Repeated communication through the mechanism *and*

Olivier Gossner* Nicolas Vieille†

October 21, 1998

Abstract

We consider the "and" communication mechanism that inputs messages 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 through finite or infinite repetition of this mechanism.

*CORE, Voie du Roman Pays, 34, Université Catholique de Louvain, Belgium and THEMA, Université Paris X-Nanterre, 200 avenue de la République, 92001 Nanterre, France

†CEREMADE, Université Paris IX-Dauphine, Place de Lattre de Tassigny, 75775 Paris 16, France

1 Introduction

Assume that two players communicate repeatedly through some mechanism (or channel) M, sending messages to and receiving signals from M, for an infinite number of stages, and finally choose decisions $\mathbf{d}^1$ and $\mathbf{d}^2$ from sets D^1 and D^2, based upon the sequence of signals received. The σ-algebras $\mathcal{H}_\infty^1$ and $\mathcal{H}_\infty^2$ which represent the informations held by the players at the end of the communication phase, are in general not comparable, hence the decisions are correlated.

For which distributions μ over $D = D^1 \times D^2$ is it possible to design communication strategies (*i.e.*, specifications of which messages to send as a function of previously received signals) and decision rules, such that

(i) the law of $(\mathbf{d}^1, \mathbf{d}^2)$ is μ,

(ii) each player knows only his decision prior to the decision stage, and

(iii) the whole procedure can not be manipulated by either player?

This question is related to issues in computer science and in game theory. 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 exchange messages without being eavesdropped. We refer to Linial [9] for references and an extensive discussion of the links between game theory and computer science. Similar questions were addressed in game theory (see Bárányi [1], Forges [4] ,[5]). A somewhat dual problem is solved in [3]: given μ, one tries to design a (simple) mechanism M, with which the players can generate μ in the above sense. The closest to our work is Lehrer [8] who studies the correlation opportunities offered by the *and*-protocol (see below). However, his focus is quite different, and the robustness requirements are much weaker than ours.

We study here a benchmark 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, taken from $\{0,1\}$, 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 $(y, and(x,y))$. The crucial feature of this mechanism is that when player 1 sends $x = 0$ to the 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 ($and(1,y)=y$).

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. Parts of the proofs below may be found in [6], [10].

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 rounds of communication are allowed. Section 3 deals with the general case, and is independent of section 2. Although the result of section 2 is encompassed in section 3, its proof is both 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 $\mathcal{P}^1 = \{\{a,c\},\{b\},\{*\}\}$. 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 $\mathcal{P}^1$ contains m. For simplicity, we sometimes write $\mathcal{P}^1 = \{N^1, I^1, *\}$. The information partition $\mathcal{P}^2$ of player 2 is defined symmetrically.

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 $\mathcal{H}_n^i$ the information available to player i in stage n, prior to sending a message: it is the sub σ-algebra of $\mathcal{H}_\infty^i$ over H_∞ generated by cylinder sets of the form $h_n^i \times H_\infty$, where $h_n^i \in (\mathcal{P}^i)^n$ is a sequence of $n-1$ elements of $\{N^i, I^i, *\}$.

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 $(H_\infty, \mathcal{H}_n^i)$ to M^i (*resp.* $\Delta(M^i)$): such a map specifies which message to send in round n, as a function of the signals received so far. A pure (*resp.* behavioural) 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 $\mathcal{S}^i$ the Borel σ-algebra on S^i. A mixed strategy of player i is a probability distribution over $(S^i, \mathcal{S}^i)$. 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 $(H_\infty^i, \mathcal{H}_\infty^i)$ 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), $P_{\sigma,\phi}$ represents the probability distribution induced by σ and ϕ on $(H_\infty \times D, \mathcal{H}_\infty \otimes 2^D)$ 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 $(H_\infty, \mathcal{H}_\infty)$. 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-stages version, the decision rule ϕ_n^i is taken as $\mathcal{H}_N^i$ 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 $\mathcal{H}_n^i$), $\mathbf{d}^i$ 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 $\mathcal{H}_n^i$, and use similar shortcuts when convenient.

