

THE PENNSYLVANIA STATE UNIVERSITY  
THE GRADUATE SCHOOL  
COLLEGE OF THE LIBERAL ARTS

ESSAYS ON COMMUNICATION,  
COORDINATION, AND  
CORRELATION

A DISSERTATION IN  
ECONOMICS  
BY  
CHUN-TING CHEN

©2015 – CHUN-TING CHEN

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

AUGUST 2015

The dissertation of Chun-Ting Chen was reviewed and approved<sup>1</sup> by the following:

**Kalyan Chatterjee**

Distinguished Professor of Economics and Management Science  
The Pennsylvania State University  
*Dissertation Adviser and Chair of Committee*

**Edward Green**

Professor of Economics  
The Pennsylvania State University

**James Jordan**

Professor of Economics  
The Pennsylvania State University

**Sona N. Golder**

Associate Professor of Political Science  
The Pennsylvania State University

**Robert C. Marshall**

Distinguished Professor of Economics  
The Pennsylvania State University  
*Head of the Department of Economics*

---

<sup>1</sup>Signatures are on file in the Graduate School.

# ESSAYS ON COMMUNICATION, COORDINATION, AND CORRELATION

## ABSTRACT

Each of the two chapters in this dissertation is based on a game theory paper. Although the topic of each chapter is different, they are linked by the question: How do players coordinate their actions through communication? Each chapter develops a communication schema, depicts equilibrium strategies, and responds to this inquiry.

In the first chapter, I study a collective action problem in a setting of discounted repeated coordination games in which players know their neighbors' inclination to participate as well as monitor their neighbors' past actions. I define strong connectedness to characterize those states in which, for every two players who incline to participate, there is a path consisting of players with the same inclination to connect them. Given that the networks are fixed, finite, connected, commonly known, undirected and without cycles, I show that if the priors have full support on the strong connectedness states, there is a weak sequential equilibrium in which the ex-post efficient outcome repeats after a finite time  $T$  in the path when discount factor is sufficiently high. This equilibrium is constructive and does not depend on public or private signals other than players' actions.

In the second chapter, I consider the three-player complete information games augmented with pre-play communication. Players can privately communicate with others, but not through a mediator. I implement correlated equilibria by letting players be able to authenticate their messages and forward the authenticated messages during communication. Authenticated messages, such as letters with signatures, cannot be duplicated but can be sent or received by players. With authenticated messages, I show that, if a game  $G$  has a worst Nash equilibrium  $\alpha$ , then any correlated equilibrium distribution in  $G$ , which has rational components and gives each player higher payoff than what  $\alpha$  does, can be implemented by a pre-play communication. The proposed communication protocol does not publicly expose players' messages in any stage during communication.

# Contents

LISTING OF FIGURES	v
LIST OF TABLES	vi
ACKNOWLEDGMENTS	vii
<b>1 COORDINATION IN SOCIAL NETWORKS</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Preliminaries . . . . .	12
1.3 Equilibrium: $k = n$ . . . . .	16
1.4 Equilibrium: $k < n$ . . . . .	18
1.5 Conclusion . . . . .	44
<b>2 CORRELATION WITH FORWARDING</b>	<b>46</b>
2.1 Introduction . . . . .	46
2.2 Model . . . . .	52
2.3 Results . . . . .	54
2.4 Discussion and Conclusion . . . . .	66
<b>APPENDIX A CHAPTER 1</b>	<b>73</b>
A.1 Proofs . . . . .	74
A.2 Equilibrium Construction . . . . .	79
<b>APPENDIX B CHAPTER 2</b>	<b>103</b>
B.1 Formal definition and proofs . . . . .	104
<b>REFERENCES</b>	<b>124</b>

# Listing of figures

2.1	An example of Player 1's 32 categories of "encoded" notes . . . . .	61
-----	---	----

# List of Tables

1.1	Notations for sequence of actions . . . . .	25
1.2	Reporting messages . . . . .	27
1.3	$j$ 's belief updating after observing $i$ 's reporting messages in the reporting period in $t$ -block . . . . .	27
1.4	Coordination messages . . . . .	34
1.5	$j$ 's belief updating after $CD_{1,1}^t$ by observing $i$ 's previous actions ( $t > 0$ ) .	35
1.6	In-path strategies in $RP^t$ , $CD_{1,1}^t$ , and $CD_{2,1}^t$ ( $t > 0$ ) . . . . .	35
1.7	In-path strategies in $CD_{m,1}^t$ , where $m \geq 2$ ( $t > 0$ ) . . . . .	36
1.8	$j$ 's belief updating after $CD_{1,2}^t$ by observing $i$ 's previous actions ( $t > 0$ ) .	37
1.9	In-path strategies in $RP^t$ , $CD_{1,1}^t$ , $CD_{1,2}^t$ , and $CD_{2,2}^t$ ( $t > 0$ ) . . . . .	37
1.10	In-path strategies in $CD_{m,2}^t$ , where $m \geq 2$ ( $t > 0$ ) . . . . .	38
1.11	In-path strategies in $CD_{1,3}^t$ , $t > 0$ . . . . .	38
1.12	In-path strategies after $CD_{m,3}^t$ , where $m \geq 2$ , $t > 0$ . . . . .	38

# Acknowledgments

I am deeply indebted to my advisor, Professor Kalyan Chatterjee. Kalyan generously shared his time and expertise with me while I was conducting my dissertation research. Without his support, this dissertation would have been impossible.

I am also grateful for the invaluable suggestions that I received from Professors Edward Green, Sona Golder, James Jordan, and Neil Wallace. Their helpful advice and comments have much improved this dissertation.

I was fortunate to have many great peers in my graduate program. I am thankful to them for the joint learning, the discussion, and the warmest friendship.

Finally, I would like to thank my family for their encouragement that came from afar but always traveled in a timely fashion.

TO SHU-CHUN CHEN  
YOU HAVE MADE ALL THE DIFFERENCE



# 1

## Coordination in Social Networks

### 1.1 INTRODUCTION

This paper studies collective actions in a setting of discounted repeated coordination games, where information and monitoring structures are modeled as networks. Players are uncertain about the states of nature but can observe their neighbors' actions. I ask what kinds of networks can induce players to solve the underlying uncertainty in order

to coordinate to the ex-post efficient outcome. Though the main motivation is to understand the dynamic of social movements, a general interest centers on the collective action behaviors within social structures.

Consider pro-democracy movements. Strong discontents overthrowing a regime may exist, but it is difficult to organized around these discontents because information about the existence of such discontents is not always transparent. For instance, in East Germany, the government had control over the electoral system and the mass media, and the eavesdropping by secret agents impedes people from showing their discontents. As [Karl-Dieter and Christiane, 1993] or [Chwe, 2000] have suggested, such discontents may be revealed “locally” between friends, organizations, or within other social structure, but are hardly revealed publicly. This lack of common knowledge about the existence of strong discontent may impede people from conducting a one-shot uprising due to the fear of possible failure (e.g., [Chwe, 2000] in proposing a static model to characterize the networks that provide common knowledge about peoples’ discontents). However, an event may trigger letter event (e.g., [Lohmann, 2011] in using informational cascade model to explain consecutive demonstrations in East Germany 1989-1991). When rebels are aware of the capacity to transmit relevant information about the level of collective discontent through their actions, they might be willing to act although it might be risky in facing the possible failure. I view such risky actions as a part of an equilibrium strategy and the entire movement as a learning process.

Inspired by [Chwe, 2000], I model such dynamic collective action in the following way. Players repeatedly play a *k-Threshold game* with a parameter  $k$  in a network. There are two types of players located in the network, one we called them *Rebel* and one we

called them *Inert*. Players' types and their actions can be observed only by their neighbors. A Rebel has two actions, which are **revolt** or **stay**, while an Inert has only one action, which is **stay**. A Rebel will get payoff as 1 if he chooses **revolt** and more than  $k$  players choose **revolt**; he will get payoff as  $-1$  if he chooses **revolt** and less than  $k$  players choose **revolt**; he will get payoff as 0 if he chooses **stay**. An Inert will get payoff as 1 if he chooses **stay**.

Since a Rebel may not know how many Rebels in this world, Rebels' payoff structure captures the idea that **stay** is a safe arm and **revolt** is a risky arm. Given a common prior  $\pi$  over players' types, players play this  $k$ -Threshold game infinitely repeatedly with a common discount factor  $\delta$ . Cheap talk is not allowed, no outside mechanism serves as an information exchange device.

Rebels then communicate with each other by playing actions. For different  $k$  and different network structures, I am looking for a sequential equilibrium which has the property of *approaching ex-post efficient* (APEX henceforth) to investigate the information sharing behavior in the networks. An equilibrium is APEX if and only if *the tails of actions in the equilibrium path repeats the static ex-post efficient outcome after a finite time  $T$* . This refinement serves to check if players learned the relevant information in the equilibrium path. If there are at least  $k$  Rebels in this society, then *all* Rebels should **revolt** after  $T$  as if they have known that more than  $k$  Rebels exist; otherwise, *all* Rebels should **stay** after  $T$ . Rebels' incentives to communicate are affected by Rebels' positions in networks since networks are structuring the information and monitoring structure.

In order to get a quick intuition about Rebel's learning process in the proposed framework, consider the  $k$ -Threshold game with  $k = n$  and assume payoff is hidden. When

$k = n$ , a Rebel can get positive payoff only if all the players are Rebels. Given that the networks are fixed, finite, connected, commonly known, and undirected (*networks* henceforth), an APEX sequential equilibrium can be constructed by a contagion-like argument. This argument is to treat **stay** as the message of “there is an Inert out there”; and treat **revolt** as the message of “there could be no Inert out there”. If a Rebel has an Inert neighbor, then he plays **stay** forever. If he has no Inert neighbors, then he plays **revolt** until he observes that some of his neighbors play **stay**, and then he shifts to play **stay** forever. Since the networks are finite, within finite periods, a Rebel will learn that there is an Inert out there if some neighbors has played **stay** and learn that there is no an Inert out there otherwise.

The non-trivial cases appear when  $k < n$ . The  $k = n$  case is easier because the underlying relevant information is to tell “Is there an Inert out there?”. I can construct equilibrium when  $k = n$  by using single-period binary actions,  $\{\mathbf{stay}, \mathbf{revolt}\}$ , to separate the states into two parts, “no Inerts” or “some Inerts”. In other words, these single-period actions can generate distinguishable distribution of signals to inform players in telling the true states of nature<sup>1</sup>. However, when  $k < n$ , the relevant information is to tell “Are there at least  $k$  Rebels out there?”, and thus these binary actions have to carry more information to reveal the states. As I will show later, several sequences of actions will be used to transmit Rebels’ private informations and to control Rebels’ beliefs in equilibrium. In the equilibrium path, two kinds of sequence will be used. The first kind, *reporting messages*, is to report their private information about the states of nature; the second one, *coordination messages*, is to inform Rebels about whether some other Rebels

---

<sup>1</sup>e.g., [Fudenberg and Yamamoto, 2010] or [Fudenberg and Yamamoto, 2011].

have known the relevant information. Specifically, in the equilibrium path, Rebels will play the coordination message to inform other Rebels whenever they have known the relevant information, and those other Rebels will play the same message again to inform other Rebels. The coordination message means to serve as a short-cut to track individuals' higher-order beliefs about "Have some Rebels known the relevant information?", "Have some Rebels known some Rebels have known the relevant information", etc.

Note that communication is not free but costly in the sense that playing **revolt** is risky. Due to being discounting, Rebels always seek the opportunity to manipulate their messages to save their costs in the time horizontal line<sup>2</sup>. A free rider problem may occur when reporting information incurs costs. I give an example here to illustrate this issue. Consider a situation where two nearby Rebels exchange information<sup>3</sup>. Suppose that these two Rebels can learn the true state after acquiring information from each other's truthful reporting. Further suppose that each of them can freely initiate the coordination after exchanging information. In this instance, truthful reporting is not a best response because a player can wait given that the other will report truthfully. The intuition behind the above scenario is to see the future coordination as a public good. This public good can only be made by Rebels' truthful reporting, which incurs some costs.

The main result will show that this coordination problem can be solved in the *acyclic* networks. Here, I define a *path* in  $G$  is a sequence consisting of nodes without repetition in which a node is a neighbor of a previous node. Then I define an acyclic network  $G$  by defining a network in which the path between different nodes is unique. After I define

---

<sup>2</sup>Indeed, allowing cheap talk or using limit-of-mean preference (e.g., [Renault and Tomala, 1998]) will solve this coordination problem.

<sup>3</sup>Example 5

*strong connectedness* as the property that there is always a path consisting of Rebels to connect any pairs of Rebels, the main result shows:

**Result 1. Main Result** *For  $n$ -person repeated  $k$ -Threshold game with parameter  $1 \leq k \leq n$  played in any acyclic network, if  $\pi$  has full support on the strong connectedness, then, there is a  $\delta^*$  such that a (weak) APEX sequential equilibrium exists whenever  $\delta > \delta^*$ .*

Here,  $\pi$  has full support on strong connectedness means that  $\pi$  assigns positive probability on same states if and only if those states has strong connectedness. This assumption is to make sure that the underlying game is not reduced to an incomplete information game without communication. To see this, recall that an Inert always plays **stay**. Rebels can not communicate with some Rebels by their actions if an Inert happens to separate them. For instance, in a wheel network, an incomplete game without communication is that the central player is an Inert while the peripheral players are all Rebels. It is impossible to find an APEX equilibrium in this instance unless  $k = 1$ .

The off-path belief serves as a grim trigger as follows. Whenever a Rebel detects a deviation, he believes that all other players outside his neighborhood are Inerts. Thus, if there are less than  $k$  Rebels in his neighborhood, he will play **stay** forever. With this off-path belief and the constructed equilibrium strategies, the belief system satisfies *updating consistency* ([Perea, 2002]), while it may not satisfies full consistency ([Kreps and Wilson, 1982]).<sup>4</sup>

---

<sup>4</sup>Updating consistency requires that, for every player, for every player's strategies, for every information sets  $s^1, s^2$  where  $s^2$  follows  $s^1$ , if  $s^2$  happens with positive probability given  $s^1$  and given players' strategies contingent on  $s^1$ , then the belief over  $s^2$  should satisfy Bayesian updating conditional on the belief over  $s^1$  and players' strategies contingent on  $s^1$ . In other words, the updating consistency require that players hold beliefs in every information sets and hold updated beliefs that follows previous beliefs. This requirement imposes restrictions on off-path beliefs that induce sequential rationality, although it is weaker than full consistency in the sense that full consistency implies updating consistency.

The equilibrium construction is starting from building a communication protocol. By exploiting the assumption of finite and commonly known network, I assign each node a distinct prime number. Then I let reporting messages carry the information about the multiplication of nodes' prime numbers. Since the multiplication of prime numbers can be de-factorized uniquely, the reporting messages thus carry the information about those nodes' locations in a network. Next, I let two phases, reporting period and coordination period, occur in turns in the time horizon, where the reporting (resp. coordination) messages are played in the reporting (resp. coordination) period. In coordination period, whenever a Rebel can tell the relevant information, such Rebel inform his nearby Rebels by sending coordination messages. Those nearby Rebels then continue to inform their nearby Rebels by sending coordination messages, etc. Then, after coordination period, if a Rebel has received a coordination message, he is certain that all Rebels have commonly known that all Rebels can tell the relevant information.

I call a complete two-phases, starting from a reporting period and ending with a following coordination period, a *block*. In a block, I control the inter-temporal incentives in playing between reporting and coordination messages as follows. First, I let both of the coordination messages, one of them can initiate the coordination to **revolt** and another one can initiate the coordination to **stay**, incur no expected cost. Second, I let Rebels play **revolt** after a block only if they have observed the coordination message to **revolt** and observed some reporting messages which incur some expected costs. However, the continuation behavior after observing the coordination message to **stay** is not contingent on any reporting message. When a Rebel looks forward future coordination to **revolt**, he may have incentive to "take costs" to influence Rebels' future behavior for-

wardly; otherwise, he just plays **stay**. Next, in the equilibrium path, I make sure that Rebels will play ex-post efficient outcome repeatedly right after a block if some Rebels have initiated the coordination in that block. I will argue that only those Rebels who have been able to tell the relevant information after reporting period have incentive to initiate the coordination since they do not need further information to tell the states. This argument is to show that a Rebel other than them will not take advantage to send that free coordination message to initiate the coordination. This is because players can not update further information if all of their neighbors continue to play the same actions in the future. When  $\delta$  is high enough, he will not initiate the coordination to impede his own learning process to achieve the ex-post efficient outcome.

I then characterize Rebels' incentive in taking costs and control how much cost they should take to sustain an APEX equilibrium. In the equilibrium path, a Rebel iteratively updates his relevant information given other Rebels' cost taking in reporting their information about the state, and a Rebel take costs only if his current relevant information has not been acquired by other Rebels. In the equilibrium path, a Rebel thus believe that "more other Rebels are out there" if and only if his nearby Rebel take costs to report their existence. Some specified forms of reporting messages are introduced, and the off-path belief is to enforce Rebels not to play differently from them.

The key step here is to construct a reporting message, "take a cost", which incurs the least expected cost, and this message should be considered as a part of the equilibrium path. I denote this special reporting message as  $\langle 1 \rangle$ . To see its importance, consider the concept of "pivotal Rebel". Here, a pivotal Rebel is the Rebel who is sure that he can know the relevant information right after a reporting period given that other Rebels



will report their information truthfully. Now suppose playing  $\langle 1 \rangle$  is not considered as a part of the equilibrium path, and suppose a Rebel find that himself is a pivotal Rebel during a reporting period while himself has not yet reported anything in that period. He may then find a profitable deviation by taking less cost, which can not be detected by at least  $k$  Rebels although some Rebels can detect such deviation. Since those Rebels who detected such deviation will play **stay** forever by the off-path belief, and this pivotal Rebel can initiate the coordination to **revolt** by convincing other Rebels to play **revolt**, the APEX fails. To solve this problem, I introduce message  $\langle 1 \rangle$  to let pivotal Rebels identify themselves, while I let coordination messages to **revolt** or to **stay** have to be initiated when  $\langle 1 \rangle$  has been played in the equilibrium path to prevent non-pivotal Rebels from mimicking pivotal Rebels.

The major difficulties remaining to solved are the situations where there are multiple pivotal players nearby each other. In such phenomenon, the APEX may fails since playing  $\langle 1 \rangle$  does not answer “how many Rebels a pivotal Rebel has known” although it does address “a pivotal Rebel exists”. The assumption of acyclic networks is crucial to solve these problems. If the networks are acyclic, I will show it later that there are only two kinds of pivotal Rebels. One kind is that they have known there are at least  $k - 1$  Rebels. The other kind is that they will know the true state given other Rebel’s truthful reporting. I call the latter case a free rider problem. If the networks are acyclic, Lemma 1.4.2 will show that the free rider problems only happen between two nearby pivotal Rebels in only one block in the equilibrium path. Further, these two nearby Rebels will know that this free rider problem will occur before the game entering into this block. The consequence of Lemma 1.4.2 is that, before the game entering into this block, I can let one of them

report the information about the state and let the other one play  $\langle 1 \rangle$  dependent on their indexed prime numbers.

This paper contributes to several fields of economics.

First, the future coordination can be viewed as a public good among all Rebels. A strand of public good literature, such as [Lohmann, 1994], is to view information as a public good while generating information is costly<sup>5</sup>. This paper models costly information generation, while adding another aspect, network-monitoring, to investigate a collective action behavior.

Second, this paper is also related to the literature in social learning<sup>6</sup>. Several papers have considered social learning in networks<sup>7</sup>. In this literature, when players are myopic, the information flows could be very complicated because the information they sent can in turns affect their future behaviors. For instance, in [Gale and Kariv, 2003], even for 3-person connected undirected networks, the complete network and incomplete network will give different convergence results which highly depend on individuals' initial private signals and their allocations in a network. In [Golub and Jackson, 2010], instead of using Bayesian learning, they use a naive learning protocol to tackle with this social learning problem. I consider the social learning in networks as a learning-in-game procedure, where individual can put more weights on the future learning results. My result gives a hint that the shape of network (without cycle) did not matter too much if players are

---

<sup>5</sup>For instance, [Lohmann, 1993][Lohmann, 1994] consider that individuals generate information by their actions, where the aggregate outcomes of actions is public. [Bolton and Harris, 1999] consider team experiment in infinite time horizon where the outcomes of experiments are public signals. [Bramoullé and Kranton, 2007] view information as a public good and consider public good provision in networks.

<sup>6</sup>Reviews can be seen in [Bikhchandani et al., 1998] [Cao and Hirshleifer, 2001].

<sup>7</sup>[Goyal, 2012] gives the reviews. Recent papers, e.g., [Acemoglu et al., 2011][Chatterjee and Dutta, 2011], also discuss this topic

far-sighted.

Third, a growing literature consider the game played in networks where various games played in various networks with various definitions<sup>8</sup>. Only few papers in this literature discuss the repeated game. In complete information game. In [Laclau, 2012], she proved a folk theorem where players play the game locally. In [Wolitzky, 2013] [Wolitzky, 2014], he consider network-like monitoring where a prisoner dilemma game played globally. My paper is the first paper to consider the incomplete information game repeatedly played in a network.

My paper is also related to the literature in folk theorems in discounted repeated game with incomplete information. In this literature, they consider more general games than the games adopted here. [Fudenberg and Yamamoto, 2010] [Fudenberg and Yamamoto, 2011] [Wiseman, 2012] considering  $n$ -person game with public signals jointly generated by the states and actions; [Yamamoto, 2014] considering 2-person game with private signals jointly generated by the states and actions. There, the full-rank conditions are imposed to let single-period actions generate informative signals to separate the states. Here, I consider  $n$ -person game without signals and thus the single-period full-rank conditions are not imposed before solving the equilibrium. And my result shows that acyclic networks are sufficient to sustain the ex-post efficiency when discount factor is sufficiently high.

The paper is organized as the followings. Section 1.2 introduces the model. Section 1.3 and Section 1.4 discusses the equilibrium construction and shows the main result. Some variations of my model will be discussed in its subsection 1.4.6. Section 1.5 makes

---

<sup>8</sup>[Jackson, 2008][Goyal, 2012] gives the reviews.

the conclusion. All the missing proofs can be found in Appendix A.1.

## 1.2 PRELIMINARIES

### 1.2.1 NOTATIONS

Given a finite set  $A$ , denote  $\#A$  as the cardinality of a set  $A$ , and denote  $\Delta A$  as the set of probability distribution over  $A$ .

The square bracket  $[]$  that follows a quantifier  $\exists, \forall$  will be read as “*such that*”. For instance,  $\exists a \in A [c \in A, c = a]$  will be read as “exists  $a$  in  $A$  such that  $c$  in  $A$  and  $c$  is equal to  $a$ ” .

### 1.2.2 MODEL

There are  $n$  players. Denote  $N = \{1, 2, \dots, n\}$  as the set of players.

We say  $G$  is a graph if  $G$  is a point-to-set function mapping from  $N$  to a subset of  $N$  containing  $i \in N$ . Moreover, we denote  $G_i = G(i)$  as  $i$ 's neighbors and also denote  $\tilde{G}_i = G_i \setminus \{i\}$  as  $i$ 's neighborhood excluded  $i$  self. We say that  $G$  is fixed if and only if  $G$  is not random. We say that  $G$  is undirected if and only if for all  $i, j$  if  $j \in G_i$  then  $i \in G_j$ . A path from  $i$  to  $j$ ,  $i \neq j$  in an undirected graph  $G$  is a finite sequence  $l_1, \dots, l_q$  such that  $l_1 = i, l_2 \in \tilde{G}_{l_1}, l_3 \in \tilde{G}_{l_2}, \dots, l_q = j$  and there is no repetition in  $\{l_1, \dots, l_q\}$ . An undirected graph is connected if and only if for all  $i, j$ ,  $i \neq j$  there is a path from  $i$  to  $j$ .

Throughout this paper, I call  $G$  a network if the graph  $G$  is finite, fixed, commonly known, connected, and undirected.

For each player  $i$ , let  $\Theta_i = \{Rebel, Inert\}$  be the set of  $i$ 's type and denote  $\theta_i \in \Theta_i$  as  $i$ 's type. The set of states of nature is  $\Theta = \prod_{j \in N} \Theta_j$ , and let  $\theta \in \Theta$  be a state of nature. Let

$\Theta_{G_i} = \prod_{j \in G_i} \Theta_j$  be the set of  $i$ 's neighbors' types, and let  $\theta_{G_i} \in \Theta_{G_i}$  be an element in it. Let  $p_{G_i} : \Theta \rightarrow 2^\Theta$  be  $i$ 's information partition function such that  $p_{G_i}(\theta) = \{\theta_{G_i}\} \times \prod_{j \notin G_i} \Theta_j$ . Denote  $\mathcal{P}_{G_i} = \{p_{G_i}(\theta)\}_{\theta \in \Theta}$  as  $i$ 's information sets about  $\theta$ .

For convenience, I also denote  $[Rebels](\theta) = \{j : \theta_j = Rebel\}$  be the set of Rebels given  $\theta$ .

There is a game,  $k$ -threshold game, infinitely repeated played with common discounted factor  $\delta$  in a fixed  $G$ . Time is discrete, infinite horizontal. At the beginning of this game, a state is realized and there is a common prior  $\pi \in \Delta\Theta$  over  $\Theta$ . After a state is realized, players simultaneously choose an action  $a_{\theta_i} \in A_{\theta_i}$  in each period afterwards. If  $\theta_i = Rebel$ , then  $A_{\theta_i} = \{\mathbf{revolt}, \mathbf{stay}\}$ . If  $\theta_i = Inert$ , then  $A_{\theta_i} = \{\mathbf{stay}\}$ . Let  $a_{\theta_i} \in A_{\theta_i}$  be  $i$ 's action if  $i$ 's type is  $\theta_i$ , and let  $a_{-\theta_i} \in \prod_{j \in N, j \neq i} A_{\theta_j}$  be the actions taken by players other than  $i$ . Player  $i$ 's static payoff function is denoted as  $u_{\theta_i} : \prod_{j \in N} A_{\theta_j} \rightarrow \mathbb{R}$ . In this  $k$ -threshold game,  $i$ 's static payoff is defined as followings.

1.  $u_{Rebel_i}(a_{Rebel_i}, a_{-\theta_i}) = 1$  if  $a_{Rebel_i} = \mathbf{revolt}$  and  $\#\{j : a_{\theta_j} = \mathbf{revolt}\} \geq k$
2.  $u_{Rebel_i}(a_{Rebel_i}, a_{-\theta_i}) = -1$  if  $a_{Rebel_i} = \mathbf{revolt}$  and  $\#\{j : a_{\theta_j} = \mathbf{revolt}\} < k$
3.  $u_{Rebel_i}(a_{Rebel_i}, a_{-\theta_i}) = 0$  if  $a_{Rebel_i} = \mathbf{stay}$
4.  $u_{Inert_i}(a_{Inert_i}, a_{-\theta_i}) = 1$  if  $a_{Inert_i} = \mathbf{stay}$

Players can only observe their neighbors' actions. In order to emphasize that their payoffs are not the signals for them to infer others' actions, I assume that payoffs are hidden until Section 1.4.6. To be more precise, let  $s \geq 0$  be a period. Let  $H_i^0 = \{\emptyset\}$  and let  $H_i^s = H_i^0 \times \prod_{t=1}^s A_{\theta_t}$  be the set of histories of actions played by player  $i$  up to period  $s$ . Let  $H_{G_i}^0 = \{\emptyset\}$  and let  $H_{G_i}^s = H_{G_i}^0 \times \prod_{t=1}^s \prod_{j \in G_i} A_{\theta_j}$  be the set of histories player  $i$  can

observe up to period  $s$ . For convenience, also denote  $H^0 = \{\emptyset\}$ ,  $H^s = H^0 \times \prod_{t=1}^s \prod_{j \in N} A_{\theta_j}$ , and  $H = H^0 \times \prod_{s=1}^{\infty} \prod_{j \in N} A_{\theta_j}$  with generic element  $h \in H$ . Up to period  $s$ ,  $i$ 's information sets about histories of actions is  $\mathcal{H}_{G_i}^s = \{\{h_{G_i}^s\} \times \prod_{j \notin G_i} H_j^s\}_{h^s \in H^s}$ , where  $h_{G_i}^s \in H_{G_i}^s$ .

$i$ 's pure strategy is a function  $\tau_{\theta_i} : (\prod_{j \in G_i} \Theta_j) \times \cup_{s=0}^{\infty} H_{G_i}^s \rightarrow A_{\theta_i}$ . For convenience, also let  $\tau = \{\tau_{\theta_i}\}_i$ .

The prior  $\pi$ , the network  $G$ , and  $\tau$  induce a joint distribution, denoted as  $\gamma_G^{\pi, \tau}$ , over  $\Theta \times H$ . Given a realization  $(\theta, h)$  according to  $\gamma_G^{\pi, \tau}$ , let  $h_{\theta}^{\tau}$  be the realized sequence of actions generated by  $\tau$  given  $\theta$ .

Denote  $\alpha_{G_i}^{\pi, \tau}(\theta, h^s | \theta_{G_i}, h_{G_i}^s)$  as the conditional distribution over  $\Theta \times H^s$  conditional on  $\theta_{G_i} \in \Theta_{G_i}$  and  $h_{G_i}^s \in H_{G_i}^s$  induced by  $\tau$  for player  $i$  at period  $s$ . For convenience, also denote  $\beta_{G_i}^{\pi, \tau}(\theta | \theta_{G_i}, h_{G_i}^s) = \sum_{h^s \in H^s} \alpha_{G_i}^{\pi, \tau}(\theta, h^s | \theta_{G_i}, h_{G_i}^s)$ . Finally, let  $E_G^{\delta}(u_{\theta_i}(\tau) | \alpha_{G_i}^{\pi, \tau}(\theta, h^s | \theta_{G_i}, h_{G_i}^s))$  be  $i$ 's continuation expected payoff conditional on  $\theta_{G_i}$  and  $h_{G_i}^s$  induced by  $\tau$ .

