THEMA

théorie économique,
modélisation et applications

THEMA Working Paper n°2025-04
CY Cergy Paris Université, France

A Byzantine Agreement Protocol for Game Theorists

Helmuts Azacis, Péter Vida

February 2025

A Byzantine Agreement Protocol for Game Theorists[*]

Helmuts Āzacis[†]and Péter Vida[‡]

February 21, 2025

Abstract

We introduce a new Byzantine agreement protocol consisting of two stages of private communication which substitutes public communication (broadcasting to all the players) in a very strong sense. At every information set, players hold the following consistent beliefs (Kreps and Wilson (1982)): every player believes, no matter what messages she has sent or received, that the bitwise-majority message of every player is the same. We provide applications of our result.

Keywords: Byzantine agreement, broadcasting, public communication, consistent beliefs

JEL Classification: C72; D82.

[*] We thank Dino Gerardi, Françoise Forges, and Marie Laclau. All remaining errors are ours.

[†] Cardiff Business School, Cardiff University, Cardiff, UK and Corvinus University of Budapest, Institute of Economics, Budapest, Hungary. E-mail: azacish@cf.ac.uk

[‡] Corresponding author: CY Cergy Paris Université, THEMA, 33 boulevard du Port, 95011 Cergy-Pontoise Cedex, France and Corvinus University of Budapest, CIAS; vidapet@gmail.com.

1 Introduction

Public and private communication are essential in real life, hence, in many economic settings, and also in computer science. One advantage of public communication is that its outcome is commonly known among the players (by definition) who can then condition and coordinate their future play on this outcome.[1] Clearly, private communication is essential when there are more than two players. Public communication cannot replace the private one. What if players cannot communicate publicly but can only use pairwise private communication channels? Is it possible to replace public communication with private communication in a way that players at least *always believe* that all the other players consider the same outcome of the given private communication?

First, we consider only the case of $n = 4$ players, $P0$, $P1$, $P2$, and $P3$, and unilateral deviations. Then in section 5, we generalize our result to $n \geq 4$ players and unilateral deviations. [2] Suppose $P3$ (the sender) would like to publicly announce an element of a finite set $x \in X$, each chosen with equal probability, but broadcasting is not possible. For example, Lamport, Shostak, and Pease (1982) describe a Byzantine agreement protocol using private communication channels as follows. In stage 1, $P3$ sends the message x to players $P0$, $P1$, and $P2$. In stage 2, $P0$, $P1$, $P2$ (the forwarders) forward the message they received in stage 1 to each other, i.e., to $P0$, $P1$, and $P2$ but not to $P3$. Players then make a choice which depends on the messages they have sent and received. Lamport et al. (1982) suggest two possible choices rule. In both cases the forwarders only use their three received messages and the sender uses the three messages she sent in stage 1. In choice rule (a), players' choice is the median of these messages. In choice rule (b), players' choice is the majority of the messages if it exists and otherwise they choose some fixed, commonly known $z \in X$.

The above protocol is *resilient* in the following sense. If only one of the players deviates from the protocol, all the players choose the same element of X and this choice is the message sent by the sender if she does not deviate from the protocol. We would like to have the following stronger version of resilience which we call *belief-resilience*: (1) the protocol is resilient; (2) in any information set, all the players believe that the choices of all the players coincide; (3) (i) the beliefs are consistent with the protocol in the sense of Kreps and Wilson (1982), and (ii) point (2) also holds conditional on that the players know what message the sender was expected to send. While points (1), (2), and (3)(i) are natural requirements, we provide an application demonstrating the importance of (3)(ii) below. Or simply think of a situation in which, besides $P3$, another player also knows the value of x.

[1] See the importance of public communication from another aspect in Farrell and Gibbons (1989).

[2] It can be shown that three players cannot replace broadcast with private communication in a (1-)resilient way (see Pease, Shostak, and Lamport (1980)). We are motivated by sequential equilibrium that considers deviations by a single player. The case of more than one deviators is left for future research.

