Preuves de l'énigme du Sphinx

Vincent Cremet

20 octobre 2003

Résumé

Ce document regroupe les plus belles preuves de l'énigme du Sphinx.

1 L'énigme

On suppose que n joueurs ($n \geq 3$) sont disposés autour d'une table ronde et on répartit $(n-1)$ cartes parmi eux. A chaque tour de jeu, un joueur qui, au début du tour, possède deux cartes ou plus, en passe une à son voisin de gauche et une à son voisin de droite. Un joueur qui, au début du tour, possède zéro ou une carte ne fait rien. La partie se termine quand aucun joueur ne peut plus passer de cartes. Le but est de montrer que la partie se termine quelle que soit la distribution initiale des cartes.

2 Preuve de Aart Blokhuis

La preuve qui suit est une reformultation de celle donnée par Aart Blokhuis, simplifiée par Sébastien Briais et l'auteur.

2.1 Jeu simultané et jeu séquentiel

Dans le jeu présenté dans l'énigme, tous les joueurs jouent simultanément. Autrement dit, leur capacité à donner ou non des cartes pendant un tour est liée uniquement aux cartes qu'ils avaient en main au début du tour et non à celles qu'ils auraient peu recevoir pendant ce tour. Mais on pourrait aussi inventer un autre jeu dans lequel, à chaque tour, seul un joueur, choisi au hasard parmi ceux possédant deux cartes ou plus, pourrait jouer. On désignera maintenant le premier jeu comme le *jeu simultané* et le deuxième comme le *jeu séquentiel*. Il faut remarquer que, contrairement au jeu simultané, le jeu séquentiel n'est pas déterministe, car pour une même distribution initiale des cartes, plusieurs parties sont possibles selon le choix à chaque tour du joueur qui passera des cartes.

Maintenant il est temps d'énoncer notre premier résultat :

Lemme 1 *Si toutes les parties du jeu séquentiel se terminent, alors la partie du jeu simultané se termine aussi.*

Preuve

La preuve est basée sur le fait qu'on peut simuler un tour du jeu simultané par plusieurs tours du jeu séquentiel. En effet il suffit de noter, au début du tour du jeu simultané tous les joueurs qui *doivent* passer des cartes, et de les faire jouer l'un après l'autre. Il est clair que si chacun de ces joueurs a *pu* jouer, alors on aura à la fin une distribution des cartes parmi les joueurs égale à celle qu'on aurait obtenue en effectuant le tour du jeu simultané. Et durant ce processus, un joueur qui *doit* jouer mais qui ne l'a pas encore fait ne peut pas avoir moins de cartes qu'au début, donc il *pourra* effectivement jouer lorsque son tour viendra.

Maintenant, supposons qu'il existe une partie infinie du jeu simultané. Comme chaque tour du jeu simultnané correspond à un ou plusieurs tours du jeu séquentiel, on aura aussi une partie infinie du jeu séquentiel.

Cqfd

Fort de ce résultat, on se contentera dans la suite de montrer le théorème suivant.

Theorem 2.1 Toutes les parties du jeu séquentiel se terminent.

2.2 Quelques définitions

Soit n le nombre de joueurs autour de la table. Ayant numéroté les joueurs de 1 à n, on représente une configuration du jeu par une suite de longueur n d'entiers, l'entier à la position i correspondant au nombre de cartes détenues par le joueur i. Par exemple, dans la configuration suivante :

$$03022000$$

le premier joueur a 0 cartes, le second 3 cartes. etc.

Remarquons tout de suite qu'on peut totalement ordonner les configurations en utilisant l'ordre lexicographique sur les suites d'entiers. On note $\leq$ cet ordre.

On dira que deux configurations v et w sont *équivalentes*, et on notera $v \equiv w$ si l'on peut passer de l'une à l'autre en décalant toutes les cartes d'un même nombre de joueurs. Par exemple, les configurations 03022000 et 22000030 sont équivalentes. On définit ainsi une relation d'équivalence sur les configurations pour laquelle chaque classe d'équivalence a exactement n éléments. On appelera *représentant* d'une configuration v, noté $\overline{v}$, la configuration de sa classe d'équivalence la plus petite pour l'ordre $\leq$ (on a $\overline{v} = v_i v_{i+1} \dots v_{i-1}$ pour une certain i). On dira aussi qu'une configuration v est *minimale* si $v = \overline{v}$. Enfin on appelera *réduction* l'action de passer d'une configuration à une autre en effectuant un tour du jeu séquentiel, et on dira qu'une configuration est *réductible* s'il est possible d'y effectuer une réduction.