Let  $\mathcal{A}_{G_i}^s = \mathcal{P}_{G_i} \times \mathcal{H}_{G_i}^s$  be  $i$ 's information sets at period  $s$ , and let  $\mathcal{A}_{G_i} = \prod_{s=0}^{\infty} \mathcal{A}_{G_i}^s$  be  $i$ 's information sets. The equilibrium concept here is the weak sequential equilibrium. A weak sequential equilibrium is a pair of  $\{\tau^*, \alpha^*\}$ , where  $\alpha^*$  is a collection of distributions over players' information sets with the property that, for all  $i$ , for all  $s$ ,  $\alpha_{G_i}^*(\theta, h^s | \theta_{G_i}, h_{G_i}^s) = \alpha_{G_i}^{\pi, \tau^*}(\theta, h^s | \theta_{G_i}, h_{G_i}^s)$  whenever  $A_{G_i}^s \in \mathcal{A}_{G_i}^s$  is reached with positive probability given  $\tau^*$ . For all  $i$ , for all  $s$ , the  $\tau_{\theta_i}^*$  maximize  $i$ 's continuation expected payoff conditional on  $\theta_{G_i}$  and  $h_{G_i}^s$

$$E_G^{\delta}(u_{\theta_i}(\tau_{\theta_i}, \tau_{-\theta_i}^*) | \alpha_{G_i}^{\pi, \tau_{\theta_i}, \tau_{-\theta_i}^*}(\theta, h^s | \theta_{G_i}, h_{G_i}^s))$$

for all  $h_{G_i}^s$ .

I am looking for a weak sequential equilibrium which is APEX.

**Definition 1.2.1.** A strategy  $\tau$  is APEX if and only if, for all  $\theta$ , there is a finite time  $T^\theta$  such that the actions in  $h_0^\tau$  after  $T^\theta$  repeats the static ex-post Pareto efficient outcome.

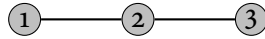
**Definition 1.2.2.** A weak sequential equilibrium  $(\tau^*, \alpha^*)$  is APEX if and only  $\tau^*$  is APEX.

In other words, in an APEX strategy profile, all the Rebels play **revolt** forever after some finite periods if there are more than  $k$  Rebels. Otherwise, all the Rebels play **stay** forever after some finite periods.

### 1.2.3 LEADING EXAMPLE

Example 1 shows that an APEX equilibrium can be founded if  $\delta$  is high enough. In this example, a Rebel (Rebel 2) acts a “coordinator” in order to reveal relevant information to others.

**Example 1.** Suppose there are 3 players in a network. This network is set as,  $G_1 = \{1, 2\}$ ,  $G_2 = \{1, 2, 3\}$ , and  $G_3 = \{2, 3\}$ , as shown in the following graph.



They play the repeated  $k$ -threshold game with  $k = 3$ . Note that after nature moves, player 2 can observe the true state of nature  $\theta$ , whereas neither player 1 or player 3 can do so. Player 2 acts as the coordinator. We can construct an equilibrium which is APEX as follows.

- After nature moves, Rebel 2 chooses **revolt** if he observes  $\theta = (Rebel, Rebel, Rebel)$ , and plays **revolt** in this period. Otherwise, he chooses **stay** and keeps playing **stay** afterwards.

- After nature moves, Rebel 1 and Rebel 3 play **stay**.
- If Rebel 2 chooses **revolt** in the last period, then Rebel 1 (or Rebel 3) plays **revolt** in this period; if Rebel 2 chooses **stay** in the last period, then Rebel 1 (or Rebel 3) continues playing **stay** afterwards.
- If a Rebel deviates from the above strategy, he will play **stay** forever; if a Rebel detects a deviation, he will play **stay** forever.

It is straightforward to check that the above strategies taken together constitute an equilibrium if  $\delta \geq \frac{1}{2}$ . In the equilibrium path, Rebel 1 and Rebel 3 believe that  $\{\theta : \#[Rebels](\theta) \geq 3\}$  with probability one if they observe that Rebel 2 has played **revolt** and believe  $\{\theta : \#[Rebels](\theta) < 3\}$  with probability one if Rebel 2 has played **stay**. Outside of the equilibrium path, Rebels arbitrarily form their beliefs.

In the following sections, I will begin to find an APEX equilibrium in general cases.

### 1.3 EQUILIBRIUM: $k = n$

In Example 1, the construction of an APEX equilibrium relies on some important features. First, as  $k = n$ , Rebel 2 will never play **revolt** if one of his neighbors is Inert. Thus, when Rebel 2 plays **revolt**, it must be the case that all Rebel 2's neighbors are Rebels. Second, Rebel 1 or Rebel 3 can force Rebel 2 to play **revolt** to reveal the true state in the first period as only Rebel 2 knows the true state and Rebel 2's actions can separate the states. Third, as  $k = n$ , a single Rebel's shifting to play **stay** forever is enough to punish a



deviation, and so that the group punishment is not necessary. For instance, if a Rebel did not play **revolt** in the first period at the state  $\theta = (Rebel, Rebel, Rebel)$ , his neighbor can punish him by playing **stay** forever. This punishment is credible because it means that a player who deviates must also play **stay** forever.

I state my result for  $k = n$  case as follows.

**Theorem 1.** *For any  $n$ -person repeated  $k$ -Threshold game with parameter  $k = n$  played in a network, then there is a  $\delta^*$  such that a sequential APEX equilibrium exists whenever  $\delta > \delta^*$ .*

*Proof.* Let a strategy profile,  $\tau^*$ , as follows. After nature moves, a Rebel plays **revolt** if he has no Inert neighbor; a Rebel plays **stay** forever if he has an Inert neighbor. After first period, if a Rebel has not detected a deviation, and if such Rebel observes that his Rebel neighbors play **revolt** continuously in the last periods, he keeps playing **revolt** in the current period; otherwise, he plays **stay** forever. If a Rebel deviates, then he play **stay** forever.

According to  $\tau^*$ , at period  $s$ , if a Rebel has not detected a deviation and if such Rebel observes his Rebel neighbors have played **stay** once in the last periods, he forms belief  $\sum_{\theta: \#[Rebels](\theta) \geq k} \beta_{G_i}^{\pi, \tau^*}(\theta | h_{G_i}^s) = 0$  after period  $s$ , and therefore playing **stay** after period  $s$  is his best response. If a Rebel detects a deviation or he has deviated to play **stay**, playing **stay** is the best response since at least one Rebel will play **stay**.

Since the network is finite, if all players do not deviate, there is a finite time  $t_\theta^s$  such that all Rebels play **revolt** forever if  $\theta \in \{\theta : \#[Rebels](\theta) \geq k\}$ ; and there is a finite time  $t_\theta^f$  such that all Rebels play **stay** forever if  $\theta \in \{\theta : \#[Rebels](\theta) < k\}$ . After  $\max\{t_\theta^s, t_\theta^f\}$ , a Rebel who deviates at most get 0. However, if all Rebels do not deviate,

all Rebels get  $\max\{1, 0\}$  after  $\max\{t_\theta^s, t_\theta^f\}$ . Then, given a period  $s > 0$ , a Rebel will not deviate if  $\sum_{\theta: \#[Rebels](\theta) \geq k} \beta_{G_i}^{\pi, \tau^*}(\theta | h_{G_i}^s) > 0$ . This because, otherwise, he has a loss in his expected continuation payoff as  $\delta^{t_\theta^s} \frac{\sum_{\theta: \#[Rebels](\theta) \geq k} \beta_{G_i}^{\pi, \tau^*}(\theta | h_{G_i}^s)}{1 - \delta}$  after  $t_\theta^s$ . There is a  $0 < \delta < 1$  to let such loss be large enough to impede Rebels deviations.

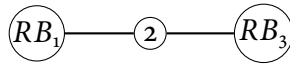
To check if  $\tau^*$  and  $\{\beta_{G_i}^{\pi, \tau^*}(\theta | h_{G_i}^s)\}_{i \in N}$  satisfy full consistency<sup>9</sup>, take any  $0 < \eta < 1$  such that Rebels play  $\tau^*$  with probability  $1 - \eta$ , and play other behavior strategies with probability  $\eta$ . Clearly, when  $\eta \rightarrow 0$ , the belief converges to  $\{\beta_{G_i}^{\pi, \tau^*}(\theta | h_{G_i}^s)\}_{i \in N}$ .  $\square$

*Remark.* Note that the first best cannot be attained in the equilibrium unless the network is complete. Consider the network in Example 1. Player 1's strategy is not contingent on the true state, and therefore players' actions in the first period are not ex-post efficient.

#### 1.4 EQUILIBRIUM: $k < n$

When  $k < n$ , the equilibrium construction for the  $k = n$  case will not work. First, a Rebel still has an incentive to play **revolt** even if an Inert neighbor is present. Second, as any Inert neighbor can only perform one action, neighbors of this type never transmit additional information. We, therefore, require more assumptions in order to obtain an APEX equilibrium. Example 2 shows why additional assumptions are necessary.

**Example 2.** Let  $k = 2$  and let the network be as follows. Assume that  $\theta = (Rebel_1, Inert_2, Rebel_3)$ .



First, since  $k = 2$ , Rebel 1 has incentive to play **revolt** when  $\pi(\{\theta : \theta_3 = Rebel\})$  is high enough and when Rebel 3's strategy is to play revolt. Second, Rebel 1 never learn

---

<sup>9</sup>Krep and Wilson (1982)

$\theta_3$  since Inert 2 cannot reveal information about  $\theta_3$ . Thus, the game is reduced to an incomplete information game without communication. Clearly, an APEX equilibrium does not exist in this case.

In order to get an APEX equilibrium and to avoid the case of Example 2, I define *Strong connectedness* and *Full support on strong connectedness* in Definition 1.4.1 and Definition 1.4.2 respectively.

**Definition 1.4.1. Strong connectedness:** Given  $G$ , a state  $\theta$  has strong connectedness if and only if for every pair of Rebels, there is a path consisting of Rebels to connect them.

**Definition 1.4.2. Full support on strong connectedness:** Given  $G$ ,  $\pi$  has full support on strong connectedness if and only if

$$\pi(\theta) > 0 \Leftrightarrow \theta \text{ has strong connectedness}$$

The goal of this paper is to show that an APEX equilibrium always exists in the  $k < n$  cases when the underlying network is without cycle. I define acyclic network in the following definition.

**Definition 1.4.3.** A network is without (with) cycles if and only if the path from  $i$  to  $j$ , for all  $i \neq j$ , is (is not) unique.

I then state my main theorem as follows.

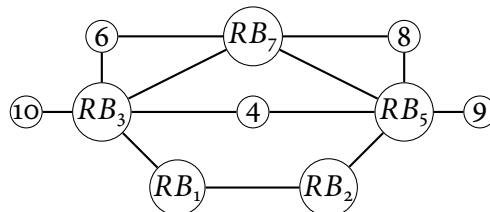
**Theorem 2.** For any  $n$ -person repeated  $k$ -Threshold game with parameter  $k < n$  played in acyclic networks, if  $\pi$  has full support on strong connectedness, then there is a  $\delta^*$  such that an APEX equilibrium exists whenever  $\delta > \delta^*$ .

The equilibrium in Theorem 2 is constructive. I will construct the equilibrium path first and then the in-path and off-path beliefs. I will then determine whether or not there is a strategy profile extending equilibrium path such that the belief system is consistent with every history constituting the equilibrium. I begin with an overview of equilibrium construction and then present an illustration of such construction. An account of the equilibrium in its entirety, together with the omitted proofs, is given in the Appendix A.1.

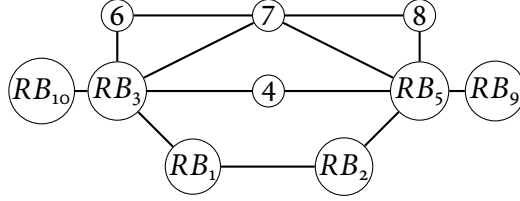
#### 1.4.1 OVERVIEW

Given that the state has strong connectedness, Rebels must find a “language” for communication. The construction of an APEX equilibrium is not trivial because the “dimension” of information is generally larger than the cardinality of Rebels’ own action space. Further, Rebels use several sequences of actions to transmit information. Therefore, it is necessary to track the belief updating in the horizontal time line and to determine whether or not such sequences can constitute an equilibrium. In order to show that Rebels need to communicate with more dimensions of information, it is instructive to compare Example 3 and Example 4.

**Example 3.** Let  $k = 5$  and let the network and the state  $\theta$  be as follows.



**Example 4.** Let  $k = 6$  and let the network and the state  $\theta$  be the following.



In Example 4, there are 6 Rebels, whereas, there are 5 Rebels in Example 3. Suppose that we have a “talking strategy” as follows. Rebel 3 and Rebel 5 report the numbers of Rebels in his neighborhood to Rebel 1 and Rebel 2 respectively. Rebel 1 and Rebel 2 then talk with each other about the combined total number of Rebels. Based on this combined total number of Rebels, Rebel 1 and Rebel 2 collaborate on the decision as whether or not to play **revolt**. According to this talking strategy, however, Rebel 1 and Rebel 2 still do not know how many Rebels are out there. This is because Rebel 3 and Rebel 5 report the same number of Rebel neighbors in both Example 4 and Example 3. Thus, “talking about how many nearby Rebels” is not enough, Rebels have to “talking about the locations of nearby Rebels” in order to construct an APEX strategy.

Moreover, in an APEX equilibrium path, all Rebels must tell whether or not there are more than  $k$  Rebels at certain time. To see this, I give the following lemma.

**Lemma 1.4.1.** *Given  $G, \pi, \delta, k$ . If a weak sequential equilibrium  $\tau^*$  is APEX, then for all  $\theta \in \Theta$ , there is a finite time  $T_i^\theta$  for a Rebel  $i$  such that  $\sum_{\theta: \#[Rebels](\theta) \geq k} \beta_{G_i}^{\pi, \tau^*}(\theta | h_{G_i}^s)$  either  $= 1$  or  $= 0$  whenever  $s \geq T_i^\theta$ .*

The question is how to track the time at which each Rebel knows the relevant information. It should be noted, too, that the higher-order belief constitutes a significant obstacle in our private monitoring setting. To overcome the difficulty of tracking each Rebel’s

learning process, I let Rebels use several “coordination sequences” to let the others know that they have known, that they have known that some other Rebels have known, ..., have known the relevant information.

In my construction, the off-path belief system yields the grim-trigger property. To be more precise, if a Rebel  $i$  detects a deviation at period  $s$ , his off-path belief will be  $\sum_{\theta \in \{\theta: \theta_j = \text{Inert}, j \neq G_i\}} \beta_{G_i}^{\pi, \tau}(\theta | h_{G_i}^{s'}) = 1$  for all  $s' \geq s$ . That is, on this basis, he will believe that all players outside his neighborhood are Inerts, and therefore he will stop updating his belief about relevant information. The consequence is that he will play **stay** forever if fewer than  $k$  Rebel neighbors in his neighborhood.

The equilibrium is constructed through three steps, described in details in the following consecutive three subsections. In the first step, I define the *information hierarchy* to specify which Rebels in  $G$  have to report their information in the equilibrium path. In the second step, I construct the equilibrium path by using binary-**{revolt, stay}** sequences, and determine the belief updating in the path. Finally, I use the grim-trigger-like off-path belief as a punishment schema to impede deviations in the third step.

#### 1.4.2 STEP 1. INFORMATION HIERARCHY IN $G$

The information hierarchy is defined on a network  $G$  immediately after nature chooses a state. I will use the term “node  $i$ ” instead of “player  $i$ ” in this step.

I define information hierarchy by defining  $\{N_i^{-1}, N_i^0, N_i^1, \dots\}$  and  $\{I_i^{-1}, I_i^0, I_i^1, \dots\}$  for each  $i \in N$ , and then define  $\{\leq^0, \leq^1, \leq^2\}$  and  $\{R^0, R^1, R^2, \dots\}$  for each iteration in  $(0, 1, 2, \dots)$ . I also use the term “blocks” to represent the “iterations”.

Given  $\theta$ , the information hierarchy is defined as follows.

- For the **0-block** Denote

$$N_i^{-1} \equiv \{i\}$$

$$I_i^{-1} \equiv \{i\}$$

Then define  $R^0$  as

$$R^0 \equiv [Rebels](\theta) \tag{1.1}$$

- For the **1-block** Denote

$$N_i^0 \equiv G_i$$

$$I_i^0 \equiv G_i \cap R^0$$

Define the set  $\leq^0$  by defining

$$i \in \leq^0 \Leftrightarrow \exists j \in \bar{G}_i [I_i^0 \subseteq N_j^0 \cap R^0] \tag{1.2}$$

Then define  $R^1$  as

$$R^1 \equiv \{i \in R^0 \mid i \notin \leq^0\} \tag{1.3}$$

- For the  $t + 1$ -**block**,  $t \geq 1$  Denote

$$N_i^t \equiv \bigcup_{k \in I_i^{t-1}} G_k$$

$$I_i^t \equiv \bigcup_{k \in G_i \cap R^t} I_k^{t-1}$$

Define the set  $\leq^t$  by defining

$$i \in \leq^t \Leftrightarrow \exists j \in \bar{G}_i [I_i^t \subseteq N_j^t \cap R^0] \quad (1.4)$$

Then define  $R^{t+1}$  as

$$R^{t+1} \equiv \{i \in R^t \mid i \notin \leq^t\} \quad (1.5)$$

In other words,  $i \in R^t$  if and only if (1)  $i$  is a Rebel and (2) at  $t$ -block, for every  $i$ 's neighbor  $k$ ,  $k \neq i$ , there is a  $j \in I_i^{t-1}$ ,  $j \neq k$ ,  $j \neq i$ , who is a Rebel and whose existence is informed to  $i$ , but  $k$  has not been informed that<sup>10</sup>. Intuitively, the  $R^t$ -nodes then have more incentives to report their information in order to let more Rebels acquire the relevant information and then to coordinate actions.

From the above definition, Theorem 3 states that, eventually, there is a  $R^t$ -node who will be informed the true state if the underlying network is acyclic and if the state has strong connectedness. Thus, it is sufficient to reveal the true state by letting  $R^t$ -node in each  $t$ -block iteratively report the information about the existence of Rebels.

**Theorem 3.** *If the network is acyclic and if the state has strong connectedness, then*

$$R^0 \neq \emptyset \Rightarrow \exists t \geq 0 [\exists i \in R^t [I_i^t = R^0]]$$

---

<sup>10</sup>A way to explain information hierarchy is that each node  $i$  is informed the existence of Rebel-nodes,  $I_i^{t-1}$ , by  $i$ 's neighbors who are  $R^t$ -nodes through *cheap talk* at each  $t$ -block.



**Table 1.1:** Notations for sequence of actions

$\bar{N}$	$\equiv$	a non-empty subset of $N$
$x_i$	$\equiv$	player $i$ 's prime-number index
$X_{\bar{N}}$	$\equiv$	$\prod_{j \in \bar{N}} x_j$
$\mathbf{s}$	$\equiv$	<b>stay</b>
$\mathbf{r}$	$\equiv$	<b>revolt</b>
$\langle \rangle$	$\equiv$	a finite binary- $\{\mathbf{s}, \mathbf{r}\}$ sequence
$ \langle \rangle $	$\equiv$	the length of $\langle \rangle$
$\langle \mathbf{stay} \rangle$	$\equiv$	$\langle \mathbf{s}, \dots, \mathbf{s} \rangle$
$\langle \mathbf{revolt} \rangle$	$\equiv$	$\langle \mathbf{r}, \dots, \mathbf{r} \rangle$
$\langle \bar{N} \rangle$	$\equiv$	$\langle \mathbf{s}, \dots, \mathbf{s}, \mathbf{r}, \mathbf{s}, \dots, \mathbf{s} \rangle$
		$\underbrace{\hspace{10em}}_{X_{\bar{N}}}$
$\langle 1 \rangle$	$\equiv$	$\langle \mathbf{s}, \dots, \mathbf{s}, \mathbf{r} \rangle$
		$\underbrace{\hspace{10em}}_1$
$\langle x_i \rangle$	$\equiv$	$\langle \mathbf{s}, \dots, \mathbf{s}, \mathbf{r}, \mathbf{s}, \dots, \mathbf{s} \rangle$
		$\underbrace{\hspace{10em}}_{x_i}$

#### 1.4.3 STEP 2: EQUILIBRIUM STRATEGIES IN THE PATH

In this step, each player in  $G$  is indexed with a distinguished prime number to indicate his “location”. Such indexation is starting from 3. To be more precise, I index each player  $i$  as  $x_i$ , where  $x_i \geq 3$  is a prime number. Since the multiplication of distinguish prime numbers can be uniquely factorized as those numbers, I then use this property to let each Rebel report both the number of his Rebel neighbors and their locations.

Denote  $\langle \rangle$  as a form of finite binary- $\{\mathbf{stay}, \mathbf{revolt}\}$  sequence. Denote  $|\langle \rangle|$  as the length of  $\langle \rangle$ . Denote  $\bar{N} \subset N$  as an non-empty subset of  $N$ . The notations for the forms of sequences are shown in Table 1.1.

The  $\langle \rangle$  and the  $|\langle \rangle|$  will jointly determine the sequences of actions in the equilibrium path. For example, if a sequence takes the form  $\langle 1 \rangle$  and has the length  $|\langle 1 \rangle| = 3$ , then this

sequence is  $\langle \mathbf{s}, \mathbf{s}, \mathbf{r} \rangle$ . Note that the length of a sequence is counted from its end.

In the equilibrium path, two phases—the *reporting period* and the *coordination period*—finitely occur in turns as follows:

$$\underbrace{\langle \text{coordination period} \rangle}_{o\text{-block}} \underbrace{\langle \text{reporting period} \rangle \langle \text{coordination period} \rangle}_{1\text{-block}} \dots$$

That is, after nature has chosen a state, all the Rebels start with the o-block, then enter to the 1-block, ..., and so on. The o-block has only one period, coordination period. The  $t$ -blocks,  $t \geq 1$  has two periods—the reporting period followed by the coordination period. The length of each phase in each block is both finite and commonly known.

If a sequence of actions is meant to be played in the reporting period (*resp.* the coordination period), I refer to it as a *reporting message* (*resp.* *coordination message*). In reporting period in each  $t$ -block ( $t \geq 1$ ), the Rebels play the sequences defined in Table 1.2. In coordination period in each  $t$ -block ( $t \geq 0$ ), the Rebels play the sequences defined in Table 1.4. After the coordination period in each  $t$ -block ( $t \geq 0$ ), players either (1) start to repeatedly play some certain actions, or (2) enter to the reporting period in the  $t + 1$ -block.

I begin to provide a detailed description of the reporting messages and the coordination messages in the following subsections.

### 1.4.3.1 REPORTING MESSAGES IN REPORTING PERIOD

The reporting period in the  $t$ -block is denoted as  $RP^t$ . Denote  $|RP^t|$  as the total number of periods in  $RP^t$ <sup>11</sup>. In the equilibrium path, the sequence of actions played in the  $RP^t$  is with length  $|RP^t|$  and has to follow one kind of the forms listed Table 1.2. Any other sequence will be considered as a deviation.

**Table 1.2:** Reporting messages

Reporting Messages
$\langle \mathbf{stay} \rangle$
$\langle I_i^{t-1} \rangle$
$\langle 1 \rangle$

Table 1.3 shows that the belief formed by Rebel  $j$  after observing his neighbor  $i$ 's reporting messages in the equilibrium path.

**Table 1.3:**  $j$ 's belief updating after observing  $i$ 's reporting messages in the reporting period in  $t$ -block

$i$ plays	the event that $j \in \tilde{G}_i$ believes with probability one
$\langle \mathbf{stay} \rangle$	$i \notin R^t$
$\langle I_i^{t-1} \rangle$	$i \in R^t$ and $l \in [Rebel](\theta)$ if $l \in I_i^{t-1}$
$\langle 1 \rangle$	$i \in R^t$ and $i$ has known $\#[Rebels](\theta) \geq k - 1$

According to Table 1.3, after the reporting period, a Rebel can identify the players who are  $R^t$ . The consequence is that, if a Rebel  $j$  has observed that all of his neighbors play  $\langle \mathbf{stay} \rangle$ , then he is sure that  $\#[Rebels](\theta) < k$  if  $\#I_j^{t-1} < k$ <sup>12</sup>.

<sup>11</sup>To be more precise,  $|RP^t| = \prod_{i \in N} x_i$ , where  $x_i$  is the prime number index of player  $i$

<sup>12</sup>Recall that  $R^t$  are those Rebels who have been informed of the existence of some Rebels, but whose neighbors has not been informed likewise.

The important feature here is that a player can play a special sequence— $\langle 1 \rangle$ —in the equilibrium path. This special sequence serves as a signal to indicate a *pivotal player* in  $RP^t$ —a player who is certain that he will acquire the the relevant information given others’ truthful reporting immediately after  $RP^t$ . I elaborate this issue as follows.

PIVOTAL PLAYERS IN  $RP^t$

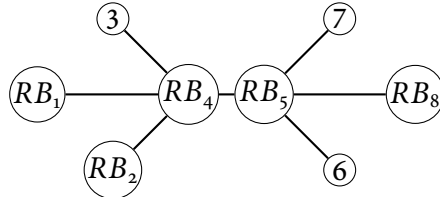
**Definition 1.4.4** (Pivotal players in  $RP^t$ ). *Let  $\theta \in \Theta$  be given. A player is pivotal in  $RP^t$  if he is certain that he can tell whether or not  $\#[Rebels](\theta) < k$  immediately after  $RP^t$  given that others report truthful in  $RP^t$ .*

There are two kinds of pivotal players in  $RP^t$ : (1), players who are certain that they can learn the true state, and (2), players who can only learn the relevant information.

For the first kind of pivotal players, we may consider the following two examples.

**Example 5. Free Rider Problem**

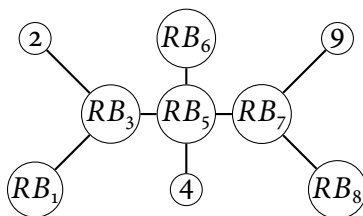
Let  $k = 5$  and assume that there are message  $\langle M_4 \rangle, \langle M_5 \rangle$  for Rebel 4, 5 respectively. To simplify the analysis, let us assume that the game is played from the 1-block (by discarding the strategies in the 0-block and starting the game from the reporting period). Further, assume that Rebels will play **revolt** forever after observing that  $\langle M_4 \rangle$  or  $\langle M_5 \rangle$  is played once by Rebel 4 or 5 right after reporting period; otherwise they will play **stay** forever. Let  $G$  be as follows.



Note that Rebel 4 and Rebel 5 are  $R^1$  members. Let  $\langle \rangle_4$  and  $\langle \rangle_5$  be the sequences of actions they may use to report the number of Rebel neighbors. If Rebel 5 report truthfully, then Rebel 4 will not report truthfully by arranging the timings in which he plays **revolt**. Since Rebel 4 can use  $\langle M_4 \rangle$  to initialize the coordination, such deviation is profitable. The same situation prevails for Rebel 5, whereby Rebel 4 and Rebel 5 will not report truthfully.

In the above example, two sources produces a free rider problem. One source is that there are coordination messages that can initiate coordination regardless how the reporting messages are played. The other source is that Rebel 4 and Rebel 5 are the pivotal players who can learn the true state. To see the later source more clearly, we may consider the following Example 6.

**Example 6. Pivotal player: Case 1** Let  $k = 6$  and suppose that there are message  $\langle M_3 \rangle, \langle M_5 \rangle, \langle M_7 \rangle$  for Rebel 3,5,7 to initiate a coordination respectively. Let the game be played from the 1-block as Example 5. Further, let's suppose that Rebels will play **revolt** forever after observing that  $\langle M_3 \rangle, \langle M_5 \rangle$ , or  $\langle M_7 \rangle$  is played once in two periods immediately after this reporting period; otherwise all these Rebels will play **stay** forever. Let  $G$  be as follows.



Note that Rebel 3, 5, 7 are  $R^1$  members. In contrast to Example 5, although Rebel 3, 7 can use their coordination messages to initiate coordination, they still have incentives to report truthfully. This is because they are not pivotal. Since the coordination to **revolt**

has to be initiated immediately after this reporting period, they have incentives to report truthfully to Rebel 5.

Rebel 5, however, has no incentive to report truthfully since he is a pivotal player who can learn the true state.

From the discussions in Example 5 and Example 6, a way to deal with the free rider problem is to assign one of those pivotal players who constitute this problem as a *free rider*. If the network is acyclic, the free rider problem can be identified before the game enters to  $RP^t$ , as shown in Lemma 1.4.2. To be more precise, first define  $TR_{ij}$  as a tree rooted in  $i$  and spanning from  $j \in \bar{G}_i$  as in Definition 1.4.5.

**Definition 1.4.5.**  $TR_{ij} \equiv \{l \in N : \text{there is a unique path } \{l, \dots, j, i\} \text{ from } l \text{ to } i \text{ through } j\}$

Then, define  $C^t$  to be a set containing  $R^t$ -nodes such that, for all  $i \in C^t$ , there are no possible Rebel nodes at  $t$ -block which connects to  $i$  by a path consisting of three or more nodes:

$$C^t = \{i \in R^t : \nexists j \in R^{t-1} \cap \bar{G}_i [\exists l, l' \in TR_{ij} [l \in N_j^{t-1} \setminus I_i^{t-1} \text{ and } l' \in \bar{G}_i]]\}$$

In other words,  $C^t$  is the set of those nodes that can learn the true state immediately after  $RP^t$ . In Example 5, for instance, Rebel 4 and Rebel 5 are  $C^1$  nodes. In Example 6, Rebel 5 is a  $C^1$  node.

The following two lemmas are useful to identify the free rider problem in  $RP^t$  before the game enters to  $RP^t$ .

**Lemma 1.4.2.** <sup>13</sup> *If the network is acyclic, and if the state has strong connectedness, then for each  $t$ -block,*

$$0 \leq |C^t| \leq 2$$

*. Moreover, suppose there are two nodes in  $C^t$ , then they are each other's neighbor.*

**Lemma 1.4.3.** *If the network is acyclic, and if the state has strong connectedness, then for each  $t$ -block*

$$i \in C^t \Rightarrow \text{there is no possible Rebel node outside of } \bigcup_{k \in N_i^{t-1}} G_k$$

By Lemma 1.4.2,  $C^t$  nodes are each other's neighbor (if there are two  $C^t$  nodes). By Lemma 1.4.3, it is straightforward to show that  $C^t$  nodes can identify themselves.<sup>14</sup> In order to solve the free rider problem in which there are multiple  $C^t$  nodes in  $RP^t$ , we can let the node in  $C^t$  who has smallest prime index to be the free rider, and then solve the problem.

For the second kind of pivotal players, who can only learn the relevant information right after  $RP^t$ , we may consider the following example.

**Example 7. Pivotal player: Case 2** Let  $k = 6$ . Again, assume that there are coordination message  $\langle M \rangle$ s for Rebels. Let the game be played from the 1-block as Example 5. Let's assume that Rebels will play **revolt** forever after observing that  $\langle M \rangle$  is played once in

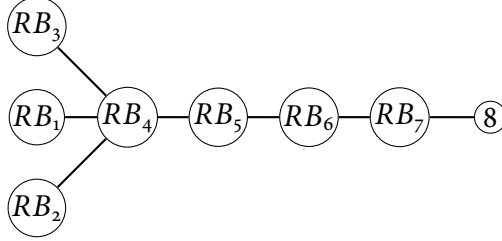
---

<sup>13</sup>Generally, this property does not hold if a network is cyclic.

