Sharing a long secret in a few public words

Olivier Gossner*

N° 2000-15

Thema

Théorie Economique, Modélisation et Applications
UMR 7536 - Centre National de la Recherche Scientifique

Sharing a long secret in a few public words

Olivier Gossner*

N° 2000-15

March, 2000

* THEMA, UMR CNRS 7536

Résumé

Nous considérons un modèle de jeu répété à trois joueurs à information complète et parfaite dans lequel les stratégies des joueurs sont représentées par des machines de Turing en temps polynômial. Nous montrons que s'il existe une collection de permutations trappe, l'ensemble des paiements d'équilibre de ce jeu coincide avec l'ensemble des paiements d'équilibres corréles du jeu répété standard.

Abstract

We consider a 3-player model of repeated game with standard monitoring in which player's strategies are implemented by polynomial time Turing machines. We prove that if a collection of trapdoor permutations exists, the set of equilibria of this game is the set of correlated equilibria of the standard repeated game.

1 Introduction

The assumption that strategic agents have a bounded rationality has led to a recent reconsideration of the set of outcomes that may arise at equilibrium in repeated games (see for instance Aumann and Sorin [2], Neyman [9] [10], Rubinstein [11], BenPorath [3], Gossner [6], Urbano and Vila [13], Hernández and Urbano [7]). Typically, the assumption of bounded rationality implies a limitation on the set of strategies available to the agents. For instance, one may assume that strategies have to be implementable by finite automata of some bounded size, as in the vein of work of Neyman [9] [10] and Rubinstein [11]. In this paper, we assume that agent's strategies must be implementable by polynomial time Turing machines which receive as input at time t the past history up to time t. This model is the most natural one when one wishes to use the tools developped in cryptography such as public-key cryptosystems or pseudo-random generators.

Public-key cryptosystems allow any pair of players to exchange secret messages through public communication. In Gossner [6], we have shown how such cryptosystems could be used between any group of players to coordinate punishments in a repeated game extended by a public communication channel. Here, we consider repeated games with 3 players, full monitoring and no oustide communication channel. Except for the limitation of the strategy spaces, the repeated game we study fits into the standard model of Aumann and Shapley [1], and Rubinstein [12]. The absence of outside communication channel does not entirely preclude communication between players. For instance, Lehrer [8] showed how correlation could result from communication in games with signals. By assuming full monitoring, we impose all communication to be public. By not allowing any oustide public communication channel, we limit the bandwith available to the players and

implicitely introduce a cost for communication.

Pseudo-random generators input random seeds of relatively small size and output long sequences of bits which cannot be distinguished from long sequences of uniformly distributed bits. The idea of this paper is that a pair of players can first use a public-key cryptosystem to exchange a secret seed, and then apply a pseudo-randon generators to this seed in order to expand the duration of coordinated play compared to the time of communication.

Public-key cryptography is possible if there exists a family of trapdoor functions. Pseudo-random generators exist provided there exists a collection of one-way permutations. We follow the construction of Goldreich [5] which combines both ideas assuming the existence of a collection of trapdoor permutation. Assuming there exists such a collection and that player's strategies are implemented by polynomial time Turing machines, we prove that the closure of the set of equilibria of an infinitely repeated game is the set of correlated equilibria of the original repeated game.

We introduce our model of repeated game and the assumption of existence of a family of trapdoor permutations in Section 2. The main results are stated in Section 3. Section 4 is devoted to the proofs.

2 The model

2.1 One-shot game

Let $G = (\{1,2,3\}, (A^i)_i, g)$ be a 3-player game in normal form in which $\{1,2,3\}$ is the set of players, A^i is player i's finite set of actions, and $g : \prod_i A^i \to \mathsf{R}^3$ is the vector payoff function. We let $A = \prod_i A^i$, and for $i \in \{1,2,3\}$, $A^{-i} = \prod_{j \neq i} A^j$. The expression "players $-i$" simply refers to "players other than i".

The min max in correlated strategies w^i for player is defined by the relation:

$$w^i = \min_{s^{-i} \in \Delta(A^{-i})} \max_{a^i \in A^i} \mathsf{E}_{s^{-i}} g^i(a^{-i}, a^i).$$

2.2 Computational complexity

We follow essentially the lines of Goldreich [5] for the treatment of computational complexity, one-way functions, pseudo-random generators and indistinguishable ensembles.

