Int J Game Theory (2001) 30:41–60

International Journal of Game Theory

Repeated communication through the mechanism *and*

Olivier Gossner*, Nicolas Vieille†

* THEMA, Université Paris X-Nanterre, 200 avenue de la République, 92001 Nanterre, France and CORE, 34 Voie du Roman Pays, Université Catholique de Louvain, Belgique.
† Laboratoire d'économétrie, Ecole Polytechnique, and Département Finance et Economie, HEC, 1 rue de la Libération, 78 351 Jouy en Josas, France (e-mail: vieille@hec.fr)

Received December 1998/Final version November 2000

Abstract. We consider the "and" communication device that receives inputs from two players and outputs the public signal *yes* if both messages are *yes*, and outputs *no* otherwise. We prove that no correlation can securely be implemented using this device, even when infinitely many stages of communication are allowed.

1. Introduction

Our goal in this paper is to analyze the intrinsic correlation opportunities offered by a given communication device (Forges [3]). It thus relates closely to the literature on preplay communication, and more precisely to the literature on mediated talk, initiated by Lehrer [8]. In this strand of literature, a game is given, and one wishes to implement correlated equilibrium distributions (c.e.d. thereinafter) of the game as the outcome of communication equilibria, using communication devices of a simple form. In Lehrer and Sorin [9], it is shown that any c.e.d. (with rational entries) coincides with the distribution induced by some communication equilibrium, where the communication device sends *public* outputs that depend deterministically on the inputs.

It is natural to allow for repeated preplay communication; namely, to consider situations in which preplay communication proceeds in stages. At each stage, the players send inputs to the device, that sends back outputs. In that case, a stronger result is obtained. Given a game, there exists a communication device with public and deterministic output, that has the following property: every c.e.d. can be approximated by the outcome of an equilibrium of the game extended by finitely many stages of preplay communication. Thus, the same communication device is used for every c.e.d.; only the length of the preplay communication depends on the particular c.e.d.

The previous devices are game-dependent[1]. We wish here to avoid this dependency, and to investigate the existence of universal protocols of communication. Given a communication device, we wish to characterize the set of distributions μ that can be implemented with it, in the sense that: as soon as μ is a c.e.d. of a game G, μ is the outcome of an equilibrium of the game G, extended with infinitely many stages of preplay communication. Moreover, we shall require that the strategies during the communication phase (the communication protocol) does not depend on G.

More precisely, the question we ask here is essentially the following. Let D_1, D_2 be finite (action) sets for two players and let a communication device be given. We allow infinitely many stages of communication. A *protocol* consists in the specification of a profile of communication strategies, and of rules used to choose an action, as a function of the sequence of signals received during preplay communication. A protocol induces a distribution μ over the product set $D = D_1 \times D_2$. A protocol *securely implements* μ if, for every game G with action sets D_1 and D_2, the protocol is a Nash equilibrium of the extended game, as soon as μ is a correlated equilibrium distribution of G. Gossner [6] establishes a convenient characterization of secure protocols. In words, a protocol securely implements μ if

(i) no player can manipulate the distribution of decisions
(ii) at the end of the communication phase, player i's belief on the other player's decision coincides with $\mu(\cdot|d^i)$, whatever be the sequence of messages received by player i: the decision player i is about to take contains all the information he has about the decision of the other player.

This question was partly addressed in Bárány [1], who assumes that at least four players communicate using «phone lines», and in addition that each player has available a STOP button, that reveals to all players all past communication. Therefore, his study does not fall into our framework. Under these assumptions, Bárány shows that any distribution with rational coefficients can be securely implemented.

We answer our question in the case of a specific communication device, which we call the *and*-mechanism. The *and*-operator in logic is defined over $\{0,1\} \times \{0,1\}$ as $and(x, y) = xy$. By analogy, we define the *and*-mechanism as a communication mechanism which receive messages x, y from two players, chosen in $\{0,1\}$, and sends them back the value of $and(x, y)$. We assume in addition that each player remembers which message he sent or, equivalently, that the signals to 1 and 2 are respectively the pairs $(x, and(x, y))$ and $(y, and(x, y))$. A matrix representation of this mechanism is given below

	0	1
0	0	0
1	0	1

The crucial feature of this mechanism is that when player 1 sends $x = 0$ to the

[1] In the first quoted result of Lehrer-Sorin, the device depends only on μ, not on the game on which μ is a c.e.d.

mechanism, the signal he gets gives him no information about the value of y ($and(0, y) = 0$) whereas when he sends $x = 1$, he is able to deduce the value of y from his signal ($and(1, y) = y$).

The main rationale for considering this device is that it is the simplest device which, when repeated, allows for a complex intertwining of the information structures of the two players. Indeed, the two information structures $\mathscr{H}_n^1$ and $\mathscr{H}_n^2$ corresponding to the first n stages of communication are so different that knowledge operators of different depth differ. It is therefore reasonable to hope that the techniques developed here may be of use in dealing with more general devices.

Our result is essentially negative: we prove that only *babbling* is secure. If decisions are not independent of the outcome of the communication phase, the procedure can be manipulated by one player. Our result can be rephrased as saying that any non-trivial attempt to use the intertwining of information structures to generate correlation after infinitely many stages of preplay communication can be manipulated by at least one player. Parts of the proofs below may be found in [5], [11].

Our result thus stands in sharp contrast with those of Lehrer [7]. Lehrer studied the *and*-mechanism in the context of repeated games with imperfect monitoring. In this context, it is natural to study the case where the whole procedure (preplay communication and decision stage) is infinitely repeated over time. Lehrer proves that any distribution with rational coefficients can be obtained. This involves a statistical monitoring of the behavior of each player.

This question is also related to issues in computer science. For instance, in the design of fault-tolerant distributed systems, protocols (*i.e.*, communication strategies) are sought for that enable interconnected processors to perform a given task, even if one (or more) is to fail. More than two processors are assumed, and the communication mechanism consists of secure communication lines between each two processors, which allow them to exchanges messages without being eavesdropped. We refer to Linial [10] for references and an extensive discussion of the links between game theory and computer science.

The paper is organized as follows. Section 1 contains the model and the statement of the result. Sections 2 and 3 contain the proof. Section 2 deals with the case where finitely many stages of communication are allowed. Section 3 deals with the general case, and is independent of Section 2. Although the result of Section 2 is included in Section 3, its proof is both much more simple and intuitive. We thus find it worthy to include it.

2. Concepts and results

We take up the study of the repeated *and*-mechanism described in the introduction. For emphasis, we label the possible messages of player $i \in \{1, 2\}$ as N^i (for non-informative) and I^i (for informative). We set $M^i = \{N^i, I^i\}$. For simplicity, we label $a, b, c, *$ the different input combinations, as specified in the next array:

	N^2	I^2
N^1	a	c
I^1	b	$*$

The signal function l^1 of player 1 is best described by introducing $\mathscr{P}^1 = \{\{a,c\},\{b\},\{*\}\}$. It is the partition of the set of message pairs induced by the signaling function of player 1: when the combination of messages sent to the mechanism is m, player 1 is told which atom of $\mathscr{P}^1$ contains m. For simplicity, we sometimes write $\mathscr{P}^1 = \{N^1, I^1, *\}$. The information partition $\mathscr{P}^2$ of player 2 is defined symmetrically. For instance, $l^1(N^1, I^2) = \{a,c\} = N^1$, while $l^2(N^1, I^2) = \{c\}$.

Repeated communication unfolds as follows: at every stage $n \in \mathbb{N}$, players send simultaneously messages m_n^1, m_n^2 to the mechanism. Player i is told $l^i(m_n^1, m_n^2)$.

The set of plays is $H_\infty = M^{\mathbb{N}} = \{a,b,c,*\}^{\mathbb{N}}$. We denote by $\mathscr{H}_n^i$ the information available to player i in stage n, prior to sending a message: it is the algebra over H_∞ generated by cylinder sets of the form $h_n^i \times H_\infty$, where $h_n^i \in (\mathscr{P}^i)^{n-1}$ is a sequence of $n-1$ elements of $\{N^i, I^i, *\}$. We also denote by $\mathscr{H}_n$ the algebra generated by histories up to stage n, namely by cylinder sets of the form $h_n \times H_\infty$, where $h_n \in \{a,b,c,*\}^{n-1}$. We denote by $\mathscr{H}_\infty^i = \sigma(\mathscr{H}_n^i, n \geq 1)$ and $\mathscr{H}_\infty = \sigma(\mathscr{H}^n, n \geq 1)$ the σ-algebras over H_∞ induced by these algebras. We shall sometimes use the natural identification of $\mathscr{H}_n$ with the finite set $H_n = \{a,b,c,*\}^{n-1}$.