2 Example

To demonstrate the notion of belief-resilience, let $X = \{0, 1, 2\}$ and $z = 1$ in which case choice rules (a) and (b) coincide. Suppose that the sender deviates from the protocol and sends three different messages to the forwarders in stage 1. Suppose that forwarder Pi receives the message i. Further suppose that forwarder $P1$ sends 0 to $P0$ and $P2$ (instead of sending 1 to both) while $P0$ and $P2$ correctly forward stage 1 messages of the sender to each other and to $P0$. Players use the following triplets of messages when making a choice: $P0$ uses (0,0,2), $P1$ uses (0,1,2), $P2$ uses (0,0,2), and $P3$ uses (0,1,2). Then, according to the protocol of Lamport et al. (1982), $P1$ and $P3$ choose 1, $P0$ and $P2$ choose 0. It is clear that $P3$ should believe that all the forwarders choose 1 because she must believe that forwarders follow the protocol. But what should $P0$, $P1$, and $P2$ believe in their corresponding information sets?

According to (2), $P0$ should believe that $P1$, $P2$, and $P3$ choose 0. To satisfy (3), we will argue that $P0$ should believe that $P3$ has sent 0 to $P1$ and $P2$ and it is only $P2$ who has sent her the wrong message 2 instead of 0. According to (2), $P2$ should believe that $P0$, $P1$, and $P3$ choose 0. To satisfy (3), we will argue that $P2$ should believe that $P3$ has sent 0 to $P0$ and $P1$ and it is only $P3$ who has sent her the wrong message 2 instead of 0. According to (2), $P1$ should believe that $P0$, $P2$, and $P3$ choose 1. $P1$ cannot believe that $P3$ has sent i to Pi for $i = 0, 2$ because then she should also believe that $P0$ and $P2$ will choose 0 (the majority of their messages). This is because she must believe that $P0$ forwarded 0 to $P2$ and $P1$ herself has sent 0 to both of them. To satisfy (3), we will argue that $P1$ should believe that $P3$ has sent 1 to $P0$ and $P2$ and both of them have forwarded a wrong message to her, namely, $P0$ has sent 0 and $P2$ has sent 2 to $P1$ instead of 1.

Tedious calculations show that the protocol of Lamport et al. (1982) under both choice rules is belief-resilient in this example when X is small.[3] We conjecture that the protocol of Lamport et al. (1982) with choice rule (a) is not belief-resilient when X is large, but it is always belief-resilient with choice rule (b) as long as the number of players is four.[4]

In this paper we offer a new choice rule, which we call *bitwise-majority*, with which the

[3] A natural candidate, paranoid beliefs à la Geffner and Halpern (2024) does not work. It would make the forwarders always believe that all the three of them have received the same message in stage 1 and, hence, choices could not follow the majority of the messages. Moreover, a deviating sender would then believe that the forwarders' choices differ and, in fact, could induce different choices of the forwarders.

[4] We do not know, whether Lamport et al. (1982) mean that $z = RETREAT$ should be understood as an element of X, i.e., whether the choices must always be in X or they only have to coincide. When $z \notin X$ and the definition of resilience is modified accordingly, then their protocol is clearly not belief-resilient with choice rule (b). $P1$ should believe the others also see three different messages and choose z. But then she should also believe that $P3$ has sent different messages to the different players which means that she believes that both $P0$ and $P2$ will choose 0 given the messages that $P1$ has sent them. Also, as we will see in section 5, not just our choice rule, but even our protocol is different from Lamport et al. (1982) when the number of players is more than four.

protocol of Lamport et al. (1982) is belief-resilient in the case of four players. We deviate from the protocol of Lamport et al. (1982) when the number of players is more than four and show that our new protocol with our new choice rule is still belief-resilient. We prove these by constructing a sequence of completely mixed strategies, the so-called justifying sequence (Kreps and Wilson (1982)), converging to our protocol.[5] We calculate beliefs along the sequence at all information sets using the Bayes rule and show that the limits of these beliefs satisfy (2) and (3) ((1) will be trivially satisfied).

