Finitely Iterated Rational Secret Sharing With Private Information

by

Chelsey Foster
B.Sc., Lakehead University, 2012

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Computer Science

© Chelsey Foster, 2014
University of Victoria

All rights reserved. This thesis may not be reproduced in whole or in part, by photocopying or other means, without the permission of the author.

Finitely Iterated Rational Secret Sharing With Private Information

by

Chelsey Foster
B.Sc., Lakehead University, 2012

Supervisory Committee

Bruce Kapron. Supervisor Main, Supervisor
(Department of Computer Science)

Audrey Yap. Member One, Outside member
(Department of Philosophy)

ABSTRACT

This thesis considers the problem of finitely iterated rational secret sharing. We describe how to evaluate this problem using game theory and finitely iterated prisoner's dilemma. The players each have a private horizon that the other player does not know. The only thing that a player knows about their opponent's private horizon is a common upper bound. The description of a synchronous and asynchronous finitely iterated secret sharing protocol with private information is followed by a game theoretic proof of the viability of such protocols.

Contents

List of Figures

Chapter 1

Introduction

1.1 Game Theory and Cryptography

The evaluation of decision making agents has been studied from both game theoretic and cryptographic perspectives. Game theory considers rational agents that are participating in a mutual decision-making process in which the combined decision determines how much utility each agent will receive. In "Essentials of Game Theory" [5] it is described as "the mathematical study of interaction among independent, self-interested agents". It can be used to model a variety of situations including resource management, business interactions, and evolution. One situation that can be analyzed using game theoretic techniques is called the prisoners' dilemma. The prisoner's dilemma involves two prisoners that are offered a deal in which they can either rat out the other prisoner (formally known as defecting), or keep quiet (cooperating). If they both keep quiet the prisoners both go to jail for the minimum sentence. If one rats on the other, the one who rats gets to go free and the one who remains silent faces a maximum sentence. If they both rat on each other they both get a sentence of mid-range length. The dilemma is that the prisoners have an incentive to defect, as that is the best response to either action the other player takes. However, the situation that yields the best for both prisoners is the one in which they both cooperate.

Within cryptography the subfield of multi-party computation deals with computations done within a network of agents. There are a group of agents with individual input who want to compute a common function. An example of this is the topic of Yao's classic paper "Protocols for secure computation" [10] and is called the millionaire

problem. There are two millionaires that want to find out which one is richer. Both millionaires want to know who the richer one is but do not want to reveal their net worth to each other. The protocol would have to imitate the following ideal model: Both millionaires give a trusted third party their personal net worth. The trusted third party then determines who is the richer of the two millionaires and shares the name of the richest millionare to all participants. In order to mimic this process without a third party, Yao describes how a cryptographic tool called one way functions (functions that are easily computed but difficult to invert) are used to provide the security and privacy of the individual's information while ensuring the validity of the final output.

Originally within this model of computation, agents are considered to be either malicous or honest. Honest agents follow the protocol as it was intended while malicious agents may deviate in arbitrary ways. The behaviour of the agents can also be thought of as simply rational and the protocol can be seen as a game and game theoretic analysis allows us to predict how rational self-interested agents will act and whether or not it is beneficial for them to act in the way that the protocol intends them to. Secret sharing is a cryptographic primitive that when first discussed in [9], treats the agents as either honest or malicous. A rational secret sharing protocol aims to distribute a secret key to a number of rational participating agents in such a way that the key can only be recovered if a set number of agents cooperate and share their piece of the secret to each other agent. Seret sharing can be thought of as a game in which agents have the choice to share or not share and we can use game theoretic principles to show that in a single round of secret sharing, rational agents will choose to not share. This is because the nature of secret sharing is analagous to the prisoner's dilemma game described above. This was first discussed in [3]. When assuming the agents to be rational, the protocol discussed in [9] is unviable because the agents will choose not to share. This is called an impossibility result and the goal of both [3] and [2] was to circumvent these results by altering thet protocol. The goal of this thesis is to do so in a new and more useful way.

1.2 Literature Review

In the (t, n) secret sharing scheme introduced in Shamir's paper [9], a secret is dealt amongst n players and the secret can be recovered as long as t players collaborate and reveal their secrets to each other. This is done by embedding a secret s=a_0 into

a degree $(t-1)$ polynomial $P^{t-1}(x) = a_0 + a_1x + a_2x^2 + ... + a_{t-1}x^{t-1}$. Each of the n players is then given a point on the graph of P. In order to recover the secret t players must share their portion of the secret, which in this case is a coordinate, with each other. Once the players have received a portion of the secret from each player they can reconstruct the polynomial using Lagrange interpolation and learn the secret (the y-intercept of the graph). If the players act in the best interest of the protocol, the secret sharing will be successful. In fact, as long as there are at most $(t-1)$ malicious agents, this protocol is secure. If the participants of the protocol are considered simply as self-interested rational agents , the analysis is quite different. If the players act in the best interest of themselves, one can use game theoretic analysis in order to determine the players' actions.

The scheme introdiced in [9] is analyzed game theoretically by Halpern and Teague in [3]. The scheme can be seen as a strategic game with n players. Each player can take one of two actions: reveal their share of the secret or not. Player i can cheat the system by not revealing her share and using the other players' piece of the secret in addition to her own in order to be the only player able to recover the secret. In rational secret sharing, the order of preference for player i is defined in the following way: *player i is the only player who learns the secret* $\geq_i$ *all players learn the secret* $\geq_i$ *no players learn the secret* $\geq_i$ *player i does not learn the secret and other players do.* As shown in [3] it turns out that not sharing the secret is a unique Nash equilibrium: which is an outcome in which it does not help any agent involved to unilaterally deviate from this outcome. What does this mean for rational secret sharing? It means as long as the secret is worth more to an agent when fewer agents know it, that rational agents will choose to not share. The purpose of this scheme is to spread the secret amongst agents so that they can eventually all learn the secret, but it turns out that as long as the agents are rational, none of them will learn the secret. This means that designing a secret sharing protocol where the agents are rational is not viable.

How could one solve this secret sharing dilemma and make this protocol viable in a rational setting? A solution to the rational secret sharing problem can be described as a protocol in which rational secret sharing participants decide to share their pieces of the secret with eachother. It must be that the protocol can be proven to be viable using game theoretic analysis. I will first describe the existing protocols within the rational secret sharing literature, and in the next section I will describe my protocol and what sets it apart from the others. In [3], Halpern and Teague develop a

randomized mechanism for rational secret sharing in a (3,3) secret sharing scheme. Their mechanism randomizes whether each participant is responsible to share in that round, which changes the game and the preferred strategy. The uncertainty introduced in this model changes the outcome of the protocol from mutual not sharing to mutual sharing. However, they show that it is impossible to get around the effect of the prisoner's dilemma in the (2,2) secret sharing scheme, assuming that the dealer always sends correct shares to the players [3]. In [2], Katz and Gordon show that this assumption is the reason that Halpern and Teague came to their impossibility result. Katz and Gordon develop a mechanism or the general (t, n) scheme where there is a probability of β that a participating agent will get a correct share and a probability $(1-\beta)$ that they will get a phony share. When the secret is recovered by a player and it is not an element of the subset of possible secrets, then both players know that at least one of them has received a phony share and the process is repeated. Using this mechanism, the dealer can adjust β according to the utilities in order to guarantee cooperation. This means that the dealer creates a level of uncertainty in order to encourage cooperation [2]. In both of these solutions the existence of uncertainty is what solves the dilemma and encourages cooperation within the protocol. In both of these models the impossibility result is circumvented, by using uncertainty about the other player's participation, and whether the secret being shared is real or phony.