The set S_n^i of pure (*resp.* Σ_n^i of mixed) strategies of communication *at stage* n is the set of all maps from $(H_\infty, \mathscr{H}_n^i)$ to M^i (*resp.* $\Delta(M^i)$): such a map specifies which message to send in stage n, as a function of the signals received so far. A pure (*resp.* behavioral) strategy of communication of player i is a sequence $\sigma^i = (\sigma_n^i)_{n \geq 1}$, where $\sigma_n^i \in S_n^i$ (*resp.* $\sigma_n^i \in \Sigma_n^i$). Thus the set of pure strategies of player i is $S^i = \times_{n \geq 1} S_n^i$, endowed with the product topology of the discrete ones on each factor. S^i is then compact and metrizable. We denote by $\mathscr{S}^i$ the Borel σ-algebra on S^i. A mixed strategy of player i is a probability distribution over $(S^i, \mathscr{S}^i)$. Since perfect recall holds, any mixed strategy is equivalent to a behavioral strategy.

At the end of the communication phase, player i takes a decision from a finite set D^i. A decision rule ϕ^i specifies which decision to choose as a function of the signals; it is a mapping from $(H_\infty^i, \mathscr{H}_\infty^i)$ to $\Delta(D^i)$. A **protocol** consists of a pair of strategies (σ^1, σ^2) together with a pair of decision rules $\phi = (\phi^1, \phi^2)$. Set $D = D^1 \times D^2$. Given a protocol (σ, ϕ), $P_{\sigma,\phi}$ stands for the probability distribution induced by σ and ϕ on $(H_\infty \times D, \mathscr{H}_\infty \otimes 2^D)$ and $\mu_{\sigma,\phi}$ and $\mu_{\sigma,\phi}^i$ are the marginals of $P_{\sigma,\phi}$ on D and D^i respectively. Similarly, P_σ is the distribution induced by σ on $(H_\infty, \mathscr{H}_\infty)$. We call $\mu_{\sigma,\phi}$ the **information structure generated** by the protocol (σ, ϕ).

It is clear how the above specializes when only finitely many stages of communication are allowed. In the N-stage version, the decision rule ϕ_N^i is $\mathscr{H}_N^i$-measurable.

We use extensively various coordinate mappings, which we represent in bold type: $\mathbf{m}_n^i$, $\mathbf{s}_n^i$ are respectively the message sent and signal received by player i in stage n, $\mathbf{h}_n^i$ is the sequence of signals by i up to stage n (such a sequence is usually identified to an atom of $\mathscr{H}_n^i$), $\mathbf{h}_\infty$ is the history up to the decision stage, and $\mathbf{d}^i$ is the decision of player i. Bold type symbols hence represent random variables.

For simplicity, we sometimes write h_n^i for the event $\{\mathbf{h}_n^i = h_n^i\}$ of $\mathscr{H}_n^i$, and use similar shortcuts when convenient. Given a strategy $\sigma^i = (\sigma_n^i)_n$ of player i, $\sigma_n^i(h_n^i)$ is the mixed move used after the history h_n^i; $\sigma_n^i(h_n^i)[m^i]$ is then the

probability of sending the message m^i. The support of a measure ν is denoted by supp ν.

We recall from Gossner [6] the definition of a secure protocol.

Definition 1. *A protocol* (σ, ϕ) *is* ***secure*** *when for any alternative strategy* τ^1 *of player 1:*

R.1 $\mu^2_{(\tau^1,\sigma^2),\phi} = \mu^2_{\sigma,\phi}$;

R.2 $\mathbf{h}^1_\infty$ *is less informative on* $\mathbf{d}^2$ *under* $P_{(\tau^1,\sigma^2),\phi}$ *than* $\mathbf{d}^1$ *under* $P_{\sigma,\phi}$, *and symmetric properties hold for player 2.*

R.1 means that player 1 can not influence the distribution of $\mathbf{d}^2$ by deviating from σ^1.

The notion of less informative in **R.2** refers to Blackwell's [2] notion of comparison of experiments. The comparison in **R.2** is meaningful since the distributions of $\mathbf{d}^2$ under $P_{\sigma,\phi}$ and $P_{(\tau^1,\sigma^2),\phi}$ are the same. **R.2** implies that player one cannot get more information on $\mathbf{d}^2$ by changing σ^1, and that $\mathbf{d}^1$ is a sufficient statistic for $\mathbf{d}^2$ for player 1 under $P_{\sigma,\phi}$, *i.e.*

$$P_{\sigma,\phi}(\mathbf{d}^2 = \cdot \mid \mathbf{d}^1) = P_{\sigma,\phi}(\mathbf{d}^2 = \cdot \mid \mathscr{H}^1_\infty), \quad P_{\sigma,\phi}\text{-a.s.}$$

This definition is motivated by the following property (Gossner [6]). Given a strategic form game G, define the two games $\Gamma_1(G)$ and $\Gamma_2(G)$ as follows:

- in $\Gamma_1(G)$, $\mathbf{d} \in D$ is drawn according to μ, player i is informed of the coordinate $\mathbf{d}^i$, then plays in G;
- in $\Gamma_2(G)$, players communicate through the mechanism, then play in G.

A protocol is secure if and only if for every G and every Nash equilibrium f of $\Gamma_1(G)$, the following is a Nash equilibrium of $\Gamma_2(G)$: communicate according to σ, take decisions following ϕ, then play in G according to f.

We call $\mu \in \Delta(D)$ a *secure distribution*, or secure information structure, if $\mu = \mu_{\sigma,\phi}$ for some secure protocol (σ, ϕ).

Our main result is the following.

Theorem 1. *The set of secure distributions is* $\Delta(D^1) \times \Delta(D^2)$.

Remark 1: let $\mu = \mu^1 \otimes \mu^2 \in \Delta(D^1) \times \Delta(D^2)$. It is straightforward to generate μ as the result of *babbling*. Define $\sigma = (\sigma^1, \sigma^2)$ arbitrarily (players babble), and let player i ignore the communication and choose $\mathbf{d}^i$ according to μ^i: ϕ^i is the constant map μ^i. Such (σ, ϕ) is clearly secure. Therefore, what our result really entails is that every non-trivial protocol based upon the *and*-mechanism can be manipulated. No correlation can be secured, even when infinitely many stages of preplay communication are allowed.

3. Finitely many stages

3.1. Reduction to minimal information structures

An information structure $\mu \in \Delta(D)$ is called **minimal** when:

- For any $d_0^1, d_1^1 \in \text{supp}\, \mu^1$, the conditional probabilities $\mu(\cdot|d_0^1)$ and $\mu(\cdot|d_1^1)$ on D^2 differ.
- A symmetric condition holds for player 2.

This amounts to assuming that the statistic $\mathbf{d}^i$ must be minimal for player i.

For instance, the only minimal information structures in $\Delta(D^1) \times \Delta(D^2)$ are the unit masses.

Remark 2: By Proposition 9.3 in [6], it is enough to prove that *minimal* secure information structures are unit masses. In the following, we focus on minimal information structures.

Remark 3: Let (σ, ϕ) be a secure protocol which generates μ. Then, $P_{\sigma,\phi}$-a.s., for every $d^i \in \text{supp}\, \phi^i(\mathbf{h}_\infty^i)$, $P_{\sigma,\phi}(\mathbf{d}^{3-i} = \cdot \mid d^i) = P_{\sigma,\phi}(\mathbf{d}^{3-i} = \cdot \mid \mathbf{h}_\infty^i)$. Therefore, since μ is minimal, $\phi^i(\mathbf{h}_\infty^i)$ is a Dirac mass, $P_{\sigma,\phi}$-a.s. In other words, ϕ^i is "pure" on the support of P_σ.

3.2. Proof for finitely many stages

We assume here that N stages of communication are allowed.

Let (σ, ϕ) be a secure protocol, and $\mu = \mu_{\sigma,\phi}$. We identify μ to a $D^1 \times D^2$-matrix, whose (d^1, d^2)-entry is $\mu(d^1, d^2)$. As noted in the previous section, we may assume that, P_σ-a.s., $\phi^i(\mathbf{h}_\infty^i)$ puts probability one on some decision. It is crucial to note that we cannot assume this to hold outside of the support of P_σ.

The proof is divided in two steps. First, we introduce a most informative deviation of player i, and argue that up to some permutation of lines and columns, μ is diagonal: at the end of the communication phase, each player knows $P_{\sigma,\phi}$-a.s. the decision of the other. Second, we introduce a least informative deviation of player i, and prove that μ is concentrated on one decision pair.

Step 1: a most informative strategy We shall define a strategy of player 1 that enables him to know at the end of the communication phase which decision player 2 is about to take. Clearly, the way to get the most information is to use the strategy $\tilde{\sigma}^1$ defined as: play I^1 in every stage, irrespective of past signals. This falls short of proving anything since the supports of $P_{(\tilde{\sigma}^1,\sigma^2),\phi}$ and $P_{\sigma,\phi}$ may be disjoint: hence, knowing which signals player 2 did receive may not enable player 1 to deduce which decision player 2 is about to take (since the decision rule might be random outside the support of $P_{\sigma,\phi}$).

Hence we amend the above definition of $\tilde{\sigma}^1$ as: play I^1 whenever player 2 finds it *plausible* that player 1 does play I^1, *i.e.*, when, conditional upon player 2's past signals, there is a positive $P_{\sigma,\phi}$-probability that player 1 sends the message I^1. Of course, this is not well-defined since the message sent by player 1 is then a function of the information held by player 2. Therefore, our first task is to show that this construction is essentially meaningful: we show inductively that if player 1 abides by this strategy up to stage n, player 1 will *know* at stage n the belief held by player 2 on player 1's message at stage n.