For a finite set X, we let X^* represent the set of finite sequences of elements of X, $X^* = \cup_{n \in \mathsf{N}} X^n$. $1^* = \{1\}^*$ represents the set N in which numbers are coded in unary. $1^n \in \{1\}^n$ is a sequence of n 1's. For $x \in X^*$, the length of x, denoted $|x|$, is the integer such that $x \in X^{|x|}$. $\Omega = \{0,1\}^{\mathsf{N}}$ is endowed with the uniform probability distribution U and is a set of aleas which can be used for randomization by probabilistic algorithms. For any finite set Z, and for any two elements x and y of Z^*, $xy \in Z^*$ denotes the concatenation of x and y. Thus, $|xy| = |x| + |y|$.

Given a finite set X_1, some sets $X_2 \dots X_k$ and Z, we let $M(X_1^*, X_2, \dots, X_k; Z)$ denote the set of applications (or algorithms) from $X_1^* \times X_2 \dots \times X_k$ to Z which are computable in polynomial time (or implementable by polynomial time Turing machines) in the length of the first input, $|x_1|$. When Z is ommited, it is assumed the output is in $\{0,1\}^*$.

The notation Pr stands for probabilities, and $x \sim V$ means that x is a random variable with distribution V. Given V and W, $V \otimes W$ represents the product of the probability distributions V and W. Hence, $x, y \sim V \otimes W$ means $x \sim V$, $y \sim W$, x and y being independent. U_n is the uniform probability over $\{0,1\}^n$.

2.3 Trapdoor one-way permutations

Definition 1 *A* **collection of functions** *is given by a infinite set of* **indices**, $\bar{K}$, *by a finite subset* D_k *of* $\{0,1\}^*$ *for each* $k \in \bar{K}$ *and a function* f_k *over* D_k *for each* $k \in \bar{K}$.

Definition 2 *A collection of functions* $\{f_k : D_k \to \{0,1\}^*\}_{k\in\bar{K}}$ *is called a* **collection of one-way permutations** *if there exists* $K \in M(1^*, \Omega)$, $D \in M(\{0,1\}^*, \Omega)$, $F \in M(\{0,1\}^*, \{0,1\}^*)$, *such that the following conditions hold:*

- *For every* n *and* ω, $K(1^n, \omega) \in \bar{K} \cap \{0,1\}^n$. *For every* $k \in \bar{K}$ *and* ω, $D(k, \omega) \in D_k$. *For every* $k \in \bar{K}$ *and* $x \in D_k$, $F(k, x) = f_k(x)$. *For every* $k \in \bar{K}$, f_k *defines a permutation over* D_k.
- *For every* $g \in M(\{0,1\}^*, \{0,1\}^*, \Omega)$, *every polynomial* p, *and all sufficiently large* n*'s:*

$$\Pr(g(f_{k_n}(x_n), k_n, \omega) \in f_{k_n}^{-1}(f_{k_n}(x_n))) < \frac{1}{p(n)}$$

  where $k_n = K(1^n, \omega')$, $x_n = D(K_n, \omega'')$, $\omega, \omega', \omega'' \sim U \otimes U \otimes U$.

Definition 3 *A* **collection of trapdoor permutations** *is a collection of algorithms* (K_1, K_2, D, F) *such that*

- *The triple* (K_1, D, F) *is a collection of one-way permutations.*
- *There exists* $G \in M(\{0,1\}^*, \{0,1\}^*)$ *such that for every* ω *and* $(k_1, k_2) = (K_1(1^n, \omega), K_2(1^n, \omega))$, *and for every* $x \in D_k$,

$$G(k_2, f_{k_1}(x)) = x.$$

In this last definition, the first condition implies that it is not feasible to compute x from $f_{k_1}(x)$ and k_1. The second condition states that x can be retrieved efficiently from k_2 and $f_{k_1}(x)$. Note that k_1 and k_2 are correlated since they are the outputs of K_1 and K_2 for the *same* ω.