Another way to overcome this problem is to model the agents as not only self-interested but also as social. This means that players are concerned for their own reputation and that by defecting now they will affect their future payoff by dirtying their reputation. A new game theoretic model can be built in order to illustrate agent's reputation. (See [1].) Stinson and Nojoumian use a reputation model in order to force a positive result within their secret sharing protocol in [7], their reputation model has multiple rounds of play. The unique thing about this model is that only a subset of the existing players is chosen to participate in that round. Each player has a value for their reputation and this value is used to determine the probability with which the player will be chosen in the current round. Defecting in a round decreases the players' reputation value and cooperating in a round increases this value. In some way this can be considered to introduce uncertainty as to whether or not the player will receive a share of the secret at all. As in the other models, this uncertainty drives the players to cooperate.

Another solution is to build in the agent's uncertainty about utility and/or game length. This idea has been explored in the game theoretic field in many papers

including [4] where player's have uncertainty of the opposing players' payoff which can be enough to encourage cooperation. Maleka shows in [6] that an infinitely repeated secret sharing game has an equilibrium of mutual cooperation. This paper also shows that a setting in which players are certain about which round will be the last round, the equilibrium is one of mutual defection. Maleka then shows that if players are uncertain of game length (i.e. which round will be the last) this is analogous to the infinitely iterated environment in which mutual cooperation is the equilibrium. Although this is a positive result, it might be rather impractical for agents to have to not know which round they would choose to stop partipating in. In a secret sharing environment it might be more practical to assume that although an agent has a level of uncertainty about the last round of their opponent, they are certain of their own last round. Another way of saying this is that each player will play a maximum number of rounds. The players know their own personal maxiumums but not the maximums of their opponents. The number of rounds that will be played is the minimum of all players' maximums.

This kind of unbalanced uncertainty about the number of rounds in a game has not been considered from a multi-party computation perspective. It has, however, been dealt with in the game theory literature in a paper written by Samuelson called "A note on uncertainty and cooperation in a finitely repeated prisoner's dilemma" [8]. This paper talks about the finite iterated prisoner's dilemma in which the agents know which round is their own last round and do not know the last round of the opposing agent. The opposing player's last round becomes a random variable with a geometric probability distribution. Samuelson gets a positive result and proves that there is an admissible game with a cooperative strategy. This result can easily be applied to the secret sharing setting.

1.3 My Claims

As in [6], we will discuss finitely iterated secret sharing. There will be more than one secret being divulged within the same group of agents. An application of this would be if after a set amount of time an encryption key expires and a new one is generated. Each time this happens, the agents must undergo a round of secret sharing.

My solution to the finitely iterated secret sharing problem is to develop a protocol that works on the assumptions that each player has their own horizon, and does not know the opposing player's horizon. A personal horizon is the round in which the

player wishes to be their last. The last round will be the minimum of all players' maximums. This way the players will have some knowledge about which round is the last. In [8], this type of game has been called a "privately informed game" and was shown to have a cooperative equilibrium where the players' beliefs about each other's horizons is represented by a geometric probability distribution. The model in this paper has never been used to represent rational secret sharing. Building a protocol based on this uncertainty model would be considered a new and unique solution to the finitely repeated secret sharing problem. We are going to extend this model and prove the existence of a cooperative equilibrium under it. We also a give a quantitative relationship between the degree of uncertainty and the conditions under which a cooperative equilibrium can be obtained. The difference between this solution and my solution is that my solution works on the assumption that there is some common upper bound on the players's horizons. The upper bound can be qualitatively described as the player's uncertainty. The higher the upper bound is the less information the player has about the opponent's horizon. My solution will offer a synchronous and asynchronous version and both versions of the protocol have a cooperative equilibrium making them viable protocols. The finitely iterated prisoner's dilemma can be used to model this situation and Chapter 4 involves a discussion of how to solve this in terms of game theoretic analysis and proving that there exists a cooperative equilibrium strategy.

1.4 Agenda

Chapter 2 describes the solution concepts of game theory used to prove the viability of rational secret sharing protocols.

Chapter 3 outlines the solution as both a synchronous and an asynchronous protocol along with a description of the way that the agent's uncertainty is represented.

Chapter 4 includes the evaluation of the protocol using solution concepts introduced in Chapter 3.

Chapter 5 summarizes the results and shows their significance to the field of secret sharing along with the possible future work.

Chapter 2

Evaluation method

2.1 Game Theory and One Shot Games

Definition 1. *A game G is a 3-tuple:*

$$G = (N, A = \{A_i | i \in N\}, U = \{U_i : A_1 \times A_2 \times ... \times A_k \to \mathbb{R} | k = |N|\})$$

Where N is the set of players, A_i is the set of actions in which player i can choose from, and U_i is the utility function that determines the utility that i will receive based on the action profile, or the list of actions taken by each player. A player's strategy can be described as the action that the player chooses.

The prisoner's dilemma is a game in which there are two players. Each player decides whether to cooperate or defect. The game definition is as follows:

$$G_{PD} = (\{A, B\}, A_i = \{1, 2\}, U_i(x, y) = i_{xy})$$

where $a_{12} < a_{22} < a_{11} < a_{21}$ and $b_{21} < b_{22} < b_{11} < b_{12}$. The values of a_{xy} and b_{xy} represent the utility earned by player A and player B respectively when player A plays x and player B plays y. Figure 2.1 is this game in a tabular format.

	1	2
1	a_{11}, b_{11}	a_{12}, b_{12}
2	a_{21}, b_{21}	a_{22}, b_{22}

Figure 2.1: Prisoner's Dilemma

Which strategy is the optimal one for each player? One way of answering this question is to find the Nash Equilibrium. A strategy of a game is considered to be a Nash Equilibrium if it best for any one player to not veer from the strategy as long as all other players also do not veer. The mathematical definition follows:

Definition 2. ***Nash Equilibrium****: An action profile (x,y) where* $U_a(x, y) \geq U_a(x', y) \forall x' \in A_b | x' \neq x$ *and* $U_b(x, y) \geq U_b(x, y') \forall y' \in A_a | y' \neq y$

The Nash Equilibrium of the prisoner's dilemma is (2,2). The intuition behind this equilibrium is to view the game from the player's perspective. Player A considers what she should do if Player B plays strategy 1, and then what she should do if player B plays strategy 2. Looking at the tabular game, it is clear to see that either way, it is better for player A to play strategy 2. The same can be said symmetrically about player B. This is a dilemma considering that from an outsider's perspective it is better for both players if the outcome is (1,1). The utility for outcome (1,1) is better for both players than the utility for outcome (2,2).

2.2 Infinitely Repeated Prisoner's Dilemma

In a repeated game, players play the same game for a certain number of rounds. Consider the repeated prisoner's dilemma. It might be the case that it is possible for the players to establish some sort of deal to cooperate in each round. There are multiple rounds and time for the players to establish a trusting relationship. In fact, in an infitely repeated prisoner's dilemma there are endless rounds to do so. In a setting where there are multiple rounds, a strategy can depend on the outcomes of previous rounds. For example, the following is an example of a strategy for the infinitely repeated prisoner's dilemma game.

