PRE-PLAY COMMUNICATION AND COORDINATION IN TWO-PLAYER GAMES*

Amparo Urbano and José E. Vila**

WP-AD 97-10

Correspondence to: Amparo Urbano, Universitat de Valéncia, Dpto. Análisis Económico, Campus de los Naranjos, Edificio Departamental Oriental, 46022 Valencia, e-mail: Amparo.Urbano@uv.es

Editor: Instituto Valenciano de Investigaciones Económicas, S.A.
First Edition December 1997
ISBN: 84-482-1645-8
Depósito Legal: V-4628-1997

---

* We wish to thank financial aid from the Valencian Institute of Economic Research (IVIE) and partial support by DGICYT under project PB93-0684. We also thank the comments and suggestions of participants of the Fourth Summer Meeting (Valencia, July 1996), the International Workshop on Game Theory and Politics and Spanish Meeting on Game Theory (Santiago de Compostela, July 1996), the Seventh International Conference on Game Theory (Stony Brook, July 1996) and the XXI Simposio de Análisis Económico (Barcelona, December 1996). The usual disclaimer applies.

**Amparo Urbano & José E. Vila: University of Valencia..

PRE-PLAY COMMUNICATION AND COORDINATION IN TWO-PLAYER GAMES

Amparo Urbano and José E. Vila

A B S T R A C T

The main result of this paper is that any correlated equilibrium pay-off of a two-player complete information game with rational parameters can be reached through an unmediated costless pre-play conversation scheme. This problem was left open by Barany and Forges' analysis. Our communication protocol does not rely on external mediators of any kind. It is also self-enforcing (in the sense that no player has an incentive to deviate if the other does not) and quasi-sure (in the sense that a 'deviation from the rules' of a player can be detected by the other with a probability as close as one as we want). Coordination failures that may arise in many economic situations are solved by applying our pre-play communication scheme.

KEYWORDS: Communication; Protocol; Coordination.

1 Introduction.

Two strands of the literature dealing with the role of communication in non-cooperative games theory have been developed recently. The first does not model the process by which players exchange messages and 'reasonable' arguments justify properties that we may expect from communication[1]. In the second approach the communication process is explicitely modelled and it is included as a preplay stage in which players exchange messages - in some specified way - before actually playing. This paper follows the second approach.

Also, it has been often suggested that if the players of a game can communicate, then the appropiate equilibrium notion should not be Nash equilibrium but the larger class of correlated equilibria (Aumann (1974, 1987), Myerson (1991)). The idea is that if agents can talk, they could reach a self-enforcing agreement to let their actions be jointly conditioned on the outcome of a stochastic trial, rather than independently as assumed by the Nash construction. However, Aumann's notion of correlated equilibrium is not built on an explicit model of verbal communication, and correlated strategies may require an outside correlation device, which may a priori depend on the parameters of the game.

One may take the view that the correlation in correlated equilibria should be thought of as the result of the players receiving 'endogenous' correlated signals, so that the notion of correlated equilibrium is particularly appropiate in situations with preplay communication, for then the players might be able to design and implement a procedure for obtaining correlate private signals. Barany (1992) shows that if there are at least *four players* any correlated equilibrium of a normal- form game with complete information coincides with a Nash equilibrium of an extended game in which the players engage in costless conversation (cheap talk) before they play the strategic-form game in question. However, under this scheme of conversation - protocol - if there are only two players then the set of Nash equilibria with cheap talk coincides with

[1]See for instance Rabin (1990, 1993), Farrell (1987, 1988), Farrell and Rabin (1996) and Hurkens (1996) among others.

the subset of correlated equilibria induced by perfectly correlated signals, i.e. publicly observed randomized devices.

Forges (1990) extends the result of Barany to games with incomplete information. She constructs a scheme of plain conversation which is a universal mechanism for all noncooperative games with incomplete information and at least *four players*[2]. In particular, she shows that every solution that can be achieved by means of an arbitrary communication mechanism - a procedure helping the players to exchange information and to coordinate decisions - is a correlated equilibrium payoff of the game extended by the scheme of plain conversation[3] and by Barany's construction a similar result holds also with the Nash equilibrium concept. The scheme of plain conversation is universal because it does not depend on the specifications of the game, nor on the solution to achieve.

Lehrer and Sorin (1994) and Lehrer (1996) relax the assumption of at least four player by using mediated communication. They use communication protocols which rely on a mediator. This mediator receives private signals from the players and makes deterministic public announcements. They show that the players can implement any correlated equilibrium with the help of this kind of communication [4]. Aumann and Hart (1992) present a type of pre-play communication, called polite talk, in complete and incomplete information games. It turns out that, in complete information games, the convex hull of the Nash equilibrium payoffs set is generated. Gossner (1996) examines how information stems from communication, therefore linking communication mechanisms and information structures.

In this paper we construct a scheme of unmediated communication (with finite message sets) which is a universal mechanism for all noncooperative two player games with complete information. Thus, we extend Barany's results to this class of games and we show that any correlated equilibrium payoff of such games can be reached through a previous costless pre-play conversation phase, that in turn, shows the power of plain conversation as a coordination mechanism.

[2]If the requirement of finite message sets is relaxed, the result holds also for the three player case. See Forges (1990).

[3]The corresponding equilibrium strategies use only finite set of messages.

[4]They also prove that any communication equilibrium of an incomplete information game can be achieved in this way. See Lehrer and Sorin (1994) for details.

Barany's scheme assumes that there is a secure channel between any two players. Hence, when there are only two individuals all messages are public and the largest set equilibrium payoffs which can be achieved by extending the game with the communication scheme is the convex hull of the Nash equilibrium payoffs (jointly controlled lotteries).

We depart from this approach and since the main problem is that in the process of exchanging messages, the players have no reason to trust each other, we organize the conversation in such a way that messages are public but with private meaning. This approach is closely related to the one used to model 'oblivious transfers'[5] which has been used to solve problem such that 'coin flipping by phone' (Blumm (1981)) or 'playing mental poker with no real cards' (Rabin (1981))[6].

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 a communication encryption scheme with private key, which is based on computing exponentials over a finite field[7]. Our communi-

[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. Obviously any player may try to cheat.

[7] 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.

cation scheme illustrates the familiar game-theoretic point that a player may gain from limiting his own information if the opponents know he has done so, because in this way he may induce the opponents to play in a desirable fashion.

We assume that the preplay communication phase is finite and that the player have bounded calculation skills, i.e. they need a non-null period of time to make any calculation[8]. Also a technical assumption, shared with Barany and Forges, is needed: the payoffs of the game must be rational.[9].

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 correlated equilibrium as a Nash equilibrium of the game extended by a preplay communication stage for the class of two-person games with complete information. Thus, it allows to solve the coordination failures that arise in many economic situations. For instance, our pre-play communication scheme can achieve complete coordination in some two-player entry games whose payoffs are qualitatively like the 'battle of sexes' and in other situations where a mixture of coordination and conflict arises.

The paper is organized as follows. Section 2 states our main result and interprets it. Some useful key points of Number Theory are presented in section 3. In section 4 we solve an example in order to make more clear our theoretical construction. The structure of the communication scheme is given in section 5. Section 6 analyzes its main properties and the proof of our main result is undertaken. Economic applications are shown in section 7. Further extensions close our work.

2 The communication game and the main result

We present first the communication game and the statement of our main result. Then we develop the communication protocol and prove our findings.

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

[9]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.

A 'protocol' or scheme of communication is universal if it does not depend on the parameters of the game (Forges (1990)). We are interested in protocols which are universal for the whole class of all two-person games with complete information. In this context, typical universal protocols are given by 'plain conversation schemes' or 'unmediated communication'[10] consisting of several rounds in which each player sends a message to the others. With such communication schemes the dependence of the environment is reflected by the behaviour of the agents, not by that of informational intermediaries.

As Forges (1990) pointed out, 'to find a universal scheme of communication is not really an issue; but to communicate through such a protocol might entail a loss of efficiency'. We will exhibit a plain conversation scheme which can be used without any loss of efficiency in all two-person games with complete information (with rational payoffs). More precisely, *take any such game and any solution achieved by adding to the game any communication system (possibly depending on the parameters of this game and the selected equilibrium). This solution can be achieved as a Nash equilibrium of the extended game obtained by adding to the basic game the universal scheme of unmediated pre-play communication.*

Consider a normal-form game Γ with two players P_1 and P_2 with feasible sets of actions $A = \{a_1, ..., a_s\}$ and $B = \{b_1, ..., b_t\}$ respectively and pay-offs functions $u_1 : A \times B \longrightarrow Q$, $u_2 : A \times B \longrightarrow Q$. $(a_i, b_j) \in A \times B$, $i = 1, ..., s$, $j = 1, ..., t$. We allow the players to communicate before they take an action. The communication stage consists of a sequence of steps where the players can exchange messages ('cheap talk', i. e. additional moves without any direct effect on their payoffs). This can be interpreted as a conversation between the players. Here, we do not restrict them to unmediated communication, they can be helped by any communication device. Thus, consider the above normal-form game Γ and add a communication system to such a game.

