

thèse», et que l'autre moitié à peu près adopte la méthode symétrique :

B. «Si je vois devant moi autant de croix noires que de croix rouges, je vote en faisant l'hypothèse que j'ai dans le dos une croix noire. Sinon, je suppose que j'ai dans le dos une croix de la couleur majoritairement présente devant moi et je vote conformément à cette hypothèse.»

Que se passe-t-il alors ? Dans le cas 1, rien de changé. Dans le cas 2, il suffit qu'un seul porteur de croix rouge joue *B* plutôt que *A* pour que le vote majoritaire soit mauvais. Et donc, sauf exception, le cas 2 sera défavorable. Le cas 3 est de même défavorable, sauf hasard exceptionnel (1 fois sur 2ⁿ).

Par rapport à notre calcul précédent, il faut maintenant doubler le nombre de cas défavorables. Il n'est plus aussi clair que la méthode soit intéressante. Un petit calcul montre cependant que, si le nombre de logiciens est supérieur à 7, alors la stratégie décrite est favorable aux logiciens. Rien d'important n'est donc changé si les logiciens n'ont pas eu la possibilité de s'entendre préalablement à l'épreuve.

LA JUSTE MAJORITÉ

Reste une question : pourquoi le raisonnement présenté dans l'énoncé est-il faux ? La réponse est liée à une remarque que connaissent bien les hommes politiques français : quand une élection se fait en plusieurs endroits, pour gagner la majorité, il n'est pas nécessaire d'avoir plus de voix que l'adversaire, mais d'en avoir un peu plus dans la majorité des sites. On peut même avoir au total moins de voix que son adversaire et gagner la majorité des élections, donc, par exemple, emporter une mairie dans une ville où l'on a moins de voix que l'opposition (Gaston Defferre, il y a quelques années, par un judicieux découpage des arrondissements de Marseille, avait réussi ce bel exploit).

Dans notre histoire, quand on évalue la probabilité de gagner, c'est comme s'il y avait plusieurs votes (un pour chaque tirage au sort de la répartition des croix rouges ou noires), et il est bien exact qu'une fois sur deux, lors du déroulement de tous les scrutins possibles, la réponse qu'un logicien propose est fautive. Toutefois, cela n'entraîne pas que le vote général est faux une fois sur deux, car lorsque le vote est bon, la majorité est souvent faible, alors que, lorsque le vote est mauvais, ce sont beaucoup de votants qui se sont trompés (dans certains cas, 100 pour cent).

Pour vous convaincre de cela, vous pourrez examiner le cas de cinq logiciens de la figure 1.

2. VOTES MAJORITAIRES MALHEUREUX

NOMBRE DE LOGICIENS	NOMBRE TOTAL DE CAS	NOMBRE DE CAS DÉFAVORABLES	PROBABILITÉ D'ERREUR
3	8	3	37,5 %
5	32	10	31,25 %
7	128	35	27,34 %
9	512	126	24,61 %
15	32768	6435	19,64 %
25	33554432	5200300	15,49 %

En conclusion, dans une série d'élections, pour gagner une majorité de fois, ce qui est important ce n'est pas d'avoir la majorité de tous les suffrages qui sont exprimés au total, mais d'avoir une majorité de fois la majorité, ce qui est bien différent et ce qui est possible, même si, en cumulant les résultats de toutes les élections, on est minoritaire.

Nos logiciens, grâce à leur intelligence, réussissent à avoir raison collectivement plus souvent qu'ils n'ont raison individuellement. Cette remarquable propriété de leur procédé de vote est peut-être celle qu'ont recherchée les concepteurs du *Scrutin majoritaire à deux tours* des élections législatives françaises. Celui-ci, on le sait bien, en défavorisant les partis extrémistes et démagogues, conduit à des résultats où les électeurs choisissent collectivement un bien plus grand nombre de fois de rester modérés qu'ils ne le choisissent individuellement. Ce problème de vote est dû à J. Aspnes, R. Beigel, M. Furst et S. Rudich et m'a été signalé par Gilles Brassard, de l'Université de Montréal.