Definition 3. *The* ***Grim Trigger*** *Strategy is one in which player i cooperates in each round unless a player has defected in a previous round.*

In order to determine whether or not a particular strategy σ is a Nash equilibrium we must assume that one player follows σ, and compare the other player's utility gained by following this strategy versus deviating from σ. In order to calculate utility over multiple rounds a **Discount Factor** may be used. Each player i will have their own unique discount factor, $D_i \in [0, 1]$. The significance of the discount factor is that round $n+1$ will have less importance than round n by a factor of D_i. This means the

utility for player i playing in rounds of the prisoner's dilemma would be calculated in the following way:

$$U_i^n = \sum_{j=0}^{\infty} D_i^j U_i(\{A_A, A_B\}_n)$$

It is well known that the grim trigger strategy σ_{GT} is a Nash equilibrium. Assume Player B follows σ_{GT}. Displayed below is the utility Player A gains by following grim trigger and also the utility Player A gains by deviating in some round.

Following σ_{GT}:

$$u_f = \sum_{j=0}^{\infty} D_a^j a_{11}$$

Deviating from σ_{GT} in round n:

$$u_d = \sum_{j=0}^{n-1} D_a^j a_{11} + D_a^n a_{21} + \sum_{j=n+1}^{\infty} D_a^j a_{22}$$

It is true that $u_f > u_d$ for large enough values of D_a. Symmetrically the same can be said for Player B. This is why the grim trigger strategy is a Nash equilibrium for the infinitely repeated prisoner's dilemma. This can be called a cooperative equilibrium because the players have incentive to cooperate in each round.

2.3 Finitely Repeated Prisoner's Dilemma

What happens if there are a finite number of rounds and the number of rounds is known to all players? This means that in the final round n_f there is no incentive for either player to cooperate, therefore both players will defect. In round $n_f - 1$ both players are aware that it is best for them to defect in round n_f. This means there is no incentive for the players to cooperate in round $n_f - 1$ either. Using backwards induction we can conclude that neither player will have incentive to cooperate in any round. In order to formalize this concept subgame and subgame-perfect equilibrium must be defined.

Definition 4. ***Subgame****: Given a repeated game G_n, which is G repeated n times, a subgame G_n^m of G rooted at round m is the repeated game that starts with round m and is played until round n.*

Definition 5. *A* ***Subgame-perfect equilibrium*** *of a game G is any strategy profile*

s such that for any subgame G' of G, the restriction of s to G' is a Nash Equilibrium of G'. (Definition as seen in [5].)

Theorem 1. *The repeated Prisoner's dilemma PD_n has a Subgame-perfect equilibrium of s, where s is the strategy profile in which each player defects in each round.*

Proof. In subgame PD_n^n the only Nash equilibrium is for both players to defect. In any subgame PD_n^m, where for all subgames PD_n^r in which $r > m$ the Subgame-perfect equilibrium of PD_n^r is to defect in each round, the subgame-perfect equilibrium of PD_n^m is also to defect in each round. Using backwards induction, it is clear that the repeated Prisoner's dilemma PD_n has a subgame-perfect equilibrium of defecting in each round. □

The utility for player i playing in n rounds of the prisoner's dilemma would be calculated in the following way:

$$U_i^n = \sum_{j=0}^{n-1} D_i^j U_i(\{A_A, A_B\}_n)$$

This utility equation can be used to calculate the utility given the actions that the players take. For example, the utility for mutual cooperation can be compared to mutual defection. It can be seen that mutual cooperation is better for both players even though the Nash equilbibrium is mutual defection as shown above. This is why even with repeated rounds, this is still considered to be a dilemma.

2.4 Uncertainty in the number of rounds

What happens if the players participating in the prisoner's dilemma are uncertain of which round will be the last round? Because each player is uncertain of whether the current round is the last or not, this situation is analogous to the infinitely repeated prisoner's dilemma and the analysis is the same. This means that the uncertainty causes the players to cooperate in a game that without the uncertainty, the players would defect in. This can be an unrealistic condition because players are likely to know how many rounds they care to participate in. This leads to an environment in which players know which round will be their last but have a degree of uncertainty about which round will be their opponent's last. This environment is used in the Samuelson paper [8].

Samuelson shows that if agents have knowledge of their personal maximum number of repetitions this can induce a cooperative equilibrium. Player A will participate in a maximum of N_A rounds and player B will participate in a maximum of N_B rounds, where N_A and N_B represent the players' planning horizon. The value represents the length of time each player is interested in interacting with the other player. The number of rounds played will be the minimum of N_A and N_B. Therefore each player has a degree of uncertainty of which round will be the last. This is known as a privately informed game because the player knows their own horizon but not the horizon of the other player.

Player A knows N_A and her knowledge of N_B can be described as follows. In any given round n, there is a k_b chance that player B will participate for at least the current round. There is a function that gives the probability that the current round will be the opposing players last. It is a probabilty distribution and can be written formally as $f_a : \mathbb{Z}_+ \to [0,1]$ where there exists a $k_b \in [0,1]$ where $f_a(n) = (1-k_b)k_b^{n-1}$. This means that Player A believes that there is a k_b chance that player B will cooperate in the current round. Player A knows N_B and her knowledge of N_A is described by the probability distribution $f_b : \mathbb{Z}_+ \to [0,1]$ where there exists a $k_b \in [0,1]$ where $f_b(n) = (1-k_a)k_a^{n-1}$.

Definition 6. *A **Privately Informed Game** is a 5-tuple (N, A, U, D, K) where $D = D_i | i \in N$ and $K = k_i | i \in N$.*

In order to calculate the utility in a privately informed game the player's discount factors and beliefs about the last round must be used in the following way:

$$U_i^n = \sum_{j=0}^{n-1} (1-k_i)k_i^j D_i^j U_i(\{A_A, A_B\}_n)$$

Using this environment, Samuelson gets a positive result. There exists an admissible privately informed game such that the players will follow the finite grim trigger strategy as described below:

Definition 7. *The **Finite Grim Trigger** Strategy is one in which player i cooperates in each round unless one of the following conditions becomes true:*
(i) A player has defected in a previous round
(ii) The current round is N_i

Chapter 3

The Protocol

In this chapter we will consider a secret sharing game in which the players are assumed to have a common upper bound on their personal maximum number of rounds they will play and call it U. This game could be considered as either asynchronous or synchronous, and the difference will be described in the first section of this chapter. In the next section we will define the player's beliefs about the opposing player's horizon. If there is some upper bound on the number of rounds the other player is interested in playing but the player has no other information about the opponent's last round, then what is the probability of each remaining round being the opponent's last? This is discussed in Section 3.2. One goal of this thesis is to show the existence of a relationship between the uncertainty that secret sharing agents have versus the existence of a cooperative equilibrium and ultimately a viable protocol and solution. In the previous chapter we discussed existing solutions and their relationship to different kinds of uncertainty. In the solution presented here, the uncertainty is linked to the upper bound on number of rounds U. The existence of a cooperative sequential equilibrium in a synchronous game as compared to the uncertainty of the players is discussed in Sections 3.3.