3 The formal statement for $n = 4$

Let I denote the set of players with $|I| = n = 4$. Without loss of generality, let X be a finite set containing all the binary numbers of n bits (digits) and let $\mu \in \Delta(X)$ be a given probability distribution over X with full support.[6] Let $S = R_i = X^3, S_i = X^2, C = X, H_3 = S, H_i = R_i \times S_i$ for $i = 0, 1, 2$. C is the set of possible choices, S is the set of triplets $P3$ can send in stage 1, R_i is the set of triplets Pi receives in stages 1 and 2, S_i the set of couples that forwarder Pi can send to the other forwarders in stage 2, and H_i is the set of messages sent and received by Pi for $i \in I$. We denote generic elements of these sets as follows: $x \in X, s \in S, r_i \in R_i, s_i \in S_i, h_i \in H_i$. Let $m : X^3 \to C$ be the function which associates to every triplet of binary numbers the choice of a player: the binary number is obtained by considering the bitwise (or digit-wise) majority value of the values of the given bit (digit) in the triplet. Extend m to H_i using R_i, i.e., the messages that Pi has received for $i = 0, 1, 2$, and using S, i.e., the messages she sent for $i = 3$. Let σ denote the protocol of Lamport et al. (1982) and consider m as the associated choice rule. Formally $\sigma_3 : X \to \Delta(S)$ and $\sigma_i : X \to \Delta(S_i)$ for $i = 0, 1, 2$, where $\Delta(Y)$ denotes the probability distributions over a finite set Y. Notice that σ here is deterministic. σ is clearly resilient under the choice rule m. A completely mixed strategy σ_i^k of Pi is a protocol for Pi such that in any of her information sets, every message profile that Pi can send to the other players, has positive probability under σ_i^k, i.e., $\sigma_i^k(x)$ is in the interior of the corresponding set of probability distributions. Consider a sequence of completely mixed strategy profile σ^k converging to σ which is called the justifying sequence. Clearly, given μ and m there is an induced probability distribution P_{σ^k} over $X \times \Pi_{i \in I}(H_i \times C)$, i.e., over the set of possible realizations of x, the set of histories of the players and over their final choices. Clearly, $P_{\sigma^k}(x, h_i) > 0$ for all $h_i \in H_i$, for all

[5] The justifying sequence for choice rule (b) is necessarily asymmetric in that it must treat different messages differently. We do not know how to construct such a justifying sequence in general, when X is large.

[6] If X does not contain all the binary numbers using n bits, then let X_b be the set of all binary numbers using n bits and $f : X_b \to X$ be a surjective function. Modify the protocol of Lamport et al. (1982) so that whenever the sender sends $x \in X$ to the other three players, let the sender now instead randomize over all $y \in f^{-1}(x)$ with positive probability.

$x \in X$, and for all $i \in I$. Let us define:

$$P(m(h_j)|x, h_i) = \lim_{k\to\infty} P_{\sigma^k}(m(h_j)|x, h_i),$$

$$P(x|h_i) = \lim_{k\to\infty} P_{\sigma^k}(x|h_i),$$

$$P(m(h_j)|h_i) = \lim_{k\to\infty} P_{\sigma^k}(m(h_j)|h_i).$$

Theorem 1. *There exists a sequence of completely mixed strategies $(\sigma^k)_{k\in\mathbb{N}}$ converging to σ such that for all $i, j \in I$, for all $h_i \in H_i, h_j \in H_j$, and for all $x \in X$ we have that $P(m(h_j) = m(h_i)|h_i) = P(m(h_j) = m(h_i)|h_i, x) = 1$. We also have that $P(x = m(h_i)|h_i) = 1$. Notice, that these probabilities do not depend on the messages sent by forwarder Pi, i.e., on s_i.*

Remark 1. We note that our theorem also holds if players have heterogenous priors over X not necessarily with full support. Then one can consider any $x \in X$ for which $\mu_i(x) > 0$.