2. L'ABSURDITÉ DU VOTE AU PLUS FORT RESTE

Examinons comment se déroule un vote au scrutin proportionnel de liste au plus fort reste. Il y a n électeurs et m représentants à élire ; chaque électeur choisit une liste qui comporte m noms. Il est de bon sens de vouloir que les listes ayant reçu le plus de votes aient le plus d'élus.

Dans une première phase du dépouillement, on compte le nombre de bulletins obtenus par la liste *A*, et l'on désigne par a ce nombre. On divise le produit $a.m$ par n , ce qui donne le quotient q et le reste r : $a.m = q.n + r$, et l'on attribue q sièges à la liste *A* (pris bien sûr en tête de la liste classée *A*).

On fait de même pour chacune des autres listes.

L'idée justifiant ce calcul est que, (i) chaque électeur vote pour m représentants, et donc que son bulletin exprime en fait m voix (d'où le calcul de $a.m$) et que, (ii) dès qu'une liste a obtenu n voix, elle gagne un siège (d'où le calcul du quotient $a.m = q.n + r$). Dans la seconde phase, on attribue les postes restants aux listes qui ont les plus forts restes dans l'ordre décroissant des restes calculés. Voici maintenant l'énoncé de l'énigme tirée du Sixième championnat international des jeux mathématiques. Il y a trois listes et sept représentants à élire. Lors du dépouillement, on compte 102 bulletins et l'on attribue deux sièges à la liste *A*, deux à la liste *B* et trois à la liste *C*. On découvre alors une double erreur : d'une part, ce n'est pas sept mais huit sièges qu'il faut pourvoir et, d'autre part, un bulletin était resté dans l'urne en faveur de la liste *A*. Après correction, la liste *A* perd un siège. Cela est paradoxal, puisqu'il y a un siège de plus à pourvoir et un bulletin de plus en faveur de la liste *A*. Sachant qu'il n'y avait ni bulletin blanc, ni bulletin nul, trouvez le nombre de bulletins en faveur de chacune des listes.

Solution

En procédant par tâtonnement, on découvre qu'il y a 21 bulletins pour *A*, 34 pour *B* et 48 pour *C*. En effet, cela répond bien au problème.

Lors du premier calcul (un siège et un bulletin oublié), on obtient : $20 \times 7 = 1 \times 102 + 38$; $34 \times 7 = 2 \times 102 + 34$; $48 \times 7 = 3 \times 102 + 30$, ce qui donne donc deux sièges pour *A* (un directement, puis un par la règle du plus fort reste), deux pour *B* et trois pour *C*.

Lors du second calcul, on obtient : $21 \times 8 = 1 \times 103 + 65$; $34 \times 8 = 2 \times 103 + 66$; $48 \times 8 = 3 \times 103 + 75$, ce qui donne donc un siège pour *A*, trois pour *B* (deux directement, puis un grâce aux restes) et quatre pour *C* (trois directement, puis un grâce aux restes).

Malgré le siège supplémentaire à pourvoir et le bulletin ajouté en faveur de la liste *A*, celle-ci, après correction, a perdu un siège !

3. LE VOTE PAR TÉLÉPHONE

Cinq personnes dans cinq pays différents doivent voter pour ou contre une certaine motion. Il leur est impossible de se déplacer, et elles doivent donc exprimer leur choix par téléphone (ou par courrier électronique). Elles ne veulent faire intervenir aucun tiers, même pas pour compter les votes de chacun, et souhaitent absolument que les votes res-

tent confidentiels (autant que lors d'un vote à bulletins secrets avec une urne s'il avait été possible). Chacune d'entre elles doit pouvoir calculer le résultat du vote. Comment doivent-elles s'y prendre? On fera l'hypothèse que les cinq personnes, parfaitement honnêtes, ne tentent pas de tricher et qu'elles savent toujours qui leur a envoyé un message (aucun anonymat n'est donc possible dans les communications).