This communication system can be formalized in the following way (Myerson (1991)): Let R_h, $(h = 1, 2)$ be the set of reports that player h can send out into the system and let M_h, $(h = 1, 2)$ be the set of messages that this player can receive from it. Denoting by $\Delta(M_1 \times M_2)$ the set of probability distributions over the set of messages $M_1 \times M_2$, we can completely characterize

[10] We use the phrases 'plain conversation' and 'unmediated communication' indistinctly. The term 'plain conversation' is due to Forges (1990).

the communication process by a function $\nu : R_1 \times R_2 \longrightarrow \Delta(M_1 \times M_2)$ such that for all $(r_1, r_2) \in R_1 \times R_2$ and $(m_1, m_2) \in M_1 \times M_2$, $\nu((m_1, m_2)|(r_1, r_2))$ is the conditional probability that (m_1, m_2) would be the messages received by the the players when they sent reports according to (r_1, r_2). Given a communication system ν, it is posssible to transform the original game Γ in a *'communication game'* denoted by Γ_ν which can be formalized in the following way:

1. The sets of pure strategies for both players in Γ_ν are $\bar{A} = \{(r_1, \delta_1)|r_1 \in R_1,\ \delta_1 : M_1 \longrightarrow A\}$ $\bar{B} = \{(r_2, \delta_2)|r_2 \in R_2,\ \delta_2 : M_2 \longrightarrow B\}$ i.e. the set of all the feasible reports that a player can send to the communication system and all his possible decision rules δ_h from the set of received messages into the set of his pure actions in the original non-cooperative game.

2. The payoff function of player h, $(h = 1, 2)$ is given by:

$$\hat{u}_h((r_1, \delta_1), (r_2, \delta_2)) = \sum_{(m_1, m_2) \in M_1 \times M_2} \nu((m_1, m_2)|(r_1, r_2)) u_h(\delta_1(m_1), \delta_2(m_2))$$

   i.e. the expected payoff under the probability distribution over the pure actions of Γ induced by the communication system from the reports and decission rules used by both players.

We are interested in the set of Nash equilibria of the game Γ_ν (for all possible ν), which can be understood as the set of all possible solutions of the original game Γ achievable through any communication system ν. Myerson (1991) proves that this set is equivalent to the subset of correlated strategies q of Γ [11] satisfying the following incentives constrains:

$\sum_{j=1}^{t} q(a_i, b_j) u_1(a_i, b_j) \geq \sum_{j=1}^{t} q(a_i, b_j) u_1(a_{i'}, b_j)$
$\sum_{i=1}^{s} q(a_i, b_j) u_2(a_i, b_j) \geq \sum_{i=1}^{s} q(a_i, b_j) u_2(a_i, b_{j'})$
$\forall\ i, i' = 1, ..., s$ and $\forall\ j, j' = 1, ..., t$.

[11] A correlated strategy is a probability distributions on $A \times B$, i. e. an element of the set $\Delta(A \times B)$.

Notice that these inequalites are the conditions for q to be a correlated equilibrium distribution of Γ (in the sense of Aumman (1974, 1987)) [12]. This fact, known as the *revelation principle* [13] for complete information games, allows us to focus our analysis on the set of correlated equilibrium distributions of the original game, instead of working with the mathematically more complex set of Nash equilibria of arbitrary communication games obtained from Γ.

Hence, the basic situation to deal with is the following: the players of a noncooperative game have the opportunity to communicate, prior to play, to reach an agreement to coordinate their actions in a mutually beneficial way. Specifically, they may try to correlate their strategies to get higher expected payoffs. Obviously this communication system might depend on some external correlation device or 'mediator' who chooses a pair of strategies according to some 'out of the game' probability distribution and informs each player about his own component using some kind of messages. However, we are interested in decentralized mechanisms, i. e. in the use of unmediated communication in strategic settings. Thus, we want to analyze the power of 'unmediated communication' as a coordination device. But, talk may be cheap: if making claims is effortless, an agent is likely to make a self-serving claim, not necessarily a truthful one. We explicitely model unmediated communication to design and implement a procedure for obtaining correlated private signals.

So, the question is, could players find a procedure of preplay communication that replaces the 'mediator'?. The answer is affirmative and the following proposition states this result:

Proposition 2.1 *Let Γ be a two-player game with complete information and rational payoffs. Let $C(\Gamma)$ be the set of payoffs associated to all the correlated equilibria of Γ.*

Then, every payoff in $C(\Gamma)$ is the Nash equilibrium pay-off of the game extended by a costless unmediated pre-play communication phase of finite

[12] These inequalities also show that the set of distributions associated to all the correlated equilibria of Γ forms a convex polyhedron.

[13] More precisely, the revelation principle for normal-form games of complete information states that any equilibrium of any communication game Γ_ν, that can be generated from a normal-form game Γ by adding a system of pre-play communication ν, must be equivalent to a canonical correlated equilibrium of Γ.

duration where both players can talk according to a universal scheme of communication. The communication protocol does not rely on any mediator of any kind and it uses messages in a finite set[14].

In general, correlated equilibrium strategies may require an outside correlation device which may depend on the parameters of the game. The statement above shows the power of unmediated communication as a coordination mechanism.

The proof of Proposition 2.1 is the subject of the following sections. Firstly, we focus just on correlated equilibrium distributions which are Q-evaluated. Once our result is established for such rational distributions, we will extend it for arbitrary R-evaluated ones. Hence, we start by constructing a protocol or communication scheme for the more restrictive class of rational distributions. The purpose of this phase of pre-play communication is to replace the effect of the correlation device. In particular, players use the ex-ante pre-play communication to agree on a protocol with public messages but secret codes[15].

The following notation is used: $q(a_i, b_j) = \frac{r_{ij}}{n} \in Q$, $r_{.j} = \sum_{i=1}^{s} r_{ij}$, $r_{i.} = \sum_{j=1}^{t} r_{ij}$ and $r_{..} = \sum_{i=1}^{s} r_{i.} = \sum_{j=1}^{t} r_{.j} = n$.

3 The set of messages and the ciphering - deciphering 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.

[14] Barany (1992) obtains the same result but with the restriction of four players. Forges (1990) proves a extension of Barany's result for incomplete information games of at least four players.

[15] Under Barany's construction there is a secure channel between any two players. In other words, each two players choose a jointly controlled lottery. However, when there are only two players in the game, the largest set of equilibrium payoffs which can be achieved by extending Γ in this way is the convex hull of the Nash equilibrium payoffs, since all messages are public and with public key.

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 strategies of the original game a pair of messages - a two letter word - from the message space. Notice that since the distribution q is Q-evaluated, it is always possible to associate to every pair of strategies (a_i, b_j) 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 (under a private coding) every letter of all two letter words and sends them to the other player. This second one selects one of the encrypted words without knowing its real meaning, and encodes his corresponding letter and sends it back to the first player.

Note, however, that in order to control the integrity of the whole exchange of information we need to impose some properties on the ciphers being used. In particular, we use cipher and decipher functions which commute among them. Commutation allows players to send public messages with private meaning without any loss of efficiency of the real information been transmitted. Thus, they can encode and decode previously encoded messages while keeping privacy and control over the real meaning of them[16].

Hence, in order to build up the communication protocol we need to use ciphering and deciphering functions with commutative properties. These functions can be defined by using exponential ciphers in the way proposed by Pohling-Hellman (1978). 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[17].

Two integers a and b are *Congruent Module* another integer m if and

[16] The situation is completely different with the arbitrary permutations used by Barany (1992).

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

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 distinct sets of this kind 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 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* [18]. 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 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 later. This set will be given by the units of $GF(p)$ except $\bar{1}$:

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

To define the ciphering and decodifying 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[19]. These 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 $\bar{m}^{\phi(p)} = \bar{1}$, we can say that $E_h(D_h(\bar{m})) = \bar{m}$. Then the two functions are inverses).

[18] 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.

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

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, in the best of the cases, a list of messages, i.e. $\bar{m}$, and its codification $\bar{m}^{e_{h'}}$. Hence, to break the code used by $P_{h'}$ is the same than to calculate 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 of calculating this logarithm[20].

4 Example.

Consider the two person game with complete information analyzed by Aumann (1987):

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

where $\{a_1, a_2\}$ is the set of feasible strategies of P_1 and $\{b_1, b_2\}$ the set of those of P_2. It is well known that the probability distribution q given by

$$\left(\begin{array}{cc} 0 & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{array} \right)$$

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

is associated to a canonical correlated equilibrium of the game with an expected payoff of $(5,5)$. Let us build up an unmediated communication protocol which allows the players to obtain the same payoff (out of the convex hull of the Nash equilibrium payoffs of the game). In order to establish this result we need to use the messages and functions defined above.