<sup>14</sup>To be more precise, they identify themselves by the following procedure. First, a  $C^t$  node,  $j$ , assumes that one of his  $R^{t-1}$  neighbor,  $i$ , is a  $R^t$ -node. Second, he check if  $i$  is in  $C^t$  by checking the definition of  $C^t$ . Third, if  $i$  is identified as a  $C^t$  node,  $i$  is the only  $C^t$  node other than  $j$  (by Lemma 1.4.2). Finally,  $j$  assumes that  $i$  will do the same procedure to identify him. Since  $j$  himself is a  $C^t$ -node,  $i$  must be able to identify him if  $i$  is a  $C^t$ -node, and thus both  $C^t$ -nodes  $i$  and  $j$  can identify each other.

four periods immediately after reporting period; otherwise they will play **stay** forever.

Let  $G$  be as follows.



In this case, there is no Rebel in  $C^1$ . Rebel 4, nevertheless, will deviate from reporting  $\langle I_4^o \rangle$ . Note that Rebel 4 has already known there are 5 Rebels in this world, and therefore he knows that the coordination to **revolt** can be initiated by him if he is informed the existence of one more Rebels. Moreover, if no more Rebels exist, the coordination to **stay** can be also initiated by him. Since he can use the message  $\langle M \rangle$  to initiate the coordination, his deviation is profitable given others' truthful reporting.

In a summary, the sequence  $\langle 1 \rangle$  is introduced in order to let the pivotal players “identify” themselves. In the Appendix A.2.1, I can show that the pivotal players in  $RP^t$  are those Rebels who are either  $C^t$  nodes or have already known there are  $k - 1$  Rebels in the equilibrium path. The equilibrium construction will enforce the pivotal players to play  $\langle 1 \rangle$  in the equilibrium path, and therefore the belief updating after observing  $\langle 1 \rangle$  is as Table 1.3 shows.

#### 1.4.3.2 COORDINATION MESSAGES IN COORDINATION PERIOD

Ignorance on the part of any given Rebel of previous reporting messages after observing a coordination message  $\langle M \rangle$  may result in untruthful reporting as the above Example 5,



6, and 7 show. The sequence  $\langle 1 \rangle$  is introduced in order to tackle this issue. However, it is evident that the concatenation of these two messages,  $\langle 1 \rangle \langle M \rangle$ , is another coordination message itself. To be more precise,  $\langle \langle \mathbf{s}, \mathbf{r} \rangle \langle M \rangle \rangle$  is another coordination message that has resulted from truncating previous actions in  $\langle 1 \rangle$  and concatenating the remaining actions to  $\langle M \rangle$ . If players' continuation behaviors after they observe  $\langle \langle \mathbf{s}, \mathbf{r} \rangle \langle M \rangle \rangle$  are independent from the previous reporting messages, then the issue of untruthful reporting is not solved.

In this section, I discuss the coordination messages. And in the equilibrium construction, I let players update their belief be not only contingent on the coordination messages but also on the previous reporting messages in the equilibrium path.

I depict the “structure” in the coordination period. There are three divisions in the coordination period and there are several sub-blocks in each division. In  $t = 0$  block, the structure is

$$\begin{array}{ccc} \text{1st division} & \text{2nd division} & \text{3rd division} \\ \underbrace{\langle \underbrace{\langle \cdot \rangle}_{1 \text{ sub-block}} \rangle}_{1 \text{ sub-block}} & \underbrace{\langle \underbrace{\langle \cdot \rangle}_{1 \text{ sub-block}} \rangle}_{1 \text{ sub-blocks}} & \underbrace{\langle \langle \cdot \rangle \cdots \langle \cdot \rangle \rangle}_{n \text{ sub-blocks}} \end{array}$$

; in  $t > 0$  blocks, the structure is

$$\begin{array}{ccc} \text{1st division} & \text{2nd division} & \text{3rd division} \\ \underbrace{\langle \langle \cdot \rangle \cdots \langle \cdot \rangle \rangle}_{n \text{ sub-blocks}} & \underbrace{\langle \langle \cdot \rangle \cdots \langle \cdot \rangle \rangle}_{t+1 \text{ sub-blocks}} & \underbrace{\langle \langle \cdot \rangle \cdots \langle \cdot \rangle \rangle}_{n \text{ sub-blocks}} \end{array}$$

, where  $n = \#N$ .

In the  $t$ -block, denote  $CD_{m,q}^t$  as the  $m$  sub-block in  $q$  division and denote  $|CD_{m,q}^t|$  as the total number of periods in  $CD_{m,q}^t$ <sup>15</sup>. The sequence of actions played in the equilibrium

<sup>15</sup>To be more precise, for all  $t > 1$ ,  $|CD_{1,1}^t| = \dots = |CD_{n,1}^t| = \max\{x_1, \dots, x_n\}$ , where  $\{x_1, \dots, x_n\}$  is the set of players' prime number indexes;  $|CD_{1,2}^t| = \dots = |CD_{t+1,2}^t| = \max\{x_1, \dots, x_n\}$ , where  $\{x_1, \dots, x_n\}$  is the set

path takes a form of sequences listed in Table 1.4, and is with length  $|CD_{m,q}^t|$  for all  $t \geq 0, m \geq 1, q \geq 1$ .

**Table 1.4:** Coordination messages

Coordination messages
$\langle x_i \rangle$
$\langle \mathbf{stay} \rangle$
$\mathbf{r}$
$\mathbf{s}$

Since the o-block has simpler structure, I will focus on introducing players' behaviors in the coordination period in  $t > 0$  block in the following paragraphs, while the Appendix A.2.1 shows the equilibrium path in  $t = 0$  block<sup>16</sup>.

THE EQUILIBRIUM PATH IN  $(CD_{1,1}^t, \dots, CD_{n,1}^t), t > 0$

Table 1.5 shows the belief updating formed by a Rebel  $j$  after he observes  $i$ 's behavior after  $CD_{1,1}^t$  in the equilibrium path. According to Table 1.5, Rebel  $j$  can tell whether or not  $\#[Rebels](\theta) < k$  after  $CD_{1,1}^t$  for some  $t > 0$ -block. As Table 1.6 and Table 1.7 show, in order to transmit the information about whether or not they have learn  $\#[Rebels](\theta) < k$ , Rebels will play  $\langle x_i \rangle$  unless they observe  $\langle \mathbf{stay} \rangle$  in  $CD_{2,1}^t$  to  $CD_{n,1}^t$ . The information about  $\#[Rebels](\theta) < k$  will then be transmitted across all players after  $CD_{n,1}^t$ .

Note that a Rebel  $j$  will play **stay** forever if he believes that  $\#[Rebels](\theta) < k$  is with

---

of players' prime number indexes;  $|CD_{1,3}^t| = \dots = |CD_{n,3}^t| = 1$ .

<sup>16</sup>In the equilibrium path (in the Appendix A.2.1), all Rebels will play **revolt** after o-block if there is a Rebel who has  $k$  or more Rebels neighbors.

probability one. Thus, the sequence  $\langle \mathbf{stay} \rangle$  played in  $CD_{1,1}^t$  to  $CD_{n,1}^t$  is interpreted as the coordination message to initiate the coordination to **stay**.

**Table 1.5:**  $j$ 's belief updating after  $CD_{1,1}^t$  by observing  $i$ 's previous actions ( $t > 0$ )

In $RP^t$	In $CD_{1,1}^t$	
$i$ plays	$i$ plays	The events that $j \in \bar{G}_i$ believe with probability one
$\langle \mathbf{stay} \rangle$	$\langle x_i \rangle$	$i \notin R^t$
$\langle I_i^{t-1} \rangle$	$\langle \mathbf{stay} \rangle$	$\#[Rebels](\theta) < k$
$\langle I_i^{t-1} \rangle$	$\langle x_i \rangle$	$i \in R^t$
$\langle 1 \rangle$	$\langle \mathbf{stay} \rangle$	$\#[Rebels](\theta) < k$
$\langle 1 \rangle$	$\langle x_i \rangle$	$\#[Rebels](\theta) \geq k$

**Table 1.6:** In-path strategies in  $RP^t$ ,  $CD_{1,1}^t$ , and  $CD_{2,1}^t$  ( $t > 0$ )

In $RP^t$	In $CD_{1,1}^t$	In $CD_{2,1}^t$
$i$ plays	$i$ plays	$j \in \bar{G}_i$ plays
$\langle \mathbf{stay} \rangle$	$\langle x_i \rangle$	$\langle x_i \rangle$
$\langle I_i^{t-1} \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$
$\langle I_i^{t-1} \rangle$	$\langle x_i \rangle$	$\langle x_i \rangle$
$\langle 1 \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$
$\langle 1 \rangle$	$\langle x_i \rangle$	$\langle x_i \rangle$

THE EQUILIBRIUM PATH IN  $(CD_{1,2}^t, \dots, CD_{t+1,2}^t)$ , GIVEN  $t > 0$

After  $CD_{n,1}^t$  and in  $CD_{1,2}^t$ , Rebels start to determine whether or not the coordination to **revolt** can be initiated. The coordination message to initiate the coordination to **revolt** is  $\langle \mathbf{stay} \rangle$  as Table 1.8 shows. The key feature here is that  $\langle \mathbf{stay} \rangle$  is a coordination mes-

**Table 1.7:** In-path strategies in  $CD_{m,1}^t$ , where  $m \geq 2$  ( $t > 0$ )

In $CD_{m,1}^t, m \geq 2$	In $CD_{m+1,1}^t, m \geq 2$
$i$ plays	$j \in \bar{G}_i$ plays
$\langle x_i \rangle$	$\langle x_i \rangle$
$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$

sage to initiate the coordination to **revolt** only if  $\langle I_i^{t-1} \rangle$  or  $\langle 1 \rangle$  has been played in  $RP^{t17}$ . Although this sequence incurs no expected cost, initiating the coordination to **revolt** by this sequence is “not free” since it requires the Rebels to play **revolt** in the previous reporting period in order to initiate the coordination to **revolt**. Since the highest continuation payoff contingent on  $\theta \in \{\theta : \#[Rebels](\theta) \geq k\}$  is the coordination to **revolt**, players then have incentive to play **revolt** in the previous reporting period.

After  $CD_{1,2}^t$ , and from  $CD_{2,2}^t$  to  $CD_{t+1,2}^t$ , Rebels start to transmit the information about whether or not they have learn that  $\#[Rebels](\theta) \geq k$ . According to Table 1.9 and Table 1.10, they will play  $\langle \mathbf{stay} \rangle$  unless they observe someone play  $\langle x_i \rangle$ . After  $CD_{t+1,1}^t$ , the information about  $\#[Rebels](\theta) \geq k$  will be transmitted across at least  $k$  Rebels.

THE EQUILIBRIUM PATH IN  $(CD_{1,3}^t, \dots, CD_{n,3}^t)$ , GIVEN  $t > 0$

The game finally enters to  $CD_{1,3}^t$ . In this period, those  $k$  Rebels who have learn that  $\#[Rebels](\theta) \geq k$  will start to play **revolt** forever. Furthermore, this is the first period in which a Rebel may get positive expected payoff by playing **revolt** (in the equilibrium path). From  $CD_{2,3}^t$  to  $CD_{n,3}^t$ , other Rebels start to transmit this information to all Rebels

<sup>17</sup> Although  $\langle \mathbf{stay} \rangle$  is also the coordination message to initiate the coordination to **stay** in  $CD_{1,1}^t$  to  $CD_{n,1}^t$ , Rebels are not confused about it.

**Table 1.8:**  $j$ 's belief updating after  $CD_{1,2}^t$  by observing  $i$ 's previous actions ( $t > 0$ )

In $RP^t$	In $CD_{1,1}^t$	In $CD_{1,2}^t$	The events $j$ believe with probability one
$i$ plays	$i$ plays	$i$ plays	
$\langle \mathbf{stay} \rangle$	$\langle x_i \rangle$	$\langle \mathbf{stay} \rangle$	$i \notin R^t$
$\langle I_i^{t-1} \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$	$\#[Rebels](\theta) < k$
$\langle I_i^{t-1} \rangle$	$\langle x_i \rangle$	$\langle \mathbf{stay} \rangle$	$\#[Rebels](\theta) \geq k$
$\langle I_i^{t-1} \rangle$	$\langle x_i \rangle$	$\langle x_i \rangle$	$i \in R^t$
$\langle 1 \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$	$\#[Rebels](\theta) < k$
$\langle 1 \rangle$	$\langle x_i \rangle$	$\langle \mathbf{stay} \rangle$	$\#[Rebels](\theta) \geq k$

**Table 1.9:** In-path strategies in  $RP^t$ ,  $CD_{1,1}^t$ ,  $CD_{1,2}^t$ , and  $CD_{2,2}^t$  ( $t > 0$ )

In $RP^t$	In $CD_{1,1}^t$	In $CD_{1,2}^t$	In $CD_{2,2}^t$
$i$ plays	$i$ plays	$i$ plays	$j \in \bar{G}_i$ plays
$\langle \mathbf{stay} \rangle$	$\langle x_i \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$
$\langle I_i^{t-1} \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$
$\langle I_i^{t-1} \rangle$	$\langle x_i \rangle$	$\langle \mathbf{stay} \rangle$	$\langle x_i \rangle$
$\langle I_i^{t-1} \rangle$	$\langle x_i \rangle$	$\langle x_i \rangle$	$\langle \mathbf{stay} \rangle$
$\langle 1 \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$	$\langle \mathbf{stay} \rangle$
$\langle 1 \rangle$	$\langle x_i \rangle$	$\langle \mathbf{stay} \rangle$	$\langle x_i \rangle$

in order to coordinate to **revolt**. Table 1.12 shows players' behavior from  $CD_{2,3}^t$  to  $CD_{n,3}^t$ .

#### 1.4.4 STEP 3: OFF-PATH BELIEF

Whenever Rebel  $i$  detects a deviation at period  $s$ , he forms the following belief:

$$\sum_{\theta \in \{\theta: \theta_j = \text{Inert}, j \notin G_i\}} \beta_{G_i}^{\pi, \tau}(\theta | h_{G_i}^s) = 1, \text{ for all } s' \geq s \quad (1.6)$$

. Thus, if  $\#I_i^o < k$ , he will play **stay** forever. This off-path belief serves as a grim trigger.

**Table 1.10:** In-path strategies in  $CD_{m,2}^t$ , where  $m \geq 2$  ( $t > 0$ )

In $CD_{m,2}^t, m \geq 2$	In $CD_{m+1,2}^t, m \geq 2$
$i$ plays	$j \in \tilde{G}_i$ plays
$\langle x_i \rangle$	$\langle x_i \rangle$
<b><math>\langle \text{stay} \rangle</math></b>	<b><math>\langle \text{stay} \rangle</math></b>

**Table 1.11:** In-path strategies in  $CD_{1,3}^t, t > 0$

In $CD_{m,2}^t, 1 \leq m \leq t+1$	In $CD_{1,3}^t$
$i$ has played	$j \in \tilde{G}_i$ plays
$\langle x_i \rangle$	<b>r</b>
Otherwise	<b>s</b>

**Table 1.12:** In-path strategies after  $CD_{m,3}^t$ , where  $m \geq 2, t > 0$

#### 1.4.5 SKETCH OF THE PROOF FOR THEOREM 2

I have provided the Rebels' behavior and their belief updating in my constructed equilibrium path in Table 1.3, Table 1.5, and Table 1.8. The following lemma shows that such equilibrium path constitutes an APEX.

**Lemma 1.4.4.** *For any  $n$ -person repeated  $k$ -Threshold game with parameter  $k \leq n$  played in an acyclic network, if  $\pi$  has full support on strong connectedness, then there exists an equilibrium path that is APEX.*

I sketch the proof for Theorem 2 as follows. First, I use the off-path belief to prevent players from making detectable deviations, such as deviating from playing the specified forms of sequences that are listed in Table 1.2 or 1.4. Then I argue that any undetectable deviation made by a Rebel before he learns the relevant information,  $\#[Rebels](\theta) \geq k$

In $CD_{m,3}^t, m \geq 2$	In $CD_{m+1,3}^t, m \geq 2$
$i$ plays	$j \in \bar{G}_i$ plays
<b>r</b>	<b>r</b>
<b>s</b>	<b>s</b>

or  $\#[Rebels](\theta) < k$ , will reduce his own expected continuation payoff. To see this, we may consider the case in which a Rebel wants to mimic pivotal plays' behaviors by sending  $\langle 1 \rangle$  in a reporting period. According to Table 1.5 and Table 1.8, his neighbors' continuation playing after observing  $\langle 1 \rangle$  is to play **stay** forever or to play **revolt** forever. But then all of his neighbors will repeat the same action afterward. Hence, the Rebel cannot get any information from which he can determine whether or not  $\#[Rebels](\theta) < k$ . When  $\delta$  is high enough, he can get a better continuation payoff by staying in the path in which he can learn the relevant information (by Lemma 1.4.1). To be more precise, by staying in the path, his static payoff eventually achieves the maximum static payoff as 1 when  $\#[Rebels](\theta) \geq k$ , and achieves the maximum static payoff as 0 when  $\#[Rebels](\theta) < k$ <sup>18</sup>.

#### 1.4.6 DISCUSSION

##### 1.4.6.1 VARIATION: PAYOFF AS SIGNALS

The hidden payoff assumption can be relaxed without change the main result. It is useful to consider a situation in which the static payoff not only depends on players' joint efforts but also on some random shocks, says the weather.<sup>19</sup> To be more precise, there is a public signal  $y \in \{y_1, y_2\}$  generated by Rebels' actions. Let Rebel  $i$ 's payoff function be

<sup>18</sup>Claim A.2.4 in the Appendix A.2.1 shows this argument

<sup>19</sup>e.g., [Shadmehr and Bernhardt, 2011]

$u_{Rebel}(a_{Rebel_i}, y)$ , and let  $u_{Rebel}(\mathbf{stay}, y_1) = u_{Rebel}(\mathbf{stay}, y_2) = u_o$ . The distribution of  $y_1$  and  $y_2$  is

$$\begin{aligned} p_{1s} &= \Pr(y = y_1 | \#\mathbf{revolt} \geq k) \\ p_{1f} &= \Pr(y = y_1 | \#\mathbf{revolt} < k) \\ p_{2s} &= \Pr(y = y_2 | \#\mathbf{revolt} \geq k) \\ p_{2f} &= \Pr(y = y_2 | \#\mathbf{revolt} < k) \end{aligned}$$

such that

$$p_{1s}u_{Rebel}(\mathbf{revolt}, y_1) + p_{2s}u_{Rebel}(\mathbf{revolt}, y_2) > u_o > p_{1f}u_{Rebel}(\mathbf{revolt}, y_1) + p_{2f}u_{Rebel}(\mathbf{revolt}, y_2) \quad (1.7)$$

and

$$1 > p_{1s} > 0, 1 > p_{2s} > 0, p_{1f} = 1 - p_{1s}, p_{2f} = 1 - p_{2s} \quad (1.8)$$

Equation 1.7 is a generalization of the  $k$ -threshold game. Equation 1.8 is a full support assumption on signal  $y$ .

If Equation 1.8 holds, we can construct exactly the same equilibrium strategy by ignoring the noisy signal  $y$ . To see this, we can check the equilibrium path constructed in the previous sections. According to Table 1.2 and Table 1.4, given a period  $s$  before some Rebels play  $\langle 1 \rangle$ , there is at most one Rebel who plays action **revolt**. Since that, the signal  $y$  is not relevant before some Rebels play  $\langle 1 \rangle$ . We then check if a Rebel wants to play  $\langle 1 \rangle$  in order to get additional information coming from  $y$ . However, playing  $\langle 1 \rangle$  will initiate either the coordination to **stay** or the coordination to **revolt** as Table 1.5 and Table 1.8



shows. After a coordination is initiated, a Rebel can not get additional information to learn the relevant information. This is because the signal  $y$  is noisy, and Rebels' actions will repeat. By the same argument in Claim A.2.4 (in the Appendix A.2.1), a Rebel is better to stay in the equilibrium path.

If Equation 1.8 does not hold, says  $p_{1s} = p_{2f} = 1$ , then the signal  $y$  is not noisy, and therefore the strategies constructed in the previous section is no longer an equilibrium. However, another APEX equilibrium can be constructed by letting all Rebels play **revolt** in the first period, and then keep playing **revolt** or **stay** contingent on the signals  $y = y_1$  or  $y = y_2$ .

#### 1.4.6.2 VARIATION: REBELS WITH DIFFERENT LEVELS OF EFFORTS

We may also consider a model in which players contribute different levels of efforts to a collective action. Let the set of states of nature be  $\hat{\Theta} = \Theta \times \Xi$ , where  $\Theta = \{Rebel, Inert\}^n$  and  $\Xi = \{1, 2, \dots, k\}^n$ . Let  $\hat{\theta} = (\theta, e)$  be a state of nature. After  $\hat{\theta}$  is realized, a player  $i$  will hold an endowment  $e_i$ , where  $e_i \in \{1, 2, \dots, k\}$ . The payoff structure is modified as the following.

1.  $u_{Rebel_i}(a_{Rebel_i}, a_{-\theta_i}) = b_i$  if  $a_{Rebel_i} = \mathbf{revolt}$  and  $\sum_{j:a_{\theta_j}=\mathbf{revolt}} e_j \geq k$
2.  $u_{Rebel_i}(a_{Rebel_i}, a_{-\theta_i}) = -e_i$  if  $a_{Rebel_i} = \mathbf{revolt}$  and  $\sum_{j:a_{\theta_j}=\mathbf{revolt}} e_j < k$
3.  $u_{Rebel_i}(a_{Rebel_i}, a_{-\theta_i}) = 0$  if  $a_{Rebel_i} = \mathbf{stay}$
4.  $u_{Inert_i}(a_{Inert_i}, a_{-\theta_i}) = 1$  if  $a_{Inert_i} = \mathbf{stay}$

After  $\hat{\theta}$  is realized, players repeatedly play the above game in a network  $G$ . To see that the strategies constructed in previous section is still an equilibrium, we can transform

$(G, \hat{\Theta})$  to  $(G', \hat{\Theta}')$ , where each player  $i$  is attached with  $\#e_i$  different players in  $G'$ , and  $\hat{\Theta}' = \Theta \times \{1\}^n$ .

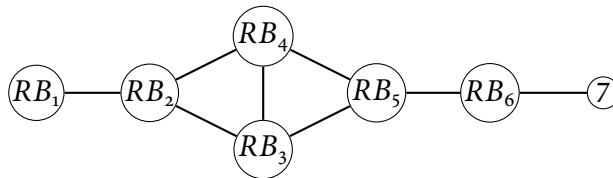
### 1.4.6.3 VARIATION: NETWORKS WITH CYCLES

The prime indexing can deal with potential free problems when players play the repeated  $k$ -threshold game in a cyclic network. We may consider the following example.

**Example 8.** Let  $k = 6$  and let  $\theta$  and  $G$  be the following. In this network, Rebel 3 and Rebel 4 have the same information

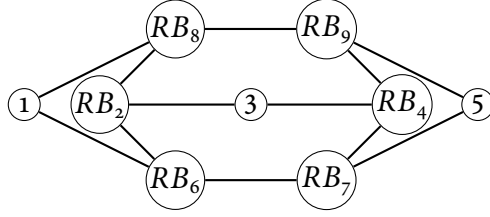
$$I_3^1 = I_4^1 = \{RB_1, RB_2, RB_3, RB_4, RB_5\}$$

. If there is no punishment, Rebel 3 (or Rebel 4) may shirk and deviate from truthfully reporting  $\langle I_3^1 \rangle$  (or  $\langle I_4^1 \rangle$ ) at a reporting period if Rebel 4 (or Rebel 3) can reports truthfully. But this kind of deviation can be detected by Rebel 5 (or Rebel 2) since  $I_3^1$  should be equal to  $I_4^1$ .

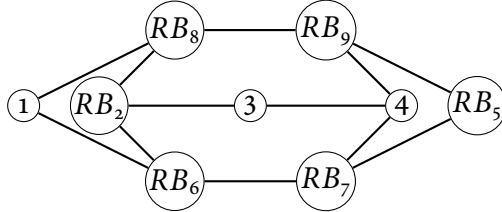


However, there is another free rider problem that is hard to solve. Remind that, when the network is acyclic, the free rider problem is solved by selecting a player as a free rider before the game enters to the reporting period. In cyclic network, we may need more elaborations to select a free rider to solve the free rider problem. Let's consider the Example 9.

**Example 9.** Let  $k = 6$ . Suppose the network and  $\theta$  is as follows.



Let's assume that players follow the equilibrium path constructed in the previous section, and assume that they are in the end of 1-block. In such case, Rebel 2 has been informed that  $I_2^1 = \{RB_2, RB_6, RB_8, RB_9, RB_7\}$ , Rebel 4 has been informed that  $I_4^1 = \{RB_4, RB_7, RB_9, RB_8, RB_6\}$ , and so on. One more round of reporting period will let Rebels 2,6,7,4,9,8 know the true state  $\theta$ , and therefore Rebels 2,6,7,4,9,8 are all pivotal players who constitute a free rider problem (as Example 5). We may select a player to be a free rider, says Rebel 4 is selected, before the game enters to the reporting period in 2-block. However, this selection is ex-post. From the point of players' view, the state could be  $\theta' \neq \theta$  as the following.



In  $\theta'$ , player 4 is an Inert and therefore not a pivotal Rebel, and hence he can not be selected as a free rider. We then need another rule in order to select a free rider during the game is played in the reporting period in the 2-block.

As Example 5 or Example 9 show, free rider problems occur if a free rider has not yet been selected before the game enters to a reporting period. In cyclic networks, this prob-

lem is considerably more difficult to solve. Unfortunately, the solution is still infeasible in this paper.

I leave a conjecture in this paper and end this section.

**Conjecture 1.4.1.** *For any  $n$ -person repeated  $k$ -Threshold game with parameter  $k < n$  played in any network, if  $\pi$  has full support on strong connectedness, then there exists a  $\delta^*$  such that an APEX equilibrium exists whenever  $\delta > \delta^*$ .*

## 1.5 CONCLUSION

I model a coordination game and illustrate the learning processes generated by strategies in a sequential equilibrium and answer the question proposed in the beginning: what kind of networks can conduct coordination in a collective action game with information barrier. In the equilibrium, players transmit the relevant information by encoding such information by their actions in the time horizontal line. Since there is an expected cost in coding information, potential free rider problems may occur to impede the learning process. When the networks are without cycle, players can always learn the underlying relevant information and conduct the coordination only by their actions. However, what kinds of equilibrium strategies can constitute a learning process to learn the relevant information in cyclic networks still remains to be answered.

The construction of communication protocol exploits the assumption of finite type space and the finite threshold. Since the relevant information has been parameterized as a threshold, players can acquire this information by jointly incrementally reporting their own private information. The major punishment to keep players staying in the equilibrium path is then the joint shifting to play same actions as the stopping to update their

information. The threshold model seems a general model in proofing that a communication protocol not only leads a learning process but also constitutes an equilibrium to reveal the relevant information in finite time.

Existing literatures in political science and sociology have recognized the importance of social network in influencing individual's behavior in participating social movements, e.g., [Passy, 2003][McAdam, 2003][Siegel, 2009]. This paper views networks as routes for communication where rational individuals initially have local information, and they can influence nearby individuals by taking actions. Such influence may take long time to travel across individuals, and the whole process incurs inefficient outcomes in many periods. A characterization in the speed of information transmission across a network is not answered here, although it is an important topic in order to give more attentions in investigating the most efficient way to let the information be spread . This question would remain for the future research.

# 2

## Correlation with Forwarding

### 2.1 INTRODUCTION

#### MOTIVATION

Suppose there are three players, *Int* (*Intermediator*), *S* (*Sender*), *R* (*Receiver*), communicating with one another by writing letters. There are two ways for *Int* to send *S*'s messages to *R*: (1) writing letters without authentication or (2) forwarding letters with *S*'s authen-

tication. In the first form, *Int* can rewrite the messages contained in *S*'s letters and then send a new letter containing the rewritten message to *R*. In contrast to the first form, *Int* cannot rewrite the messages without *S*'s authentication and therefore *Int* can only forward *S*'s letters to *R*. The first kind can be interpreted as the *cheap talk*, while the second kind, *forwarding*, is an added feature in this paper in order to identify the origin of a message.

Provided that players can communicate by using *both* forwarding and cheap talk, this paper concerns whether or not any correlated equilibrium distribution ([Aumann, 1974]) (c.e.d. henceforth) of a game can be generated by an augmented pre-play communication procedure. The notion of correlation equilibrium is plausible, since, in the equilibrium, players have enforced themselves to act as if an outcome drawn from a joint distribution. When this joint distribution assigns probability zero to some outcomes that degrade players' welfare, players' welfare can then be better than that in a Nash equilibrium. However, it is well known that a *mediator*, not a player herself, inhabits in this notion to enforce players' behaviors. *Without a mediator*, we may ask if players can enforce themselves to act coordinately such that the outcome is still generated by a c.e.d..

Without a mediator, pioneering works have created different pre-play communication procedures to implement c.e.d. by cheap talk. Those protocols vary with deviation-detecting procedures and punishment schema. Notably, when the number of players is fewer than four, a procedure seems indispensable—publicly exposing all previous messages. [Gerardi, 2004] has five or more players and use the majority rules (also proposed by [Forges, 1990] in the second part of her protocol): each player can receive same messages that came from three different players, and therefore unitary deviation

can be detected, but punishment is not needed. [Barany, 1987] ([Barany] henceforth) (or [Forges, 1990] in the first part of her protocol) has four players, and detect unitary deviation by letting each player receive same messages from two different players. *After* deviation, a *perfect public recording device*—a device that can perfect and publicly reveals all players’ previous message— will be activated. The deviation is punished by minmax. When the number of players is less than four, [Ben-Porath, 1998] ([Ben-Porath] henceforth) directly uses perfect public recording device to detect deviation<sup>1</sup>. In [Ben-Porath], this device is randomly activated *before* a deviation has been detected. When deviation is detected by this device, players are punished by playing a worst Nash equilibrium. For two-player game, it is impossible to implement any c.e.d. as [Ben-Porath] shows.