Definition 2. *Let P be a probability distribution, X be a random variable defined over $(H_\infty, \mathcal{H}_\infty)$, and $n \in \mathbb{N}$. We say that player 1 knows X under P at stage n if there exists an $\mathcal{H}_n^1$-measurable version of X under P.*

Thus, player 1 knows X under P if there exists a $\mathscr{H}_n^1$-measurable variable Y such that $P(X = Y) = 1$.

It is convenient to introduce the set $C_n^1(h_n^2)$ of sequences of signals (to player 1) which are consistent with the fact that player 2 receives h_n^2:

$$C_n^1(h_n^2) = \{h_n^1, h_n^1 \cap h_n^2 \neq \varnothing\}$$

where the intersection $h_n^1 \cap h_n^2$ is taken as of elements of $\mathscr{H}_\infty$: $h_n^1 \in C_n^1(h_n^2)$ if, for some sequence h_n, the signals received along h_n by the two players are respectively h_n^1 and h_n^2. $C_n^2(h_n^1)$ is defined similarly.

Let $\mathbf{p}_n^2 = P_{\sigma,\phi}[\cdot|\mathscr{H}_n^2]$ be the posterior belief on $\mathscr{H}_n^1$ given $\mathscr{H}_n^2$. Notice that $\mathbf{p}_1^2$ is a constant ($\mathscr{H}_1^2$ is trivial), hence known to player 1 at stage 1.

We construct σ_+^1 inductively. Assume that $\sigma_{+,m}^1$ has been defined for $m < n$, and that player 1 knows $\mathbf{p}_n^2$ at stage n under $P_{\sigma_+^1,\sigma^2}$ (this depends only upon the definition of (σ_+^1, σ^2) in the first $n-1$ stages). Denote by $\tilde{\mathbf{p}}_n^2$ an $\mathscr{H}_n^1$-measurable version of $\mathbf{p}_n^2$. We set

$$\begin{cases} \sigma_{+,n}^1(h_n^1) = I^1 & \text{if } \tilde{\mathbf{p}}_n^2(h_n^1)\{\mathbf{m}_n^1 = I^1\} > 0 \\ \sigma_{+,n}^1(h_n^1) = N^1 & \text{otherwise} \end{cases}$$

In the first case, player 1 knows that player 2 asserts a strictly positive probability on I^1 being played in stage n. In the second case, player 1 knows that player 2 does not expect I^1 to be played.

Lemma 1. *Player 1 knows* $\mathbf{p}_{n+1}^2$ *at stage* $n+1$ *under* $P_{\sigma_+^1,\sigma^2}$

Proof: consider any sequence of signals $h_{n+1}^1 \in \mathscr{H}_{n+1}^1$ that belongs to the support of $P_{\sigma_+^1,\sigma^2}$. We need to prove that $\mathbf{p}_{n+1}^2$ is constant over $C_{n+1}^2(h_{n+1}^1) \cap \operatorname{supp} P_{\sigma_+^1,\sigma^2}$. Write h_{n+1}^1 as (h_n^1, s_n^1) where h_n^1 contains the signals to player 1 up to stage n. Let $h_{n+1}^2 = (h_n^2, s_n^2) \in C_{n+1}^1(h_{n+1}^1) \cap \operatorname{supp} P_{\sigma_+^1,\sigma^2}$. We distinguish three cases.

In the first case we assume that player 1 knows that player 2 expects N^1 to be played:

Case 1: $s_n^1 = N^1$. Then:

$$\mathbf{p}_n^2(h_n^2)\{\mathbf{m}_n^1 = N^1\} = 1,$$

and the belief $\mathbf{p}_{n+1}^2(h_{n+1}^2)$ of player 2 at stage $n+1$ is given by

$$\mathbf{p}_{n+1}^2(h_{n+1}^2)[\tilde{h}_n^1, \tilde{s}_n^1] = \begin{cases} \mathbf{p}_n^2(h_n^2)[\tilde{h}_n^1] & \text{if } \tilde{s}_n^1 = N^1 \\ 0 & \text{otherwise} \end{cases}$$

In words, after any history $\tilde{h}_n^1$ consistent with h_n^2, player 1 is supposed to play N^1, hence the probability assigned by player 2 to the sequence $(\tilde{h}_n^1, N^1)$ coincides with the probability assigned to $\tilde{h}_n^1$.

In the last two cases, $\mathbf{m}_n^1 = I^1$, hence player 1 gets to know s_n^2. Since he knew the belief p_n^2 of player 2, he can compute the belief held in stage $n+1$.

Case 2: $s_n^1 = I^1$.

In that case, $s_n^2 = N^2$ and the belief of player 2 at stage $n+1$ is given by

$$\mathbf{p}_{n+1}^2(h_{n+1}^2)[\tilde{h}_n^1, \tilde{s}_n^1] = \begin{cases} \mathbf{p}_n^2(h_n^2)[\tilde{h}_n^1] \times \sigma^1(\tilde{h}_n^1)[I^1] & \text{for } \tilde{s}_n^1 = I^1 \\ \mathbf{p}_n^2(h_n^2)[\tilde{h}_n^1] \times \sigma^1(\tilde{h}_n^1)[N^1] & \text{for } \tilde{s}_n^1 = N^1 \\ 0 & \text{for } \tilde{s}_n^1 = * \end{cases}$$

Case 3: $s_n^1 = *$.

In that case, $s_n^2 = *$, and Bayes' rule yields

$$\mathbf{p}_{n+1}^2(h_{n+1}^2)[\tilde{h}_n^1, \tilde{s}_n^1] = \begin{cases} \dfrac{\mathbf{p}_n^2(h_n^2)[\tilde{h}_n^1] \times \sigma^1(\tilde{h}_n^1)[I^1]}{\Sigma_{\hat{h}_n^1} \mathbf{p}_n^2(h_n^2)[\hat{h}_n^1] \times \sigma^1(\hat{h}_n^1)[I^1]} & \text{for } \tilde{s}_n^1 = * \\ 0 & \text{otherwise} \end{cases}$$

In each case, the belief of player 2 in stage $n+1$ is known to player 1. Therefore, under $(\sigma_+^1, \sigma^2, \phi)$, player 1 knows at stage N the belief held by player 2 over $\mathscr{H}_N^1$, hence the belief over $\mathbf{d}^1$. Using the minimality assumption, this implies that, $P_{\sigma_+^1, \sigma^2, \phi}$-a.s., player 2 knows $\mathbf{d}^2$ at stage N. By secureness, $\mathbf{h}_N^1$ is less informative on $\mathbf{d}^2$ under $P_{\sigma_+^1, \sigma^2, \phi}$ than $\mathbf{d}^1$ on $\mathbf{d}^2$ under $P_{\sigma, \phi}$. Thus, for every $d^1 \in \operatorname{supp} \mu^1$, $d^2 \in D^2$, $\mu(d^2|d^1)$ is either equal to 0 or 1. Using once again the minimality assumption, μ is a diagonal matrix (up to some permutation of lines and columns and after deletion of lines and columns containing only 0's). This ends the proof of Lemma 1. ♣

Step 2: a least informative strategy Clearly, the strategy of player 1 that provides him with the least information about signals received by player 2 is to send repeatedly the message N^1. As above, this has to be amended, since it might be the case that player 2 knows at some stage that player 1 should play I^1 according to σ^1. We define σ_-^1 as: play N^1 whenever N^1 is played with positive probability according to σ^1, $\sigma_-^1(h_n^1) = N^1$ if $\sigma^1(h_n^1)[N^1] > 0$, and $\sigma_-^1(h_n^1) = I^1$ otherwise. It is clear that $P_{\sigma_-^1, \sigma^2} \ll P_\sigma$ (absolutely continuous). We set $S = \operatorname{supp} P_{\sigma_-^1, \sigma^2}$. We prove in Lemma 2 that $\mathbf{d}^1$ is constant on S. Since $S \subseteq \operatorname{supp} P_\sigma$ and μ is diagonal, $\mathbf{d}^2$ is also constant on S. Since the distributions of $\mathbf{d}^2$ under $P_{\sigma_-^1, \sigma^2}$ and P_σ are the same, this implies that μ is concentrated on a single decision pair $d \in D$. This concludes the proof of the theorem in the finitely repeated case.

We first briefly give the intuition behind Lemma 2. If the decision of player 1 were to depend upon the signals received in the stages in which he plays I^1, there would be a sequence h_n^1 such that (h_n^1, I^1) and $(h_n^1, *)$ belong to S, and the distributions of $\mathbf{d}^1$ conditional on these sequences differ. One then can define a strategy of player 2 which enables him to know at stage n whether player 1 did receive h_n^1 or not. By playing either N^2 or I^2 in that case, and properly mimicking σ^2 afterwards, player 2 would be able to influence the distribution of $\mathbf{d}^1$. This would contradict the secureness of (σ, ϕ).

