UNMEDIATED COMMUNICATION IN REPEATED GAMES WITH IMPERFECT MONITORING*

Amparo Urbano and José Vila**

WP-AD 98-27

Correspondence to:
Amparo Urbano. Departamento de Análisis Económico. Facultad de CC. Económicas y Empresariales.
Campus de los Naranjos. Edificio departamental oriental - 46022 Valencia (Spain).
E-mail: amparo.urbano@uv.es

Editor: Instituto Valenciano de Investigaciones Económicas, S.A.
First Edition December 1998
ISBN: 84-482-1971-6
Depósito Legal: V-4878-1998

IVIE working-papers offer in advance the results of economic research under way in order to encourage a discussion process before sending them to scientific journals for their final publication.

---

* We want to thank partial support by DGICYT under project PB95-1074.

** A. Urbano and J.E. Vila: University of Valencia.

UNMEDIATED COMMUNICATION IN REPEATED GAMES WITH IMPERFECT MONITORING

Amparto Urbano and José E. Vila

ABSTRACT

We show that any correlated equilibrium payoff of two-player repeated games with imperfect monitoring and without discounting can be reached as the Nash equilibrium payoff of the game extended by a universal mechanism of unmediated communication. This result holds regardless the particular concept of equilibrium involved (upper, lower, Banach or uniform equilibrium). The communication mechanism is built up by using commutative one-way functions. These functions are designed with the help of cryptographic tools.

Key words: Unmediated communication, imperfect monitoring; cryptosystems.

1 Introduction.

There exists a growing body of papers dealing with long time repeated strategic interactions with imperfect monitoring, i. e. repeated games where actions are not observable. Most of them[1] are concerned with characterizing the set of all the Nash equilibrium payoffs. In particular, Lehrer (1991), shows that two-player symmetric games with standard-trivial information[2] are saturated, i. e. payoffs sustainable by external correlation devices are also Nash equilibrium payoffs. In other words, that any external correlation can be substituted by an internal correlation which utilizes only the information structure of the game. However, the extension of this result to more general information structures under imperfect monitoring is still unsolved.

The purpose of our paper is to show that correlated devices in two-player infinitely repeated games with imperfect monitoring and with rational payoffs can be emulated by plain conversation. Or, in other words, that any correlated distribution can be produced in a way that is immunized against unilateral deviations. In particular, by adding two phases of unmediated communication to the stage game of any infinitely repeated game with imperfect monitoring, any correlated equilibrium payoff of the original game can be obtained as a Nash equilibrium payoff of the extension[3].

Thus, our work pertains to two branches of the literature. It relates on one hand to the analysis of Forges (1986, 1990) and Barany (1992) who decentralize communication and correlated equilibrium, respectively, by means of 'plain conversation', if the number of players is at least four. Urbano and Vila (1997, 1998) extend their result to the class of two-player games of complete and incomplete information by constructing an unmediated communication encryption scheme with private key which is based on computing exponential functions over finite fields. Lehrer (1991) treats correlation through private histories in long games. Gossner (1997), examines how information stems

[1] See for instance Lehrer (1990, 1991, 1992a, 1992b, 1992c), Radner (1986), Rubinstein and Yaari (1983), Abreu, Pearce and Stachetti (1986), Fundenberg, Levine and Maskin (1994), Fundenberg and Levine (1991), Compte (1994, 1997) and Ben-Porath and Kahneman (1995) among others.

[2] In these games the signal a player gets is either revealing the actions played (standard) or completely concealing it (trivial).

[3] Any two-player infinitely repeated game with imperfect monitoring has an extension which is saturated.

from communication, therefore linking communication mechanisms and information structures. Finally, Lehrer (1996) and Lehrer and Sorin (1997), reproduce the correlated distribution through 'mediated talk'.

On the other hand, our analysis relates to papers written on the subject of cheap talk. See, for instance, Farrell (1987, 1988), Farrell and Rabin (1996), Matthews and Postlewaite (1989) among others. Aumann and Hart (1993) define 'polite talk' as that talk that allows players to talk one at a time and show that, by means of it, players can get the bi-span [4] of the Nash equilibria of the original game and when they extend their model to the case of one-side incomplete information they show that the equilibrium involves the informed player revealing some of his information, as well as both players performing joint randomization. Mor Amitai (1996) extends the above model to incomplete information on both sides.

We construct a scheme of unmediated communication with finite message sets which is a universal mechanism for all infinitely repeated two-player games without discounting and with imperfect monitoring, which shows the power of plain conversation as an internal correlation mechanism. Our approach follows that of Urbano and Vila (1997, 1998) with public messages but with private meaning. This approach is closely related to the one used to model 'oblivious transfers'[5] and those used to solve problem such that 'coin flipping by phone' (Blumm (1981)) or 'playing Mental Poker with no real cards' (Rabin (1981))[6].

[4]The bi - span of a set $A \subseteq R^2$ is defined as follows: it is the set of all vectors $(x,y) \in R^2$ for which there exists a bounded martingale $\{(X_n, Y_n)\}_{n=1,2,...}$ with values in R^2 that starts at (x,y) (i. e. $(X_1, Y_1) = (x,y)$); it converges to A (i. e. $(X_n, Y_n) \longrightarrow (X_\infty, Y_\infty) \in A$ almost surely); and finally it satisfies the 'bi' property that for each n either $x_{n+1} = x_n$ a. s. or $y_n = y_{n+1}$ a. s. Thus, at each stage of the martingale, either the X-coordinate stays constant (and the Y-coordinate 'splits'), or the Y-coordinate is constant (and the X-coordinate 'splits'). Note that if one drops the 'bi' requirement, then the resulting set is precisely the convex hull of A.

[5]An oblivious transfer is a probabilistic information exchange such that both the sender and the receiver cannot be sure of the real meaning of the message.

[6]In the 'coin flipping by phone', the problem is to devise a scheme whereby a player, say Bob, can call heads or tails and the other, say Alice, can flip in such way that each has a 50% chance of winning. Flipping a real coin over the phone is clearly unsatisfactory because if Bob call 'heads', Alice can simply say 'Sorry, tails'.

Mental poker is played like ordinary poker but without cards and without real verbal communication; all exchange between the players must be accomplished using messages.

However, these public and private characteristics of messages have to be related in some specific way in order to control the integrity of the whole exchange of information. Thus we have to use ciphers with some properties, in particular, that they commute among them. The use of commutative ciphers is also appealing by their 'fairness' and 'usefulness' in games where players may cheat as the ones mentioned above. However, the main problem with this approach is that it is very difficult to build up commutative ciphering and deciphering functions in general spaces. In this paper we solve this problem by using exponential ciphers over a finite Galois field of prime order p (p a prime number). Thus, we construct[7] a communication encryption scheme with private key, which is based on computing exponential functions over a finite field[8].

We assume that the pre-play communication phase is finite and that the player have bounded calculation skills[9], i.e. they need a non-null period of time to make any calculation[10]. Also a technical assumption, shared with Barany, Forges and Urbano and Vila is needed: the payoffs of the game must

It may perhaps make the ground rules clearer if we imagine two players, Bob and Alice again, who want to play poker over the telephone. Since it is impossible to send playing cards over a phone line, the entire game (including the deal) must be realized using only spoken (or digitally transmitted) messages between the two players. Obviously any player may try to cheat. A fair method of playing Mental Poker should preclude any sort of cheating.

[7]Alternative constructions to ours are those based on pseudorandom generators. A pseudorandom generator is a deterministic algorithm expanding short random seeds into much longer bit sequences which 'appear' to be random (although they are not).

[8]See Pohling and Hellman (1978), River, Shamir and Adleman (1978). The enciphering and deciphering transformations are based on Euler's generalization of Fermat's theorem. The security of the scheme rest on the complexity of computing discrete logarithms in the Galois fields. This is like a one-way function which is easy to compute but hard to invert.

[9]Constructions of secure encryption schemes are based on various intractability assumptions. Classical cryptography assumes that two agents, say A and B, share some secret information before they start to exchange messages, while another agent, say C, tries to spy them. In modern cryptography, A and B share no secret information before they communicate. In typical modern cryptosystems, messages are sent from A to B using some keys. Why C cannot replicate the above agents computations?. Here intervenes the boundedness of agent's rationality. All the computations needed by A and B can be done in reasonable time, whereas that of C would need ages. Also, this distinction between computations that can be implemented in relatively short time and computations which are intractable may be modeled by polynomial and unpolynomial Turing machines.

[10]This time can be as short as we want.

be rational.[11].

We will show that our scheme is self-enforcing, in the sense that no player wants to deviate from it if the other does not, and that it implements any extensive form correlated equilibrium as a Nash equilibrium of the game extended by two phases of communication.

To the best of our knowledge, the only application of modern cryptography to game theory, apart from Urbano and Vila (1997,1998) is Gossner (1998). He does not rely on a particular protocol but rather on the fundamental[12] and unproved theoretical assumption of the existence of a trapdoor function. Assuming that players are represented by Turing machines, Gossner obtains a 'Folk Theorem' in which the usual minmax level in mixed strategies is replaced by the minmax in correlated strategies.

Apart from the cryptographic design of our communication protocol, the proof of our result resembles that of Lehrer (1991). In particular, and like him, we take advantage of two previous results. The first one, is a characterization of correlated equilibria in repeated games with imperfect monitoring (Lehrer, 1992a). The second result is that the limit of certain finitely repeated game payoffs - those associated with strategies from which any profitable deviation is detectable - are sustainable by equilibria in the infinitely repeated game (Lehrer, 1992c). The idea is to show that any extensive form correlated equilibrium payoff of the repeated game is a limit of such payoffs.

Also, since the game is of imperfect monitoring, we have to describe its information structure. Thus, following Lehrer (1992a), we introduce two relations between a player's actions. Two actions of a player are *indistinguishable* if they yield the same signal for the opponent, no matter what the latter is playing. Additionally, in order to define an undetectable deviation, we introduce the following relation: an action a' is *more informative* than a,

[11]This assumption is needed to replicate some probability distributions by choosing a message uniformly at random from a finite set. Anyway this assumption is not a limitation since it is always possible to approximate a real parameter by a rational one.

[12]A major tool in the construction of cryptographic protocols is the concept of 'zero knowledge' proofs systems, and the fact that they exist for all languages in NP (provided that one -way functions exist). Loosely speaking, zero-knowledge proofs yield nothing but the validity of the assertion. They provide a tool for 'forcing' parties to follow a given protocol properly. We thank S. Hart for pointing us this remark.

if by playing a' a player can distinguish between two actions of his opponent better than by playing a.

Thus, our result can be seen as a way to generalize internal correlation in infinitely repeated two-player games with imperfect monitoring[13] and, in this way, as a generalization to general information structures of Lehrer (1991). When applied to games with symmetric standard-trivial information it provides a universal mechanism for internal correlation instead of the particular channel used by him.

The plan of the paper is as follows. In sections 2 and 3 we set up the model of repeated games and their underlying information structure. In section 4 we allow players to communicate by means of a mediator: we define an autonomous device, the different correlated equilibria and the relationships among them. The main result is given in section 5. The communication protocol unfolds in sections 6 and 7. Its properties are analyzed in section 8. The new type of strategies to generate our result are constructed in section 9 and section 10 is devoted to illustrate them by means of an example. Finally, section 11 proves the main theorem and section 12 concludes the paper.

2 The model

A two-player infinitely repeated game Γ with complete information and imperfect monitoring can be described by the following elements[14]:

A one-shot normal-form game with two players P_h with finite sets of feasible actions $A_h = \{a_h^1, ..., a_h^{s_h}\}$, $(h = 1, 2)$. Let us denote by $A = A_1 \times A_2$. The one-shot game payoff functions are given by $u_h : A \longrightarrow Q$ $(h = 1, 2)$. In each stage game, both players simultaneously select an action on their own sets.

