# CORRELATION AND AUTHENTICATION IN REPEATED GAMES WITH NETWORK MONITORING

TRISTAN TOMALA

ABSTRACT. We study repeated games with *network monitoring* where players observe the moves of their neighbors. The Folk theorem holds for such a game if every feasible and individually rational payoff is an equilibrium payoff. Renault and Tomala [RT98] prove that given a network, the Folk theorem holds in Nash equilibria for every payoff function if and only if the graph is 2-connected. This paper shows that if players share correlated authentication keys, the connectivity requirement can be relaxed, i.e. the Folk theorem holds in correlated equilibria for every payoff function if and only if the graph is 2-edge-connected. The problem is also formulated in terms of communication protocol construction and the result is similar to others in the computer science literature: the distribution of private authentication keys helps reliability of communication.

VERY PRELIMINARY DRAFT.

## 1. MODEL

The primitive data of our model are given by an undirected graph $G = (V, E)$ and a family of finite sets $(A^i)_{i\in V}$, where: the set of vertices $V$ is a finite set of players with $|V| \geq 3$, $E$ is the set of pairs $(i, j) \in V \times V$ such that there is a link between $i$ and $j$ and $A^i$ is the set of actions available to player $i$ with $\left|A^i\right| \geq 2$. The interpretation is that players $i$ and $j$ *see* or monitor each other: when player $i$ takes an action, $j$ directly observes it, or when player $i$ sends a message to player $j$, this message is recieved securely by $j$. The graph is throughout assumed to be undirected, so the monitoring relation is symmetric.

### 1.1. The repeated game.

To the graph $G = (V, E)$ and the actions sets $(A^i)_{i\in V}$, we add for each player a payoff function $u^i : \prod_{j\in V} A^j (:= A) \to \mathbb{R}$. These data define a *repeated game with imperfect monitoring* as follows.

At each stage $t \in \mathbb{N}\backslash\{0\}$, players choose synchronously actions in their own actions sets. If $a_t = (a_t^j)_{j\in V}$ is chosen, player $i$ observes the actions of its neighbors in the graph $(a^j)_{(i,j)\in E}$. The game proceeds then to stage $t + 1$.

We let $Gi = \{j \in V : (i, j) \in E\}\cup\{i\}$ be the set of players that player $i$ monitors including itself. The set of histories at stage $t$ for player $i$ is $H_t^i = (A^{Gi})^t$. A *pure strategy* for player $i$ is a mapping $s^i : \cup_{t\geq 1} H_t^i \to A^i$ prescribing the actions to play at each stage as a function of past observations. A *behavioral strategy* is a mapping $\sigma^i : \cup_{t\geq 1} H_t^i \to \Delta(A^i)$, the set of probability distributions over $A^i$ prescribing the lottery used to choose the action to play given past observations. A profile of behavior strategies $\sigma = (\sigma^i)_{i\in V}$ induces a probability distribution $\mathbb{P}_\sigma$ over the set of plays of the game, $H = A^{\mathbb{N}}$ endowed with the usual product sigma-field and we shall denote $\mathbb{E}_\sigma$ the correspondig expectation operator.

**Definition 1.1.** *A profile of behavior strategies $\sigma = (\sigma^i)_{i\in V}$ is a* uniform equilibrium *of the repeated game induced by $(G, (A^i)_{i\in V}, (u^i)_{i\in V})$ if:*

---

*Date*: June 19, 2007.

(1) *For all $i$ in $V$, $\lim_n \mathbb{E}_\sigma[\frac{1}{n}\sum_{t=1}^n u^i(a_t)] = x^i$ exists;*
(2) *For all $\varepsilon > 0$, $\exists N$, such that for all $n \geq N$, for all $i$ and strategy $\tau^i$:*

$$\mathbb{E}_{\tau^i,\sigma^{-i}}[\frac{1}{n}\sum_{t=1}^n u^i(a_t)] \leq \mathbb{E}_\sigma[\frac{1}{n}\sum_{t=1}^n u^i(a_t)] + \varepsilon$$

*The vector $x = (x^i)_{i\in V}$ is an* equilibrium payoff. *The set of equilibrium payoffs induced by $(G, (A^i)_{i\in V}, (u^i)_{i\in V})$ shall be denoted $E(u)$ with $u = (u^i)_{i\in V}$.*

1.2. **Correlated equilibria.** The main equilibrium concept of this paper is the correlated equilibrium (introduced by Aumann [Aum74]). We shall focus on *normal form* correlated equilibria where players receive correlated inputs only before the game is played.

