

plus que ce qu'il y a dans l'ensemble des lettres qui le composent.

Il est vrai que dans le mot COMPLEXE, il y a plus que dans la donnée de l'ensemble de ses lettres C, E, L, M, O, P, X, mais c'est bien évidemment parce qu'on ordonne les lettres et qu'on en répète, et que cet ordre et ces répétitions ajoutés aux parties constituent un «plus» qu'on trouve dans le *tout* et qui est absent de la somme des *parties*.

De telles illustrations de la maxime étudiée sont triviales et sans portée, puisqu'elles sont fondées sur un ajout caché quand on constitue le *tout*. Les cas soi-disant spectaculaires de synergie, d'effets cocktail et autres doivent le plus souvent s'interpréter de la même façon. Oui, un vélo est plus que ses parties étalées au sol, mais c'est parce qu'on organise ses parties en les assemblant de la bonne façon et que cette bonne organisation ajoute aux parties.

LA COMPLEXITÉ COMME CONTENU EN CALCUL

La théorie algorithmique de l'information qui détaille ce qu'on peut dire et démontrer sur la complexité de Kolmogorov a introduit une notion qui va nous sauver: la «profondeur logique de Bennett» qui est le temps de calcul du plus court programme qui produit l'objet numérique fini auquel on s'intéresse. C'est une mesure de complexité structurelle, ou encore, une mesure de «contenu en organisation et en calcul», alors que la complexité de Kolmogorov n'est qu'une mesure de «contenu incompressible d'information». Plus un objet est finement structuré, comme l'est par exemple un organisme vivant, plus sa profondeur logique est grande.

Ces deux mesures de complexité, complexité de Kolmogorov et profondeur logique, diffèrent radicalement pour les objets aléatoires dont l'exemple typique est une suite finie de 0 et de 1 obtenue par des tirages successifs à pile ou face. Pour un tel objet aléatoire, la complexité de Kolmogorov est maximale: on ne peut pas le décrire de manière sensiblement plus brève qu'en en donnant les éléments un à un, ce qui est la pire situation pour un objet numérique de taille n , puisque l'objet à produire doit alors être écrit explicitement dans le programme, lequel est nécessairement aussi long que l'objet décrit: une suite aléatoire des bits est incompressible.

À l'inverse, la profondeur logique d'une suite aléatoire de longueur n est minimale pour les suites de longueur n . Une suite aléatoire n'est pas structurée, son contenu en organisation est presque nul. Sa profondeur logique de Bennett est réduite au minimum, puisque exécuter le programme le plus court

2

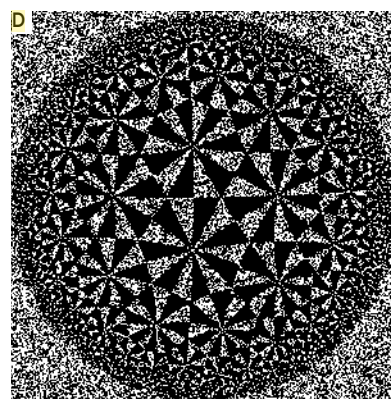
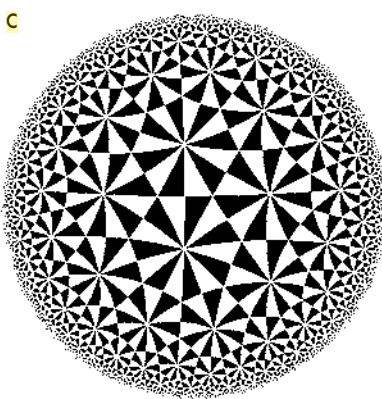
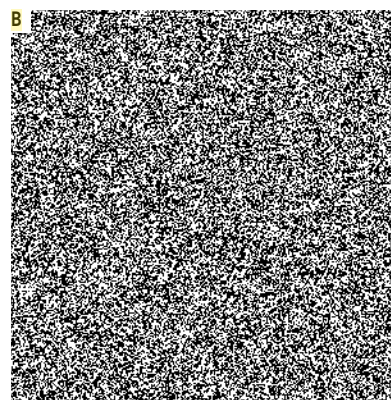
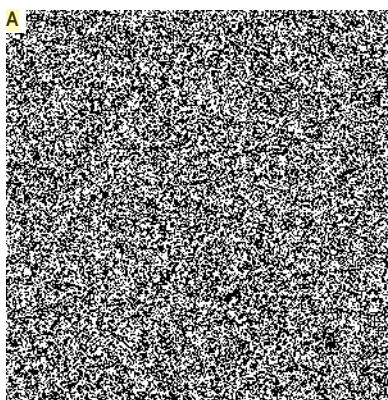
LA CRYPTOGRAPHIE VISUELLE À LA RESCOURSE

La cryptographie visuelle fournit un exemple incontestable de situation où le tout est plus que la somme des parties, plus précisément où le contenu en structures du tout est bien supérieur à la somme des contenus en structures de chacune de ses deux parties prises isolément.

On considère une image A composée à parts égales de points noirs et blancs disposés aléatoirement. Cette image n'a aucun contenu en structure, ou, dit autrement, sa profondeur logique de Bennett est très faible. On considère une image C ayant, elle, un contenu en structure important: il s'agit ici d'un pavage du plan hyperbolique. On calcule l'image $B = A \text{ xor } C$.