Monitoring or information functions. Since monitoring in Γ is imperfect, P_h is not allow to see the action chosen by $P_{h'}$ nor the payoff

[13]The key is that players can generate private information through public messages with a modern cryptosystem.

[14]We will follow very closely the terminology of Lehrer (1992a), since we will make use of some of his results.

obtained in the stage game[15]. Nevertheless, players receive some information on the effects of their actions. This information of P_h is resumed in a 'signal' from a finite set L_h. Hence, P_h has an 'information function' l_h defined on the set A and range on L_h. After each stage game, when (a_1^i, a_2^j) is played, P_h receives the signal $l_h(a_1^i, a_2^j)$. Let us notice that perfect monitoring is just a particular case of the above situation, when $L_h = A$ and l_h is the identity function.

Strategies. A pure strategy of player h is a sequence of functions $f_h = (f_h^t)_{t \in N}$ such that $f_h^t : L_h^{t-1} \longrightarrow A_h$, where L_h^{t-1} is the Cartesian product of L_h with itself $t-1$ times. Denote by Σ_h the set of all pure strategies of player h in the repeated gamed and by $\Sigma = \Sigma_1 \times \Sigma_2$. For each $f = (f_1, f_2) \in \Sigma$, $u_h^t(f)$ denotes the payoff of player h at stage t if f is played.

A mixed strategy of P_h is an element of $\Delta(\Sigma_h)$, i. e. a probability distribution on Σ_h. For each $\sigma = (\sigma_1, \sigma_2) \in \Delta(\Sigma_1) \times \Delta(\Sigma_2)$, $E_\sigma(u_h^t)$ denotes the expected payoff of player h at stage t where the expectation is taken with respect to the measure induced by σ.

A payoff function of the repeated game, defined by the limit of average payoffs of the finitely repeated truncated games, i. e. if both players follow the strategy $\sigma = (\sigma_1, \sigma_2) \in \Delta(\Sigma_1) \times \Delta(\Sigma_2)$, the payoff of P_h in Γ is given by:

$$U_h(\sigma) = \lim_{T \to \infty} \frac{1}{T} \sum_{t=1}^{T} E_\sigma(u_h^t)$$

if the limit exits.

Equilibrium in Γ shall be defined in the usual way: a pair of (mixed) strategies is a Nash equilibrium if there does not exist unilateral profitable deviations. However, deviation payoffs may not be comparable with $U_h(\sigma)$: the existence of $\lim_{T \to \infty} \frac{1}{T} \sum_{t=1}^{T} E_\sigma(u_h^t)$ does not guarantee the existence of the average limit payoff when the deviating strategy is played.

[15]Both players have some kind of 'bank account' where payoffs are saved. A players is not informed on the amount of his own stage payoff.

Since the sequence of average expected payoffs induced by any (mixed) strategy of Γ is bounded, the existence of other kinds of limits is always guarantied. This is the case of the upper, lower, Banach and uniform limits. Each one of them supports a definition of 'Nash equilibrium' in the usual way:

Definition 1 *Let $\sigma = (\sigma_1, \sigma_2) \in \Delta(\Sigma_1) \times \Delta(\Sigma_2)$ be a pair of mixed strategies of Γ.*

1. *We say that σ is an upper Nash equilibrium of Γ if $U_h(\sigma)$ exists and it satisfies that for any other pair of strategies $(\bar{\sigma}_1, \bar{\sigma}_2)$:*

   (a) $U_h(\sigma) \geq \lim sup_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\bar{\sigma}_1, \sigma_2)}(u_h^t)$.

   (b) $U_h(\sigma) \geq \lim sup_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\sigma_1, \bar{\sigma}_2)}(u_h^t)$.

   Let us denote by UNP the set of all the payoffs associated to upper equilibrium strategies.

2. *Similarly, σ is a lower Nash equilibrium of Γ if $U_h(\sigma)$ exists and it satisfies that for any other pair of strategies $(\bar{\sigma}_1, \bar{\sigma}_2)$:*

   (a) $U_h(\sigma) \geq \lim inf_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\bar{\sigma}_1, \sigma_2)}(u_h^t)$.

   (b) $U_h(\sigma) \geq \lim inf_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\sigma_1, \bar{\sigma}_2)}(u_h^t)$.

   Denote by LNP the set of all the payoffs associated to lower equilibrium strategies.

3. *Let L be a Banach limit. Denote by*

$$U_h^L(\sigma) = L_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_\sigma(u_h^t)$$

   Then σ is a Banach Nash equilibrium of Γ for the Banach limit L if for any other pair of strategies $(\bar{\sigma}_1, \bar{\sigma}_2)$:

   (a) $U_h^L(\sigma) \geq L_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\bar{\sigma}_1, \sigma_2)}(u_h^t)$.

(b) $U_h^L(\sigma) \geq L_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T} E_{(\sigma_1,\bar{\sigma}_2)}(u_h^t)$.

$B_L NP$ is the set of all the payoffs associated to Banach Nash equilibrium strategies for Banach limit L.

4. *We say that σ is a uniform Nash equilibrium of Γ if $U_h(\sigma)$ exists and for any positive ε, σ is an ε-equilibrium in any sufficiently long game, i. e. $\forall\varepsilon > 0$, $\exists\ T_0$ such that $\forall\ T \geq T_0$ and $\forall\ (\bar{\sigma}_1, \bar{\sigma}_2)$ pair of strategies of Γ:*

   (a) $U_h(\sigma) + \varepsilon \geq \frac{1}{T}\sum_{t=1}^{T} E_{(\bar{\sigma}_1,\sigma_2)}(u_h^t)$.

   (b) $U_h(\sigma) + \varepsilon \geq \frac{1}{T}\sum_{t=1}^{T} E_{(\sigma_1,\bar{\sigma}_2)}(u_h^t)$.

   Let us denote by UNIFNP the set of all the payoffs associated to uniform equilibrium strategies.

3 The information structure

Since past actions in an imperfect monitoring game are not always observed, histories are not common knowledge. Moreover, signals received by both player can also be private information. In order to establish the information structure of players in these games[16], we define an equivalence and partial order relations on action sets:

Definition 2 *A pair of actions $a, a' \in A_h$ are indistinguishable (denoted $a \sim a'$) if and only if $\forall b \in A_{h'}$, $(h' \neq h)$ we have that $l_{h'}(a,b) = l_{h'}(a',b)$. In words, a and a' are indistinguishable when $P_{h'}$ has no way to distinguish whether P_h has played a or a'.*

$\sim$ is clearly a binary equivalence relation. Its quotient set $A_h^{\sim}$ summarizes the information structure of the game. For instance, if $A_h^{\sim} = A_h$ $(h = 1, 2)$, Γ is a perfect monitoring game, This information structure is called standard information. If both sets $A_h^{\sim}$ collapse to a single point, a player has no possibility to distinguish between any action of the other one. In this case Γ is said to be a game of trivial information. The relation $\sim$ can be easily extended to mixed actions.

[16] See Lehrer (1992a).

Definition 3 *An action $a \in A_h$ is more informative than $a' \in A_h$ (denoted $a \succ a'$) if and only if $a \sim a'$ and $\forall b, b' \in A_{h'}$, $(h' \neq h)$ $l_h(a,b) \neq l_h(a,b')$ implies that $l_h(a',b) \neq l_h(a',b')$, i. e. P_h obtains more information on $P_{h'}$'s moves by playing a rather than a'.*

$\succ$ is a partial order on each set A_h. A fundamental property of this relation is that P_h can mimic any of his pure strategies f_h by another g_h, satisfying $g_h^t(l) \succ f_h^t(l)$ without being detected: at each stage he computes the history consistent with g and then he plays according to f. As we will see later, deviation to less informative actions may be detectable, since the deviating player has less information than he was supposed to get. $\succ$ can be directly extended to mixed actions.

4 Mediated communication.

We allow the players to communicate before simultaneously choosing their actions at every stage game. This communication, which has no direct effect on the payoffs, can be performed with the help of an external mediator who sends correlated and private signals to both players at each stage of Γ. We model this mediator as an 'autonomous device' as follows (see Forges (1986)): an autonomous device for Γ is a collection $d = \{O_h^t, P^t\}_{h=1,2,\ t\in N}$ where O_h^t is a set of outputs for P_h at stage t and P^t is a transition probability that chooses outputs at stage t as a function of all past outputs. An autonomous device is called canonical when $O_h^t = A_h$, $\forall h, t$. A correlation device is an autonomous device where all O_h^t for $t > 1$ are singletons[17]. An autonomous device is also called an extensive form correlation device.

Once an extensive form correlation device d is selected, the game Γ can be extended to another infinitely repeated game Γ_d where each player receives an output $o_h^t \in O_h^t$ before choosing his action at stage t. Strategies in Γ_d depend on the outputs received by players. Formally, a pure strategy of player h is a sequence of functions $f_h = (f_h^t)_{t\in N}$ such that $f_h^t : L_h^{t-1} \times O_h^{t-1} \longrightarrow A_h$, where the exponent $t-1$ represents the Cartesian product of a set with itself $t-1$ times. Denote by $\Sigma_h^{d\star}$ the set of all pure strategies of player h in the repeated

[17] A correlation device is an autonomous device which only works at the first stage of Γ and afterwards remains inactive.

gamed and by $\Sigma^{d\star} = \Sigma_1^{d\star} \times \Sigma_2^{d\star}$. For each $f = (f_1, f_2) \in \Sigma^{d\star}$, $E_P(u_h^t(f))$ denotes the expected payoff of player h at stage t if f is played (expectations are taken for the product distribution $P = \times_{t\in N} P_t$). A mixed strategy of P_h is an element of $\Delta(\Sigma_h^{d\star})$, i. e. a probability distribution on $\Sigma_h^{d\star}$. For each $\sigma = (\sigma_1, \sigma_2) \in \Delta(\Sigma_1^{d\star}) \times \Delta(\Sigma_2^{d\star})$, $E_{\sigma,P}(u_h^t)$ denotes the expected payoff of player h at stage t where the expectation is taken with respect to the measure induced by σ and the product distribution $P = \times_{t\in N} P_t$

The payoff for the whole game can be also defined by computing the limit of expected average payoffs of finitely repeated truncated games

$$U_h^{d\star}(\sigma) = \lim_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{\sigma,P}(u_h^t)$$

if this limit exists.

The extensive form correlated equilibria of Γ can be defined as Nash equilibria of the mediated communication game Γ_d. Since we have four different concepts of Nash equilibria for undiscounted infinitely repeated games, four concepts of extended form correlated equilibrium arise[18]:

Definition 4 *Let $d = \{O_h^t, P^t\}_{h=1,2,\ t\in N}$ be an autonomous device for the game Γ. Let $\sigma = (\sigma_1, \sigma_2) \in \Delta(\Sigma_1^{d\star}) \times \Delta(\Sigma_2^{d\star})$ be a pair of (mixed) strategies of Γ_d.*

1. *We say that σ is an upper extensive form correlated equilibrium of Γ if $U_h(\sigma)$ exists and it satisfies that for any other pair of strategies of Γ_d $(\bar\sigma_1, \bar\sigma_2)$:*

   (a) $U_h^{d\star}(\sigma) \geq limsup_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\bar\sigma_1,\sigma_2,P)}(u_h^t)$.

   (b) $U_h^{d\star}(\sigma) \geq limsup_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\sigma_1,\bar\sigma_2,P)}(u_h^t)$.

   Let us denote by $UCP^\star$ the set of all the payoffs associated to upper extensive form correlated equilibrium strategies.