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* $P_{\sigma,\phi}$*.*

Similar conditions hold for player 2.

The notion of less informative refers to Blackwell's (1953,[2]) 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. A consequence of **R**.2 is that $\mathbf{d}^1$ is a sufficient statistic for $\mathbf{d}^2$ for player 1 under $P_{\sigma,\phi}$ (*i.e.*, $P_{\sigma,\phi}(\mathbf{d}^2 = \cdot|\mathbf{d}^1) = P_{\sigma,\phi}(\mathbf{d}^2 = \cdot|\mathcal{H}^1_\infty)$, $P_{\sigma,\phi}$-a.s.).

This definition is motivated by the following property (Gossner [7]). A protocol is secure if and only if for every strategic form game G:

- for every Nash equilibrium f of the game in which $d \in D$ is drawn according to μ, player i is informed of the coordinate $\mathbf{d}^i$, then plays in G

- it is a Nash equilibrium of the game in which players communicate through the mechanism, then play in G

- to 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).

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 straighforward 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.

3 Finitely many stages

3.1 Reduction to minimal information structures

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

- For any $d^1_0, d^1_1 \in \text{supp}\mu^1$, the conditional probabilities $\mu(\cdot|d^1_0)$ and $\mu(\cdot|d^1_1)$ on D^2 differ.

- A similar 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 Dirac masses.

Remark 2: It is proven in [7] that Theorem 1 follows if we only prove that *minimal* secure information structures are Dirac masses.

Remark 3: Let (σ, ϕ) be a secure protocol which generates μ. Then, $P_{\sigma,\phi}$-a.s., for every $d^i \in \text{supp}\phi^i(\mathbf{h}^i_\infty)$, $P_{\sigma,\phi}(\mathbf{d}^{3-i} = \cdot | d^i) = P_{\sigma,\phi}(\mathbf{d}^{3-i} = \cdot | \mathbf{h}^i_\infty)$. Therefore, if μ is minimal, $\phi^i(\mathbf{h}^i_\infty)$ is a Dirac mass, $P_{\sigma,\phi}$-a.s.

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 view μ as a $D^1 \times D^2$-matrix. As noted in the previous section, we may assume that, P_σ-a.s., $\phi^i(\mathbf{h}^i_\infty)$ 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.

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 it might be random).

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, he will *know* at stage n the belief held by player 2.

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.*

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

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

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

Let $\mathbf{p}_n^2 = P_{\sigma,\phi}[\cdot|\mathcal{H}_n^2]$ be the posterior belief on $\mathcal{H}_n^1$ given $\mathcal{H}_n^2$. Notice that $\mathbf{p}_1^2$ is a constant ($\mathcal{H}_1^2$ 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 first $n-1$ first coordinates of (σ_+^1, σ^2)). Denote by $\tilde{\mathbf{p}}_n^2$ an $\mathcal{H}_n^1$-measurable version of $\mathbf{p}_n^2$. We set

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

Claim: player 1 knows $\mathbf{p}_{n+1}^2$ at stage $n+1$ under $P_{\sigma_+^1,\sigma^2}$.

Proof: let $h_{n+1}^1 \in \mathcal{H}_{n+1}^1$ in the support of $P_{\sigma_+^1,\sigma^2}$. We need to prove that $\mathbf{p}_{n+1}^2$ is constant over $C_{n+1}^2(h_{n+1}^1) \cap \text{supp}P_{\sigma_+^1,\sigma^2}$. 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 $h_{n+1}^2 = (h_n^2, s_n^2) \in C_{n+1}^1(h_{n+1}^1) \cap \text{supp}P_{\sigma_+^1,\sigma^2}$. We distinguish three cases.

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

By construction and the induction hypothesis, one has

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

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

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

Case 2: $s^1_n = I^1$.

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

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

Case 3: $s^1_n = *$.