Un point est blanc dans B si les points correspondants de A et C sont tous les deux blancs ou tous les deux noirs; sinon, il est noir. L'image B est du même type que l'image A: elle n'a aucun contenu en structure et donc une profondeur très faible. Celui qui dispose de A et de B peut pourtant reconstituer C en calculant $A \text{ xor } B = A \text{ xor } (A \text{ xor } C) = (A \text{ xor } A) \text{ xor } C = C$. Il en résulte que $\text{Profondeur}(A \text{ et } B) \approx \text{Profondeur}(C)$, qui est supérieure à $\text{Profondeur}(A) + \text{Profondeur}(B)$.

Notons que si l'on imprime A et B sur des feuilles transparentes et qu'on les superpose, on voit apparaître l'image D, une forme bruitée de l'image C. C'est le principe de base de la cryptographie visuelle.



> qui engendre la suite aléatoire revient à exécuter un programme qui recopie une donnée explicitement inscrite dans le programme et qu'une telle copie ne prend presque pas de temps (contrairement par exemple à la production de chiffres du nombre π par un programme court).

Dans le cas le plus général, la profondeur logique de Bennett n'indique pas que le *tout* a une complexité supérieure à la somme des complexités des *parties*. En effet, si vous prenez un *tout* composé de k fois le même objet, sa profondeur logique sera à peu de chose près la complexité d'un seul objet, et donc sera nettement inférieure à la somme des complexités

des objets pris un à un. Il ne peut y avoir un théorème du *tout* et des *parties* exprimant sans restriction la maxime, même avec la profondeur logique de Bennett!

En revanche, et c'est là une belle surprise, il existe des cas où l'on peut établir avec certitude (ce qui est assez rare quand on manie le concept de profondeur logique) que la complexité d'un tout composé de plusieurs objets est supérieure à la complexité de la somme de chacun d'eux. Voici un tel exemple imparable.

Considérons les deux images A et B de l'encadré 2. Chacune est composée de 0 (pixels blancs) et de 1 (pixels noirs) d'une manière

UN CAS ÉLÉMENTAIRE FAVORABLE

3

Mesurons la complexité d'un ensemble d'objets par le nombre de liens que ces objets peuvent avoir entre eux. Quatre objets A, B, C, D ont par exemple potentiellement 6 relations possibles entre eux : A avec B, A avec C, A avec D, B avec C, B avec D, C avec D.

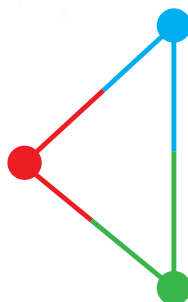
Ce nombre, 6, est le nombre de poignées de mains que 4 personnes s'échangent quand elles se rencontrent, ou le nombre de conversations en face-à-face que 2 personnes parmi 4 peuvent avoir. C'est le nombre d'arêtes possibles dans un graphe (non orienté et sans arête joignant un sommet à lui-même) ayant 4 sommets (*ci-contre, en bas*).

Pour n sommets, ce nombre devient $n(n-1)/2$. Ce nombre est une mesure envisageable de la complexité d'un ensemble d'éléments, car il correspond à la richesse des interactions possibles entre des paires d'éléments. Si l'on considérait les interactions à trois, la formule $n(n-1)/2$ deviendrait $n(n-1)(n-2)/6$ et une généralisation est possible pour les interactions à k , qui conduirait à utiliser les éléments du triangle de Pascal.

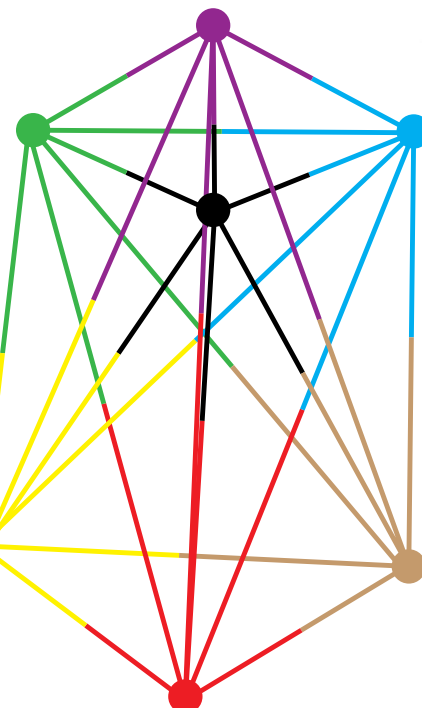
Pour cette mesure de complexité, a-t-on la propriété suggérée par la maxime attribuée à Aristote ? La réponse est oui. Si par exemple on considère n objets et qu'on les groupe en deux parties ayant respectivement a et b objets avec $a+b=n$ ($a \geq 1, b \geq 1$), alors il est facile d'établir que : $n(n-1)/2 > a(a-1)/2 + b(b-1)/2$. La richesse en interactions mesurée comme nous venons de le faire croît non linéairement en fonction du nombre d'éléments, et c'est ici la raison du succès de l'idée que le tout est plus que la somme des parties.



Complexité = 3



Complexité = 21



Complexité = 6

