

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 :

$$a = a_1 + a_2 + a_3 + a_4 + a_5,$$

$$b = b_1 + b_2 + b_3 + b_4 + b_5, \text{ etc.}$$

Chacun communique aux quatre autres un des quatre termes de sa décomposition. Par exemple, A recevra les nombres b_1 , c_1 , d_1 et e_1 , B recevra a_2 , c_2 , d_2 et e_2 , etc. La personne A additionne le nombre a_1 qu'elle n'a pas communiqué, aux quatre qu'elle a reçus et obtient $N_1 = a_1 + b_1 + c_1 + d_1 + e_1$; la personne B additionne $a_2 + b_2 + c_2 + d_2 + e_2 = N_2$, etc. Remarquez que $N_1 + N_2 + N_3 + N_4 + N_5 = a + b + c + d + e = N$.

Les participants se communiquent alors N_1 , N_2 , N_3 , N_4 et N_5 et calculent chacun de leur côté la somme $N_1 + N_2 + N_3 + N_4 + N_5 = N$.

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 b_1 (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 $b = b_1 + b_2 + b_3 + b_4 + b_5$, 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 $3 + 12 + 30 + 7 + 8$

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

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

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

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

(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

$$3 + 3 + 10 + 3 + 10 = 29 = N_1$$

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

$$12 + 11 + 2 + 3 + 11 = 39 = N_2$$

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

$$30 + 11 + 8 + 3 + 12 = 64 = N_3$$

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

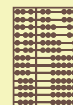
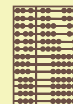
$$7 + 6 + 5 + 9 + 8 = 35 = N_4$$

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

$$8 + 6 + 5 + 1 + 1 = 21 = N_5$$

Les nombres N_1 , N_2 , N_3 , N_4 , N_5 sont rendus publics.

La somme $N_1 + N_2 + N_3 + N_4 + N_5$ 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 N_1 , N_2 , N_3 , N_4 et N_5 , 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 N_5 un nombre qui donne une somme $N = N_1 + N_2 + N_3 + N_4 + N_5$ conforme au résultat qu'elle souhaite. Ce risque est facile à écarter : il suffit, lors de l'échange des nombres N_1 , ..., N_5 , de procéder en deux temps. D'abord A communique N_1 à B uniquement, B communique N_2 à C uniquement... E communique N_5 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 $N_1 + N_2 + N_3 + N_4 + N_5$ 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.