3.1 Asynchronous vs Synchronous

A synchronous network protocol is one in which the participating agents send and receive their messages at the same time. A synchronous secret sharing protocol would require that each agent receives each piece of the secret at the same time. This can be represented by a Normal-Form Game as in figure 3.1. Each player makes a decision

mutually unaware of each other's decision. As in [6], the players share their secrets according to a global clock. In order to implement the synchronous secret sharing game a synchronous channel must be modelled. This can be done by using a trusted third party. The agents each send their share of the secret or their decision not to share to a third party. Once the third party has received the information from each player, the third party sends along this information to each of the agents. This is required in order to model the idea that the players make each decision without information of what the other players have done.

The benefit of the asynchronous secret sharing game is that no such third party is necessary. In the asynchronous model there is no global clock. The shares of the secret are distributed to each player and then Player A will make the decision to share or not share. Once receiving both Player A's decision and secret (if her decision was to share), Player B will then make the decision to share or not share. Once Player A receives Player B's decision, Player A will notify the dealer and the next round can start. This type of protocol is better represented by Perfect-Information-Extensive-Form Games [5] as in figure 3.1.

3.2 Player's Beliefs

Instead of the players having beliefs about the likelihood of players cooperating in the current round, the players will have beliefs about the value of their opponent's last round. The only information that the player has is that the upper bound is U. Let N_A be player A's last round and N_B be player B's last round. Player A knows that $N_B < U$ and Player B knows that $N_A < U$. This signifies that the players are certain that the other player will not play past round U and have no reason to believe that one round is more likely to be the other player's last than another round. Thus at every round before U, players believe that any remaining round is equally likely to be their opponent's last. In other words, in the first round Player A believes that all rounds n where $n \leq U$ are equally likely to be N_B. Assuming this is true means that it is true of all rounds. In any round $r \leq U$, Player A believes that all rounds n where $r \leq n \leq U$ are equally likely to be N_B. This is shown in the proposition below. We use Baye's rule to prove it.

Definition 8. *Baye's Rule:*

$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B|A)\Pr(A)+\Pr(B|\neg A)\Pr(\neg A)}$$

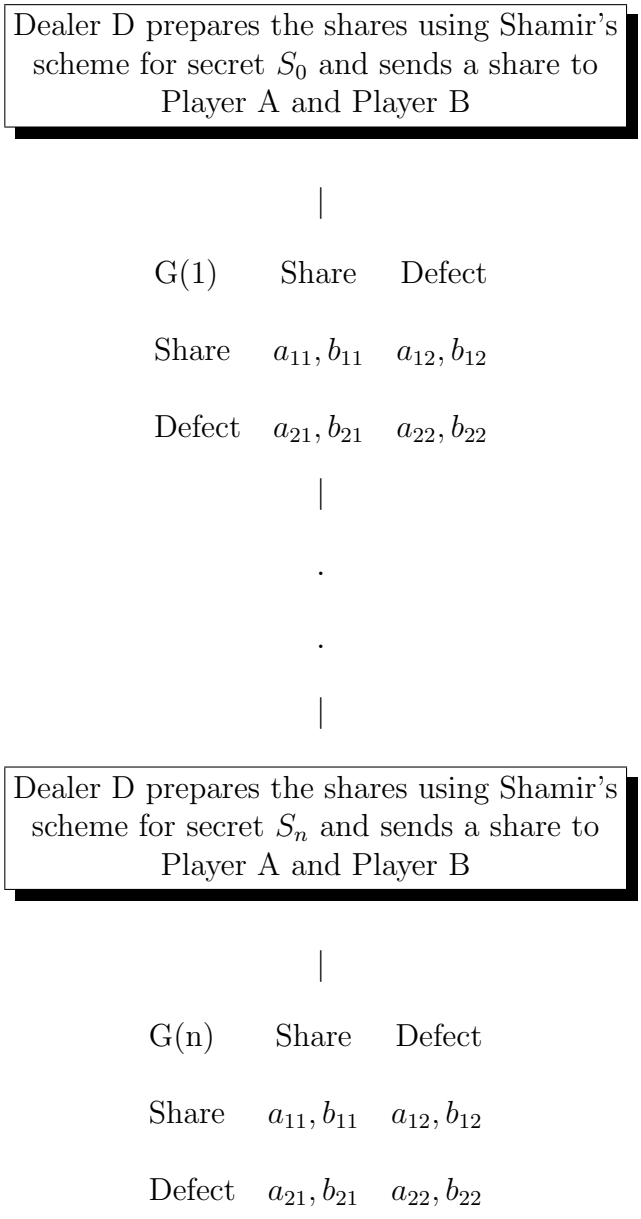

Figure 3.1: Synchronous Repeated Secret Sharing Represented by Sequential Normal Form Game