2. *Similarly, σ is a lower extensive form correlated equilibrium of Γ if $U_h(\sigma)$ exists and it satisfies that for any other pair of strategies of Γ_d $(\bar\sigma_1, \bar\sigma_2)$:*

[18] See Lehrer (1992a).

(a) $U_h^{d\star}(\sigma) \geq liminf_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\bar{\sigma}_1,\sigma_2,P)}(u_h^t)$.

(b) $U_h^{d\star}(\sigma) \geq liminf_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\sigma_1,\bar{\sigma}_2,P)}(u_h^t)$.

Denote by LCP* the set of all the payoffs associated to lower extensive form correlated equilibrium strategies.

3. *Let L be a Banach limit and let*

$$U_h^{L\ d\star}(\sigma) = L_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{\sigma,P}(u_h^t)$$

Then σ is a Banach extensive form correlated equilibrium of Γ for the Banach limit L if for any other pair of strategies Γ_d, $(\bar{\sigma}_1, \bar{\sigma}_2)$:

(a) $U_h^{L\ d\star}(\sigma) \geq L_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\bar{\sigma}_1,\sigma_2,P)}(u_h^t)$.

(b) $U_h^{L\ d\star}(\sigma) \geq L_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} E_{(\sigma_1,\bar{\sigma}_2,P)}(u_h^t)$.

$B_L CP^\star$ is the set of all the payoffs associated to Banach extensive form correlated equilibrium strategies for a Banach limit L.

4. *We say that σ is a uniform Nash equilibrium of Γ if $U_h^{d\star}(\sigma)$ exists and for any positive ε, σ is an ε-equilibrium in any sufficiently long game, i. e. $\forall \varepsilon > 0$, $\exists\ T_0$ such that $\forall\ T \geq T_0$ and $\forall\ (\bar{\sigma}_1, \bar{\sigma}_2)$ pair of strategies of Γ_d:*

(a) $U_h^{d\star}(\sigma) + \varepsilon \geq \frac{1}{T} \sum_{t=1}^{T} E_{(\bar{\sigma}_1,\sigma_2,P)}(u_h^t)$.

(b) $U_h^{d\star}(\sigma) + \varepsilon \geq \frac{1}{T} \sum_{t=1}^{T} E_{(\sigma_1,\bar{\sigma}_2,P)}(u_h^t)$.

Let us denote by UNIFCP* the set of all the payoffs associated to uniform equilibrium strategies.

The same definitions can be obtained by adding to Γ a correlation device which is not an autonomous device, i. e. a device which only operates at the first stage of Γ and remains inactive afterwards. Hence, four different definitions of correlated equilibrium arise, with payoff sets defined by UCP, LCP, B$_L$CP and UNIFCP respectively.

The following relationships are a direct consequence of the definitions of the twelve sets of payoffs[19]:

1. UNP $\subseteq$ UCP $\subseteq$ UCP*
2. LNP $\subseteq$ LCP $\subseteq$ LCP*
3. B$_L$UNP $\subseteq$ B$_L$CP $\subseteq$ B$_L$CP*, $\forall$ Banach limit L.
4. UNIFNP $\subseteq$ UNIFCP $\subseteq$ UNIFCP*
5. UNP $\subseteq$ LNP, UCP $\subseteq$ LCP and UCP* $\subseteq$ LCP*.
6. UNIFNP $\subseteq$ UNP, UNICP $\subseteq$ UCP and UNIFCP* $\subseteq$ UCP*.
7. UNIFNP $\subseteq$ B$_L$NP, UNICP $\subseteq$ B$_L$CP and UNIFCP* $\subseteq$ B$_L$CP*, $\forall$ Banach limit B.

Moreover, Lehrer (1992a) shows that

1. LNP = LCP = LCP *
2. UCP = UCP* = B$_L$CP = B$_L$CP* = UNIFCP = UNIFCP*, $\forall$ Banach limit L.

Hence, adding an autonomous device does not enlarge the Nash equilibrium payoff set of players when we consider the 'lower' equilibrium concept: any infinitely repeated game with any kind of imperfect monitoring is 'lower-saturated'[20]. The question whether games with imperfect monitoring are in general saturated (i.e. saturated for the other three equilibrium definitions) remains still open. Partial results have been obtained for particular information structures. For standard information, the result is a direct consequence of the folk theorem (see Aumann 1985). Lehrer (1991) shows that general saturation holds in games with symmetric standard-trivial information[21]

We say that a game with imperfect monitoring has symmetric standard-trivial information when its information functions satisfy that, $\forall(a,b) \in$

[19] See Lehrer (1992a).

[20] A game is said to be saturated when its Nash and correlated equilibrium payoff sets coincide.

[21]

A either:00161 053¡p type="texpara" tag="Body Text" et="enumerate" ¿$l_1(a,b) = l_2(a,b) = (a,b)$, and in this case we say that the information is standard or00162 053¡p type="texpara" tag="Body Text" et="enumerate" ¿$l_1(a,b) = a$ and $l_2(a,b) = b$, and in this case we say that the information is trivial.00169 038¡p type="texpara" tag="Body Text" ¿In this types of games, any pair of indistinguishable actions are not comparable by using the partial order relation $\succ$.00000 .

5 Unmediated communication: the main result.

We want to consider the decentralized situation in which players communicate without the help of any external mediator: P_1 and P_2 just exchange messages from a finite set along the whole game. This communication mechanism is known as plain conversation or unmediated communication. Clearly, if a payoff is obtained by adding to Γ a plain conversation scheme, the same payoff could be also obtained by adding an autonomous device. The question that arises at this point is: given an extensive form correlated equilibrium payoff of Γ (with any equilibrium definition), could players obtain the same payoff with the help of no external mediator, by just using a plain conversation scheme? Moreover, could it be used in any game, regardless of its particular information structure?. The answers to these questions are affirmative:

Theorem (Main result) *Let Γ be a two-player infinitely repeated game without discounting, with imperfect monitoring and with rational payoffs. Given an element $x \in$ in $UCP = UCP^{\star} = B_L CP = B_L CP^{\star} = UNIFCP = UNIFCP^{\star}$, $\forall$ Banach limit L, there exists an extension of Γ by a universal*[22] *unmediated communication scheme such that x is the (Upper, Banach, Uniform) Nash equilibrium payoff of the extended game.*

This result shows the power of unmediated communication as a way of generating internal correlation by means of the underlying information structure, in repeated games with imperfect monitoring. Jointly with the main results of Urbano and Vila (1997, 1998), we have that players can eliminate

[22] *Which does not depend on the particular information structure of Γ.*

the mediator role in a wide class of two-player games without any loss of efficiency.

Our main result is closely related to that of Lehrer (1991). It is shown there that the mediator of an imperfect monitoring repeated game can be substituted by unmediated communication in the particular case of symmetric standard-trivial information. Hence, our main result could be understood as an extension of this saturation theorem for arbitrary imperfect information structures. However, it is important to point out a basic difference between both approaches: Lehrer builds up conversation schemes by using actions as messages at some stages. We interpret this process as an *investment in communication*: players choose actions that could be inefficient at some one-shot games in order to coordinate and to obtain bigger future payoffs. Since average payoffs are considered and short communication phases are able to support coordination during a large number of stages[23], the whole process is actually efficient. Under this approach of low cost communication, internal correlation arises from the private histories of both players and the saturation of the original game is established. The problem with this analysis is that it cannot be easily extended to more general information structures, since players could learn about the rivals' actions during the process and problems of incentive compatibility may appear. In other words, the symmetric standard-trivial information structure is needed also in the design of the master plan. In the latter, the players play over and over again according to the same correlation and, due to the symmetric standard-trivial information, without impairing its effectiveness (i.e., the correlation remains incentive compatible).

In contrast, our communication scheme is based on a cheap talk mechanism which allows players to exchange messages, out from the original game itself. Hence, we deal with the extension of the original game by a universal unmediated costless communication scheme. This extended game is saturated, and we establish that its Nash equilibrium payoffs include all the (upper, Banach, uniform) extensive form correlated equilibrium payoffs of the original game.

[23]This fact is a consequence of the symmetry of the information structure involved, where a player is unable to learn about the action played by the other one without giving him extra information about his own action.

The next sections are devoted to constructing this communication protocol and to proving the theorem. To this end, and following Lehrer (1992a), we characterize the (extensive form) correlated equilibrium payoffs in terms of the one-shot game parameters. This characterization is based on two subsets B_h $(h = 1, 2)$ of $\Delta(A)$ = the set of probability distributions on A. These subsets are defined as follows:

$$B_h = \{q \in \Delta(A) | \sum_{b \in A_{h'}} q(a_0, b) u_h(a_0, b) \geq \sum_{b \in A_{h'}} q(a_0, b) u_h(a, b)$$

$\forall a_0, a \in A_h$ *such that* $a \succ a_0\}$. In words, B_h contains the probability distributions on A which do not admit any unilateral profitable deviation by P_h to indistinguishable and more informative actions. Let us notice that the condition defining B_h is analogous to the characterization of a canonical correlated equilibrium of a one-shot game (see, for instance, Aumann 1974). Hence, we can understand $B_1 \cap B_2$ as the 'canonical correlated distributions' of the one-shot game considering only indistinguishable and more informative deviations. Is it easy to check that the set $B_1 \cap B_2$ is a convex polyhedron contained in $\Delta(A)$.

Let IR denote the individually rational payoffs of the one-shot game, i.e. the payoff in which each player receives at least his minimax payoff. We have the following proposition that characterizes the extensive form correlated equilibrium payoffs of the repeated game in terms of the parameters of the one-shot game:

Proposition 1 *(Lehrer, 1992a)* $UCP = UCP^* = B_L CP = B_L CP^* = UNIFCP = UNIFCP^* = u(B_1 \cap B_2) \cap IR$,

$\forall$ *Banach limit* L, *where* $u = (u_1 \times u_2)$.

To prove the main result, we must show that $\forall q$ such that $u(q) \in (u_1 \times u_2)(B_1 \cap B_2) \cap IR$, *there exist a (uniform, upper, Banach) Nash equilibrium of* Γ *extended by a plain conversation protocol which gives a payoff of* $u(q)$. The first step consists on building up a communication protocol that allows players to choose their actions according to q (or, at least, to a probability distribution very close to q in a sense that will be specified below). Secondly, we have to establish mechanisms to prevent indistinguishable less informative

deviations that could be profitable. These ideas will unfold in the next sections: let us start by defining the finite message set and the one-way functions needed in the sequel. Then, we define formally the universal communication protocol and we analyze its main properties.

6 The set of messages and the one-way functions.

A protocol is an agreed upon procedure according to which players exchange a set of messages. A message is a piece of information transmitted from one player to another one.

Thus, in order to construct a communication procedure, both players have to agree first on the space of messages and to associate to every pair of actions of the original game a pair of messages - a two letter word - from the message space. Notice that if we work with distributions q that are Q-evaluated, it is always possible to associate to every pair of actions $(a_i, b_j) \in A$ a number of different two letter words such that if one of these words is selected uniformly at random, the probability that it is associated to the pair (a_i, b_j) is exactly $q(a_i, b_j)$. Once the space of two letter words is constructed, players proceed to exchange messages, i.e. words.

However, since the main problem is that in this process of exchanging messages players have no reason to trust each other, we organize the conversation in such a way that messages are public but with private meaning. Hence, one of the players, say player 1, encodes separately (by using a one-way function) every letter of all two letter words and sends them to the other player. This second one selects a encrypted word without knowing its real meaning, and encodes its letters and send them back to the first player.

