# 7

# Vote inconscient

*Le vote inconscient pondéré, combinant oubli et hasard, accroît les choix d'un électeur.*

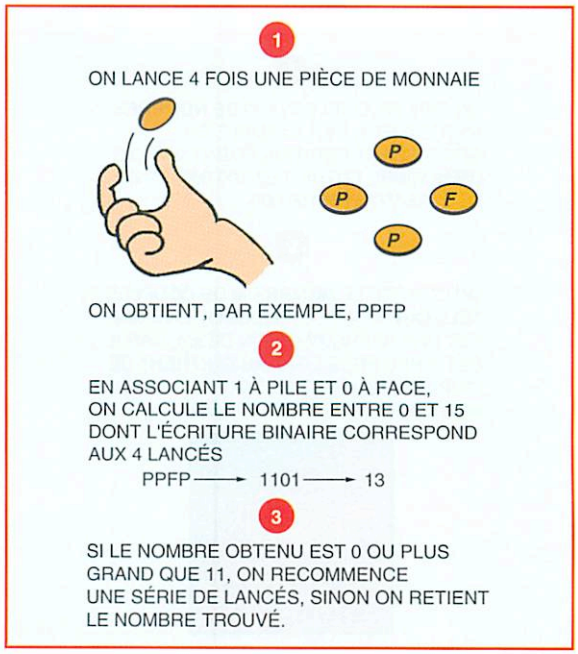
Oublier est chose facile pour l'ordinateur ; pour nous, c'est parfois impossible. Un programme peut faire un calcul, en mettre le résultat dans une mémoire $M$, puis oublier ce calcul par la seule utilisation de l'instruction d'affectation «$M := 0$». Vous, vous ne pouvez pas faire l'équivalent de ce «$M := 0$». Essayez, par exemple, d'oublier votre date de naissance! Une prescription amusante d'un médecin psychanalyste intimait au malade de faire trois fois le tour de son pâté de maison sans penser au mot «éléphant».

À l'inverse, déterminer un nombre au hasard est une chose que nous pouvons faire facilement, soit à l'aide des objets physiques qui nous entourent, soit mentalement, comme nous le verrons plus loin. Pour les ordinateurs, ce n'est pas si simple et, pour la plupart d'entre eux, cela est même totalement impossible.

Peut-on tirer des conclusions philosophiques de ces aptitudes opposées des cerveaux humains et des ordinateurs face au hasard et à l'oubli? Je pense que ce serait hasardeux et j'oublierai de le faire dans ce chapitre. Ce que je souhaite ici, c'est illustrer, par une série de problèmes, que ces aptitudes peuvent, chez l'un comme chez l'autre, être obtenues au moins partiellement à l'aide d'algorithmes spéciaux.

Le premier problème porte sur le tirage au sort équitable. Sous sa forme générale, c'est le suivant : vous voulez choisir un nombre entier au hasard, équitablement, entre 1 et $n$. «Équitablement» signifie que vous voulez que la probabilité de choisir chacun des nombres soit la même, c'est-à-dire $1/n$. Comment vous y prendre? Nous traiterons le cas $n = 11$, les généralisations étant évidentes.

Voici d'abord la solution utilisant une pièce de monnaie qu'on lance plusieurs fois. Pour commencer, vous lancez quatre fois de suite la pièce (non truquée bien sûr!) et vous calculez le nombre entre 0 et 15, dont l'écriture binaire est donnée par les quatre résultats des lancés, en interprétant *face* comme 0 et *pile* comme 1. Si le nombre obtenu est 0 ou dépasse 11, vous ne tenez pas compte du résultat et vous recommencez, autant de fois que nécessaire. Exemple : les quatre premiers lancés donnent *PPFP*, c'est-à-



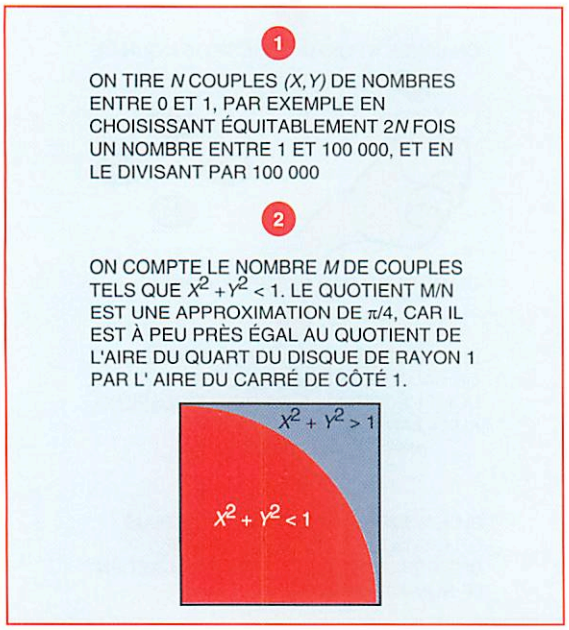

**1. Choix aléatoire équitable, avec une pièce de monnaie, d'un nombre entre 1 et 11.**

dire $[1101]_2 = 13$. Il faut recommencer. Les quatre lancés suivants donnent *PFFP*, c'est-à-dire $[1001]_2 = 9$. Donc, 9 est choisi.