Solution

Chacune des cinq personnes A, B, C, D et E choisit un nombre entier (respectivement a , b , c , d , et e) qu'elle prend multiple de 6 si elle veut voter OUI ou multiple de 6 plus 1 (comme $31 = 6 \times 5 + 1$) si elle veut voter NON. La somme $N = a + b + c + d + e$ sera donc de la forme «un multiple de 6, plus le nombre de voix NON» (par exemple, $604 = 6 \times 100 + 4$ signifie «4 NON»).

Chaque participant choisit maintenant une décomposition arbitraire de son nombre sous la forme d'une somme de cinq nombres entiers :

$$a = a1 + a2 + a3 + a4 + a5,$$

$$b = b1 + b2 + b3 + b4 + b5, \text{ etc.}$$

Chacun communique aux quatre autres un des quatre termes de sa décomposition. Par exemple, A recevra les nombres $b1$, $c1$, $d1$ et $e1$, B recevra $a2$, $c2$, $d2$ et $e2$, etc. La personne A additionne le nombre $a1$ qu'elle n'a pas communiqué, aux quatre qu'elle a reçu et obtient $N1 = a1 + b1 + c1 + d1 + e1$; la personne B additionne $a2 + b2 + c2 + d2 + e2 = N2$, etc. Remarquez que $N1 + N2 + N3 + N4 + N5 = a + b + c + d + e = N$.

Les participants se communiquent alors $N1$, $N2$, $N3$, $N4$ et $N5$ et calculent chacun de leur côté la somme $N1 + N2 + N3 + N4 + N5 = N$.

Si N est «un multiple de 6», c'est que tous ont voté OUI ; si N est «un multiple de 6 plus 1», c'est qu'il y a eu un vote NON ; si N est «un multiple de 6 plus 2», c'est qu'il y a eu deux votes NON, etc.

Si toutes les opérations se déroulent normalement, aucun des participants au vote ne dispose d'informations sur le vote des autres, en dehors de celles déduites normalement du résultat. En effet, connaître la valeur de $b1$ (ce qui est la seule chose que A connaisse du vote de B) ne fournit aucune indication sur le reste de la division par 6 de $b = b1 + b2 + b3 + b4 + b5$, et donc A ne connaît rien du vote de B. Par symétrie, aucun participant ne peut tirer quoi que ce soit concernant le vote des autres des informations qu'il a eues entre les mains.

Nous avons supposé que les participants étaient honnêtes, mais il est inté-

3. LE VOTE PAR TÉLÉPHONE

Comment 5 personnes peuvent-elles voter une motion par téléphone en préservant le secret du vote ?

Pour voter OUI, choisir un multiple de 6 (par exemple 60)

Pour voter NON, choisir un multiple de 6 plus 1 (par exemple 37)

A vote OUI : il choisit 60 qu'il décompose en $\boxed{3} + \boxed{12} + \boxed{30} + \boxed{7} + \boxed{8}$

B vote NON : il choisit 37 qu'il décompose en $\boxed{3} + \boxed{11} + \boxed{11} + \boxed{6} + \boxed{6}$

C vote OUI : il choisit 30 qu'il décompose en $\boxed{10} + \boxed{2} + \boxed{8} + \boxed{5} + \boxed{5}$

D vote NON : il choisit 19 qu'il décompose en $\boxed{3} + \boxed{3} + \boxed{3} + \boxed{9} + \boxed{1}$

E vote OUI : il choisit 42 qu'il décompose en $\boxed{10} + \boxed{11} + \boxed{12} + \boxed{8} + \boxed{1}$

(les décompositions sont arbitraires et laissées au choix de chacun)

La somme est $60 + 37 + 30 + 19 + 42 = 188 = 31 \times 6 + 2$.

Le 2 indique le nombre de NON.