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

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

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 $\mathcal{H}^1_N$, 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, $\mathbf{h}^1_N$ 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 $d^1 \in \text{supp}\mu^1$, $d^2 \in D^2$, $P(d^2|d^1)$ 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 and columns containing only 0's.

Step 2: a least informative strategy

Clearly, the least informative way of communicating 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, $\sigma^1_-(h^1_n) = N^1$ if $\sigma^1(h^1_n)[N^1] > 0$, and $\sigma^1_-(h^1_n) = I^1$ otherwise. It is clear that $P_{\sigma^1_-, \sigma^2} << P_\sigma$ (absolutely continuous). We set $S = \text{supp}P_{\sigma^1_-, \sigma^2}$. We prove in Lemma 2 that $\mathbf{d}^1$ is constant on S. Since $S \subseteq \text{supp}P_\sigma$ 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 $d \in D$, and 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 signal 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 $P_\sigma[\mathbf{d}^1 = \cdot | \mathcal{H}_n^1]$ is constant, $P_{\sigma_-^1, \sigma^2}$-a.s. There is nothing to prove for $n = 1$ since $\mathcal{H}_1^1$ is trivial; we assume this is true for some n. We shall prove that

$$P_\sigma[\mathbf{d}^1 = \cdot | \mathcal{H}_{n+1}^1] = P_\sigma[\mathbf{d}^1 = \cdot | \mathcal{H}_n^1], \tag{1}$$

$P_{\sigma_-^1, \sigma^2}$-a.s.

Fix $h_n^1 = (s_1^1, \ldots, s_{n-1}^1) \in \mathcal{H}_n^1$ 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 $P_{\sigma_-^1, \sigma^2}[\mathbf{m}_n^2 = I^2 | h_n^1] \in]0, 1[$. In that case h_{n+1}^1 may either be (h_n^1, I^1) or $(h_n^1, *)$. We need to prove that

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

Define a strategy σ_+^2 for the first $n-1$ stages as: play N^2 in stage $p \leq n-1$ if $s_p^1 = I^1$, and I^2 otherwise. Define $h_n^2 = (s_1^2, \ldots, s_{n-1}^2)$ by

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

By construction of S, $P_{\sigma^1, \sigma_+^2}(h_n^2) > 0$ and $P_{\sigma^1, \sigma_+^2}(h_n^1 | h_n^2) = 1$.

Based upon σ_+^2, we define *two* strategies $\tilde{\sigma}_+^2$ and $\overline{\sigma}_+^2$ 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 $\mathbf{h}^2_n \neq h^2_n$;

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

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

1. same as 1 for $\tilde{\sigma}^2_+$;

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

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

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

therefore

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

By construction,

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

and

$$P_{\sigma^1,\overline{\sigma}^2_+}[\mathbf{d}^1 = d^1|h^2_n] = P_\sigma[\mathbf{d}^1 = d^1|h^1_n, *].$$

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

Finally, remark that $P_{\sigma^1_-,\sigma^2}[\mathbf{d}^1 = \cdot|\mathcal{H}^1_N] = 1_{\mathbf{d}^1=\cdot}$, $P_{\sigma^1_-,\sigma^2}$-a.s., since $\mathbf{d}^1$ has a $\mathcal{H}^1_N$-measurable version. 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 3 *Assume (σ, ϕ) is a secure protocol generating the minimal information structure μ, and $\sigma^1 = p\sigma_0^1 + (1-p)\sigma_1^1$ with $0 < p \leq 1$. Then $\mu_{(\sigma_0^1, \sigma^2), \phi} = \mu$.*

In this statement, σ^1 is interpreted as a *mixed* strategy, and $\sigma^1 = p\sigma_0^1 + (1-p)\sigma_1^1$ 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). For simplicity of notations let $P = P_{\sigma,\phi}$ and $P' = P_{\left(\sigma_0^1, \sigma^2\right), \phi}$, so that $P' << P$. The proof of Proposition 3 is postponed to the end of the section.