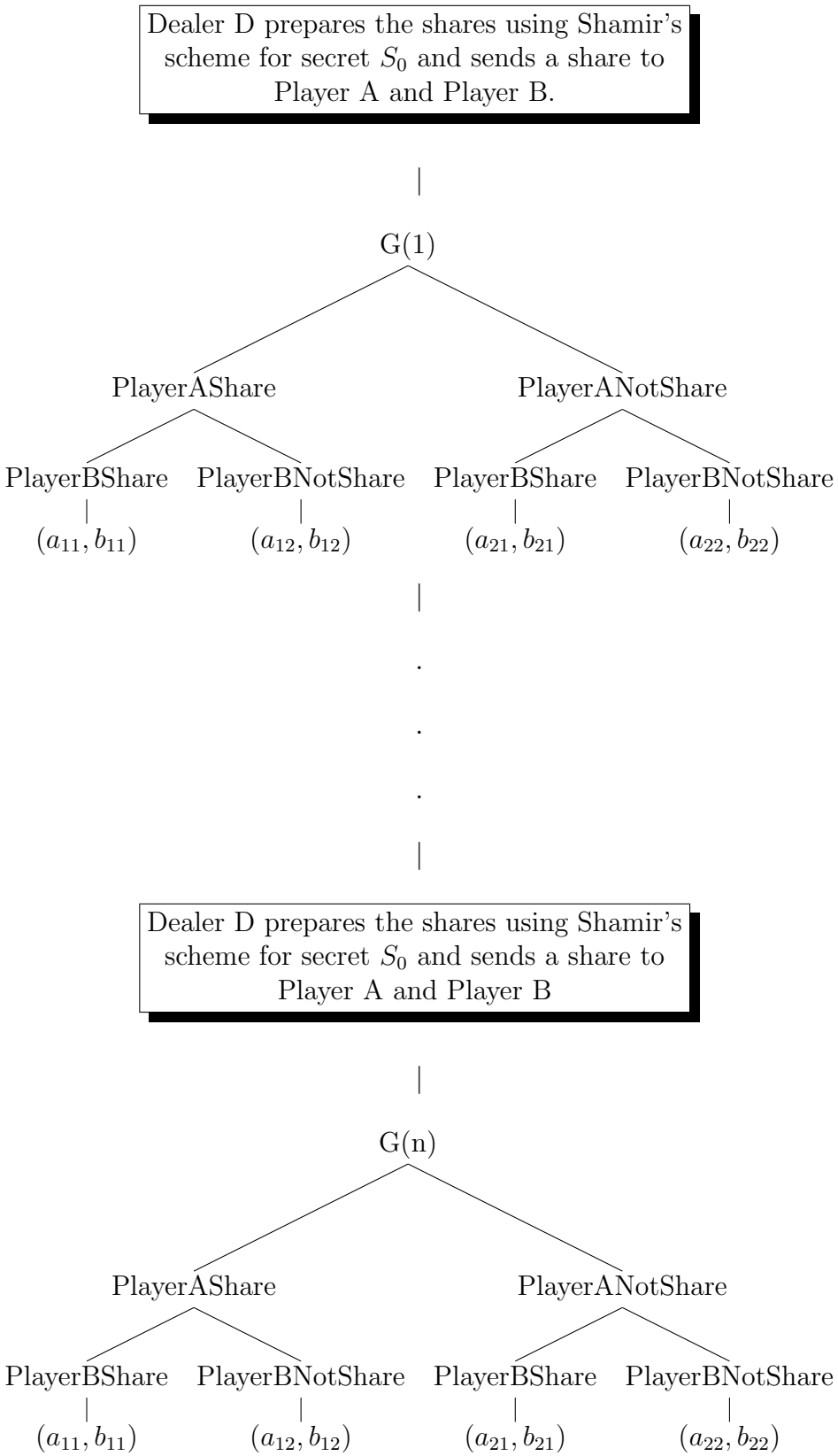

Figure 3.2: Repeated Asynchronous Secret Sharing Represented by a Sequential Extensive Game. (The length 2 vector in this figure represents the utility earned by each player. The first element corresponds to the utility gained by A, second to B)

Proposition 1. *Assuming player B is playing the finite grim trigger strategy, if neither player has defected in any round $r < n$, then in round n it is Player A's belief that each round k after the current round and before the common upper bound ($n \leq k < U$) is equally likely to be N_B. It is a uniform probability distribution over the remaining rounds.*

Proof. Let $k' \geq k$

$$P[N_B = k' | N_B \neq 1, N_B \neq 2, ..., N_B \neq k-1]$$

$$= \frac{P[N_B \neq 1, N_B \neq 2, ..., N_B \neq k-1 | N_B = k'] P[N_B = k']}{P[k \wedge N_B \neq 1, N_B \neq 2, ..., N_B \neq k-1]}$$

$$= \frac{\frac{1}{U}}{\frac{U-k}{U}} = \frac{1}{U-k}$$

□

3.3 Definition of Uncertainty

Definition 9. ***Degree of Uncertainty***

Let U be the upper bound on the number of rounds. As in Player A knows that $N_B \leq U$ and Player B knows that $N_A \leq U$ where $U = N_A + K = N_B + L$. K represents Player A's level of uncertainty and L represents Player B's level of uncertainty.

It is accepted that beyond these values K and L that the players have no beliefs that one round is more likely to be the last round than another. If we can compare these values to the existence of a cooperative equilibrium then we can show the relationship between the uncertainty of a player and the existence of a cooperative equilibrium.

Chapter 4

Evaluation, Analysis and Comparisons

4.1 Cooperative Equilibrium in a Synchronous Protocol

The following Lemmas and theorems show that in the synchronous finitely repeated prisoner's dilemma, as laid out in chapter 3, the finite grim trigger strategy is a sequential equilibrium. This means that in all rounds except the minimum of N_A and N_B, players will cooperate and therefore can be considered a cooperative equilibrium.

Lemma 1. *It is best for Player A to defect in round N_A.*

Proof. In round N_A Player A knows there will be no future rounds. This is the same situation as a one shot prisoner's dilemma game and it is a dominant strategy to defect. □

Lemma 2. *Any best response strategy is of the form of a series of unbroken cooperation followed by a series of unbroken defection.[8]*

Proof. If player A has defected in a round r, then player B will be defecting in all rounds after r including round n according to the finite grim trigger strategy. Since Player A's best response to Player B choosing to defect is to defect as well, Player A will defect in round n as well. This means that in any of the strategies considered to be player A's best response to the finite grim trigger strategy it must be true that once player A defects in any round r, they will defect in all future rounds $n > r$.

□

Lemma 3. $(i) \wedge (ii) \wedge (iii) \Rightarrow (iv)$:
(i) No player has defected in any rounds previous to the current round n_c
(ii) $n_c < N_A$
(iii) Player A defects in the next round $n_c + 1$
(iv) There exists an admissible game in which it is best for Player A to cooperate in round n_c

Proof. The following table describes the utility gained by player A for all rounds after the current round n_c for each possible value of N_B, assuming that N_B has not already been reached. Each row of the table represents the possible values of N_B, where the first row represents $N_B = n_c$, the second row represents $N_B = n_c + 1$, the third row represents $n_c + 2 \leq N_B \leq N_A$ and the fourth row represents $N_B > N_A$. The second column indicates the probability that round $n = N_B$. Since condition (i) states that neither player has defected in any previous rounds, this means that N_B has not yet been reached and there are r remaining possible values of N_B, where $r = U - n + 1$. The chance that any of the remaining rounds including n_c are equal to N_B is $\frac{1}{r}$. Table 4.1 summarizes the utility gained by player A cooperates assuming (i), (ii) and (iii) from Lemma 3, and table 4.1 summarizes the utility gained by player A when she defects with these assumptions.

n	$P[n = N_B]$	Utility if $round = N_B$
n_c	$\frac{1}{r}$	(a_{12})
$n_c + 1$	$\frac{1}{r}$	$(a_{11} + D_a a_{22})$
$[n_c + 2, N_A]$	$\frac{1}{r}$	$(a_{11} + D_a a_{21} + \sum_{t=2}^{n} D_a^t a_{22})$
$[N_A + 1, U]$	$\frac{1}{r}$	$(a_{11} + D_a a_{21} + \sum_{t=2}^{N_A} D_a^t a_{22})$

Figure 4.1: Utility Summary for Player A Cooperating

In order to calculate Player A's total expected utility over all rounds $n \geq n_c$, we must sum the product of the probability of round n being N_B and the utility that player A earns in the case that the round n is N_B. Using tables 4.1 and 4.1 as reference, we sum the product of the second and third column from each row. Figure 4.1 describes Player A's utility upon cooperating or defecting in round $n_c < N_A$ where Player A cooperates in round $n_c + 1$ is given first and needs to be larger than the

n	$P[n = N_B]$	Utility if $round = N_B$
n_c	$\frac{1}{r}$	(a_{22})
$n_c + 1$	$\frac{1}{r}$	$(a_{21} + D_a a_{22})$
$[n_c + 2, N_A]$	$\frac{1}{r}$	$(a_{21} + \sum_{t=1}^{n} D_a^t a_{22})$
$[N_A + 1, U]$	$\frac{1}{r}$	$(a_{21} + \sum_{t=1}^{N_A} D_a^t a_{22})$

Figure 4.2: Utility Summary for Player A Defecting

utility when A defects which is given second. We will then prove that there is an admissible game with this property in order to prove Lemma 3.

