paire de baleines non-voisines forment un angle droit. Ces deux baleines forment alors un triangle rectangle isocèle dont les deux côtés perpendiculaires sont de longueur 1. La longueur de la diagonale du pentagone régulier formé par les extrémités des arêtes à l'ouverture appropriée du parapluie est donc de  $\sqrt{2}$  au lieu de  $2d$  et le rayon du cercle circonscrit de ce pentagone régulier est de  $\sqrt{2}/(2d)$  fois la valeur

$\frac{\sqrt{2}}{\sqrt{\sqrt{5}\sqrt{\sqrt{5}-1}}}$  du rayon calculé pour le pentagone régulier

de la Figure 5 a.) :  $\frac{\sqrt{\sqrt{5}-1}}{\sqrt{\sqrt{5}}}$ .

On obtient donc, par une application de plus du théorème de Pythagore, que la projection orthogonale des baleines du parapluie sur le manche est de longueur  $1/\sqrt{\sqrt{5}}$ . Si on choisit alors cet axe comme « axe  $x$  », la première coordonnée de toutes les arêtes est  $1/\sqrt{\sqrt{5}}$ .



**Figure 5** – Calculs sur  $C_5$ .

Cette équation exprime exactement ce qui nous manque : si on a une représentation orthonormale de  $G^r$  et de  $G^s$  et qu'on représente la concaténation de deux vecteurs par le produit tensoriel de leur représentation, alors on obtient une représentation orthonormale de  $G^{r+s}$  !

Nous avons vu (encadré) une représentation orthonormale de  $C_5$ , où la première coordonnée de chaque représentant est  $1/\sqrt{\sqrt{5}}$ . Donc pour tous les vecteurs de la représentation de  $G = C_5^k$  obtenue par produit tensoriel on a  $r_1^2 = (1/\sqrt{5})^k$ . En substituant ce résultat dans le lemme, on obtient que le nombre maximum de mots de longueur  $k$  qu'on ne peut pas confondre est inférieur ou égal à  $(\sqrt{5})^k$ , c'est à dire pour  $2k$  la borne est  $5^k$ , d'où (\*). La conjecture de Shannon qui a été une cible bien connue des chercheurs pendant 22 ans, est démontré !

## La perfection et au-delà

Bien avant que la capacité de Shannon de  $C_5$  ait pu être calculée, le problème posé par Shannon a stimulé un chapitre de la théorie des graphes qui a été pendant longtemps l'un de ses moteurs et a eu un rayonnement bien au-delà. Ce chapitre est celui des *graphes parfaits*, définis par Claude Berge, qui a aussi énoncé deux conjectures devenues célèbres les concernant, sous les noms de conjecture faible et forte des graphes parfaits. (Voir les notes historiques de Berge, dans son dernier article [RR].)

Un ensemble de sommets mutuellement non-voisins d'un graphe est dit *stable* ; un ensemble de sommets mutuellement voisins est un graphe *complet*. Nous avons vu que  $\alpha(G^k) \geq (\alpha(G))^k$ . Rappelons la source de difficulté exprimée par  $\alpha(C_5) = 2$ ,  $\alpha(C_5^2) = 5 > 2^2$ .

Quels sont les graphes pour lesquels ce phénomène ne se présente pas, c'est-à-dire  $\alpha(G^k) = (\alpha(G))^k$  ? Pour ceux-là la capacité de Shannon est égal au nombre de stabilité. Nous laissons au lecteur le plaisir de montrer que  $\alpha(G) = \chi(\bar{G})$  est une condition suffisante pour avoir cette propriété. On note par  $\bar{G}$  le *complémentaire* d'un graphe  $G$ , c'est-à-dire le graphe dont les sommets  $u$  et  $v$  sont voisins si et seulement si ils ne sont pas voisins dans le graphe original ;  $\chi(G)$  est le *nombre chromatique* de  $G$ , c'est-à-dire le nombre minimum de classes d'une partition des sommets en stables.

On a vu que  $C_5$  n'a pas cette propriété. Il est facile de voir que les graphes « cycles impairs » et leurs complémentaires ne l'ont pas non plus. La conjecture célèbre de Berge [LL], [RR], [AS] énonce : *si à partir d'un graphe  $G$  on ne peut pas arriver à un de ces graphes en supprimant des sommets (et toutes les arêtes qui les contiennent), alors  $\alpha(G) = \chi(\bar{G})$* . Une variante plus faible a été démontré par Lovász en 1972, et cette conjecture « forte » par Chudnovsky, Robertson, Seymour et Thomas en 2002. Colorier les sommets d'un graphe, ou reconnaître une sous-classe par un algorithme efficace (polynomial) reste un problème utile et intéressant : les recherches sur les graphes parfaits et leurs sous-classes gardent encore beaucoup de secrets [RR], dont Chudnovsky et Seymour ou Maffray et Trotignon continuent à révéler certains, même après la grande percée que représente le théorème fort. Un grand problème reste ouvert : pour les graphes parfaits le stable max, le nombre chromatique (et par conséquent la capacité de Shannon) se laissent calculer en temps polynomial en utilisant la programmation semidéfinie (faisant appel à la méthode des ellipsoïdes) mais il n'y a pas d'algorithme combinatoire !