2.3 Croissance

Dans l'exemple suivant, on montre le déroulement d'une partie séquentielle, avec pour chaque configuration atteinte son représentant :

020012	(001202)
101012	(010121)
201020	(010202)
201101	(011012)
011102	(011102)
111110	(011111)

On voit que dans le déroulement de cette partie séquentielle, la suite des représentants est strictement croissante pour l'ordre lexicographique $\leq$.

Si on arrive à montrer que c'est en fait vrai pour *toute* partie séquentielle, alors on aura fini la preuve. En effet, supposons qu'on aie une partie infinie du jeu séquentiel. On aurait alors une suite infinie strictement croissante de configurations : la suite $(\overline{v_i})_i$ des représentants. Comme cette suite est infinie et qu'il n'y a qu'un nombre fini de configurations, forcément elle repasse par une même configuration. Autrement dit, il existe k et l ($k < l$) tels que $\overline{v}_k = \overline{v}_l$. Mais par transitivité, on a aussi $\overline{v}_k < \overline{v}_l$, ce qui est contradictoire.

Jusqu'à maintenant, on a réussi à ramener le problème de la terminaison du jeu simultané à la preuve du théorème suivant.

Theorem 2.2 Etant donné deux configurations v et w, si $v \to w$ alors $\overline{v} < \overline{w}$.

Dans le théorème ci-dessus, $v \to w$ signifie que w est une configuration atteinte en un tour de jeu séquentiel à partir de v.

On va maintenant donner une démonstration de ce théorème et cela achèvera notre preuve.

Mais auparavant on a encore besoin du lemme fondamental suivant qui caractérise les configurations réductibles minimales.

2.4 Caractérisation

Lemme 2 *Si v est réductible et minimale, alors v peut s'écrire 01^k0a avec $k \geq 0$ et a un mot quelconque.*

Preuve

Si on arrive à montrer que toute configuration réductible v est équivalente à une configuration de la forme 01^k0a, alors on aura fini. En effet, si $v = 01^k0a$, comme $\overline{v} \leq v$, $\overline{v}$ est forcément aussi de cette forme.

Soit v une configuration réductible. Il est facile de voir qu'on peut construire une configuration équivalente à v de la forme $0a_1 \ldots 0a_p$, c.-à-d. consistant en une suite de séquences $0a_i$ où a_i est un bloc, éventuellement vide, de joueurs possédant au moins une carte. De plus comme v est réductible, elle contient au moins deux zéros et donc forcément $p \geq 2$.

Raisonnons maintenant par l'absurde. Supposons que chaque bloc a_i soit non vide et contienne un joueur avec strictement plus d'une cartes, on pourrait alors lui prendre une carte et la donner au joueur qui précède le bloc. On obtiendrait ainsi une configuration où chaque joueur possède au moins une carte, ce qui est impossible avec $n-1$ cartes pour n joueurs.

Cqfd

Remarquez que la preuve de ce lemme utilise explicitement l'hypothèse fondamentale qui dit qu'il y a une carte de moins que de joueurs.

2.5 Conclusion

Il est temps maintenant de conclure notre preuve.

Soient v et w deux configurations telles que $v \to w$. On veut montrer que $\overline{v} < \overline{w}$.

Si w est irréductible, alors $\overline{w} = 01...1$, et clairement $\overline{v}$ est strictement plus petit que $\overline{w}$, car par le lemme précédent, $\overline{v} = 01^k0a$ avec $k < n-1$.

On considère maintenant le cas où w est réductible.

Par le lemme précédent, on sait que $\overline{v}$ et $\overline{w}$ ont une forme bien particulière :

$$\begin{array}{rcll} \overline{v} & = & 01^k0a & (k \geq 0) \\ \overline{w} & = & 01^l0b & (l \geq 0) \end{array}$$

On s'intéresse maintenant à la portion initiale 01^l0 de $\overline{w}$ et on distingue deux cas.

Cas 1 : Cette portion n'a pas été modifiée par la réduction. Autrement dit, elle existait déjà dans v et n'a reçu aucune carte pendant la réduction.

On considère la configuration $v' = 01^l0a'$ équivalente à v dans laquelle cette portion est en tête. Comme $\overline{v}$ est minimale, on a $\overline{v} \leq v'$.

Mais on a aussi

$$v' = 01^l0a' < 01^l0b = \overline{w}$$

car b est égal à a' dans laquelle on a effectué une réduction.

Cas 2 : La portion 01^l0 a été *créée* par la réduction.