2.4 The repeated game

Let $H_t = (A)^t$ be the set of histories of length t, and recall that $A^* = \cup_t H_t$. Let Σ^i be the set of mappings from A^* to $\Delta(A^i)$. Any triple $\sigma = (\sigma^i) \in \prod_i \Sigma^i$ induces a probability measure $\Pr_\sigma$ on the set of plays $H_\infty = (A)^{\mathsf{N}}$ endowed with the product of the discrete sigma-algebras. Given a Banach limit $\mathcal{L}$, we let

$$g_\infty(\sigma) = \mathsf{E}_{P_\sigma} \mathcal{L}(\frac{1}{T} \Sigma_{t=1}^T g(a_t))_T$$

denote the expectation of the $\mathcal{L}$-limit of the sequence of Cesaro means of the vector payoffs. The standard infinitely repeated version of G is $G_\infty = (\{1,2,3\}, (\Sigma^i)_i, g_\infty)$.

Let $\Sigma^i_{PT} = M(A^*, \Omega; A^i)$ be the set of mappings from A^* to A^i which can be implemented by probabilistic polynomial time algorithms. For each $\omega^i \in \Omega$, $\sigma^i(., \omega^i)$ defines a pure strategy of player i, hence σ^i defines a mixed strategy, and so a behavioral strategy. We therefore identify Σ^i_{PT} to a subset of Σ^i. We shall study the game $G^{PT}_\infty = (\{1,2,3\}, (\Sigma^i_{PT})_i, g_\infty)$, where g_∞ denotes here the restriction of the previously defined mapping to $\prod_i \Sigma^i_{PT}$.

3 The results

Our first result concerns the min max values in G^{PT}_∞. For $i \in \{1,2,3\}$, let $\Sigma^{-i}_{PT} = \prod_{j \neq i} \Sigma^j_{PT}$.

Proposition 4 *If there exists a collection of trapdoor permutations* (K_1, K_2, D, F) *such that* $D(k_1, \omega)$ *is uniformly distributed in* D_{k_1} *when* $\omega \sim U$*, then for every* $i \in \{1, 2, 3\}$*,*

$$\min_{\tau^{-i} \in \Sigma_{PT}^{-i}} \max_{\tau^i \in \Sigma_{PT}^i} g_\infty^i(\tau^i, \tau^{-i}) = w^i$$

For every $\varepsilon > 0$, it is clear that player i can guarantee $w^i - \varepsilon$ by playing repeatedly a mixed strategy that approximates an optimal strategy in the zero sum game in which player i faces the other players as a unique opponent. In the next section, we construct for a given $\varepsilon > 0$ strategies τ_ε^{-i} of players $-i$ such that for every $\tau^i \in \Sigma_{PT}^i$,

$$g_\infty^i(\tau^i, \tau_\varepsilon^{-i}) \leq w^i + \varepsilon.$$

Theorem 5 *If there exists a collection of trapdoor permutations* (K_1, K_2, D, F) *such that* $D(k_1, \omega)$ *is uniformly distributed in* D_{k_1} *when* $\omega \sim U$*, and if* G *admits a vector payoff which is strictly individually rational in correlated strategies, then the closure of the set of equilibrium payoffs of* G_∞^{PT} *is the set of correlated equilibrium payoffs of* G_∞*.*

Proof of Theorem 5 from Proposition 4:

Let $F = \operatorname{co} g(A)$ be the set of feasible payoffs, and $CIR = \{v \in \mathsf{R}^3, \forall i \; v^i \geq w^i\}$ be the set of individually rational payoffs in correlated strategies. The set of correlated equilibrium payoffs of G_∞ is $F \cap CIR$. Since each player can guarantee $w^i - \varepsilon$ for every $\varepsilon > 0$ in G_∞^{PT}, the set of equilibrium payoffs of G_∞^{PT} is a subset of $F \cap CIR$. We need to prove that any element of $F \cap CIR$ can be approximated by equilibrium payoffs of G_∞^{PT}. Because there exists a strictly individually rational payoff in correlated strategies, any payoff in $F \cap CIR$ can be approximated by strictly indivivually rational payoffs in correlated strategies that are rational combinations of payoffs in

$g(A)$. Hence, it is enough to prove that any payoff $v = \frac{1}{l}\sum_{k=1}^{l} a_k$ for $l \in \mathbb{N}$ and $(a_k)_k \in A^l$, such that $v^i > w^i$ for every $i \in \{1,2,3\}$, is an equilibrium payoff of G_∞^{PT}.

To do this, we use the classical construction of equilibrium strategies divided in a Main Path (MP), and a Punishment against player i ($P(i)$).

The Main Path consists of repetitions of the cycle of actions $a_1 \dots a_l$. In case player i deviates from MP, players $-i$ trigger to $P(i)$.