Firstly, both players agree on the use of a prime number, say 43. Once this number has been established they build up a common set of basic messages (alphabet) $M = \{\bar{2}, \bar{3}, ..., \bar{42}\}$ where $\bar{a}$ denotes the corresponding residual module 43.

To every pair of strategies $(a_i, b_j) \in A \times B$, r_{ij} distinct two-letter words belonging to $M \times M$ are associated. For instance:

$$\begin{array}{ll} (a_1, b_2) & (\bar{2}, \bar{3}) \\ (a_2, b_1) & (\bar{4}, \bar{5}) \\ (a_2, b_2) & (\bar{6}, \bar{7}) \end{array}$$

To avoid that the knowledge of a letter gives a player more information than the knowledge of the action associated to it, new words must be added. These new words are just replications of the original ones following the next tree[21] (Notice that bold numbers are refered to the letters which permute in the next branches):

$$\begin{array}{lcccccc} & & & & (\bar{2}, \bar{3}) & & \\ & & & & (\bar{\mathbf{4}}, \bar{5}) & & \\ & & & & (\bar{\mathbf{6}}, \bar{7}) & & \\ & & (\bar{2}, \bar{\mathbf{3}}) & & & & (\bar{2}, \bar{\mathbf{3}}) \\ \mathbf{a_2} \longrightarrow & & (\bar{4}, \bar{5}) & & & & (\bar{6}, \bar{5}) \\ & & (\bar{6}, \bar{\mathbf{7}}) & & & & (\bar{4}, \bar{\mathbf{7}}) \\ & (\bar{2}, \bar{3}) & & (\bar{2}, \bar{7}) & & (\bar{2}, \bar{3}) & & (\bar{2}, \bar{7}) \\ \mathbf{b_2} \longrightarrow & (\bar{4}, \bar{5}) & & (\bar{4}, \bar{5}) & & (\bar{6}, \bar{5}) & & (\bar{6}, \bar{5}) \\ & (\bar{6}, \bar{7}) & & (\bar{6}, \bar{3}) & & (\bar{4}, \bar{7}) & & (\bar{4}, \bar{3}) \end{array}$$

[21] Every row of 'branches' of the tree is obtained by combining every permutation of the letters associated to an action of the player with any 'branch' obtained in the previous step. In order to complete the tree, a row of 'branches' must be added to every action of both player which was associated to at least two different letters. Obviously, the order in which the 'branches' are added has no effect on the final result.

Hence, we obtain a set of 2! 2! 3 = 12 two letter words denoted by V and given by:

$$\begin{array}{cccc} (a_1,b_2) & (\bar{2},\bar{3}) & (\bar{2},\bar{3}) & (\bar{2},\bar{7}) & (\bar{2},\bar{7}) \\ (a_2,b_1) & (\bar{4},\bar{5}) & (\bar{6},\bar{5}) & (\bar{4},\bar{5}) & (\bar{6},\bar{5}) \\ (a_2,b_2) & (\bar{6},\bar{7}) & (\bar{4},\bar{7}) & (\bar{6},\bar{3}) & (\bar{4},\bar{3}) \end{array}$$

Notice that there are 2! 2! = 4 words associated to any feasible pair of actions of the original game. Hence, if a word is selected uniformly at random on the set of 12 words we built up above, the probability of this selection to be associated to any pair of strategies is, precisely, $\frac{1}{3}$ as under the correlated equilibrium distribution q.

The conversation that both players will engage in, consists of the exchange of encrypted words from the above list. The ciphering and deciphering functions will be build up as exponentiations on the subset of residuals M in the way shown in section 3. Hence, let us assume that the first player codifies every letter $\bar{m}$ of the common alphabet by calculating $E_1(\bar{m}) = \bar{m}^5$ and decodifies it by using $D_1(\bar{m}) = \bar{m}^{17}$. The same holds for player two, assuming that he is using the fuctions $E_2(\bar{m}) = \bar{m}^{11}$ and $D_2(\bar{m}) = \bar{m}^{23}$. Let us remark that these four functions commute among them. (For instance, $E_1(E_2(\bar{m})) = \bar{m}^{5^11} = \bar{m}^{5*11} = \bar{m}^{11^5} = E_2(E_1(\bar{m}))$).

Once these elements have been established, both player talk through the following steps:

Step 1 P_1 calculates and adds a control letter to all the 12 two-letter words. For instance, $E_1(\bar{2}\ \bar{3}) = E_1(\bar{6}) = \bar{6}^5 = 3\bar{6}$ and obtains the three letter word $(\bar{2},\bar{3},3\bar{6})$. Hence, he constructs and sends to P_2:

$$\begin{array}{cccc} (a_1,b_2) & (\bar{2},\bar{3},3\bar{6}) & (\bar{2},\bar{3},3\bar{6}) & (\bar{2},\bar{7},2\bar{3}) & (\bar{2},\bar{7},2\bar{3}) \\ (a_2,b_1) & (\bar{4},\bar{5},2\bar{6}) & (\bar{6},\bar{5},1\bar{2}) & (\bar{4},\bar{5},2\bar{6}) & (\bar{6},\bar{5},1\bar{2}) \\ (a_2,b_2) & (\bar{6},\bar{7},4\bar{2}) & (\bar{4},\bar{7},\bar{5}) & (\bar{6},\bar{3},1\bar{9}) & (\bar{4},\bar{3},3\bar{4}) \end{array}$$

Step 2 P_2 codifies these three letter words, using the exponent $e_2 = 11$. Then $(\bar{2}^{e_2},\bar{3}^{e_2},3\bar{6}^{e_2}) = (2\bar{7},3\bar{0},\bar{6})$. Working in the same way with all the words, he obtains:

$$\begin{array}{ccccc}
(a_1, b_2) & (\bar{2}\bar{7}, \bar{3}\bar{0}, \bar{6}) & (\bar{2}\bar{7}, \bar{3}\bar{0}, \bar{6}) & (\bar{2}\bar{7}, \bar{3}\bar{7}, \bar{2}\bar{5}) & (\bar{2}\bar{7}, \bar{3}\bar{7}, \bar{2}\bar{5}) \\
(a_2, b_1) & (\bar{4}\bar{1}, \bar{3}\bar{4}, \bar{1}\bar{9}) & (\bar{3}\bar{6}, \bar{3}\bar{4}, \bar{2}\bar{6}) & (\bar{4}\bar{1}, \bar{3}\bar{4}, \bar{1}\bar{9}) & (\bar{3}\bar{6}, \bar{3}\bar{4}, \bar{2}\bar{6}) \\
(a_2, b_2) & (\bar{3}\bar{6}, \bar{3}\bar{7}, \bar{4}\bar{2}) & (\bar{4}\bar{1}, \bar{3}\bar{7}, \bar{3}\bar{4}) & (\bar{3}\bar{6}, \bar{3}\bar{0}, \bar{2}\bar{9}) & (\bar{4}\bar{1}, \bar{3}\bar{0}, \bar{3})
\end{array}$$

At this point, the second player should change the order of the words not to give extra information to the other player. We keep the same order to make the example more clear. Next, the second player sends to the first one this list of codified words.

Step 3 P_1 applies his cipherying function to the first two letters of every word, obtaining $(\bar{2}\bar{7}^{e_1}, \bar{3}\bar{0}^{e_1}, \bar{6}) = (\bar{2}\bar{2}, \bar{1}\bar{2}, \bar{6})$. Thus, the set of messages becomes:

$$\begin{array}{ccccc}
(a_1, b_2) & (\bar{2}\bar{2}, \bar{1}\bar{2}, \bar{6}) & (\bar{2}\bar{2}, \bar{1}\bar{2}, \bar{6}) & (\bar{2}\bar{2}, \bar{7}, \bar{2}\bar{5}) & (\bar{2}\bar{2}, \bar{7}, \bar{2}\bar{5}) \\
(a_2, b_1) & (\bar{1}\bar{1}, \bar{3}\bar{3}, \bar{1}\bar{9}) & (\bar{6}, \bar{3}\bar{3}, \bar{2}\bar{6}) & (\bar{1}\bar{1}, \bar{3}\bar{3}, \bar{1}\bar{9}) & (\bar{6}, \bar{3}\bar{3}, \bar{2}\bar{6}) \\
(a_2, b_2) & (\bar{6}, \bar{7}, \bar{4}\bar{2}) & (\bar{1}\bar{1}, \bar{7}, \bar{3}\bar{4}) & (\bar{6}, \bar{1}\bar{2}, \bar{2}\bar{9}) & (\bar{1}\bar{1}, \bar{1}\bar{2}, \bar{3})
\end{array}$$

P_1 analyzes the integrity of these words, checking whether the product of the two first letters is equal to the third $\bar{2}\bar{2}\ \bar{1}\bar{2} = 2\bar{6}4 = \bar{6}$. Once all the words have been checked, the first player selects any three words of the list such that in the first two positions there are six different letters. This selection could be, for instance [22]:

$$\begin{array}{c}
(\bar{2}\bar{2}, \bar{1}\bar{2}, \bar{6}) \\
(\bar{6}, \bar{3}\bar{3}, \bar{2}\bar{6}) \\
(\bar{1}\bar{1}, \bar{7}, \bar{3}\bar{4})
\end{array}$$

This step finishes when P_1 sends these three words to P_2.