Les nombres de la colonne 1 sont envoyés à A, qui les additionne

$$\boxed{3} + \boxed{3} + \boxed{10} + \boxed{3} + \boxed{10} = 29 = N1$$

Les nombres de la colonne 2 sont envoyés à B, qui les additionne

$$\boxed{12} + \boxed{11} + \boxed{2} + \boxed{3} + \boxed{11} = 39 = N2$$

Les nombres de la colonne 3 sont envoyés à C, qui les additionne

$$\boxed{30} + \boxed{11} + \boxed{8} + \boxed{3} + \boxed{12} = 64 = N3$$

Les nombres de la colonne 4 sont envoyés à D, qui les additionne

$$\boxed{7} + \boxed{6} + \boxed{5} + \boxed{9} + \boxed{8} = 35 = N4$$

Les nombres de la colonne 5 sont envoyés à E, qui les additionne

$$\boxed{8} + \boxed{6} + \boxed{5} + \boxed{1} + \boxed{1} = 21 = N5$$

Les nombres $N1$, $N2$, $N3$, $N4$, $N5$ sont rendus publics.

La somme $N1 + N2 + N3 + N4 + N5$ est calculée. Le résultat est $188 = 6 \times 31 + 2$, et ainsi chaque participant connaît le résultat du vote sans connaître le vote des autres participants.



ressant de savoir si le système proposé est robuste aux tentatives de tricheries.

Deux possibilités de tricherie sont à envisager. Lorsque les cinq personnes font connaître les nombres $N1$, $N2$, $N3$, $N4$ et $N5$, si l'une d'entre elles, par exemple E, connaît les quatre autres résultats avant d'indiquer le sien, elle peut tricher en choisissant d'indiquer pour $N5$ un nombre qui donne une somme $N = N1 + N2 + N3 + N4 + N5$ conforme au résultat qu'elle souhaite. Ce risque est facile à écarter : il suffit, lors de l'échange des nombres $N1$, ..., $N5$, de procéder en deux temps. D'abord A communique $N1$ à B uniquement, B communique $N2$ à C uniquement... E communique $N5$ à A uniquement. Ensuite les nombres sont communiqués à tous. Personne, au moment où il divulgue son nombre, ne connaît tous les autres, donc personne ne peut forcer N à être comme il le désire.

Une autre tricherie est à envisager : un des participants pourrait choisir un nombre qui soit «un multiple de 6 plus 2», ce qui revient pour lui à voter deux fois NON. Toutefois, ce type de tricherie se retournera contre le tricheur si les quatre autres participants choisissent le NON, car alors il y a un total de 6 NON, apparaissant comme un vote à l'unanimité pour le OUI (puisque la somme $N1 + N2 + N3 + N4 + N5$ est un multiple de 6). Un tel résultat serait contraire au désir du tricheur (qui veut faire gagner

le NON). De plus, cette tricherie serait détectée par chaque participant puisque, ayant voté NON, il s'attendra à découvrir, lors du dépouillement, un NON au moins. Lorsqu'une telle tricherie est découverte, les participants, s'ils acceptent de lever le secret du vote, donc de communiquer les nombres qu'ils ont utilisés, sont en mesure de savoir qui a triché. Cette tricherie est donc doublement risquée pour le tricheur : il peut faire gagner le OUI et il est susceptible de se faire repérer. On pourra raisonnablement supposer que personne ne se laisse tenter.

Jean Paul DELAHAYE est directeur adjoint du Laboratoire d'informatique fondamentale de Lille du CNRS.

James ASPNES, Richard BEIGEL, Merrick FURST et Steven RUDICH, *The Expressive Power of Voting Polynomials*, 23rd Annual ACM Symposium on Theory of Computing, 1991, pp. 402-409.

Douglas BLAIR et Robert POLLACK, *La logique du choix collectif*, in *Pour La Science*, p. 104-111, octobre 1993.

Gilles COHEN, *Mathématiques du citoyen : élections piège à...* *Matheux*, in *Tangente*, n° 30, pp. 12-15, janvier-février 1993.

Nicholas FALLETTA, *Le livre des paradoxes*, chapitre 5, éditions Belfond, 1985.