Note, however, that in order to control the integrity of the whole exchange of information process, we need to impose some properties on the one-way functions being used. In particular, we need that they commute among them. Commutation allows players to deal with public messages but private meaning, since they can encode and decode previously encoded messages while keeping privacy over their real meaning. A nice physical analogy for the above process is the following: we can view encryption as equivalent

to placing a padlock on a box containing the message. A player, say Bob, initially locks all the messages in individual indistinguishable boxes with padlocks all of which have key B. The other player, say Alice, selects a box and then sends it back to him the chosen box to which she has also added her own padlock with key A. Bob removes his padlock from the box and returns to Alice the box still locked with her padlock. Notice the implicit use of commutativity in the order in which padlocks are locked and unlocked.

Hence, in order to build up the communication protocol we need to use ciphering and deciphering one-way functions with commutative properties. These functions are defined by using exponential ciphers in the way proposed by Pohling-Hellman (1978)[24]. This methodology is based on Number Theory results. In this section we show the basic concepts of Number Theory in order to understand our constructions[25].

Two integers a and b are *Congruent Module* another integer m if and only if $\exists\ k$ integer such that $a - b = km$. Let us denote by $a + mZ$ the set of all integers congruent to a module m. When the integer m is clear from the context, we write $a + mZ = \bar{a}$. Given m, it can be proved that there exist exactly m of these distinct sets given by $\bar{0}, \bar{1}, ..., \overline{m-1}$. We write $Z_m = \{\bar{0}, \bar{1}, ..., \overline{m-1}\}$.

Algebraic operations with these sets are performed in a similar way to common integers, i. e. $\bar{a} + \bar{b} = \overline{(a+b)}$ $\bar{a}\bar{b} = \overline{(ab)}$. It can be proved that $(Z_m, +, .)$ is a *commutative ring*. It is easy to see that $\bar{a} \in Z_m$ has an inverse in Z_m if and only if a is prime to m (i.e. the maximum common divisor of a and m is 1). If $\bar{a}$ has an inverse it is said that it is a *unit* of the ring Z_m. The number of units of Z_m is then the number of integers lower than m and prime to m. This number is denoted by $\phi(m)$, where ϕ is known as *Euler function* [26]. If $\bar{a}$ is a unit, then $\bar{a}^{-1} = \bar{a}^{\phi(m)-1}$. So, $\bar{a}^{\phi(m)} = \bar{1}$.

Let us consider the ring Z_p with p a prime number. Then, every no null

[24]The existence of one-way functions is still an open problem. The schemes of Pohling and Hellman (1978) and Rivest, Adleman and Shamir (1978) are usually considered as functions with this property. For a more detailed discussion of this topic, see Gossner (1998).

[25]A more complete exposition of them can be found in Vinogradov (1955) and Le Veque (1977)

[26]This function is given by $\phi(m) = \prod_{i=1}^{t} p_i^{m_i - 1}(p_i - 1)$ where $m = p_1^{m_1}...p_t^{m_t}$ is the prime factor decomposition of m.

element of Z_p is a unit. The ring Z_p is in fact a finite field of p elements called Galois Field of order p and denoted by $GF(p)$.

To define the set of basic messages (or 'letters'), both players choose jointly a prime number p *large enough* in a sense that we will make precise below. This set will be given by all the units of $GF(p)$ but $\bar{1}$:

$$M = Units\ GF(p) - \{\bar{1}\} = \{\bar{2}, ..., \overline{p-1}\}$$

To define the ciphering and deciphering functions of the players, each one of them, P_h, takes secretly and independently two integers e_h, d_h such that

$$(e_h + \phi(p)Z)(d_h + \phi(p)Z) = (1 + \phi(p)Z)$$

where $\phi(p)$ is the Euler function acting over p[27]. Functions are constructed from these numbers in the following way, $\forall \bar{m} \in M$, $E_h(\bar{m}) = \bar{m}^{e_h}$ and $D_h(\bar{m}) = \bar{m}^{d_h}$. It can be proved that:

1. E_h y D_h are inverse. (Since $(e_h + \phi(p)Z)(d_h + \phi(p)Z) = (1 + \phi(p)Z)$ we have that $\exists t \in Z$ such that $e_h d_h = t\phi(p) + 1$. Hence $E_h(D_h(\bar{m})) = \bar{m}^{t\phi(p)+1} = \bar{m}\bar{m}^{\phi(p)^t}$ and because $\bar{m}^{\phi(p)} = \bar{1}$, then $E_h(D_h(\bar{m})) = \bar{m}$ and these two functions are inverses).

2. The four permutations commute. $(E_h(D_{h'}(\bar{m})) = \bar{m}^{e_h d_{h'}} = \bar{m}^{d_h e_{h'}} = D_h(E_{h'}(\bar{m}))$ and similarly for any other combination.)

3. $\bar{m}$ cannot be calculated by P_h $(h = 1, 2)$ from $E_{h'}(\bar{m})$ and $D_{h'}(\bar{m})$ $(h \neq h')$. In order to break the cipher, P_h needs to know the keys $e_{h'}$ and $d_{h'}$ of player $P_{h'}$. The knowledge of one of these integers allows to ascertain the other, since they are inverses in $Z_{\phi(p)}$. The information that a player has is just a list of messages, i.e. $\bar{m}$, and its codification $\bar{m}^{e_{h'}}$. Hence, breaking the code used by $P_{h'}$ is the same than calculating the logarithm in base $\bar{m}$ of $\bar{m}^{e_{h'}}$ in the Galois field $GF(p)$, i.e. $e_h = \log_{\bar{m}}(\bar{m}^{e_{h'}})$. The fact that P_h cannot decipher this key is due to the difficulties to calculate this logarithm[28].

[27] Since p is already a prime integer, we have that $\phi(p) = p - 1$.

[28] This calculation takes $\exp((ln(p)ln(ln(p)))^{\frac{1}{2}})$ steps (See Adleman (1979)). If both

7 Structure of the communication protocol.

In this section we show the structure of the game extended by the universal scheme of plain conversation. This communication protocol acts twice in every stage of the repeated game. Firstly, both player communicate before simultaneously choosing their actions. This part of the protocol will be called 'correlation phase'. After playing actions and receiving signals, both player engage in a 'report phase' where information on the chosen actions and on the received signals is exchanged. This report phase is constructed in order to check deviations. If a deviation is observed, the cheating player will be punished by pushing him down to his minmax payoff for the rest of the repeated game. Before formally describing the stage communication phases, let us build up the set of messages to be exchanged in them.

The common language space V.

The protocol is a communication scheme defined on a common language space. This space is jointly constructed by the players from the set A by using the distribution q and its rationality.

This construction is made in two steps: Firstly, both players jointly select the set of messages (or alphabet) by choosing a big prime number p and taking $M = GF(p) - \{\bar{1}\}$. Any element of the set $M \times M$ will be called a *two letter word*. Secondly, both players selects n words from $M \times M$ with no letter in common [29]. Afterwards, they associate to each pair of strategies $(a_i, b_j) \in A$, r_{ij} words (α_k^i, β_l^j) from the set previously chosen. Hence if one of these n words is selected at random uniformly, the probability of this word to be associated to a pair of actions (a_i, b_j) is $\frac{r_{ij}}{n} = q(a_i, b_j)$[30].

players agree on the use of a prime large enough (200 digits, for instance), it would take 1.2×10^{23} steps to calculate it. Even if it is assumed that P_h may use a computer, which could make an operation every μseg (i. e. 10^{11} steps a day), he would need 10^{12} days or, in other words, several billions of years to make the above calculation. Thus, it is not possible to ascertain $\bar{m}$ from its codification. This kind of exponential ciphers, jointly with the one proposed by Rivest-Shamir-Adleman (1978), are being applied in real situations where the integrity of the exchanged information is very important (military cryptography, sales through Internet, etc.) and they are usually considered as one-way like functions.

[29] The n selected words will be formed by $2n$ different letters of M.

[30] So, if an external mediator selects one of these words and says both players the letter associated to their actions, every pair of strategies will be suggested with the same probability than the induced by the distribution q.

However, notice that the knowledge of his own letter by a player may give him more information about the other player's strategy than the knowledge of the action he is suggested to play. This information can be used in a strategic way. Hence, in order to reduce a player information, it is needed to associate new words to every pair of actions. This process is performed by building a 'replication tree' in the following way: let us consider the original set of two letter words. They form the first 'branch' of our replication tree. We proceed from this 'branch' by induction. For every action a_1,..., a_s, b_1,...,b_t we add a new row of 'branches' to our tree in the following way: for every 'branch'

$$\begin{array}{c} (\alpha^i_1, *) \\ \dots \\ (\alpha^i_{r_{i.}}, *) \\ (*, *) \\ \dots \\ (*, *) \end{array}$$

in the previous row we add $r_{i.}!$ new 'branches' by permuting $\alpha^i_1, ..., \alpha^i_{r_{i.}}$ in all the feasible ways and keeping the other letters (denoted by $*$) in their old order[31]:

$$\mathbf{a_i} \longrightarrow \begin{array}{cccc} (\alpha^i_{\sigma_1(1)}, *) & (\alpha^i_{\sigma_2(1)}, *) & & (\alpha^i_{\sigma_{r_{i.}!}(1)}, *) \\ \dots & \dots & & \dots \\ (\alpha^i_{\sigma_1(r_{i.})}, *) & (\alpha^i_{\sigma_2(r_{i.})}, *) & ..... & (\alpha^i_{\sigma_{r_{i.}!}(r_{i.})}, *) \\ (*, *) & (*, *) & & (*, *) \\ \dots & \dots & & \dots \\ (*, *) & (*, *) & & (*, *) \end{array}$$

for all σ_w $(w = 1, .., r_{i.}!)$ in the group of permutations of $\alpha^i_1, ..., \alpha^i_{r_{i.}}$.

Let us denote by V the subset of $M \times M$ which is formed by the words of all the 'branches' of the last row obtained after the above construction [32]. This set of valid words, which may be much bigger than the original one, satisfies the following properties:

[31] We show the construction for any action a_i of player 1. The addition of new rows for an action b_j of player 2 is done in the same way.

[32] It is easy to check that this construction does not depend on the order in which these actions are considered.

1. $Car(V)$ is a multiple of n (i.e. $Car(V) = \nu\, n$ where $\nu = r_{1.}!...r_{s.}!\, r_{.1}!...r_{.t}!$).

2. The number of words associated to any pair of strategies (a_i, b_j) is νr_{ij}.

3. The knowledge of any letter associated to a_i does not give more information than that of a_i. [33].

Thus, the probability of choosing a pair of messages in V associated to the strategies (a_i, b_j) is $\frac{r_{ij}}{n}$ and the knowledge of a component of the message gives the same information about the other than the correlated equilibrium distribution $q(a_i|b_j)$ and $q(b_j|a_i)$, respectively.

We have now all the elements to write down a formal description of both the correlation and the report phases:

The correlation phase.

Each player selects independently two functions E_h and D_h, permutations of M, by using exponential ciphers, in the way above considered.

Notice that there will not be a previous agreement about the pair of actions to play, since every player may prefer a different choice. Thus, to choose a pair of messages at random, our communication scheme is based on a codification of every word by, say, player 1, to allow the second one to select a pair of strategies at random without knowing its actual meaning. In the encryption process every letter of a words is codified independently of the other. Also, to avoid a player to change the order of the letters among different words, to make some actions more likely than others, we add to every word an extra letter which, once encrypted, allows players to check if two codified letters are members of the same original word. In particular, this third letter could be calculated as the product of the two letters of every word[34] , i. e. $\gamma^{ij}_{kl} = \alpha^i_k \beta^j_l$.

Our protocol has the following steps:

[33] It is important to remark that different words can appear a different number of times. In this way, although a player does not know the real meaning of a word, he could obtain some advantages by analyzing the frequencies of the different words in the list of messages.