Et qu'y a-t-il au-delà de la perfection ? L'imperfection ! Les graphes imparfaits ont été étudiés en grande partie pour résoudre la conjecture de Berge [RR], mais la preuve utilise peu ces résultats.

Cependant le monde discret n'est pas toujours complètement lisse, et il faut faire avec. On peut souvent remédier à l'imperfection – dans un sens plus général avec des méthodes non moins profondes.

Le problème du partitionnement des sommets d'un graphe en deux parties,  $A$  et  $B$ , de façon à maximiser le nombre, ou plus généralement la somme des poids, des arêtes qui sont « à cheval » entre les deux parties, est un des problèmes les plus utilisés de la théorie des graphes. On l'appelle *coupe max*. C'est un problème difficile (NP-difficile) et donc on ne peut pas espérer le résoudre « parfaitement ». Par une idée extrêmement originale de Goemans et Williamson, ce problème admet une solution « imparfaite », mais intéressante, et similaire aux parapluies. Nous allons l'esquisser pour montrer comment des idées similaires apparaissent dans des situations différentes.

Etant donnés des poids  $w_{ij}$  ( $i, j = 1, \dots, n$ ) sur les paires de sommets d'un graphe (qu'on peut supposer être complet, c'est-à-dire toutes les paires de sommets sont des arêtes) on peut résoudre le problème de représenter les points sur la sphère de dimension  $n$  et maximiser

$$\sum_{i < j = 1}^n \text{dist}(x_i, x_j)^2 w_{ij}, \tag{*}$$

où  $x_i, x_j$  représentent les sommets  $i, j$ , et  $\text{dist}(a, b)$  est la distance euclidienne entre  $a$  et  $b$ .

Ceci est un « programme semidéfini ». Le lecteur intéressé par l'algèbre linéaire pourra facilement démontrer que ce problème d'optimisation est équivalent à déterminer la matrice symétrique semidéfinie  $X_{n \times n}$  dont les entrées sur la diagonale sont égales à 1, et pour laquelle

$$\sum_{i < j=1}^n X_{ij} w_{ij}$$

est minimal.

Un programme semidéfini est traitable (par des algorithmes polynomiaux) et ceci découle du fait que « la contrainte qu'une matrice soit semidéfinie » est une contrainte qui peut être traitée similairement à la non-négativité de la programmation linéaire.

Si nous choisissons la sphère de diamètre 1, *le maximum  $S$  de la somme dans (\*) nous donnera une borne supérieure à la valeur maximum  $M$  d'une coupe*, (on peut placer les sommets dans deux points antipodaux de la sphère), d'autre part, *si dans (\*) on remplace  $\text{dist}(i, j)$  par l'angle  $x_i O x_j$  où  $x_i, x_j$  représentent les sommets  $i$  et  $j$ ,  $O$  est le centre de la sphère, et on mesure les angles en demi-tours (la mesure de l'angle de  $180^\circ$  est 1 et les autres angles ont une mesure proportionnelle) – on notera cette quantité  $\text{angle}(x_i, x_j)$  –, alors  $S$  devient  $S'$  et il se trouve qu'on peut trouver une coupe de taille  $S'$ , de plus,  $S'$  n'est pas beaucoup plus petit que  $S$ , que nous prouvons :*

Un hyperplan aléatoire qui passe par l'origine sépare les sommets en deux, définissant une partition. (La probabilité d'avoir des sommets sur l'hyperplan, est 0.) Cette partition sépare  $x_i$  et  $x_j$  avec probabilité égale à  $\text{angle}(x_i, x_j)$ . Et donc l'espérance mathématique de la contribution de l'arc  $ij$  est  $\text{angle}(x_i, x_j) w_{ij}$ . Par conséquent l'espérance mathématique de la coupe est juste  $S'$ , donc il existe une coupe de taille au moins  $S'$  qu'on peut déterminer en temps polynomial avec la technique de la dérandomisation ! Il ne reste plus qu'à vérifier  $0,878S \leq S' \leq S$ , où on sait déjà  $S' \leq S$ , et le lecteur pourra à nouveau vérifier ceci avec le théorème de Pythagore et de la trigonométrie de lycée : on est de nouveau dans le plan de dimension 2 – défini par le centre de la sphère et  $x_i, x_j$  –, et on peut calculer  $\text{dist}(i, j)$  en fonction du sinus et cosinus de l'angle. Il est surprenant mais vrai que *l'angle divisé par la distance au carré reste toujours supérieur ou égal à 0,878*, vérifiez le avec votre calculette !