In order for cooperate to dominate defect in any round $n < N_A$ it must be true that:

$$u_c > u_d \tag{4.1}$$

$$a_{11}+a_{12}-a_{21}-a_{22}+\sum_{i=2}^{N_A-n} a_{11}+D_a a_{21}-a_{21}-D_a a_{22}+\sum_{i=N_A-n+1}^{U-n} a_{11}+D_a a_{21}-a_{21}-D_a a_{22} > 0 \tag{4.2}$$

$$a_{11} + a_{12} - a_{21} - a_{22} + \sum_{i=2}^{U-n} a_{11} + D_a a_{21} - a_{21} - D_a a_{22} > 0 \tag{4.3}$$

$$a_{11} + a_{12} - a_{21} - a_{22} + (U - n - 1)(a_{11} - a_{21} + D_a a_{21} - D_a a_{22}) > 0 \tag{4.4}$$

Since $U = N_A + K$, in order for equation (4.4) to hold true for $n = N_A - 1$, it must be true that:

$$a_{11} + a_{12} - a_{21} - a_{22} + (K)(a_{11} - a_{21} + D_a a_{21} - D_a a_{22}) > 0 \tag{4.5}$$

The first four terms, $a_{11} + a_{12} - a_{21} - a_{22}$, of (4.4) add up to a negative number because $a_{12} < a_{22} < a_{11} < a_{21}$. The final term, $(U-n-1)(a_{11}-a_{21}+D_a a_{21}-D_a a_{22})$ must be positive in order for (4.4) to hold true. So if (4.4) holds then by decreasing n we will only be increasing the overall value of the left side of (4.4). In other words as long as equation (4.4) holds for $n = N_A - 1$ then it holds for all lesser n.

The following inequality is the analogous necessary condition but for Player B:

Cooperate:

$$u_c = \frac{1}{r}(a_{12})$$

$$+\frac{1}{r}(a_{11} + D_a a_{22})$$

$$+ \sum_{i=2}^{N_A-n} \frac{1}{r}(a_{11} + D_a a_{21} + \sum_{t=2}^{i} D_a^t a_{22})$$

$$+ \sum_{i=N_A-n+1}^{U-n} \frac{1}{r}(a_{11} + D_a a_{21} + \sum_{t=2}^{N_A-n} D_a^t a_{22})$$

Defect:

$$u_d = \frac{1}{r}(a_{22}) + \frac{1}{r}(a_{21} + D_a a_{22})$$

$$+ \sum_{i=2}^{N_A-n} \frac{1}{r}(a_{21} + \sum_{t=1}^{i} D_a^t a_{22})$$

$$+ \sum_{i=N_A-n+1}^{U-n} \frac{1}{r}(a_{21} + \sum_{t=1}^{N_A-n} D_a^t a_{22})$$

Figure 4.3: Utility Comparison

$$b_{11} + b_{21} - a_{21} - b_{22} + (L)(b_{11} + b_{12} + D_b b_{12} + D_b b_{22}) > 0 \tag{4.6}$$

In order for this to be an admissible game by the definition of discount factors, it must be true that $D_a \leq 1$ which means there must exist a $k, a_{21}, a_{11}, a_{22}, a_{12}$ such that Equation (4.7) is true. This equation comes from rearranging Equation (4.5) for D_a and noting that D_a must be between the resulting formula and 1.

$$1 > D_a > \frac{a_{21} + a_{22} - a_{12} - a_{11}}{K(a_{21} - a_{22})} \tag{4.7}$$

which holds as long as $(K+1) > \frac{(a_{12}-a_{21})}{(a_{22}-a_{11})}$

Analogously for player B

$$1 > D_b > \frac{b_{12} + b_{22} - b_{21} - b_{22}}{L(b_{12} - b22)} \tag{4.8}$$

which holds as long as $(L+1) > \frac{(b_{21}-b_{12})}{(b_{22}-b_{11})}$

□

Theorem 2. *There exists an admissible synchronous prisoner's dilemma game in which the finite grim trigger strategy is a sequential equilibrium.*

Proof. I will now show that the finite grim trigger strategy is one of Player A's best responses to player B following the finite grim trigger strategy in an admissible game that follows the conditions laid out in equations (4.7) and (4.8)

Assume player B is playing the finite grim trigger strategy. I will show that in each round n Player A will act accordingly to the finite grim trigger strategy:

Assume neither player has defected in a previous round and $n < N_A$.

If Player A defects in round $n+1$ it is best for Player A to cooperate in round n by Lemma 3.

If Player A cooperates in round $n+1$ it is best for Player A to cooperate in round n by Lemma 2.

Assume that one player has defected in a previous round and $n < N_A$. Then by Lemma 2, it is best for Player A to defect in round n.

By Lemma 1 it is best for player A to defect in round $n = N_A$ and by Lemma 2 it is best for player A to defect in all rounds $n > N_A$ and $n > N_B$.

Therefore player A will cooperate until player B has defected or until the current round is N_A.

□

4.2 Cooperative Equilibrium in an Asynchronous Protocol

The analysis for the asynchronous protocol must be done separately. The knowledge of the action of the first player can affect the action of the second player. This means that the finite grim trigger strategy for the asynchronous protocol is slightly different than the one for the synchronous protocol. The second player will defect in the current round if the first player has done so.

Definition 10. *The **Asynchronous Finite Grim Trigger** Strategy is one in which player i cooperates in each round unless one of the following conditions becomes true:*
(i) A player has defected in a previous round
(ii) Player i plays second and the first player has defected in the current round (iii) The current round is N_i

Lemma 1 and Lemma 2 hold true and the proofs also suffice for the asynchronous protocol. Lemma 3 changes slightly and is rewritten as Lemma 4 for the asynchronous version of the protocol.

Lemma 4. $(i) \wedge (ii) \wedge (iii) \wedge (iv) \Rightarrow (v)$:
(i) No player has defected in any rounds previous to the current round n_c
(ii) If Player B is the first player then Player B cooperates in round n_c
(iii) $n_c < N_A$
(iv) Player A defects in the next round $n_c + 1$
(v) There exists an admissible game in which it is best for Player A to cooperate in round n_c

Proof. First we will assume that player A goes first. The following table is analogous to 4.1 and describes the utility gained by player A for all rounds after the current round n_c for each possible value of N_B, assuming that N_B has not already reached. Since in part (i) of this Lemma, it states that neither player has defected in any previous rounds, this means that N_B has not yet reached. Table 4.2 summarizes the utility gained by player A cooperates assuming (i), (ii), (iii), and (iv) from Lemma 4,

and table 4.2 summarizes the utility gained by player A when she defects with these assumptions. Since player A goes first this table stays the same as before if player A decides to cooperate. However, if player A decides to defect, then player B will definitely defect in the current round n_c and all following rounds regardless of the value of N_B.

n	$P[n = N_B]$	Utility if $round = N_B$
n_c	$\frac{1}{r}$	(a_{12})
$n_c + 1$	$\frac{1}{r}$	$(a_{11} + D_a a_{22})$
$[n_c + 2, N_A]$	$\frac{1}{r}$	$(a_{11} + D_a a_{22} + \sum_{t=2}^{n} D_a^t a_{22})$
$[N_A + 1, U]$	$\frac{1}{r}$	$(a_{11} + D_a a_{22} + \sum_{t=2}^{N_A} D_a^t a_{22})$

Figure 4.4: Utility Summary for Player A Cooperating in the Asynchronous model where player A goes first

n	$P[n = N_B]$	Utility if $round = N_B$
n_c	$\frac{1}{r}$	(a_{22})
$n_c + 1$	$\frac{1}{r}$	$(a_{22} + D_a a_{22})$
$[n_c + 2, N_A]$	$\frac{1}{r}$	$(\sum_{t=0}^{n} D_a^t a_{22})$
$[N_A + 1, U]$	$\frac{1}{r}$	$(\sum_{t=0}^{N_A} D_a^t a_{22})$

Figure 4.5: Utility Summary for Player A Defecting in the Asynchronous model where player A goes first

The following table describes Player A's utility upon cooperating or defecting in round $n_c < N_A$ where Player A defects in round $n_c + 1$ is given first and needs to be larger than the utility when A defects which is given second. We will then prove that there is an admissible game with this property in order to prove Lemma 4.