Dans ce cas il suffit d'énumérer toutes les possibilités de créer une telle séquence pendant une réduction. Il y en a en fait trois :

minimalité de $\overline{v}$	v	$\rightarrow$	w	l
$l' \geq k$	$\ldots 01^{l'}02 \ldots$	$\rightarrow$	$\ldots 01^{l'+1}0 \ldots$	$l'+1$
$l' \geq k$	$\ldots 201^{l'}0 \ldots$	$\rightarrow$	$\ldots 01^{l'+1}0 \ldots$	$l'+1$
$l_1 \geq k$, $l_2 \geq k$	$\ldots 01^{l_1}0301^{l_2}0 \ldots$	$\rightarrow$	$\ldots 01^{l_1+l_2+3}0 \ldots$	l_1+l_2+3

Les propriétés apparaissant dans la première colonne sont justifiées par la minimalité de $\overline{v}$.

Dans la dernière colonne, on a la valeur de l dans chaque cas et on peut montrer en utilisant les inégalités de la première colonne que $k < l$, ce qui a pour conséquence que $\overline{v} < \overline{w}$.

Cqfd

3 Preuve de Geoff Bailey

La preuve qui suit est une simplification par l'auteur de la preuve de Geoff Bailey (Fred the Wonder Worm) postée sur le forum *rec.puzzle*.

On peut décomposer la preuve en trois grandes étapes :

- Montrer que l'on peut se ramener au jeu séquentiel (voir preuve précédente).
- Montrer que s'il existe une partie du jeu séquentiel qui se termine, alors toutes les parties du jeu séquentiel se terminent.
- Montrer qu'il existe *une* partie du jeu séquentiel qui se termine.

On se contentera ici de traiter les deux derniers points.

3.1 Longueur d'une partie

Lemme 3 *Pour une configuration initiale donnée, s'il existe une partie du jeu séquentiel qui se termine, alors toutes les parties du jeu séquentiel se terminent.*

Preuve

L'idée originale de cette preuve est de comptabiliser le nombre de fois où un joueur a joué.

On suppose qu'il existe une partie du jeu séquentiel qui se termine. On raisonne maintenant par l'absurde : supposons qu'il existe une partie du jeu séquentiel qui ne se termine pas. Alors il existe forcément un joueur qui a joué plus de fois dans la partie infinie que dans la partie finie (car si aucun joueur n'a joué plus de coups, la partie infinie n'est pas plus longue que la partie finie, ce qui est absurde). On s'intéresse maintenant au tour crucial de la partie infinie où pour la première fois il existe un joueur, appelons le A, qui va dépasser en jouant à ce tour le nombre de coups a qu'il a joué dans la partie finie. Soient b et c le nombre de coups que ses deux voisins ont joué dans la partie finie. Au début du tour de la partie infinie en question, le joueur A a donc déjà joué a fois. Si ses voisins ont déjà joué b_0 et c_0 fois, alors forcément $b_0 \leq b$ et $c_0 \leq c$ car A est le premier joueur à dépasser, dans la partie infinie, le nombre de coups qu'il a joué dans la partie finie.

Maintenant, intéressons nous au nombre $w(A)$ de cartes détenues par le joueur A au début de ce tour du jeu infini. Si $v(A)$ est le nombre de cartes initialement détenues par le joueur A, on a

$$w(A) = v(A) - 2a + b_0 + c_0$$

Comme $b_0 \leq b$ et $c_0 \leq c$, on peut déduire que

$$w(A) \leq v(A) - 2a + b + c$$

Or $v(A) - 2a + b + c$ est aussi le nombre de cartes détenues par le joueur A à la fin de la partie finie, c'est-à-dire 0 ou 1 vu que la partie est finie.

On en déduit qu'au début de ce tour de la partie infinie, le joueur A possède 0 ou 1 cartes. Autrement dit il ne peut pas jouer, ce qui est absurde.

Cqfd

Il faut noter que cette preuve peut être facilement adaptée pour montrer que toutes les parties séquentielles ont la même longueur. Et elle marche également avec n cartes pour n joueurs. En effet la seule hypothèse que l'on fait sur le nombre totale de cartes est que, à la fin d'une partie, chaque joueur possède une carte ou moins.

3.2 Existence d'une partie qui termine

Lemme 4 *Pour toute distribution initiale des cartes, il existe une partie du jeu séquentiel qui se termine.*

Preuve

On montre que pour toute configuration réductible, il existe une séquence finie de coups qui permet d'atteindre une autre configuration contenant strictement moins de joueurs sans carte. Comme on ne peut pas faire décroître indéfinement le nombre de joueurs sans carte, il est clair qu'en répétant la procédure on atteint un jour une configuration irréductible.

Mais tout d'abord quelques définitions : on appelle *bloc* un ensemble de joueurs consécutifs qui possèdent tous au moins une carte et qui sont entourés par deux joueurs sans carte. Un joueur *riche* est un joueur pouvant jouer, c.-à-d. un joueur détenant au minimum deux cartes. Un *bloc* riche est un joueur contenant au moins un joueur riche.