Lemma 4 *For $h_n \in H_n$, $P'(h_n |\ \mathcal{H}_n^1) = P(h_n |\ \mathcal{H}_n^1)$ $\quad P'$ almost surely.*

Shortly, $P'(\cdot|\mathcal{H}_n^1) = P(\cdot|\mathcal{H}_n^1)$, 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 $h_n^i = \mathbf{h}_n^i(h_n)$ be the sequence of signals received by player i along h_n, and $(m_1^i, \ldots, m_{n-1}^i)$ the messages sent by player i along h_n^i. 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 $S'(h_n^1) = \prod \sigma_{0,t}^1(h_t^1)[m_t^1]$ 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 $\mathcal{H}_n^2$ 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:

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

♣

Lemma 5 *For $d^2 \in D^2$, $P(\mathbf{d}^2 = d^2|\mathcal{H}_\infty^1) = P'(\mathbf{d}^2 = d^2|\mathcal{H}_\infty^1)$ $\quad P'$ almost surely.*

Proof: Lemma 4 shows that for any $h_m \in H_m$ and $n \geq m$, $P(h_m|\mathcal{H}_n^1) = P'(h_m|\mathcal{H}_n^1)$ P'-a.s.. The left side is a $(P, (\mathcal{H}_n)_n)$ martingale converging to $P(h_m|\mathcal{H}_\infty^1)$ P-a.s. while the right side is a $(P', (\mathcal{H}_n)_n)$ martingale converging to $P'(h_m|\mathcal{H}_\infty^1)$ P'-a.s.. Since $P' << P$, $P(h_m|\mathcal{H}_\infty^1) = P'(h_m|\mathcal{H}_\infty^1)$ P'-a.s.. Since $\mathcal{H}_\infty$ is generated by the countable family of events $\{\mathbf{h}_m = h_m\}$, $P(A|\mathcal{H}_\infty^1) = P'(A|\mathcal{H}_\infty^1)$ P'-a.s. for any $A \in \mathcal{H}_\infty$. Since $\mathbf{d}^2$ has a $\mathcal{H}_\infty$–measurable version under P', this completes the proof.♣

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

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

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

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 5. ♣

Lemma 7 *Under P', $\mathbf{d}^1$ is a minimal sufficient statistic for $\mathbf{d}^2$ for player 1.*

Proof: Let $d^1, d'^1 \in \text{supp}P'$, and assume that $P'(d^2|d^1) = P'(d^2|d'^1)$ for all $d^2 \in D^2$. Since $P' << P$, $d^1, d'^1 \in \text{supp}P$. 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 3: By **R**.2, $\mathbf{h}^1_\infty$ is less informative on $\mathbf{d}^2$ both under $P' = P_{(\sigma^1_0,\sigma^2),\phi}$ and under $P_{(\sigma^1_1,\sigma^2),\phi}$ than $\mathbf{d}^1$ under $P = pP_{(\sigma^1_0,\sigma^2),\phi} + (1-p)$ $P_{(\sigma^1_1,\sigma^2),\phi}$. Therefore $\mathbf{h}^1_\infty$ is equally informative on $\mathbf{d}^2$ under P and under P'.

For each $d^2 \in D^2$, consider the random variables $\boldsymbol{\rho}(d^2) = P(d^2|\mathbf{d}^1) = P(d^2|\mathcal{H}^1_\infty)$ and $\boldsymbol{\rho}'(d^2) = P'(d^2|\mathbf{d}^1) = P'(d^2|\mathcal{H}^1_\infty)$. Set $\boldsymbol{\rho} = (\boldsymbol{\rho}(d^2))_{d^2 \in D^2}$ and $\boldsymbol{\rho}' = (\boldsymbol{\rho}'(d^2))_{d^2 \in D^2}$. $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ are the standard experiments (see Blackwell [2]) characterizing the information of $\mathbf{h}^1_\infty$ on $\mathbf{d}^2$ under P and P' respectively. Since $\mathbf{h}^1_\infty$ is equally informative under P and P', the random vectors $\boldsymbol{\rho}$ 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.♣