Cette méthode est correcte, car elle aboutit, en un temps fini (non connu à l'avance), à un choix, et ce choix est équitable. Pour montrer que ce choix est équitable, on remarque que la procédure fait jouer un rôle symétrique à chacun des nombres de 1 à 11, et donc chacun a exactement une chance sur 11 d'être obtenu à l'issue de la procédure.

L'inconvénient de cette méthode est que, avec une probabilité de 5/16, vous devrez faire plus d'une série de quatre lancés (plus généralement, avec une probabilité de $(5/16)^m$ vous devrez procéder à plus de $m$ séries de quatre lancés). Éviter cet inconvénient n'est pas si facile que cela et, par exemple, décider que le nombre 0 fera choisir 1, que 12 fera choisir 2, que 13 fera choisir 3, que 14 fera choisir 4 et que 15 fera choisir 5 est une mauvaise idée, car on ne préserve pas l'équité du tirage : 1, 2, 3, 4 et 5 ont chacun une probabilité de 2/16 d'être choisis, alors que les autres nombres 6, 7, 8, ..., 11 n'ont qu'une chance sur 16 d'être retenus.

Le nombre $(5/16)^m$ diminue très vite quand $m$ augmente et donc, concrètement, vous ne ferez jamais de tirages prolongés avec la méthode que je propose. Sauf pour des valeurs particulières de $n$ (comme 2, 4, 8, ..., $2^p$), je ne crois pas qu'il existe des protocoles n'utilisant qu'une pièce de monnaie et garantissant que le choix sera fait équitablement en un temps fini déterminé à l'avance.




**2. Calcul de π par une méthode de tirage au sort de type Monte-Carlo.**

La méthode décrite s'adapte bien sûr si, au lieu de disposer d'une pièce de monnaie, vous disposez d'un dé (il faut calculer en base 6 et non plus en base 2). Avec un dé, une erreur à ne surtout pas commettre, et que mentionne tout professeur de mathématiques dans son premier cours de probabilités, est de croire que, pour choisir un nombre au hasard équitablement entre 2 et 12, il suffit de lancer le dé deux fois de suite et d'additionner les résultats. Cette méthode donne 1/36 de chance d'avoir 2 ou 12, 2/36 d'avoir 3 ou 11 (car 3 peut provenir de 1 + 2 ou de 2 + 1, et 11 de 5 + 6 ou de 6 + 5), 3/36 d'avoir 4 ou 10, 4/36 d'avoir 5 ou 9, 5/36 d'avoir 6 ou 8, 6/36 d'avoir 7.

Si vous n'avez à votre disposition ni pièce de monnaie ni dé, vous pouvez ouvrir un gros livre au hasard et regarder le chiffre des dizaines du numéro de page (attention : le chiffre des unités ne convient pas, car il est toujours pair à gauche et impair à droite). Les calculs se font alors en base 10, ce qui est assez pratique.

## Tirages au sort mentaux et tirages au sort pondérés

La méthode de la pièce de monnaie suggère une idée pour le tirage au sort mental (qui vous sera bien utile si, un jour, vous êtes prisonnier, les mains attachées dans le dos et que vous voulez choisir au hasard, équitablement, entre les sept méthodes d'évasion que vous avez imaginées). Penser à un mot moyennement long, *chaussure* par exemple, comptez alors son nombre de lettres : si ce nombre est pair, vous avez obtenu un 0 ; s'il est impair, vous avez obtenu un 1. Vous recommencez comme avec la pièce de monnaie de tout à l'heure. À moins que vous n'ayez la faculté de voir immédiatement le nombre de lettres d'un mot, et à la condition de ne pas tricher avec vous-mêmes, cette procédure mentale permet le tirage équitable d'un nombre entre 1 et $n$.

Comment vous y prendre maintenant si vous voulez faire un tirage pondéré à la place d'un tirage équitable, comme par exemple choisir avec des probabilités proportionnelles à leur âge entre les deux charmantes personnes susceptibles d'aller au cinéma ce soir avec vous. Rien de plus simple : à la première, qui a 24 ans, vous associez les nombres 1, 2, ..., 24 ; à la seconde, qui a 27 ans, vous associez les 27 nombres suivants : 25, 26, ...,