Step 4 The second player checks both that the two first letters of the three words are distinct and that every pair is a member of an original one. This last control is made by verifying that the product of the first two letters of each word is equal to the third: $\bar{2}\bar{2}\ \bar{1}\bar{2} = 2\bar{6}4 = \bar{6}$;

[22] Really, P_1 is selecting one of the reordered copies of the three original words which have been added before. In our example, P_1 has selected the codified 'branch' of the replication tree given by $(\bar{2}, \bar{3})$, $(\bar{6}, \bar{5})$ and $(\bar{4}, \bar{7})$.

$\bar{6}\ \bar{33} = 1\bar{98} = 2\bar{6}$ and $1\bar{1}\ \bar{7} = 7\bar{7} = 3\bar{4}$. Once P_2 knows that the messages are correct, he selects one of them at random. Let us suppose that the chosen one is $(1\bar{1}, \bar{7}, 3\bar{4})$. Afterwards, the second player calculates $D_2(1\bar{1}) = 1\bar{1}^{23} = 3\bar{5}$ and sends P_1 the letter $\bar{7}$.

Step 5 P_1 decodifies the received message $D_1(\bar{7}) = \bar{7}^{17} = 3\bar{7}$.

Step 6 Both players exchange the letters corresponding to the selected word[23]. So, P_1 receives the message $3\bar{5}$ and P_2 the letter $3\bar{7}$.

Step 7 Every player decodifies his message $D_1(3\bar{5}) = 3\bar{5}^{17} = \bar{4}$ and $D_2(3\bar{7}) = 3\bar{7}^{23} = \bar{7}$. Thus the first player knows that the strategy suggested to him by the protocol is a_2 and the second knows that he must play b_2. This element has been selected with probability $\frac{1}{3}$, the same probability induced by the original distribution q.

Let us see what would happen if the first player deviates at step 6 and sends his opponent a message different from the suggested one, $3\bar{7}$. Since P_1 cannot discover that $e_2 = 11$, when he sends the altered message, he cannot control the strategy that he is suggesting to the second one. In fact, he cannot even be sure of sending a valid letter.

Let us remark that P_2 can realize that P_1 is cheating. In this case, out of the equilibrium path, P_2 can approach the distribution q by playing the mixed strategy given by the marginal distribution $(q(b_1), q(b_2))$.

Specifically, P_1 sends the second player a letter at random from the set

$$M - \{3\bar{7}\} = \{\bar{2}, \bar{3}, ..., 4\bar{2}\} - \{3\bar{7}\}$$

and two cases may take place:

1. If the message is different of $3\bar{0}$ or $3\bar{4}$, P_2 realizes that P_1 is cheating. This possibility will happen with probability $\frac{38}{40}$ and it is possible to made this number as close as one as we want, taking the prime p large enough. Let us denote by $\rho(a_i)$, $i = 1, 2$, the mixed strategy of P_1 which is a best response to the strategy of P_2 given by following the

[23] This is the point of the protocol where players have an incentive to cheat.

marginal distributions $q(b_j)$, $j = 1, 2$. The biggest payoff that P_1 can obtain, π_d, is then[24]:

$$\pi_d = \rho(a_1)(\sum_{j=1}^{t} q(b_j)u_1(a_1, b_j)) + \rho(a_2)(\sum_{j=1}^{t} q(b_j)u_1(a_2, b_j)) = \frac{14}{3} \leq 5$$

where 5 is the correlated equilibrium payoff, denoted by π_c. Hence $\pi_d \leq \pi_c$.

2. If the message is equal to $3\bar{0}$ o $3\bar{4}$ (this possibility will happen with probability $\frac{1}{2}$ in each case) the second player will not detect the deviation and the protocol will generate an altered distribution $\bar{q}$. Let us calculate this distribution.

$$\begin{aligned}
\bar{q}(b_1|a_1) &= q(b_1|a_1) * prob(P_2 \ plays \ b_1 | q \ suggests \ (a_1, b_1)) \\
&+ q(b_2|a_1) * prob(P_2 \ plays \ b_1 | q \ suggests \ (a_1, b_2)) \\
&= 0 * prob(P_2 \ plays \ b_1 | the \ selected \ letter \ is \ 3\bar{0}) \\
&+ 1 * prob(P_2 \ plays \ b_1 | the \ selected \ letter \ is \ 3\bar{4} \ or \ 3\bar{7})
\end{aligned}$$

Since the altered protocol always sends a letter different from the selected one and player 2 plays b_1 if and only if the letter received by him is $3\bar{0}$, we have

$prob(P_2 \ plays \ b_1 | the \ selected \ letter \ is \ 3\bar{0}) = 0$

$prob(P_2 \ plays \ b_1 | the \ selected \ letter \ is \ 3\bar{4} \ or \ 3\bar{7}) = \frac{1}{2}$

Then, $\bar{q}(b_1|a_1) = \frac{1}{2}$. Since P_2 has followed faithfully the protocol, $\bar{q}(a_1) = \bar{q}(a_2) = \frac{1}{3}$. Then $\bar{q}(a_1, b_1) = \bar{q}(b_1|a_1)\bar{q}(a_1) = \frac{1}{6}$.

Similarly, we are able to calculate all the distribution $\bar{q}$, which is given by:

[24]Note that here, the best response to $q(b_j)$ is $q(a_i)$, since the marginal distributions form the mixed strategy Nash equilibrium of the underlying game.

$$\begin{pmatrix} \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{3}{6} \end{pmatrix}$$

Let us see that in the second situation the first player cannot obtain an ex-ante expected payoff bigger than the correlated equilibrium payoff. Hence, if the first player deviates and alters the protocol, his best responses are given by:

$$\hat{a}_1 = arg \quad max_{l=1,2}(\bar{q}(b_1|a_1)u_1(a_l, b_1) + \bar{q}(b_2|a_1)u_1(a_l, b_2)) = a_2$$
$$\hat{a}_2 = arg \quad max_{l=1,2}(\bar{q}(b_1|a_2)u_1(a_l, b_1) + \bar{q}(b_2|a_2)u_1(a_l, b_2)) = a_1.$$

In this case the biggest expected pay-off that he can get by playing $\hat{a}_i$ when a_i is suggested, denoted by π_{nd}, is $\frac{29}{6}$, lower than the profit obtained by faithfully playing and reaching the correlated equilibrium payoff of 5. Thus, $\pi_{nd} \leq \pi_c$.

Hence, the best payoff that P_1 can get ex-ante by deviating from the protocol is lower or equal than $\frac{38}{40}\pi_d + \frac{2}{40}\pi_{nd} \leq \frac{38}{40}\pi_c + \frac{2}{40}\pi_c = \pi_c = 5$. Then, player 1 has no incentives to deviate and the conversation process built up is self enforcing (i.e. a player has not an incentive to deviate from the protocol is the other one is following it faithfully [25]).

5 Structure of the communication protocol.

A protocol seeking to replace any correlation device should satisfy some properties. For instance, for each player P_h, $h = 1, 2$, and once the communication is over, the information set of player h, I_h[26], determines de corresponding component on h's strategy set uniquely; i.e. there is a map F_h (known to P_h) with $F_1(I_1) = a_i$ and $F_2(I_2) = b_j$ such that:

$$Prob(F_1(I_1) = a_i, F_2(I_2) = b_j) = q(a_i, b_j)$$

$$Prob(F_1(I_1) = a_i, F_2(I_2) = b_j|I_1) = q(a_i, b_j|a_i)$$

[25] We will make this concep more precise in section 6.

[26] I_h is given by all the messages sent and received during the communication phase

$$Prob(F_1(I_1) = a_i, F_2(I_2) = b_j | I_2) = q(a_i, b_j | b_j)$$

for all $(a_i, b_j) \in A \times B$.

The meaning of the last two conditions is that I_h does not give more information to P_h than the knowledge of his suggested strategy.

Notice however, that players may be willing to cheat in order to get strategic information from the communication scheme. Thus, for instance, a player may send a different message than the one suggested by the protocol in order to get some advantages[27]. Also, when the communication is over, they may disobey the actions recommended by the protocol.

Our protocol has the property that strategic deviations are detected with probability as close as to one as we wish[28]. But, more than that, we show that our communication scheme is self-enforcing: i.e. even if a deviation by a player were not detected by the second one, the first player would not have an incentive to deviate if the other does not.