Lemma 2. $\mathbf{d}^1$ *is constant on* S.

Proof: we prove inductively that the conditional distribution $P_\sigma[\mathbf{d}^1 = \cdot \mid \mathscr{H}_n^1]$ is constant, $P_{\sigma_-^1, \sigma^2}$-a.s. In words, under (σ_-^1, σ^2), the belief over $\mathbf{d}^1$ held by player

1 at stage n is independent of the particular sequence of signals that is obtained at stage n. We emphasize that the belief is computed under the original profile σ.

There is nothing to prove for $n = 1$ since $\mathscr{H}_1^1$ is trivial; we assume this is true for some n. We shall prove that, $P_{\sigma_-^1,\sigma^2}$-a.s.

$$P_\sigma(\mathbf{d}^1 = \cdot \mid \mathscr{H}_{n+1}^1) = P_\sigma(\mathbf{d}^1 = \cdot \mid \mathscr{H}_n^1), \tag{1}$$

Fix $h_n^1 = (\bar{s}_1^1, \ldots, \bar{s}_{n-1}^1) \in \mathscr{H}_n^1$ with $P_{\sigma_-^1,\sigma^2}(h_n^1) > 0$. If there is only one sequence h_{n+1}^1 which has positive probability under (σ^1, σ^2) given h_n^1, then (1) holds trivially. Therefore, we need to discuss the case where $\sigma_-^1(h_n^1) = I^1$ and $P_{\sigma_-^1,\sigma^2}[\mathbf{m}_n^2 = I^2 \mid h_n^1] \in]0, 1[$. In that case $\mathbf{h}_{n+1}^1$ may either be (h_n^1, I^1) or $(h_n^1, *)$. We need to prove that

$$P_\sigma(\mathbf{d}^1 = \cdot \mid (h_n^1, I^1)) = P_\sigma(\mathbf{d}^1 = \cdot \mid (h_n^1, *)). \tag{2}$$

We define a strategy σ_+^2 that enables player 2 to assess whether or not player 1 receives the sequence h_n^1 in the first $n-1$ stages. Define σ_+^2 for the first $n-1$ stages as: play N^2 in stage $p \leq n-1$ if $\bar{s}_p^1 = I^1$, and I^2 otherwise. Define $h_n^2 = (\bar{s}_1^2, \ldots, \bar{s}_{n-1}^2)$ by

$$\bar{s}_p^2 = \begin{cases} N^2 & \text{if } \bar{s}_p^1 = I^1 \\ I^2 & \text{if } \bar{s}_p^1 = N^1 \\ * & \text{if } \bar{s}_p^1 = * \end{cases}$$

By construction of S, $P_{\sigma^1,\sigma_+^2}(h_n^2) > 0$ and $P_{\sigma^1,\sigma_+^2}(h_n^1 | h_n^2) = 1$. Indeed, since $P_{\sigma_-^1,\sigma^2}(h_n^1) > 0$, all the stages for which $\bar{s}_p^1 = I^1$(and thus, all the stages for which $\bar{s}_p^2 = N^2$) are stages in which σ^1 prescribes to play I^1.

Given σ_+^2, we define *two* strategies $\tilde{\sigma}_+^2$ and $\bar{\sigma}_+^2$ which differ only after h_n^2.

- $\tilde{\sigma}_+^2$ is defined as:

1. follow σ_+^2 up to stage n and continue with σ^2 if $\mathbf{h}_n^2 \neq h_n^2$;
2. if $\mathbf{h}_n^2 = h_n^2$, play N^2 in stage n, select a *fictitious past* $\tilde{h}_{n+1}^2$ according to $P_\sigma[\cdot \mid (h_n^1, I^1)]$ and continue with σ^2 *as if* the sequence of signals received in the first n stages had been $\tilde{h}_{n+1}^2$.

- $\bar{\sigma}_+^2$ is defined as:

1. same as 1 for $\tilde{\sigma}_+^2$;
2. if $\mathbf{h}_n^2 = h_n^2$, play I^2 in stage n, select a *fictitious past* $\tilde{h}_{n+1}^2$ according to $P_\sigma[\cdot \mid (h_n^1, *)]$ and continue with σ^2, *as if* the sequence of signals received in the first n stages had been $\tilde{h}_{n+1}^2$.

By secureness, for every $d^1 \in D^1$,

$$P_{\sigma^1,\tilde{\sigma}_+^2}(\mathbf{d}^1 = d^1) = P_{\sigma^1,\bar{\sigma}_+^2}(\mathbf{d}^1 = d^1),$$

therefore

$$P_{\sigma^1,\tilde{\sigma}^2_+}(\mathbf{d}^1 = d^1 \mid h^2_n) = P_{\sigma^1,\tilde{\sigma}^2_+}(\mathbf{d}^1 = d^1 \mid h^2_n). \tag{3}$$

By construction,

$$P_{\sigma^1,\tilde{\sigma}^2_+}(\mathbf{d}^1 = d^1 \mid h^2_n) = P_\sigma(\mathbf{d}^1 = d^1 \mid (h^1_n, I^1))$$

and

$$P_{\sigma^1,\tilde{\sigma}^2_+}(\mathbf{d}^1 = d^1 \mid h^2_n) = P_\sigma(\mathbf{d}^1 = d^1 \mid h^1_n, *).$$

Thus, (2) follows from (3), which ends the proof of the induction step.

Finally, remark that $P_{\sigma^1_-,\sigma^2}(\mathbf{d}^1 = \cdot \mid \mathscr{H}^1_N) = 1_{\mathbf{d}^1 = \cdot}$, $P_{\sigma^1_-,\sigma^2}$-a.s., since $\mathbf{d}^1$ has a $\mathscr{H}^1_N$-measurable version under P_σ. (Recall that ϕ^1 is deterministic on supp P_σ. It is therefore enough to modify in an appropriate way the definition of $\mathbf{d}^1$ outside supp P_σ to get such a version.) Since $P_{\sigma^1_-,\sigma^2} \ll P_\sigma$, any such version is also a version under $P_{\sigma^1_-,\sigma^2}$. The result follows. ♣

4. Infinitely many stages

4.1. Secure protocols generating minimal information structures

We start with some preliminary results on secure protocols.

Proposition 1. *Let (σ, ϕ) be a secure protocol generating the minimal information structure μ, and $\sigma^1 = p\sigma^1_0 + (1-p)\sigma^1_1$ with $0 < p \leq 1$.*

Then, for $n \in \mathbf{N}$ and $d \in D$, one has, $P_{(\sigma^1_0,\sigma^2),\phi}$-a.s.:

$$P_{(\sigma^1_0,\sigma^2),\phi}(\mathbf{d} = d \mid \mathscr{H}^1_n) = P_{\sigma,\phi}(\mathbf{d} = d \mid \mathscr{H}^1_n). \tag{4}$$

In this statement, σ^1 is interpreted as a *mixed* strategy, and $\sigma^1 = p\sigma^1_0 + (1-p)\sigma^1_1$ is an equality between probability distributions (elements of $\Delta(S^1)$). The proposition holds for any general communication mechanism, as long as players remember their past messages (perfect recall). Loosely speaking, it asserts that, for any pure strategy in the support of σ^1, the induced distribution on decisions is the same.

For simplicity of notations let $P = P_{\sigma,\phi}$ and $P' = P_{(\sigma^1_0,\sigma^2),\phi}$, so that $P' \ll P$. We start with a few preliminary results. We then prove Proposition 1 at the end of the section.

Lemma 3. *For $h_n \in H_n$, $P'(h_n|\mathscr{H}^1_n) = P(h_n|\mathscr{H}^1_n)$ P' almost surely.*

Shortly, $P'(\cdot|\mathscr{H}^1_n) = P(\cdot|\mathscr{H}^1_n)$, P'-a.s.: at stage n, the beliefs of player 1 on the actual play are the same under P and P'.