[34] P_1 has no chance of changing letters from an original word to another without being detected by P_2, since he needs to find e_2 what, as we saw above, it is not possible. The checking that the second player has to make when he receives $((\alpha^i_k)^{e_1}, (\beta^j_l)^{e_1}, (\gamma^{ij}_{kl})^{e_1 e_2})$ is to calculate $(\gamma^{ij}_{kl})^{e_1 e_2 d_2} = (\gamma^{ij}_{kl})^{e_1}$ and to control if this element, which belongs to $GF(p)$, is the product of the two first letters of the work. It is important to remark that this

Step 1 Player 1 adds to every word (α_k^i, β_l^j) a third control letter $E_1(\gamma_{kl}^{ij})$ and he sends them to P_2.

Step 2 For every word in the list, the second player calculates $(E_2(\alpha_k^i)$, $E_2(\beta_l^j)$, $E_2(E_1(\gamma_{kl}^{ij})))$ and he sends them to P_1.

Step 3 For every word $(E_2(\alpha_k^i), E_2(\beta_l^j), E_2(E_1(\gamma_{kl}^{ij})))$, P_1 calculates $(E_1(E_2((\alpha_k^i))$, $E_1(E_2((\beta_l^j))$, $E_2(E_1(\gamma_{kl}^{ij})))$ and he checks that every (α_k^i, β_l^j) corresponds to an original word. Afterwards, P_1 selects n different codified words satisfying that $2n$ different letters appear in them (without considering the control letters)[35]. These n words are sent to P_2.

Step 4 P_2 checks that there are exactly $2n$ distinct codified letters in the list of n words received from P_1. Afterwards he calculates

$$D_2(E_1(E_2(\alpha_k^i))) = E_1(\alpha_k^i)$$

$$D_2(E_1(E_2(\beta_l^j))) = E_1(\beta_l^j)$$

$$D_2(E_1(E_2(\gamma_{kl}^{ij}))) = E_1(\gamma_{kl}^{ij})$$

and he checks, by using $E_1(\gamma_{kl}^{ij})$, that the two codified letters $(E_1(\alpha_k^i), E_1(\beta_l^j))$ are members of the same original word of the set V [36]. If it is detected that P_1 has deviated, the protocol will start again. Otherwise,

---

checking procedure is made by the second player without having any information about the real meaning of the words ciphered by P_1.

[35] A more intuitive way to see what P_1 is doing at this step is the following: after building up the replication tree some new 'branches' of words have been added to the original list. Each one of these 'branches' is a replication of the original list, where the way in which the letters are combined has been altered. At this step of the protocol, P_1 selects one of these 'branches' (without knowing which is the chosen one) and sends it to P_2. Afterwards, P_2 can select uniformly at random a word of this block. The two-step selection is necessary to restrict P_2 extra information from analyzing the number of times that every word appears in V. For instance, one can realize that in the set V of our example (section 4) the words associated to (a_2, b_2) appear once, but those associated to the other pairs of actions appear twice. Since the codifying and deciphering functions are bijections, the same difference in the number of words will be maintained after their encryption.

[36] In order that the protocol works correctly, the knowledge of $E_1(\gamma_{kl}^{ij})$ must allow P_2 to be sure that $(E_1(\alpha_k^i), E_1(\beta_l^j))$ are the two letters which constitute an original word, without giving him any information about the real meaning of the associated word (α_k^i, β_l^j).

P_2 selects at random uniformly a pair $(E_1(\bar{\alpha}_k^i), E_1(\bar{\beta}_l^j))$ and he sends $(E_2(E_1(\bar{\alpha}_k^i)), E_2(E_1(\bar{\beta}_l^j)))$ to P_1.

Step 5 P_1 calculates $D_1(E_2(E_1(\bar{\alpha}_k^i))) = E_2(\bar{\alpha}_k^i)$ and $D_1(E_2(E_1(\bar{\beta}_l^j))) = E_2(\bar{\beta}_l^j)$.

Step 6 P_1 sends $E_2(\bar{\beta}_l^j)$ to P_2 and P_2 sends $E_1(\bar{\alpha}_k^i)$ to P_1.

Step 7 P_1 calculates $D_1(E_1(\bar{\alpha}_k^i)) = \bar{\alpha}_k^i$ and P_2 calculates $D_2(E_2(\bar{\beta}_l^j)) = \bar{\beta}_l^j$.

At the end of this correlation phase, both player are suggested to play actions $(a_i, b_j) \in A$. These actions have been selected according to the probability distribution q. Let us notice that the way in which the protocol is established guaranties that the only information that P_1 has about the action to be played by P_2 is $q(b_j|a_i)$. The same remark can be done on the information which P_2 has about P_1 suggestion.

This correlation phase allows players to choose a pair of actions in A according to a rational probability distribution. However, the distribution $q \in B_1 \cap B_2$ that we are trying to emulate is not, necessarily, rational. Forges (1990) and Urbano and Vila (1997) show a way to extend this kind of protocols to real distributions by just adding a previous jointly controlled lottery: the convex polyhedron $B_1 \cap B_2$ is defined by linear inequalities whose parameters are rational numbers (the payoffs of the stage game, that are rational in our case). Hence, the vertices of $B_1 \cap B_2$ are rational distributions and any $q \in B_1 \cap B_2$ can be written as a convex combination of a finite number of Q-evaluated distributions (the vertices of the set). Therefore, the one-stage payoffs associated to q can be obtained by playing firstly a jointly controlled lottery in order to choose a vertex. The probability to choose any vertex is given by the convex coordinate of q in that given vertex[37]. Then, players apply the described coordination phase to choose a pair of actions in A according to the vertex distribution previously selected. See Forges (1990) for details. Hereafter, we consider that the distributions involved are rational. This assumption is done without loss of generality[38].

Once the correlation phase is finished, P_1 and P_2 play their actions (not necessarily the suggested ones) and receive their signal. It is clear that if

[37] Two concrete ways to performance this jointly controlled lottery can be found in Aumann, Maschler and Stearns (1968) and Urbano an Vila (1997).

[38] Otherwise, both players would engage in the described jointly controlled lottery before performing the correlation phase of the protocol.

both players follow the above protocol for a distribution q such that $u(q) \in u(B_1 \cap B_2) \cap IR$, they obtain the same payoff than that of the extensive form correlated equilibrium associated to q. But player may have incentives to deviate from the suggested actions[39]. Hence, further controls are necessary.

The report phase.

After playing the action of the stage game, a second communication phase takes place. This report phase, much shorter than that of the correlation phase, will be used by players in order to decide whether ascribing or not a deviation to the opponent and hence whether starting or not a punishment strategy. The steps of this phase can be described as follows:

Step 8 P_1 sends the signal[40] $l_1(\bar{a}_i, \bar{b}_j)$, where $(\bar{a}_i, \bar{b}_j)$ are the actions actually played in the stage game. P_2 sends $l_1(\bar{a}_i, \bar{b}_j)$ to P_1.

Step 9 P_1 sends $E_2(\bar{\alpha}_k^i)$ to P_2 and P_2 sends $E_1(\bar{\beta}_l^j)$ to P_1.

Step 10 P_1 calculates $D_1(E_1(\bar{\beta}_j^l)) = \bar{\beta}_j^l$ and he discovers that P_2 has been actually suggested to play b_j. By the same procedure, P_2 discovers that the action suggested to P_1 was a_i.

This report phase will provide the players with the elements that they need to detect deviations and to support the equilibrium by the threat of minmax punishments. These aspects will be clarified when the equilibrium strategies will be precisely defined.

[39]Since $q \in B_1 \cap B_2$ it can be shown that there does not exist profitable unilateral deviations from the protocol if players are restricted to use indistinguishable more informative deviations (this can be proved by just replicating the proof of appendix 1 of Urbano and Vila (1997) for more informative deviations.). However, distinguishable and indistinguishable but less informative deviations may produce profitable results. Therefore, more complex strategies must be defined in order to establish our main result.

[40]Since the signal sets L_h are finite, players are able to associate to each signal an element of $GF(p)$ and to exchange the associate element of $GF(p)$ instead of the signal itself. We prefer to describe the step as if the actual signal were sent, in order to avoid unnecessary complexity in the process.

8 ε - sureness of communication protocol.

In this section we analyze the security level of our protocol, i. e. the probability of a player to detect a rival's deviation[41]. This analysis is undertaken under the assumption that player 1 deviates and player 2 faithfully follows the protocol.

A 'deviation from the rules' by a player is a plan to correlate actions in a way different from that prescribed by the protocol. Here, the plan consists of sending different messages from the ones specified by the rules.

Definition 5 *A communication protocol is ε-sure if any deviation from the rules is detected with probability $1-\varepsilon$.*

As it was said above, to construct the set of messages both players have to start by choosing jointly a prime number p. The next proposition shows that this prime can be chosen in such a way that the correlation phase and part of the report phase are ε-sure, for each positive ε.

Proposition 2 *The communication protocol (but step 8) is ε-sure, i.e. $\forall\, \varepsilon > 0$, $\exists$ p prime such that P_2 detects that P_1 has deviated with probability $1-\varepsilon$.*

Proof: Let us analyze first the correlation phase. Let $E_2(\bar{\beta})$ be the message suggested by the protocol to player 1 at step 6. The deviation of P_1 consists of sending to P_2 a message $E_2(\beta^\star)$ different from $E_2(\bar{\beta})$. P_2 will detect this deviation if and only if $\beta^\star$ is not associated to any feasible action b_j, $j = 1, ..., t$.

Since $\beta^\star \neq \bar{\beta}$, there are $card(M) - 1 = p - 3$ possible values[42] from which $\beta^\star$ can be selected uniformly at random. Also notice that there are exactly $card(M) - n = p - 2 - n$ messages associated to no action of P_2. So

[41] Notice that we are dealing with deviations from the rules that define the communication protocol, not with deviations of a player from his suggested action when he plays the stage game. This second kind of deviations will be analyzed when proving the main result.

[42] Notice that $Card(M) = Card(Units\ of\ GF(p) - \{\bar{1}\}) = p - 2$.

$$\begin{aligned} Prob(P_2 \text{ detects}) &= Prob(\beta^\star \text{ is associated to no action } b_j) \\ &= \frac{p-n-2}{p-3} \end{aligned}$$

Given q, n is fixed, thus

$$\lim_{p\to\infty} Prob(P_2 \quad detects) = \lim_{p\to\infty} \frac{p-n-2}{p-3} = 1$$

and then the result of the proposition follows.

The same reasoning can be applied to prove that sending a message different from $E_2(\bar{\alpha}_k^i)$ at step 9 will lead with probability $1-\varepsilon$ to a message in $GF(p)$ associated to no action in A_1.

□

If the distribution q satisfies that $u(q) \in \text{IR}$, the above proposition guaranties that the threat of a minimax punishment is enough to prevent deviations from the rules at every step of the protocol, but step 8: with a probability as high as we want, P_1's deviation will reduce his average expected payoff until his minmax payoff. This idea will be formalized below.

9 Strategies of the extended game.

We have now all the elements to construct a uniform equilibrium of the game Γ extended by a universal mechanism of unmediated communication. This equilibrium emulates any extensive form correlated equilibrium payoff of the original game. The key ideas of the construction can be expressed in the following way. We know that given x an extensive form correlated equilibrium payoff of Γ there exists $q \in \Delta(A)$ such that $u(q) \in u(B_1 \cap B_2) \cap IR$ and $u(q) = x$. Since $q \in B_1 \cap B_2$ there are no profitable unilateral indistinguishable more informative deviations from q. Hence, if a player, say P_1, is suggested to play a according to q (by the correlation phase of our protocol), the only way to get an extra profit consists on deviating to a distinguishable or less informative action $\bar{a}$. But this kind of deviation can be detected in the report phase of the protocol:

1. If P_1 deviates to a distinguishable action, it may be detected as follows: by steps 9 and 10, P_2 knows that the suggested action for P_1 was a. Then, he computes $l_2(a,b)$ (where b is the action actually played by P_2) and compares it with his received signal. These signals *may* be different and the deviation may be detected.