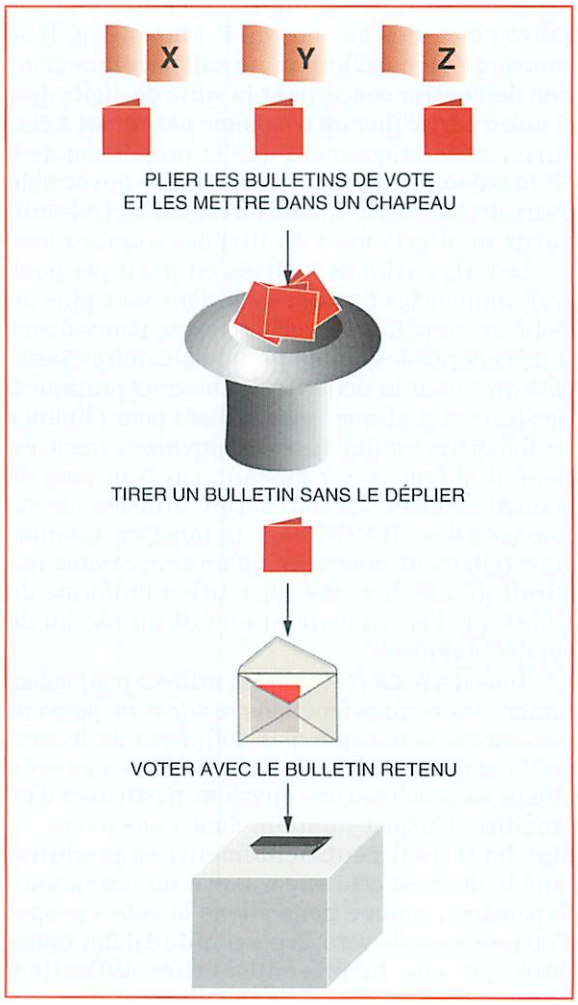
51. Vous choisissez ensuite équitablement un nombre au hasard entre 1 et 51, par une des méthodes expliquées plus haut. Si le nombre choisi est un des nombres associés à la première personne, c'est elle que vous inviterez ; sinon, c'est l'autre. Bien sûr, il est nécessaire que vous vous entraîniez à l'avance si vous voulez éviter d'avoir l'air hésitant au moment du choix en utilisant la méthode mentale!

Venons-en maintenant aux ordinateurs. Les langages de programmation offrent presque toujours une instruction qui est censée produire un nombre aléatoire à chaque fois que vous l'appelez. Cette fonction se nomme le plus souvent *random* (parfois elle se note *rnd*). Pour simplifier, nous ne considérerons que des fonctions renvoyant un 0 ou un 1. Ce que nous avons expliqué plus haut a d'ailleurs montré qu'avec une telle fonction, on peut toujours se débrouiller. La difficulté pour ceux qui conçoivent les langages de programmation et cherchent à programmer une telle fonction *random* provient de ce que, dans un ordinateur, rien ne marche au hasard. Tout est parfaitement déterministe lorsque l'ordinateur fonctionne bien et donc, sans contact avec l'extérieur, l'ordinateur ne peut pas produire de nombres aléatoires : c'est pour cela que les méthodes utilisées créent souvent des difficultés aux programmeurs.

Voici quelques-unes des idées qui sont utilisées. On peut lier l'ordinateur à un système physique (classique ou quantique) qui fasse des tirages au sort, mais cette méthode est rarement retenue, car trop lente. La lecture d'une table où sont stockés des nombres aléatoires est parfois choisie. Elle présente bien sûr l'inconvénient de coûter cher en mémoire. Son utilisation est donc réservée aux situations où l'on veut avoir une garantie très forte sur l'aspect aléatoire des digits utilisés, ce qui est le cas en cryptographie, mais pas en calcul numérique, où les méthodes, dites de Monte-Carlo, utilisent des tirages au sort uniquement pour répartir à peu près uniformément des points dans un espace *(voir la figure 2)*.

Certaines méthodes utilisent l'horloge interne, mais le plus souvent, aujourd'hui, la méthode retenue pour la conception des langages informatiques consiste à programmer les fonctions *random* avec «semence». Au lieu d'écrire «*R* := random» pour obtenir un nombre aléatoire, vous écrivez : «*R* := random (13425)», et le résultat que vous obtenez est calculé à partir de la semence : 13425. La deuxième fois que vous faites appel à «*R* := random(13425)», le nombre aléatoire fourni est différent, mais parfaitement déterminé. La semence peut bien sûr être changée, ou même demandée à l'utilisateur du programme quand c'est nécessaire. Ce qu'il faut savoir, c'est qu'à chaque fois que vous faites appel à la fonction *random*, le nombre obtenu dépend de la semence et du nombre d'appels précédents.