$P(i)$ consists of strategies τ_P^{-i} of players $-i$ such that:

$$\max_{\tau^i \in \Sigma_{PT}^i} g_\infty^i(\tau^i, \tau_P^{-i}) < v^i,$$

the existence of which is provided by the Proposition 4.

Clearly, the above constructed strategies form a Nash equilibrium of G_∞^{PT} with associated Nash payoff v. ¥

4 Proof of Proposition 4

The punishing strategies rely on a method that permits players $-i$ to share a long secret in a few words. More explicitly, we shall define a protocol between players $-i$ starting by some t stages of communication and that allows players $-i$ to play during some $p(t)$ stages in a way that player i cannot distinguish from a *i.i.d.* repetition of the correlated punishing strategies, where p can be arbitrary polynomial. The construction of such protocols relies on pseudo-random generators. First we introduce hard-core predicates for a family of trapdoor permutations and recall their existence. Then, we construct a pseudo-randon generator from a family of trapdoor permutations and a hard-core predicate. We finally construct the punishing strategies and prove that player i cannot gain more than $w^i + \varepsilon$ against those strategies.

4.1 Hard-core predicates

A collection of one-way functions $\{f_k, k \in \bar{K}\}$ may well be such that even if x cannot be found from k and $f_k(x)$, one could guess some bits of x from k and $f_k(x)$. A hard-core predicate is a bit of information which is easily computable from x, but hard to guess (with a probability significantly larger than $\frac{1}{2}$) from k and $f_k(x)$.

Definition 6 *A* **hard-core predicate** *for a collection of functions* $\{f_k : D_k \to \{0,1\}^*\}_{k\in\bar{K}}$ *is an algorithm* $B \in M(\{0,1\}^*;\{0,1\})$ *such that for every* $g \in M(\{0,1\}^*,\{0,1\}^*,\Omega;\{0,1\})$*, for every polynomial* p *and for sufficiently large* n*'s:*

$$\Pr(g(k_n, f_{k_n}(x_n), \omega) = B(x_n)) < \frac{1}{2} + \frac{1}{p(n)}$$

where $k_n = K(1^n, \omega')$*,* $x_n = D(k_n, \omega'')$*,* $\omega, \omega', \omega'' \sim U \otimes U \otimes U$*.*

The following Lemma is a consequence of Theorem 2.5.2 of Goldreich [5].

Lemma 7 *If there exists a collection of trapdoor permutations, there exists a collection of trapdoor permutations with a hard-core predicate.*

4.2 Indistinguishability and pseudo-random generators

Definition 8 *An ensemble indexed by* $\mathbf{N}$*, or simply an* **ensemble***, is a collection of random variables* $X = (x_n)_{n\in\mathbf{N}}$*.*

Definition 9 *Two ensembles* $X = (x_n)_{n\in\mathbf{N}}$ *and* $Y = (y_n)_{n\in\mathbf{N}}$ *are* **indistinguishable in polynomial time** *if all random variables* $(x_n)_{n\in\mathbf{N}}$ *and* $(y_n)_{n\in\mathbf{N}}$ *take their values in the same space* Z^* *and if for every* $D \in M(Z^*, 1^*, \Omega; \{0,1\})$*, every polynomial* p *and for sufficiently large* n*'s:*

$$|\Pr(D(x_n, 1^n, \omega) = 1) - \Pr(D(y_n, 1^n, \omega) = 1)| < \frac{1}{p(n)}$$

where $\omega \sim U$ *is independent of* x_n *and of* y_n*.*

Construction 10 *Let (K_1, D, F) be a collection of one-way permutations, and let B be a hard-core predicate for this collection. For $t \in \mathsf{N}$ and $x \in D_{k_1}$, we define the pseudo-random generator $G_{k_1,t}(x) = \sigma_1 \dots \sigma_t$ by:*

$$\begin{cases} s_0 &= x \\ s_j &= f_{k_1}^{(j)}(x) \quad \textit{for } 1 \leq j \leq t. \\ \sigma_j &= B(s_{j-1}) \end{cases}$$

where $f_{k_1}^{(j)}$ denotes j applications of the function f_{k_1}.

The proof of the next proposition can be found in Goldreich [5], (Proposition 3.4.4 page 94).