2. If P_1 deviates to $\bar{a}$ such that $a \succ \bar{a}$, $\exists b_1, b_2 \in A_2$ such that $l_1(a,b_1) \neq l_1(a,b_2)$ but $l_1(\bar{a},b_1) \neq l_1(\bar{a},b_2)$. Hence if P_2 plays b_1 and he knows that P_1 should play a, he will expect to receive at step 8, $l_1(a,b_1)$. But, since P_1 has actually played $\bar{a}$, player 1 is not able to distinguish if P_2 has played b_1 or b_2. Hence, an inconsistency on reports may take place and the deviation may be detected.

Since Γ has an infinite number of stages, P_1 needs to deviate an infinite number of times in order to change the global average payoff. Hence, the probability to detect one of these deviation (by the above checking procedures) should be large enough to prevent cheating by the threat of the punishment.

Let us notice that in order to distinguish among distinguishable actions, a player may need to play an action out of the support of q, and this situation will never take place (actions out of support of q have zero probability to happen). To avoid this problem, we will apply the above ideas not to q but to a perturbation of it, denoted by q_k, such that $\lim_{k\to\infty} q_k = q$ and every q_k is of full support. Every q_k will be used in a number of stage games large enough to guarantee that profitable deviations will be detected with a high probability. Then, the threat of punishment will prevent any deviation.

Let us formally write the strategies to be used by the players.

Formal description of the strategies.

Let x be an extensive correlated equilibrium payoff and $q \in B_1 \cap B_2 \subseteq \Delta(A)$ such that $x = u(q) \in u(B_1 \cap B_2) \cap IR$. Let us define first a sequence of full support distributions converging to q. Let $supp(q)$ denote the support of q. q_k is defined as follows:

1. $q_k(a,b) = q(a,b) - \frac{1}{k|supp(q)|},\ if\ (a,b) \in supp(q)$

2. $q_k(a,b) = \frac{1}{k(|A|-|supp(q)|)},\ if\ (a,b) \in A - supp(q)$

Let us remark that for low values of k it may happen that $q(a,b) - \frac{1}{k|supp(q)|} < 0$. To avoid this situation, we define the distributions q_k just for $k \geq k_0$, where k_0 is the lower natural number such that that $q(a,b) \geq \frac{1}{k_0|supp(q)|}$ $\forall (a,b) \in supp(q)$.

In words, q_k is a full-support perturbation of q where $\frac{1}{k}$ of the probability density has been taken away from actions in $supp(q)$ and equally shared among the actions out of the support of q. Clearly, $\lim_{k\to\infty} q_k = q$.

For any $k \geq k_0$, let us consider the finitely repeated truncated game S_k, formed by the λ_k first stages of Γ. Each S_k will be called thereafter a block. The size of such a block, λ_k, will be made precise below and it will be large enough in order that profitable deviations along a block could be detected with high probability.

Let us denote by $\hat{a} = arg\ min_{a\in A_1}\ max_{b\in A_2}\ u_2(a,b)$ the action that induces the minmax payoff of P_2 and $\hat{b}$ the corresponding to P_1. We define now the strategies for the block S_k. At every stage game of S_k, players act as follows:

1. Both players engage in the correlation phase of the communication protocol in order to choose a pair of actions $(a,b) \in A$ according to q_k. If P_1 detects a deviation from the rules of P_2[43], he will play $\hat{a}$. P_2 acts in the same way[44]. At the end of the correlation phase, players know their suggested actions, say a for P_1 and b for P_2.

2. P_1 and P_2 play their actions following the suggestion of the correlation phase. Let us denote by $(\bar{a},\bar{b})$ the actually played actions[45]. Once the stage game is finished, P_h receives the signal $l_h(\bar{a},\bar{b})$.

3. Players engage in the report phase. If a deviation from the rules is detected at steps 9 or 10, the non-cheating player will punish the cheating one by 'minmaxing' him from this moment until the end of the game.

[43]Since the correlation phase is $\varepsilon - sure$ a deviation from the rules will be detected with a probability as high as we want.

[44]If both players detected simultaneously a deviation from the rules they would play an action at random and they would go to the next stage game

[45]Although played and suggested actions should coincide if both players follow the described strategy, we use different symbols for them in order to write down clearly the checking procedures that players will perform.

At the end of the report phase, P_1 knows b and has received a signal s_2 from P_2. If the second player has faithfully followed the process, $s_2 = l_2(\bar{a}, b)$. P_2 also receives the corresponding messages s_1 and a.

4. P_1 computes $l_1(\bar{a}, b)$ and compares it with $l_1(\bar{a}, \bar{b})$. If these signals are different, he ascribes to P_2 a deviation to a distinguishable action from the suggested one. In this case, P_1 will play $\hat{a}$ all the remaining stages. P_2 develops the same checking procedure.

5. P_1 calculates $l_2(\bar{a}, b)$ and compares it with the signal s_2 received at step 8. If these signals are different, P_1 knows that P_2 has deviated from the suggested action b to another action $\bar{b}$ such that $b \succ \bar{b}$. The reason is the following: if P_2 deviated to $\bar{b}$ at the stage game, he would receive the signal $l_2(\bar{a}, \bar{b})$. Since $\bar{b}$ is less informative than b, it may exist $\bar{\bar{a}} \in A_1$ such that $l_2(\bar{a}, \bar{b}) = l_2(\bar{\bar{a}}, \bar{b})$. Hence, P_2 does not know whether P_1 has played $\bar{\bar{a}}$ or $\bar{a}$. At step 8, P_2 must report his signal but he doubts on sending $l_2(\bar{a}, b)$ or $l_2(\bar{\bar{a}}, b)$, since he does not know which action has P_1 actually played. Therefore, with some positive probability, P_2 will send the wrong signal an it will be detected by P_1. Let us remark that the order in which the steps of the report phase are organized is a key point of this checking procedure: if the report of s_2 took place after step 9 and 10, P_2 would know the chosen action of P_1 and he would report correctly his signal. If P_1 discovers that P_2 has cheated at this point, he will play $\hat{a}$ thereafter.

   The checking procedure for P_2 can be established in the same way.

Let (τ_1^k, τ_2^k) denote the strategies of the block S_k above described. It is clear that:

1. By following (τ_1^k, τ_2^k), P_h only ascribes a deviation to $P_{h'}$ if the latter has actually cheated. However, some deviations of a player may take place and remain undetected.

2. Any deviation of P_h to an distinguishable or less informative action has a positive probability of being detected.

3. The limit average expected payoff of (τ_1^k, τ_2^k) exists and coincides with $u(q)$, i. e.

$$\exists \lim_{k\to\infty} \sum_{t=1}^{\lambda_k} E_{(\tau_1^k,\tau_2^k)}(u_t) = u(q)$$

4. Since the protocol (but step 8) is ε-sure for any $\varepsilon > 0$, we can prevent deviations from the rules by just taking ε low enough or, what is the same, a prime number p large enough.

10 Example.

Let us analyze an example of the above construction. The concerned game is an adaptation of an example of Aumann (1987)[46], whose stage game can be described by the following payoff matrix:

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array} \begin{array}{c} \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \\ \left(\begin{array}{ccc} (0,0) & (0,0) & (0,0) \\ (0,0) & (0,0) & (7,2) \\ (0,0) & (2,7) & (6,6) \end{array} \right) \end{array}$$

where $A_1 = \{a_1, a_2, a_3\}$ is the set of feasible strategies of P_1 and $A_2 = \{b_1, b_2, b_3\}$ the set of those of P_2.

Let us assume that the information structure of this one-shot game is trivial (i.e. $l_1(a_i, b_j) = a_i$ and $l_2(a_i, b_j) = b_j$) but in the next two cases:

1. $l_1(a_2, b_1) = (a_2, b_1)$
2. $l_2(a_1, b_1) = (a_1, b_1)$

Let Γ be the infinite repetition of the above one-shot game. Notice that, in this case the quotient sets for the equivalence relation $\sim$ are as follows[47]:

[46] Alternative adaptations of this basic example have been also developed in Lehrer (1991, 1992a) and Urbano and Vila (1997).

[47] The information structure in this example is not a symmetric standard-trivial one, since there exists pairs of actions where a player receives standard information and the other one does not.

1. $A_1^{\sim} = \{\{a_1\}, \{a_2, a_3\}\}$

2. $A_2^{\sim} = \{\{b_1\}, \{b_2, b_3\}\}$

and also notice that a_3 is indistinguishable and less informative than a_2 (since $l_1(a_2, b_1) = (a_2, b_1) \neq a_2 = l_1(a_2, b_2)$ and $l_1(a_3, b_1) = a_3 = l_1(a_3, b_2)$).

It is easy to check that the probability distribution $q \in \Delta(A)$, given by

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array} \begin{array}{c} \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \end{array}$$

is an element of the set $B_1 \cap B_2$ [48]. Moreover

$$(5, 5) = u(q) \in u(B_1 \cap B_2) \cap IR$$

and by proposition 1, $(5, 5)$ is the average expected payoff of an extensive form correlated equilibrium of Γ.

Fixed $k \in N$, let us construct the strategies (τ_1^k, τ_2^k) in the following way. We start by defining q_k, a full-support perturbation of q given by [49]:

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array} \begin{array}{c} \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \\ \begin{pmatrix} \frac{1}{6k} & \frac{1}{6k} & \frac{1}{6k} \\ \frac{1}{6k} & \frac{1}{6k} & \frac{k-1}{3k} \\ \frac{1}{6k} & \frac{k-1}{3k} & \frac{k-1}{3k} \end{pmatrix} \end{array}$$

Recall that the block S_k is the truncated game formed by the first λ_k one-shot games in Γ. The strategies (τ_1^k, τ_2^k) are given by:

First communication round: the correlation phase. Both players build up the elements to engage in the communication procedure. They start

[48] It is, in fact, a canonical correlated equilibrium of the stage game.

[49] q_k can be defined $\forall k \geq k_0 = 2$.

by selecting a large prime number p. Let us assume that, in our concrete case[50], $p = 43$. Afterwards, both players choose $6k$ elements from the message set $M \times M = (GP(p) - \{\bar{0}, \bar{1}\}) \times (GP(p) - \{\bar{0}, \bar{1}\})$ (whose elements are called 'words') and associate them to pair of actions in A as follows:

$$
\begin{array}{lcc}
(a_1, b_1) & \longleftarrow & (\bar{2}, \bar{3}) \\
(a_1, b_2) & \longleftarrow & (\bar{4}, \bar{5}) \\
(a_1, b_3) & \longleftarrow & (\bar{6}, \bar{7}) \\
(a_2, b_1) & \longleftarrow & (\bar{8}, \bar{9}) \\
(a_2, b_2) & \longleftarrow & (\bar{10}, \bar{11}) \\
(a_3, b_1) & \longleftarrow & (\bar{12}, \bar{13}) \\
 & & \\
(a_2, b_3) & \longleftarrow & (\bar{14}, \bar{15})... \\
 & & ((14 + (\bar{4}k - 6)), (14 + (\bar{4}k - 5)) \\
(a_3, b_2) & \longleftarrow & ((14 + (\bar{4}k - 4)), (14 + (\bar{4}k - 3))... \\
 & & ((14 + (\bar{8}k - 10)), (14 + (\bar{8}k - 9)) \\
(a_3, b_2) & \longleftarrow & ((14 + (\bar{8}k - 8)), (14 + (\bar{8}k - 7))... \\
 & & ((14 + (\bar{12}k - 14)), (14 + (\bar{12}k - 13))
\end{array}
$$

In words, players associate

1. a single word to each pair of actions that has probability of $\frac{1}{6k}$ to happen
2. $2(k-1)$ words to each pair of actions with probability $\frac{k-1}{3k}$ to appear.