Cette méthode est pratique, car si vous exécutez votre programme plusieurs fois, vous obtiendrez la même suite exactement de nombres «aléatoires». Mais cette méthode possède aussi plusieurs inconvénients. Le premier est que vous ne pouvez pas faire un vrai tirage au sort, puisque les résultats obtenus dépendent de la semence de façon parfaitement déterministe. Même si vous ne connaissez pas la fonction utilisée pour calculer les nombres «aléatoires», cette fonction est fixée une fois pour toutes, et il n'y a donc en réa-




**3. Le vote inconscient équitable.**

lité aucun tirage au sort. Le deuxième inconvénient est que les fonctions utilisées pour engendrer du hasard ne sont jamais des fonctions donnant des suites aléatoires au sens mathématique du terme, pour la simple raison que les suites aléatoires au sens mathématique du terme – qu'on appelle suites aléatoires de Martin-Löf, car introduites par le mathématicien suédois P. Martin-Löf en 1965 *(voir le chapitre 4)* – ne peuvent pas être engendrées par des algorithmes déterministes, et donc ne peuvent pas être produites à l'intérieur d'un ordinateur usuel.

En particulier, l'idée d'utiliser les digits du développement infini de $\pi$ en base 2 est une très mauvaise idée : même si on n'a pas trouvé de propriétés statistiques singularisant $\pi$ par rapport à une suite obtenue par une authentique série de lancés de pièce de monnaie, le seul fait que la suite des digits de $\pi$ soit calculable par ordinateur exclut cette suite de digits de l'ensemble des suites aléatoires au sens de P. Martin-Löf. Il se trouve qu'aujourd'hui on ne sait pratiquement rien démontrer concernant la suite de digits de $\pi$ et qu'en particulier on n'a même pas réussi à établir mathématiquement que la proportion de 0 est la même que la proportion de 1, ce qui semble pourtant bien le cas quand on étudie les trois milliards de digits dont on dispose aujourd'hui.

Les algorithmes utilisés en pratique pour programmer les fonctions *random* sont plus ou moins mauvais, et les recherches se poursuivent pour générer des suites pseudo-aléatoires satisfaisantes pour la majorité des besoins pratiques. Des tests statistiques sont utilisés pour éliminer les fonctions vraiment trop mauvaises, mais, en général, il faut rester méfiant, car beaucoup de mauvaises fonctions sont encore utilisées : je me souviens d'un BASIC dont la fonction *random* était tellement mauvaise qu'un programme qui aurait dû afficher une répartition uniforme de points sur l'écran donnait en fait un réseau de bandes obliques!

Tous les tests statistiques utilisés pour sélectionner les bonnes fonctions *random* ne peuvent rien contre le fait que, par définition du hasard mathématique absolu, il est impossible à un ordinateur sans mécanisme physique particulier d'en produire. L'esprit humain, dont nous avons vu plus haut qu'il peut (lentement) en produire, semble donc en cela supérieur à un ordinateur. Cependant, comme nous allons le voir à propos d'un problème de vote, la possibilité d'oubli volontaire, qui, elle, ne présente aucune difficulté à une machine, fait parfois cruellement défaut à l'esprit humain.

## Les avantages du vote au hasard

L'un de mes amis, fatigué de voter de la manière habituelle, m'avait expliqué son point de vue : «Je souhaite soutenir le régime démocratique dans lequel nous vivons, donc je veux voter. En revanche, je n'ai pas vraiment d'opinions arrêtées sur les différents partis et candidats entre lesquels je dois choisir, sauf à propos de certains que j'élimine, car ils défendent des idées opposées à la démocratie. Je souhaite donc voter au hasard, pour l'un des candidats démocrates. Toutefois, je préférerais ne pas savoir pour qui je vote.»