Cooperate:

$$u_c = \tfrac{1}{r}(a_{12})$$

$$+\tfrac{1}{r}(a_{11} + D_a a_{22})$$

$$+ \sum_{i=2}^{N_A-n} \tfrac{1}{r}(a_{11} + D_a a_{22} + \sum_{t=2}^{i} D_a^t a_{22})$$

$$+ \sum_{i=N_A-n+1}^{U-n} \tfrac{1}{r}(a_{11} + D_a a_{22} + \sum_{t=2}^{N_A-n} D_a^t a_{22})$$

Defect:

$$u_d = \tfrac{1}{r}(a_{22}) + \tfrac{1}{r}(a_{22} + D_a a_{22})$$

$$+ \sum_{i=2}^{N_A-n} \tfrac{1}{r}(\sum_{t=0}^{i} D_a^t a_{22})$$

$$+ \sum_{i=N_A-n+1}^{U-n} \tfrac{1}{r}(\sum_{t=0}^{N_A-n} D_a^t a_{22})$$

In order for cooperate to dominate defect in any round $n < N_A$ it must be true that $u_c > u_d$ for all $n < N_A$. This inequality simplifies to the condition below:

$$a_{11} + a_{12} - 2a_{22} + (U - n - 1)(a_{11} - a_{22}) > 0 \tag{4.9}$$

Since $U = N_A + K$, in order for equation (4.9) to hold true for $n = N_A - 1$, it must be true that:

$$a_{11} + a_{12} - 2a_{22} + (K)(a_{11} - a_{22}) > 0 \tag{4.10}$$

The final term, $(U_B - n - 1)(a_{11} - a_{22})$, must be positive in (4.9), because $a_{12} < a_{22} < a_{11} < a_{21}$. So by decreasing n we will only be increasing the overall value of the left side of (4.9). This means that as long as (4.10) is true then so is (4.9).

The following inequality is the analogous necessary condition but for Player B:

$$b_{11} + b_{21} - 2b_{22} + (L)(b_{11} + b_{22}) > 0 \tag{4.11}$$

In order for this to be an admissible game by the definition of discount factors, it must be true that $0 < D_a \leq 1$. Since the value of D_a is independent of Equations (4.10) and (4.11), this has no effect on the limitation of the uncertainty variable K.

Now, we will assume that player A goes second and creates the corresponding tables to compare the utility of Player A cooperating when playing second and defecting when playing second. Since player A goes second and we are assuming that there has been no defection in previous rounds (see (i) of Lemma 4), then player B cooperates in round n_c (see (ii) of Lemma 4).

n	$P[n = N_B]$	Utility if $round = N_B$
n_c	0	(a_{12})
$n_c + 1$	$\frac{1}{r-1}$	$(a_{11} + D_a a_{22})$
$[n_c + 2, N_A]$	$\frac{1}{r-1}$	$(a_{11} + D_a a_{21} + \sum_{t=2}^{n} D_a^t a_{22})$
$[N_A + 1, U]$	$\frac{1}{r-1}$	$(a_{11} + D_a a_{21} + \sum_{t=2}^{N_A} D_a^t a_{22})$

Figure 4.6: Utility Summary for Player A Cooperating in the Asynchronous model where player B goes first

n	$P[n = N_B]$	Utility if $round = N_B$
n_c	0	(a_{22})
$n_c + 1$	$\frac{1}{r-1}$	$(a_{21} + D_a a_{22})$
$[n_c + 2, N_A]$	$\frac{1}{r-1}$	$(a_{21} + \sum_{t=1}^{n} D_a^t a_{22})$
$[N_A + 1, U]$	$\frac{1}{r-1}$	$(a_{21} + \sum_{t=1}^{N_A} D_a^t a_{22})$

Figure 4.7: Utility Summary for Player A Defecting in the Asynchronous model where player B goes first

The table that describes Player A's utility upon cooperating or defecting in round $n_c < N_A$ where Player A defects in round $n_c + 1$ is given first and needs to be larger than the utility when A defects which is given second. We will then prove that there is an admissible game with this property in order to prove Lemma 4.

Cooperate:

$$+\tfrac{1}{r-1}(a_{11} + D_a a_{22})$$

$$+ \sum_{i=2}^{N_A-n} \tfrac{1}{r-1}(a_{11} + D_a a_{21} + \sum_{t=2}^{i} D_a^t a_{22})$$

$$+ \sum_{i=N_A-n+1}^{U-n} \tfrac{1}{r-1}(a_{11} + D_a a_{21} + \sum_{t=2}^{N_A-n} D_a^t a_{22})$$

Defect:

$$u_d = \tfrac{1}{r-1}(a_{21} + D_a a_{22})$$

$$+ \sum_{i=2}^{N_A-n} \tfrac{1}{r-1}(a_{21} + \sum_{t=1}^{i} D_a^t a_{22})$$

$$+ \sum_{i=N_A-n+1}^{U-n} \tfrac{1}{r-1}(a_{21} + \sum_{t=1}^{N_A-n} D_a^t a_{22})$$

In order for cooperate to dominate defect in any round $n < N_A$ it must be true that $u_c > u_d$ for all $n < N_A$. This inequality simplifies to the condition below:

$$a_{11} - a_{21} + (U - n - 1)(a_{11} - a_{21} + D_a a_{21} - D_a a_{22}) > 0 \tag{4.12}$$

Since $U = N_A + K$, in order for equation (4.12) to hold true for $n = N_A - 1$, it must be true that:

$$a_{11} - a_{21} + (K)(a_{11} - a_{21} + D_a a_{21} - D_a a_{22}) > 0 \tag{4.13}$$

The first two terms of Equation (4.12) when added together are negative. The final term, $(U - n - 1)(a_{11} - a_{21} + D_a a_{21} - D_a a_{22})$, of (4.9) must be positive in order for Equation (4.12) to hold, because $a_{12}a_{22}a_{11}a_{21}$. So by decreasing n we will only be increasing the overall value of the left side of (4.12). This means that as long as (4.13) is true then so is (4.12).