Proposition 11 *Let p be an arbitrary polynomial. Assume the distribution of $D(k_1, \omega)$ is uniform in D_{k_1} when $\omega \sim U$. Then the ensembles*

$$(k_{1,n} f_{k_{1,n}}^{(p(n))}(x_n) G_{k_{1,n},p(n)}(x_n))_{n \in \mathsf{N}}$$

and

$$(k_{1,n} f_{k_{1,n}}^{(p(n))}(x_n) u_{p(n)})_{n \in \mathsf{N}}$$

where $k_{1,n} = K_1(1^n, \omega)$, $x_n = D(k_{1,n}, \omega')$, and $u_{p(n)}, \omega, \omega' \sim U_{p(n)} \otimes U \otimes U$, are polynomial time indistinguishable.

In words, this means that no algorithm that inputs $k_{1,n}$ and $f_{k_{1,n}}^{(p(n))}(x_n)$ can distinguish a $p(n)$ bits sequence coming from $G_{k_{1,n},p(n)}$ from a uniform sequence of length $U_{p(n)}$.

4.3 Construction of the min max strategies

Assume for simplicity that $i = 3$. The case in which player 1 or player 2's action set is reduced to one element is trivial since w^i is then equal to the

min max in mixed strategies in G. Hence, we assume that A^1 and A^2 both contain at least two elements. Fix $\varepsilon > 0$, and let $\delta \in \Delta(A^{-3})$ be a distribution with diadic coefficients such that:

$$\max_{a^3} \mathsf{E}_\delta g^3(a^{-3}, a^3) < w^3 + \varepsilon.$$

We select $m \in \mathsf{N}$ and a mapping $\mathrm{cod} : \{0,1\}^m \to A^{-3}$ such that the image of the uniform distribution $\{0,1\}^m$ by cod is δ. Since $D_{k_1} = \{D(i_1, \omega), \omega \in \Omega\}$ for every i_1, and since D is a polynomial algorithm, there exists a polynomial q such that $D_{k_1} \subseteq \cup_{1 \le t \le q(|i_1|)} \{0,1\}^t$. Let p be any polynomial such that $\lim_{n\to\infty} \frac{p(n)}{q(n)} = +\infty$ and such that $p(n) \ge 0$ for $n \ge 0$, (for instance $p = nq$).

In order to introduce a communication protocol between players 1 and 2, we now define codings of messages into actions. First, select two distinct elements a_0^i and a_1^i of A^i, $i \in \{1,2\}$. Let $\alpha^i(b) = a_b^i$, for $b \in \{0,1\}$.

Let com_1 be defined by $\mathrm{com}_1(b_1 ... b_n) = \alpha^1(b_1) \dots \alpha^1(b_n)$. Then com_1 codes sequences of bits of length n into sequences of actions of player 1 of same length.

Given n, $t \le n$, and a sequence of bits $b_1 \dots b_t$, we let $\mathrm{com}_2(1^n, b_1 \dots b_t)$ be the sequence of length $2q(n)$ that writes $\alpha^2(b_1)a_1^2\alpha^2(b_2)a_1^2 \dots \alpha^2(b_t)a_1^2a_0^2 \dots a_0^2$ (the end consists of a sequence of $2(q(n) - t)$ times a_0^2). Thus, com_2 codes sequences of bits of length less or equal than $q(n)$ into sequences of actions of player 2 of length exactly $q(n)$.

Construction 12 *For a given value of n, we define strategies $\tau^1_{\varepsilon,n}$ and $\tau^2_{\varepsilon,n}$ in the following way:*

1. *Player 1 picks $\omega_n^1 \sim U$ and computes $k_{1,n} = K_1(1^n, \omega_n^1)$, $k_{2,n} = K_2(1^n, \omega_n^1)$. Player 1 then plays the sequence of actions $\mathrm{com}_1(k_{1,n})$ during n stages. Meanwhile, player 2 plays repeatedly the action a_0^2.*

2. *Player 2 picks* $\omega_n^2 \sim U$, *computes* $x_n^2 = D(k_{1,n}, \omega_n^2)$ *and* $f_{k_{1,n}}^{mp(n)}(x_n^2)$. *Player 2 then plays the sequence of actions* $\mathrm{com}_2(1^n, f_{k_{1,n}}^{mp(n)}(x_n^2))$. *Meanwhile, player 1 plays repeatedly the action* a_0^1.

