Rational broadcast

1 Notes

27/Mar/2024
Attendees: Girisha, Shreyas, Bhavana, Chaya, Sujit, Varul

1. Start with modelling the broadcast with incentives for the sender.
2. Initially assume synchronous setting for communication model.
3. Come up with definition for the broadcast which is independent of the underlying comm model.
4. Is Censorship inherent with all rational parties?
5. Proposal: Positive utility for agreement and bit higher utility for their own value being agreed upon.
6. Single-peaked preferences: Value that party wants agreed upon is its highest utility. As moved away from the peak, the utility decreases.
7. Approximate Agreement: definitions and the robust midpoint protocol
8. Shreyas to present: `https://groups.csail.mit.edu/tds/papers/Lynch/jacm86.pdf`
9. Overleaf project to be created

2 Approximate agreement

Model: Each party starts with an arbitrary real number → wants to agree on approximate value.
Assumption:

- each party can send/receive arbitrary real values
- can store arbitrary real values

Definition 1. *For any $\epsilon > 0$, approximate agreement protocol satisfies the following:*

- ***Agreement:*** *all honest parties, after a finite rounds, output values that are within ϵ of each other*
- ***Validity:*** *Every honest party outputs a value that is within the range of the values honest parties started with.*

Note that the definition implies regular consensus if all honest parties start with the same value.

Some results in the paper:

- **Synchronous:** (each message arrives before a maximum time τ) authors guarantee convergence if $n > 3t$ ($t < n/3$)
- **Asynchronous:** In this setting, exact agreement is impossible in a protocol that is guarantees termination (can be achieved if it terminates w.p. 1 (?)). For approximate agreement, termination can be guaranteed depending on ϵ (for every $\epsilon > 0$) in the case $t < n/5$.

2.1 Protocol overview

- every party starts with a value v_i (in the current round)
- receives a set of values V from other parties
- computes an approximation function f on the set of all values in current round ($f(V)$)
- sets the output in last step as the input for the next round

Note that the function f should take care of t-malicious parties and f should guarantee fast convergence. Authors prove that the f used by them achieves fastest convergence.

2.2 Properties of the approximation function f

Let $P_1, P_2, \ldots, P_m$ be the set of parties starting with values $v_1, v_2, \ldots, v_m$ respectively. Let $u_0 \leq u_1 \leq \ldots \leq u_{m-1}$ be an ordering of the set of values. Let $U = \{u_0, \ldots, u_{m-1}\}$. Let

- $reduce(U) = \{u_1, \ldots, u_{m-2}\}$
- $select_k(U) = \{u_0, u_k, u_{2k}, \ldots\}$. $|select_k(U)| = \left[\frac{m-1}{k}\right] + 1 = c(m.k)$
- $mean(U) = \frac{\Sigma_i u_i}{m}$

From above functions, a function $f_{k,t}$ is dedfined as follows:

$$f_{k,t}(U) = mean(select_k(reduce^t(U))) \tag{1}$$

whenever $|U| > 2t$

Then, $f = f_{t,t}$ in synchronous setting and $f = f_{2t,t}$ in asynchronous setting for asynchronous setting.

2.3 Problems with this setting

The approximate agreement protocol already assumes an underlying broadcast protocol, in the step where each party sends their value in current round to every other party. But in our setting of no honest parties, this assumption can not be made. In this sense, approximate broadcast only relaxes the conditions for agreement but does not help us get to a definition of rational broadcast. We can use such relaxation to approximate on top of a definition in rational setting but it seems the definition can not take much from this setting. Therefore, we independently try to define rational broadcast (consensus) next.

3 Defining rational broadcast

The regular broadcast assumes a set of honest parties and a set of corrupt parties (controlled by central adversary) and defines broadcast as successful if set of all honest parties outputs same value. Since, in the regular setting there is an honest set of parties, defining broadcast is easy. In our setting where all parties are rational (and perhaps act for their individual gain but may collude), we need to have an alternative for this honest set of parties. Hence we define rational broadcast as follows:

Definition 2. *Let, Π, be a protocol between n-parties, $P_1, P_2, \ldots, P_n$. Let P_1 be denoted as 'sender', and start with an input v. Π is called a rational broadcast if it partitions the set of parties into classes $C_1, C_2, \ldots, C_k$, such that:*

1. *if a player $P_a \in C_i$, then P_a outputs (v_i, C_i), where v_i was sent by P_1 to at least one party in C_i*
2. *if every party is rational, then $|C_i| = 0, \forall i > 1$ and $v_1 = v$ (subject to relaxation based on utilities).*

Note that the first point in definition, we do not demand rationality. We want to achieve it with just cryptography. But since a malicious party can always output a random value independent of Π, we would treat the 'output' as contained in the view of the party and output can be same as that depending on the utility of the party.