With the price of forwarding, this paper removes perfect public recording device for three-player games, while allowing players to detect unitary deviation *without exposing players’ messages publicly at any stage* in the pre-play communication procedure. It is not hard to see that perfect public recording is powerful. It is powerful not only because it reveals all previous messages publicly, but it also actually enforces players not to “cheap” talk *on or before* the timing in which this device is activated; otherwise, a deviation has to be detected. Moreover, since such device reveals all previous messages, if players do not deviate in the pre-play communication, but this communication ends right after players activate this device, then only Nash equilibrium in game  $G$  can be implemented. This is because players’ previous messages have become commonly known, and therefore players’ recommended actions that are contingent on those messages are commonly

---

<sup>1</sup>Although [Abraham et al., 2006] [Abraham et al., 2007] does not explicitly states they use perfect public recording, their protocol is very likely endowed with such device. I discuss their protocol in Section 2.4.



known. This substantial margin separates [Barany] from [Ben-Porath], where [Barany] requires four players, but [Ben-Porath] only requires three players. Let's imagine that players do not deviate during pre-play communication, and this communication could be stopped at any stage by a "strike", such as a postal strike if players communicate by letters. In [Barany]'s communication protocol, if players are asked to play  $G$  after this strike, there is a chance to let their actions fall outside the set of Nash equilibrium in  $G$ . This is because players have not yet deviated and therefore not yet activated perfect public recording. According to [Ben-Porath], if this strike happens at the timing when such device activates, however, players' actions have to fall into the set of Nash equilibrium in  $G$ .

The above discussion also explains why both cheap talk and forwarding are used in my protocol. Intuitively, since players' notes can be authenticated, the ability of forwarding enforces  $Int$  to deliver  $S$ 's real message to  $R$ . This ability is like an activating perfect public recording device. But that is the case when  $Int$  cannot store  $S$ 's notes or when each of  $S$ 's notes are distinguishable. If  $S$ 's indistinguishable notes can be stored by  $Int$ , then  $Int$  can manipulate  $S$ 's messages by pretending himself as  $S$  to send  $S$ 's notes. Messages circulated by forwarding have to be "encoded" well to qualify themselves. But if all messages are forwarded without cheap talk, every player can trace the origin of the message that has been circulated around them, and then players' messages will become commonly known. Thus, cheap talk is indispensable. And, in order to detect deviation, messages transmitted by cheap talk also have to be well "encoded" if we want to remove a procedure that can reveal players' message at some stages.

Although the encoding rule is technical, the protocol proposed here is based on a

simple fact: the joint distribution is the marginal distribution multiple conditional distribution. Recall what a mediator does in a correlated equilibrium  $q$ . This mediator recommends  $a_i$  to each player  $i$ , while letting  $i$ 's conditional distribution given his observation over others' action profile  $a_{-i}$  be  $q(a_{-i}|a_i)$ . The above idea suggests that a protocol has generated  $q$  if such protocol has let  $a_i$  be "chosen" according to  $q(a_i)$  (the marginal distribution on  $a_i$ ) while letting  $a_{-i}$  be "chosen" according to  $q(a_{-i}|a_i)$ . The remaining question is how to make sure that  $i$  can only observe the messages that guide  $i$  to act  $a_i$ . Based on those ideas, Example 1 in Section gives a protocol to implement a *c.e.d.* for a simple three-players game (discussed by [Barany]), in which there is a player who has only one action, but such *c.e.d.* can not implemented by cheap talk without perfect public recording. Example 2 in Section shows my protocol for a case when players have two actions.

In short, this paper obtains a positive result as follows. Suppose that  $G$  has three players and has a Nash equilibrium  $\alpha$  that gives all players the worst payoff among all Nash equilibria. Then, for any *c.e.d.*  $q$  in  $G$ , which has rational number components and gives all players higher expected payoff than what  $\alpha$  does, this  $q$  can be realized as a Nash equilibrium in the pre-play communication extension  $\Gamma(G)$  of  $G$ , in which both cheap talk and forwarding can be used.

#### LITERATURE REVIEW

Here, I briefly review the literature that does not employ the existing results in the literature in Computer Science. I broaden my literature review related to Computer Science in Section 4.

For a Bayesian game, [Forges, 1986] (, also see [Myerson, 2004]) extends the notion of correlated equilibrium to communication equilibrium. In the pre-play communication literature, if players can only use cheap talk, correlated equilibrium implementation and communication equilibrium implementation share the same deviation-detecting procedure. As described above, [Gerardi, 2004] adopts majority rule instead of punishment schema for five or more players. [Forges, 1990] or [Ben-Porath, 2003]<sup>2</sup> uses perfect public recording for four-player and three-player Bayesian game respectively. In [Forges, 1990], she implements communication equilibria by implementing correlated equilibria in a strategic form game as her first step when players are in the ex-ante stage. Since she applies [Barany]'s protocol in her first step, players check deviations before perfect public recording activates. [Ben-Porath, 2003] implements communication equilibrium when players are in the interim stage, but use perfect public recording to randomly check deviations as in [Ben-Porath]. For two-player game, [Vijay Krishna, 2007] shows that implementing all communication equilibria is hopeless. However, for two-player game, implementing correlated equilibria or communication equilibria can be successful under additional assumptions. [Lehrer, 1996][Lehrer and Sorin, 1997][Vida and Āzakis, 2013] assume that there is a simple device, “mediated-talk”. Dependent on how simple this device is, [Lehrer and Sorin, 1997] shows that implementing c.e.d. can be accomplished in one-step pre-play communication, while [Vida and Āzakis, 2013] requires possibly finite steps by employ [Gossner and Vieille, 2001]'s AND device as well as perfect public recording. [Vijay Krishna, 2007] implements communication equilibria, assumes the existence of “urns”, and also use randomly-activated perfect public recording to de-

---

<sup>2</sup>Also see [Forges, 2009]

tect deviations. I emphasize that, in the two-player case, the proposed assumption—forwarding—cannot implement all correlated equilibria. I discuss my assumption in more details in Section 3. For a complete survey, [Forges, 2009] gives an excellent review.

The paper is organized as follows. I describe my model in Section 2.2. I state my main result and depict my communication protocol by two examples in Section 2.3. In Section 2.4, I discuss the papers related to Computer Science, and I compare the required assumptions in implementing correlated equilibria for future extensions. The proof for my main result are in the Appendix B.1

## 2.2 MODEL

For a set  $X$ , I denote  $|X|$  as the cardinality of  $X$  and denote  $\Delta X$  as the set of probability distribution over  $X$ . If  $X$  is a finite set,  $\wp(X)$  denotes the set of all permutations of  $X$ .

Let  $G$  be a game in the strategic form in which  $I = \{1, 2, 3\}$  is the set of players and  $i \in I$  is a player. Denote  $A_i$  as  $i$ 's set of action with generic element  $a_i$ , and denote the set of action profile by  $A = \times_{i \in I} A_i$  with generic element  $a$ . For each  $i$ , let  $u_i : \times_{i \in I} A_i \rightarrow \mathbb{R}$  be  $i$ 's von Neumann-Morgenstern utility function. A randomized action for  $i$  is an element in  $\Delta A_i$  and is denoted by  $\sigma_i$ . Let  $\sigma \in \times_{i \in I} \Delta A_i$  be a randomized action profile. For convenience, denote  $a_{-i}$  as an element in  $\times_{j \neq i} A_j$  and denote  $\sigma_{-i}$  as an element in  $\times_{j \neq i} \Delta A_j$ .

We say  $\sigma = (\sigma_i)_{i \in I}$  is a Nash equilibrium (NE henceforth) if and only if, for all  $i$ , for

all  $\sigma'_i \in \Delta A_i$

$$u(\sigma_i, \sigma_{-i}) \geq u(\sigma'_i, \sigma_{-i})$$

. We say a distribution  $q \in \Delta A$  is a c.e.d. if and only if, for all  $i$ , for all  $a_i$ , for all  $a'_i$ ,

$$\sum_{a_{-i}} q(a_{-i}|a_i)u(a_i, a_{-i}) \geq \sum_{a_{-i}} q(a_{-i}|a_i)u(a'_i, a_{-i})$$

for  $q(a_i) > 0$ , where  $q(a_i)$  is the marginal distribution of  $a_i$  and  $q(\cdot|a_i)$  is the conditional distribution conditional on  $a_i$ .

I then consider an extension  $\Gamma(G)$  of  $G$  such that, for all  $S \in \mathcal{N}$ , it allows  $S$  stages of communication before  $G$  is played. In these communication stages, players can send or receive costless messages. The question is whether or not players can enforce themselves to act according to  $q$  in  $G$  by pre-play communication in  $\Gamma(G)$ . I employ three assumptions to answer this question:

- **A1**:  $G$  has a worst NE.
- **A2**(cheap talk): Without cost, each player  $i$  can write “letters” to send to others, or receive letters from others.
- **A3**(forwarding): Without cost, each Player  $i$  can write “letters” with his own authentication. Moreover,  $j$  can pass  $i$ ’s authenticated letters to others, but cannot rewrite  $i$ ’s authenticated letters without  $i$ ’s authentication.

**A1** assumes that  $G$  has a NE  $\alpha$  that gives all players the minimum payoff among all NE in  $G$ . **A2** assumes that players can send or receive costless messages by writing letters. **A3** gives players the ability of forwarding by assuming that the letters are enhanced by

players' authentication, such as their signatures. The formal definition of forwarding is given in the Appendix.

### 2.3 RESULTS

In this section, I state my main result and spell out my pre-play communication protocol by two examples. In Example 1, I consider an easier case proposed by [Barany] in which there is a player who has only one action. In such case, [Barany] has shown that there is a c.e.d. that cannot be implemented by cheap talk without randomly-activated perfect public recording, while I will show that such c.e.d. can be implemented without perfect public recording by assuming **A2-A3**. In Example 2, I consider a case in which each player has two actions, while letting **A1-A3** hold. The proof of my main result and the protocol for general cases to support my result are in the Appendix.

I state my main result as follows.

**Theorem 4.** *Let  $G$  be a three-player game in which there is a worst NE  $\alpha$  (i.e. **A1** holds). For any c.e.d. in  $G$  that has rational number coefficients and gives all players higher expected payoff than what  $\alpha$  does, if players can communicate by cheap talk and forwarding (i.e. **A2-A3** holds), then there exists a  $\Gamma(G)$  such that this c.e.d. can be realized as a NE in  $\Gamma(G)$ .*

*Proof.* In the Appendix. □

I begin to show my protocols by two examples. In the remainder of the paper, the term “jointly” will be referred to as “Aumann’s *Jointly-Controlled Lottery* (J.C.L. henceforth) ([Aumann and Maschler, 1995])”. Jointly-Controlled Lottery is a procedure to generate

a distribution by two or more players, while unitary deviation is not able to change the distribution meant to be generated. Aumann's Jointly-Controlled Lottery will publicly inform an outcome that is drawn from such generated distribution to players.

### 2.3.1 EXAMPLE 1

To see how forwarding helps players to correlate actions, we may consider [Barany]'s example. In this example,  $A_1 = \{0, 1\}$ ,  $A_2 = \{0, 1\}$ ,  $A_3 = \{0\}$  and the payoff function is described as follows, where Player 1 is the column player and Player 2 is the row player.

	0	1
0	(6,6,0)	(2,7,0)
1	(7,2,0)	(0,0,8)

In this game, we may consider a c.e.d. that gives players highest welfare. As the following figure shows, such c.e.d.  $q$  assigns equal probabilities on  $(0, 0, 0)$ ,  $(0, 1, 0)$  and  $(1, 0, 0)$

	0	1
0	1/3	1/3
1	1/3	0

If players only communicate by cheap talk and if there is no perfect public recording device to detect deviation, then  $q$  cannot be implemented by a pre-play communication procedure. The reason is as follows. Suppose, after communication, Player 1 and Player 2's actions are contingent only on the messages transmitted between them, then only NE in  $G$  can be implemented. This is because those messages are public between Player 1 and Player 2. In order to correlate their actions, their actions have to be contingent on Player 3's messages. Since  $q$  assigns positive weight on  $(0, 1, 0)$  and  $(1, 0, 0)$ , there is

a pair of Player 3's messages, one of which recommends Player 1 to play 1, and one of which recommends Player 2 to play 1. But then Player 3 will send this pair of messages to recommend Player 1 to play 1 as well as recommend Player 2 to play 1, since  $(1, 1, 0)$  gives Player 3 the highest payoff.

As follows, I show a pre-play communication protocol to implement  $q$  by assuming that **A2-A3** hold.

First, let  $T = \{1, 2, 3\}$  and let  $U = \{1, 2\}$ . Here, note that  $|T| = 3$  is the least common multiple of the denominators of the list of reduced  $(q(a))_{a:q(a)>0}$ , and note that  $|\{1, 2\}| = 2$  is the least common multiple of the denominators of the list of reduced  $(q(a_2|a_1))_{a_2:q(a_2|a_1)>0, a_1:q(a_1)>0}$ . This protocol is described as follows

1. **STEP 1** In the beginning of the protocol, Player 2 is the dummy. In this step, Player 1 and Player 3 jointly choose a permutation  $\phi$  from  $\wp(T)$  with equal probability. At this point,  $\phi(t)$  will simulate Player 1's recommended action. To be more precise, given an  $x$  that will be chosen later, Player 1's recommended action will be 0 if  $\phi(x) \in \{1, 2\}$  and will be 1 if  $\phi(x) \in \{3\}$ .
2. **STEP 2** In this step, Player 1 is the dummy. For each  $t \in T$ , Player 2 and Player 3 jointly choose a number  $y_t \in U$  with equal probability.
3. **STEP 3** In this step, Player 2 is the dummy. Player 1 and Player 3 also jointly choose a permutation  $\psi_t$  from  $\wp(U)$  with equal probability for each  $t \in T$ .
4. **STEP 4** There are  $T$  sub-steps. For each  $t \in T$  sub-step, Player 1 authenticates and



passes two letters, two vectors, to Player 3. These letters are

$$\begin{aligned} &(\mathbf{Player\ 1}, 0, \psi_t(1), t) \text{ and } (\mathbf{Player\ 1}, 1, \psi_t(2), t) && \text{if } \phi(t) \in \{1, 2\} \\ &(\mathbf{Player\ 1}, 0, \psi_t(1), t) \text{ and } (\mathbf{Player\ 1}, 0, \psi_t(2), t) && \text{if } \phi(t) \in \{3\} \end{aligned}$$

At this point, the first element of a letter indicates who authenticates this letter; the second element will simulate Player 2's recommended action; the third element gives an "identifier" to a letter for each  $t$ ; and the fourth element is a "time stamp" specified for each  $t$ .

In this  $t$ -sub-step and after Player 1 passes his letters, Player 3 forwards the letter

$$(\mathbf{Player\ 1}, k(t), y_t, t)$$

to Player 2, where  $k(t)$  indicates the second element of the forwarded letter.

In each  $t$ -sub-step, players also perform a deviation-detecting procedure for themselves. If Player  $i$ 's deviation is detected by Player  $j$ , *both* Player  $i$  and Player  $j$  send a letter (**STOP**) to the third party; otherwise, *both* of them send a letter (**OK**) to the third party.

5. **STEP 5** After Player 3 forwards a list  $((k(t), y, t))_{t \in T}$ , and therefore Player 2 gets such a list, Player 1 is the dummy. In this step, Player 3 and Player 2 check if  $|\{t \in T | k(t) = 0\}| = 2$  and  $|\{t \in T | k(t) = 1\}| = 1$ . At this point, given an  $x$  that will be chosen later, Player 2's recommended action will be  $k(x)$ .

If not, Player 3 and Player 2 both send a letter (**FALSE**) to Player 1 and then players

restart the protocol from **STEP 1**; if so, Player 3 and Player 2 both send a letter (**OK**) to Player 1, and then the players go to the next step.

6. **STEP 6** In this step, Player 3 is the dummy. Player 1 and Player 2 jointly choose a number  $x \in T$ , and then this protocol ends. Player 2's recommended action is  $k(x)$ , while the recommended action for Player 1 is 0 if  $\phi(x) \in \{1, 2\}$ ; is 1 if  $\phi(x) \in \{3\}$ .

The punishment schema is as follows. After protocol ends, if Player 1 received one (**STOP**) in **STEP 4**, players play the NE  $(1, 0, 0)$  that gives the best outcome to Player 1 but the worst outcome to themselves; if Player 2 received one (**STOP**) in **STEP 4**, players play the NE  $(0, 1, 0)$  that gives the best outcome to Player 2 but the worst outcome to themselves. Note that a detected deviation will alert a (**STOP**) to a third party in **STEP 4**. If players do not deviate, it is straightforward to check that the conditional probability conditional on each player's recommended action over others' is the same as that induced by  $q$ .

The sub-procedure, **STEP 2** to **STEP 4**, is the main procedure. Due to this sub-procedure, when Player 3 forward Player 1's letters to Player 2 (in **STEP 4**), Player 1 does not know which letters specified by  $(y_t)_{t \in T}$  has been chosen. This is because Player 1 is the dummy in **STEP 2**. In the meanwhile, Player 3 cannot change the written vector in Player 1's letters since those letters are authenticated by Player 1. Therefore, given a  $t \in T$  in **STEP 4**, Player 2 can check whether or not Player 3 has forwarded the correct letter in the  $t$ -sub-step by checking  $(y_t)$  and  $t$ . Furthermore, since Player 2 is the dummy in **STEP 1**, Player 2 does not know  $\phi$ , and thus he does not know Player 1's recommend action in **STEP 6**.

In **STEP 5**, since the letters has been authenticated, Player 2 and Player 3 can check whether or not the set of players' action profiles  $\{(\phi(t), k(t), o)_{t \in T}\}$  is the same as the support of c.e.d.  $q$ . Since  $x$  has been uniformly drawn from  $T$  in **STEP 6**, the chosen action profile  $(\phi(x), k(x), o)$  is indeed following the distribution of  $q$ .

Henceforth, I will call the above sub-procedure—from **STEP 2** to **STEP 4**—*Randomized Forwarding*. By Randomized Forwarding, the sequence of tuple  $(y_t, \psi_t, t)_{y_t \in U, \psi_t \in \emptyset(U), t \in T}$ , is chosen, Player 2 has been informed  $(y_t)_{t \in T}$  (in **STEP 2**), and Player 1 has written down  $(\psi_t, t)$  into the last two elements in his authenticated letter at the  $t$  sub-step (in **STEP 4**) in which Player 1 passes his letters to Player 3. In the remainder of the paper, in order to save notations, the list,  $(y_t, \psi_t, t)_{y_t \in U, \psi_t \in \emptyset(U), t \in T}$ , used in the Randomized Forwarding will not be noticed.

### 2.3.2 EXAMPLE 2

I begin to spell out the protocol used in my main result by an example. In this example, I consider a game in which players have two actions and **A1** holds. I depict a protocol, given **A2-A3**, in which the probability of detecting players' deviations is larger than  $1/2$ . In the Appendix, this protocol is generalized for three-player games given that **A1-A3** holds, and the probability of detecting deviations can be made arbitrarily close to one.

The main idea in constructing the protocol is very close to that in Example 1. At this time, however, Player 1's authenticated letter will “encode” both Player 2 and Player 3's recommended actions, not just Player 2's. This encoding rule is jointly decided by Player

1 and Player 3. After Player 3 forwards Player 1's letters to Player 2 (as Example 1), Player 2 will report Player 3's "encoded" recommended action to Player 3 by cheap talk. After that, Player 1 and Player 3 will tell Player 2 how to "decode" Player 2's recommended action. Based on such encoding rule, I can show that players' unitary deviation can very likely be detected, and I can check whether or not the conditional probabilities induced by the protocol is consistent with that induced by  $q$ .

Let  $A_i = \{0, 1\}$  be the set of action for each player  $i$ , and let a c.e.d.  $q$  assigns equal probability over the action profiles  $\{(0, 0, 0), (0, 1, 0), (0, 1, 1), (1, 0, 0)\}$ .

In this example, the set of letters is  $L = N \cup C \cup \{\mathbf{STOP}, \mathbf{OK}, \mathbf{FALSE}\}$ , where  $N$  or  $C$  is a set of vector. We may call  $N$  the set of *notes* and call  $C$  the set of *categories*. The generic element in  $N$  (or  $C$ ) will be denoted as  $n$  (or  $c$ ), and the  $j$ th element in  $n$  (or  $c$ ) is denoted by  $n_j$  (or  $c_j$ ). I will use parentheses to indicate a note and use bold-text number to indicate a category.

Let  $T = \{1, \dots, 64\}$  and let  $\bar{T} = \{1, \dots, 32\}$ . Here, note that the number 4 is the least common multiple of the denominators of the list of reduced  $(q(a))_{a:q(a)>0}$ , and  $|T| = 2 \cdot |\bar{T}| = 2 \cdot 4 \cdot |A_1| \cdot |A_2| \cdot |A_3|$ .

- Step 1: In this step, Player 2 is the dummy.

There are two sub-steps. In the first sub-step, Player 1 and Player 3 jointly choose three permutations. First, they jointly choose  $\theta_0$  and  $\theta_1$ , each of them is from  $\wp(\{1, \dots, |A_3|\})$ . In this example, let us suppose

$$\theta_0(1) = 1, \theta_0(2) = 2$$

$$\theta_1(1) = 2, \theta_1(2) = 1$$

**Figure 2.1:** An example of Player 1's 32 categories of "encoded" notes

<b>00011, 00012</b> (0, 0, 1, $\phi(1)$ ) (1, 0, 1, $\phi(2)$ ) (1, 1, 2, $\phi(3)$ )	<b>00111, 00112</b> (0, 1, 2, $\phi(4)$ ) (1, 1, 2, $\phi(5)$ ) (1, 0, 1, $\phi(6)$ )	<b>01011, 01012</b> (1, 0, 1, $\phi(7)$ ) (0, 0, 1, $\phi(8)$ ) (0, 1, 2, $\phi(9)$ )	<b>01111, 01112</b> (1, 1, 2, $\phi(10)$ ) (0, 1, 2, $\phi(11)$ ) (0, 0, 1, $\phi(12)$ )
<b>10011, 10012</b> (0, 0, 1, $\phi(13)$ )	<b>10111, 10112</b> (0, 1, 2, $\phi(14)$ )	<b>11011, 11012</b> (1, 0, 1, $\phi(15)$ )	<b>11111, 11112</b> (1, 1, 2, $\phi(16)$ )
<b>00021, 00022</b> (0, 0, 2, $\phi(17)$ ) (1, 0, 2, $\phi(18)$ ) (1, 1, 1, $\phi(19)$ )	<b>00121, 00122</b> (0, 1, 1, $\phi(20)$ ) (1, 1, 1, $\phi(21)$ ) (1, 0, 2, $\phi(22)$ )	<b>01021, 01022</b> (1, 0, 2, $\phi(23)$ ) (0, 0, 2, $\phi(24)$ ) (0, 1, 1, $\phi(25)$ )	<b>01121, 01122</b> (1, 1, 2, $\phi(26)$ ) (0, 1, 2, $\phi(27)$ ) (0, 0, 1, $\phi(28)$ )
<b>10021, 10022</b> (0, 0, 1, $\phi(29)$ )	<b>10121, 10122</b> (0, 1, 1, $\phi(30)$ )	<b>11021, 11022</b> (1, 0, 2, $\phi(31)$ )	<b>11121, 11122</b> (1, 1, 2, $\phi(32)$ )

. Second, Player 1 and Player 3 jointly choose a permutation  $\phi$  from  $\wp(\bar{T})$ .

Given the above permutations, Figure 2.1 shows the notes authenticated by Player 1 with respect to categories. Let us say " $n$  is with  $c$ " if  $n$  and  $c$  is within the same box in Figure 2.1, and denote  $N_c = \{n | n \text{ is with } c\}$ .

The key idea is that Player 1 and Player 3 "encode" the third element in a note by letting  $n_3 = \theta_{n_2}(c_4)$  if  $n$  is with  $c$ . This encoding rule will be used in **STEP 5.1** as a deviation-detecting. As for the other aspects in Figure 2.1,

- $c_1$  indicates Player 1's recommended actions.
- $c_2$  (or  $c_3$ ) is interpreted as a permutation of Player 2's (or Player 3's) recommended actions.

- $n_1$  (or  $n_2$ ) is interpreted as permuted Player 2's (or Player 3's) recommended actions.
- If  $n$  is with  $c = (c_1, c_2, c_3, c_4, c_5)$  then  $n$  is with  $c' = (c_1, c_2, c_3, c_4, c'_5)$  for all  $c, c'$ .

In the second sub-step, Player 1 and Player 3 jointly and uniformly pick up a function  $f$  from set the  $F$ , where

$$F = \{f : T \rightarrow C \mid |\{t \mid f(t) = c\}| = |N_c|, \text{ for all } t \in T\}$$

. At this point,  $f$  is a multiset combination in  $T$ .

- In Step 2, players first perform a  $T$  sub-steps Randomized Forwarding.<sup>3</sup> For each  $t \in T$  sub-step, Player 2 and Player 3 jointly pick one of Player 1's notes in  $N_{f(t)}$ , and Player 3 forwards such note to Player 2.

After that, Player 2 and Player 3 have a list of notes, denoted as  $(k(t))_{t \in T}$ .

- Step 3 is a checking point. Both Player 2 and Player 3 check if  $(k(t))_{t \in T}$  is without repetition. If this is so, Player 3 and Player 2 both send a letter **OK** to Player 1, and then all players continue to Step 4; otherwise, Player 3 and Player 2 both send a letter **FALSE** to Player 1, and then all players restart the protocol from Step 1.
- In Step 4, Player 1 and Player 2 jointly and uniformly pick an element  $x \in T$ . Player 2 reports  $(k(x)_2, k(x)_3)$  to Player 3 by cheap talk. Players continue to Step 5.1.

---

<sup>3</sup>In this case, Player 2 and Player 3 choose a sequence  $(y_t)_{t \in T}$ , where  $y_t \in \{1, \dots, \max_c |N_c|\}$  for  $t \in T$ ; Player 1 and Player 3 choose  $(\psi_t)_{t \in T}$ , where  $\psi_t \in \wp(\{1, \dots, \max_c |N_c|\})$ . Player 1 writes down the pair  $(\psi_t, t)$  on his note for each  $t \in T$  when he passes his notes to Player 3 in the procedure in which Player 3 forwards Player 1's notes to Player 2.

- In Step 5.1, simultaneously,
  - Player 1 reports  $f(x)_2$  to Player 2. Let this message be  $m^2$ .
  - Player 1 reports  $(f(x)_2, f(x)_3, f(x)_4, f(x)_5)$  to Player 3. Let this message be  $m^3$ .
  - Player 3 report to  $\theta_{k(x)_3}^{-1}(k(x)_2)$  to Player 1.

by cheap talk. If  $m_3^3 \neq \theta_{k(x)_2}^{-1}(k(x)_3)$ , then Player 1 and Player 3 send **STOP** to the other players, and then play the worst Nash equilibrium. Otherwise, all players go to Step 5.2.

- In Step 5.2, Player 3 constructs a set  $D$  to check possible deviations occurred in Step 5.1. Denote

$$E_{c_1, c_2, c_3, c_4} = \{t | (f(t)_2, f(t)_3, f(t)_4, f(t)_5) = (c_2, c_3, c_4, c_5)\}$$

. Player 3 randomly chooses an element  $u \in \{1, 2\}$  with probability  $1/2$ . Then let  $D' = E_{m_1^3, c'_3, m_3^3, u}$ , where  $c'_4 \neq m_2^3$ , and let  $D'' = E_{m_1^3, m_2^3, m_3^3, m_4^3}$ . Finally, he reports  $D = D' \cup D''$  and  $m_1^3$  to Player 2 .

- In Step 5.3, Player 2 checks: if  $x \in D$ , if  $m^2 = m_1^3$  and check if the distribution of notes in the sequence  $(k(t))_{t \in D}$  can be generated by the procedure in Step 5.2.

If one of the above criteria fails, Player 2 sends **STOP** to the other players, while the other players (Player 1 or Player 3) who let these criteria fail *also* send **STOP** to the others<sup>4</sup>; otherwise, all players send **OK** to the others and then go to Step 6.

---

<sup>4</sup>In short, the player who detects deviation sends **STOP**, and the player who deviates also sends **STOP**.

- Step 6 is the final step in which players “decode the recommended actions”. The way to interpret the recommendation is as follows.
  - Player 1’s recommended action,  $a_1$ , is  $f(x)_1$ .
  - Player 2’s recommended action,  $a_2$ , is  $k(x)_1 + m^2 \pmod{2}$ .
  - Player 3’s recommended action,  $a_3$ , is  $k(x)_2 + m_2^3 \pmod{2}$ .

Now I can show that players’ unitary deviations can be detected with probability larger than  $1/2$ .

**Proposition 2.3.1.** *In the above protocol, players’ unitary deviation (despite of J.C.L. schema) can be detected with probability larger than  $1/2$ .*

*Proof.* Step 1 is J.C.L., and therefore I omit it. Players cannot deviate from Step 2 since they use Randomized Forwarding (as Example 1 shows). Their deviation will be detected in Step 3 (as Example 1 shows). Step 4 is J.C.L., and therefore I omit it. Step 6 is the interim stage in which players has got recommended action but before actions are played. I then check the possible deviations during Step 5.1 to Step 5.4.

I begin with Player 1’s possible deviations in Step 5.1. Suppose Player 1 report  $m^{3'} \neq m^3$ . Then the probability of  $x \in D''$  is zero by the definition of  $D''$ . Now I check the probability of  $x \in D'$ . By the construction in Step 5.2, there are two candidates for the  $D'$ :  $E_{m_1^3, c_3', m_3^3, 1}$  and  $E_{m_1^3, c_3', m_3^3, 2}$ . Since Player 3 chooses the candidates for  $D'$  with equal probability,  $E_{m_1^3, c_3', m_3^3, 1}$  and  $E_{m_1^3, c_3', m_3^3, 2}$  will be chosen with equal probability. The probability that  $x \in D'$  is equal  $1/2$ , and hence Player 1’s deviation can be detected with probability  $1/2$  in Step 5.3.



I then check Player 2's deviation in Step 5.1. Let's suppose, as an instance, that Player 2 reports  $(k(x)_2, k(x)_3) = (0, 2)$  to Player 1 if Player 2 follows the protocol. In such case,  $m_3^3 = 2$ . Then, if Player 2 reports  $(0, 1)$  to Player 3, Player 3 will detect this deviation for sure in Step 5.1 since  $m_3^3 \neq \theta_0^{-1}(1)$ ; if Player 2 reports  $(1, 2)$ , this deviation is still detected for sure in Step 5.1 since  $m_3^3 \neq \theta_1^{-1}(2)$ . Player 2's undetectable deviation is thus to report  $(1, 1)$ . Player 2, however, does not know the permutations  $\theta_0$  and  $\theta_1$  because he is the dummy in Step 1, and thus the conditional probability conditional on  $(k(x)_2, k(x)_3) = (0, 2)$  over  $\{(1, 1), (1, 2)\}$  is  $(1/2, 1/2)$  given that Player 1 and Player 3 jointly and uniformly pick up  $\theta_1$ . And therefore Player 2's possible deviation can be detected with probability larger than  $1/2$ .