3. *Players 1 and 2 compute* $G_{k_{1,n},mp(n)}(x_n^2) \in \{0,1\}^{mp(n)}$, *where* $G_{k_{1,n},mp(n)}$ *is the pseudo-random generator defined in Construction 10. Decompose this sequence of* $mp(n)$ *bits as* $G_{k_{1,n},mp(n)}(x_n^2) = y_1 \dots y_{p(n)}$ *with* $y_t \in \{0,1\}^m$ *for* $1 \leq t \leq p(n)$. *Players 1 and 2 play the sequence of actions* $a_1^{-3} \dots a_{p(n)}^{-3}$, *where* $a_t^{-3} = \mathrm{cod}(y_t)$ *for* $1 \leq t \leq p(n)$.

The strategies $\tau_{\varepsilon,n}^{-3}$ are defined for a duration of $n + 2q(n) + p(n)$ stages. For $n \geq 0$, let $T(n) = \sum_{k=1}^{n+1} k + 2q(k) + p(k)$. We define the block n to be the stages t such that $T(n)+1 \leq t \leq T(n+1)$. Let τ_ε^j ($j \in \{1,2\}$) be the strategies that follow $\tau_{\varepsilon,n}^j$ during each block n, where the families of random variables $(\omega_n^1)_n$ and $(\omega_n^2)_n$ are independent. All computations above of player 1 and 2 can be done in polynomial time in n. Indeed, $k_{1,n}$ can be computed from $\mathrm{com}_1(k_{1,n})$ and $f_{k_{1,n}}^{p(n)}(x_n^2)$ can be computed from n and $\mathrm{com}_2(1^n, f_{k_{1,n}}^{p(n)}(x_n^2))$ in polynomial time in n. In the third step, player 1 first computes x_n^2 from $k_{2,n}$ and $f_{k_{1,n}}^{mp(n)}(x_n^2)$ by inverting $mp(n)$ times $f_{k_{1,n}}$. Therefore, $\tau_\varepsilon^1 \in \Sigma_{PT}^1$ and $\tau_\varepsilon^2 \in \Sigma_{PT}^2$.

The definition of $\tau_{\varepsilon,n}^1$ and of $\tau_{\varepsilon,n}^2$ is divided into a communication phase (steps 1 and 2), and a play phase (step 3). The aim of the communication phase is to exchange a secret sequence of bits, x_n^2, that serves during the play phase a a seed for the pseudo-random generator $G_{k_{1,n},mp(n)}$. During the play phase, player 3 is unable to distinguish the output of the strategies $\tau_{\varepsilon,n}^1$ and of $\tau_{\varepsilon,n}^2$ from a sequence of $p(n)$ *i.i.d.* random variables distributed according to δ. This is the idea that we formalize now.

Define the random variable $A_n^{-3} = A_n^{-3}(\omega_n^1, x_n^2)$ with values in $A^{-3*} = (A^{-3})^*$ as the sequence of actions played by players 1 and 2 during block

n, $A_n^{-3} = \mathrm{com}_1(k_{1,n})\,\mathrm{com}_2(1^n, f_{k_1,n}^{p(n)})\,\mathrm{cod}(y_1)\ldots\mathrm{cod}(y_{p(n)})$. Let $\delta_1\ldots\delta_{p(n)}$ be a *i.i.d.* sequence of random variables independent of $(\omega_n^1)_n$ and of $(x_n^2)_n$, $\delta_1 \sim \delta$, and let $B_n^{-3} = \mathrm{com}_1(k_{1,n})\,\mathrm{com}_2(1^n, f_{k_1,n}^{p(n)})\,\mathrm{cod}(\delta_1)\ldots\mathrm{cod}(\delta_{p(n)})$.

Lemma 13 *The ensembles $(A_n^{-3})_n$ and $(B_n^{-3})_n$ are indistinguishable in polynomial time.*