A *correlation device* is a product of measurable spaces $(\Omega, \mathcal{F}) = (\prod_{i\in V}\Omega_i, \otimes_{i\in V}\mathcal{F}_i)$ endowed with a probability measure $P$ and we let $c = (\Omega, \mathcal{F}, P)$. The game extended by the device proceeds as follows: at a preliminary stage, the device selects $\omega = (\omega_i)_{i\in V}$ according to $P$ and player $i$ is informed of $\omega^i$. The repeated game is then played. In the extended game, a (behavioral) strategy for player $i$ is a measurable mapping $f^i : \Omega^i \to \Sigma^i$ where $\Sigma^i$ is the set of strategies in the repeated game. The probability measure $P$ and the strategy profile $f = (f^i)_{i\in V}$ induce a probability distribution $\mathbb{P}_{P,f}$ on $\Omega \times H$.

**Definition 1.2.** *A* correlated equilibrium *of the repeated game induced by $(G, (A^i)_{i\in V}, (u^i)_{i\in V})$ is a pair $(c, f)$ where $c$ is a correlation device and $f$ is a strategy profile in the extended game such that:*

(1) *For all $i$ in $V$, $\lim_n \mathbb{E}_{P,f}[\frac{1}{n}\sum_{t=1}^n u^i(a_t)] = x^i$ exists;*
(2) *For all $\varepsilon > 0$, $\exists N$, such that for all $n \geq N$, for all $i$ and strategy $g^i$:*

$$\mathbb{E}_{P,g^i,f^{-i}}[\frac{1}{n}\sum_{t=1}^n u^i(a_t)] \leq \mathbb{E}_{P,f}[\frac{1}{n}\sum_{t=1}^n u^i(a_t)] + \varepsilon$$

*The vector $x = (x^i)_{i\in V}$ is a* correlated equilibrium payoff. *The set of correlated equilibrium payoffs induced by $(G, (A^i)_{i\in V}, (u^i)_{i\in V})$ shall be denoted $C(u)$.*

This notion extends uniform equilibria: if $\sigma$ is a uniform equilibrium, for every correlation device the constant mappings $f^i \equiv \sigma^i$ induce a correlated equilibrium. Therefore $E(u) \subset C(u)$ for every repeated game.

1.3. **Folk theorems.** Given a repeated game, we shall say that the Folk theorem holds for this game when every feasible and individually rational payoff is an equilibrium payoff. More precisely, consider a repated game with actions set $(A^i)_{i\in V}$ and payoff function $(u^i)_{i\in V}$, the *feasible set* is the convex hull of $u(A) = \{(u^i(a))_{i\in V} : a \in A\}$. The *independant minmax level* of player $i$ is:

$$v^i = \min_{\alpha^{-i}\in\prod_{j\neq i}\Delta(A^j)} \max_{a^i\in A^i} g^i(a^i, \alpha^{-i})$$

The *correlated minmax level* of player $i$ is:

$$w^i = \min_{\alpha^{-i}\in\Delta(\prod_{j\neq i}A^j)} \max_{a^i\in A^i} g^i(a^i, \alpha^{-i})$$

The set of feasible and individualy rational payoffs with respect to independant minmax levels is:

$$FIR(u) = \operatorname{co} u(A) \cap \{x \in \mathbb{R}^V : \forall i,\, x^i \geq v^i\}$$

The set of feasible and individualy rational payoffs with respect to correlated minmax levels is:

$$FIRC(u) = \operatorname{co} u(A) \cap \{x \in \mathbb{R}^V : \forall i,\, x^i \geq w^i\}$$

In every game, $w^i \leq v^i$ so $FIR(u) \subset FIRC(u)$. It is also well known that $C(u) \subset FIRC(u)$: every correlated equilibrium payoff is clearly feasible and player $i$ has a strategy that guarantees a payoff no less than $w^i$ at each stage. Indeed, $w^i$ is the value of the two-player zero-sum game where the maximizing player chooses $a^i$, the minimizing player chooses $a^{-i}$ and the payoff is $u^i(a^i, a^{-i})$.

It might however not be the case that $E(u) \subset FIR(u)$....