4.2 Proof for infinitely many stages

We fix a secure protocol (σ, ϕ) generating a minimal information structure, and write $\boldsymbol{\pi}_n^1 = P_{\sigma,\phi}(d^1|\mathcal{H}_n)$, where d^1 is fixed. We shall prove:

Proposition 8 *For every n, $\boldsymbol{\pi}_n^1$ is constant $P_{\sigma,\phi}$ almost surely.*

We first show how to derive Theorem 1 from Proposition 8. One has $\lim_{n\to\infty} \boldsymbol{\pi}_n^1 = \mathbf{1}_{\mathbf{d}^1=d^1}$, $P_{\sigma,\phi}$-a.s. From Proposition 8, one derives the existence of $d^1 \in D^1$ sucg that $d^1 = d^1$ $P_{\sigma,\phi}$-a.s.. The support of μ^1 is thus a singleton, and the same argument applies for μ^2.♣

We shall prove Proposition 8 using first an informative deviation of player 2, then deviations "in probabilities" of players 1 and 2.

4.2.1 Informative deviations: c's become a's

The title of this section is best understood with the statement of Lemma 9. 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, $\boldsymbol{\pi}_n^1(h_n) = \boldsymbol{\pi}_n^1(\tilde{h}_n)$.

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

For emphasis, we denote by $\mathbf{h}_n^i(h_n)$ the sequence of signals to player i along h_n (it is the value of the r.v. $\mathbf{h}_n^i$ on the set h_n).

Let u^2 be a completely mixed strategy of player 2: by this, we mean that $u_p^2(h_p^2)$ has full support for every p and h_p^2.

This implies that, for every n and $X_0 a X_1 a \cdots a X_k \in \{a, b, c, *\}^{n-1}$,

$$P_{\sigma^1,u^2}(X_0 a X_1 a \cdots a X_k) > 0 \Leftrightarrow P_{\sigma^1,u^2}(X_0 c X_1 c \cdots c X_k) > 0, \tag{4}$$

since $\mathbf{h}_n^1(X_0 a X_1 a \cdots a X_k) = \mathbf{h}_n^1(X_0 c X_1 c \cdots c X_k)$.

Lemma 9 *For any history $XcY \in \{a, b, c, *\}^{n-1}$ such that $P_{\sigma^1,u^2}(XcY) > 0$:*

$$\boldsymbol{\pi}_n^1(XaY) = \boldsymbol{\pi}_n^1(XcY) \tag{5}$$

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 (5) holds for sequences with less than k b's and let XcY be a sequence with exactly k b's. Write X as $X_0aX_1\cdots aX_l$, $Y = Y_0aY_1\cdots aY_m$, 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_p^2 and y_q^2 denote the sequences of signals to player 2 along X_p and Y_q respectively.

Thus,

$$\mathbf{h}_n^2(XaY) = x_0^2N^2x_1^2\cdots N^2x_l^2N^2y_0^2N^2\cdots y_m^2,$$

and

$$\mathbf{h}_n^2(X_0cX_1\cdots cX_lcY_0cY_1\cdots cY_m) = x_0^2I^2x_1^2\cdots I^2x_l^2I^2y_0^2I^2\cdots y_m^2.$$

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

For any sequence $h_n = \tilde{X}_0c\tilde{X}_1\cdots c\tilde{X}_lc\tilde{Y}_0c\tilde{Y}_1\cdots c\tilde{Y}_m$ such that $\mathbf{h}_n^2(h_n) = \tilde{h}_n^2$, we denote by $r(h_n)$ the sequence $\tilde{X}_0a\tilde{X}_1\cdots a\tilde{X}_la\tilde{Y}_0a\tilde{Y}_1\cdots a\tilde{Y}_m$. 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

$$\sum_{\mathbf{h}_n^2(h_n)=\tilde{h}_n^2} P_{\sigma^2,u^2}(h_n)[\boldsymbol{\pi}_n^1(h_n) - \boldsymbol{\pi}_n^1(r(h_n))] = 0 \tag{6}$$

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, (6) yields

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

♣

4.3 Deviations in probabilities

For every $n \in I\!N$, and any pair (f^1, f^2) of pure strategies, we denote by $M_n(f^1, f^2) \in \{a, b, c, *\}^{n-1}$ the induced sequence of message pairs up to stage n.