Proof: Let Q be the element of $M(\{0,1\}^*, 1^*; A^{-3*})$ that on input $(Z_n, 1^n)$ first decomposes Z_n as $Z_n = Z_1 Z_2 Z_{3,1}\ldots Z_{3,p(n)}$ with $Z_1 \in \{0,1\}^n$, $Z_2 \in \{0,1\}^*$ and $Z_{3,t} \in \{0,1\}^m$ for every $1 \leq t \leq p(n)$, and outputs the sequence $\mathrm{com}_1(Z_1)\,\mathrm{com}_2(Z_2)\,\mathrm{cod}(Z_{3,1})\ldots\mathrm{cod}(Z_{3,p(n)})$. By construction of $\tau_{\varepsilon,n}^{-3}$, the distributions of $Q(k_{1,n} f_{k_1,n}^{(p(n))}(x_n) G_{k_{1,n},p(n)}(x_n))$ when $k_{1,n} = K_1(1^n, \omega)$, $x_n = D(k_{1,n}, \omega')$, $\omega, \omega' \sim U \otimes U$ and of A_n^{-3} are the same. Similarly, the distributions of $Q(k_{1,n} f_{k_1,n}^{(p(n))}(x_n) u_{p(n)}))$ when $k_{1,n} = K_1(1^n, \omega)$, $x_n = D(k_{1,n}, \omega')$, $u_{p(n)}, \omega, \omega' \sim U_{p(n)} \otimes U \otimes U$ and of B_n^{-3} are the same. Recall that the images of polynomial time indistinguishable distributions by polynomial time algorithms are also polynomial time indistinguishable (see for instance Goldreich, Exercise 1 p.120). The result follows from Proposition 11. ¥

Lemma 14 *The ensembles $(A_1^{-3}\ldots A_{n-1}^{-3}A_n^{-3})_n$ and $(A_1^{-3}\ldots A_{n-1}^{-3}B_n^{-3})_n$ are indistinguishable in polynomial time.*

Proof: First, note that $A_1^{-3}\ldots A_{n-1}^{-3}$ is independent of A_n^{-3} and of B_n^{-3}. Then, apply the same argument as above with Q being the element of $M(\{0,1\}^*, 1^*, \Omega; A^{-3*})$ that on input $(Z_n, 1^n)$ first computes $Z_1\ldots Z_{n-1}$ distributed as $A_1^{-3}\ldots A_{n-1}^{-3}$ using the algorithms that define $\tau_{\varepsilon,1}^{-3}\ldots\tau_{\varepsilon,n-1}^{-3}$, and outputs the sequence $Z_1\ldots Z_{n-1}Z_n$. ¥

Lemma 15 *For every $\tau^3 \in \Sigma_{PT}^3$, $g_\infty^3(\tau^3, \tau_\varepsilon^{-3}) < w^3 + \varepsilon$.*

Proof: Starting with τ^3, we construct a polynomial time probabilistic algorithm that inputs $h^{-3}_{T(n+1)} = (a^{-3}_t)_{1\leq t\leq T(n+1)}$ and ω^3, and that computes a^3_t and h_t for $1 \leq t \leq T(n+1)$ defined inductively $h_0 = \emptyset$ and by $a^{-3}_{t+1} = \tau^3(h_t, \omega)$ and $h_{t+1} = (h_t, (a^{-3}_{t+1}, a^3_{t+1}))$. Note that the probability induced on $H_{T(n+1)}$ by $h^{-3}_{T(n+1)} = (A^{-3}_1 \dots A^{-3}_{n-1}A^{-3}_n)$ and by $\omega^3 \sim U$ in the above construction is $\Pr_{\tau^3,\tau^{-3}_\varepsilon}$. Let $\Pr_{\delta,n}$ be the probability induced on $H_{T(n+1)}$ by $h^{-3}_{T(n+1)} = (A^{-3}_1 \dots A^{-3}_{n-1}B^{-3}_n)$ and $\omega^3 \sim U$ in the above construction. We shall study the average payoff of player 3 during block n, $\gamma_n = \frac{1}{T(n+1)-T(n)} \sum_{t=T_n}^{T_{n+1}} g(a_t)$.

Claim 1: $\forall \eta > w^3 + \varepsilon$, $\lim_{n\to\infty} \Pr_{\delta,n}[\gamma_n \geq \eta] = 0$.

Decompose γ_n as $\alpha_n\gamma_{n,\text{com}} + (1-\alpha_n)\gamma_{n,\text{cod}}$, with $\alpha_n = \frac{n+1+2q(n+1)}{T(n+1)-T(n)}$, $\gamma_{n,\text{com}} = \frac{1}{n+1+2q(n+1)} \sum_{t=T(n)+1}^{T(n)+n+1+2q(n+1)} g(a_t)$, $\gamma_{n,\text{cod}} = \frac{1}{p(n+1)} \sum_{t=T(n)+n+1+2q(n+1)}^{T(n+1)} g(a_t)$. Since $(\gamma_{n,\text{com}})_n$ is bounded and α_n goes to 0 as n goes to ∞, it is enough to prove that $\forall \eta > \omega^3 + \varepsilon$, $\lim_{n\to\infty} \Pr_{\delta,n}[\gamma_n \geq \eta] = 0$. This last fact can be seen as a consequence of Blackwell's [4] approachability theory (since no strategy of player 3 yields an expected payoff greater than $w^3 + \varepsilon$ in the one shot game), and does not rely on the fact that $\tau^3 \in \Sigma^3_{PT}$.