Finally, I check Player 3's deviation in Step 5.2. There are two possible deviations: deviating from reporting  $D$ , or deviating from reporting  $m_1^3$ . The first kind of deviation can be detected with probability larger than  $1/2$  by the same argument in checking Player 1's deviation in Step 5.1—as if Player 3 mimics Player 1's deviation. The second kind of deviations is detected with probability one since  $m^2 \neq m_1^{3'}$  if  $m_1^{3'} \neq m_1^3$ .

In summary, players' unitary deviation can be detected with probability larger than  $1/2$ . □

I should then check whether or not players' conditional probabilities over players' recommended action is the same as that induced by  $q$ . The proof is technical and is included in the proof for general three-player case, therefore I omit this proof. But I state the following claim.

**Proposition 2.3.2.** *Let A2-A3 hold. After Step 6, if players has not received STOP, player  $i$ 's conditional probability conditional on recommended action  $a_i$  over recommended actions*

$a_{-i}$  is the same as that induced by  $q$ .

*Proof.* In the Appendix. □

## 2.4 DISCUSSION AND CONCLUSION

The underlying question is to answer if any c.e.d. in a three-player game  $G$  can be implemented as a NE of a game  $\Gamma(G)$ . This paper shows a positive result through the major assumption on the ability of forwarding. Indeed, it is a strong assumption compared to cheap talk. However, a benefit exploited from this assumption is to remove any procedure that will expose all previous messages that may decide players' recommended actions. According to my argument in the introduction, this kind of procedure, such as an activating perfect public recording, may be only able to implement Nash equilibrium in  $G$  in some circumstances. In contrast, if players can only use cheap talk, it is impossible to detect deviations before a perfect public recording device activates as [Barany] shows. Thus, the result is tight.

Indeed, by using a perfect public recording to randomly detect deviations, [Ben-Porath] has shown that implementing c.e.d. is possible by cheap talk only. Is there a protocol that does not endow a perfect public recording but implements any c.e.d. through cheap-talk-only pre-play communication? [Heller, 2010] and [Heller et al., 2012] apply the results in Computer Science and seems to confirm this conjecture. I, however, believe there is still a gap to meet such a requirement. In this section, I broaden my literature review to the literature in Computer Science according to my best knowledge, and discuss the potential ability of forwarding.

In the following discussion, the number of players is always  $|I| = 3$ .

#### 2.4.1 SECRET SHARING AND MULTIPARTY COMPUTATION

##### 2.4.1.1 MULTIPARTY COMPUTATION

[Heller, 2010] applies [Ben-Or and Wigderson, 1988]’s ([BGW] henceforth) result on multiparty computation to implement c.e.d. for three-player game (also see Theorem 10 in [Heller et al., 2012]). However, it is not obvious that he has checked possible deviations. When players may deviate, [BGW]’s result holds for four players<sup>5</sup>. Most importantly, in their construction, it is not clear that the conditional probability conditional on each player  $i$ ’s recommended action over others’ recommended actions is the same as  $q(a_{-i}|a_i)$ , for each recommended action  $a_i$  for each  $i \in I$ .

As follows, I rephrase [BGW]’s protocol to my best knowledge. In [BGW], “...each player holding **some input**  $s \in E$ ”<sup>6</sup> where  $E$  is a finite field. Let us assume that each player  $i$  has a  $s_i \in E$ . We may name  $s_i$  as  $i$ ’s *secret* that is only known by  $i$ . Let  $x_i \in E$  be a constant for each  $i \in I$ . In the beginning of the protocol, every player  $i$  receives *shares of secret*, denoted as  $r_i(x_i)$ , by [Shamir, 1979]’s secret-sharing schema. Here,  $r_i(x_i) \in E^{|I|}$ , and the  $j$ th element of  $r_i(x_i)$  is a point on a 1-degree random-coefficient polynomial. To be more precise,  $r_i(x_i)(j) = s_j + a_j x_i$ , where  $(a_j)_{j \in I} \in E^{|I|}$  is uniformly and independently drawn from the set of non-zero elements of  $E$ . Since that, for each  $i \in I$ , conditional on  $r_i(x_i)(j)$ , the conditional distribution over other players’ share of secret  $(r_k(x_k)(j))_{j,k \neq i}$ ,

---

<sup>5</sup> [BGW] page 3, Theorem 3 and Theorem 4

<sup>6</sup> [BGW] page 3

are independently and uniformly on  $E$ . [BGW] wants to “**compute**” a function  $F$  that has  $|I|$  inputs and  $|I|$  outputs, while “**player  $i$  knows the  $i$ th input and  $i$ th output but nothing else**”<sup>7</sup>. The term “nothing else” is vague, and [BGW] seems to refer to “nothing else” by stating: conditional on  $i$ th output, the conditional probability over  $j$ th input is uniformly over  $E$ <sup>8</sup>, instead of stating about the conditional probability over  $j$ th output conditional on  $i$ th output.

In [BGW]’s Computation Stage<sup>9</sup>, given two secret  $s, s' \in E$ , given a constant  $c$ , and given two 1-degree random-coefficient  $f(x) = s + ax$  and  $g(x) = s' + a'x$ , where  $a, a'$  are uniformly and independently drawn from  $E$ , a player  $i$  who get the value of  $f(x_i)$  and  $g(x_i)$  can “compute”  $s + cs'$  by  $f(x_i) + cg(x_i)$ . Due to the above result, a Lemma in [BGW]<sup>10</sup> shows that, for any linear function  $F(x_1, \dots, x_{|I|}) = \sum_{i \in I} \alpha_i x_i$ , where  $x_i$  is player  $i$ ’s input and  $\alpha_i$  is a constant, can be “computed”. At this point,  $i$ ’s input seems to be referred to  $f(x_i)$  (or  $g(x_i)$ ). He then states the following Matrix Multiplication Corollary:

Let  $A$  be a  $|I| \times |I|$  matrix, let  $X = (x_1, \dots, x_{|I|})$  be players’ input, then

$Y = XA$  can be computed, and the **only information to player  $i$**  is  $Y_i$

. The proof is as follows: this is because we can “compute”  $Y_i$  linear independently, and **only reveal the value of  $Y_i$  to player  $i$** .<sup>11</sup>

---

<sup>7</sup> [BGW] page 2

<sup>8</sup> [BGW] page 3, The final stage

<sup>9</sup> [BGW] page 3-4

<sup>10</sup> [BGW] page 3

<sup>11</sup> [BGW] also considers how to “compute” the multiplication of two secret  $s, s'$ , and also use his Matrix Multiplication Corollary to accomplish the multiparty computation.

[BGW]'s protocol then seems unsuitable to implement correlated equilibria. I then ask:

- If we do not have a mediator, how do we only reveal the value of  $Y_i$  to player  $i$ ?
- Furthermore, given  $A$ , if each player  $i$  use his own shares of secret,

$$X_i = (r_i(x_i)(1), \dots, r_i(x_i)(|I|))$$

, to calculate  $Y^i = X_i A$  ( $Y^i$  is a vector) and to interpret  $Y_i^i$  as his recommended action, is the conditional probability conditional on  $Y_i^i$  over  $Y_{-i}^i$  is the same as  $q(Y_{-i}^i | Y_i^i)$ ? If so, then  $X_i = (r_i(x_i)(1), \dots, r_i(x_i)(|I|))$  should be correlated with  $X_j = (r_j(x_j)(1), \dots, r_j(x_j)(|I|))$  for some  $j$ . But according to [BGW]'s construction, these two vectors are independent.

- How do we interpret the secret or the shares of a secret in game-theoretic setting ? Are the shares of a secret indeed players recommended actions?

#### 2.4.1.2 VERIFIABLE SECRET SHARING

Following the above section, and despite how we may translate the above secret sharing procedure to the procedure in implementing correlated equilibria ([Heller, 2010][Heller et al., 2012]), or implementing communication equilibrium ([Abraham et al., 2006], [Abraham et al., 2007]), by cheap talk, there is at least one timing in which player may deviate: before each player  $i$  get his secret share  $r_i(x_i)(j)$  from  $j \in i$ , player  $j$  may send different  $\overline{r_i(x_i)(j)}$  to  $j$  by changing  $s_j$  to  $\overline{s_j}$ . How can we detect possible deviations? In [Abraham et al., 2007], the protocol will randomly ask players to privately and truthfully

report their secret shares  $((s_i)_{i \in I})$  to others, and to let each player be able to solve the secret  $((s_i)_{i \in I})$  by polynomial interpolation. In order to impede deviation from truthfully reporting, they adopt [Rabin and Ben-Or, 1989]’s *Information Checking Procedure* (ICP henceforth). In [Heller et al., 2012], in the proof of their Theorem 10, they let players randomly broadcast (by assuming that players can communicate publicly) their secret shares, and use ICP to impede players from misreporting their secret shares. Thus, the secrets will be randomly and publicly known in the protocols designed by [Abraham et al., 2006], [Abraham et al., 2007] and [Heller et al., 2012]. Their methods for detecting deviation are thus very close to using perfect public recording in order to reveal previous possible deviations, while using ICP instead.

Is it true that ICP can impede the unitary deviation? I rephrase ICP here as best I can. There are three players, *Dealer*, *Intermediator*, and *Recipient*. The Dealer holds a data,  $d \in E$ , where  $E$  is a finite field. In the schema, the Dealer first uniformly chooses two random numbers  $y$  and  $b \neq 0$  from  $E$ . Dealer then privately sends  $(d, y)$  to Intermediator and  $(b, d + by)$  to Recipient. They call such pair  $(b, d + by)$  as *Checking Vector*<sup>12</sup>. Then they want to show as well as has proved that: if Intermediator deviates by reporting  $\overline{(d, y)}$  to Recipient, there is a very high possibility (dependent on  $|E|$  is) such that Recipient will detect; and there is a very low possibility preventing Intermediator knowing whether or not Recipient will detect  $\overline{(d, y)} \neq (d, y)$ .

However, if the Dealer initially sends  $(d', y)$  to the Intermediator as well as sends  $(b, d' + by)$  to the Recipient, the above statement still holds. This is because either Intermediator or Recipient at most knows that  $d'$  is the data sent by the Dealer (by truthfully

---

<sup>12</sup>The Checking Vector is very close to my encoding rule in encoding  $n_2$  by  $(n_2, n_3)$ , where  $n_3 = \theta_{n_2}(c_3)$ , in Example 2.

report their  $(d', y)$  and  $(b, d' + by)$  to each other). Let such  $d$  be a secret or a secret share hold by a player  $i$ . Given player  $i$  being a dealer who distributes the Checking Vectors in order to use ICP, player  $i$  may deviate by sending  $d'$  instead of  $d$ . It is not obvious that [Heller et al., 2012] has checked such player's possible deviations since they directly apply ICP. In [Abraham et al., 2006], the researchers employ an "issuer" (page 59) to distribute such Checking Vectors. Is that issuer a player? This question might need to be answered.

#### 2.4.2 FORWARDING, URNS, AND COMPUTATIONAL BOUNDEDNESS

For the two-player case, [Ben-Porath] uses *urns* and perfect public recording to accomplish his result, while [Urbano and Vila, 2002][Dodis et al., 2000] (, also see [Teague, 2008]) assumes that players have bounded ability to solve some difficult mathematical problems. In the sense used by [Ben-Porath, 1998], an urn is a device such that, when player  $i$  puts some balls with different colors in an urn and hand such urn over to player  $j$ , player  $j$  can draw a ball from this urn without knowing the distribution of balls, while player  $i$  does not know which ball  $j$  has drawn. Interestingly, by assuming that players are computationally bounded, such an urn can be created ([Dodis et al., 2000][Goldreich et al., 1987]). In order to give the ability of forwarding to players, the assumption on computational boundedness seems necessary since it requires players can authenticate their messages (, such as Digital Authentication). However, forwarding should be weaker assumption than the urns. This is because, by forwarding, implementing any c.e.d. in a two-player case is impossible. By the same argument when players can only use cheap talk, forwarding allows those contents that decide players' recommended actions to be publicly known in two-player case. Thus, the difference between forwarding

and urns is whether or not the content itself has been “encrypted”. In [Urbano and Vila, 2002] or [Dodis et al., 2000], the content of a message has been encrypted by computational boundedness. On the contrary, forwarding strengthens the ability to identify the origin of the messages but does not encrypt the content itself.

The origin of a message is not essential in the two-player case, but it should be crucial in the three-player case if we want to remove a procedure that exposes players’ previous messages. The ability of forwarding is therefore in the middle between urns and cheap talk.



A

Chapter 1

## A.1 PROOFS

### proof for Lemma 1.4.1

*Proof.* The proof is done by contradiction. Suppose Rebels' strategies constitute an APEX. By definition of APEX, there is a time  $T^\theta$  when actions start to repeat at state  $\theta$ . Let  $T = \max_{\theta \in \Theta} T^\theta$ . Let  $T_i = T + 1$  and suppose the consequence does not hold so that  $0 < \sum_{\theta: \#[Rebels](\theta) \geq k} \beta_{G_i}^{\pi, T^*}(\theta | h_{G_i}^s) < 1$  for some  $s \geq T_i$ . Then Rebel  $i$  puts some positive weights on some  $\theta \in \{\theta : \#[Rebels](\theta) < k\}$  and puts some positive weights on  $\theta \in \{\theta : \#[Rebels](\theta) \geq k\}$  at that time  $s$ . Note this Rebel  $i$  has already known  $\theta_j$  if  $j \in G_i$ , and therefore Rebel  $i$  put some positive weights on  $\theta \in \{\theta : \#[Rebels](\theta) < k, \theta_l = Rebel, l \notin G_i\}$  and  $\theta \in \{\theta : \#[Rebels](\theta) < k, \theta_l = Inert, l \notin G_i\}$ . Since actions start to repeat at  $T$ , all  $i$ 's neighbors will play the actions at time  $T$  repeatedly, and therefore Rebel  $i$  can not update information from his neighborhood after time  $T$ .

Suppose  $i$ 's continuation strategy is to play **revolt** repeatedly, then players' action profile is not ex-post efficient if  $\#[Rebels](\theta) < k$  after time  $T$ . Suppose  $i$ 's continuation strategy is to play **stay** repeatedly, then players' action profile is not ex-post efficient if  $\#[Rebels](\theta) \geq k$  after  $T$ . In either case, it contradicts that Rebels' strategies constitute an APEX.  $\square$

### proof for Theorem 3

This proof follows three useful claims, Claim A.1.1, Claim A.1.2 and Claim A.1.3. First

note that  $I_i^t$  and  $N_i^t$ ,  $t \geq 1$  can be expressed as

$$I_i^t = \bigcup_{k_0 \in \tilde{G}_i \cap R^t} \bigcup_{k_1 \in \tilde{G}_{k_0} \cap R^{t-1}} \dots \bigcup_{k_{t-1} \in \tilde{G}_{k_{t-2}} \cap R^1} G_{k_{t-1}} \cap R^0 \quad (\text{A.1})$$

, while  $H_i^t$  can be expressed as

$$N_i^t = \bigcup_{k_0 \in \tilde{G}_i \cap R^{t-1}} \bigcup_{k_1 \in \tilde{G}_{k_0} \cap R^{t-2}} \dots \bigcup_{k_{t-2} \in \tilde{G}_{k_{t-3}} \cap R^0} G_{k_{t-2}} \quad (\text{A.2})$$

**Claim A.1.1.**  $I_i^t \subset N_i^t$  for  $t \geq 1$

*Proof.*  $I_i^t \subset N_i^t$  by definition. Since  $R^t \subset R^{t-1}$  for  $t \geq 1$ , we then have  $I_i^t \subset N_i^t$  for  $t \geq 1$  by comparing Equation A.1 and Equation A.2.  $\square$

**Claim A.1.2.** *If the network is without cycle, then for each  $t \geq 1$  block, we have*

$$i \in R^t \Leftrightarrow i \in R^{t-1}$$

and

$$\exists k_1, k_2 \in R^{t-1} \cap \tilde{G}_i, \text{ where } k_1 \neq k_2$$

.

*Proof.* The proof is done by induction. I first show that the statement is true for  $t = 1$ .

**Base:**  $i \in R^1 \Leftrightarrow [i \in R^0] \wedge [\exists k_1, k_2 \in (R^0 \cap \tilde{G}_i)]$ .

$\Rightarrow$ : Since  $i \in R^1$ , then  $i \in R^0$  and then  $I_i^0 \not\subset N_j^0$  for all  $j \in \tilde{G}_i$  by definition. Since  $I_i^0 = R^0 \cap \tilde{G}_i$ , then  $\forall j \in \tilde{G}_i [\exists k \in (R^0 \cap \tilde{G}_i) [k \notin N_j^0]]$ . Since the  $j \in \tilde{G}_i$  is arbitrary, we then have a pair of  $k_1, k_2 \in (R^0 \cap \tilde{G}_i)$  such that  $k_1 \notin N_{k_2}^0$  and  $k_2 \notin N_{k_1}^0$ .

$\Leftarrow$ : Pick  $k \in \{k_1, k_2\} \subseteq (R^0 \cap \bar{G}_i)$ , and pick an arbitrary  $j \in \bar{G}_i \setminus \{k\}$ . Note that  $k \notin N_j^0$ , otherwise there is a cycle from  $i$  to  $i$ . Hence  $[k \in (R^0 \cap \bar{G}_i)] \wedge [k \notin N_j^0]$  and therefore  $[k \in I_i^0] \wedge [k \notin N_j^0]$ . Then we have  $I_i^0 \not\subseteq N_j^0$  for arbitrary  $j \in \bar{G}_i$ , and thus  $i \in R^1$ .

**Induction hypothesis:** the statement is true for  $\{1, 2, \dots, t\}$  where  $t \geq 1$ .

If the hypothesis is true, then  $i \in R^{t+1} \Leftrightarrow [i \in R^t] \wedge [\exists k_1, k_2 \in (R^t \cap \bar{G}_i)]$

$\Rightarrow$ : since  $i \in R^{t+1}$ , then  $i \in R^t$  and  $I_i^t \not\subseteq N_j^t$  for all  $j \in \bar{G}_i$  by definition. Recall that  $I_i^t$  can be expressed as Equation A.1 and  $H_i^t$  can be expressed as Equation A.2, then for every  $l \in I_i^{t-1}$ , we can find a path connecting  $i$  to  $l$  by the induction hypothesis. If  $j \in \bar{G}_i$ , then we can find a path connecting  $j$  to  $l$  by connecting  $j$  to  $i$ , and then connecting  $i$  to  $l$ . Thus, if  $l \in I_i^{t-1}$  then  $l \in N_j^t$ , and hence  $I_i^{t-1} \subseteq N_j^t$  for all  $j \in \bar{G}_i$ . Recall that  $I_i^t = \bigcup_{k \in N_i \cap R^t} I_k^{t-1}$  and  $i \in R^{t+1}$ , then we must have  $\forall j \in \bar{G}_i [\exists k \in (R^t \cap \bar{G}_i) [I_k^{t-1} \not\subseteq N_j^t]]$ , since  $I_i^{t-1} \subseteq N_j^t$ . Note that such  $j \in \bar{G}_i$  is arbitrary, we then have a pair of  $k_1, k_2 \in (R^t \cap \bar{G}_i)$  such that  $k_1 \notin N_{k_2}^t$  and  $k_2 \notin N_{k_1}^t$ .

$\Leftarrow$ : By the induction hypothesis, we have a chain  $k_{1_0}, \dots, k_{1_t}, i, k_{2_t}, \dots, k_{2_0}$  with  $k_{1_0} \in R^0, \dots, k_{1_t} \in R^t, i \in R^t, k_{2_t} \in R^t, \dots, k_{2_0} \in R^0$ , where  $k_{1_t}, k_{2_t} \in (R^t \cap \bar{G}_i)$ ,  $k_{1_0} \in I_{k_{1_t}}^{t-1}$  and  $k_{2_0} \in I_{k_{2_t}}^{t-1}$ . Note that  $k_{1_0} \notin N_j^t$  whenever  $j \in \bar{G}_i$ , otherwise there is a cycle from  $i$  to  $i$  since  $\{i, k_{2_t}, \dots, k_{2_0}\} \in N_j^t$ , and hence  $[k_{1_0} \in I_{k_{1_t}}^{t-1}] \wedge [k_{1_0} \notin N_j^t]$  for all  $j \in \bar{G}_i$ . Therefore we have  $[I_{k_{1_0}}^{t-1} \in I_i^t] \wedge [I_{k_{1_0}}^{t-1} \notin N_j^t]$  for all  $j \in \bar{G}_i$  since  $k_{1_t}, k_{2_t} \in (R^t \cap \bar{G}_i)$  and  $[k_{1_0} \in I_{k_{1_t}}^{t-1}] \wedge [k_{1_0} \notin N_j^t]$  for all  $j \in \bar{G}_i$ . Then we have  $I_i^t = \bigcup_{k \in N_i \cap R^t} I_k^{t-1} \not\subseteq N_j^t$  for arbitrary  $j \in \bar{G}_i$ , and thus  $i \in R^{t+1}$ .

We can then conclude that the statement is true by induction. □

**Claim A.1.3.** *If the network is without cycle and if the state has strong connectedness, then if there is a pair of  $R^t$  nodes, then there exists a  $R^t$ -path connecting them.*

*Proof.* The proof is done by induction and by Claim A.1.2. Since the state has strong connectedness, we have a  $R^0$ -path connecting each pair of  $R^0$  nodes. Since all pairs of  $R^0$  nodes are connected by a  $R^0$ -path, then for all pairs of  $R^1$  nodes must be in some of such paths by Claim A.1.2, and then connected by a  $R^0$ -path. But then all the  $R^0$ -nodes in such path are all  $R^1$  nodes by Claim A.1.2 again and by  $R^t \subseteq R^{t-1}$  for  $t \geq 1$  by definition. Thus, for all pairs of  $R^1$  nodes has a  $R^1$ -path connecting them. The similar argument holds for  $t > 1$ , we then get the result. □

I begin to prove Theorem 3. I first claim that if  $R^t \neq \emptyset$  and if  $R^{t+1} = \emptyset$ , then  $R^0 \subset I_i^t$  whenever  $i \in R^t$ . Then I claim that if  $R^t \neq \emptyset$  then  $\#R^{t+1} < \#R^t$ . Finally, I iterate  $R^t$  with  $t \geq 0$  to get the conclusion.

If  $R^t \neq \emptyset$  but  $R^{t+1} = \emptyset$ , I claim that  $R^0 \subset I_i^t$  for all  $i \in R^t$ . The proof is by contradiction. If  $R^0 \not\subset I_i^t$ , there is a  $j \in R^0$  but  $j \notin I_i^t$ . Since  $I_i^t$  can be expressed as Equation A.1, there is no such a path  $\{i, k_0, k_1, \dots, k_{t-1}, j\}$ , where  $k_0 \in G_i \cap R^t, k_1 \in G_{k_0} \cap R^{t-1}, \dots, k_{t-1} \in N_{k_{t-2}} \cap R^1$ . Since  $R^{t+1} = \emptyset$  and therefore  $R^{t'} = \emptyset$  if  $t' \geq t + 1$ , and hence there is no such a path containing a node in  $R^{t'} = \emptyset$ , where  $t' \geq t + 1$  connecting  $i$  to  $j$ . But  $i \in R^t$  and  $j \in R^0$ , if there is no such a path, then it violate either Claim A.1.3 or Claim A.1.2. Contradiction.

Next I claim that if  $R^t \neq \emptyset$  then  $\#R^{t+1} < \#R^t$ . The proof is the followings. Given a node  $i$  in  $R^t$ , let  $j \in R^t$  (could be  $i$  itself) be the node connected with  $i$  with the maximum shortest  $R^t$  path. This  $j$  can be found since  $R^t \neq \emptyset$  and the network is finite. Then there is no  $R^t$ -node in  $j$ 's neighborhood other than the nodes in this path. Since the network is without cycle, there is at most one  $R^t$ -node in  $j$ 's neighborhood. But then  $j \notin R^{t+1}$  since it violate Claim A.1.2.

Starting from  $R^0 \neq \emptyset$  and iterating  $R^t$  with  $t \geq 0$ , if  $R^t \neq \emptyset$  but  $R^{t+1} = \emptyset$ , then there is some  $i$  with  $R^0 \subset I_i^t$  as the above paragraph shows; if  $R^t \neq \emptyset$  and  $R^{t+1} \neq \emptyset$ , then we starting from  $R^{t+1}$  and iterating  $R^{t+1}$  with  $t \geq t + 1$ . Since  $\#R^{t+1} < \#R^t$  as the above paragraph shows, there is a time  $t^*$  with  $R^{t^*} = \emptyset$ , then we get the conclusion.

**proof for Lemma 1.4.2**

*Proof.* Denote  $(i, j)$ -path as the set of paths from  $i$  to  $j$ . The proof is by contradiction. Suppose there are three or more  $R^t$ -nodes in  $C^t$ , then pick any three nodes of them, and denote them as  $i_1, i_2, i_3$ . Let's say  $i_2$  is in a  $(i_1, i_3)$ -path by strong connectedness, and therefore  $i_2 \in TR_{i_1 i_2}$  and  $i_3 \in TR_{i_2 i_3}$ . First we show that  $i_1 \in G_{i_2}$  (or  $i_3 \in G_{i_2}$ ). Suppose  $i_1 \notin N_{i_2}$ , since  $i_1, i_2 \in R^t$ , then the  $(i_1, i_2)$ -path is a  $R^t$ -path by Claim A.1.2. Let this  $(i_1, i_2)$ -path be  $\{i_1, j_1, \dots, j_n, i_2\}$ . Since  $i_1, j_1, \dots, j_n, i_2 \in R^t$ , we then have  $I_{i_1}^{t-1} \not\subseteq N_{j_1}^{t-1}, \dots, I_{j_n}^{t-1} \not\subseteq N_{i_2}^{t-1}$  and  $I_{j_1}^{t-1} \not\subseteq N_{i_1}^{t-1}, \dots, I_{i_2}^{t-1} \not\subseteq N_{j_n}^{t-1}$ . Since  $I_{i_1}^{t-1} \subseteq N_{i_1}^{t-1}, \dots, I_{i_2}^{t-1} \subseteq N_{i_2}^{t-1}$  by Claim A.1.1, we further have  $\exists k_1 \in R^0[k_1 \in N_{j_1}^{t-1} \setminus I_{i_1}^{t-1}], \dots, \exists k_n \in R^0[k_n \in N_{j_n}^{t-1} \setminus I_{i_2}^{t-1}]$ . Since the state has strong connectedness, there is a  $R^0$  path connecting  $k_1, \dots, k_n$  by Claim A.1.3. But then we have already found  $k_1, k_2$  such that  $k_1 \in N_{j_1}^{t-1} \setminus I_{i_1}^{t-1}$  and  $k_2 \in \bar{G}_{k_1}$ . It is a contradiction that  $i_1 \in C$ .

Now,  $i_1, i_2, i_3$  will form a  $R^t$ -path as  $\{i_1, i_2, i_3\}$ . With the same argument as the above, we then have  $\exists k_1 \in R^0[k_1 \in N_{i_2}^{t-1} \setminus I_{i_1}^{t-1}]$  and  $\exists k_2 \in R^0[k_2 \in N_{i_3}^{t-1} \setminus I_{i_2}^{t-1}]$ , and thus  $i_1$  is not in  $C$ . □

**proof for Lemma 1.4.3**

*Proof.* The proof is done by contradiction. Since  $i \in R^t$ , there is a  $j \in (R^{t-1} \cap \bar{G}_i)$  by Lemma A.1.2. Note that  $N_j^{t-1} \subseteq \bigcup_{k \in N_i^{t-1}} N_k$  since  $N_j^{t-1} = \bigcup_{k \in I_j^{t-2}} N_k$ , and  $I_j^{t-2} \subseteq I_i^{t-1} \subseteq N_i^{t-1}$ . If there is another node outside  $\bigcup_{k \in N_i^{t-1}} N_k$  in  $TR_{ij}$ , then there must be another node such

that there is a path connected to some nodes in  $N_j^{t-1}$  since the network is connected. It is a contradiction that  $i \in C$ .

□

## A.2 EQUILIBRIUM CONSTRUCTION

### A.2.1 EQUILIBRIUM

#### A.2.1.1 OUT-OFF-PATH BELIEF

If Rebel  $i$  detects a deviation at  $m$  period, he forms the belief as

$$\beta_i(\{\theta : \theta \in \times_{j \in G_i} \{\theta_j\} \times \{Inert\}^{n-\#G_i} | h_{G_i}^{m'}\}) = 1, m' \geq m \quad (\text{A.3})$$

#### A.2.1.2 EQUILIBRIUM PATH: NOTATIONS

- $\langle \rangle$  is a finite sequence.
- $|\langle \rangle|$  is the length of finite sequence  $\langle \rangle$ .
- $\langle \rangle_r$  is the set of finite sequences in which the action  $\mathbf{r}$  occurs once and only once.
- $PF(\langle \rangle, m)$  is the  $m$ -periods prefix of a finite sequence  $\langle \rangle$ .
- If  $\langle \rangle \in \langle \rangle_r$ , then let  $||\langle \rangle|| = \arg \min\{m \in \{1, \dots, |\langle \rangle|\} | PF(\langle \rangle, m) \in \langle \rangle_r\}$
- $(i, j)$ -path is the set of paths from  $i$  to  $j$ .
- $\uparrow RP^t$  is the period in the end of  $RP^t$ .

### A.2.1.3 EQUILIBRIUM PATH: REPORTING PERIOD

#### A.2.1.3.1 REPORTING PERIOD: NOTATIONS

- $m$  is a period in reporting period in  $t$  block.
- $O_i^{m,t}$  is the set of  $i$ 's neighbor  $j$  who has played a sequence  $M$  such that  $M = PF(\langle I_j^{t-1} \rangle, m)$  and  $M \in \langle \rangle_r$  at period  $m$ .
- $I_i^{m,t} \equiv (\bigcup_{k \in O_i^{m,t}} I_k^{t-1}) \cup I_i^{t-1}$  is the updated information gathered by  $i$  at period  $m$ .  
Note that  $I_i^{0,t} = I_i^{t-1}$  and  $I_i^{|RP^t|,t} = I_i^t$ .
- $N_i^{m,t} \equiv (\bigcup_{k \in O_i^{m,t}} N_k^{t-1}) \cup N_i^{t-1}$  is the updated neighborhood that contains  $I_i^{m,t}$
- Let

$$EX_{I_i^{m,t}} \equiv \{l \notin N_i^{m,t} | \exists l' \in I_i^{m,t} \text{ such that there exists a } (l, l')\text{-path}\}$$

be all the possible Rebel nodes outside of  $N_i^{m,t}$  given  $I_i^{m,t}$

- Let

$$TR_{I_i^{m,t},j} \equiv TR_{ij} \cap (EX_{I_i^{m,t}} \cup I_i^{m,t})$$

be all the possible Rebel nodes in the  $TR_{ij}$  given  $I_i^{m,t}$ .