Proof: This proof relies on perfect recall but does not require the secureness of (σ, ϕ). Let $h^i_n = \mathbf{h}^i_n(h_n)$ be the sequence of signals received by player i along h_n, and $(m^i_1, \ldots, m^i_{n-1})$ the messages sent by player i along h^i_n. It is enough to

prove $P'(h_n|h_n^1) = P(h_n|h_n^1)$. Set $S(h_n^i) = \prod \sigma_t^i(h_t^i)[m_t^i]$ and $S'(h_n^1) = \prod \sigma_{0,t}^1(h_t^1) \cdot [m_t^1]$ where h_t^i is the truncation of h_n^i at stage t. Note that $P(h_n) = S(h_n^1)S(h_n^2)$. Denote by $C(h_n^1)$ the sequences in $\mathscr{H}_n^2$ which are consistent with h_n^1 (see Section 3.2 for related definitions). For any $h_n' \in C(h_n^1)$, $h_n'^2$ and $S(h_n'^2)$ are defined as above. By Bayes' rule:

$$P'(h_n|h_n^1) = \frac{S'(h_n^1)S(h_n^2)}{\sum_{h_n' \in C(h_n^1)} S'(h_n^1)S(h_n'^2)} = \frac{S(h_n^2)}{\sum_{h_n' \in C(h_n^1)} S(h_n'^2)} = P(h_n|h_n^1) \qquad \clubsuit$$

Lemma 4. *For $d^2 \in D^2$, $P(\mathbf{d}^2 = d^2 \mid \mathscr{H}_\infty^1) = P'(\mathbf{d}^2 = d^2 \mid \mathscr{H}_\infty^1)$ P' almost surely.*

Proof: let $h_m \in H_m$ be fixed. For $n \geq m$, h_m may be viewed as a subset of H_n (the subset of all histories in H_n that begin with h_m). By applying Lemma 3 to each history in this subset, one obtains

$$P(h_m|\mathscr{H}_n^1) = P'(h_m|\mathscr{H}_n^1) \ P'\text{-a.s.}$$

The right side is a $(P', (\mathscr{H}_n)_n)$ martingale converging to $P'(h_m|\mathscr{H}_\infty^1)$ P'-a.s.. The left side is a $(P, (\mathscr{H}_n)_n)$ martingale converging to $P(h_m|\mathscr{H}_\infty^1)$ P-a.s.. Since $P' \ll P$, it also converges to $P(h_m|\mathscr{H}_\infty^1)$, P'-a.s.. Therefore, $P(h_m|\mathscr{H}_\infty^1) = P'(h_m|\mathscr{H}_\infty^1)$ P'-a.s..

Since $\mathscr{H}_\infty$ is generated by the countable family of events $\{\mathbf{h}_m = h_m\}$,

$$P(A|\mathscr{H}_\infty^1) = P'(A|\mathscr{H}_\infty^1), \quad P'\text{-a.s. for any } A \in \mathscr{H}_\infty. \tag{5}$$

Let X be a $\mathscr{H}_\infty$–measurable version of $\mathbf{d}^2$ under P (see the beginning of Section 3.2). Hence $\{X = d^2\} \in \mathscr{H}_\infty$ and

$$P(X = d^2 \mid \mathscr{H}_\infty^1) = P(\mathbf{d}^2 = d^2 \mid \mathscr{H}_\infty^1), \quad P\text{-a.s., hence also } P'\text{-a.s..} \tag{6}$$

Using (5), this completes the proof. $\clubsuit$

Lemma 5. *Under P', $\mathbf{d}^1$ is a sufficient statistic for $\mathbf{d}^2$ for player 1.*

Proof: It is enough to prove that $P'(d^2|\mathscr{H}_\infty^1) = P'(d^2|\mathbf{d}^1)$ P' a.s., for any $d^2 \in D^2$. Fix d^1 such that $P'(d^1) > 0$:

$$\begin{aligned}
P'(d^2|d^1) &= \frac{1}{P'(d^1)} \int_{\phi^1(h_\infty^1)=d^1} P'(d^2|h_\infty^1)\, dP'(h_\infty^1) \\
&= \frac{1}{P'(d^1)} \int_{\phi^1(h_\infty^1)=d^1} P(d^2|h_\infty^1)\, dP'(h_\infty^1) \\
&= \frac{1}{P'(d^1)} \int_{\phi^1(h_\infty^1)=d^1} P(d^2|d^1)\, dP'(h_\infty^1) \\
&= P(d^2|d^1).
\end{aligned}$$

The initial equality expresses Bayes's rule, the second equality is derived from Lemma 4, and the third one uses that, by secureness, $P(d^2|h_\infty^1) = P(d^2|d^1)$ P-a.s., hence also P'-a.s. since $P' \ll P$.

Thus, $P'(d^2|\mathbf{d}^1) = P(d^2|\mathbf{d}^1)$, P'-a.s.. The result follows by secureness (**R.2**) and Lemma 4. ♣

Lemma 6. *Under P', $\mathbf{d}^1$ is a minimal sufficient statistic for $\mathbf{d}^2$ for player 1.*

Proof: Let $d^1, d'^1 \in \operatorname{supp} P'$, and assume that $P'(d^2|d^1) = P'(d^2|d'^1)$ for all $d^2 \in D^2$. Since $P' \ll P$, $d^1, d'^1 \in \operatorname{supp} P$. Now $P(d^2|d^1) = P'(d^2|d^1)$ (see the previous proof), and similarly $P(d^2|d'^1) = P'(d^2|d^1)$. Since $\mathbf{d}^1$ is a minimal sufficient statistic for $\mathbf{d}^2$ for player 1 under P, $d^1 = d'^1$. ♣

Proof of Proposition 1: For each $d^2 \in D^2$, consider the random variables $\boldsymbol{\rho}(d^2) = P(d^2|\mathbf{d}^1) = P(d^2|\mathscr{H}_\infty^1)$, $\boldsymbol{\rho}'(d^2) = P'(d^2|\mathbf{d}^1) = P'(d^2|\mathscr{H}_\infty^1)$ and $\boldsymbol{\rho}''(d^2) = P_{(\sigma_1^1,\sigma^2),\phi}(d^2|\mathbf{d}^1)$. Set $\boldsymbol{\rho} = (\boldsymbol{\rho}(d^2))_{d^2 \in D^2}$, $\boldsymbol{\rho}' = (\boldsymbol{\rho}'(d^2))_{d^2 \in D^2}$ and $\boldsymbol{\rho}'' = (\boldsymbol{\rho}''(d^2))_{d^2 \in D^2}$: $\boldsymbol{\rho}$, $\boldsymbol{\rho}'$ and $\boldsymbol{\rho}''$ are the standard experiments (see Blackwell [2]) characterizing the information of $\mathbf{h}_\infty^1$ on $\mathbf{d}^2$ under P, P' and $P_{(\sigma_1^1,\sigma^2),\phi}$ respectively. For any convex function g on $\Delta(D^2)$, $\mathbf{h}_\infty^1$ being less informative on $\mathbf{d}^2$ under P' than under P implies that $\int g d\boldsymbol{\rho} \geq \int g d\boldsymbol{\rho}'$ and similarly $\int g d\boldsymbol{\rho} \geq \int g d\boldsymbol{\rho}''$. On the other hand, $P = p.P' + (1-p).P_{(\sigma_1^1,\sigma^2),\phi}$ implies $\int g d\boldsymbol{\rho} \leq p.\int g d\boldsymbol{\rho}' + (1-p).\int g d\boldsymbol{\rho}''$. Therefore $\int g d\boldsymbol{\rho} = \int g d\boldsymbol{\rho}'$ for every g, which implies that $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ have the same distribution under P and P'. For $d^1 \in D^1$, define now $r(d^1)$ and $r'(d^1)$ in $\Delta(D^2)$ by $r(d^1)[d^2] = P(d^2|d^1)$ and $r'(d^1)[d^2] = P'(d^2|d^1)$. One has:

$$P'(d^1) = P'(\boldsymbol{\rho}' = r'(d^1)) = P(\boldsymbol{\rho} = r(d^1)) = P(d^1),$$

where the first and third equalities use minimality properties. Hence the marginals of P and P' on D^1 are equal. Since furthermore $P(d^2|d^1) = P'(d^2|d^1)$, the marginals of P and P' on $D = D^1 \times D^2$ are also equal. This proves the first claim.

To prove the second claim, fix $n \in N$ and $h_n^1 \in H_n^1$. Let τ_0^1 be the strategy defined as: play according to σ^1 until stage n, then follow σ_0^1 after histories compatible with h_n^1 and σ^1 after other histories. Let τ_1^1 be the strategy defined similarly by replacing σ_0^1 by σ_1^1. It is easily seen that $\sigma^1 = p \cdot \tau_0^1 + (1-p) \cdot \tau_1^1$. Hence by the first claim $\mu_{(\tau_1^1,\sigma^2),\phi}(d) = \mu(d)$ for every $d \in D$. This rewrites

$$P_\sigma(h_n^1) \times P_{(\sigma_0^1,\sigma^2),\phi}[d|h_n^1] + (1 - P_\sigma(h_n^1)) \times P_{(\sigma_0^1,\sigma^2),\phi}[d|H_n^1 - \{h_n^1\}]$$

$$= P_\sigma(h_n^1) \times P_{\sigma,\phi}[d|h_n^1] + (1 - P_\sigma(h_n^1)) \times P_{\sigma,\phi}[d|H_n^1 - \{h_n^1\}]$$

Hence $P_{(\sigma_0^1,\sigma^2),\phi}[d|h_n^1] = P_{\sigma,\phi}[d|h_n^1]$ whenever $P_\sigma(h_n^1) > 0$. This completes the second claim. ♣

4.2. Proof for infinitely many stages

4.2.1. Organization of the proof

We fix a secure protocol (σ, ϕ) generating a minimal information structure. Let $d^1 \in D^1$ be fixed throughout this section. For $h_n \in \mathscr{H}_n$, σ, ϕ and h_n induce a

probability $P_{\sigma,\phi}^{h_n}$ over $(\mathscr{H}_\infty \cap h_n) \times D$ (it corresponds to the probability induced by σ after history h_n). We write $\boldsymbol{\pi}_n^1 = P_{\sigma,\phi}^{h_n}(d^1)$. $\boldsymbol{\pi}_n^1$ is thus a function from $\{a,b,c,*\}^{n-1}$ to $[0,1]$ and for $h_n \in \operatorname{supp} P_\sigma$, $\boldsymbol{\pi}_n^1 = P_{\sigma,\phi}(d^1|h_n)$. We shall prove:

Proposition 2. *For every n, $\boldsymbol{\pi}_n^1$ is constant $P_{\sigma,\phi}$ almost surely.*

Before to proceed with the proof, we first show how to derive Theorem 1 from Proposition 2: The sequence $(\boldsymbol{\pi}_n^1)_n$ is an $(\mathscr{H}_n)$-martingale, that converges $P_{\sigma,\phi}$-a.s. to $P_{\sigma,\phi}[\mathbf{d}^1 = d^1 \mid \mathscr{H}_\infty^1]$. By Remark 3, the limit coincides with $\mathbf{1}_{\mathbf{d}^1=d^1}$, $P_{\sigma,\phi}$-a.s. By Proposition 2, $\boldsymbol{\pi}_n^1$ is a.s. constant, hence so is $\mathbf{1}_{\mathbf{d}^1=d^1}$. Thus, either $\mathbf{d}^1 = d^1$, $P_{\sigma,\phi}$-a.s., or $\mathbf{d}^1 \neq d^1$, $P_{\sigma,\phi}$-a.s. The support of μ^1 is thus a singleton, and the same argument applies for μ^2. ♣

Let us describe the organization of the proof.
By Proposition 1, one has

P.1 $E_{\tau^1,\sigma^2}[\boldsymbol{\pi}_n^1] = E_{\sigma^1,\sigma^2}[\boldsymbol{\pi}_n^1]$, as soon as the mixed strategy σ^1 puts a positive probability on τ^1.

For any strategy f_2 of player 2, consider the strategy τ^2 that coincides with f^2 up to stage n, and with σ^2 from stage $n+1$. Then, $P_{(\sigma^1,\tau^2),\phi}(\mathbf{d}^1 = d^1) = E_{\sigma^1,f^2}[\boldsymbol{\pi}_n^1]$. From **R.1**, one deduces:

P.2 For each f^2, $E_{\sigma^1,f^2}[\boldsymbol{\pi}_n^1] = E_{\sigma^1,\sigma^2}[\boldsymbol{\pi}_n^1]$.

Let $u^2 = (u_p^2)_p$ be any fully mixed strategy of player 2 (i.e. the distribution $u_p^2(h_p^2)$ has full support, for each $h_p^2 \in \mathscr{H}_p^2$). We prove in the next section that:

P.3 For P_{σ^1,u^2}-almost every sequence $h_n \in \{a,b,c,*\}^{n-1}$, one has $\boldsymbol{\pi}_n^1(h_n) = \boldsymbol{\pi}_n^1(\tilde{h}_n)$, where $\tilde{h}_n \in \{a,b,c,*\}^{n-1}$ is the sequence obtained from h_n by replacing each occurrence of c in the sequence by an a.

We shall prove that any function $p_n : \{a,b,c,*\}^{n-1} \to [0,1]$ that satisfies **P.1**, **P.2** and **P.3** is P_σ-a.s. constant. Observe that the three properties involve only the definition of $\sigma = (\sigma^1, \sigma^2)$ in the first $n-1$ stages of communication. Therefore we may focus on these stages. We call *strategy up to stage n* the specification σ^i of a strategy for the first $n-1$ stages of communication, that is of a sequence $(\sigma_p^i)_{p=1,\ldots,n}$, where $\sigma_p^i : (H_\infty, \mathscr{H}_p^i) \to \Delta(M^i)$. Observe that there are finitely many pure strategies up to stage n.

For a pair of strategies σ up to stage n, define the set of *histories consistent with* σ for player 1 as: $C_\sigma^1 = \{h_n, P_\sigma(\mathbf{h}_n^1(h_n)) > 0\}$.

Given that **P.1**, **P.2** and **P.3** hold, Proposition 2 is a consequence of Proposition 3 below.

Proposition 3. *Let (σ^1, σ^2) be strategies up to stage n. Let p_n be a function $\{a,b,c,*\}^{n-1}$ to $[0,1]$. Assume that **A.1**, **A.2** and **A.3** below hold:*

A.1 *For every $f^1 \in \operatorname{supp} \sigma^1$,*

$$E_{f^1,\sigma^2}[p_n] = E_{\sigma^1,\sigma^2}[p_n].$$

A.2 *For every strategy f^2 up to stage n,*

$$E_{\sigma^1,f^2}[p_n] = E_{\sigma^1,\sigma^2}[p_n].$$

A.3 *For P_{σ^1,u^2}-almost every sequence $h_n \in \{a,b,c,*\}^{n-1}$, one has $p_n(h_n) = p_n(\tilde{h}_n)$, where $\tilde{h}_n \in \{a,b,c,*\}^{n-1}$ is the sequence obtained from h_n by replacing each occurrence of c in the sequence by an a.*

Then p_n is constant on C^1_σ.

We prove in Section 4.2.2 that **P.3** holds. Next, we prove Proposition 3 in Section 4.2.3.

4.2.2. Informative deviations: c's become a's

The title of this section is best understood with the statement of Lemma 7. We sketch informally the argument used in this section. Assume that player 2, upon receiving the signal I^2 in stage 1 (*i.e.*, if the combination of messages is c) continues as if he had received N^2. In that case, the distribution of $\mathbf{d}^1$ is what it would have been, had the combination of messages been a. Since the distribution of $\mathbf{d}^1$ is invariant under deviations of player 2, one has $\boldsymbol{\pi}^1_1(c) = \boldsymbol{\pi}^1_1(a)$.

We extend the argument and show that if the signals to player 1 along two sequences h_n and $\tilde{h}_n$ are the same, $\boldsymbol{\pi}^1_n(h_n) = \boldsymbol{\pi}^1_n(\tilde{h}_n)$. This is the content of Lemma 7 below.

We follow standard notations and write $XcY \in \{a,b,c,*\}^n$ to denote the sequence obtained by concatenation of the sequence X, then c, then the sequence Y (where X and Y may be empty).

Recall that $\mathbf{h}^i_n(h_n)$ is the sequence of signals to player i along h_n (it is the value of the random variable $\mathbf{h}^i_n$ on the set h_n).

Let u^2 be a completely mixed strategy of player 2. For every n and $X_0aX_1a\cdots aX_k \in \{a,b,c,*\}^{n-1}$,

$$P_{\sigma^1,u^2}(X_0aX_1a\cdots aX_k) > 0 \Leftrightarrow P_{\sigma^1,u^2}(X_0cX_1c\cdots cX_k) > 0, \tag{7}$$

since $\mathbf{h}^1_n(X_0aX_1a\cdots aX_k) = \mathbf{h}^1_n(X_0cX_1c\cdots cX_k)$.

Lemma 7. *For any history $XcY \in \{a,b,c,*\}^{n-1}$ such that $P_{\sigma^1,u^2}(XcY) > 0$:*

$$\boldsymbol{\pi}^1_n(XaY) = \boldsymbol{\pi}^1_n(XcY) \tag{8}$$

Proof: We prove the result by induction over the number of b's in XcY. The proofs of the initial and induction steps are the same. Assume (8) holds for sequences containing less than kb's and let XcY be a sequence with exactly k b's. Write $X = X_0aX_1\cdots aX_l$, and $Y = Y_0aY_1\cdots aY_m$, where the X_p's and Y_q's contain *no* a's. For $p \in \{0,\ldots,l\}$, $q \in \{0,\ldots,m\}$, we let x^2_p and y^2_q denote the sequences of signals to player 2 along X_p and Y_q respectively.

Thus,

$$\mathbf{h}^2_n(XaY) = x^2_0N^2x^2_1\cdots N^2x^2_lN^2y^2_0N^2\cdots y^2_m,$$

and

$$\mathbf{h}_n^2(X_0 c X_1 \cdots c X_l c Y_0 c Y_1 \cdots c Y_m) = x_0^2 I^2 x_1^2 \cdots I^2 x_l^2 I^2 y_0^2 I^2 \cdots y_m^2.$$

We denote by h_n^2 the former, and by $\tilde{h}_n^2$ the latter.

For any sequence $h_n = \tilde{X}_0 c \tilde{X}_1 \cdots c \tilde{X}_l c \tilde{Y}_0 c \tilde{Y}_1 \cdots c \tilde{Y}_m$ such that $\mathbf{h}_n^2(h_n) = \tilde{h}_n^2$, we denote by $r(h_n)$ the sequence $\tilde{X}_0 a \tilde{X}_1 \cdots a \tilde{X}_l a \tilde{Y}_0 a \tilde{Y}_1 \cdots a \tilde{Y}_m$.

