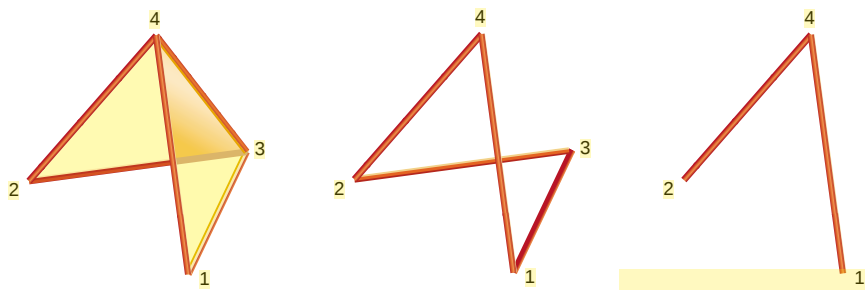


Avec ces règles, examinons quelques parties entre deux joueuses, Anastasia et Barbara. Anastasia joue toujours en premier. Quand $n = 1$, l'ensemble S n'a aucun sous-ensemble strict. Lorsque $n = 2$, $S = \{1, 2\}$, Anastasia ne peut que jouer $\{1\}$ ou $\{2\}$: quoi qu'elle choisisse, Barbara prend le second sous-ensemble et gagne, puisque Anastasia ne peut alors plus rien retirer.

Pour $n = 3$ et $S = \{1, 2, 3\}$, Anastasia peut choisir le sous-ensemble à deux éléments $\{1, 2\}$. Barbara prend alors le sous-ensemble complémentaire $\{3\}$. Comme Anastasia ne peut plus choisir de sous-ensemble contenant $\{3\}$, elle doit prendre un sous-ensemble de $\{1, 2\}$: le jeu est identique à celui où $S = \{1, 2\}$, et Barbara gagne encore. Le déroulement du jeu est semblable quel que soit le sous-ensemble de deux éléments pris au départ. Anastasia, qui se lasse de perdre, décide alors de commencer avec un sous-ensemble à un élément, par exemple $\{3\}$. Cependant, Barbara prend alors le complémentaire $\{1, 2\}$ et elle gagne encore. Au total, puisque Anastasia ne peut commencer qu'avec un sous-ensemble à un ou deux éléments, Barbara a une stratégie gagnante qui consiste à prendre systématiquement le complémentaire du sous-ensemble d'Anastasia. Quand n est supérieur à trois, Barbara a-t-elle encore une stratégie gagnante ?

Pour le savoir, examinons des problèmes de topologie, cette «géométrie des surfaces déformables». En topologie, on s'intéresse à des objets que l'on peut se représenter comme du caoutchouc qui pourrait se traverser, mais pas se déchirer. La représentation géométrique du «un sous-ensemble à emporter» impose une triangulation d'une surface, c'est-à-dire son fractionnement en triangles joints par leurs côtés. Cette méthode a été initialement mise au point pour des surfaces (à deux dimensions, donc), mais elle est généralisable à des objets de dimensions supérieures ; les triangles sont alors remplacés par des formes élémentaires nommées simplexes. Par exemple, un simplexe à trois dimensions, ou 3-simplexe, est un tétraèdre (voir la figure 1). Un tétraèdre a quatre sommets, quatre faces et six arêtes. Les faces sont des triangles (des 2-simplexes), les arêtes sont des segments (des 1-simplexes) et les sommets, des points (des 0-simplexes).

Ces composants du tétraèdre correspondent exactement aux sous-ensembles de $\{1, 2, 3, 4\}$: le tétraèdre est l'ensemble entier ; les faces sont les sous-ensembles de trois éléments $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$ et $\{2, 3, 4\}$; les arêtes sont les sous-ensembles à



a - ANASTASIA CHOISIT $\{1, 2\}$

b - BARBARA PREND $\{3, 4\}$

c - ANASTASIA CHOISIT $\{3\}$

2. La stratégie du complémentaire échoue dans cette partie de «ôte simplexe», car Barbara ne peut prendre le complémentaire du sous-ensemble choisi par Anastasia au deuxième tour (c).

deux éléments $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$ et $\{3, 4\}$; enfin, les sommets sont les sous-ensembles à un élément $\{1\}$, $\{2\}$, $\{3\}$ et $\{4\}$.