4 The proof of the theorem

We construct σ_i^k as follows. Whenever σ_3 specifies for the sender to send the message profile $(x, x, x) \in S$ to the other players in stage 1, i.e., when x has been selected according to μ, the sender selects a message profile to be sent in the following way. The sender randomizes independently across the bits over the triplets of bits she sends using the following probabilities. Suppose that lth bit of x is 0. Then the sender selects the triplet of bits (0,0,0) with probability close to 1, selects (1,1,1) with probability in the order of ϵ^e, selects (1,0,0),(0,1,0),(0,0,1) in the order of ϵ^b, and selects (0,1,1),(1,1,0),(1,0,1) in the order of ϵ^c. The error probabilities are symmetric if the lth bit of x is 1. Forwarders forward the wrong bit to any forwarder independently across forwarders and across bits (digits) in the order of ϵ^a. We specify the values of $a, b, c, e > 0$ later. Let $\epsilon = 1/k$, then $\sigma^k \to \sigma$ as $k \to \infty$.

Now, it is sufficient to show that our theorem holds for $X = \{0, 1\}$ because the randomization of the players are independent across the bits conditional on x. To see this: $P(m_j, m_i|x) = \Pi_{1\le l\le n} P(m_j^l, m_i^l|x) = \Pi_{1\le l\le n} P(m_j^l, m_i^l|x^l)$, where the superscript l denotes the lth bit of the object and m_j, m_i stand for $m(h_j), m(h_i)$. Also, $P(m_j, m_i) = \sum_{x\in X} P(m_j, m_i|x)\mu(x) = \sum_{x\in X} \mu(x)\Pi_{1\le l\le n} P(m_j^l, m_i^l|x^l)$. From now on we assume that $X = \{0, 1\}$.

Our conditions in the theorem about the beliefs of the sender are trivially satisfied because those can be calculated by assuming that the forwarders follow the protocol, i.e., they forward the bit which was sent by the sender. For the forwarders it is sufficient to show that they believe, given h_i, that the sender has sent $m(h_i)$ to the other forwarders. This is because Pi must believe that the other forwarders forwarded the correct message to each other and, hence, they receive the message $m(h_i)$ from the sender and from the other forwarder and therefore, their choice is $m(h_i)$ irrespective of what Pi forwards.

To this end, let us assume that $x = 0$. We construct the table below. The case of $x = 1$ is symmetric by construction, i.e., one only has to swap the 0-s and the 1-s in the table. Clearly, the belief of forwarder Pi about $s \in S$ does not depend on s_i. Hence, consider the eight possible triplets $r_i \in R_i$ that a forwarder Pi can receive, one by one, and the order of the joint probabilities, conditional on $x = 0$, of the corresponding four possible triplets $s \in S$ that the sender may have sent (one of the coordinates of the triplets is fixed by the message Pi has received from the sender). In the table below, the first coordinate in any triplet is the bit that Pi has received from the sender and we do not make a difference which forwarder sends a bit different from what Pi has received from the sender, hence, we only have six cases for r_i. We also do not make a difference which forwarder has sent a bit to Pi different from what she has received from the sender, hence, for each r_i we only have three possible s. Let us choose $e = 4, b = 13, c = 14$ and $a = 8$ to satisfy $e + a < b < c < 2a$ which will imply our theorem. Intuitively, these choices of probabilities ensure: that two forwarders forward the wrong bit to the same forwarder is infinitely less likely than that the sender has sent the wrong bits to two of the forwarders which is infinitely less likely than that the sender has sent the wrong bit to one of the forwarders which is infinitely less likely than that the sender has sent the wrong bit to all the forwarders and one of the forwarders forwarded a bit different from what she received. Given that $e + a < b < c < 2a$, we have that always the first (bold) triplet of s, given r_i, converges to 0 in the slowest order. Hence, the first statement of our theorem follows.