Since the distribution of $\mathbf{d}^1$ must remain unaffected if player 2 plays after $\tilde{h}_n^2$ *as if* he had received h_n^2, one has

$$\sum_{\mathbf{h}_n^2(h_n)=\tilde{h}_n^2} P_{\sigma^2,u^2}(h_n)\boldsymbol{\pi}_n^1(h_n) = \sum_{\mathbf{h}_n^2(h_n)=\tilde{h}_n^2} P_{\sigma^2,u^2}(h_n)\boldsymbol{\pi}_n^1(r(h_n))$$

or equivalently

$$\sum_{\mathbf{h}_n^2(h_n)=\tilde{h}_n^2} P_{\sigma^2,u^2}(h_n)[\boldsymbol{\pi}_n^1(h_n) - \boldsymbol{\pi}_n^1(r(h_n))] = 0 \tag{9}$$

For any such sequence h_n, either h_n contains strictly less than k b's, or $h_n = XcY$. In the first case, $\boldsymbol{\pi}_n^1(h_n) = \boldsymbol{\pi}_n^1(r(h_n))$ by the induction assumption.

Therefore, (9) implies

$$P_{\sigma^1,u^2}(XcY)[\boldsymbol{\pi}_n^1(XcY) - \boldsymbol{\pi}_n^1(XaY)] = 0. \quad \clubsuit$$

4.2.3. Proof of Proposition 3

The proof goes by induction over n. We shall drop the qualifier "up to stage n". For $n = 1$, there is nothing to prove. We assume that the result has been established for n, and consider a pair of strategies (up to stage $n+1$) (σ^1, σ^2) and p_{n+1} that satisfy the assumptions of the proposition.

Given $s^i \in \{I^i, N^i, *\}$, we denote by $\sigma^i(\cdot|s^i)$ the continuation strategy of σ^i given s^i. Formally, $\sigma_p^i(h_p^i|s^i) = \sigma_p^i((s^i, h_p^i))$ for $h_p^i \in H_p^i$.

For $s^i \in \{I^i, N^i, *\}$, we also denote by $\sigma^{3-i}(\cdot|s^i)$ the belief held by player $3-i$ on the continuation strategy of player i after stage 1. Thus,

$$\begin{cases} \sigma^i(\cdot|I^{3-i}) = \sigma^i(\cdot|N^i) \\ \sigma^i(\cdot|N^{3-i}) = P_\sigma(\mathbf{m}_1^i = N^i) \times \sigma^i(\cdot|N^i) + P_\sigma(\mathbf{m}_1^i = N^i) \times \sigma^i(\cdot|I^i) \end{cases}$$

The notation $\sigma^i(\cdot|*)$ is not ambiguous since $\sigma^i(\cdot \mid \mathbf{s}^1 = *) = \sigma^i(\cdot|\mathbf{s}^2 = *)$.

We prove that $p_{n+1}(h_{n+1})$ is constant over $C_\sigma^1 \cap \{\mathbf{s}_1^1 = *\}$, over $C_\sigma^1 \cap \{\mathbf{s}_1^1 = N^1\}$, and over $C_\sigma^1 \cap \{\mathbf{s}_1^1 = I^1\}$ in Steps 1, 2, and 3 respectively. We then conclude by showing in Step 4 that those constants are equal.

STEP 0:

Observe that $p_{n+1}(ch_n) = p_{n+1}(ah_n)$ whenever $ch_n \in \operatorname{supp} P_{\sigma^1,u^2}$.

STEP 1:

We argue here that $p_{n+1}(h_{n+1})$ is constant over $C^1_\sigma \cap \{s^1_1 = *\}$. Define $p_n(\cdot|*) : \{a, b, c, *\}^{n-1} \to [0, 1]$ by $p_n(h_n|*) = p_{n+1}(*h_n)$.

Lemma 8. *If, $P_\sigma(\mathbf{s}_1 = (*, *)) > 0$ then $\sigma^1(\cdot|*)$, $\sigma^2(\cdot|*)$ and $p_n(\cdot|*)$ satisfy **A.1**, **A.2** and **A.3**.*

Proof: We start with **A.3**. Let $XcY \in \operatorname{supp} P_{\sigma^1(\cdot|*),u^2}$ be a sequence of length $n-1$. Then $p_n(XcY|*) = p_{n+1}(*XcY) = p_{n+1}(*XaY)$ since $P_{\sigma^1,u^2}(*XcY) > 0$. Therefore, $p_n(XcY|*) = p_n(XaY|*)$.

We turn to **A.2**. Let f^2, $\bar{f}^2$, and $\tilde{f}^2$, be strategies up to stage n. Define strategies τ^2 and $\bar{\tau}^2$ up to stage $n+1$ by:

- play I^2 in stage 1;
- switch to f^2 (resp. $\bar{f}^2$) if $\mathbf{s}^2_1 = *$; to $\tilde{f}^2$ otherwise.

More explicitly $\tau^2(*\cdot) = f^2(\cdot)$, $\tau^2(I^2\cdot) = \tilde{f}^2(\cdot)$ and a similar definition holds for $\bar{\tau}^2$. Applying **A.2** to τ^2 and to $\bar{\tau}^2$ yields:

$$E_{\sigma^1,\tau^2}[p_{n+1}] = E_{\sigma^1,\bar{\tau}^2}[p_{n+1}].$$

This implies, since τ^2 and $\bar{\tau}^2$ coincide after I^1,

$$E_{\sigma^1(\cdot|*),f^2}[p_n(\cdot|*)] = E_{\sigma^1(\cdot|*),\bar{f}^2}[p_n(\cdot|*)],$$

hence **A.2** holds. A symmetric proof shows that **A.1** holds (except that $f^1, \tilde{f}^1$ should be taken in $\operatorname{supp}\sigma^2(\cdot|*)$). ♣

Corollary 1. *$p_{n+1}(h_{n+1})$ is constant over $C^1_\sigma \cap \{\mathbf{s}^1_1 = *\}$.*

Proof: If $P_\sigma(\mathbf{s}_1 = (*, *)) = 0$ there is nothing to prove. Otherwise, the induction hypothesis applied to $\sigma^1(\cdot|*)$, $\sigma^2(\cdot|*)$, and $p_n(\cdot|*)$ shows that p_{n+1} is constant over $\{*h_n, h_n \in C^1_{\sigma^1(\cdot|*),\sigma^2(\cdot|*)}\}$. But then, $C^1_\sigma \cap \{\mathbf{s}^1_1 = *\} = \{*h_n, h_n \in C^1_{\sigma^1(\cdot|*),\sigma^2(\cdot|*)}\}$. ♣

Let p^* be this value.

STEP 2:

We argue here that $p_{n+1}(h_{n+1})$ is constant over $C^1_\sigma \cap \{s^1_1 = N^1\}$. Define $p_n(\cdot|N^1) : \{a, b, c, *\}^{n-1} \to [0, 1]$ as

$$\begin{aligned} p_n(h_n|N^1) &= P_\sigma(\mathbf{m}^2_1 = N^2) \times p_{n+1}(ah_n) + P_\sigma(\mathbf{m}^2_1 = I^2) \times p_{n+1}(ch_n) \\ &= p_{n+1}(ch_n) \text{ by Step 0.} \end{aligned}$$

Lemma 9. *If $P_\sigma(\mathbf{s}^1_1 = N^1) > 0$, then $\sigma^1(\cdot|N^1), \sigma^2(\cdot|N^1)$ and $p_n(\cdot|N^1)$ satisfy **A.1**, **A.2** and **A.3**.*

Proof: The proof of **A.3** follows from the one in Lemma 8. We now prove **A.2**. Given strategies $f^2, \bar{f}^2$ and $\tilde{f}^2$ up to stage n, define τ^2 and $\bar{\tau}^2$ as:

- play I^2 in stage 1;
- switch to f^2 (resp. $\bar{f}^2$) if $\mathbf{s}_1^2 = I^2$; switch to $\tilde{f}^2$ otherwise.

A.2 applied to τ^2 and $\bar{\tau}^2$ yields

$$E_{\sigma^1,\tau^2}[p_{n+1}] = E_{\sigma^1,\bar{\tau}^2}[p_{n+1}],$$

and hence

$$E_{\sigma^1(\cdot|N^1),f^2}[p_{n+1}(c,\cdot)] = E_{\sigma^1(\cdot|N^1),\bar{f}^2}[p_{n+1}(c,\cdot)]. \tag{10}$$

From Step 0,

$$E_{\sigma^1(\cdot|N^1),f^2}[p_{n+1}(a,\cdot)] = E_{\sigma^1(\cdot|N^1),\bar{f}^2}[p_{n+1}(a,\cdot)]. \tag{11}$$

By a linear combination of (10) and (11),

$$E_{\sigma^1(\cdot|N^1),f^2}[p_n(\cdot|N^1)] = E_{\sigma^1(\cdot|N^1),\bar{f}^2}[p_n(\cdot|N^1)].$$

It remains to prove **A.1.** Given $f^1 \in \operatorname{supp}\sigma^1(\cdot|N^1)$, define τ^1 by:

- play N^1 in stage 1;
- switch to f^1 from stage 2 on.