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 $A \times B$ using the distribution q and its rationality.

This construction is made in two steps: Firstly, both player select jointly 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 $(a_i, b_j) \in A \times B$, r_{ij} words (α_k^i, β_l^j) from the set previously choosen. Hence if one of these n words is selected uniformly at random, the probability that this word is associated to a pair of actions (a_i, b_j) is $\frac{r_{ij}}{n} = q(a_i, b_j)$[30].

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

[27] We add some 'built-in checking' to avoid some trivial (nonstrategic) mistakes.

[28] Under Barany's protocol these strategies deviations are detected with probability one.

[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.

of the action he is suggested to play[31]. 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 done by bulding 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[32]:

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

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 [33].

[31] Let us show this situation for the example of section 4. Assume that the set V has not been built up and that both players are just dealing with the original associations given by $(a_1, b_2) \to (\bar{2}, \bar{3})$, $(a_2, b_1) \to (\bar{4}, \bar{5})$, $(a_2, b_2) \to (\bar{6}, \bar{7})$. If a external mediator suggests P_1 to play a_2, his probability about the action suggested to P_2 is $prob(b_1) = prob(b_2) = \frac{1}{2}$. But if P_1 receives the message $\bar{4}$ he knows that the chosen word is $(\bar{4}, \bar{5})$ and that player 2 is suggested to play b_1.

[32] 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.

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

This set of valid words, which may be much bigger than the original one, satisfies the following properties:

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. [34].

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. Hence, the three properties of the maps F_h and the information sets I_h, $(h = 1, 2)$, above established holds.

The communication scheme.

Each player select independently two functions E_h and D_h, permutations of M, by using exponential cipher, in the way considered in section 3.

Before describing the specific steps of our protocol, 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 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 strategies 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, i. e. $\gamma^{ij}_{kl} = \alpha^i_k \beta^j_l$ [35].

Our protocol has the following steps:

[34] 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.

[35] 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

Step 1 Player 1 adds to every word (α_k^i, β_l^j) a third control letter $E_1(\gamma_{kl}^{ij})$ and 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 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 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 these choosen words (without considering the control letters)[36]. 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, 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 [37]. If it is detected

to calculate $(\gamma_{kl}^{ij})^{e_1 e_2 d_2} = (\gamma_{kl}^{ij})^{e_1}$ and to control if this element, which belongs to $GF(p)$, is the product of the two first letters of the word. It is important to remark that this checking process is made by the second player without having any information about the real meaning of the words ciphered by P_1.

[36] 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 restric 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 decipherig fuctions are bijections, the same difference in the number of words will be mantained after encryption.

[37] 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).

that P_1 has deviated, the protocol will start again. Otherwise, P_2 selects uniformly at random a pair $(E_1(\bar{\alpha}_k^i), E_1(\bar{\beta}_l^j))$ and sends $E_2(E_1(\bar{\beta}_l^j))$ to P_1

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

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 plays a_i, and P_2 calculates $D_2(E_2(\bar{\beta}_l^j)) = \bar{\beta}_l^j$ and plays b_j.

If both players follow the above protocol, they obtain the same pay-off than that of the correlated equilibrium under the distribution q. But we must still solve a key question: *Do players have an incentive to follow the protocol if there is not any binding contract between them?*. To give a positive answer to this question is the main goal of the following sections.

Note that the above steps completely describe both players' actions along the equilibrium path of the communication phase. However a player, say P_1, can deviate from the protocol path and, with some probability, the other player P_2 may realize of it. To describe, in this case, the strategies out of the equilibrium path, we assume that P_2 will follow the mixed strategy induced by the marginal distribution on his actions, i.e. $q(b_j)$, $j = 1, ..., t$. This would suffice to deter P_1 from deviating. Also, with the complementary probability, P_1 can deviate and not to be detected by P_2. Now, P_2 would choose his actions according to the induced probability distribution which would follow the 'altered' message.

6 Properties of the communication protocol.

We analyze next whether players have an incentive to deviate from the protocol. This analysis is developed under the assumption that player 1 deviates and player 2 faithfully follows the protocol. The same results would follow when P_2 is the cheating player.

6.1 ε-sure protocols.

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.

Our next result shows that it is always possible to construct a communication scheme such that deviations from the rules are detected with probability as close as 1 as we wish. First, we define:

Definition 6.1 *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 protocol is ε-sure, for each positive ε.

Proposition 6.1 *The protocol 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 $E_2(\bar{\beta})$ 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[38] 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

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

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.

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

□

We do not just consider ε-sure protocols, but a more demanding protocols. In particular, communication schemes where a player has no incentive to deviate even if he is not detected by the other player, as long as this last one follows the scheme (i.e. self-enforcing protocols). In order to show that our protocol satisfies this property, we need to analyze the distribution associated to a player's deviation.

Notice that given a protocol that seeks to implement the correlated probability distribution q on $A \times B$, if player 1 plans to 'deviate from the rules' according to a uniform transition probability over $M - \{\bar{\beta}\}$, and assuming he is not detected, then the induced probability distribution over action profiles is given by $\bar{q}(a_i, b_j) = f(q(a_i, b_j), \bar{\beta}, \beta^\star)$, $\forall (a_i, b_j) \in A \times B$, $\beta^\star \in M - \{\bar{\beta}\}$, $\bar{\beta} \in M$, where f is a function which depends on q and the messages involved. The next section characterizes and analyzes the main properties of the new induced distribution $\bar{q}$.

6.2 Self-enforcing protocols.

Let us remark that deviations at step 6 are uncontrolled, so that we can think that their effect is to break the coordination induced by the correlated equilibrium. This intuition is confirmed by the following propositions.

Proposition 6.2 *Undetected deviations from the rules by a player do not change the probability of the other one to play a given strategy*[39]*, i.e.:*

Prob (P_2 *plays* $b_j | P_1$ *deviates from the rules and is not detected*) = $q(b_j)$

Proof: As we have pointed out above, if P_1 deviates from the rules he sends to P_2 a message $E_2(\beta^\star)$ distinct from the suggested one $E_2(\bar{\beta})$. The deviation is not detected if and only if $\beta^\star$ is any of the $n-1$ messages associated to the actions $b_1, ..., b_t$ and different from $\bar{\beta}$.

P_2 will play b_j if the altered message $\beta^\star$ is one of the $r_{.j}$ letters associated to this action. The probability of $\beta^\star$ to be a message associated to b_j depends on the actual value of the suggested letter $\bar{\beta}$. Hence,

[39] Gossner (1996) also shows that this property refers to any self-enforcing protocol, although he calls these protocols 'sure protocols'.

$Prob\ (P_2\ plays\ b_j\ when\ P_1\ deviates\ from\ the\ rules\ and\ he\ is\ not\ detected) =$
$\sum_{u=1}^{t} Prob\ (\beta^\star\ is\ associated\ to\ b_j | \bar{\beta}\ is\ associated\ to\ b_u)$
$Prob(\bar{\beta}\ is\ associated\ to\ b_u)$

As $\bar{\beta}$ is selected uniformly at random from the set of n messages associated to $b_1, ..., b_t$, we have $Prob(\bar{\beta}\ is\ associated\ to\ b_u) = \frac{r_{.u}}{n}$. Moreover, since $\beta^\star$ is also selected uniformly at random from the set of $n-1$ element of feasible messages but $\bar{\beta}$, we can write:

$Prob\ (\beta^\star\ is\ associated\ to\ b_j | \bar{\beta}\ is\ associated\ to\ b_u) = \frac{r_{.j}}{n-1} \quad \forall u \neq j$

$Prob\ (\beta^\star\ is\ associated\ to\ b_j | \bar{\beta}\ is\ associated\ to\ b_j) = \frac{r_{.j}-1}{n-1}$

Hence,

$$Prob\ (P_2\ plays\ b_j\ when\ P_1\ deviates\ from\ the\ rules\ and\ he\ is\ not\ detected)$$
$$= \sum_{u=1, u\neq j}^{t} \frac{r_{.j}}{n-1}\frac{r_{.u}}{n} + \frac{r_{.j}-1}{n-1}\frac{r_{.j}}{n} = \frac{r_{.j}}{n(n-1)}(\sum_{u=1}^{t} r_{.u} - 1) = \frac{r_{.j}}{n} = q(b_j)$$

□

Let us assume that P_2 has not detected the deviation of P_1. Let $\bar{q}(a_i, b_j)$ be the new probability distribution on (a_i, b_j) generated by P_1's deviation. $\bar{q}(a_i, b_j)$ satisfies:

1. $\bar{q}(b_j) = q(b_j)$ by proposition 6.2.
2. $\bar{q}(a_i) = q(a_i)$ since P_2 follows the protocol.