Finally, to prove that $P(x = m(h_i)|h_i) = 1$, it is enough to see that $P(x = m(h_i)|h_i) = P(x = m(r_i)|r_i) = 1$, where $h_i = (r_i, s_i)$ and that $\lim_{k\to\infty} \frac{P_{\sigma^k}(r_i|x\neq m(r_i))}{P_{\sigma^k}(r_i|x=m(r_i))} = 0$. This is true because both the numerator and the denominator converge to 0 in the order of the slowest corresponding s. Direct calculation from the table below (and from the one where the 0-s and the 1-s are swapped) verifies our statement.

r_i	order of $P_{\sigma^k}(s, r_i \mid x = 0)$	s
(0,0,0)	0	(0,0,0)
	e	**(1,1,1)**
(1,1,1)	c+a	(1,0,1)
	b+2a	(1,0,0)
	e+a	**(1,1,1)**
(1,0,1)	c	(1,0,1)
	b+a	(1,0,0)
	c	**(0,1,1)**
(0,1,1)	2a	(0,0,0)
	b+a	(0,1,0)
	a	**(0,0,0)**
(0,1,0)	b	(0,1,0)
	c+a	(0,1,1)
	b	**(1,0,0)**
(1,0,0)	e+2a	(1,1,1)
	c+a	(1,0,1)

5 Generalization of the theorem to $n > 4$

Suppose that besides $P0, P1, P2, P3$ there are other players: $P4, \dots, P(n-1)$. It is still $P3$ who wants to publicly announce some $x \in X$. We complement σ above with the following. In stage 2, players $P0, P1, P2$ forward their messages received from $P3$ to players $P4, \dots, P(n-1)$. The latter players do not receive any message from $P0$ in stage 1 and they do not send any message in stage 2. However, given the received messages from players $P0, P1, P2$, players $P4, \dots, P(n-1)$ apply the bitwise majority choice on these messages. We note that this protocol is different from Lamport et al. (1982).[7] The protocol is clearly resilient. Suppose that $P0, P1, P2, P3$ make mistakes as specified previously, but $P0, P1, P2$ never make a mistake when forwarding their messages to $P4, \dots, P(n-1)$.[8] The beliefs of $P4, \dots, P(n-1)$ can already be calculated using the Bayes rule. They will believe that the messages they received are the ones that $P3$ has sent to $P0, P1, P2$. It follows that the beliefs of these players about

[7] We do not know how to specify the choice rule and the justifying sequence for the protocol of Lamport et al. (1982) when $n > 4$. They require that the sender sends the message to all the other players and these players forward the message to each other in stage 2.

[8] Alternatively, assume that these error probabilities converge to 0 in a sufficiently fast order so that these players believe that it is $P0$ who has deviated.

the other players' choices satisfy our theorem. Also, the beliefs of $P0, P1, P2, P3$ about the choices of $P4, \ldots, P(n-1)$ satisfy our theorem, because, as before, $P3$ believes that $P0, P1, P2$ forward her messages correctly, and any forwarder from $P0, P1, P2$ believes that the other two forwarders received the bitwise majority of her messages and that they have forwarded this message to $P4, \ldots, P(n-1)$.

6 Applications and further properties

6.1 Two applications to Gerardi (2004)

Our theorem can be directly applied to theorem 1 in Gerardi (2004). In his theorem 1, Gerardi (2004) implements the set of correlated equilibria as sequential equilibria of a game, extended with unmediated communication with five (or more) players. Gerardi (2004) assumes that at the very first stage of this extended game, a player can broadcast a message to either three or two other players. From our theorem, it is clear how to mimic broadcasting when the number of involved players is four, consisting of the sender and three forwarders. It is also easy to mimic a broadcasting to two players, i.e., when only three players are involved, but there are in fact five players in the game. Assume that $P0$ wants to mimic a broadcast of $x \in X$ to players $P1$ and $P2$. Let $P0$ choose $y \in X$ uniformly and let $z \in X$ be such that $y + z \mod |X| = x$. Let $P0$ mimic the public announcement of y using players $P1, P2, P3$ and do the same with z using players $P1, P2, P4$. Then $P3$ and $P4$ obtain no information about x but $P1$ and $P2$ can calculate x.