#### A.2.1.3.2 REPORTING PERIOD: AUTOMATA

$i \notin R^t$

##### • WHILE LOOP

- At  $m \geq 0$ , if  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} < k$ , report  $\langle \mathbf{stay} \rangle$  and then play  $\mathbf{stay}$  forever.



– Otherwise, **runs POST-CHECK**

$i \in R^t$

• **WHILE LOOP**

– At  $m \geq 0$ , if  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} < k$ , report  $\langle \mathbf{stay} \rangle$  and then play **stay** forever.

– Otherwise, **runs MAIN**

• **MAIN**

At  $m \geq 0$ ,

1. At  $m = 0$  and if  $\#I_i^{t-1} = \#I_i^{0,t} = k - 1$ , then **runs POST-CHECK**

2. At  $m = 0$  and if  $i \in R^t$  and

$$\nexists j \in R^{t-1} \cap \bar{G}_i \text{ such that } \exists l_1, l_2 \in TR_{ij}[[l_1 \in N_j^{t-1} \setminus I_i^{t-1}] \wedge [l_2 \in \bar{G}_i]]]$$

, then runs **CHECK.o**. Otherwise, recall **MAIN**

3. At  $0 \leq m \leq |RP^t| - \|\langle I_i^{t-1} \rangle\|$ , play

**stay**

4. At  $m = |RP^t| - \|\langle I_i^{t-1} \rangle\| + 1$ , then

(a) if  $O_i^{m,t} = \emptyset$ , then report

$\langle I_i^{t-1} \rangle$

(b) if  $O_i^{m,t} \neq \emptyset$ , then **runs CHECK.k**

• **CHECK.o**

At  $m = 0$ , if  $i \in C^t$ , i.e. if  $i \in R^t$  and

$$\nexists j \in R^{t-1} \cap \tilde{G}_i \text{ such that } [\exists l_1, l_2 \in TR_{ij}[[l_1 \in N_j^{t-1} \setminus I_i^{t-1}] \wedge [l_2 \in \tilde{G}_l]]]$$

, then

1. If  $\#C^t = 1$ , then **runs POST-CHECK**
2. If  $\#C^t = 2$ , then denote  $i_1, i_2 \in C$  such that  $I_{i_1}^{t-2} < I_{i_2}^{t-2}$ , and then
  - if  $i = i_1$ , then **runs POST-CHECK**
  - if  $i = i_2$ , then report

$$\langle I_i^{t-1} \rangle$$

• **CHECK.m**

At  $m > 0$ , if  $O_i^{m,t} \neq \emptyset$ , then there are two cases,

1. Case 1: If  $i \in R^t$  and

$$\exists j \in O_i^m \text{ such that } \exists l_1, l_2 \in TR_{ij}^{m,t}[[l_1 \in I_j^{t-1} \setminus I_i^{t-1}] \wedge [l_2 \in \tilde{G}_l]]]$$

, then report

$$\langle I_i^{t-1} \rangle$$

2. Case 2: If  $i \in R^t$  and

$$\nexists j \in O_i^m \text{ such that } \exists l_1, l_2 \in TR_{I_i^{m,t}, j} [[l_1 \in I_j^{t-1} \setminus I_i^{t-1}] \wedge [l_2 \in \tilde{G}_{l_1}]]]$$

(a) Case 2.1: If  $i \in R^t$  and

$$\nexists j \in R^{t-1} \cap (G_i \setminus O_i^{m,t}) \text{ such that } [\exists l_1, l_2 \in TR_{I_i^{m,t}, j} [[l_1 \in N_j^{t-1} \setminus I_i^{t-1}] \wedge [l_2 \in \tilde{G}_{l_2}]]]$$

**Note: this case is the case when  $i \in C$ , thus recall Check.o**

(b) Case 2.2: If  $i \in R^t$  and

$$\exists j \in R^{t-1} \cap (G_i \setminus O_i^{m,t}) \text{ such that } [\exists l_1, l_2 \in TR_{I_i^{m,t}, j} [[l_1 \in N_j^{t-1} \setminus I_i^{t-1}] \wedge [l_2 \in \tilde{G}_{l_2}]]]$$

- if  $\#I_i^{m,t} = k - 1$ , then **runs POST-CHECK**
- if  $\#I_i^{m,t} < k - 1$ , then report

$$\langle I_i^{t-1} \rangle$$

• **CHECK.k**

At  $m \geq 1$ ,

1.  $O_i^{m,t} \neq \emptyset$ , and

$$\#I_i^{m,t} \geq k$$

, then **runs POST-CHECK**

2.  $O_i^{m,t} \neq \emptyset$ , and

$$\#I_i^{m,t} < k$$

, then **runs CHECK.m**

• **POST-CHECK**

1. At  $m = |RP^t|$ , then

(a) If  $i \in R^t$  and if  $\#I_i^{m,t} \geq k - 1$ , then  $i$  plays **revolt**

(b) if  $i \notin R^t$ , then  $i$  plays **stay**

A.2.1.4 EQUILIBRIUM PATH: COORDINATION PERIOD

A.2.1.4.1 COORDINATION PERIOD: NOTATIONS

•  $m$  is a sub-block in the coordination period.

• Let

$$EX_{I_i^t} \equiv \{l \notin I_i^t \mid \exists l' \in I_i^t \setminus I^{t-1} \text{ such that there exists a } (l, l')\text{-path}\}$$

be all the possible Rebel nodes outside of  $N_i^t$  given  $I_i^t$ .

• Let

$$TR_{I_i^t j} \equiv TR_{ij} \cap (EX_{I_i^t} \cup I_i^t)$$

be the set of possible Rebel nodes in the  $TR_{ij}$  given  $I_i^t$ .

A.2.1.4.2 COORDINATION PERIOD: AUTOMATA

- **1st Division**

In 1st division, for  $t = 0$  block,

- If  $\#EX_{I_i^t} \cup I_i^t < k$ , then  $i$  plays **stay** forever.
- If  $\#EX_{I_i^t} \cup I_i^t \geq k$ , and if  $i \notin R^1$ , then  $i$  plays

$\langle \mathbf{stay} \rangle$

- If  $\#EX_{I_i^t} \cup I_i^t \geq k$ , and if  $i \in R^1$ , then  $i$  plays

$\langle x_i \rangle$

In 1st division, for  $t > 0$  block and for  $1 \leq m \leq n$  sub-block,

- If  $i$  has played  $\langle 1 \rangle$ , then  $i$  plays

$\langle x_i \rangle$

- If  $\#EX_{I_i^t} \cup I_i^t < k$ , then  $i$  plays **stay** forever.
- If  $\#EX_{I_i^t} \cup I_i^t \geq k$ , and there are some  $j \in \bar{G}_i$  have played  $\langle \mathbf{stay} \rangle$ , then  $i$  plays **stay** forever.
- If  $\#EX_{I_i^t} \cup I_i^t \geq k$ , and there is no  $j \in \bar{G}_i$  has played  $\langle \mathbf{stay} \rangle$ , then  $i$  plays

$\langle x_i \rangle$

- **2nd Division**

In  $t = 0$  block

- If  $i \notin R^1$ , then  $i$  plays

$\langle \mathbf{stay} \rangle$

.

- If  $i \in R^1$ , and if  $\#I_i^0 \geq k$ , then  $i$  plays

$\langle \mathbf{stay} \rangle$

.

- If  $i \in R^1$ , if  $\#I_i^0 < k$ , if  $\#EX_{I_i^t} \cup I_i^t \geq k$  and if some  $j \in \tilde{G}_i$  has played  $\mathbf{1}_j$  in the 1st division, then  $i$  plays

$\langle \mathbf{stay} \rangle$

.

- If  $i \in R^1$ , if  $\#I_i^0 < k$ , if  $\#EX_{I_i^t} \cup I_i^t \geq k$  and if no  $j \in \tilde{G}_i$  has played  $\mathbf{1}_j$  in the 1st division, then  $i$  plays **stay** forever.

In  $t > 0$  block, if there is no  $j \in G_i$  such that  $j$  has played  $\langle \mathbf{stay} \rangle$  in the **1st Division**, then run the following automata. Otherwise,  $i$  plays **stay** forever.

- $i \notin R^t$

- \* In the 1-sub-block:  $i$  plays

$\langle \mathbf{stay} \rangle$

- \* In the  $2 \leq m \leq t + 1$  sub-blocks:

1. If  $i \in R^{t'}$  for some  $t' \geq 0$  and if there is a  $j \in R^{t'+1} \cap \bar{G}_i$  has played

(a)  $\langle \mathbf{stay} \rangle$  in  $m = 1$  sub-block

(b) or  $\langle \mathbf{1}_j \rangle$  in  $m \geq 2$  sub-blocks

, then  $i$  plays

$\langle x_i \rangle$

in  $m + 1$  sub-block.

2. Otherwise,  $i$  plays

$\langle \mathbf{stay} \rangle$

in current sub-block

–  $i \in R^t$

\* In the 1-sub-block:

1. If  $i$  has played  $\langle \mathbf{1} \rangle$ , then  $i$  plays

$\langle \mathbf{stay} \rangle$

2. If  $i$  has not played  $\langle \mathbf{1} \rangle$  and if there is a  $j \in \bar{G}_i$  has played  $\langle \mathbf{1} \rangle$ , then  $i$  plays

$\langle \mathbf{stay} \rangle$

3. If  $i$  has not played  $\langle \mathbf{1} \rangle$  and if there is no  $j \in \bar{G}_i$  has played  $\langle \mathbf{1} \rangle$ , then

• If  $\#I_i^{|RP^t|,t} \geq k$ , then  $i$  plays

$\langle \mathbf{stay} \rangle$

· If  $\#I_i^{R^{P^t}|,t} < k$ , then  $i$  plays

$\langle \mathbf{1}_i \rangle$

\* In the  $m \geq 2$ -sub-block:

1. If  $i \in R^{t'}$  for some  $t' \geq 0$  and if there is a  $j \in R^{t'} \cap \tilde{G}_i$  has played

(a)  $\langle \mathbf{stay} \rangle$  in  $m = 1$  sub-block, or

(b)  $\langle \mathbf{1}_j \rangle$  in  $m \geq 2$  sub-blocks

, then  $i$  plays

$\langle x_i \rangle$

in  $m + 1$  sub-block.

2. Otherwise,  $i$  plays

$\langle \mathbf{stay} \rangle$

in current sub-block.

### • 3rd Division

#### 1. INITIATING

If  $i$  has observed that  $j \in \tilde{G}_i$  has played

(a)  $\langle \mathbf{stay} \rangle$  in 1-sub-block in **2nd Division** or

(b)  $\langle \mathbf{1}_j \rangle$  in  $m \geq 2$  sub-blocks **2nd Division** or

(c) **s** in the **3rd Division**

, then  $i$  plays **revolt** forever



## 2. NOT INITIATING

Otherwise,  $i$  plays **stay** in current period.

### A.2.1.5 PROOF FOR THEOREM 2

The proof is organized as follows. In Claim A.2.1 and Lemma 1.4.4, I show that a Rebel will learn  $\#[Rebels](\theta) \geq k$  or  $\#[Rebels](\theta) < k$  in the equilibrium path. Lemma 1.4.4 also show that the equilibrium path is ex-post efficient. Since that, there is a  $T$  such that a Rebel's static payoff after  $T$  is 1 if  $\#[Rebels](\theta) \geq k$ ; is 0 if  $\#[Rebels](\theta) < k$ . Such payoff is the maximum static payoff contingent on  $\theta$  after time  $T$ . In Claim A.2.2, I show that if a Rebel makes detectable deviation, then there is a positive probability event  $E$  (by the full support assumption) contingent on this deviation such that his expected static payoff is strictly lower than that in equilibrium path after  $T$ . Finally, in Claim A.2.3, Claim A.2.4, Claim A.2.5, and Claim A.2.6, I show that if a Rebel makes undetectable deviation, then there is a positive probability event  $E$  (by the full support assumption) contingent on this deviation such that his expected static payoff is also strictly lower than that in the equilibrium path after  $T$ . Since the static payoff after  $T$  is maximum for all  $\theta$  in equilibrium path, there is a  $\delta$  such that a Rebel will not deviate. I then conclude this theorem.

To simplify the notations, if  $P(\theta)$  is a property of  $\theta$ , then I abuse the notations by letting  $\beta_{G_i}^{\pi, \tau^*}(P(\theta)|h_{G_i}^m) \equiv \sum_{\theta: P(\theta)} \beta_{G_i}^{\pi, \tau^*}(\theta|h_{G_i}^m)$ . I also say “ $i$  knows  $P(\theta)$ ” to mean  $\beta_{G_i}^{\pi, \tau^*}(P(\theta)|h_{G_i}^m) = 1$ .

**Claim A.2.1.** *Assume that players follow the equilibrium path. For each  $i$ , if  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} \geq$*

$k$ , where  $m$  is a period in  $RP^t$ , then if  $i$  reports  $\langle 1 \rangle$  in  $RP^t$ , then either

*Rebels coordinate to **revolt** after  $t$ -block*

, or

$$\#R^0 < k$$

.

*Proof.* By directly checking the equilibrium path, we have

1. if  $\#I_i^{|RP^t|,t} \geq k$ , then the coordination can be initiated by such  $i$ .
2. if  $\#I_i^{|RP^t|,t} = k - 1$ , and if there is one more node who reported  $\langle 1 \rangle$ , then the coordination can be initiated by  $i$ .
3. if  $\#I_i^{|RP^t|,t} = k - 1$ , and if there are no nodes who reported in current reporting period, then  $\#I_i^{|RP^t|,t} = \#I_i^t = k - 1$ . We now check the conditions guiding  $i$  to **POST-CHECK**.

- If  $i$  is coming from the conditions in **MAIN**, it means that there are no further Rebels outside  $I_i^{t-1}$ , thus outside  $\bigcup_{k \in I_i^{t-1}} G_k$ .
- If  $i$  is coming from the conditions in **CHECK.o**, it means that there are no further Rebels outside  $\bigcup_{k \in I_i^{t-1}} G_k \cap R^0$ , and thus outside  $\bigcup_{k \in I_i^{t-1}} G_k$ .
- If  $i$  is coming from the conditions in **CHECK.m**, it means that there are no further Rebels outside  $\bigcup_{k \in I_i^{t-1}} G_k \cap R^0$ , and thus outside  $\bigcup_{k \in I_i^{t-1}} G_k$ .

Since  $I_i^t = \bigcup_{k \in I_i^{t-1}} G_k \cap R^0 \subset \bigcup_{k \in I_i^{t-1}} G_k$ , and since  $\#I_i^t < k$ , and therefore  $\#R^0 < k$ .

□

**proof for Lemma 1.4.4**

*Proof.* We want to show that all Rebels play **revolt** eventually when  $\theta$  satisfies  $\#[Rebels](\theta) \geq k$ ; all Rebels play **stay** eventually when  $\theta$  satisfies  $\#[Rebels](\theta) < k$ .

1. If all Rebels only play  $\langle I^{t-1} \rangle$  or  $\langle \mathbf{stay} \rangle$  in the reporting period for all  $t \geq 1$  block, then, in the equilibrium path, those nodes played  $\langle I^{t-1} \rangle$  are  $R^t$ -node, and those nodes played  $\langle \mathbf{stay} \rangle$  are non- $R^t$ -nodes.

If there are some Rebels play  $\langle \mathbf{stay} \rangle$  in  $CD_{1,1}^t$ , then all the Rebels play **stay** eventually; If  $R^t$  Rebels play  $\langle \mathbf{stay} \rangle$  in  $CD_{1,2}^t$ , then all the Rebels will play **revolt** after third division in coordination period in this block. Otherwise, all the Rebels go to the next reporting period.

By Theorem 3, there is a  $t^*$  such that there is a  $R^{t^*}$  node knows  $\theta$ , and therefore he knows whether or not  $\theta$  satisfying  $\#[Rebels](\theta) \geq k$  or  $\#[Rebels](\theta) < k$ . In the equilibrium path, such node that plays  $\langle \mathbf{stay} \rangle$  is either in  $CD_{1,1}^{t^*}$  or in  $CD_{1,2}^{t^*}$ . Thus, the equilibrium path is APEX.

2. If there are some Rebels play  $\langle 1 \rangle$  in reporting period in  $t \geq 1$  block, then by Claim A.2.1, such nodes will know whether or not  $\theta$  satisfies  $\#[Rebels](\theta) \geq k$  or  $\#[Rebels](\theta) < k$  after  $RP^t$ . Then  $\langle \mathbf{stay} \rangle$  is either played in the first sub-block in first division or played in the first sub-block in second division in coordination period. Thus, the equilibrium path is APEX.

□

Next, I prepare the claims to show that a Rebel will not deviate from the equilibrium path.

**Claim A.2.2.** *Assume that player  $i$  follows equilibrium path before period  $m$ . Denote  $D$  be the set of Rebels who detect  $i$ 's deviation at  $m$  period. Then if  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} \geq k$ , if  $\#I_i^{m,t} < k$  and if  $D \neq \emptyset$ , there is a  $\delta$  such that  $i$  will not deviate.*

*Proof.* Denote  $D$  as the set of neighbors who detect  $i$ 's deviation. Let

$$\begin{aligned} E_1 &= \{\theta : \#[Rebels](\theta) < k\} \\ E_2 &= \{\theta : k \leq \#[Rebels](\theta) < k + \#D\} \\ E_3 &= \{\theta : \#[Rebels](\theta) \geq k + \#D\} \end{aligned}$$

In the equilibrium path, there is a period  $t^s$  ( $t^f$ ) such that, if  $\theta$  satisfying  $\#[Rebels](\theta) \geq k$  ( $\#[Rebels](\theta) < k$ ) then Rebels play **revolt (stay)** forever. If  $i$  follows the equilibrium path, the expected static payoff after  $\max\{t^s, t^f\}$  is

$$\beta_i(E_2|h_{N_i}^m) + \beta_i(E_3|h_{N_i}^m)$$

If  $i$  deviate, the expected static payoff after  $\max\{t^s, t^f\}$  is

$$\beta_i(E_3|h_{N_i}^m)$$

Therefore there is a loss in expected static payoff of

$$\beta_i(E_2|h_{N_i}^m)$$

Thus, there is a loss in expected continuation payoff contingent on  $E_2$  by

$$\delta^{\max\{t^s, t^f\}} \frac{\beta_i(E_2 | h_{N_i}^m)}{1 - \delta}$$

Note that  $\beta_i(E_2 | h_{N_i}^m) > 0$ . This is because  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} \geq k$ , and therefore  $\beta_i(\#[Rebels])(\theta) \geq k | h_{N_i}^m) > 0$  by full support assumption.  $\square$

Next, I prepare the claims to show that a Rebel will not deviate if such deviation is undetectable.

**Claim A.2.3.** *Assume that player  $i$  follows equilibrium path before period  $m$ . Then if  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} \geq k$ , if  $m$  is a period in  $RP^t$ , if  $\#I_i^{m,t} < k$ , then there is a  $\delta$  such that  $i$  will not deviate by reporting  $\bar{I}_i^{t-1} \neq I_i^{t-1}$  if such deviation is not detected by  $i$ 's neighbor.*

*Proof.* Assume  $\bar{I}_i^{t-1} \neq I_i^{t-1}$ . Since a detection of deviation has not yet occurred, it must be the case that there is a non-empty set  $F = \{j \in \bar{I}_i^{t-1} : \theta_j = Inerts\}^1$ .

Let

$$E_1 = \{\bar{\theta} : \bar{\theta}_j = Rebel \text{ if } j \in F \text{ and } \bar{\theta}_k = \theta_k \text{ if } k \notin F\}$$

, and let

$$E_2 = \{\theta : \theta_j = Inert \text{ if } j \in F \text{ and } \bar{\theta}_k = \theta_k \text{ if } k \notin F\}$$

.

---

<sup>1</sup>Otherwise, there is a detection of deviation. Recall the definition in information hierarchy:  $I_i^{-1} \subset I_i^0 \subset \dots \subset I_i^{t-1}$  for all  $i \in R^0$

Then consider the event

$$\begin{aligned} E &= \{\bar{\theta} \in E_1 : \#[Rebels](\bar{\theta}) \geq k\} \\ &= \{\theta \in E_2 : \#[Rebels](\theta) \geq k - \#F\} \end{aligned}$$

Partition  $E = E_3 \cup E_4$ , where

$$\begin{aligned} E_3 &= \{\theta \in E_2 : \#[Rebels](\theta) \geq k\} \\ E_4 &= \{\theta \in E_2 : k > \#[Rebels](\theta) \geq k - \#F\} \end{aligned}$$

By Lemma 3 and by checking the strategies in equilibrium path (since  $i$  has not been detected), there is a block  $\bar{t}^s$  with respect to  $\bar{\theta}$  such that, if  $\bar{\theta} \in E$ , then there are some  $R^{\bar{t}^s}$ -Rebel  $js$ , denoted as  $J$ , will initiate the coordination, and hence Rebels will play **revolt** forever after  $\bar{t}^s$ -block. Note that such  $j$  is with  $\#I_j^{\bar{t}^s} \geq k$  by checking the equilibrium path.

We have several cases:

1. Case 1: If  $i \in J$ , his own initiation will only depends on  $\#I_i^{\bar{t}^s}$  by Claim A.2.4 and Claim A.2.5. He is strictly better off by not deviating since playing  $\langle \bar{I}_i^{t-1} \rangle$  is more costly than  $\langle I_i^{t-1} \rangle$  (since  $X_{\bar{I}_i^{t-1}} > X_{I_i^{t-1}}$ ).
2. Case 2: If there is another  $j$  such that  $\bar{I}_i^{t-1} \notin I_j^{\bar{t}^s}$ , then since such  $j$ 's initiation of coordination dependent on his own information  $I_j^{\bar{t}^s}$  by Claim A.2.4 and Claim A.2.5, and since  $i$ 's deviation does not change  $j$ 's information,  $i$  is strictly better by not deviating since playing  $\langle \bar{I}_i^{t-1} \rangle$  is more costly than  $\langle I_i^{t-1} \rangle$  (since  $X_{\bar{I}_i^{t-1}} > X_{I_i^{t-1}}$ ).
3. Case 3: Suppose there is another  $j$  such that  $\bar{I}_i^{t-1} \subset I_j^{\bar{t}^s}$  and  $\#I_i^{\bar{t}^s} \geq k$ , then such  $j$  will

initiate the coordination to **revolt** at  $\bar{t}^s$  block. If  $i$  does not follow  $j$ 's initiation of coordination, then there is a detection of deviation by checking the equilibrium path. In this situation,  $i$  will not deviate as Claim A.2.2 shows. If  $i$  follows, and  $\#I_i^{\bar{t}^s} \geq s$ , then  $i$  is in the Case 1, and therefore  $i$  is better off by staying in the equilibrium path. If  $i$  follows, but  $\#I_i^{\bar{t}^s} < s$ , then  $i$ 's expected static payoff after  $\bar{t}^s$  is at most

$$\max\{\beta_i(E_3|h_{N_i}^m) \times 1 + \beta_i(E_4|h_{N_i}^m) \times (-1), 0\}$$

However, if  $i$  follows the equilibrium path, there are  $t^s, t^f$  such that the expected static payoff after  $\max\{t^s, t^f\}$  is

$$\max\{\beta_i(E_3|h_{N_i}^{m'}), 0\}$$

Thus, there is a loss in expected continuation payoff contingent on  $E$  by

$$\delta^{\max\{t^s, t^f\}} \frac{\min\{\beta_i(E_3|h_{G_i}^m), \beta_i(E_4|h_{G_i}^m)\}}{1 - \delta}$$

Note that  $\beta_i(E_3|h_{N_i}^m) > 0$  and  $\beta_i(E_4|h_{N_i}^m) > 0$ . This is because  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} \geq k$  and  $\#I_i^{m,t} < k$ , and therefore  $1 > \beta_i(\#[Rebels](\theta) \geq k|h_{N_i}^m) > 0$  by full support assumption.

□

**Claim A.2.4.** *Assume that player  $i$  follows equilibrium path before period  $m$ . Then if  $\#EX_{I_i^{m,t}} \cup I_i^{m,t} \geq k$ , if  $m$  is a period in  $RP^t$ , if  $\#I_i^{m,t} \leq k - 1$ , then  $i$  will not play  $\langle 1 \rangle$  if  $i \notin C^t$  or  $i$  is not allowed to play  $\langle 1 \rangle$  according to the equilibrium path.*

*Proof.* Let

$$E' = \{\theta : \#I_i^{RP^t,t} \leq k - 1\}$$

. Note that such event is not empty by checking the timing where  $i$  deviated:

1. If  $i$  has a neighbor  $j \in C^t$ , then  $j \notin O_i^{RP^t,t}$ , and therefore we can construct  $E'$  by assuming that all other neighbors (other than  $i, j$  and other than  $l \in O_i^{m,t}$ ) are non- $R^t$ .

2. If

$$\exists j \in R^{t-1} \cap \tilde{G}_i \text{ such that } \exists k_1, k_2 \in TR_{ij}[[k_1 \in N_j^{t-1} \setminus I_i^{t-1}] \wedge [k_2 \in \tilde{G}_{k_2}]]$$

, then just let  $E' = \{\theta : N_i^t \cap R^0 \leq k - 1\} = \{\theta : I_i^t \leq k - 1\}$ <sup>2</sup>.

Next, let

$$E_1 = \{\theta : \#[Reble](\theta) < k\} \cap E'$$

$$E_2 = \{\theta : \#[Reble](\theta) \geq k\} \cap E'$$

Note that  $E_1$  and  $E_2$  are not empty. According to the equilibrium path, if  $i$  does not meet the criteria to play  $\langle 1 \rangle$ , it must be the case that there are some nodes outside  $I_i^t$  but there is a path consisting of Rebels to connect them. By strong connectedness,  $E_1$  and  $E_2$  are not empty.

If  $i$  deviates to play  $\langle 1 \rangle$ , his behavior after  $CD_{1,1}^t$  will have the following consequences:

---

<sup>2</sup>note that  $I_i^t = I_i^{RP^t,t}$



1. If  $i$  plays **<stay>** in  $CD_{1,1}^t$ , then the coordination to **stay** starts after  $CD_{1,1}^t$ .
2. If  $i$  plays  $\langle x_i \rangle$  in  $CD_{1,1}^t$ , then the coordination to **revolt** will be initiated after  $CD_{1,2}^t$  if he mimics the behavior of a pivotal player (i.e., by mimicking those players who played  $\langle 1 \rangle$  in the equilibrium path).
3. If  $i$  plays  $\langle x_i \rangle$  in  $CD_{1,1}^t$ , but he does not mimic the behavior of pivotal player, then such deviation will be detected.

Thus,  $i$ 's expected static payoff after the coordination period in this  $t$ -block is at most

$$\max\{\beta_i(E_2|h_{N_i}^m) \times 1 + \beta_i(E_1|h_{N_i}^m) \times (-1), 0\}$$

However, if he stay in the equilibrium, there is a  $t^s$  ( $t^f$ ) such that Rebels play **revolt** (**stay**) contingent on  $E_2$  ( $E_1$ ), and thus after  $t^* = \max\{t^s, t^f\}$  he get the expected static payoff as

$$\max\{\beta_i(E_2|h_{N_i}^m) \times 1, 0\}$$

After some calculation, after  $t^*$ , there is a loss of

$$\delta^{t^*} \frac{\min\{\beta_i(E_2|h_{G_i}^m), \beta_i(E_1|h_{G_i}^m)\}}{1 - \delta}$$

Note that  $\beta_i(E_1|h_{N_i}^m) > 0$  and  $\beta_i(E_2|h_{N_i}^m) > 0$ . This is because  $E_1$  and  $E_2$  are not empty and by the full support assumption.

□

**Claim A.2.5.** Assume that player  $i$  follows equilibrium path before  $\uparrow RP^t - 1$  period. Then if  $\beta_i(\#[Rebels](\theta) \geq k|h_{G_i}^{\uparrow RP^t-1}) > 0$ , then if  $i$  can report  $\langle 1 \rangle$ ,  $i$  will not report  $\langle \text{stay} \rangle$  when  $\delta$  is high enough.

*Proof.* There are two cases in which  $i$  can play  $\langle 1 \rangle$  in the equilibrium path:

- Case 1: If  $\#I_i^{|RP^t|-1,t} \geq k$ , let the event  $E$  be

$$E = \{\theta : \#[Rebels](\theta) = \#I_i^{|RP^t|,t}\}$$

In words,  $E$  is the event in which no more Rebels outside  $i$ 's information  $I_i^{|RP^t|,t}$ . Contingent on  $E$ , there is no more Rebel can initiate the coordination. This is because for all  $j \in O_i^{|RP^t|-1,t}$ ,  $j$  is with  $\#I_j^{t-1} < k - 1$ , and because, for all  $j \in \bar{G}_i$  who have not yet reported,  $j \notin R^t$  (since all Rebels are in  $I_i^{|RP^t|-1,t}$ ). Since only  $i$  can initiate the coordination, if  $i$  deviated, then there is a loss in expected continuation payoff as

$$\delta^q \frac{\beta_i(E|h_{G_i}^{\uparrow RP^t-1})}{1 - \delta}$$

, where  $q$  is a period after  $t$ -block.

- Case 2: If  $\#I_i^{|RP^t|-1,t} = k - 1$ , since  $\beta_i(\#[Rebels](\theta) \geq k|h_{G_i}^{\uparrow RP^t}) > 0$ , the following event  $E_1$  must have positive probability

$$E_1 = \{\theta : \exists j \in \bar{G}_i, j \notin O_i^{|RP^t|-1,t} [\#I_j^{|RP^t|-1,t} \geq k - 1]\}$$

3.