## Une place (trop) discrète ?

La méthode des représentations géométriques similaires et l'application de la programmation semidéfinie sont maintenant choses courantes en optimisation combinatoire voir [RR]. D'autres idées géométriques ou algébriques ont montré leur puissance en théorie des graphes. Par exemple le nombre de Colin de Verdière – la multiplicité de la plus petite valeur propre positive d'une certaine matrice associée à un graphe – qui permet d'exprimer des représentations importantes et profondes (dans le plan ou d'une manière avantageuse en trois dimension) du graphe. La méthode utilise de l'algèbre linéaire et des arguments analytiques. Encore un autre des multiples exemples : Lovász, Bárány, Matoušek et récemment un jeune étudiant grenoblois Frédéric Meunier, utilisent des résultats de la topologie pour démontrer des théorèmes combinatoires qui ne se laissent pas aborder d'une manière élémentaire, (voir une introduction à ce sujet dans le joli livre de Matoušek).

A l'inverse, on voit de plus en plus que les autres domaines des mathématiques utilisent des méthodes ou des résultats combinatoires. Quelques exemples : la topologie (la théorie des noeuds utilise la théorie des graphes et des résultats de la combinatoire polyédrale), la géométrie algébrique (relations proches avec la programmation en nombres entiers), et les statistiques mathématiques (qui utilisent la théorie des structures régulières comme les « bloc design »), etc. Les relations tissent les liens entre mathématiques discrètes et les autres domaines des mathématiques. Beaucoup de jolis problèmes viennent aussi de l'informatique, d'autres sciences, de l'industrie, ou de l'économie (recherche opérationnelle), etc. Le domaine reste proche de ses applications, qui demeurent une ressource importante de problèmes.

Un autre domaine d'application mérite d'être mentionné : l'enseignement des mathématiques. Le discret est ludique, et fait bien travailler le cerveau même à un niveau de débutant : on y trouve des mini-théories prêtes à être enseignées dans le secondaire ; elles pourraient remplacer ou compléter certains enseignements classiques. Des collègues y travaillent (« maths à modéliser », « math-en-jeans », etc), et avec beaucoup de succès auprès des élèves. Espérons que ce bruit d'enfants joyeux qui aiment les maths sans être nécessairement « matheux » arrivera bientôt aux adultes qui déterminent le programme des écoles.

Quelle est la place des mathématiques discrètes dans le paysage scientifique ? En Allemagne<sup>3</sup>, en Hongrie<sup>4</sup>, ou encore dans de nombreuses universités d'Amérique du Nord<sup>5</sup>, elles ont une place consolidée, leur importance dans les formations universitaires modernes a été reconnue. En France cette place reste encore discrète. Le besoin de son enseignement – pour les informaticiens, ingénieurs, économistes, biologistes, etc. – est identifié, mais la nécessité d'une expertise importante n'est pas partout réalisée. Pourtant plusieurs équipes font une recherche appréciée au niveau international avec un nombre croissant de jeunes, dans le cadre de collaborations florissantes (exemple : le projet européen « Marie Curie training network »<sup>6</sup>), et pourraient fournir des enseignants spécialisés.

Il y a un quart de siècle, Lovász [LL] a écrit : « ... It is often forcefully stated that Combinatorics is a collection of problems, which may be interesting in themselves but are not linked and do not constitute a theory ... In my opinion, Combinatorics is growing out of this early stage. There are techniques to learn ... There are branches which consist of theorems forming a hierarchy and which contain central structure theorems forming the backbone of study ... There are notions abstracted to many non-trivial results, which unify large parts of the theory ... » Ceci s'est confirmé depuis, le domaine est devenu adulte, bien que toujours jeune et dynamique ; nous espérons que cette mini-photo condensée en donne une image déchiffrable.

## Pour en savoir plus

[LL] LOVÁSZ (L.), *Combinatorial problems and exercises*, North Holland and Akadémiai Kiadó (1979).

[RA] Perfect Graphs, recueil d'articles édité par RAMIREZ-ALFONSIN J., REED B., Springer (2001).

[AS] SCHRIJVER (A.), *Combinatorial Optimization*, 1-3, Springer (2003).

Je voudrais remercier Zoli Szigeti pour ses remarques pédagogiques, Nicolas Trotignon pour son aide professionnelle et linguistique consciencieuse et Sophie Sebó pour son aide stylistique. Le travail a été effectué dans le cadre du réseau ADONET, qui est un « Marie Curie Training Network ».

3. [www.or.uni-bonn.de/index.eng.html](http://www.or.uni-bonn.de/index.eng.html).

4. [www.cs.elte.hu/egres/](http://www.cs.elte.hu/egres/)

5. par exemple [www.math.uwaterloo.ca/CandO\\_Dept/](http://www.math.uwaterloo.ca/CandO_Dept/)

6. [www.ads.tuwien.ac.at/adonet/sites.html](http://www.ads.tuwien.ac.at/adonet/sites.html)