Implémentation Bayésienne et réseaux de communication

Ludovic Renou[1], Tristan Tomala[2]

[1] University of Leicester
lr78@le.ac.uk
[2] HEC Paris
tomala@hec.fr

Mots-Clés : *Jeux Bayésiens, Cryptographie, Réseaux.*

1 Introduction

Cet article étudie la communication fiable et sécurisée dans un réseau, entre plusieurs émetteurs et un récepteur. Le récepteur est un centre de décision, les émetteurs sont des joueurs rationnels qui possèdent chacun une information privée et partielle sur l'état du monde. Chaque joueur cherche à maximiser son paiement qui dépend de l'état du monde et de la décision du récepteur. La théorie de l'implémentation étudie les fonctions des états vers les décisions qui sont induites par des équilibres Nash-Bayésiens de jeux de transmission d'information entre les émétteurs et le récepteur. Une telle fonction doit nécéssairement vérifier les contraintes d'incitation : chaque joueur préfère annoncer son vrai type à l'équilibre (IC).

Si chaque joueur est relié au récepteur par un canal de communication privé, toute fonction IC est implémentable par un jeu de communication directe et privée entre le récepteur et chaque émetteur. Toutefois, dans beaucoup d'interactions économiques, les agents sont des noeuds distants dans un réseau de communication. Le but de cet article est de caractériser les réseaux qui permettent d'implémenter toutes les fonctions IC par de la communication dans le réseau.

2 Modèle

On se donne un ensemble $N := \{1, \dots, n\}$ de joueurs (les émetteurs) et un récepteur (le joueur 0). Chaque joueur $i \in N$ est informé de son type $\theta_i \in \Theta_i$, Θ_i étant un ensemble fini. On note $\Theta := \times_i \Theta_i$ and $\Theta_{-i} := \times_{j \neq i} \Theta_j$. Un état du monde est un profil de types $\theta \in \Theta$. Un joueur i de type θ_i a une croyance $P_i(\cdot|\theta_i)$ sur Θ_{-i} et on suppose $P_i(\theta_{-i}|\theta_i) > 0$ pour tout $(\theta_i, \theta_{-i}) \in \Theta$, $i \in N$. Soit A un ensemble fini d'actions pour le récepteur. Chaque joueur i a une fonction de paiement $u_i : A \times \Theta \to \mathbb{R}$. L'ensemble de ces données sera appelé *environnement* par la suite et on suppose qu'il existe une *action dominée* $\underline{a}$ telle que $u_i(\underline{a}, \theta) < u_i(a, \theta)$ pour tous $a \in A \setminus \{\underline{a}\}$, $\theta \in \Theta$, et $i \in N$.

Une fonction de choix social $f : \Theta \to A$ vérifie les *contraintes d'incitation* (IC) si pour chaque

joueur $i \in N$, et pour tout θ_i, θ'_i :

$$\sum_{\theta_{-i}} u_i(f(\theta_i, \theta_{-i}), \theta_i, \theta_{-i}) P_i(\theta_{-i}|\theta_i) \geq \sum_{\theta_{-i}} u_i(f(\theta'_i, \theta_{-i}), \theta_i, \theta_{-i}) P_i(\theta_{-i}|\theta_i).$$

Réseau de communication. On se donne un graphe orienté $\mathcal{N}$ dont les $n+1$ noeuds sont les joueurs et le récepteur. Une arète orientée ij indique que i peut envoyer un message à j de manière fiable et sécurisée. On note $C(i) = \{j \in N \cup \{0\} : ij \in \mathcal{N}\}$ l'ensemble des joueurs à qui i peut envoyer un message et $D(i) = \{j \in N \cup \{0\} : ji \in \mathcal{N}\}$ l'ensemble des joueurs qui peuvent envoyer un message à i. On suppose que le graphe est fortement 1-connexe dans le sens suivant : pour tout $i \in N$, il existe un chemin orienté de i vers 0. On suppose de plus que le graphe est acyclique. Par conséquence, $ii \notin \mathcal{N}$ et $C(0) = \emptyset$, le récepteur n'envoie pas de messages.

Un jeu de communication $G_{\mathcal{N}}$ sur le réseau se déroule comme suit : 1) les joueurs apprennent leur type, 2) chaque joueur i attend de recevoir un message de chaque $j \in D(i)$ et envoie un message à chaque $j \in C(i)$, 3) 0 attend de recevoir un message de chaque $j \in D(0)$ et choisit une action.

Grâce à l'acyclicité, l'instant $t(i)$ auquel i envoie ses messages est bien défini. Dans ce jeu, chaque joueur ne parle qu'une fois.

Définition 1 *La fonction de choix social f est implémentable sur le réseau $\mathcal{N}$ si il existe un équilibre Nash-Bayésien σ^* de $G_{\mathcal{N}}$ tel que pour tout état $\theta \in \Theta$, $g((m^*_{i0})_{i \in D(0)}) = f(\theta)$ quel que soit le profil de messages $(m^*_{i0})_{i \in D(0)}$ reçus par le récepteur avec probabilité positive à l'équilibre dans l'état θ.*

3 La caractérisation

Le graphe $\mathcal{N}$ est *faiblement 2-connexe* si pour tout joueur $i \in N \setminus D(0)$, il deux chemins disjoints de i à 0 dans le graphe non-orienté associé à $\mathcal{N}$.

Théorème 1 *Toute fonction IC est implémentable sur $\mathcal{N}$, pour tout environnement avec action dominée, si et seulement si, $\mathcal{N}$ est faiblement 2-connexe.*

Pour démontrer ce résultat, on construit un protocole de communication tel que : a) le récepteur apprend l'état du monde, b) aucun joueur n'apprend les types des autres joueurs, c) une déviation unilatérale du protocole est détectée avec probabilité arbitrairement grande par le récepteur. On utilise d'une part des techniques de codages probabilistes, et d'autre part on montre qu'un graphe faiblement 2-connexe, fortement 1-connexe et acyclique se décompose en une juxtaposition de sous-graphes fortement 2-connexes.

Références

[1] Danny Dolev, Cynthia Dwork, Orli Waarts and Moti Yung, *Perfectly Secure Message Transmission*, Journal of the ACM, 1993, 40, pp. 17–47

[2] Dov Monderer and Moshe Tennenholtz, *Distributed Games : From Mechanisms to Protocols*, Sixteenth National Conference on Artificial Intelligence, 1999, pp. 32–37

[3] Jérôme Renault and Tristan Tomala, *Probabilistic Reliability and Privacy of Communication Using Multicast in General Neighbor Networks*, Journal of Cryptology, 2008, 21, pp. 250-279