In this example, words have been assigned consecutively, but any other association procedure could be used.

The role of the communication phase is to allow players to choose one of this words at random uniformly. Then, the probability of a pair of actions (a_i, b_j) to be associated to the selected word is precisely

[50] The assumption of such a small prime number is made in order to simplify the example. Actually, both players should choose a p much larger (a two hundred digits one, for instance). The size of p is determined by the security level of the functions E_h, D_h an it will be made precise in the proof of our main result.

$q_k(a_i, b_j)$. A complete description of how this correlation phase works for this concrete example is too long to be considered here (see Urbano and Vila (1997) for a detailed example of this communication protocol in a simpler case). An sketch of the main facts of this message exchange procedure is the following:

The replication of the associated words and steps one to four of our protocol, allows P_2 to choose one of the $6k$ words above at random without obtaining extra information. This situation is possible since P_2 does not know the real words (α_l, β_m), $(l, m = 1, ..., 6k)$ but their codification by E_1. Let us suppose that, in this example, the chosen codified word is $(E_1(\bar{8}), E_1(\bar{9}))$. At step 5, P_1 knows $(E_2(\bar{8}), E_2(\bar{9})) = D_1(E_2(E_1(\bar{4}))), D_1(E_2(E_1(\bar{5}))))$. By steps 6 and 7, P_1 learns that his suggested action is associated to $\bar{8}$ and he keeps the information that P_2 has been advised to play according to a message whose codification is $E_2(\bar{9})$. The situation is symmetric for player 2.

Let us remark that if P_1 deviates at step 6 (checking procedures prevent deviation from the rules at the other steps), he does it in a completely uncontrolled way: since he does not know E_2, he can only send a message $\hat{\beta} \neq E_2(\bar{9})$. Then, P_2 deciphers this message by calculating $D_2(\hat{\beta})$. If $D_2(\hat{\beta})$ is not one of the $6k$ valid letters (i.e. $D_2(\hat{\beta}) \notin \{\bar{3}, \bar{5}, ..., \overline{(1+12k)}\}$) P_2 discovers the deviation and punishes P_1. Let us notice that, since P_1 has no control on the cheating process, his probability to be discovered increases with the size of the message set[51].

Stage game. Both players act according to the protocol's suggestions: P_1 plays a_2 associated to $\bar{8}$ and P_2 plays b_1 associated to $\bar{9}$. Then, P_1 receives the signal $l_1(a_2, b_1) = (a_2, b_1)$ and P_2 receives $l_2(a_2, b_1) = b_1$.

Second communication round: the report phase. At this phase, players exchange information about their past behavior. At step 8, they make public their received signals ((a_2, b_1) for P_1 and b_1 for P_2). By steps 9 and 10, P_1 is able to calculate $D_1(E_1(\bar{9})) = \bar{9}$ and he discovers

[51]The probability of not being detected is given by the ratio of the number of valid messages (fixed) over the cardinal of the whole message set. Hence, the larger is the set of messages, the smaller is the probability of a deviation to be undetected.

that P_2 was suggested to play b_1. In the same way, P_2 is informed about the action selected for P_1, say a_2.

Deviations here have the same properties than in the correlation phase: since there is no control on the meaning of a false message, a cheating behavior can be detected with high probability by making wide enough the set of messages. Let us notice that the order of the steps in the report phase is a key point for the checking procedures to work (if P_1 knew the suggested action of P_2 before reporting about his signal, he would be able to calculate the signal corresponding to his suggested action and to send it to P_2, instead of the actually observed one).

Checking procedures. P_h $(h = 1, 2)$ compares the received and expected signal in order to detect deviations. To clarify this control process, let us suppose that P_1 deviates at the stage game by playing an action distinct from a_2. Two possibilities arises:

1. P1 can play an action distinguishable from a_2, say a_1. Since P_2 knows that P_1 should have played a_2, he expects to receive $l_2(a_2, b_1) = b_1$ but he actually receives a different signal $l_2(a_1, b_1) = (a_1, b_1)$. Hence, he ascribes a deviation to P_2.
2. P1 can play an action indistinguishable from a_2 but less informative, say a_3. Since P_2 knows that P_1 should have played a_1, he assumes that P_1 knows when P_2 is playing b_1 or b_2 $(l_1(a_2, b_1) = (a_2, b_1) \neq a_2 = l_1(a_2, b_2))$. But, after the deviation, the situation is completely different: P_1 has actually received $l_1(a_3, b_1) = a_3 = l_1(a_3, b_2)$ and he does not know if P_2 has played either b_1 or b_2. Hence, when P_1 is asked to report his observed signal at step 8, he hesitates between sending either $l_1(a_2, b_1)$ or $l_1(a_2, b_2)$ which are, in fact, different. If P_1 finally sends $l_1(a_2, b_2)$, P_2 will discover that a deviation has taken place. Let us remark that the probability of this situation to happen is always positive.

11 Proof of the main result.

The key idea of the proof is the following: Let us suppose that P_1 is the cheating player. Since q_k is very close to $q \in B_1 \cap B_2$ the payoff that P_1

could obtain by just deviating to indistinguishable but more informative actions should be very close to the expected payoff of q. Hence, to reach a more profitable payoff, he should play with distinguishable or less informative deviations. If the length of S_k is very large, many of these deviations will take place in order to increase significativelly the average payoff of the block. But, P_2 is able to detect such deviations at the end of each one-shot game with a positive probability. Hence, by making λ_k very large we can guarantee that the total probability of detecting a deviation will be high enough to prevent P_1 from cheating. The formal proof of this idea is as follows:

Let x be an extensive form correlated equilibrium payoff of Γ. Without loss of generality, we assume that x assigns to each player a payoff that is strictly bigger than his minmax level[52]. We will show that x is a uniform equilibrium payoff of the game extended by plain conversation. To reach this goal, we will use the following characterization (See Sorin 1990): x is a uniform equilibrium payoff if and only if there exists a sequence ε_n with $\lim_{n\to\infty} \varepsilon_n = 0$ and sequences of strategies (τ_1^n, τ_2^n) and natural numbers λ_{k_n} such that (τ_1^n, τ_2^n) is an ε_n-equilibrium of the truncanted repeated game consisting on the first λ_{k_n} stages of Γ, leading to a payoff within ε_n of x. Fix $\varepsilon_n > 0$.

Given x, we know that there exists a (rational) probability distribution $q \in \Delta(A)$ such that $x = u(q) \in u(B_1 \cap B_2) \cap IR$. Let $u_1(q)$ denote the expected payoff of P_1 at the one-shot game, when both players are choosing their actions according to q:

$$u_1(q) = \sum_{a\in A_1,\ b\in A_2} q(a,b)u_1(a,b)$$

In the same way, $\forall k \geq k_0$[53], we define:

$$u_1(q_k) = \sum_{a\in A_1,\ b\in A_2} q_k(a,b)u_1(a,b)$$

[52]If one player is assigned his minimax payoff by x, he will be indifferent between following or defeating the protocol. Since Nash equilibrium inequalities are defined by using 'lower or equal' conditions, following the strategies constitutes a Nash equilibrium of the extended game.

[53]Recall that k_0 is the lower natural number such that $q(a,b) \geq \frac{1}{k_0|supp(q)|}$.

Let u_1^{mM} and u_1^{MM} denote the minimax and the maximax[54] payofss of P_1 at the stage game.

Before engaging in each correlation communication phase, P_1 has to decide whether following faithfully the protocol or cheating. Let us notice that, since $u_1^{mM} < u_1(q)$, there exists a $\eta_n > 0$ such that

$$\eta_n u_1^{MM} + (1 - \eta_n) u_1^{mM} \leq u_1(q)$$

Hence, if the probability of P_1 to be detected when he deviates is at least $1 - \eta_n$, the threat of the minimax punishment is enough to prevent any deviation. Since the protocol is η_n-sure for every $\eta_n > 0$, both players can choose a prime number p_n large enough in order to make unilateral deviations from the rules unprofitable. Let us assume that this is the case.

By deviating to indistinguishable more informative actions, P_1 can hardly increase his expected payoff: let $u_1^\star(q_k)$ be the biggest payoff that P_1 can obtain at any stage game of the block S_k if he deviates in this way, i. e.:

$$u_1^\star(q_k) = \sum_{a \in A_1,\ b \in A_2} q_k(a,b) u_1(a^\star, b)$$

where $a^\star = \ arg\max_{a_i \in A_1,\ a_i \succ a} \sum_{b \in A_2} q(a,b) u_1(a_i, b)$. Hence,

$$\begin{aligned} u_1^\star(q_k) &= \sum_{a \in A_1,\ b \in A_2} q(a,b) u_1(a^\star, b) \\ &= \sum_{(a,b) \in supp(q)} (q(a,b) - \frac{1}{k|supp(q)|}) u_1(a^\star, b) \\ &+ \sum_{(a,b) \notin supp(q)} \frac{1}{k(|A| - |supp(q)|)} u_1(a^\star, b) \\ &= \sum_{(a,b) \in supp(q)} q(a,b) u_1(a^\star, b) + \frac{1}{k} N \end{aligned}$$

where

[54] $u_1^{MM} = max_{a \in A_1} max_{b \in A_2} u_1(a,b)$.

$$N = \sum_{(a,b)\notin supp(q)} \frac{1}{(|A| - |supp(q)|)} u_1(a^\star, b) - \sum_{(a,b)\in supp(q)} \frac{1}{|supp(q)|} u_1(a^\star, b)$$

is a constant that does not depend on k.

Since $q \in B_1 \cap B_2$, no indistinguishable more informative deviation may improve the expected payoff of q. Then

$$\sum_{(a,b)\in supp(q)} q(a,b) u_1(a^\star, b) \leq u_1(q)$$

Let $k_1 \in N$ such that $\forall k \geq k_1$, $\frac{1}{k}N < \frac{\varepsilon_n}{3}$. Assuming that $k \geq k_1$, we have that:

$$u_1^\star(q_k) \leq u_1(q) + \frac{\varepsilon_n}{3}$$

Therefore, if P_1 wanted to increase his average payoff in S_k by more than $\frac{\varepsilon_n}{3}$ he would have to play actions that are distinguishable or less informative than those he has been suggested to play. Let d_k the minimum proportion of repetitions of the stage games in S_k in which P_1 needs to make detectable deviations in order to reach an average payoff of at least $u_1(q) + \frac{2\varepsilon_n}{3}$. Let us define δ_k as the lower bound probability of P_2 to detect a deviation of P_1 to a distinguishable or less informative action in each stage game. δ_k is always greater than zero, since q_k is of full support and the action from A_2 that precisely allows to detect any deviation has a positive probability to be suggested by the correlation phase.

Thus, if P_2 deviates to a distinguishable or less informative action, he will be detected with a probability at least δ_k. Since S_k lasts λ_k stages, to obtain an extra profit of $\frac{\varepsilon_n}{3}$, P_2 need to risk to commit detectable deviations at least in $\lambda_k d_k$ one-shot games. Hence, he will be detected with probability at least of $\lambda_k d_k \delta_k$. We take λ_k such that[55].

$$\lambda_k d_k \delta_k u_1^{mM} + (1 - \lambda_k d_k \delta_k) u_1^{MM} \leq u_1(q_k)$$

[55]Since $u_1^{mM} < u_1(q)$, there exists $k_3 \in N$, such that $\forall k \geq k_3$, $u_1^{mM} < u_1(q_k)$. For any k satisfying this assumption, it is clear that there exists a λ_k that satisfies this property.