We say that two pure strategies f^1 and $\overline{f}^1$ are n-equivalent if $M_n(f^1, f^2) = M_n(\overline{f}^1, f^2)$ for every f^2. For simplicity, we call an equivalence class of n-equivalent pure strategies a *pure strategy up to stage* n.

Therefore a pure strategy f^i up to stage $n+1$ can be described as (N^i, f^i_N) or $(I^i, (f^i_I, f^i_*))$ where the first coordinate is the message sent in stage 1, and the second one is the *continuation* strategy: f^i_N, f^i_I, f^i_* are pure strategies of player i up to stage n. We denote by v_n the number of strategies up to stage n: it is determined by $v_1 = 2$ and the induction formula $v_{n+1} = v_n^2 + v_n$.

This enables us to view M_n as a square matrix of size v_n with entries in $\{a, b, c, *\}^{n-1}$.

The relations between M_n and M_{n+1} are summarized in the next self-explanatory array:

$$M_{n+1} = \begin{array}{c} \\ N^1, f^1_N \\ I^1, (f^1_I, f^1_*) \end{array} \begin{array}{c} \begin{array}{cc} N^2, f^2_N & I^2, (f^2_I, f^2_*) \end{array} \\ \begin{pmatrix} aM_n(f^1_N, f^2_N) & cM_n(f^1_N, f^2_I) \\ bM_n(f^1_I, f^2_N) & *M_n(f^1_*, f^2_*) \end{pmatrix} \end{array}$$

Given $\boldsymbol{\pi} : \{a, b, c, *\}^{n-1} \to I\!R$, we denote by $< \boldsymbol{\pi}, M_n >$ the matrix obtained by replacing entry e of M_n by $\boldsymbol{\pi}(e)$.

A mixed strategy of player 1 up to stage n is identified to a vector in $\mathcal{M}_{v_n,1}$ (row matrices of size v_n) with nonnegative components which sum up to 1. The corresponding set is denoted by S^1_n. The subset S^2_n of $\mathcal{M}_{1,v_n}$ of mixed strategies of player 2 is defined similarly.

Given $\tau^i_n \in S^i_n$, τ^i denotes the strategy which plays according to τ^i_n up to stage n, and then to σ^i. More formally, τ^i first selects a n -equivalence class of pure strategies using τ^i_n, plays according this class up to stage n, and coincides afterwards with the behavioral strategy σ^i.

Also, we denote by σ^i_n the distribution induced by the mixed strategy σ^i over the set of pure strategies up to stage n.

Note that this notation is at variance with earlier notations, where σ^i_n denoted the behavior in stage n. For simplicity, we abbreviate $(\sigma^i_n)_p(h^i_p)$ to $\sigma^i_n(h^i_p)$.

By construction, one has

$$P_{(\tau^1,\tau^2),\phi}(d^1) = \tau^1_n < \boldsymbol{\pi}^1_n, M_n > \tau^2_n. \tag{7}$$

Since (σ, ϕ) is a secure protocol, one has therefore, for all $\tau^2_n \in S^2_n$,

$$\sigma^1_n < \boldsymbol{\pi}^1_n, M_n > \tau^2_n = \sigma^1_n < \boldsymbol{\pi}^1_n, M_n > \sigma^2_n.$$

On the other hand, let $f_n^1 \in \text{supp}\sigma_n^1$, and consider the strategy f^1 as defined above. In terms of mixed strategies, it is clear that $\sigma^1 = \sigma_n^1(f_n^1) + (1 - \sigma^1(f_n^1))\sigma_1^1$, for some σ_1^1, where $\sigma_n^1(f_n^1)$ is the probability assigned to (the equivalence class) f_n^1 by σ_n^1. Thus, by Proposition 3,

$$f_n^1 < \boldsymbol{\pi}_n^1, M_n > \sigma_n^2 = f_n^1 < \boldsymbol{\pi}_n^1, M_n > \sigma_n^2,$$

for any f_n^1 in the support of σ_n^1.