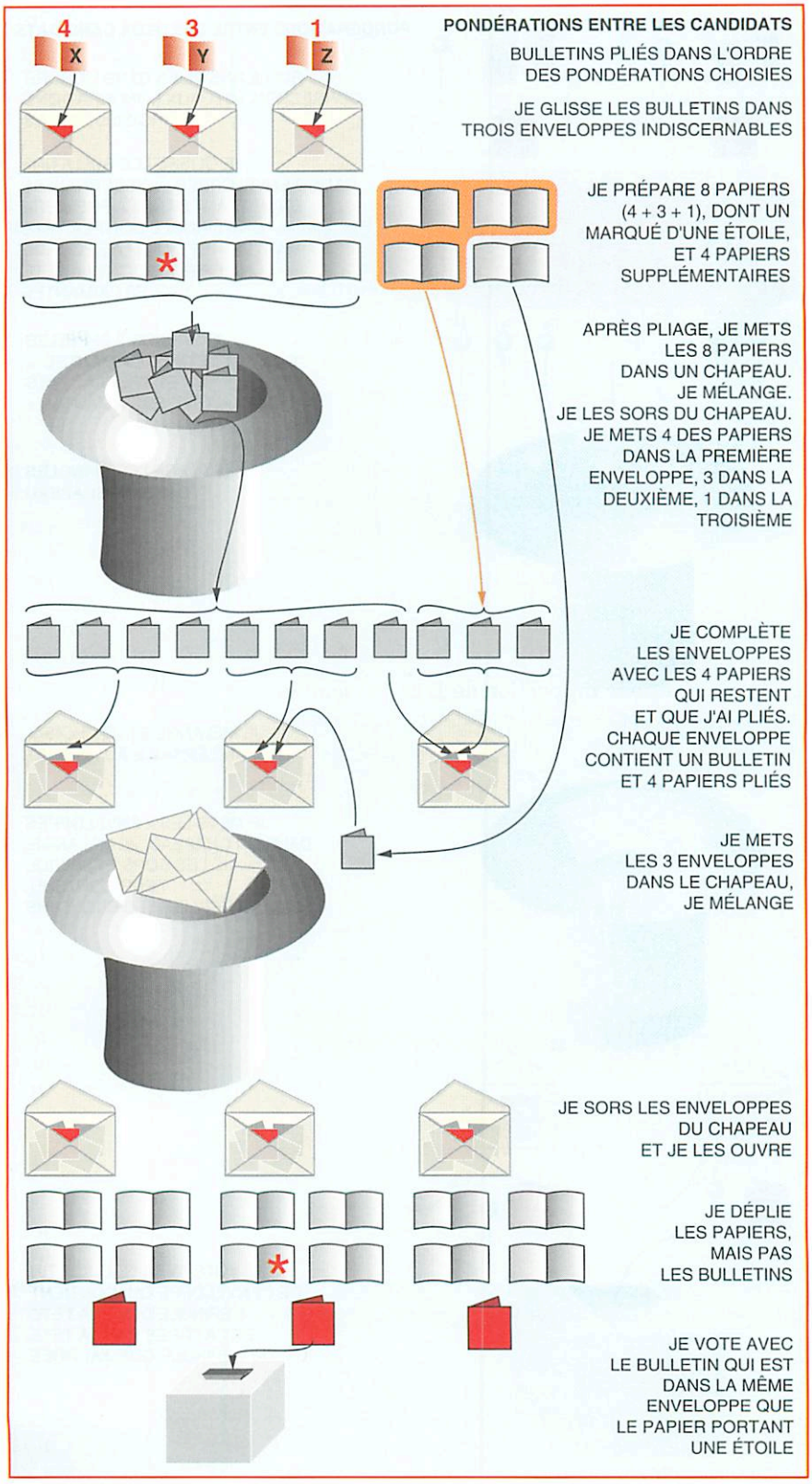
Il s'agit d'un problème d'oubli. Mon ami souhaite voter au hasard pour un candidat démocrate, mais ne veut pas savoir pour qui. Je lui ai répondu : «Avant chaque élection, la mairie t'envoie les bulletins de vote des différents candidats. Élimine ceux qui te déplaisent, plie les autres, mets-les dans un chapeau, mélange, choisis au hasard l'un des bulletins pliés, mets-le dans ta poche, déchire ou brûle les autres et va voter avec le bulletin qui est dans ta poche sans le regarder» *(voir la figure 3)*.

Mon ami semblait très satisfait. En effet, le protocole de vote proposé assure à la fois l'équité entre les candidats retenus et l'impossibilité pour lui de savoir pour qui il vote, ce qu'il désirait. Un tel protocole de vote «inconscient équitable» est amusant, car il permet de voter contre quelques-uns et non plus seulement pour quelqu'un, comme avec la méthode habituelle. En effet, statistiquement, en procédant selon la méthode décrite, on vote à parts égales – les probabilistes diraient «avec une espérance mathématique égale» – pour tous les candidats non éliminés, ce qui n'est pas le cas lorsqu'on s'abstient ou lorsqu'on vote blanc ou nul. En un certain sens donc, ce mode de vote élargit l'éventail des choix qu'offre une élection. S'il était plus connu, il y aurait peut-être un peu moins d'abstentions.