3.1 rational consensus

Definition 3. *Let Π be a protocol between n-parties $P_1, \ldots, P_n$. Every party P_i starts with an input v_i. Π is a rational consensus protocol if it partitions the set of parties into k classes, $C_1, \ldots, C_k$ such that:*

1. *if $P_a \in C_i$, then P_a outputs (u_i, C_i), such that at least one party $P_b \in C_i$ had the input $v_b = u_i$*
2. *if every party is rational, then $|C_i| = 0, \forall i > 1$.*

3.2 On equivalence of rational broadcast and rational consensus

In the regular setting, broadcast and consensus are equivalent in honest majority setting ($t < n/3$?). But are they equivalent in rational setting too? Composition of protocols has always been a problem in rational setting. Even if we guarantee that rational parties do not cheat inside a rationally secure protocol, how do we guarantee that these parties even provide correct protocol to begin with? A broadcast protocol can be thought to be constructed from a consensus protocol, in rational setting, as follows:

1. P_1 sends v_i to P_i
2. P_i gives the input v_i to a consensus protocol.
3. parties run a consensus on what P_1 sent.

Note that Even if we ensure step 1 and 3 are correct, consensus only implies broadcast if parties are honest in step 2. This step needs an additional mechanism to ensure parties are honest with their inputs to consensus protocol (may be a digital signature?) Therefore, Consensus only implies broadcast with an added assumption of such a mechanism. Therefore, consensus implies broadcast only with such an added assumption and in general can not be thought of as equivalent.

3.3 Construction of rational broadcast

1. (assumption): All parties have a public key associated with every other party (same as authenticated channel?)
2. P_1 sends $(v_i, \sigma_1(v_i))$ to party P_i
3. Every P_i sends $(v_i, \sigma_1(v_i), \sigma_i(v_i))$ to every other party P_j
4. Continue till the set of signatures received is same as the last round
5. output $(v_i, \{k | P_i \text{ received } \sigma_k(v_i) \text{ and } \sigma_k(v_i), \sigma_1(v_i) \text{ verifies}\})$

3.4 Correctness of construction

We need to prove that the construction partitions the set of parties and each class outputs the same value and class.

Lemma 1. *If $P_a, P_b \in C_i$, then their output is same.*

Lemma 2. *$\exists P_a \in C_i$ such that $\forall P_b \in C_i$, output is v_a.*

Lemma 3. *If $P_a \in C_i$ and $P_a \in C_j$, then $i = j$.*

4 Utility agnostic Broadcast

In this approach, we try to achieve broadcast in the presence of Rational Players agnostic to their utility function. Towards this, we relax the definition of security in the Rational setting.

4.1 Threat Model

Consider $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ players. Each player wants to agree on (broadcast) some value (which gives them the highest utility out of all the outcomes). These are k distinct values $\mathbf{v} = \{v_1, v_2, \ldots, v_k\}$ and set $\mathcal{C} = \{C_1, C_2, \ldots C_k\}$ for $k \leq n$. P_i has highest valuation for agreement on v_j then $P_i \in C_j$. Wlog, we assume the sender/leader for a particular round is P_1, and correctness is when all players agree on v_a such that $P_1 \in C_a$.

Definition 4 (Weak Rational Broadcast)**.** *A protocol* Π *is said to achieve weak rational broadcast if*

- ***Validity*** *If sender* P_1 *broadcasts* v_a *then all players output* v_a

- ***Agreement*** *The protocol terminates in finite rounds.*

The threat model is $\langle \mathcal{P}, \mathcal{C}, \mathbf{v}, \mathbf{U}, U_{max} \rangle$ where sets $\mathcal{P}, \mathcal{C}, \mathbf{v}$ are as defined above and $\mathbf{U} = \{U_1, U_2, \ldots, U_n\}$ is the set of utility function of each player and $U_max \geq U_i$ for all values taken by U_i for all $i \in [1, n]$.

Definition 5 ($t-$Nash Secure)**.** *A protocol* Π *is Nash Secure against threat model* $\langle \mathcal{P}, \mathcal{C}, \mathbf{v}, \mathbf{U}, U_{max} \rangle$ *such that for any* $\mathcal{S} \subseteq \mathcal{P}$ *such that* $|\mathcal{S}| \geq |\mathcal{P}| - t$ *following* Π *is Nash-Equilibrium irrespective of strategy followed by* $\mathcal{P}/\mathcal{S}$*.*

4.2 Accountable Consensus protocols

To be filled after literature review. For now, assuming Accountable Byzantine Consensus Π_{ABC} achieves agreement for $t < n/2$ faults and in case of deviation, outputs $\frac{n}{3}$ deviating players.

4.3 Results

Note that our results are agnostic to utility functions given that (1) there is some desired value v_a for each player where she achieves maximum utility[1] and (2) U_{max} is known.

1 Π_{ABC} achieves $t-$Nash Secure BA/BB for $t < \frac{n}{2}$.

  a for $t < \frac{n}{3}$ is trivially satisfied through existing BA/BB protocols.

  b for $\frac{n}{3} \geq t < \frac{n}{2}$ is satisfied through Π_{ABC}

[1] this v_a can also be unknown to us

2 Π_{ABC} achieves $t-$Nash Secure BA/BB for $t < n$ if $|C_a| > \frac{|\mathcal{P}|}{2}$ for $P_1 \in C_a$. This also follows through simple observation that any deviating player should belong to $C_b \neq C_a$ and hence, can form a collusion of size $< \frac{|\mathcal{P}|}{2}$. In this scenario, the case is similar to (1).

3 $t-$Nash Secure BA/BB for $\frac{n}{2} < t < n$ is still open for $|C_a| < \frac{|\mathcal{P}|}{2}$.