Notice that, given a distribution q defined over $A \times B$, with marginals $q(a_i)$, $q(b_j)$, if $q(a_i, b_j) - q(a_i)q(b_j) = 0$, $\forall (a_i, b_j) \in A \times B$, q does not have any correlation power. Thus, if q is associated to a correlated equilibrium of a game and the condition above holds, the suggestions of the correlation device can be understood as playing the uncorrelated mixed estrategies given by the corresponding actions' independent marginal distributions.

Let us define the *correlation power* of q, $\forall (a_i, b_j) \in A \times B$, as $C_{i,j} = q(a_i, b_j) - q(a_i)q(b_j)$. Obviously, correlation on $A \times B$ may induce the probability associated to the pair (a_i, b_j) to be higher or lower than the product of the marginal distributions of a_i and b_j. Also let 'sign of C_{ij}' be the *coordination power* of q, $\forall (a_i, b_j) \in A \times B$.

Similary, let us denote by $\bar{C}_{ij}$ the correlated power of $\bar{q}$ at the pair of actions (a_i, b_j), i. e.: $\bar{C}_{i,j} = \bar{q}(a_i, b_j) - \bar{q}(a_i)\bar{q}(b_j)$ and by 'sign of $\bar{C}_{ij}$' the associated coordination power of $\bar{q}$.

Notice that the *complexity* of the rational distribution q is given by the parameter n, since the higher is n the more complex must be the randomization device used to generate this probability distribution on the event spaces.

Proposition 6.3 .

i) *The new probability distribution over actions generated when P_1 deviates and P_2 does not detect him, is given by*[40] $\bar{q}(a_i, b_j) = q(a_i)q(b_j) - \frac{1}{n-1}C_{ij}$.

ii) *The correlation power of the altered distribution $\bar{q}$ is given by $\bar{C}_{ij} = -\frac{1}{n-1}C_{ij}$ and, obviously, sign $\bar{C}_{ij} = -$ sign C_{ij}.*

Proof: Let us suppose that a_i is the strategy suggested by q to P_1. Then, the probability that P_2 plays any strategy b_j is given by:

$$\bar{q}(b_j|a_i) = \sum_{u=1}^{t} q(b_u|a_i) Prob(P_2 \text{ plays } b_u \mid q \text{ suggests } (a_i, b_j))$$

The original messages $\bar{\beta}$ is associated to the suggested action b_j. The undetected deviation of P_1 means that this original message has been deleted from the *list* of feasible messages in such a way that only $n-1$ valid messages remain, $r_{.j}$ of them associated to b_j and $r_{.u}$ associated to any b_u different from b_j. Hence, we have:

$$\begin{aligned} \bar{q}(b_j|a_i) &= q(b_j|a_i)\frac{r_{.j}-1}{n-1} + \sum_{u=1, u\neq j}^{t} q(b_u|a_i)\frac{r_{.j}}{n-1} \\ &= \frac{1}{n-1}\left(\sum_{u=1}^{t} q(b_u|a_i)r_{.j} - q(b_j|a_i)\right) \end{aligned}$$

[40] Notice that if q does not have any correlation power, i. e. $C_{ij} = q(a_i, b_j) - q(a_i)q(b_j) = 0$, then $\bar{q}(a_i, b_j) = q(a_i, b_j)$. In other words, if players play a mixed strategy equilibrium, a deviation from the rules has no effect on the probability distribution generated by this deviation.

$$= \frac{1}{n-1}(r_{\cdot j} - q(b_j|a_i))$$
$$= q(b_j) + \frac{1}{n-1}(q(b_j) - q(b_j|a_i))$$

Multiplying this expresion by $q(a_i)$ and using the definition of correlation power we obtain that $i)$ holds.

To prove ii), we can write i) as

$$\bar{q}(a_i, b_j) - \bar{q}(a_i)\bar{q}(b_j) = \bar{q}(a_i, b_j) - q(a_i)q(b_j) = -\frac{1}{n-1}C_{ij}$$

and then, by applying the definition of coordination power for the involved distributions, the result follows.

□

Hence, a deviation by a player has the effect of both decreasing the correlation power and breaking the coordination power of the probability distributions over actions. Moreover, this decrease on the correlation power is related with the value of $n \geq 2$. When this parameter takes its lowest value, $n = 2$, we have that $\bar{C}_{ij} = -C_{ij}$ and no correlation power is lost but the coordination power is broken. When n encreases, i. e. when the original distribution gets more complexity, the correlation power of $\bar{q}$ becomes lower.

At this point, notice that there is another possible deviation from the protocol. This deviation consists of not following the strategy suggested by the communication scheme. Thus, if a player deviates in step 6 and generates, then, a new distribution on any pair of actions, he may consider not following the suggested strategy under the new distribution[41]. Hence, following the action suggested by the altered protocol distribution $\bar{q}$ may not be the best response for the first player. The next lemma, proved in the Appendix, shows that P_1 cannot expect to encrease his payoff by deviating from the protocol:

[41]Since the initial distribution q is associated to a correlated equilibrium of Γ, there is no reason to play an action different from the suggested by q. But, if a player deviates at step 6 and the distribution generated by him is not q, an incentive to deviate from the suggestion may arise.

Lemma 6.1

$$\sum_{i=1}^{s} \bar{q}(a_i) max_{a_{l_i} \in A} \sum_{j=1}^{t} \bar{q}(b_j|a_i) u_1(a_{l_i}, b_j) \leq \sum_{i=1}^{s} \sum_{j=1}^{t} q(a_i, b_j) u_1(a_i, b_j)$$

Next, we prove that our protocol is self-enforcing.

Definition 6.2 *A pre-play communication protocol admits a feasible deviation if any player can obtain a profit by deviating, meanwhile the other player follows the protocol.*

Definition 6.3 *A pre-play communication protocol is self-enforcing if it does not admit any feasible deviation by any player.*

Proposition 6.4 *The protocol defined in section 5 is self-enforcing.*

Proof: To establish this result we need to prove that the biggest ex-ante payoff that P_1 can get by deviating is lower than the correlated equilibrium payoff. This 'highest payoff from deviating', π, satisfies that: $\pi \leq \varepsilon \pi_d + (1 - \varepsilon)\pi_{nd}$, where π_d and π_{nd} are the biggest payoffs that P_1 can obtain when P_2 detects and does not detect, respectivily, his deviation.

Let us denote by π_c the correlated equilibrium payoff. Since Lemma 6.1 holds, we have that $\pi_{nd} \leq \pi_c$. Hence, to prove this proposition, we only need to show that $\pi_d \leq \pi_c$.

Assume that $\rho(a_i)$, $i = 1, ..., s$ is the best response (mixed strategy) of P_1 to the second player's strategy given by his marginal distribution on actions. We have that:

$$\begin{aligned}
\pi_d &= \sum_{i=1}^{s} \rho(a_i) \sum_{j=1}^{t} q(b_j) u_1(a_i, b_j) \\
&= \sum_{i=1}^{s} \rho(a_i) \sum_{j=1}^{t} \sum_{i'=1}^{s} q(a_{i'}, b_j) u_1(a_i, b_j) \\
&= \sum_{i=1}^{s} \rho(a_i) (\sum_{j=1}^{t} q(a_i, b_j) u_1(a_i, b_j) + \sum_{i'=1, i' \neq i}^{s} \sum_{j=1}^{t} q(a_{i'}, b_j) u_1(a_i, b_j))
\end{aligned}$$

Since q is a correlated equilibrium distribution,

$$\sum_{j=1}^{t} q(a_{i'}, b_j) u_1(\hat{a}_i, b_j)) \leq \sum_{j=1}^{t} q(a_{i'}, b_j) u_1(\hat{a}_{i'}, b_j))$$

Hence,

$$\pi_d \leq \sum_{i=1}^{s} \rho(a_i) \sum_{j=1}^{t} \sum_{i'=1}^{s} q(a_{i'}, b_j) u_1(\hat{a}_{\prime i}, b_j) = \sum_{i=1}^{s} \rho(a_i) \pi_c = \pi_c$$

and the proposition holds.

□

Proof of proposition 2.1 **(Main result).**

A straight consequence of the above proposition is that the main result holds for every correlated equilibrium with a Q - evaluated associated probability distribution. To extend this result to R - evaluated distributions, although under the assumption that the original game has rational parameters, we can apply the same construction than Forges (1990): any arbitrary R-evaluated distribution is a convex combination of a finite number of Q-evaluated distribution (the vertices of the convex polyhedron of correlated equilibrium distributions). Hence, the payoff associated to the real distribution can be achieved by two phases of plain conversation. In the first step a vertex is selected depending on the convex coordenates of the R- evaluated distribution and in the secon step our protocol provides the payoff associated to the Q-evaluated distribution corresponding to the vertex previously selected (See Forges (1990) for details) [42].