In his theorem 2, Gerardi (2004) uses Forges (1990) to implement the set of (regular) communication equilibria in sequential equilibria of a game, extended with unmediated communication with five players. However, Forges (1990) and, hence, Gerardi (2004) assume that a player can make a public announcement to the other four players. This case is covered by our generalization of our theorem in section 5.

We note that by remark 1, it does not matter when the public communication takes place in an extensive form game. Also, if at some successive information sets, a player receives an information which seemingly contradicts to her beliefs about the past choices of the other players, this can always be explained by deviations outside the mimicking-public-announcement phase by choosing the error probabilities during the mimicking phase sufficiently small.

6.2 Further properties

The importance of (3)(ii) which is implied by our theorem can be demonstrated with the following situation. Suppose that there is another player, say $P2$ besides $P3$, who also knows the value of x. We clearly need (3)(ii). Furthermore, suppose that $P2$ also uses the corresponding variant of σ to transmit the value of x. Let us denote by σ^2 and σ^3 the protocols of $P2$ and $P3$. We also use superscripts 2 and 3 for the histories, and sent and received messages corresponding to σ^2 and σ^3, respectively. What if $P1$ observes h_1^2, h_1^3 such that $m(h_1^2) \neq m(h_1^3)$? **(a)** What is $P(m(h_j^2) = m(h_1^2), m(h_j^3) = m(h_1^3)|h_1^2, h_1^3)$? We claim it can be equal to 1. **(b)** What does $P1$ believe about the true value of x? Can $P1$ always believe for example in the transmission of $P2$? Namely, can we have that $P(x = m(h_1^2)|h_1^2, h_1^3) = 1$ for any h_1^2, h_1^3? An application of the answer to this question, which is affirmative, can be found in Āzacis, Laclau, and Vida (2025).

We now prove points **(a)** and **(b)**. To this end, assume that the completely mixed sequences converging to σ^2 and σ^3 are the same (once the players' roles are permuted accordingly), possibly with different values for a^i, b^i, c^i, e^i for $i = 2, 3$ (with $e^i + a^i < b^i < c^i < 2a^i$), but are independent conditional on (the bits of) $x \in X$. Let $P_{\sigma^{2k},\sigma^{3k}}$ be the induced distribution over $X \times (\Pi_{i\in I}(H_i \times C))^2$.

For **(a)**, we claim that $P(m(h_j^2) = m(h_1^2), m(h_j^3) = m(h_1^3)|h_1^2, h_1^3) = 1$. To see this define:

$$P_{\sigma^2}(m(h_j^2)|x, h_1^2) = \lim_{k\to\infty} P_{\sigma^{2k}}(m(h_j^2)|x, h_1^2),$$

and $P_{\sigma^3}(m(h_j^3)|x, h_1^3)$ similarly. Define

$$P(m(h_j^2), m(h_j^3)|x, h_1^2, h_1^3) = \lim_{k\to\infty} P_{\sigma^{2k},\sigma^{3k}}(m(h_j^2), m(h_j^3)|x, h_1^2, h_1^3)$$

which is equal to

$$\lim_{k\to\infty} P_{\sigma^{2k}}(m(h_j^2)|x, h_1^2)P_{\sigma^{3k}}(m(h_j^3)|x, h_1^3) = P_{\sigma^2}(m(h_j^2)|x, h_1^2)P_{\sigma^3}(m(h_j^3)|x, h_1^3).$$