**Definition 1.3.** (1) *The Folk theorem holds for the repeated game induced by* $(G, (A^i)_{i\in V}, (u^i)_{i\in V})$ *if* $FIR(u) \subset E(u)$.

(2) *The correlated Folk theorem holds for the repeated game induced by* $(G, (A^i)_{i\in V}, (u^i)_{i\in V})$ *if* $FIRC(u) = C(u)$.

Most Folk theorems are proved in a constructive way. Players agree on a contract implementing the target payoff. In case of unilateral deviation from the contract, the deviating player is punished to his minmax level. In games with imperfect monitoring, some players might not observe the deviation. The question is then, can observation be replaced by message exchange within the graph. If the players who are aware of the deviation try to signal it to other player through their actions, will they manage to do it in a reliable way? This typically depends on the connectivity of the graph.

The first results in this line are the following.

**Result 1.** [BPK96]. *In the repeated game induced by* $(G, (A^i)_{i\in V}, (u^i)_{i\in V})$*, if the players are allowed to make* public announcments *between stages, and if each player has two neighbors, then the Folk theorem holds.*

[BPK96] consider a particular case of *communication equilibria* where players are allowed to communicate between stages through a communication device. This concept was proposed for extensive games by [For86], an extensive study of communication equilibria for undiscounted repeated games with imperfect monitoring can be found in [RT04a]. From [RT04a]'s characterization, one can easily rephrase [BPK96]'s result as follows:

*Given the graph $G$ and the action sets, the Folk theorem holds for communication equilibria for every payoff function if and only if each player has two neighbors.*

**Definition 1.4.** *The graph $G$ is* 2-connected *if it is connected and remains connected after deletion of any single vertex.*

Equivalently, the graph is 2-connected if and only if for each pair of vertices $(i, j)$, there are at least two distinct paths from $i$ to $j$.

[RT98] considered uniform equilibria (with no device) and proved the following:

**Result 2.** [RT98]. *Given the graph $G$ and the action sets, the Folk theorem holds for every payoff function if and only if the graph is 2-connected.*

## 2. The main result

This aim of this paper is to study normal form correlated equilibria and to show the type of connectivity needed to get the correlated Folk theorem.

**Definition 2.1.** *The graph $G$ is* 2-edge-connected *if it is connected and remains connected after deletion of any single edge.*

The main result is:

**Theorem 2.2.** *Given the graph $G$ and the action sets, the correlated Folk theorem holds for every payoff function if and only if the graph is 2-edge-connected.*

## References


[Aum74] R.J. Aumann. Subjectivity and correlation in randomized strategies. *Journal of Mathematical Economics*, 1:67–95, 1974.

[BF99] A. Beimel and M. Franklin. Reliable communication over partially authenticated networks. *Theoretical computer science,* 220:185–210 (1999).

[BPK96] E. Ben-Porath and M. Kahneman. Communication in repeated games with private monitoring. *Journal of Economic Theory*, 70:281–297, 1996.

[Ber70] C. Berge. Graphes et Hypergraphes. Editions Dunod, Paris, 1970.

[DDWY] D. Dolev, C. Dwork, O. Waarts and M. Yung. Perfectly secure message transmission. *J. Assoc. Comput. Mach.,*40(1):17-47 (1993).

[For86] F. Forges. An approach to communication equilibria. *Econometrica*, 54:1375–1385, 1986.

[FW00] M. Franklin and R.N. Wright. Secure Communication in minimal connectivity models. *Journal of Cryptology*, 13:9–30, 2000.

[RT98] J. Renault and T. Tomala. Repeated proximity games. *International Journal of Game Theory*, 27:539–559, 1998.

[RT04a] J. Renault and T. Tomala. Communication equilibrium payoffs of repeated games with imperfect monitoring. *Games and Economic Behavior*, In press, 2004.

[RT04b] J. Renault and T. Tomala. Learning the state of nature in repeated game with incomplete information and signals. *Games and Economic Behavior*, 47:124–156, 2004.

[RT05] J. Renault and T. Tomala. Reliability and security of multicast communication in general networks. *Cahier du Ceremade* 0521, 2005.

[Sim92] G.J. Simmons. A survey of information authentication. *In Contemporary Cryptology, The Science of Information Integrity*, G.J. Simmons (ed.), IEEE Press, New York, 441–497, 1992.