Since τ^1 belong to supp σ^1, one has

$$E_{\tau^1,\sigma^2}[p_{n+1}] = E_{\sigma^1,\sigma^2}[p_{n+1}] \tag{12}$$

The left-hand side is also equal to

$$P_\sigma(\mathbf{m}_1^2 = N^2)E_{f^1,\sigma^2(\cdot|N^2)}[p_{n+1}(a,\cdot)] + P_\sigma(\mathbf{m}_1^2 = I^2)E_{f^1,\sigma^2(\cdot|I^2)}[p_{n+1}(c,\cdot)].$$

By Step 0, this is also equal to

$$\begin{aligned} &P_\sigma(\mathbf{m}_1^2 = N^2)E_{f^1,\sigma^2(\cdot|N^2)}[p_{n+1}(c,\cdot)] + P_\sigma(\mathbf{m}_1^2 = I^2)E_{f^1,\sigma^2(\cdot|I^2)}[p_{n+1}(c,\cdot)] \\ &\quad = E_{f^1,\sigma^2(\cdot|N^1)}[p_{n+1}(c,\cdot)] \\ &\quad = E_{f^1,\sigma^2(\cdot|N^1)}[p_n(\cdot|N^1)]. \end{aligned}$$

Hence $E_{f^1,\sigma^2(\cdot|N^1)}[p_n(\cdot|N^1)]$ does not depend on $f^1 \in \operatorname{supp}\sigma^1(\cdot|N^1)$. ♣

Corollary 2. *$p_{n+1}(h_{n+1})$ is constant over $C_\sigma^1 \cap \{\mathbf{s}_1^1 = N^1\}$.*

Proof: The case $P_\sigma(\mathbf{s}_1^1 = N^1) = 0$ is trivial. Otherwise, applying the induction hypothesis to $\sigma^1(\cdot|N^1), \sigma^2(\cdot|N^1)$ and $p_n(\cdot|N^1)$ shows that p_{n+1} is constant

on $\{ch_n, h_n \in C^1_{\sigma^1(\cdot|N^1),\sigma^2(\cdot|N^1)}\}$. By Step 0 it also takes the same value on $\{ah_n, h_n \in C^1_{\sigma^1(\cdot|N^1),\sigma^2(\cdot|N^1)}\}$. Finally, $C^1_\sigma \cap \{\mathbf{s}^1_1 = N^1\} = \{ah_n, h_n \in C^1_{\sigma^1(\cdot|N^1),\sigma^2(\cdot|N^1)}\} \cup \{ch_n, h_n \in C^1_{\sigma^1(\cdot|N^1),\sigma^2(\cdot|N^1)}\}$. ♣

Call p^a this value.

STEP 3:

We argue here that $p_{n+1}(h_{n+1})$ is constant over $C^1_\sigma \cap \{s^1_1 = I^1\}$. Define $p_n(\cdot|I^2) : \{a, b, c, *\}^{n-1} \to [0, 1]$ by

$$p_n(h_n|I^2) = p_{n+1}(bh_n).$$

Lemma 10. *If $P_\sigma(\mathbf{s}_1 = (I^1, N^2)) > 0$, then $\sigma^1(\cdot|I^1)$, $\sigma^2(\cdot|N^2)$ and $p_n(\cdot|I^2)$ satisfy **A.1**, **A.2** and **A.3**.*

Proof: The proof of **A.3** is a straightforward adaptation of the one in Lemma 8. We now prove **A.1**. Given $f^1, \bar{f}^1 \in \operatorname{supp}\sigma^1(\cdot|I^1)$ and $\tilde{f}^1 \in \operatorname{supp}\sigma^1(\cdot|*)$, define τ^1 and $\bar{\tau}^1$ as:

- play I^1 in stage 1;
- switch to f^1 (resp. $\bar{f}^1$) if $\mathbf{s}^1_1 = I^1$; switch to $\tilde{f}^1$ otherwise.

Then,

$$E_{\tau^1,\sigma^2}[p_{n+1}] = E_{\bar{\tau}^1,\sigma^2}[p_{n+1}]$$

implies

$$E_{f^1,\sigma^2(\cdot|N^2)}[p_{n+1}(b\cdot)] = E_{\bar{f}^1,\sigma^2(\cdot|N^2)}[p_{n+1}(b\cdot)]. \tag{13}$$

which is **A.1.**

We finally prove **A.2**. Given a strategy f^2 up to stage n, define τ^2 by:

- play N^2 in stage 1;
- switch to f^2 from stage 2 on.

By **A.2**, one has

$$E_{\sigma^1,\tau^2}[p_{n+1}] = E_{\sigma^1,\sigma^2}[p_{n+1}]. \tag{14}$$

The left-hand side is also equal to

$$P_\sigma(\mathbf{m}^1_1 = N^1)E_{\sigma^1(\cdot|N^1),f^2}[p_{n+1}(a\cdot)] + P_\sigma(\mathbf{m}^1_1 = I^1)E_{\sigma^1(\cdot|I^1),f^2}[p_{n+1}(b\cdot)].$$

By Step 2, this is also equal to

$$E_{\sigma^1,\tau^2}[p_{n+1}] = P_\sigma(\mathbf{m}^1_1 = N^1)p^a + P_\sigma(\mathbf{m}^1_1 = I^1)E_{\sigma^1(\cdot|I^1),f^2}[p_{n+1}(b\cdot)]$$

Hence, $E_{\sigma^1(\cdot|I^1),f^2}[p_{n+1}(b\cdot)]$ does not depend on f^2; **A.2** follows. ♣

Corollary 3. *$p_{n+1}(h_{n+1})$ is constant over $C^1_\sigma \cap \{s^1_1 = I^1\}$*

Proof: Assume $P_\sigma(\mathbf{s}_1 = (I^1, N^2)) > 0$, apply the induction hypothesis and remark that $C^1_\sigma \cap \{s^1_1 = N^1\} = \{bh_n, h_n \in C^1_{\sigma^1(\cdot|I^1),\sigma^2(\cdot|N^2)}\}$. ♣

We denote by p^b the common value.

STEP 4:

We argue here that $p_{n+1}(h_{n+1})$ is constant over C^1_σ. Assume first that σ^1 sends N^1 with probability one in the first stage. In that case, $C^1_\sigma = C^1_\sigma \cap \{\mathbf{s}^1_1 = N^1\}$ and p_{n+1} is constant and equal to p^a.

Now assume that σ^1 sends I^1 with positive probability in the first stage. Let τ^2 and $\bar{\tau}^2$ be the strategies that send respectively N^2 and I^2 in the first stage, and coincide with σ^2 afterwards. One has

$$E_{\sigma^1,\tau^2}[p_{n+1}] = P_\sigma(\mathbf{m}^1_1 = N^1) \times p^a + P_\sigma(\mathbf{m}^1_1 = I^1) \times p^b$$

and

$$E_{\sigma^1,\bar{\tau}^2}[p_{n+1}] = P_\sigma(\mathbf{m}^1_1 = N^1) \times p^a + P_\sigma(\mathbf{m}^1_1 = I^1) \times p^*.$$

Since $E_{\sigma^1,\tau^2}[p_{n+1}] = E_{\sigma^1,\bar{\tau}^2}[p_{n+1}]$, one gets $p^b = p^*$.

If σ^1 sends I^1 with probability one in the first stage, $C^1_\sigma = (C^1_\sigma \cap \{\mathbf{s}^1_1 = I^1\}) \cup (C^1_\sigma \cap \{\mathbf{s}^1_1 = *\})$ so that p_{n+1} is constant and equal to p^* on this set.

Finally, consider the case where σ^1 sends both messages N^1 and I^1 with positive probability in the first stage. Let τ^1 and $\bar{\tau}^1$ be the strategies that send respectively N^1 and I^1 in the first stage, and coincide with σ^1 afterwards. One has

$$E_{\tau^1,\sigma^2}[p_{n+1}] = p^a$$

and

$$E_{\bar{\tau}^1,\sigma^2}[p_{n+1}] = p^*.$$

Since $E_{\tau^1,\sigma^2}[p_{n+1}] = E_{\bar{\tau}^1,\sigma^2}[p_{n+1}]$, one gets $p^a = p^*$. ♣

References

[1] Bárány I (1992) Fair distribution protocols or how players replace fortune. Mathematics of Operations Research 17:327–340

[2] Blackwell D (1953) Equivalent comparison of experiments. Annals of Mathematical Statistics 24:265–272

[3] Forges F (1986) An approach to communication equilibria. Econometrica 54:1375–1385

[4] Forges F (1990) Universal mechanisms. Econometrica 58:1341–1364

[5] Gossner O (1996) Jeux répétés et mécanismes de communication. Thèse, Université Paris 6

[6] Gossner O (1998) Secure protocols-or how communication generates correlation. Journal of Economic Theory 83:69–89

[7] Lehrer E (1991) Internal correlation in repeated games. International Journal of Game Theory 19:431–456
[8] Lehrer E (1996) Mediated talk. International Journal of Game Theory 25:177–188
[9] Lehrer E, Sorin S (1997) One-shot public mediated talk. Games and Economic Behavior 20:131–148
[10] Linial N (1995) Games computers play: game-theoretic aspects of computing. In Handbook of Game Theory with Economic Applications, volume 2. Elsevier Science Publishers BV
[11] Vieille N (1994) Cheap talk with imperfect monitoring. mimeo