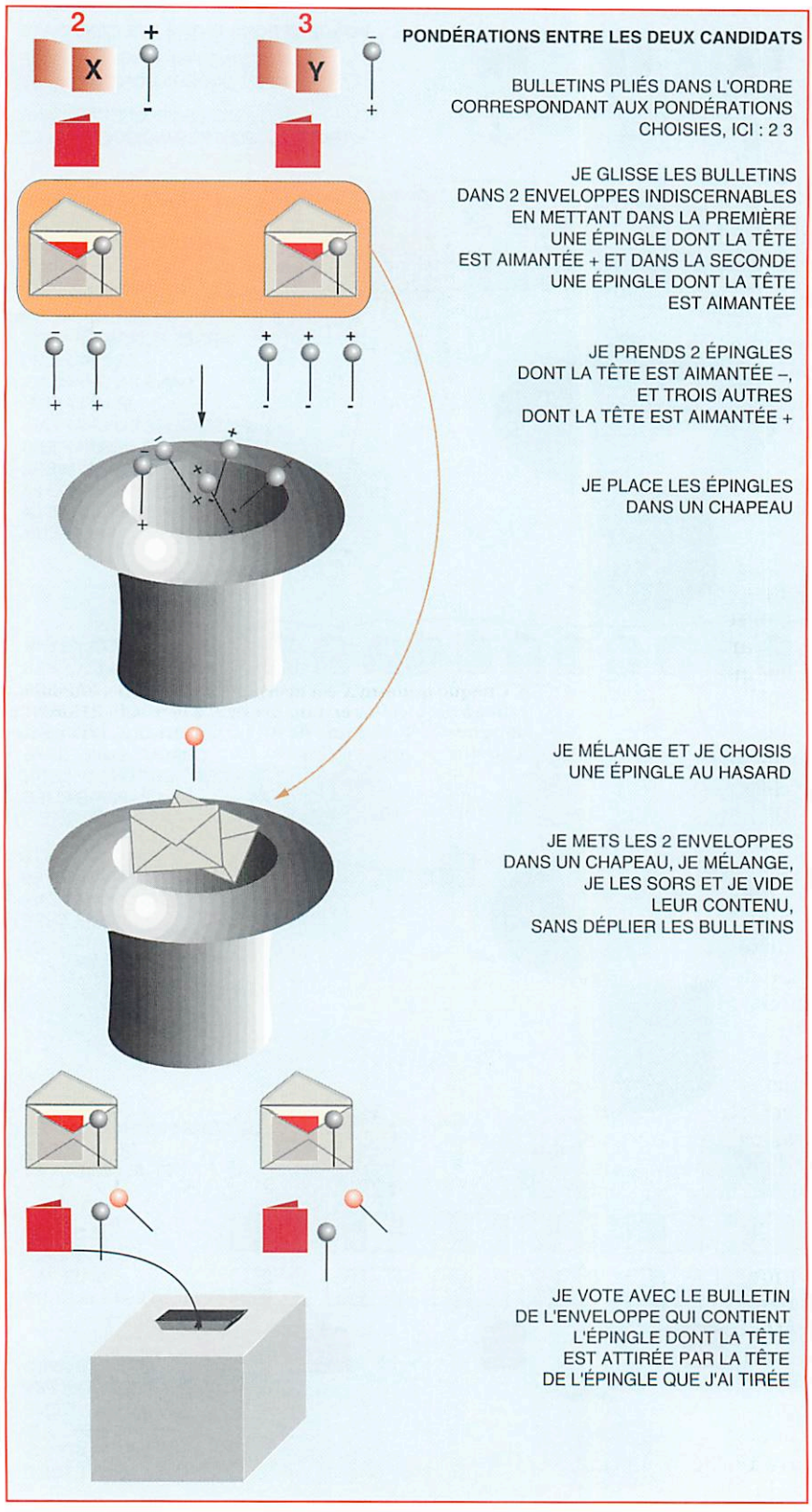
## Le problème du vote inconscient pondéré

Malheureusement, mon ami est exigeant et, après avoir utilisé le protocole de vote inconscient équitable aux dernières élections, il m'a expliqué que ce que je lui avais indiqué ne lui convenait pas vraiment.

«Imagine, me dit-il, que beaucoup de *gens* fassent comme moi ; imagine même que tout le monde fasse comme moi. Que va-t-il se passer? Les candidats les plus farfelus auront à peu près autant de voix que les autres. Je ne le souhaite




**4. Vote inconscient pondéré avec un seul bulletin par candidat : la procédure avec papiers, enveloppes et chapeau. On veut choisir l'un des trois candidats *X*, *Y* ou *Z* au hasard, avec une pondération de 4, 3, 1. On ne veut pas connaître le choix fait ; on ne dispose que d'un bulletin par candidat.**