Claim 2: $\forall \eta > w^3 + \varepsilon$, $\lim_{n\to\infty} \Pr_{\tau^{-3}_\varepsilon,\tau^3}[\gamma_n \geq \eta] = 0$.

Fix $\eta > w^3 + \varepsilon$ and $\eta^- \in]\omega^3 + \varepsilon, \eta[$. By making approximations of the payoffs associated to the actions, we can construct a polynomial time algorithm $Q \in M(A^*; \{0,1\})$ that on input $h_{T(n+1)}$ outputs 1 if $\gamma_n \geq \eta$ and 0 if $\gamma_n \leq \eta^-$. First, note that $\Pr_{\delta,n}[Q(h_{T(n+1)}) = 1] \leq \Pr_{\delta,n}[\gamma_n \geq \eta^-]$, which implies $\lim_{n\to\infty} \Pr_{\delta,n}[Q(h_{T(n+1)} = 1] = 0$ using Claim 1. Since $(A^{-3}_1 \dots A^{-3}_{n-1}B^{-3}_n)_n$ and $(A^{-3}_1 \dots A^{-3}_{n-1}A^{-3}_n)_n$ are indistinguishable in polynomial time, one also has $\lim_{n\to\infty} \Pr_{\tau^{-3}_\varepsilon,\tau^3}[Q(h_{T(n+1)}) = 1] = 0$. The result follows by observing that $\Pr_{\tau^{-3}_\varepsilon,\tau^3}[\gamma_n \geq \eta] \leq \Pr_{\tau^{-3}_\varepsilon,\tau^3}[Q(h_{T(n+1)} = 1]$.

From Claim 2, it follows that $\limsup_{n\to\infty} \gamma_n \leq w^i + \varepsilon$ $\Pr_{\tau^{-3}_\varepsilon,\tau^3}$ almost surely, hence the result. ¥

References

[1] R.J. Aumann and L.S. Shapley. Long-term competition—A game theoretic analysis. In N. Megiddo, editor, *Essays on Game Theory in Honor of Michael Maschler*, pages 1–15. Springer-Verlag, New-York, 1994.

[2] R.J. Aumann and S. Sorin. Cooperation and bounded recall. *Games and Economic Behavior*, 1:5–39, 1989.

[3] E. Ben Porath. Repeated games with finite automata. *Journal of Economic Theory*, 59:17–32, 1993.

[4] D. Blackwell. An analog of the minimax theorem for vector payoffs. *Pacific Journal of Mathematics*, 6:1–8, 1956.

[5] O. Goldreich. *Foundations of cryptography (fragments of a book).* ftp://theory.lcs.mit.edu/pub/people/oded/BookFrag, 1998. Version 2.03.

[6] O. Gossner. Repeated games played by cryptographically sophisticated players. Document de travail THEMA 9907, 1999.

[7] P. Hernández and A. Urbano. Communication and automata. mimeo, 1999.

[8] E. Lehrer. Internal correlation in repeated games. *International Journal of Game Theory*, 19:431–456, 1991.

[9] A. Neyman. Bounded complexity justifies cooperation in the finitely repeated prisoner's dimema. *Economic Letters*, 19:227–229, 1985.

[10] A. Neyman. Finitely repeated games with finite automata. *Mathematics of Operations Research*, 23:513–552, 1998.

[11] A. Rubinstein. Finite automata play the repeated prisoner's dilemma. *Journal of Economic Theory*, 39:83–86, 1986.

[12] A. Rubinstein. Equilibrium in supergames. In N. Megiddo, editor, *Essays on Game Theory in Honor or Michael Maschler*, pages 17–27, Berlin, 1994. Springer-Verlag.

[13] A. Urbano and J. E. Vila. Unmediated communication in repeated games with imperfect monitoring. WP-AD, Instituto Valenciano de Investigaciones Economicas, 1998.