[42]The jointly controlled lottery of this proof can also be generated by using our communication protocol. Hence, P_1 and P_2 are able to choose a number in $\{0,1\}$ with the same probability by using the communication protocol built up in this paper to replicate the distribution

$$\begin{array}{cc} & \begin{array}{cc} 0 & 1 \end{array} \\ \begin{array}{c} 0 \\ 1 \end{array} & \left(\begin{array}{cc} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{array} \right) \end{array}$$

which can be understood as a correlated equilibrium of a 2×2 trivial game with null payoffs. Repeating this process we can obtain the binary codification of a concrete realization of the random variable v, which is uniformly distributed in $[0,1)$. This is an

7 Economic application: simoultaneous entry game.

Consider the following situation, widely analyzed in the literature (for instance Dixit and Shapiro (1985), Farrell (1987)): two identical firms produce a good and they are perfectly accommodated in a market wide enough to grow. These firms analyze the possibility of producing a second good whose market is a natural monopoly. Both firms must simultaneously decide whether to enter or not this second market. Since this new market is a natural monopoly, the worst posible situation is that both firms enter. If only one of the firms enters the second market, their profits will strongly depend on the relationship between the new and the old goods.

In order to formalize this situation, we denote the action of entering the second market as In and the action of remaining out as Out. If both firms stand out, they get a payoff of N ($N \geq 0$). If one of them enters and the other does not, the first one receives M and the second B. If they do not coordinate and both of them enter, every ones looses L. Let us assume that all these payoffs are rational numbers. Payoffs are displayed in the following matrix where firm 1 chooses the row and firm 2 chooses the column:

$$\begin{array}{cc} & \begin{array}{cc} In & Out \end{array} \\ \begin{array}{c} In \\ Out \end{array} & \left(\begin{array}{cc} (-L,-L) & (M,B) \\ (B,M) & (N,N) \end{array} \right) \end{array}$$

Firms play "coordinated actions" if just one enters. If both of them remain out or enter simultaneously, they act in an uncoordinated way. In the coordinated solution the payoff of the firm which enters is, of course, bigger than the profit of the other one, i.e. $-L < B < M$.

Since the parameter B determines the payoff of the firm that stands out in coordinate actions, we have that its sign models the relationship between the old product and the new one. Thus, if $B = 0$ the firm that stays out is not affected by the other's decision (independent goods); if $B > 0$ it prefers the other to enter (complementary goods), and if $B < 0$ the firm that enters decreases the profits of the one which stays out (substitute goods).

---

alternative construction to the one of Aumman, Maschler and Stearns (1968), used in the proof of Forges (1990).

Let us consider first the perfect information game associated to the case of complementary goods (Farrell (1987)): $-L < 0 = N < B < M$. Then, the payoff matrix is a 'battle of sexes' and the game has three Nash equilibria: two of them in pure strategies (In,Out), (Out,In) and the other in mixed strategies ($p\ In + (1-p)\ Out$, $p\ In + (1-p)\ Out$), where p is given by $p = \frac{M}{B+L+M}$. This last equilibrium is known as the 'Dixit-Shapiro equilibrium' of the game.

Since both player are identical and have the same negotiation power, it seems reasonable to think that they will play a symmetric equilibrium: the Dixit-Shapiro one (Dixit and Shapiro (1985)). In this equilibrium both firms coordinate with probability $p(1-p)$. The expected payoff obtained by each firm in this case is $u_{DS} = \frac{MB}{B+L+M}$ and a coordination failure will take place with probability $f_{DS} = p^2 + (1-p)^2 = \frac{M^2+(B+L)^2}{(B+L+M)^2}$. In this context it seems logical that firms have an strong incentive to communicate before playing the game in order to eliminate the possibility of coordination failures.

We extend the basic game by adding the pre-play communication scheme developed in this paper to show that both firm can always coordinate themselves in a symmetric way [43]. To this end, we focus in the unique symmetric completely coordinated solution of the game [44], given by its associated probability distribution over every pair of strategies

[43] Farrel (1987) also builds up a communication protocol with T rounds. In each round, every firm can send one message in the set $\{In, Out\}$. The extended game has, of course, many equilibria but there is only one with the following properties:

1. It is symmetric to both firms.

2. If at any step a firm says In and the other says Out, firms send the same messages in all remaining steps and finally they play the corresponding actions.

3. If the communication phase ends and both firms have said either In or Out at every step, the Dixit-Shapiro equilibrium is played.

Farrell proves that the expected payoff is always bigger than u_{DS} and encreases with T. Also, the probability of a coordination failure is always lower than f_{DS} and decreases with T. However, even in the limit case of an infinite communication phase the expected payoff is not greater than B and the probability of failure does not converge to zero.

[44] This is done without loss of generality. This outcome is clearly focal in this symmetric model. However, we could assume asymmetric firms and consider correlated equilibria in which (In, Out) is played with probability γ and (Out, In) with probality $(1-\gamma)$ (with $\gamma \in (0,1)$ and depending on the 'negotiation power' of each firm.

$$\begin{array}{cc} & \begin{array}{cc} In & Out \end{array} \\ \begin{array}{c} In \\ Out \end{array} & \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \end{array}$$

Since this distribution is a convex combination of two Nash equilibria it is trivially associated to a correlated equilibrium in the sense of Aumann (1987). Moreover, with this solution we have that the expected payoff of each firm is $u = \frac{1}{2}M + \frac{1}{2}B$ and that the probability of coordination failure is zero, i.e. $f = 0$.

Once the complete coordination is expressed as a correlated equilibrium of the original game, we can apply *Proposition 2.1* and we have that the perfect coordination payoff for both firms can be achieved as a Nash equilibrium payoff of the game extended by a costless pre-play communication phase, as we have already shown.

Also notice that deviations from the protocol are not profitable for players. By *Proposition 6.4*, any undetected deviation by a player would induce a new distribution $\bar{q}$ on the set of actions of the firms given by:

$$\begin{array}{cc} & \begin{array}{cc} In & Out \end{array} \\ \begin{array}{c} In \\ Out \end{array} & \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \end{array}$$

As we have remarked above, since $n = 2$, $\bar{q}$ has the same correlation power but the opposite coordination power than the original distribution q. Hence, the deviating firm will always disobey the suggestion of the altered protocol in order to maintain coordination and its expected payoff will be the same than it will have obtained by following the protocol. Thus, there is no incentive for a firm to deviate and the communication protocol is self-enforcing.

Let us realize that, in the above case, coordination failures can be completely avoided by using a jointly controlled lottery. This is not true for all the correlated equilibria of the general simultaneous entry game. For instance, consider the case where there exists substitubility between the old and the new product. Then $M > N \geq L > 0 > B > -L$ and the equilibria remain the same. A firm prefers to enter but that both stay out rather than to be the only one which stays out. It is easy two check that the following probability distribution q

$$\begin{array}{cc} & \begin{array}{cc} In & Out \end{array} \\ \begin{array}{c} In \\ Out \end{array} & \left(\begin{array}{cc} 0 & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{array} \right) \end{array}$$

is a correlated equilibrium distribution of the simultaneous entry game. Clearly, the correlated equilibrium payoff associated with this distribution is not achievable by using any jointly controlled lottery. Hence, more complex communication schemes are nedeed in this case. Since our main result holds, we know that this payofs can be reached as a Nash equilibrium payoff by extending the original game with an ex-ante communication phase.

Our communication scheme can also be applied to achieve coordination in the choice of compatibility standards and all the economic situations where payoffs are like these of the battle of the sexes (see Farrell (1987) and Farrell and Saloner (1988)).

8 Conclusions and further extensions.

Our results are usefully summarized in the following statements:

i) Any outcome of any mediated communication two-person normal form game (with rational payoffs) of complete information is also an outcome of an unmediated communication two-person normal form game of complete information.

ii) And such outcomes are the Nash equilibriun outcomes of a normal form two-person game of complete information extended by a pre-play costless communication scheme involving a universal mechanism of unmediated 'plain conversation'.

The natural extensions of these results are mainly two:

Firstly, the extension to n players. This extension of our result may be easily obtained if we assume, as in Barany (1992) and Forges' (1990) papers, that players cannot form coalitions. The pattern of the information in our protocol will form a loop. In other words, the information starting from a player will follow a one arrow direction to another player and, it

will come back to the first one in the opposite direction [45]. Obviously, the more appealing extension is for the three player case (with a finite set of messages), since for four or more player satisfactory results are provided by Barany (1992).

Secondly, the extension to general two-person games with incomplete information. In this class of games players have private information and hence the communication protocol has to achieve two effects at the same time: information transmission and coordination of the players.

Satisfactory results are avaliable for first, all games of incomplete information with at least four players (Forges (1990)), and second, for games of information transmission with independent senders (Forges (1988)). Again, for three person games of incomplete information the above result extends once the requeriment of finite message sets is relaxed. Hence, the only open question here concerns the finiteness of the sets of messages.