The following inequality is the analogous necessary condition but for Player B:

$$a_{11} - a_{21} + (K)(a_{11} - a_{21} + D_a a_{21} - D_a a_{22}) > 0 \tag{4.14}$$

In order for this to be an admissible game by the definition of discount factors, it must be true that $D_a \leq 1$ which means there must exist a $k, a_{21}, a_{11}, a_{22}, a_{12}$ such that Equation (4.15) is true. This equation comes from rearranging Equation (4.12) for D_a and noting that D_a must be between the resulting formula and 1. This is because the discount factor is the ratio of how much the player cares about the next round to how much the player cares about this round. The player must care an equal or less amount.

$$K > \frac{2(a_{21} - a_{11})}{(a_{21} - a_{22})} \tag{4.15}$$

□

I would now like to show that the Asynchronous Finite Grim Trigger Strategy is a Nash Equilibrium of the sequential game defined in Section 4. In order to do so I must show that when Player B plays the AFGT strategy, it best for player A to play the AFGT strategy whether she plays first or second in the sequential game.

Theorem 3. *There exists an admissible prisoner's dilemma asynchronous game in which the asynchronous finite grim trigger strategy is a sequential equilibrium.*

Proof. I will now show that the asynchronous finite grim trigger strategy is one of Player A's best responses to player B following the asynchronous finite grim trigger strategy in an admissible game that follows the conditions laid out in equations (4.7) and (4.8)

Assume player B is playing the asynchronous finite grim trigger strategy. I will show that in each round n Player A will act accordingly to the asynchronous finite grim trigger strategy:

Assume neither player has defected in a previous round and $n < N_A$ and a defection has not occurred in the current round.

If Player A defects in round $n+1$ it is best for Player A to cooperate in round n by Lemma 4.

If Player A cooperates in round $n+1$ it is best for Player A to cooperate in round n by Lemma 2.

Assume that one player has defected in a previous round and $n < N_A$. Then by Lemma 2, it is best for Player A to defect in round n.

By Lemma 1 it is best for player A to defect in round $n = N_A$ and by Lemma 2 it is best for player A to defect in all rounds $n > N_A$ and $n > N_B$.

Therefore player A will cooperate until player B has defected or until the current round is N_A.

□

Chapter 5

Conclusions

5.1 Contribution to Game Theory

There exists a set of admissible synchronous prisoner's dilemma games X and a set of admissible asynchronous prisoner's dilemma games Y in which there is a cooperative sequential equilibrium and the existence of a cooperative equilibrium depends on the degree of uncertainty the player has about the last round. Particularly, in these finitely iterated prisoner's dilemma games, players are privately informed of the number of iterations and have a publicly known upper bound of the number of iterations. Another interesting observation about this setting is that a higher level of uncertainty (which corresponds to the value of the upper bound on the player's maximum rounds played U) means that the utilities can take on a wider range of values without compromising the existence of a cooperative equilibrium.

5.2 Significance to Secret Sharing

The secret sharing protocols described in Chapter 3 are viable secret sharing protocols. This means that, in both the asynchronous and the synchronous secret sharing protocols, rational players will choose to share their piece of the secret.

How does this solution to rational secret sharing differ from others? First of all, and most obviously it allows the protocol to be repeated in a situation where the secret expires over time and is regenerated. This can also be done with the protocol given by Halpern and Teauge in [3]. However the model in this paper offers a solution without the dealer having to deal the players a false share of the secret with some

probability. The protocol in maleka offers a solution with this quality as well, but assumes quite strongly that neither player has any idea of when the last round will be. Meaning that each agent doesn't even know how many rounds of secret sharing they themselves will participate in. However, in our protocol agents know how the maximum number of rounds they are willing to participate in. This is more practical because agents will know how many secrets they themselves would like to share.

The model given by Samuelson in "A note on uncertainty and cooperation in a finitely repeated prisoner's dilemma" could be used in order to build a synchronous iterated secret sharing protocol where each player is privately informed about the number of secrets that are being shared. Player A knows how many secrets he himself would like to share and Player B knows how many secrets he himself would like to share. The practical perspective of this is that each player has a unique length of interest in the information being encrypted by the keys that are being shared. Once the information is no longer valuable to them, the key becomes worthless and the player will not continue to participate in the secret sharing protocol. The players assume that there is some probability P in which for each round n, the opposing player will cooperate for at least one round. For example, the players might believe that there is a 50 percent chance that the opposing player is interested in sharing at least one more key. Using the model given in this thesis to represent secret sharing would have a similar flavor as using Samuelson's. What sets our protocol apart is that the possible number of secrets being shared is upper bounded by some value known to all players.

The most general result in terms of secret sharing of this paper is that incorporating uncertainty into the model can circumvent the impossibility result of Halpern and Teague in [3]. There are many different ways of doing so. In some cases you can hardcode this uncertainty in by dealing false shares of the secret as done in [2]. Using the game theoretic conclusion above you can assume that players have some level of uncertainty about the number of rounds. I.e the players know how many secrets they would like to share but only know an upper bound of how many secrets their opponent would like to share. This type of uncertainty is also enough to encourage cooperation and make for a viable secret sharing protocol (both synchronous and asynchronous).

5.3 Future Work

For future work the goal would be to further relax the probabilistic assumptions. In this work, the assumption is that the probability distribution for each player's "last round belief" is uniform. This assumption might be too strong. We might be able to show the relationship between the entropy of the distribution and the existence of a cooperative equilibrium. The entropy could be included as a part of the player's uncertainty. Another possibility is to show for which probability distributions this doesn't work. For example, if the belief is highly concentrated to the earlier rounds being the last round, will this encourage defection, whereas if the belief is highly concentrated to the later rounds being the last round, will this encourage cooperation? Considering the result given previously that the larger the upper bound on the possible final rounds, the easier it is to encourage cooperation (the more values the utilities can take on), it might also make sense that if it is more likely that the opposing player's last round is later (rather than uniform), then it is easier to encourage cooperation.

Bibliography

[1] Larry Samuelson George J. Mailath. *Repeated Games and Reputations: Long-Run Relationships*. Oxford University Press, 2006.

[2] S.Dov Gordon and Jonathan Katz. Rational secret sharing, revisited. In Roberto De Prisco and Moti Yung, editors, *Security and Cryptography for Networks*, volume 4116 of *Lecture Notes in Computer Science*, pages 229–241. Springer Berlin Heidelberg, 2006.

[3] Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation: Extended abstract. In *Proceedings of the Thirty-sixth Annual ACM Symposium on Theory of Computing*, STOC '04, pages 623–632, New York, NY, USA, 2004. ACM.

[4] David M. Kreps and Robert Wilson. Reputation and imperfect information. *Journal of Economic Theory*, 27(2):253–279, 1982.

[5] Kevin Leyton-Brown and Yoav Shoham. *Essentials of Game Theory*. Morgan Claypool Publishers, 2008.

[6] Shaik Maleka, Amjed Shareef, and C.Pandu Rangan. Rational secret sharing with repeated games. In Liqun Chen, Yi Mu, and Willy Susilo, editors, *Information Security Practice and Experience*, volume 4991 of *Lecture Notes in Computer Science*, pages 334–346. Springer Berlin Heidelberg, 2008.

[7] Mehrdad Nojoumian and Douglas R. Stinson. Socio-rational secret sharing as a new direction in rational cryptography. Cryptology ePrint Archive, Report 2011/370, 2011. http://eprint.iacr.org/.

[8] L. Samuelson. A note on uncertainty and cooperation in a finitely repeated prisoner's dilemma. *International Journal of Game Theory*, 16(3):187–195, 1987.

[9] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[10] Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82, pages 160–164, Washington, DC, USA, 1982. IEEE Computer Society.