Then define:

$$P(m(h_j^2), m(h_j^3)|h_1^2, h_1^3) = \lim_{k\to\infty} P_{\sigma^{2k},\sigma^{3k}}(m(h_j^2), m(h_j^3)|h_1^2, h_1^3),$$
$$P(x|h_1^2, h_1^3) = \lim_{k\to\infty} P_{\sigma^{2k},\sigma^{3k}}(x|h_1^2, h_1^3).$$

Hence we have that:

$$P(m(h_j^2) = m(h_1^2), m(h_j^3) = m(h_1^3)|h_1^2, h_1^3) = \sum_{x\in X} P(m(h_j^2) = m(h_1^2), m(h_j^3) = m(h_1^3)|x, h_1^2, h_1^3)P(x|h_1^2, h_1^3)$$

$$= \sum_{x\in X} P_{\sigma^2}(m(h_j^2) = m(h_1^2)|x, h_1^2)P_{\sigma^3}(m(h_j^3) = m(h_1^3)|x, h_1^3)P(x|h_1^2, h_1^3) = \sum_{x\in X} P(x|h_1^2, h_1^3) = 1,$$

where in the penultimate equality we applied our theorem for P_{σ^2} and for P_{σ^3}.

For **(b)**, we can still assume that $X = \{0, 1\}$. In case $m(h_1^2) = m(h_1^3)$, $P1$ must believe that

$x = m(h_1^2) = m(h_1^3)$ with probability 1.[9] Suppose that $x = m(h_1^2) \neq m(h_1^3)$. Clearly, the answer will depend on the values a^i, b^i, c^i, e^i for $i = 2, 3$, i.e., it depends on which player makes mistakes with larger probability. Let us write

$$P(x|h_1^2, h_1^3) = P(x|r_1^2, r_1^3) = \lim_{k\to\infty} \frac{P_{\sigma^{2k}}(r_1^2|x)P_{\sigma^{3k}}(r_1^3|x)\mu(x)}{\sum_{x'\in X} P_{\sigma^{2k}}(r_1^2|x')P_{\sigma^{3k}}(r_1^3|x)\mu(x')}.$$

We want this limit to be 1, for $x = m(h_1^2)$, i.e., $P1$ believes that the transmission of $P2$ is true (and $P3$ deviated). What we need is that:

$$\lim_{k\to\infty} \frac{P_{\sigma^{2k}}(r_1^2|x')P_{\sigma^{3k}}(r_1^3|x')}{P_{\sigma^{2k}}(r_1^2|x)P_{\sigma^{3k}}(r_1^3|x)} = 0$$

for $x' \neq x$.[10] Suppose w.l.o.g. that $0 = m(h_1^2) = x \neq x' = m(h_1^3) = 1$. We can show that

$$\frac{P_{\sigma^{2k}}(r_1^2|1)}{P_{\sigma^{2k}}(r_1^2|0)} \frac{P_{\sigma^{3k}}(r_1^3|1)}{P_{\sigma^{3k}}(r_1^3|0)} < 1/k \tag{1}$$

by using the table in the proof of our theorem, and choosing h_1^2 and h_1^3 to upper bound the two factors independently, and with appropriately choosen a^i, b^i, c^i, e^i for $i = 2, 3$. The tedious calculation can be found in section A of the Appendix.

References

Āzacis, H., M. Laclau, and P. Vida (2025): "Unmediated communication in games with (in)complete information: the 4-player case," *working paper*.

Farrell, J. and R. Gibbons (1989): "Cheap Talk with Two Audiences," *The American Economic Review*, 79, 1214–1223.

Forges, F. (1990): "Universal Mechanisms," *Econometrica*, 58, 1341–64.

Geffner, I. and J. Y. Halpern (2024): "Communication Games, Sequential Equilibrium, and Mediators," *Journal of Economic Theory*, 221, 105890.

Gerardi, D. (2004): "Unmediated communication in games with complete and incomplete information," *Journal of Economic Theory*, 114, 104–131.