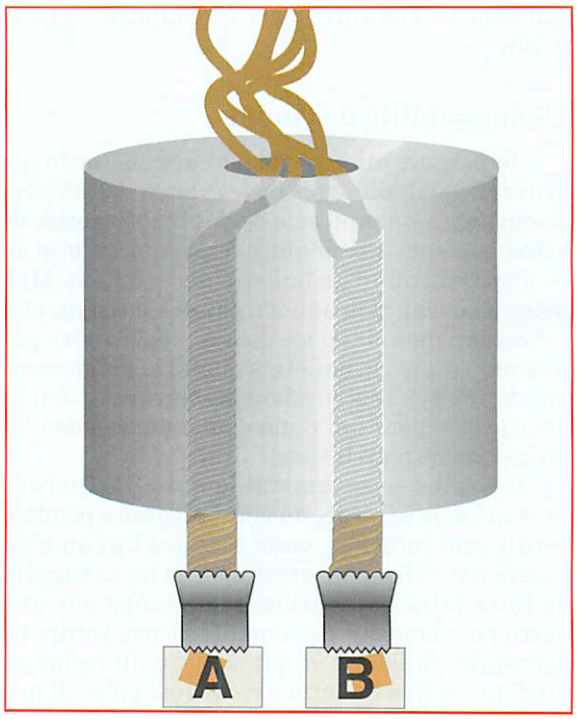



**5. Vote inconscient pondéré avec un seul bulletin par candidat : la procédure avec des épingles aimantées.**

pas. Je ne veux pas faire de choix ferme, mais je voudrais pondérer les candidats. Très précisément, je voudrais que le candidat $X$ ait 4 fois plus de chances d'être choisi par moi que $Z$, et que le candidat $Y$ ait 3 fois plus de chances d'être choisi que $Z$. J'ai bien pensé généraliser ton protocole, en mettant, dans le chapeau qui me sert au tirage, 4 bulletins pour $X$, 3 bulletins pour $Y$ et 1 pour $Z$, mais, malheureusement, la mairie ne m'envoie qu'un bulletin pour chaque candidat, et je ne me vois pas attendre d'être dans le bureau de vote pour y prendre les bulletins nécessaires, puis entrer dans l'isoloir avec mon chapeau pour effectuer mon tirage au sort. Comment dois-je m'y prendre pour déterminer mon vote chez moi, avec un seul bulletin pour chaque candidat?»

La méthode la plus naturelle consiste à faire comme tout à l'heure pour pondérer des choix dans le problème de la personne à inviter au cinéma, mais, en faisant cela, mon ami va savoir pour qui il vote, et il ne le souhaite pas. C'est bien l'impossibilité d'oublier quelque chose à volonté qui bloque tout. Comment s'en sortir? Comment faire un choix pondéré au hasard, l'exécuter et l'oublier quand on ne dispose que d'un bulletin par candidat? Si mon ami était une machine, le problème serait résolu par une instruction $M$ :=0, mais mon ami n'est pas une machine.

Puisqu'un programme peut oublier, peut-être existe-t-il une méthode utilisant un ordinateur. Après un peu de réflexion, j'ai imaginé une méthode, que j'ai proposée à mon ami : «Tu mets devant toi, sur une table, les trois bulletins pliés dans l'ordre $X$, $Y$, $Z$. Tu utilises ensuite un programme qui fait les choses suivantes. Il choisit au hasard, en fonction de l'heure (que tu ne regarderas pas au moment de l'utilisation), avec les pondérations que tu as fixées, un candidat $X$, $Y$ ou $Z$ (il est immédiat d'écrire un tel programme en utilisant le principe de pondération expliqué plus haut). Après cela, 20 fois de suite, le programme choisit au hasard (toujours avec l'horloge interne) un nombre 1, 2 ou 3, qu'il affiche à l'écran. S'il affiche 1, tu permutes les bulletins 2 et 3 ; s'il affiche 2, tu permutes les bulletins 1 et 3 ; s'il affiche 3, tu permutes les bulletins 1 et 2. Le programme, dans toutes ces permutations, suit le bulletin qu'il a choisi au départ, alors que, de ton côté, tu ne tentes pas de suivre des yeux les bulletins. Après les 20 permutations, le programme t'indique la nouvelle place du bulletin qu'il avait choisi au début. Tu le prends. Tu détruis les autres bulletins et tu éteins l'ordinateur – ce qui rend impossible la connaissance du choix qu'il avait




**6. Chaque bulletin $X$ est accroché à une corde, elle-même reliée à des ficelles en nombre égal à la pondération retenue pour $X$. On tire une ficelle au hasard, cela fait monter un bulletin, on va voter avec.**

### Procédure permettant, avec une pièce de monnaie, de faire des choix pondérés par des nombres irrationnels

On veut choisir entre les deux possibilités $A$ et $B$, avec des probabilités proportionnelles aux deux nombres $\pi$ et $e$. On ne dispose que d'une pièce de monnaie pour faire des tirages à pile ou face.

**0**

Faire un programme qui donne, une par une, les décimales successives de $\pi/(e + \pi) = 0{,}536119...$

**1**

Choisir équitablement un nombre $n$ entre 0 et 9,

(1) si $n$ est strictement plus petit que la première décimale de $\pi/(e /+ \pi)$, la possibilité $A$ est choisie.

(2) si $n$ est strictement plus grand que la première décimale de $\pi/(e + \pi)$, la possibilité $B$ est choisie.

(3) sinon (c'est-à-dire si $n = 5$) :

**2**

Choisir équitablement un nouveau nombre $n$ entre 0 et 9,

(1) si $n$ est strictement plus petit que la deuxième décimale de $\pi/(e + \pi)$, la possibilité $A$ est choisie.

(2) si $n$ est strictement plus grand que la deuxième déci-male de $\pi/(e + \pi)$, la possibilité $B$ est choisie.

(3) sinon (c'est-à-dire si $n = 3$) :

**3**

etc.

fait – et tu vas voter avec ce bulletin, sans le déplier.»