Then, the length λ_k guaranties that P_1 has no incentives to deviate to detectable actions in $\lambda_k d_k$ or in more stage games. Hence, P_1 will obtain an average payoff in S_k within $u_1(q) + \frac{2\varepsilon_n}{3}$ no matter what he has done. Notice that λ_k depends of ε_n and that the lower is ε_n the larger is λ_k.

By taking k_n large enough (in a sense that will be made precise at the end of the proof), we have defined a pair of strategies (τ_1^n, τ_2^n) for the block game S_k that satisfies:

1. (τ_1^n, τ_2^n) is a ε_n-equilibrium of S_{k_n}.

   Proof: Let us assume that P_1 deviates by playing an arbitrary strategy $\bar{\tau}_1^n$. We have that:

$$\begin{aligned} u_1(q_k) &= \sum_{a \in A_1,\ b \in A_2} q(a,b) u_1(a,b) \\ &= \sum_{(a,b) \in supp(q)} (q(a,b) - \frac{1}{k|supp(q)|}) u_1(a,b) \\ &+ \sum_{(a,b) \notin supp(q)} \frac{1}{k(|A| - |supp(q)|)} u_1(a,b) \\ &= \sum_{(a,b) \in supp(q)} q(a,b) u_1(a,b) + \frac{1}{k} M \\ &= u_1(q) + \frac{1}{k} M \end{aligned}$$

   where

$$M = \sum_{(a,b) \notin supp(q)} \frac{1}{(|A| - |supp(q)|)} u_1(a,b) - \sum_{(a,b) \in supp(q)} \frac{1}{|supp(q)|} u_1(a,b)$$

   is a constant that does not depend on k. Hence, there exists $k_2 \in N$ such that, $\forall k \geq k_2$

$$u_1(q_k) \leq u_1(q) + \frac{\varepsilon_n}{3}$$

and we have that:

$$\frac{1}{\lambda_{k_n}} \sum_{t=1}^{\lambda_{k_n}} E_{(\tau_1^n, \tau_2^n)}(u_1^t) = u_1(q_k) < u_1(q) + \frac{\varepsilon_n}{3}$$

Moreover,

$$\frac{1}{\lambda_{k_n}} \sum_{t=1}^{\lambda_{k_n}} E_{(\bar{\tau}_1^n, \tau_2^n)}(u_1^t) \leq u_1(q) + \frac{2\varepsilon_n}{3}$$

Hence, by deviating from τ_1^n, P_1 cannot increase his payoff in more than ε_n.

2. The average expected payoff of (τ_1^n, τ_2^n) is within ε_n of $x = u_1(q)$, as we can observe from the above inequalities.

Summarizing, given an extensive form correlated equilibrium payoff x of Γ and given any ε_n from a sequence converging to zero, by taking $k_n = max\ \{k_0, k_1, k_2, k_3\}$ we have built up a block game S_{k_n} of size λ_{k_n} and a pair of strategies of S_{k_n} denoted by (τ_1^n, τ_2^n) such that: (1) (τ_1^n, τ_2^n) is an ε_n-equilibrium of S_{k_n} and (2) (τ_1^n, τ_2^n) leads a payoff within ε_n of x.

Thus, we have that x is a uniform equilibrium payoff of the game Γ extended by our universal communication protocol. The fact that the uniform equilibrium payoff set is included in both the upper and the Banach equilibrium payoff sets concludes the proof.

□

12 Concluding remarks.

We have applied an unmediated communication protocol to generate internal correlation in infinitely repeated two-player games with imperfect monitoring and without discounting. The key of our approach is that players can

generate private information through public messages with a modern cryptosystem. Our main result states that the Nash equilibrium payoffs of the extended game contain the extensive form correlated equilibrium payoffs of the usual repeated game. Similar results have been obtained by Gossner (1998) by modeling agents by polynomial Turing machines (and assuming the existence of a one-way function) in a context of perfect monitoring and by Lehrer (1991) for the case of the symmetric standard-trivial information structure of the perfect monitoring.

Communication using public messages in repeated games with discounting (and imperfect monitoring) may be not too efficient. In particular, providing incentives for players to reveal their observations generate revelation constraints which, combined with signal imperfections, may be a source of inefficiencies. Hence, strong assumptions have to be made to keep payoffs close to the Pareto frontier (see, for instance, Fundenberg, Levine and Maskin (1994), Fundenberg and Levine (1991), Ben-Porath and Kahneman (1996) and Compte (1994, 1998), among others). Hence, one may wonder if our result extends to infinitely repeated games with discounting or to finitely repeated games in order to achieve efficiency. Gossner (1998) claims that no equivalent result could hold for such cases (with perfect monitoring) when players are modeled as Turing machines. The reason is that the limitation of the computational power is only effective when the horizon tends to ∞. Although we have not develop any intuition for these situations, we unfortunately suspect that this negative result may be true.

The extension to games with more than two players seems to need some work. In the case of two players, a deviation can be attributed to one player: the opponent. However, if there are more than two players, who should be blamed for the deviation and who should be punished?. Also, it may be the case that not all the players realized the deviation and the information about the alleged deviation should be spread among the players. This is left for future research.

References.

L. Abreu, D. Pearce and E. Stachetti (1986): 'Optimal cartel equilibria with imperfect monitoring.' *JET 39, 251-269.*

L. Adleman (1979): 'A subexponential algorithm for the discrete logarithm with applications to cryptography.' *Proc. IEEE 20th annual symp. on Found. of Comp. Sci. 55-60.*

M. Amitai (1996): 'Cheap talk with incomplete information on both sides.' *Discussion paper 90. The Hebrew University of Jerusalem. Center for rationality and interactive decision theory.*

R. Aumann (1974): 'Subjectivity and correlation in randomized strategies.' *Journal of Mathematical Economics 1, 67-96.*

R. Aumann (1985): 'Repeated games.' in 'Issues in contemporary microeconomics and welfare' 209-242 (G. R. Feiwel, ed.) *Macmillan, New York.*

R. Aumann (1987): 'Correlated equilibrium as an expression of bayesian rationality.' *Econometrica 55, 1-18.*

R. Aumann, M Maschler and R. E. Stearns (1968): 'Repeated games of incomplete information.' *Mathematical Inc. Princeton. (Chapter IV 117 - 216)*

R. Aumann and S. Hart (1993): 'Polite talk isn't cheap' *Mimeo.* Hebrew University of Jerusalem.

I. Barany (1992): 'Fair distribution protocols or how the players replace fortune.' *Mathematics of Operations Research 17, 327-340.*

E. Ben-Porath and M. Kahneman (1996): 'Communication in repeated games with private monitoring.' *JET 70, 281-297.*

M. Blum (1981): 'Three applications of the oblivious transfer: Coin flipping by telephone, How to exchange secrets and How to send certified electronic mail.' *Dept. EECS, Univ of California, Berkeley.*

O. Compte (1994): 'Comunication in repeated games with private monitoring.' *Unpublished Ph. D. dissertation, Stanford.*

O. Compte (1998): 'Comunication in repeated games with imperfect private monitoring.' *Econometrica 66, 597-626.*

A. Dixit and C. Shapiro (1985): 'Entry dynamics with mixed strategies.' L. G. Thomas, ed. *The economics of strategic planning Lenxington Books, Lenxington.*

J. Farrell (1987): 'Cheap talk, coordination and entry.' *Rand Journal of Economics 18, 34-39.*

J. Farrell (1988): 'Communication, coordination and Nash equilibrium.' *Econ. Lett. 27, 209-214.*

J. Farrell and M. Rabin (1996): 'Cheap talk.' *Journal of Economic Perspectives 10, 103-118.*

J. Farrell and G. Saloner (1988): 'Coordination through committees and markets.' *Rand Journal of Economics 19, 235-252.*

F. Forges (1986): 'An approach to communication equilibria.' *Econometrica 54, 1375-1385.*

F. Forges (1988): 'Can sunspots replace a mediator?.' *Journal of Mathematical Economics 17, 347-368.*

F. Forges (1990): 'Universal mechanisms.' *Econometrica 58, 1341-1364.*

D. Fundenberg and D. Levine (1991): 'An approximate folk theorem with imperfect private monitoring.' *JET 54, 26-47.*

D. Fundenberg, D. Levine and E. Maskin (1994): 'The folk theorem with imperfect public information.' *Econometrica 62, 997-1040.*

O. Gossner (1997): 'Secure protocols or how communication generates correlation.' *Forthcoming in Journal of Economic Theory.*

O. Gossner (1998): 'Repeated games played by crytographically sophisticated players.' *Mimeo, CORE.*

S. Hurkens (1996): 'Multi-sided pre-play communication by burning money.' *JET 69, 186-197.*

E. Lehrer (1990): 'Nash equilibria of n-player repeated games with semi-standard information.' *International Journal of Game Theory 19, 191-297.*

E. Lehrer (1991): 'Internal correlation in repeated games.' *International Journal of Game Theory 19, 431-456.*

E. Lehrer (1992a): 'Correlated equilibria in two-player repeated games with nonobservable actions.' *Mathematics of Operations Research 17, 175-199.*

E. Lehrer (1992b): 'Two-player repeated games with nonobservable actions and observable payoffs.' *Mathematics of Operations Research 17, 200-224.*

E. Lehrer (1992c): 'On the equilibrium payoffs set of two player repeated games with imperfect monitoring.' *International Journal of Game Theory 20, 211-226.*

E. Lehrer (1996): 'Mediated talk.' *International Journal of Game Theory 25, 177-188.*

E. Lehrer and S. Sorin (1997): 'One shot public mediated talk.' *Games and Economic Behavior 20, 132-148.*

S. A. Matthews and A. Postlewaite (1989): 'Pre-play communication in two-person sealed-bid double auctions.' *JET 48, 238 - 263.*

R. B. Myerson (1991): 'Game Theory. Analysis of Conflict.' *Harvard University Press, Cambridge.*

S. Pohling and M. Hellman (1978): 'An improved algorithm for computing logarithms over GF(p) and its cryptographic significance.' *IEEE Trans. on info. theory 24, 106-110.*

M. Rabin (1981): 'Exchange of secrets.' *Dept. of Applied Physics, Harvard Univ. Cambridge, Mass.*

M. Rabin (1990): 'Communication between rational agents.' *JET 51, 144-170.*

M. Rabin (1993): 'A model of pre-game communication.' *JET 63, 370-391.*

R. Radner (1986): 'Repeated partnership games with imperfect monitoring and no discounting.' *Review of economic studies 53, 1, 43-58.*

R. L. Rivest, A. Shamir and L. Adleman (1978): 'A method for obtaining digital signatures and public key cryptosystems.' *Comm. ACM 21(2), 120-126.*

A. Rubinstein and M. Yaari (1983): 'Repeated insurance contracts and moral hazard.' *JET 30, 74-97.*

S. Sorin (1990): 'Supergames', in T. Ichiisi, A. Neyman and Y. Tauman (eds.), 'Game theory and applications', 46-63 *Academic Press.*

A. Urbano and J. E. Vila (1997): 'Pre-play communication and coordination in two-player games.' *IVIE working paper WP-AD 97-26.*

A. Urbano and J. E. Vila (1998): 'Unmediated communication under incomplete information.' *Depto. Analisis Economico. Universitat de Valencia. Mimeo.*

W. J. Le Veque (1977): 'Fundamentals of number theory.' *Addison-Wesley, Mass.*

I. M. Vinogradov (1955): 'An introduction to the theory of numbers.' *Pergamon press, Elmsford, N.Y.*