N'importe quel $(n-1)$ -simplexe représente un ensemble $S = \{1, 2, 3, \dots, n\}$, et chaque simplexe de dimension inférieure à $n-1$ est un sous-ensemble strict de l'ensemble S . Le «un sous-ensemble à emporter» devient alors un nouveau jeu, le «ôte simplexe» : à partir d'un simplexe donné, chaque joueur choisit un sous-simplexe strict de n'importe quelle dimension et en élimine l'intérieur, ainsi que tous les intérieurs des sous-simplexes qui le contiennent, sans toutefois supprimer les frontières du sous-simplexe choisi, par exemple les côtés d'une face triangulaire ou les deux extrémités d'une arête.

Nous pouvons utiliser cette représentation pour analyser une partie de «ôte simplexe» avec un 3-simplexe, qui équivaut à une partie de «un sous-ensemble à emporter» pour $n = 4$. La position initiale est un tétraèdre. La figure 1 illustre une série de mouvements autorisés. Une étude systématique des parties montre que Barbara a une stratégie gagnante pour $n = 4$, $n = 5$ et $n = 6$. D. Gale n'a pas encore réussi à démontrer que Barbara a une stratégie gagnante quel que soit n . Quelle est la stratégie gagnante de Barbara pour

n supérieur à trois ? Doit-elle toujours choisir le complémentaire du choix d'Anastasia ? Quand $n = 4$, Anastasia peut choisir un sommet, une arête ou une face. Lorsqu'elle choisit un sommet, Barbara prend alors le complémentaire, et le jeu se réduit à une partie où $n = 3$: Barbara gagne. Quand Anastasia choisit une face triangulaire, Barbara, en prenant le sommet complémentaire, réduit à nouveau le jeu, et gagne encore.

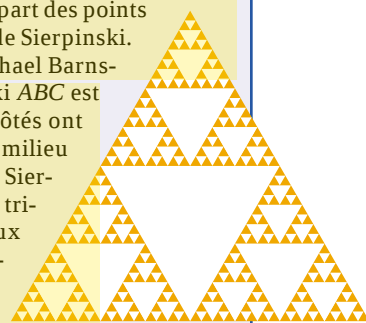
Cependant, quand Anastasia prend un segment, par exemple $\{1, 2\}$, et Barbara le complémentaire $\{3, 4\}$ (voir la figure 2), le jeu n'est pas réduit à une partie où n est inférieur. Anastasia prend ensuite $\{3\}$: Barbara ne peut choisir le complémentaire $\{1, 2, 4\}$, car c'est un coup non autorisé ; la face triangulaire correspondante a déjà été éliminée. La stratégie du complémentaire échoue ici. Certains mathématiciens ont proposé que pour tout n , Barbara a intérêt à choisir le complémentaire du coup d'Anastasia. Toutefois, cette stratégie n'est pas possible à chaque coup.

Anastasia est-elle condamnée à perdre chaque partie ? Les ordinateurs aideront à répondre à cette question pour des petites valeurs de n . Pour des n supérieurs, la réponse nécessite une approche plus fine.

Réactions

Ron Menendez, de Chatham, a découvert une propriété intéressante du triangle de Sierpinski (voir *Le triangle omniprésent*, *Pour la Science*, septembre 1999). Choisissez un point X de l'intérieur d'un triangle équilatéral ABC , puis un des sommets au hasard (par exemple, avec un dé). Le milieu du segment joignant X à ce sommet devient le nouveau point X . Répétez la procédure en choisissant à chaque fois un sommet au hasard. Pour la plupart des points initiaux, l'ensemble des points obtenus forme le triangle de Sierpinski.

La théorie des formes fractales autosimilaires de Michael Barnsley explique cet étrange résultat. Le triangle de Sierpinski ABC est composé de trois copies réduites de lui-même, dont les côtés ont une longueur égale à la moitié du triangle ABC initial. Le milieu d'un segment joignant un point quelconque du triangle de Sierpinski et l'un des sommets A , B ou C appartient aussi au triangle de Sierpinski. Cette particularité correspond aux chemins aléatoires de R. Menendez. M. Barnsley a démontré que tout chemin aléatoire de ce type converge vers le triangle de Sierpinski.