## L'impossibilité de l'oubli

Je pensais lui avoir fourni une méthode qui éviterait qu'il aille grossir les rangs des abstentionnistes. Mon protocole devait lui permettre de voter sans savoir pour qui, avec pondération et en ne disposant que d'un bulletin par candidat. Malheureusement mon ami n'a pas été satisfait, et il est revenu me voir en me disant : «Je n'arrive pas à *ne pas suivre* les bulletins quand le programme me donne ses instructions de permutation, et donc je sais pour qui il me demande de voter. Ta procédure ne marche pas!»

Un robot programmable qui effectuerait, sans qu'on le regarde, un choix aléatoire pondéré serait une solution, mais aujourd'hui on n'en trouve pas si facilement, et donc je lui ai suggéré de faire faire l'opération de mélange par une autre personne qui ne connaîtrait pas l'ordre de départ des bulletins et qui, à la fin du mélange, lui donnerait le bulletin avec lequel voter. Il m'a répondu que la personne en question pourrait très bien suivre des yeux les bulletins et donc qu'à eux deux, il leur serait tout à fait possible de déduire pour qui il vote. «Certes, en utilisant une tierce personne, me dit-il, il m'est impossible à moi seul de savoir pour qui je vote, et il est impossible à l'autre personne seule de le savoir aussi, mais les informations que nous pouvons posséder chacun de notre côté suffisent à retrouver le candidat pour qui je vote et que je veux ignorer.» L'imperfection était réelle.

Persuadé que ce problème du «vote inconscient pondéré avec un seul bulletin par candidat» devait posséder une solution simple, j'en ai parlé autour de moi. J'ai bien fini, de mon côté, par trouver une solution n'utilisant, en plus des bulletins, que des enveloppes, des petits papiers et un chapeau pour effectuer des tirages au sort, mais elle était assez compliquée et moins bonne que celle que m'a proposée Luc Dauchet, le fils d'un collègue *(cette solution est décrite à la figure 4)*.

Une autre solution utilisant des épingles aimantées a été imaginée par Philippe Boulanger *(voir la figure 5)*. Elle ne nécessite que des épingles et un aimant, mais ne permet que le choix pondéré entre deux candidats (une généralisation est possible pour $n$ candidats, que le lecteur pourra rechercher). À la place d'épingles aimantées, on pourrait utiliser des verres polarisés. Une autre solution n'utilise que de la corde et de la ficelle *(voir la figure 6)*. Ces protocoles de vote élargissent encore l'éventail des possibilités offertes par une élection, et il semblerait donc que maintenant les abstentionnistes n'aient plus d'excuse!

## Deux petits problèmes

Voici deux problèmes liés.

**Problème 1.** Trouver une procédure permettant de faire un choix aléatoire entre deux éventualités $A$ et $B$, avec des probabilités respectives pour $A$ et pour $B$ proportionnelles aux nombres irrationnels $\pi$ et $e$. Remarque : on ne veut pas que les probabilités soient approximativement proportionnelles à $\pi$ et $e$, mais qu'elles soient exactement proportionnelles à $\pi$ et $e$, et bien sûr la procédure doit se terminer.

**Problème 2.** Trouver une procédure de vote permettant, avec un seul bulletin par candidat, de choisir inconsciemment entre deux candidats $A$ et $B$ avec des probabilités proportionnelles aux deux nombres irrationnels $\pi$ et $e$.

Les solutions de ces problèmes sont :

### Procédure de vote inconscient avec pondérations irrationnelles et un seul bulletin par candidat

On veut voter sans savoir pour qui, après avoir fait un choix aléatoire entre les deux candidats $A$ et $B$, les probabilités de choisir $A$ et $B$ étant respectivement proportionnelles aux deux nombres $\pi$ et $e$. On ne dispose que d'un bulletin par candidat.

**0**

Faire un programme qui donne, une par une, les décimales successives de $\pi/(e + \pi) = 0{,}536119...$

**1**

Utiliser une procédure de vote inconscient pondéré, avec une pondération de 5 pour $A$, de $4 = 9 - 5$ pour $B$ et de 1 pour un candidat fictif $C$ dont le bulletin est discernable des deux autres.

(5 est la première décimale de $\pi/(e /+ \pi)$).

Si le bulletin déterminé par la procédure n'est pas le bulletin de $C$, alors aller voter avec le bulletin choisi.

Sinon :

**2**

Utiliser une procédure de vote inconscient pondéré, avec une pondération de 3 pour $A$, de $6 = 9 - 3$ pour $B$ et de 1 pour un candidat fictif $C$ dont le bulletin est discernable des deux autres.

(3 est la deuxième décimale de $\pi/(e + \pi)$).

Si le bulletin déterminé par la procédure n'est pas le bulletin $C$, alors aller voter avec le bulletin choisi.

Sinon :

**3**

etc.