On définit une fonction f qui prend en arguments une configuration réductible et un bloc riche de cette configuration et qui renvoie la suite de réductions permettant d'atteindre une configuration avec strictement moins de joueurs sans cartes.

Dans la suite on représente l'action de réduire une configuration par la notation

$$\ldots a \ldots \quad \rightarrow \quad \ldots b \ldots$$

La partie à gauche de la flèche représente la configuration initiale et la partie à droite de la flèche la configuration obtenue après avoir effectué la réduction. Les pointillés représentent les parties d'une configuration qui n'ont pas été affectée par la réduction. a est une suite de joueurs parmi lesquels se trouve le joueur qui a joué, et b correspond à cette même suite de joueurs après le coup.

De la même manière, on représente plusieurs étapes de réductions par

$$\ldots a \ldots \quad \rightarrow^{+} \quad \ldots b \ldots$$

Définition de f Soit donc v une configuration réductible et b un bloc riche de v (représentable par l'indice de son joueur le plus à gauche).

L'idée de la fonction f est de répéter l'opération consistant à faire jouer le joueur le plus à gauche dans le bloc, jusqu'à obtenir une configuration avec strictement moins de joueurs sans carte. La suite n'est qu'une formalisation mathématique de cette idée avec une preuve de sa correction.

On commence par remarquer qu'un bloc riche est de la forme

$$1^k na$$

où $k \geq 0$, $n \geq 2$ et a est une séquence de longueur l ($l \geq 0$) de joueurs possédant au moins une carte.

On distingue quatre cas en fonction des valeurs de k et l.

Si $k = 0$ **et** $l = 0$, alors

$$f(v, b) \quad = \quad \underbrace{\ldots 0 \overbrace{n}^{b} 0 \ldots}_{v} \rightarrow \underbrace{\ldots 1(n-2)1 \ldots}_{w}$$

Les deux joueurs qui entouraient b ont maintenant une carte chacun et seul le joueur qui a joué a pu passé à zéro cartes (si $n = 2$), donc globalement il y a moins de joueurs sans carte dans w que dans v.

Si $k = 0$ **et** $l > 0$, alors on distingue deux sous-cas.

Si $n > 0$

$$f(v, b) \quad = \quad \underbrace{\ldots 0 \overbrace{na_0a'}^{b} 0 \ldots}_{v} \rightarrow \underbrace{\ldots 1(n-2)(a_o+1)a'0 \ldots}_{w}$$

et il est clair que w contient un joueur de moins sans carte que v.

Par contre, si $n = 2$ le nombre de joueurs sans cartes est resté le même et on appelle récursivement f :

$$f(v,b) \quad = \quad \underbrace{\dots 0\,\overbrace{na_0a'}^{b}\,0\dots}_{v} \to \underbrace{\dots 1(n-2)\,\overbrace{(a_0+1)a'}^{b'}\,0\dots}_{w}, f(w,b')$$

Il est important de noter que b' est un bloc riche car $a_0 \geq 0$ et qu'il est strictement plus court que b.

Si $k > 0$ **et** $l = 0$, alors

$$f(v,b) \quad = \quad \underbrace{\dots 0\,\overbrace{1^k n}^{b}\,0\dots}_{v} \to^+ \underbrace{\dots 101^{k-1}(n-1)1\dots}_{w}$$

Dans cette suite de réductions, on a fait jouer le joueur avec n cartes, puis son voisin gauche, puis le voisin gauche de son voisin gauche, etc, jusqu'à atteindre le joueur sans carte en bordure du bloc. On voit que w possède un joueur sans carte de moins que v.

Si $k > 0$ **et** $l > 0$, alors

$$f(v,b) \quad = \quad \underbrace{\dots 0\,\overbrace{1^k na_0a'}^{b}\,0\dots}_{v} \to^+ \underbrace{\dots 10\,\overbrace{1^{k-1}(n-1)(a_0+1)a'}^{b'}\,0\dots}_{w}, f(w,b')$$

Dans ce dernier cas, on a appliqué la même séquence de réductions que dans le cas précédent, mais le nombre de joueurs sans carte est resté inchangé. On rappelle donc récursivement f sur la configuration w avec un bloc riche b' strictement plus court que b.

Conclusion Il est facile de voir que la fonction f est bien définie car les appels récursifs se font toujours avec comme argument un bloc strictement plus court. De plus on peut montrer par récurrence que la configuration finale contient strictement moins de joueurs sans carte que la configuration intiale.

Cqfd