---

<sup>3</sup>otherwise, since no neighbors will report after the current period, we must have  $\beta_i(\#[Rebels](\theta) \geq$

Let  $E'_1 \subset E_1$  such that

$$E'_1 = \{\theta : \text{exist a unique } j \in \bar{G}_i, j \notin O_i^{|RP^t|-1,t}[\#I_j^{|RP^t|-1,t} \geq k-1]\}$$

Note that this  $E'_1$  can be constructed if the network is acyclic. The construction for  $E'_1$  is as follows. If there is  $\theta \in E'_1$  admits 2 or more  $js$  in the definition  $E_1$ , these  $js$  are not each others' neighbor. Then, if there are two  $js$ , says  $j, j'$ , at least one of them is in  $I_j^{|RP^t|-1,t}$ , but another is outside of  $I_{j'}^{|RP^t|-1,t}$ . We can then find another state that is in  $E'_1$  by picking a  $j$ , and supposing those nodes outside  $I_j^{|RP^t|-1,t}$  are all Inerts.

Now, dependent on such  $j$  we have picked, let

$$E = \{\theta : \#[Rebels](\theta) = \#I_j^{|RP^t|-1,t} \cup I_i^{|RP^t|-1,t}\}$$

If  $i$  reports  $\langle \text{stay} \rangle$ , since there is no more Rebel outside  $I_j^{|RP^t|-1,t} \cup I_i^{|RP^t|-1,t}$  contingent on  $E$  and since  $\#I_j^{|RP^t|-1,t} = \#I_j^t < k$ , therefore there is no coordination to **revolt**.

However, if  $i$  plays  $\langle 1 \rangle$ , coordination can be initiated by himself in the following coordination period. Thus, there is a loss in expected continuation payoff by

$$\delta^q \frac{\beta_i(E|h_{G_i}^{\uparrow RP^t-1})}{1-\delta}$$

, where  $q$  is a period after  $t$ -block.

---


$$k|h_{G_i}^{\uparrow RP^t} = 0$$

□

**Claim A.2.6.** Assume that player  $i$  follows equilibrium path before  $\uparrow RP^t$ . Then, suppose there is no  $j \in G_i$  has played  $\langle 1 \rangle$  in  $RP^t$ , suppose  $\#I_i^t < k$ , and suppose  $\#EX_{I_i^t} \cup I_i^t \geq k$ , then there is  $\delta$  such that

- if  $i$  has not observed  $\langle \mathbf{stay} \rangle$  played by  $j \in G_i$  in  $CD_{1,2}^t$ , or
- if  $i$  has not observed  $\langle \mathbf{1}_j \rangle$  played by  $j \in G_i$  in  $CD_{q,2}^t$ ,  $g \geq 2$

, then  $i$  will not play

- $\langle \mathbf{stay} \rangle$  in  $CD_{1,2}^t$  and
- $\langle \mathbf{1}_j \rangle$  in  $CD_{q+1,2}^t$ ,  $g \geq 2$

*Proof.* If  $i$  deviates, all  $i$ 's neighbors who do not detect the deviation will play **revolt** after coordination period in this block; if  $i$ 's deviation is detected by some neighbors, we are in the case of Claim A.2.2 and so that  $i$  will not deviate. We then check the case in which  $i$  deviates while no neighbors detecting it. Let

$$E' = \{\theta : \#I_i^t \leq k - 1\}$$

and let

$$E_1 = \{\theta : \#[Reble](\theta) < k\} \cap E'$$

$$E_2 = \{\theta : \#[Reble](\theta) \geq k\} \cap E'$$

Since  $\#I_i^t < k$  and  $\#EX_{I_i^t} \cup I_i^t \geq k$ , due to the full support assumption and the equilibrium strategies played by  $i$ 's neighbors, we have

$$0 < \beta_i(\#[Rebels])(\theta) \geq k|h_{G_i}^{\uparrow RP^t} < 1$$

. Since that,  $E_1$  or  $E_2$  has positive probability.

If  $i$  deviates, since all Rebels will play **revolt** after this block, and therefore  $i$ 's expected static payoff after the coordination period in this  $t$ -block is at most

$$\max\{\beta_i(E_2|h_{N_i}^{\uparrow RP^t}) \times 1 + \beta_i(E_1|h_{N_i}^{\uparrow RP^t}) \times (-1), 0\}$$

However, if he stay in the equilibrium path, there is a  $t^s$  ( $t^f$ ) such that Rebels play **revolt** (**stay**) contingent on  $E_2$  ( $E_1$ ), and thus after  $t^* = \max\{t^s, t^f\}$  he get the expected payoff as

$$\max\{\beta_i(E_2|h_{N_i}^{\uparrow RP^t}) \times 1, 0\}$$

After some calculation, after  $t^*$ , there is a loss of

$$\delta^{t^*} \frac{\min\{\beta_i(E_2|h_{G_i}^m), \beta_i(E_1|h_{G_i}^m)\}}{1 - \delta}$$

□

After the above claims, we can take a sufficiently high  $\delta$  to let all the above claims hold. Since a deviation is either detectable or non-detectable, and a deviation happens either in reporting period or coordination period, I conclude that this theorem holds by the

above claims.

# B

## Chapter 2

## B.1 FORMAL DEFINITION AND PROOFS

### B.1.1 DEFINITION OF FORWARDING

Denote  $\Gamma(G)$  as an extension of  $G$  such that, for all  $L \in \mathbb{N}$ , it allows  $L$  stages of communication before  $G$  is played. Let  $l \in \{1, \dots, L\}$ . At  $l$ -stage, there is a countable set of messages denoted as  $M_i^l$  with generic elements  $m_i^l$  and three elements, **STOP**, **FALSE**, and **OK**, for each player  $i \in I$ . Player  $i$  sends a subset of messages in  $M_i^l$  or receive a subset of messages in  $\times_{j \neq i} M_j^l$ . Denote  $O_{i,s}^l \subset M_i^l$  as the set of messages sent by player  $i$ . Denote  $O_{i,r}^l \subset \times_{j \neq i} M_j^l$  as the set of messages received by player  $i$ . Players have perfect recall.

Let  $\mathbf{L}$  be a countable set with elements  $\mathbf{l}$ . A letter authenticated by  $i$  is a tuple and denoted as  $\langle i, \mathbf{l} \rangle$ . The tuple  $(\langle i, \mathbf{l} \rangle, M_i^l, O_{i,s}^l, O_{i,r}^l, \mathbf{fw}_i^l)$  is recursively defined as follows.

- $\mathbf{fw}_i^l : O_{i,r}^l \rightarrow M_i^{l+1}$
- $\langle i, \mathbf{l} \rangle \in M_i^l$
- $\mathbf{fw}_i^l(\langle j, \mathbf{l} \rangle) = \langle j, \mathbf{l} \rangle$

, for all  $i$ , for all  $\mathbf{l} \in \mathbf{L}$ , for all  $L \in \mathcal{N}$ , for all  $l \in \{1, \dots, L\}$ .

In short,  $\mathbf{fw}_i^l$  is a function depicting that player  $i$  forward a message in  $O_{i,r}^l$  to some players by transforming it to a message in  $M_i^{l+1}$ . Players can cheap talk and forward messages since  $\langle i, n \rangle \in M_i^l$  and  $\mathbf{fw}_i^l(\langle j, n \rangle) = \langle j, n \rangle$ , for all  $i$ , for all  $\mathbf{l} \in \mathbf{L}$ , for all  $L \in \mathcal{N}$ , for all  $l \in \{1, \dots, L\}$ .



## B.1.2 PROOF FOR THEOREM 4

### B.1.2.1 THE PROTOCOL

For convenience, let  $A_i = \{1, \dots, |A_i|\}$  be  $i$ 's action set with generic element  $a_i$  for  $i = 1, 2, 3$ , where  $|A_i|$  is the cardinality of  $A_i$ . Assume  $q$  is a rational distribution. Let  $\text{lcm}_q$  be the least common multiple of the denominators of the list of reduced fractions  $(q(a))_{a \in A_1 \times A_2 \times A_3, q(a) \neq 0}$ . Let  $P = \{1, \dots, \text{lcm}_q\}$  and let  $r : P \rightarrow A_1 \times A_2 \times A_3$  be a function such that  $\frac{|\{p \in P | r(p) = a\}|}{\text{lcm}_q} = q(a)$ . Denote  $\text{lcm}_{a_1} = |\{p \in P | r(p)_1 = a_1\}|$ .

Let  $C = A_2 \times A_3 \times V \times U$  be the set of categories with generic element  $c$ . Let  $T = \{1, \dots, |T|\}$ , where  $|T| = |C| \sum_{a_1} \text{lcm}_{a_1}$ . The set of notes is denoted by  $N = A_2 \times A_3 \times V \times T \cup \{\text{OK}, \text{FALSE}, \text{STOP}\}$ . The  $j$ th element in  $c$  (or  $n$ ) will be denoted as  $c_j$  (or  $n_j$ ).

- Step 1:

While Player 2 is the dummy, Player 1 and Player 3 jointly choose two kinds of permutations. They jointly choose a permutation  $\phi$  from  $\wp(T)$  with probability  $1/|\wp(T)|$ ; for each  $n_2 \in A_3$ , they jointly choose a permutation  $\theta_{n_2}$  from  $\wp(V)$  with probability  $1/|\wp(V)|$ . All the permutation are chosen independently.

Let  $F$  be the set of subjective functions  $f : T \rightarrow A_1 \times C$  satisfying  $|\{t \in T | f(t) = (a_1, c)\}| = \text{lcm}_{a_1}$ . While Player 2 is the dummy, Player 1 and Player 3 jointly select a function  $f$  from  $F$  with probability  $1/|F|$  and independently from the above chosen permutations. The  $j$ th element in  $f(t)$  will be denoted as  $f(t)_j$  for some  $t \in T$ . If  $f(t)_j$  is a vector, then further denote  $f(t)_{j,l}$  as the  $l$ th element in  $f(t)_j$ .

Denote  $N_{a_1, c} \subset N$  as the set of notes issued by Player 1 with Player 1's authentication for each  $a_1 \in A_1$  and  $c \in C$ .  $N_{a_1, c}$  satisfies following conditions, **C.1-C.6**, which are

known to all players:

1. **C.1** For all  $a_1 \in A_1$ , for all  $c \in C$ ,

$$|N_{a_1,c}| = \text{lcm}_{a_1}$$

2. **C.2** For all  $a_1 \in A_1$ , for all  $c \in C$ ,

$$\frac{|N_{a_1,c}|}{\sum_{a_1} |N_{a_1,c}|} \frac{|\{n \in N_{a_1,c} | n_1 + c_1 \equiv a_2 \pmod{|A_2|}, n_2 + c_2 \equiv a_3 \pmod{|A_3|}\}|}{|N_{a_1,c}|} = q(a)$$

3. **C.3** For all  $a_1 \in A_1$ , for all  $c \in C$ , for all  $n \in N_{a_1,c}$ ,

$$n_3 = \theta_{n_3}(c_3)$$

4. **C.4** For all  $a_1 \in A_1$ , for all  $c \in C$ , for all  $n \in N_{a_1,c}$ ,

$$n_4 \in \{t \in T | f(\phi(t)) = (a_1, c)\}$$

5. **C.5** For all  $a_1 \in A_1$ , for all  $c \in C$ , for all  $n \in N_{a_1,c}$ ,

$$\text{If } n \neq n', \text{ then } n_4 \neq n'_4 \text{ for all } n, n' \in N_{a_1,c}$$

*Remark.* **C.1** says that each category has the same amount of notes. **C.1** characterizes the notes in each category, which will determine the recommended actions. Different categories are thus different kinds of copies of other categories. By **C.3**,

the third element of a note is an index attached to the second element of such note. Moreover, this index is only varied with  $c_3 \in V$ . **C.4** roughly states that the relationship between the first element and the function  $f$  has been perturbed by the permutation  $\phi$ . By combining **C.4** and **C.5**, and by the fact that  $f$  is a function, each note is indexed by distinguished  $t \in T$  in the fourth element.

- In Step 2, players first perform a  $|T|$  sub-steps Randomized Forwarding<sup>1</sup>. That is to say, for each sub-step  $1 \leq t \leq |T|$ , Player 3 asks Player 1 to pass all the notes in  $N_{f(t)}$  to him. Player 3 and Player 2 randomly select a note from  $N_{f(t)}$ , denoted as  $k(t)$ , with probability  $1/|N_{f(t)}|$ , and then Player 3 forwards such note to Player 2.

After  $|T|$  sub-steps Randomized Forwarding, Player 2 and Player 3 have both observed a list of notes authenticated by Player 1. Denote this list of notes by  $k = (k(t))_{t \in T}$ , and denote the  $j$ th element of  $k(t)$  for some  $t \in T$  by  $k(t)_j$ .

- In Step 3, Player 2 and Player 3 check if  $(k(t)_4)_{t \in T}$  is without repetition. If this is so, Player 2 and Player 3 both send **OK** to Player 1, and then players continue to Step 4; otherwise, Player 2 and Player 3 both send **FALSE** to player 1, and then all players restart Step 0.
- In Step 4, Player 1 and Player 2 jointly pick an element  $x \in T$  with probability  $1/|T|$ . Player 2 reports  $(k(x)_2, k(x)_3)$  to Player 3 by cheap talk. Players continue to Step 5.1.
- In Step 5.1, simultaneously,

---

<sup>1</sup>as the sub-procedure from **STEP 2** to **STEP 4** in Example 1

- Player 1 reports  $m^2 = f(x)_{2,1}$  to Player 2.
- Player 1 reports  $m^3 = (f(x)_{2,1}, f(x)_{2,2}, f(x)_{2,3}, f(x)_{2,3})$  to Player 3.
- Player 3 report  $\theta_{k(x)_3}^{-1}(k(x)_2)$  to Player 1.

If  $f(x)_{2,3} \neq \theta_{k(x)_3}^{-1}(k(x)_2)$ , then Player 1 and Player 3 send **STOP** to the other players. After that, players stop the protocol and play the worst Nash equilibrium. Otherwise, all players go to Step 5.2.

Denote the  $j$ th element in  $m^2$  or  $m^3$  by  $m_j^2$  or  $m_j^3$ .

- In Step 5.2, Player 3 constructs a set  $D$  and report this set to Player 2. First, let

$$E_{c_1, c_2, c_3, c_4} = \{t | (f(t)_{2,1}, f(t)_{2,2}, f(t)_{2,3}, f(t)_{2,4}) = (c_1, c_2, c_3, c_4)\}$$

. Then for each  $c'_2 \in A_2, c'_2 \neq m_2^3$ , he randomly chooses an element  $u_{c'_2} \in U$  with probability  $1/|U|$ . Then let  $D' = \bigcup_{c'_2 \in A_2, c'_2 \neq m_2^3} E_{m_1^3, c'_2, m_3^3, d_{c'_2}}$ , and let  $D'' = E_{m_1^3, m_2^3, m_3^3, m_4^3}$ . Finally, he reports  $D = D' \cup D''$  to Player 2 .

All players then go to Step 5.3.

- In Step 5.3, Player 2 check
  - if  $x \in D$ ,
  - if  $m^2 = m^3$ , and
  - if there exists a  $f' \in F$ , a  $\bar{c}_3 \in V$ , such that  $k(t) \in \bigcup_{a_1, c \in C, c_1 = m^2, c_3 = \bar{c}_3} N_{a_1, c}$  for all  $t \in D$ .

If one of the above criteria fails, Player 2 sends **STOP** to the other players, while the other players (Player 1 or Player 3) who let these criteria fail *also* send **STOP** to others<sup>2</sup>; otherwise, all players send **OK** to others and then go to Step 6.

- Step 6 is the final step in which player get their recommended actions.
  - Player 1's recommended action is  $f(x)_1$ .
  - Player 2's recommended action is  $k(x)_1 + m^2(\text{mod}|A_2|)$ .
  - Player 3's recommended action is  $k(x)_2 + m^3(\text{mod}|A_3|)$ .

I list some observations for later exposition.

**Observation B.1.1.** *Given  $x, x', x'' \in X$ , if  $x + x' \equiv x + x'' \pmod{|X|}$ , then  $x' = x''$ .*

**Observation B.1.2.** *Given the action profile  $a$ ,*

$$|\{n \in N_{a_1, c} | n_1 + c_1 \equiv a_2(\text{mod}|A_2|), n_2 + c_2 \equiv a_3(\text{mod}|A_3|)\}|$$

*is the same for all  $c$ .*

**Observation B.1.3.**  *$N_{a_1, c} \cap N_{a'_1, c'} = \emptyset$  for all  $a_1 \neq a'_1$  and for all  $c \neq c'$ .*

I begin to prove Theorem 4. To ease reading and save notations,  $n_j + c_j \equiv a_{j+1}(\text{mod}|A_{j+1}|)$  will be written as  $n_j + c_j \equiv a_{j+1}$ . And  $n_j + c_j \equiv n'_j + c'_j(\text{mod}|A_{j+1}|)$  will be written as  $n_j + c_j \equiv n'_j + c'_j$  for all  $n_j, n'_j, c_j, c'_j \in A_{j+1}$ .

---

<sup>2</sup>In short, the player who detects deviation sends **STOP**, and the player who deviates also sends **STOP**.

### B.1.2.2 DEVIATION DETECTING

In the following lemma, I show that the unitary deviation will be detected with probability larger than  $\min\{1 - 1/|V|, 1 - 1/|U|\}$ .

**Lemma B.1.1.** *Despite the J.C.L. procedure, the unitary deviation can be detected with probability larger than  $\min\{1 - 1/|V|, 1 - 1/|U|\}$ .*

*Proof.* In Step 1, if Player 1 do not follow the protocol to authenticate his notes, since the outcome of  $\theta_{n_2}$  is known to Player 1 and Player 3 by J.C.L., then Player 3 will detect Player 1's deviation in the Randomized Forwarding procedure in Step 2. In Step 2, players' deviation will be detected for sure since they are in the Randomized Forwarding procedure. In Step 3, if there is a repetition in  $(k(t)_4)_{t \in T}$ , then it will be detected by both Player 2 and Player 3, and therefore by Player 1. I then check the deviation during Step 4 to Step 5.3.

In Step 4, if Player 2 reports  $k'(x)_2 = k(x)_2$  and  $k'(x)_3 \neq k(x)_3$ , then  $\theta_{k_2^x}^{-1}(k'(x)_3) \neq \theta_{k_2^x}^{-1}(k(x)_3)$ , therefore  $\theta_{k_2^x}^{-1}(k'(x)_3) \neq f(x)_{2,3}$ , and hence it will be detected for sure in Step 5.1. If Player 2 reports  $k'(x)_2 \neq k(x)_2$  but  $k'(x)_3 = k(x)_3$  or  $k'(x)_3 \neq k(x)_3$ , then there is a probability  $1/|V|$  such that  $\theta_{k_2^x}^{-1}(k'(x)_3) = f(x)_{2,3}$ , and therefore it will be detected with probability  $1 - 1/|V|$  in Step 5.1.

In Step 5.1, if  $m^{3'} \neq m^3$ , then the probability that  $x \in D''$  is zero by the definition of  $D''$ . Now I check the probability that  $x \in D'$ . By the construction in Step 5.3, if  $m^{3'}_1 \neq m^3_1$  or  $m^{3'}_3 \neq m^3_3$ , then  $x \notin D$  for sure. Now I check the case when  $m^{3'}_2 \neq m^3_2$  or  $m^{3'}_4 \neq m^3_4$ . Since there are  $|U|$  candidates  $d_{c'_2}$  for each  $c'_2$  to construct  $E_{m_1^3, c'_2, m_3^3, d_{c'_2}}$ . The probability that  $x \in D'$  is less than  $1/|U|$ , and hence Player 1's deviation can be detected with probability

larger than  $1 - 1/|U|$  in Step 5.3.

Finally I check Player 3's deviation in Step 5.2. There are two possible deviations: reporting another set instead of  $D$ , or reporting  $m_1^3$  instead of  $m_1^3$ . The first kind of deviation can be detected with probability larger than  $1 - 1/|U|$  as if it were Player 1's deviation in Step 5.1. The second kind of deviations is detected for sure since  $m^2 \neq m_1^3$ .  $\square$

### B.1.2.3 CONDITIONAL PROBABILITIES

In the next three sections, I will show that, if players have not yet received **STOP** during the protocol, a player conditional probability over other players' recommended actions conditional on his own recommended action is the same as that induced by  $q$  in Step 6.

Let

$$\Pr(k, f, \phi, (\theta_{n_4})_{n_4 \in A_3}, x)$$

be the joint probability induced by the protocol through Step 1 to Step 4.

After Step 4 and before Step 5.1, Player 2 observes  $(k, x)$ , but does not observe the chosen  $(f, \phi, (\theta_{n_4})_{n_4 \in A_3})$ ; Player 1 observes  $(f, \phi, (\theta_{n_4})_{n_4 \in A_3}, x)$ , but not  $k$ ; Player 3 observes  $(k, f, \phi, (\theta_{n_4})_{n_4 \in A_3})$  but not  $x$ .

To ease the reading, the main lemmas are Lemma B.1.7, Lemma B.1.8, and Lemma B.1.9.

### PLAYER 2'S CONDITIONAL PROBABILITIES OVER PLAYERS' RECOMMENDED ACTIONS

I begin with Player 2. Let's define the consistency of  $f$  given Player 2's observation as follows.

**Definition B.1.1** ( $f$  is consistent with  $k$ ). *Given a list of notes  $k$  observed by Player 2, a*

function  $f$  is consistent with  $k$  if and only if  $f$  is a function in  $F$  and  $k(t) \in N_{f(t)}$  for all  $t \in T$ .

The following lemma shows Player 2's conditional probability at  $f(x) = (a_1, c)$  after he observes  $(k, x)$ .

**Lemma B.1.2.** *Given  $x \in T$ , given  $f$  that is consistent with  $k$ , then*

$$\Pr(f(x) = (a_1, c) | k(x) = \bar{n}, k) = \frac{|\{n \in N_{a_1, c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1} \sum_c |\{n \in N_{a_1, c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}$$

*Proof.* Let  $f_k$  be a function consistent with  $k$ . Denote  $T_{\bar{n}} = \{t | k(t)_1 = \bar{n}_1, k(t)_2 = \bar{n}_2\}$ . Then define

$$F_{k, f_k, T_{\bar{n}}} = \{f \in F | \forall t' \notin T_{\bar{n}} [f(t') = f_k(t')] \text{ and } \forall t' \in T_{\bar{n}} [k(t') \in N_{f(t')}]\}$$

. It is straightforward to show that the cardinality of  $F_{k, f_k, T_{\bar{n}}}$  is not dependent on how such  $f_k$  is chosen: if there are two functions  $f_k, f'_k$  that are consistent with  $k$ , and there is a function  $f \in F_{k, f_k, T_{\bar{n}}}$ , then we can define a  $f'$  such that  $f'(t) = f(t)$  if  $t \in T_{\bar{n}}$  and  $f'(t) = f'_k(t)$  if  $t \notin T_{\bar{n}}$ . Then  $f'$  will be a function in  $F_{k, f'_k, T_{\bar{n}}}$ , and therefore  $|F_{k, f_k, T_{\bar{n}}}| = |F_{k, f'_k, T_{\bar{n}}}|$ .

Next, let's define

$$T_{f_k, (a_1, c), \bar{n}} = \{t \in T_{\bar{n}} | f_k(t) = (a_1, c)\}$$

for all  $(a_1, c)$ . Then I can characterize the cardinality of  $F_{k, f_k, T_{\bar{n}}}$  by the following claim.

**Claim B.1.1.**  *$f \in F_{k, f_k, T_{\bar{n}}}$  if and only if there is a multiset combination in  $T_{\bar{n}}$  by multisets  $(D_{f, (a_1, c), \bar{n}})_{a_1, c}$ , which satisfy*



1. for each  $(a_1, c)$ ,

$$|D_{f,(a_1,c),\bar{n}}| = |T_{f_k,(a_1,c),\bar{n}}| \quad (\text{B.1})$$

2. for every  $\bar{c}_3 \in V$ , for every  $t, t' \in \bigcup_{c \in C, c_3 = \bar{c}_3} D_{f,(a_1,c),\bar{n}}$ ,

$$k(t)_3 = k(t')_3 \quad (\text{B.2})$$

*Proof.*  $\Rightarrow$ : Let  $D_{f,(a_1,c),\bar{n}} = \{t \in T_{\bar{n}} | f(t) = (a_1, c)\}$ . Since the total number of notes that are with  $n_1 = \bar{n}_1$  and  $n_2 = \bar{n}_2$  is fixed in each  $(a_1, c)$ , we then have  $|D_{f,(a_1,c),\bar{n}}| = |T_{f_k,(a_1,c),\bar{n}}|$ .  
 $\Leftarrow$ : Define  $f(t) = (a_1, c)$  if  $t \in D_{f,(a_1,c),\bar{n}}$ , and then define  $f(t) = f_k(t)$  if  $t \notin T_{\bar{n}}$ . Such  $f$  is then in  $F_{k,f_k,T_{\bar{n}}}$ .  $\square$

Two consequences follow the above claim: first,  $|F_{k,f_k,T_{\bar{n}}}| = |V|!|U|! \frac{(|T_{\bar{n}}|/|V||U|)!}{|T_{f_k,(a_1,c),\bar{n}}|! \dots |T_{f_k,(a'_1,c'),\bar{n}}|!}$ ; second, the conditional probability  $\Pr(f(x) = (a_1, c) | k(x) = \bar{n}, k)$  can be then derived as  $\frac{|T_{f_k,(a_1,c),\bar{n}}|}{|T_{\bar{n}}|}$ , which is not dependent on  $x$ . Note that  $|T_{f_k,(a_1,c),\bar{n}}|$  is equal to  $|\{n \in N_{a_1,c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|$  and  $|T_{\bar{n}}|$  is equal to  $\sum_{a_1} \sum_c |\{n \in N_{a_1,c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|$ , and therefore  $\Pr(f(x) = (a_1, c) | k(x) = \bar{n}, k) = \frac{|\{n \in N_{a_1,c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1} \sum_c |\{n \in N_{a_1,c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}$   $\square$

From Lemma B.1.2, the conditional probability conditional on Player 2's observation  $(k, x)$  at the category  $f(x)$  does not depend on  $x$  if  $f$  is consistent with Player 2's observation. This conditional probability only depend on  $k(x)_1$  and  $k(x)_2$ . However, it is not obvious that the conditional probability over categories is still only dependent on  $k(x)_1$  and  $k(x)_2$  if Player 2 has been informed that  $f$  is drawn from a certain subset of  $F$ . By condition C.3,  $k(x)_3$  is varied with  $c_3$  and dependent on  $k(x)_2$  by permutation  $\theta_{k(x)_2}$ .

By condition **C.2**, the amount of notes with second element  $k(x)_2$  is varied across  $c_2$ . By **C.3** and **C.4** together,  $k(x)_3$  can be used to infer possible pairs of  $(c_2, c_3)$ .

I use next lemma to characterizes a subset of  $F$  from which  $f$  can be drawn and be informed to Player 2, but the conditional probability conditional on Player 2's observation over categories still only depend on  $k(x)_1$  and  $k(x)_2$ .

**Lemma B.1.3.** *Let  $\bar{C} = \{c' \in C | c'_3 = \bar{c}_3, c'_4 = \bar{c}_4\}$  for some  $\bar{c}_3, \bar{c}_4$ . Let  $T_f = \{t | f(t) \in \bigcup_{a_1, c \in \bar{C}} \{a_1, c\}\}$  for a  $f$  in  $F$  that is consistent with  $k$ . Denote  $\bar{n} = k(x)$  for  $x \in T_f$ . Then*

$$\Pr(f(x) = (a_1, c) | k(x) = \bar{n}, k, T_f) = \frac{|\{n \in N_{a_1, (c_1, c_2, \bar{c}_3, \bar{c}_4)} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1, c \in \bar{C}} |\{n \in N_{a_1, c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}$$

*Proof.* Define

$$T_{f, \bar{n}} = \{t | k(t) = \bar{n}\} \cap T_f$$

, and define

$$F_{k, f, T_{f, \bar{n}}} = \{f' \in F | \forall t' \notin T_{f, \bar{n}} [f'(t') = f_k(t')] \text{ and } \forall t' \in T_{f, \bar{n}} [k(t') \in N_{f'(t')}, f'(t') \in \bigcup_{a_1, c \in \bar{C}} \{a_1, c\}]\}$$

. Denote  $T_{f, (a_1, c), \bar{n}} \subset T_{f, \bar{n}}$  for all  $(a_1, c)$ , where  $c \in \bar{C}$ , as

$$T_{f, (a_1, c), \bar{n}} = \{t \in T_{f, \bar{n}} | f(t) = (a_1, c)\}, \text{ where } c \in \bar{C}$$

. Then I can show the following claim.

**Claim B.1.2.**  $f' \in F_{k, f, T_{f, \bar{n}}}$  if and only if there is a combination of multisets  $(D_{f', (a_1, c), \bar{n}})_{a_1, c \in \bar{C}}$  in  $T_{f, \bar{n}}$ , where  $(D_{f', (a_1, c), \bar{n}})_{a_1, c \in \bar{C}}$  satisfies

1. for each  $(a_1, c)$ , where  $c \in \bar{C}$ ,

$$|D_{f',(a_1,c),\bar{n}}| = |T_{f,(a_1,c),\bar{n}}| \quad (\text{B.3})$$

2. for every  $\bar{c}_3 \in V$ , for every  $t, t' \in \bigcup_{c \in \bar{C}, c_3 = \bar{c}_3} D_{f',(a_1,c),\bar{n}}$ ,

$$k(t)_3 = k(t')_3 \quad (\text{B.4})$$

*Proof.* Since  $c \in \bar{C}$ , Equation (4) holds. The proof follows the same proof in Claim B.1.2.3 (in Lemma B.1.2).  $\square$

Finally, by following the same proofing procedure in Lemma B.1.2 again, the conditional probability  $\Pr(f(x) = (a_1, c) | k(x) = \bar{n}, k, T_f)$ , is equal to  $\frac{|\{n \in N_{a_1, (c_1, c_2, \bar{c}_3, \bar{c}_4)} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1, c \in \bar{C}} |\{n \in N_{a_1, c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}$ .  $\square$

To save notations in discussing Player 2's conditional probability, I use the following lemma and define a conditional probability induced by  $\Pr(\cdot)$  that is only conditional on  $(k(x)_1, k(x)_2) = (n_1, n_2)$ .

**Lemma B.1.4.** *Given  $(\bar{n}_1, \bar{n}_2) \in A_2 \times A_3$ , then*

$$|\{n \in N_{a_1, (c_1, c_2, \bar{c}_3, \bar{c}_4)} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}| = |\{n \in N_{a_1, (c_1, c_2, \bar{c}'_3, \bar{c}'_4)} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}| \quad (\text{B.5})$$

, for all  $(c_1, c_2) \in A_2 \times A_3$ , for all  $\bar{c}_3, \bar{c}'_3 \in V$ , for all  $\bar{c}_4, \bar{c}'_4 \in U$ .