Kreps, D. M. and R. Wilson (1982): "Sequential Equilibria," *Econometrica*, 50, 863–894.

[9] This immediately follows from our theorem where this is true in case of a single sender.

[10] When X is larger, we have to consider the factors of $\lim_{k\to\infty} \Pi_{1\leq l\leq n} \frac{P_{\sigma^{2k}}(r_1^{2^l}|x'^l)P_{\sigma^{3k}}(r_1^{3^l}|x'^l)}{P_{\sigma^{2k}}(r_1^{2^l}|x^l)P_{\sigma^{3k}}(r_1^{3^l}|x^l)} = 0$,, where $r_1^{2^l}$ is the triplet obtained by using the lth digits of the triplet r_1^2.

Lamport, L., R. Shostak, and M. Pease (1982): "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4, 382–401.

Pease, M., R. Shostak, and L. Lamport (1980): "Reaching Agreement in the Presence of Faults," *J. ACM*, 27.

A The proof of inequality 1

All the four probabilities appearing in inequality 1 can be written as sums with respect to the corresponding s^2 and s^3. For example, $P_{\sigma^{2k}}(r_1^2|1) = \sum_{s^2} P_{\sigma^{2k}}(r_1^2, s^2|1)$. In the limit only the terms with the smallest exponents determine the value of the product. Consider the table in the proof of our theorem. The table should be read as follows. All 0-s and 1-s are swapped (because $x = 1$), $r_i = r_1^2$, and $s = s^2$. The term with the smallest exponent is the first (bold) triplet in the table in the column of s given r_i. We consider all possible realizations of r_1^2. Consider $r_1^2 = (1,0,0)$. Then the probability corresponding to $s^2 = (1,0,0)$ has the smallest exponent both under $x = 1$ and under $x = 0$ (change back the 0-s and 1-s). Then, $\frac{P_{\sigma^{2k}}(r_1^2|1)}{P_{\sigma^{2k}}(r_1^2|0)} \approx \frac{P_{\sigma^{2k}}(s^2,r_1^2|1)}{P_{\sigma^{2k}}(s^2,r_1^2|0)} \approx \epsilon^{c^2-b^2}$. Consider $r_1^2 = (0,0,0)$. Then the probability corresponding to $s^2 = (0,0,0)$ has the smallest exponent under both $x = 0$ and $x = 1$. Then, $\frac{P_{\sigma^{2k}}(r_1^2|1)}{P_{\sigma^{2k}}(r_1^2|0)} \approx \epsilon^{e^2}$. Finally, consider $r_1^2 = (0,1,0)$. Then the probability corresponding to $s^2 = (0,0,0)$ has the smallest exponent under both $x = 0$ and $x = 1$. Then, $\frac{P_{\sigma^{2k}}(r_1^2|1)}{P_{\sigma^{2k}}(r_1^2|0)} \approx \epsilon^{e^2}$. For r_1^3 one can do the same exercise and get that either $\frac{P_{\sigma^{3k}}(r_1^3|1)}{P_{\sigma^{3k}}(r_1^3|0)} \approx \epsilon^{-(c^3-b^3)}$ or $\frac{P_{\sigma^{3k}}(r_1^3|1)}{P_{\sigma^{3k}}(r_1^3|0)} \approx \epsilon^{-e^3}$. If $\min(c^2 - b^2, e^2) > \max(c^3 - b^3, e^3)$, then we have that the factor converges to 0. This is satisfied if we choose a^3, b^3, c^3, e^3 to be a, b, c, e as above ($a = 8, b = 13, c = 14$ and $e = 4$) and choose a^2, b^2, c^2, e^2 to be $5a, 5b, 5c, 5e$ $(20 = 5e^3 = e^2 > \min(c^2 - b^2, e^2) = c^2 - b^2 = 5(c^3 - b^3) = 5 > e^3 = 4)$.