For two player games of incomplete information no results are avaliable for the general case under unmediated talk. However, some answers have been given for specific games. Thus, for two person Sealed Bid Double Auctions games, Matthews and Postlewaite (1989) proved that the set of Bayesian-Nash equilibrium outcomes of the unmediated communication-bidding game defined by adding one round of simultaneous message exchange contains the equilibrium outcomes of all other communication-bidding games. But, their result relies on simultaneous rather than sequential message exchange and

[45] The sketch of the information flow in the three player case would be the following:

1. The three player agree on the use of an alphabet and assign to each trio of actions a set of three letter words $(\alpha_i, \beta_j, \gamma_k)$ in the same way as in the two player case.

2. Each player selects indepentdtly exponential encription and deciphering functions E_h, D_h, $(h = 1,2,3,)$.

3. The first player codiphies each word $(\alpha_i, \beta_j, \gamma_k)$ by applying his function E_1 and sends all the codified words $(E_1(\alpha_i), E_1(\beta_j), E_1(\gamma_k))$

4. The second player applies E_2 to the last two letters of every word and sends to the third player $(E_1(\alpha_i), E_2(E_1(\beta_j)), E_2(E_1(\gamma_k)))$

5. The third player selects one of these words (say $(E_1(\alpha), E_2(E_1(\beta)), E_2(E_1(\gamma))))$ without knowing its real meaning. Afterward, he sends $(E_2(E_1(\beta)), E_3(E_2(E_1(\gamma))))$ to the first player. The first one calculates $(E_2(\beta), E_3(E_2(\gamma)))$ and sends $E_3(E_2(\gamma))$ to the second player. The second one calculates $E_3(\gamma)$.

6. The first player sends $E_2(\beta)$ to the second one. The second player sends $E_3(\gamma)$ to the third one. The third player sends $E_1(\alpha)$ to the first one.

7. Every player deciphers his message and plays the corresponding action.

communication in their equilibria plays only a coordination role[46]. Also for mediated talk results are provided by Lehrer and Sorin (1997). For the convex hull of the Nash equilibrium payoffs, results are provided by Aumann and Hart (1992).

The main difficulty with designing unmediated communication protocols for two player general games of incomplete information is to combine together signaling and decision making. Examples in Forges (1990) show that this is not an easy task. Our future work goes through first investigating this kind of examples.

[46]Farrell and Gibbons (1989) were the first to consider communication in a double auction. Although their game is a special case of that of Matthews and Postlewaite, their equilibrium is a true communication equilibrium in the sense that it both transmits information and coordinates decisions.

Appendix: Proof of Lemma 6.1.

The biggest pay-off that P_1 can get ex-ante with his deviation is

$$\sum_{i=1}^{s} \bar{q}(a_i) max_{a_{l_i} \in A} \sum_{j=1}^{t} \bar{q}(b_j|a_i) u_1(a_{l_i}, b_j) =$$

$$= \sum_{i=1}^{s} \bar{q}(a_i) \sum_{j=1}^{t} \bar{q}(b_j|a_i) u_1(\hat{a}_i, b_j) = \sum_{i=1}^{s} \sum_{j=1}^{t} \bar{q}(a_i, b_j) u_1(\hat{a}_i, b_j)$$

where $\hat{a}_i = arg \quad max_{a_{l_i} \in A} \sum_{j=1}^{t} \bar{q}(b_j|a_i) u_1(a_{l_i}, b_j)$. Using proposistion 6.3 and the properties that characterizes q as a correlated equilibrium distribution, we have that:

$$\sum_{i=1}^{s} \sum_{j=1}^{t} \bar{q}(a_i, b_j) u_1(\hat{a}_i, b_j)$$

$$= \frac{1}{n-1} (n \sum_{i=1}^{s} q(a_i) \sum_{j=1}^{t} q(b_j) u_1(\hat{a}_i, b_j) - \sum_{i=1}^{s} \sum_{j=1}^{t} q(a_i, b_j) u_1(\hat{a}_i, b_j))$$

$$= \frac{1}{n-1} (n \sum_{i=1}^{s} q(a_i) \sum_{j=1}^{t} (q(a_i, b_j) + \sum_{k=1, k \neq i}^{s} q(a_k, b_j)) u_1(\hat{a}_i, b_j)$$

$$- \sum_{i=1}^{s} \sum_{j=1}^{t} q(a_i, b_j) u_1(\hat{a}_i, b_j))$$

$$\leq \frac{1}{n-1} (n \sum_{i=1}^{s} q(a_i) \sum_{j=1}^{t} (q(a_i, b_j) u_1(\hat{a}_i, b_j) + \sum_{k=1, k \neq i}^{s} q(a_k, b_j) u_1(a_k, b_j))$$

$$- \sum_{i=1}^{s} \sum_{j=1}^{t} q(a_i, b_j) u_1(\hat{a}_i, b_j))$$

Writing $u_1(\hat{a}_i, b_j)$ as $u_1(a_i, b_j) - u_1(a_i, b_j) + u_1(\hat{a}_i, b_j)$, we obtain that:

$$
\begin{aligned}
& \sum_{i=1}^{s}\sum_{j=1}^{t}\bar{q}(a_i,b_j)u_1(\hat{a}_i,b_j) \\
\leq\ & \frac{1}{n-1}(n\sum_{i=1}^{s}q(a_i)\sum_{j=1}^{t}(q(a_i,b_j)(u_1(a_i,b_j)-u_1(a_i,b_j)+u_1(\hat{a}_i,b_j)) \\
& +\sum_{k=1,k\neq i}^{s}q(a_k,b_j)u_1(a_k,b_j))-\sum_{i=1}^{s}\sum_{j=1}^{t}q(a_i,b_j)u_1(\hat{a}_i,b_j)) \\
=\ & \frac{1}{n-1}(n\sum_{j=1}^{t}\sum_{k=1}^{s}q(a_k,b_j)u_1(a_k,b_j)(\sum_{i=1}^{s}q(a_i)) \\
& -n\sum_{i=1}^{s}q(a_i)\sum_{j=1}^{t}q(a_i,b_j)(u_1(a_i,b_j)-u_1(\hat{a}_i,b_j)) \\
& -\sum_{i=1}^{s}\sum_{j=1}^{t}q(a_i,b_j)u_1(\hat{a}_i,b_j))
\end{aligned}
$$

Since $\sum_{i=1}^{s}q(a_i)=1$, we can write:

$$
\begin{aligned}
& \sum_{i=1}^{s}\sum_{j=1}^{t}\bar{q}(a_i,b_j)u_1(\hat{a}_i,b_j)\leq\sum_{i=1}^{s}\sum_{j=1}^{t}q(a_i,b_j)u_1(a_i,b_j) \\
& +\frac{1}{n-1}(\sum_{i=1}^{s}(1-nq(a_i))\sum_{j=1}^{t}q(a_i,b_j)(u_1(a_i,b_j)-u_1(\hat{a}_i,b_j)))
\end{aligned}
$$

Hence, we need only to prove that the terms

$$
(1-nq(a_i))\sum_{j=1}^{t}q(a_i,b_j)(u_1(a_i,b_j)-u_1(\hat{a}_i,b_j))
$$

are non-positive. But this conclusion is straight by considering these two cases:

i) If $q(a_i)\neq 0$ we have that $nq(a_i)\geq 1$ since n is the minimum common multiple of the denominators of $q(a_i,b_j)$. Moreover $\sum_{j=1}^{t}q(a_i,b_j)(u_1(a_i,b_j)-$

$u_1(\hat{a}_i, b_j)) \geq 0$ given that q is a distribution associated to a correlated equilibrium, and then $(1-nq(a_i)) \sum_{j=1}^{t} q(a_i, b_j)(u_1(a_i, b_j) - u_1(\hat{a}_i, b_j)) \leq 0$

ii) If $q(a_i) = 0$ we have $q(a_i, b_j) = 0 \ \forall j = 1, ..., t$ and then $(1 - nq(a_i)) \sum_{j=1}^{t} q(a_i, b_j)(u_1(a_i, b_j) - u_1(\hat{a}_i, b_j)) = 0$

References.

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.*

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

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

R. Aumann, M Maschler and R. E. Stearns (1968): 'Repeted games of incomplete imformation.' *Mathematica 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.*

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.*

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): 'Comunication, 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.*

O. Gossner (1996): 'Secure protocols.' *Working Paper 9630. CEREMADE* Universite Paris Dauphine.

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

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

E. Lehrer and S. Sorin (1994): 'One shot public mediated communication.' Forthcoming in *Games and Economic Behavior.*

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 algorythm for computing logarythms over GF(p) and its cryptographyc 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. L. Rivest, A. Shamir and L. Adleman (1978): 'A method for obtaining digital signatures and public key cryptosystems.' *Comm. ACM 21(2), 120-126.*

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.*