*Proof.* The proof follows **Observation A.1** and **Observation A.2**.  $\square$

From the above Lemma B.1.4, if  $c_3, c_4$  are fixed to be some  $\bar{c}_3, \bar{c}_4$ , I can define  $\overline{\Pr}(a, c_1, c_2 | \bar{n}, k)$  as follows in order to save notations.

**Definition B.1.2.**

$$\begin{aligned} \overline{\Pr}(a, c_1, c_2 | \bar{n}, k) &:= \frac{|\{n \in N_{a_1, (c_1, c_2, \bar{c}_3, \bar{c}_4)} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1, c \in \bar{C}} |\{n \in N_{a_1, c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|} \\ &= \Pr(f(x) = (a_1, c) | k(x) = \bar{n}, k, c_3 = \bar{c}_3, c_4 = \bar{c}_4) \end{aligned}$$

, where  $\bar{C} = \{c \in C | c_3 = \bar{c}_3, c_4 = \bar{c}_4\}$  for some  $\bar{c}_3, \bar{c}_4$ .

Next, I relate the conditional probability over  $f$  conditional on Player 2's observation to the conditional probability  $q(a_1, a_3 | a_2)$ . In this discussion, I let  $\bar{C} = \{c \in C | c_3 = \bar{c}_3, c_4 = \bar{c}_4\}$  for some  $\bar{c}_3, \bar{c}_4$ , and I let the notation  $c$  refer to an element in  $\bar{C}$  to save notations. Also let  $\bar{n}$  be a note with  $n_1 = \bar{n}_1$  and  $n_2 = \bar{n}_2$ , while letting  $\bar{c}$  be a category in  $\bar{C}$  with  $c_1 = \bar{c}_1$  and  $c_2 = \bar{c}_2$  to save notations. It is convenience to state a proposition which describes how  $\bar{n}$  relates to a given category  $\bar{c} \in \bar{C}$ . The following lemma shows such proposition.

**Lemma B.1.5.** *Let  $\bar{C} = \{c \in C | c_3 = \bar{c}_3, c_4 = \bar{c}_4\}$  for some fixed  $\bar{c}_3$  and  $\bar{c}_4$ . Define  $\cup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} = \cup_{c \in \bar{C}} \{n \in N_{a_1, c} | n_1 = \bar{n}_1, n_2 = \bar{n}_2\}$  with generic element  $\bar{n}$ . The given a category  $\bar{c} \in \bar{C}$ , there is a one-to-one mapping  $g : \cup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} \rightarrow N_{a_1, \bar{c}}$  such that  $g(\bar{n})_1 + \bar{c}_1 \equiv \bar{n}_1 + c_1$  and  $g(\bar{n})_2 + \bar{c}_2 \equiv \bar{n}_2 + c_2$ .*

*Proof.* Suppose  $\cup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c}$  is not empty, then there is a category  $c \in \bar{C}$  such that  $\bar{n} \in N_{a_1, c}$ . Define  $g' : \cup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} \rightarrow N_{a_1, \bar{c}}$  such that  $g'(\bar{n})_1 + \bar{c}_1 \equiv \bar{n}_1 + c_1$  and  $g'(\bar{n})_2 + \bar{c}_2 \equiv \bar{n}_2 + c_2$  for all such  $c$ . Note that either  $g'(\bar{n})_1$  or  $g'(\bar{n})_2$  is unique by **Observation A.1**. Let  $a_2 \equiv \bar{n}_1 + c_1$  and  $a_3 \equiv \bar{n}_2 + c_2$ . Either  $a_2$  or  $a_3$  is unique by **Observation A.1** again. According

to **Observation A.2**, given such  $a_2$  and  $a_3$ ,  $|\{n \in N_{a_1,c} | n_1 + \bar{c}_1 \equiv a_2 \pmod{|A_2|}, n_2 + \bar{c}_2 \equiv a_3 \pmod{|A_3|}\}|$  is equal to  $|\{\bar{n} \in N_{a_1,c} | \bar{n}_1 + c_1 \equiv a_2 \pmod{|A_2|}, \bar{n}_2 + c_2 \equiv a_3 \pmod{|A_3|}\}|$  for all such  $c$ . Since that,  $g'$  can be made to be injective for all such  $c$ s. Call this injective function made by  $g'$   $g$ . I claim that  $g$  is also surjective. Suppose  $g$  is not surjective, then there is a  $n' \in N_{a_1,\bar{c}}$  such that, for all  $c \in \bar{C}$ ,  $g(\bar{n})_1 + c_1 \neq n'_1 + \bar{c}_1$  and  $g(\bar{n})_2 + c_2 \neq n'_2 + \bar{c}_2$ . It contradicts **Observation A.2** again since there should be a  $c' \in \bar{C}$  such that  $|\{\bar{n} \in N_{a_1,c} | \bar{n}_1 + c'_1 \equiv a'_2 \pmod{|A_2|}, \bar{n}_2 + c'_2 \equiv a'_3 \pmod{|A_3|}\}| = |\{n \in N_{a_1,c} | n'_1 + \bar{c}_1 \equiv a'_2 \pmod{|A_2|}, n'_2 + \bar{c}_2 \equiv a'_3 \pmod{|A_3|}\}|$ , where  $a'_2 \equiv n'_1 + \bar{c}_1$  and  $a'_3 \equiv n'_2 + \bar{c}_2$ . I then conclude that there is a one-to-one mapping  $g$  between  $\bigcup_{c \in \bar{C}} N_{a_1,\bar{n}_1,\bar{n}_2,c}$  and  $N_{a_1,\bar{c}}$ .  $\square$

The following corollary is a consequence of Lemma B.1.5.

**Corollary B.1.1.** *Let  $\bar{C} = \{c \in C | c_3 = \bar{c}_3, c_4 = \bar{c}_4\}$  for some fixed  $\bar{c}_3$  and  $\bar{c}_4$ . Given  $a_2 = \bar{a}_2$ , given  $\bar{c} \in \bar{C}$ , and given  $\bar{n}$ , the summation*

$$\sum_{a_1} \sum_{a_3} |\{n \in N_{a_1,\bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a_3\}| \quad (\text{B.6})$$

is equal to

$$\sum_{a_1} \sum_{c \in \bar{C}} |\{\bar{n} \in N_{a_1,c} \cap \bigcup_{c \in \bar{C}} N_{a_1,\bar{n}_1,\bar{n}_2,c} | \bar{n}_1 + c_1 \equiv \bar{a}_2\}| \quad (\text{B.7})$$

*Proof.* Given  $a_1$ , denote  $E_{a_1} = \{n \in N_{a_1,\bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2\}$  and denote  $\bar{E}_{a_1} = \{\bar{n} \in \bigcup_c N_{a_1,\bar{n}_1,\bar{n}_2,c} | \bar{n}_1 + c_1 \equiv \bar{a}_2\}$ . By Lemma B.1.5, there is a mapping  $g$  such that for each  $n$  in  $E_{a_1}$ , there is an corresponding  $g^{-1}(n)$  satisfying  $g^{-1}(n)_1 + c_1 \equiv n_1 + \bar{c}_1 \equiv \bar{a}_2$  for some  $c \in \bar{C}$ . Therefore,  $g^{-1}(n) \in F_{a_1}$ . Moreover, given  $c \in \bar{C}$ , for each  $\bar{n}$  in  $\bar{E}_{a_1}$ , there is a corresponding  $g(\bar{n})$  such that  $g(\bar{n})_1 + \bar{c}_1 \equiv \bar{n}_1 + c_1 \equiv \bar{a}_2$ , and therefore  $g(\bar{n}) \in E_{a_1}$ . Since  $g$  is one-to-one, we then have  $|E_{a_1}| = |\bar{E}_{a_1}|$  for all  $a_1$ .

Next I show that  $\sum_{a_3} |\{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a_3\}| = |E_{a_1}|$ . By **Observation A.1**,  $\{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a_3\} \cap \{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a'_3\} = \emptyset$  if  $a_3 \neq a'_3$ . Thus  $|\cup_{a_3} \{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a_3\}| = \sum_{a_3} |\{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a_3\}|$ . Since  $\cup_{a_3} \{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a_3\} = E_{a_1}$ , we have  $\sum_{a_3} |\{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv \bar{a}_2, n_2 + \bar{c}_2 \equiv a_3\}| = |E_{a_1}|$ .

I then have to show that  $\sum_{c \in \bar{C}} |\{\bar{n} \in N_{a_1, c} \cap \cup_{c' \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c'} | \bar{n}_1 + c_1 \equiv \bar{a}_2\}| = |\bar{E}_{a_1}|$ . From **Observation A.3**,  $N_{a_1, c} \cap N_{a_2, c'} = \emptyset$  for all  $c, c' \in \bar{C}$ , and therefore  $\{\bar{n} \in N_{a_1, c} \cap \cup_{c' \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c'} | \bar{n}_1 + c_1 \equiv \bar{a}_2\} \cap \{\bar{n} \in N_{a_1, c'} \cap \cup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} | \bar{n}_1 + c_1 \equiv \bar{a}_2\} = \emptyset$  for all  $c, c' \in \bar{C}$ . And hence  $\sum_{c \in \bar{C}} |\{\bar{n} \in N_{a_1, c} \cap \cup_{c' \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c'} | \bar{n}_1 + c_1 \equiv \bar{a}_2\}| = |\cup_{c \in \bar{C}} \{\bar{n} \in N_{a_1, c} \cap \cup_{c' \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c'} | \bar{n}_1 + c_1 \equiv \bar{a}_2\}| = |\bar{E}_{a_1}|$ .  $\square$

In the following lemma, I build up the relationship between  $q$  and Player 2's conditional probability induced by players' randomization process during Step 1 to Step 4.

**Lemma B.1.6.**

$$q(a_1, a_3 | a_2) = \overline{\text{Pr}}(a_1, c_2 | \bar{n}, c_1, k)$$

, where  $c_1, c_2$  satisfy  $\bar{n}_1 + c_1 \equiv a_2$  and  $\bar{n}_2 + c_2 \equiv a_3$ .

*Proof.* Let  $\bar{C} = \{c \in C | c_3 = \bar{c}_3, c_4 = \bar{c}_4\}$  for some fixed  $\bar{c}_3$  and  $\bar{c}_4$ . Let  $c, \bar{c} \in \bar{C}$ . Given  $\bar{n}$  and let  $c_1$  and  $c_2$  satisfy  $\bar{n}_1 + c_1 \equiv a_2$  and  $\bar{n}_2 + c_2 \equiv a_3$ . Follow Corollary B.1.1 and let  $g$  be that

function in Lemma B.1.5, we then have

$$q(a_1, a_3 | a_2) \tag{B.8}$$

$$= \frac{|\{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv a_2, n_2 + \bar{c}_2 \equiv a_3\}|}{\sum_{a_1, a_3} |\{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv a_2, n_2 + \bar{c}_2 \equiv a_3\}|} \tag{B.9}$$

$$= \frac{|\{n \in N_{a_1, \bar{c}} | n_1 + \bar{c}_1 \equiv a_2, n_2 + \bar{c}_2 \equiv a_3\}|}{\sum_{a_1, c \in \bar{C}} |\{\bar{n} \in N_{a_1, c} \cap \bigcup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} | \bar{n}_1 + c_1 \equiv a_2\}|} \tag{B.10}$$

$$= \frac{|\{g(\bar{n}) \in N_{a_1, \bar{c}} | g(\bar{n})_1 + \bar{c}_1 \equiv a_2, g(\bar{n})_2 + \bar{c}_2 \equiv a_3\}|}{\sum_{a_1, c \in \bar{C}} |\{\bar{n} \in N_{a_1, c} \cap \bigcup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} | \bar{n}_1 + c_1 \equiv a_2\}|} \tag{B.11}$$

$$= \frac{|\{\bar{n} \in N_{a_1, c} \cap \bigcup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} | \bar{n}_1 + c_1 \equiv a_2, \bar{n}_2 + c_2 \equiv a_3\}|}{\sum_{a_1, c \in \bar{C}} |\{\bar{n} \in N_{a_1, c} \cap \bigcup_{c \in \bar{C}} N_{a_1, \bar{n}_1, \bar{n}_2, c} | \bar{n}_1 + c_1 \equiv a_2\}|} \tag{B.12}$$

$$= \overline{\text{Pr}}(a_1, c_2 | \bar{n}, c_1, k) \tag{B.13}$$

, where Equation (B.8) implies Equation (B.9) by **Observation A.2**, Equation (B.9) implies Equation (B.10) by Corollary B.1.1, Equation (B.10) implies Equation (B.11) by taking the function  $g$  in Lemma B.1.5, Equation (B.11) implies Equation (B.12) by the definition of that  $q$  in Lemma B.1.5, Equation (B.12) implies Equation (B.13) by Definition B.1.2.  $\square$

Finally, I get the following lemma which relates Player 2's conditional probability conditional on his observation after Step 5.3.

**Lemma B.1.7.** *Let  $a_1 = f(x)_1$ ,  $c_1 = m^2 = f(x)_{2,1}$  and  $c = m^3 = (f(x)_{2,1}, f(x)_{2,2}, f(x)_{2,3}, f(x)_{2,4})$  be an outcome generated by players after Step 5.3. Then the conditional probability over  $(a_1, (c_1, c_2))$  conditional on Player 2's observation  $(k(x), c_1, k)$  is  $q(a_1, a_3 | a_2)$  if and only if  $k(x)_1 + c_1 \equiv a_2$ , and  $k(x)_2 + c_2 \equiv a_3$*

*Proof.* First, it is straightforward to modify Lemma B.1.3 when  $\bar{c}_4$  is a function of  $c_2$ . More precisely, let  $\bar{c}_2 = u_{c_2}$ , where  $(u_{c_2})$  is drawn from  $U$  with probability  $1/|U|$ . Then

substitute  $\bar{C}$  with  $\bar{\bar{C}} = \{c' \in C \mid c' = \bar{c}_3, c'_4 = \bar{c}_4(c_2)\}$ . In such case, one can show that

$$\Pr(f(x) = (a_1, c) \mid k(x) = \bar{n}, k, T_f) = \frac{|\{n \in N_{a, (c_1, c_2, \bar{c}_3, u_{c_2})} \mid n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1} \sum_{c_2} |\{N_{a, (c_1, c_2, \bar{c}_3, u_{c_2})} \mid n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}$$

. Then, by Lemma B.1.4,  $\frac{|\{n \in N_{a, (c_1, c_2, \bar{c}_3, u_{c_2})} \mid n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1} \sum_{c_2} |\{N_{a, (c_1, c_2, \bar{c}_3, u_{c_2})} \mid n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|} = \frac{|\{n \in N_{a, (c_1, c_2, \bar{c}_3, c_4)} \mid n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}{\sum_{a_1} \sum_{c_2} |\{N_{a, (c_1, c_2, \bar{c}_3, c_4)} \mid n_1 = \bar{n}_1, n_2 = \bar{n}_2\}|}$

for all  $c_4$ , and therefore  $\Pr(f(x) = (a_1, c) \mid k(x) = \bar{n}, k, T_f) = \bar{\Pr}(a_1, c_1, c_2 \mid \bar{n}, k)$ .

Note that  $\bar{\Pr}(a_1, c_2 \mid \bar{n}, c_1, k)$  is just the conditional probability derived from  $\bar{\Pr}(a_1, c_1, c_2 \mid \bar{n}, k)$  by Definition B.1.2, I have shown that the conditional probability over  $(a_1, (c_1, c_2))$  conditional on Player 2's observation  $(\bar{n} = k(x), c_1, k)$  is  $q(a_1, a_3 \mid a_2)$  if and only if  $k(x)_1 + c_1 \equiv a_2$ , and  $k(x)_2 + c_2 \equiv a_3$ .  $\square$

Due to Lemma B.1.7, in Step 6, Player 2's conditional probabilities conditional on his own recommended action over other recommended actions is the same as that induced by  $q$ .

#### PLAYER 1'S CONDITIONAL PROBABILITIES OVER PLAYERS' RECOMMENDED ACTIONS

**Lemma B.1.8.** *Let  $a_1 = f(x)_1$ ,  $c_1 = m^2 = f(x)_{2,1}$  and  $c = m^3 = (f(x)_{2,1}, f(x)_{2,2}, f(x)_{2,3}, f(x)_{2,4})$  be an outcome generated by players after Step 5.3. Then the conditional probability over  $k(x)$  conditional on Player 1's observation  $f(x)$  is  $q(a_2, a_3 \mid a_1)$  if and only if  $f(x) = (a_1, c)$ ,  $k(x)_1 + c_1 \equiv a_2$ , and  $k(x)_2 + c_2 \equiv a_3$ .*



*Proof.* By condition **C.2**, we then have

$$\begin{aligned}
& q(a_2, a_3 | a_1) \\
&= \frac{|\{n \in N_{a_1, c} | n_1 + c_1 \equiv a_2 \pmod{|A_2|}, n_2 + c_2 \equiv a_3 \pmod{|A_3|}\}|}{|N_{a_1, c}|} \\
&= \Pr(k(x) = n | f(x) = (a_1, c))
\end{aligned}$$

, where  $n$  and  $c$  satisfies  $n_1 + c_1 \equiv a_2$  and  $n_2 + c_2 \equiv a_3$ . By **Observation A.1**,  $c_1$  and  $c_2$  is unique given  $a_2$  and  $a_3$ , and vice versa. Therefore, I conclude this lemma.  $\square$

Due to Lemma B.1.8, in Step 6, Player 1's conditional probabilities conditional on his own recommended action over other recommended actions is the same as that induced by  $q$ .

#### PLAYER 3'S CONDITIONAL PROBABILITIES OVER PLAYERS' RECOMMENDED ACTIONS

**Lemma B.1.9.** *Let  $a_1 = f(x)_1$ ,  $c_1 = m^2 = f(x)_{2,1}$  and  $c = m^3 = (f(x)_{2,1}, f(x)_{2,2}, f(x)_{2,3}, f(x)_{2,4})$  be an outcome generated by players after Step 5.3. Then the conditional probability over  $(a_1, k(x)_1)$  conditional on Player 3's observation  $(c, k(x)_2, k, f)$  is  $q(a_1, a_2 | a_3)$  if and only if  $k(x)_1 + c_1 \equiv a_2$  and  $k(x)_2 + c_2 \equiv a_3$ .*

By condition **C.2**. we have

$$\begin{aligned}
& q(a_1, a_2 | a_3) \\
&= \frac{|\{n \in N_{a_1, c} | n_1 + c_1 \equiv a_2 \pmod{|A_2|}, n_2 + c_2 \equiv a_3 \pmod{|A_3|}\}|}{\sum_{a_1, a_2} |\{n \in N_{a_1, c} | n_1 + c_1 \equiv a_2 \pmod{|A_2|}, n_2 + c_2 \equiv a_3 \pmod{|A_3|}\}|} \\
&= \Pr(f(x) = (a_1, c), k(x)_1 = n_1 | c, k(x)_2 = n_2, k, f)
\end{aligned}$$

, where  $k(x)_1, k(x)_2$  and  $c$  satisfies  $k(x)_1 + c_1 \equiv a_2$  and  $k(x)_2 + c_2 \equiv a_3$ . By **Observation A.1**,  $c_1$  and  $c_2$  is unique given  $a_2$  and  $a_3$ , and vice versa. Therefore, I conclude this lemma.

Due to Lemma B.1.9, in Step 6, Player 3's conditional probabilities conditional on his own recommended action over other recommended actions is the same as that induced by  $q$ .

#### B.1.2.4 CONCLUSION

Finally, I conclude that Theorem 4 has been proved. Denote the worst NE in  $G$  as  $\alpha$ . Given a c.e.d.  $q$  in  $G$ , if all players' payoffs in  $q$  are equal to those in  $\alpha$ , then all players play  $\alpha$  after the protocol. If a player  $i$ 's payoff in  $q$  is strictly larger than that in  $\alpha$ , then we can find a  $\eta_i$  such that  $U_i(q) > \eta_i U_i(\alpha) + (1 - \eta_i) U_i(\beta)$ , where  $U_i(q)$  and  $U_i(\alpha)$  is player  $i$ 's expected payoff in  $q$  and in  $\alpha$  respectively, and  $U_i(\beta)$  is the maximal expected payoff in  $G$ , which  $i$  can get. Then we can take

$$\eta^* = \arg \max_{i: U_i(q) > U_i(\alpha)} \{ \eta_i | U_i(q) > \eta_i U_i(\alpha) + (1 - \eta_i) U_i(\beta) \}$$

, and then take two finite set  $\bar{V}$  and  $\bar{U}$  such that

$$\min\{1 - 1/|\bar{V}|, 1 - 1/|\bar{U}|\} = \eta^*$$

. Finally, by Lemma B.1.1, we can take  $V = \{1, \dots, |\bar{V}|\}$  and  $U = \{1, \dots, |\bar{U}|\}$  in the construction of the protocol to impede profitable unitary deviation. Since I have checked that, if players do not receive **STOP** during the protocol, each player's conditional probability conditional on his recommended action over others' recommended actions after

Step 6 is the same as that induced by  $q$ , and since players' unitary deviation do not affect the generated distribution in the J.C.L. procedures, I conclude the Theorem 4.

# References

- I. Abraham, D. Dolev, R. Gonen, and J. Halpern. Distributed Computing Meets Game Theory: Robust Mechanisms for Rational Secret Sharing and Multiparty Computation. *Proceedings of the Twenty-fifth Annual ACM Symposium on Principles of Distributed Computing*, pages 53–62, 2006.
- I. Abraham, D. Dolev, and J. Y. Halpern. Lower Bounds on Implementing Robust and Resilient Mediators. *CoRR*, Apr. 2007.
- D. Acemoglu, M. A. Dahleh, I. Lobel, and A. Ozdaglar. Bayesian Learning in Social Networks. *The Review of Economic Studies*, 78(4):1201–1236, 2011.
- R. J. Aumann. Subjectivity and Correlation in Randomized Strategies. *Journal of Mathematical Economics*, 1(1):67–96, 1974.
- R. J. Aumann and M. Maschler. *Repeated Games With Incomplete Information*. MIT Press, 1995.
- I. Barany. Fair Distribution Protocols or How The Players Replace Fortune. *Mathematics of Operations Research*, 17:327–340, Jan. 1987.
- M. Ben-Or and A. Wigderson. Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation. In *Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88*, pages 1–10, New York, New York, USA, Jan. 1988. ACM Press.
- E. Ben-Porath. Correlation without Mediation: Expanding the Set of Equilibrium Outcomes by “Cheap” Pre-play Procedures. *Journal of Economic Theory*, 80(1):108–122, May 1998.
- E. Ben-Porath. Cheap Talk in Games with Incomplete Information. *Journal of Economic Theory*, 108(1):45–71, Jan. 2003.

- S. Bikhchandani, D. Hirshleifer, and I. Welch. Learning from the Behavior of Others: Conformity, Fads, and Informational Cascades, 1998.
- P. Bolton and C. Harris. Strategic Experimentation. *Econometrica*, 67(2):349–374, 1999.
- Y. Bramoullé and R. Kranton. Public Goods in Networks. *Journal of Economic Theory*, 135(1):478–494, 2007.
- H. H. Cao and D. A. Hirshleifer. Conversation, Observational Learning, and Informational Cascades. *SSRN Electronic Journal*, Nov. 2001.
- K. Chatterjee and B. Dutta. Credibility and Strategic Learning in Networks, Jan. 2011.
- M. S.-Y. Chwe. Communication and Coordination in Social Networks. *Review of Economic Studies*, 67(1):1–16, 2000.
- Y. Dodis, S. Halevi, and T. Rabin. A cryptographic solution to a game theoretic problem. In *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '00, pages 112–130, London, UK, UK, 2000. Springer-Verlag.
- F. Forges. An Approach to Communication Equilibria. *Econometrica*, 54(6):1375–85, 1986.
- F. Forges. Universal Mechanisms. *Econometrica*, 58(6):1341–1364, 1990.
- F. Forges. Correlated Equilibrium and Communication in Games. *Encyclopedia of Complexity and Systems Science*, pages 1587–1596, 2009.
- D. Fudenberg and Y. Yamamoto. Repeated Games Where the Payoffs and Monitoring Structure Are Unknown. *Econometrica*, 78(5):1673–1710, 2010.
- D. Fudenberg and Y. Yamamoto. Learning from Private Information in Noisy Repeated Games. *Journal of Economic Theory*, 146(5):1733–1769, 2011.
- D. Gale and S. Kariv. Bayesian Learning in Social Networks. *Games and Economic Behavior*, 45(2):329–346, 2003.
- D. Gerardi. Unmediated Communication in Games with Complete and Incomplete Information. *Journal of Economic Theory*, 114(1):104–131, Jan. 2004.
- O. Goldreich, S. Micali, and A. Wigderson. How to Play ANY Mental Game. In *Proceedings of the nineteenth annual ACM conference on Theory of computing - STOC '87*, pages 218–229, New York, New York, USA, Jan. 1987. ACM Press.

- B. Golub and M. O. Jackson. Naïve Learning in Social Networks and the Wisdom of Crowds. *American Economic Journal: Microeconomics*, 2(1):112–149, 2010.
- O. Gossner and N. Vieille. Repeated Communication through The Mechanism And. *International Journal of Game Theory*, 30(1):41–60, Sept. 2001.
- S. Goyal. *Connections: An Introduction to the Economics of Networks*. Princeton University Press, 2012.
- Y. Heller. Minority-proof Cheap-talk Protocol. *Games and Economic Behavior*, 69(2):394–400, July 2010.
- Y. Heller, E. Solan, and T. Tomala. Communication, Correlation and Cheap-talk in Games with Public Information. *Games and Economic Behavior*, 74(1):222–234, 2012.
- M. O. Jackson. *Social and Economic Networks*. Princeton University Press, 2008.
- O. Karl-Dieter and G. Christiane. Dissident Groups, Personal Networks, and Spontaneous Cooperation: The East German Revolution of 1989. *American Sociological Review*, 58(5):659–680, 1993.
- D. M. Kreps and R. Wilson. Sequential Equilibria. *Econometrica*, 50(4):863–94, July 1982.
- M. Laclau. A Folk Theorem for Repeated Games Played on a Network. *Games and Economic Behavior*, 76(2):711–737, 2012.
- E. Lehrer. Mediated Talk. *International Journal of Game Theory*, 25(2):177–188, June 1996.
- E. Lehrer and S. Sorin. One-shot Public Mediated Talk. *Games and Economic Behavior*, 20(2):131–148, Aug. 1997.
- S. Lohmann. A Signaling Model of Informative and Manipulative Political Action. *American Political Science Review*, 87(2):319–333, 1993.
- S. Lohmann. Information Aggregation Through Costly Political Action. *The American Economic Review*, 84(3):518–530, 1994.
- S. Lohmann. The Dynamics of Informational Cascades: The Monday Demonstrations in Leipzig, East Germany, 1989fb91. *World Politics*, 47(01):42–101, June 2011.

- D. McAdam. Beyond Structural Analysis: Toward a More Dynamic Understanding of Social Movements. In *Social Movements and Networks*. Oxford University Press, Oxford, 2003.
- R. B. Myerson. *Game Theory*. Harvard University Press, 2004.
- F. Passy. Social Networks Matter. But How? In *Social Movements and Networks*, pages 21–48. Oxford U Press, 2003.
- A. Perea. A Note on The One-deviation Property in Extensive Form Games. *Games and Economic Behavior*, 40(2):322 – 338, 2002.
- T. Rabin and M. Ben-Or. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing - STOC '89*, pages 73–85, New York, New York, USA, Feb. 1989. ACM Press.
- J. m. Renault and T. Tomala. Repeated Proximity Games. *International Journal of Game Theory*, 27(4):539–559, 1998.
- M. Shadmehr and D. Bernhardt. Collective Action with Uncertain Payoffs: Coordination, Public Signals, and Punishment Dilemmas. *American Political Science Review*, 105(04):829–851, Nov. 2011.
- A. Shamir. How to Share A Secret. *Communications of the ACM*, 22(11):612–613, Nov. 1979.
- D. A. Siegel. Social Networks and Collective Action. *American Journal of Political Science*, 53(1):122–138, 2009.
- V. Teague. Problems With Coordination in Two-Player Games: Comment on ”Computational Complexity and Communication”. *Econometrica*, 76(6):1559–1564, 2008.
- A. Urbano and J. E. Vila. Computational Complexity and Communication: Coordination in Two-Player Games. *Econometrica*, 70(5):1893–1927, Sept. 2002.
- P. Vida and H. Āzakis. A Detail-free Mediator. *Games and Economic Behavior*, 81: 101–115, Sept. 2013.
- R. Vijay Krishna. Communication in Games of Incomplete Information: Two Players. *Journal of Economic Theory*, 132(1):584–592, Jan. 2007.
- T. Wiseman. A Partial Folk Theorem for Games with Private Learning. *Theoretical Economics*, 7(2):217–239, 2012.

A. Wolitzky. Cooperation with Network Monitoring. *Review of Economic Studies*, 80(1):395–427, 2013.

A. Wolitzky. Communication with Tokens in Repeated Games on Networks. *Theoretical Economics*, Jan. 2014.

Y. Yamamoto. Individual Learning and Cooperation in Noisy Repeated Games. *Review of Economic Studies*, 81(1):473–500, 2014.



# CHUN-TING CHEN

Address: Department of Economics Telephone: (814) 753-0168 (cell)  
608 Kern Graduate Building E-mail: cuc230@psu.edu  
The Pennsylvania State University Website: <http://chuntingchen.weebly.com/>  
University Park, PA 16802

## Curriculum Vitae

- EDUCATION:
- Ph.D. in Economics, The Pennsylvania State University, 2015
  - MA in Economics, National Taiwan University, 2008
  - BSc in Civil Engineering, National Taiwan University, 2002
- Ph.D. THESIS:
- Essays on Communication, Coordination, and Correlation  
**Thesis Advisor:** Professor Kalyan Chatterjee
- FIELDS:
- **Primary:** Game Theory, Microeconomic Theory
  - **Secondary:** Network Economics
- WORKING PAPERS:
- “Coordination in Social Networks”
  - “A Window of Cognition: Eyetracking the Reasoning Process in Spatial Beauty Contest Games” (with Chen-Ying Huang, Joseph Tao-Yi Wang)
- WORK IN PROGRESS:
- “Correlation with Forwarding”
  - “Mechanism for Borrowing and Lending” (with Rakesh Chaturvedi)
- GRANTS & FELLOWSHIPS:
- Graduate Assistantship, Department of Economics, The Pennsylvania State University, 2009-2014
  - The Best Master Thesis Award, Taiwan Economics Association, 2008
- PERSONAL:
- **Citizenship:** Taiwan
  - **Language:** Taiwanese, Mandarin Chinese, English