Therefore, $\sigma_n^1 < \boldsymbol{\pi}_n^1, M_n >$ is a constant lign vector and $< \boldsymbol{\pi}_n^1, M_n > \sigma_n^2$ is a column vector which is constant on the support of σ_n^1.

Proposition 8 follows from the next Lemma:

Lemma 10 *Let $n \in \mathbb{N}$, $(\sigma_n^1, \sigma_n^2) \in S_n^1 \times S_n^2$, and $p_n : \{a, b, c, *\}^n \to \mathbb{R}$. Assume that:*

(a) *$p_n(XaY) = p_n(XcY)$ for every $XaY \in \text{supp}P_{\sigma_n^1, u_n^2}$.*

(b) *$\sigma_n^1 < p_n, M_n >$ is a constant vector*

(c) *$< p_n, M_n > \sigma_n^2$ is a constant vector on the support of σ_n^1.*

then p_n is constant on the support of $P_{\sigma_n^1, u_n^2}$.

Recall that u_n^2 is the probability distribution on S^2 induced by the completely mixed strategy u^2. We prove Lemma 10 by induction on n.

Proof: First assume $n = 1$. If $\sigma_1^1(\emptyset)[N^1] = 1$ condition (a) implies the result. If $\sigma_1^1(\emptyset)[I^1] = 1$ condition (b) implies the result. If $0 < \sigma_1^1(\emptyset)[I^1] < 1$, first (a) implies $p_1(c) = p_1(a)$, then (b) implies $p_1(b) = p_1(*)$, and finally (c) implies $p_1(*) = p_1(a)$.

Assume that the lemma holds for some n. We discuss only the case $0 < \sigma_{n+1}^1(\emptyset)[I^1] < 1$ and $0 < \sigma_{n+1}^2(\emptyset)[N^2] < 1$, since other cases can be dealt with in a similar way. Denote by Z_{n+1} the matrix $< p_{n+1}, M_{n+1} >$ from which all rows that have zero probability under σ_{n+1}^1 have been deleted. We need to prove that Z_{n+1} is constant. Given a square matrix M of size v_{n+1}, we let M_+ be the matrix M from which all lines with zero probability under σ_{n+1}^1 have been deleted. Note that Z_{n+1} is of the form:

$$Z_{n+1} = \begin{pmatrix} < p_{n+1}, aM_n(.,.) > & < p_{n+1}, cM_n(.,.) > \\ < p_{n+1}, bM_n(.,.) > & < p_{n+1}, *M_n(.,.) > \end{pmatrix}_+$$

The induction proof is divided in 4 steps, of which Step 1 and Step 2 are independent.
STEP 1: From (a), Z_{n+1} writes:

$$Z_{n+1} = \begin{pmatrix} < p_{n+1}, aM_n(.,.) > & < p_{n+1}, aM_n(.,.) > \\ < p_{n+1}, bM_n(.,.) > & < p_{n+1}, *M_n(.,.) > \end{pmatrix}_+$$

(the top two submatrices of Z_{n+1} are identical for rows in the support of σ^1_{n+1}, given (4) and Lemma 9).
STEP 2: Define σ^1_n, σ^2_n and p_n by:

- $p_n(h_n) = p_{n+1}(*h_n)$
- $\sigma^1_n(h^1_p) = \sigma^1_{n+1}(*h^1_p)$, $p \leq n$
- $\sigma^2_n(h^2_p) = \sigma^2_{n+1}(*h^2_p)$, $p \leq n$.

p_n, σ^1_n, σ^2_n should be interpreted as the play until stage $n+1$, conditional on the *common knowledge* fact that $*$ was played in the first stage.