Le tatouage des images numériques

CAROLINE FONTAINE

Le tatouage des images, qui protège les créateurs, est indécélable par l'observateur : l'image de droite, tatouée, semble identique à la figure de gauche. Le tatouage est une signature qui prouve l'origine de la copie. Il n'est efficace que s'il résiste aux divers traitements de l'image, compression, ajout de bruit, changement de contraste, etc.



Le développement des réseaux de communication et des supports numériques comme le Compact Disc, le CD-ROM, le Digital Versatile Disc... entraîne une diffusion massive de documents stockés à l'aide de formats numériques, tels JPEG, MPEG, MP3. Ces techniques, qui permettent d'emmagasiner une grande quantité d'information en peu de place, facilitent aussi l'utilisation illégale des documents : il est en effet extrêmement aisé de récupérer un document sur Internet, ou sur un CD-ROM, et de le copier un grand nombre de fois avant de diffuser ces duplications. Non seulement la copie est facile, mais elle est parfaite : alors qu'un document analogique se détériore lorsqu'on le duplique, la copie numérique a exactement les mêmes qualités que l'original. Ces manipulations, si elles débouchent sur la commercialisation des copies, ou sur toute utilisation autre que privée, sont illégales tant que les droits d'auteur n'ont pas été versés à l'ayant droit du document.

L'objectif est d'associer à un document le nom du ou des ayant(s) droit associé(s) (il peut y avoir plusieurs ayants droit : le créateur, le producteur et le diffuseur, par exemple).

LA NÉCESSITÉ DE NOUVELLES TECHNIQUES

La recherche sur la protection des images a principalement débuté vers 1993, et aujourd'hui plus d'une centaine d'articles sont annuellement consacrés à ce sujet. Les premières techniques, comme le contrôle d'accès (destiné à autoriser ou

à refuser l'accès au document) ou la cryptographie (chiffrer ou signer le document) se sont révélées insuffisantes ou d'un emploi difficile. En effet, les dispositifs de cryptographie protègent l'image lors d'une transaction, mais pas au-delà : le destinataire retrouve après déchiffrement (ou vérification de la signature) la même version de l'image que celle qui précédait l'envoi, donc sans protection. Une technique complémentaire a alors été envisagée : le tatouage, dérivé de la stéganographie.

La stéganographie est l'art de cacher une information, une signature, dans un message que n'importe qui va pouvoir observer. Ce message peut être de diverses natures : texte, image, son. Une manière très simple est, par exemple, d'écrire un texte et de considérer le premier mot de chaque ligne : le texte «acrostiche» semble innocent dans sa globalité, mais la phrase constituée des premiers mots de chaque ligne peut avoir un sens tout différent. On peut aussi, dans un message électronique, placer des espaces en fin de ligne, le nombre d'espaces déterminant le «caractère» caché dans cette ligne ; on peut aussi inscrire l'information dans certaines composantes de l'image. Ainsi, toute personne non avertie ne s'apercevra pas qu'une information importante est transmise par l'intermédiaire d'un document d'apparence innocente.

L'idée est de cacher dans le document une information propre à son ayant droit sous la forme d'une marque qui ne pourra être enlevée sans une altération importante de ce document (rendant alors son

utilisation impossible). Cette marque, dénommée filigrane, devra rester imperceptible et faire suffisamment corps avec le document pour rester présente malgré les manipulations que ce dernier risque de subir. Les transformations pouvant altérer la marque sont des rotations, des changements d'échelle, des symétries, des découpages, des changements de format, l'application de filtres, l'ajout de bruit etc. La marque peut aussi être dégradée lors d'une impression/renumérisation par scanner.

Ces manipulations peuvent avoir pour but la destruction de la marque, ou tout simplement une utilisation facilitée de l'image (compression JPEG ou changement d'échelle, par exemple). On doit reconnaître la marque même quand le contenu numérique de l'image a changé.

Un système de tatouage dépend du contexte de son utilisation ; les spécialistes prennent en considération les contraintes des ressources informatiques (temps d'exécution des programmes de tatouage et de vérification, mémoire disponible) et les impératifs de la sécurité (environnement ouvert, fermé, qui va avoir accès à quoi, qui va exécuter les programmes de tatouage, de vérification).

LE PRINCIPE DE VÉRIFICATION

L'algorithme de tatouage, supposé connu de tous, est paramétré par une clé qui reste secrète : il n'est pas raisonnable de faire reposer la sécurité du système sur l'idée que personne ne connaît l'algorithme, car on sait bien que, dans la