Properties (a) (b) and (c) for $\sigma^1_{n+1}, \sigma^2_{n+1}$ and p_{n+1} imply properties (a) (b) and (c) respectively for σ^1_n, σ^2_n and p_n. Hence the induction assumption implies the existence of $p^* \in I\!R$ such that $p_{n+1}(*h_n) = p^*$ for any $*h_n \in \text{supp}P_{\sigma^1_{n+1}, u^2_{n+1}}$. Therefore, letting E_n denote the square matrix of size v_n with all entries equal to 1, Z_{n+1} writes:

$$Z_{n+1} = \begin{pmatrix} < p_{n+1}, aM_n(.,.) > & < p_{n+1}, aM_n(.,.) > \\ < p_{n+1}, bM_n(.,.) > & p^*E_n \end{pmatrix}_+$$

STEP 3: Next, consider σ^1_n, σ^2_n and p_n defined by:

- $p_n(h_n) = p_{n+1}(ch_n)$
- $\sigma^1_n(h^1_n) = \sigma^1_{n+1}(N^1 h^1_n)$
- $\sigma^2_n(h^2_n) = \sigma^2_{n+1}(I^2 h^2_n)$

These can be seen as continuation strategies conditional to the fact that N^1 and I^2 have been played in the first round. Property (a) goes from $\sigma^1_{n+1}, \sigma^2_{n+1}$ and p_{n+1} to σ^1_n, σ^2_n and p_n. Property (b) for σ^1_n and p_n is implied by STEP 1 and by (b) for σ^1_{n+1} and p_{n+1}. Property (c) for σ^2_n and p_n is

implied by STEP 2 and (c) for σ^2_{n+1} and p_{n+1}. The induction assumption therefore implies the existence of $p^c \in I\!R$ such that $p_{n+1}(h_{n+1}) = p^c$ for any $h_{n+1} = ch_n$ in $\text{supp}P_{\sigma^1_{n+1},u^2_{n+1}}$. By (a), $p_{n+1}(h_{n+1}) = p^c$ for any $h_{n+1} = ah_n$ in $\text{supp}P_{\sigma^1_{n+1},u^2_{n+1}}$. Thus,

$$Z_{n+1} = \begin{pmatrix} p^c E_n & p^c E_n \\ < p_{n+1}, bM_n(.,.) > & p^* E_n \end{pmatrix}_+$$

STEP 4: Applying the same reasoning to:

- $p_n(h_n) = p_{n+1}(bh_n)$
- $\sigma^1_n(h^1_n) = \sigma^1_{n+1}(I^1 h^1_n)$
- $\sigma^2_n(h^2_n) = \sigma^2_{n+1}(N^2 h^2_n)$

shows the existence of p^b with $p_{n+1}(bh_n) = p^b$ for any $bh_n \in \text{supp}P_{\sigma^1_{n+1},u^2_{n+1}}$. Hence,

$$Z_{n+1} = \begin{pmatrix} p^c E_n & p^c E_n \\ p^b E_n & p^* E_n \end{pmatrix}_+$$

STEP 5: To conclude, (b) implies $p^b = p^*$, and finally (c) implies $p^* = p^a$.♣

References

[1] I. Bárányi. Fair distribution protocols or how players replace fortune. *Mathematics of Operations Research*, 17:327–340, 1992.

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

[3] Lehrer E. and S. Sorin. One-shot public mediated talk. *Games and Economic Behavior*, 20:131–148, 1997.

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

[5] F. Forges. Universal mechanisms. *Econometrica*, 58:1341–1364, 1990.

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

[7] O. Gossner. Secure protocols-or how communication generates correlation. *Core D.P 9792*, 1997. to appear in Journal of Economic Theory.

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

[9] N. Linial. Games computers play: game-theoretic aspects of computing. In *Handbook of Game Theory with Economic Applications*, volume 2. Elsevier Science Publishers B.V., 1995.

[10] N. Vieille. Cheap talk with imperfect monitoring. mimeo, 1994.