Verification of PBAR systems

Dileepa Fernando

July 6, 2017

Abstract

A Proofs

In general, given a set of Byzantine players $Z \subset [n]$, a global state s, the pay-off of i playing the game for k steps should be as follows.

$$v_i'^k(Z,s) = \begin{cases} \text{if } \mathbf{k > 0 \wedge i \notin Z} \\ max_{\pi_i'^a \in \Pi_{t=0}^{k-1} A_i}(min_{\pi_Z'^a \in \Pi_{t=0}^{k-1} A_Z}\{E_{\pi'^a_{[n]-Z-\{i\}} \in \Pi_{t=0}^{k-1} A_{[n]-Z-\{i\}}} \\ \qquad (\Sigma_{t=0}^{k-1}\beta_i^t H_i(\pi'^s(t), \pi'^a(t)))| \\ BT(Z\cup\{i\}, \pi'^s(t), \pi'^a(t), \pi'^s(t+1)) \wedge \pi'^s(0) = s \wedge |\pi'| = k\}) \\ \text{if } \mathbf{k > 0 \wedge i \in Z} \\ max_{\pi_i'^a \in \Pi_{t=0}^{k-1} A_i} min_{\pi'^a_{[Z]-\{i\}} \in \Pi_{t=0}^{k-1} A_{[Z]-\{i\}}}\{\{E_{\pi'^a_{[n]-Z} \in \Pi_{t=0}^{k-1} A_{[n]-Z}} \\ \qquad (\Sigma_{t=0}^{k-1}\beta_i^t H_i(\pi'^s(t), \pi'^a(t)))| \\ BT(Z, \pi'^s(t), \pi'^a(t), \pi'^s(t+1)) \wedge \pi'^s(0) = s \wedge |\pi'| = k\}\} \\ \text{if } \mathbf{k = 0} \\ 0 \end{cases}$$

where π' is a path of length k.

In the case of $k > 0 \wedge i \notin Z$, $\pi'^s(t)$ is the state at position t in the path π' and $\pi'^a(t)$ is the action at position t in the path π'. Hence, $H_i(\pi'^s(t), \pi'^a(t))$ defines the pay-off of i on the transition at position t. The pay-offs of length k is the sum of each position, with every pay-off weighted with discount factor β_i^t, i.e., $\Sigma_{t=0}^{k-1}\beta_i^t H_i(\pi'^s(t), \pi'^a(t))$. Note that given a choice, we have a tree, containing a set of paths. For each path in the tree, calculation of the pay-off of the path is as above. The expected pay-off of the tree can be calculated using these pay-offs, by considering the probabilities in each path. This process is denoted by $E_{\pi'^a_{[n]-Z-\{i\}} \in \Pi_{t=0}^{k-1} A_{[n]-Z-\{i\}}}$. The possible trees are grouped by the rational players' choices of non-deterministic actions, i.e., for one choice, there are a set of trees due to that there may be different choices for Byzantine players. For each set/group of trees, we choose the tree that minimised the expected pay-off, denoted by $min_{\pi_Z'^a \in \Pi_{t=0}^{k-1} A_Z}$, because we assume that the Byzantine players try to minimise i's pay-offs. Now in each group (i.e., for a choice of the rational player), there is only the minimised tree, and each group has exactly one choice of non-deterministic actions of i. We choose the one which gives the maximum expected pay-off, denoted by $max_{\pi_i'^a \in \Pi_{t=0}^{k-1} A_i}$, meaning that the rational player i always makes the choice that gives the maximised pay-off. In addition, we ensure that each transition in each path is valid $(BT(Z\cup\{i\}, \pi'^s(t), \pi'^a(t), \pi'^s(t+1)))$, the initial state of each path is s and the length of each path is k. Hence, in summary, the formula captures the intuitive calculate of i's pay-off in length k starting from s w.r.t. $Z \cup \{i\}$.

If $k > 0 \wedge i \in Z$, since $i \in Z$, the set of altruistic and Byzantine players differ from the set of altruistic and Byzantine players in the case of $i \notin Z$, that is, in the case of $i \notin Z$, i can be altruistic or rational, whereas in the case of $i \in Z$, i can be Byzantine or rational. Hence, the grouping of trees due to the rational players' choices is different in these two cases. Therefore, in the case of $i \in Z$, the process of calculating the expected pay-off of trees is denoted differently as $E_{\pi'^{a}_{[n]-Z} \in \Pi_{t=0}^{k-1} A_{[n]-Z}}$. The second difference is in the BT functions. Since $i \in Z$, we do not need to additionally add i to Z to capture the rational behaviour of i. If $k = 0$, we initialise the pay-off as 0.

Similarly, we define the correct pay-off for $u_i^{'k}(Z, s)$ as follows:

$$u_i^{'k}(Z,s) = \begin{cases} \text{if } \mathbf{k} > \mathbf{0} \wedge \mathbf{i} \notin \mathbf{Z} \\ E_{a_i \in A_i}\big(min_{a_Z \in A_Z}\{ \\ E_{a_{[n]-Z-\{i\}} \in A_{a_{[n]-Z-\{i\}}}}(\Sigma_{t=0}^{k-1} \beta_i^t H_i(\pi'^s(t), \pi'^a(t)))| \\ BT(Z, \pi'^s(t), \pi'^a(t), \pi'^s(t+1)) \wedge \pi'^s(0) = s \wedge |\pi'| = k\}) \\ \text{if } \mathbf{k} > \mathbf{0} \wedge \mathbf{i} \in \mathbf{Z} \\ min_{a_i \in A_i}\{min_{a_{Z-\{i\}} \in A_{Z-\{i\}}}\{ \\ E_{a_{[n]-Z} \in A_{[n]-Z}}(\Sigma_{t=0}^{k-1} \beta_i^t H_i(\pi'^s(t), \pi'^a(t)))| \\ BT(Z, \pi'^s(t), \pi'^a(t), \pi'^s(t+1)) \wedge \pi'^s(0) = s \wedge |\pi'| = k\}) \end{cases}$$

A.1 Correctness of the dynamic programming definition

$$v_i^{'k}(Z,s) = \begin{cases} \text{if } \mathbf{k} > \mathbf{0} \wedge \mathbf{i} \in \mathbf{Z} \\ max_{\pi_i'^a \in \Pi_{t=0}^{k-1} A_i} min_{\pi'^a_{[Z]-\{i\}} \in \Pi_{t=0}^{k-1} A_{[Z]-\{i\}}} \{\{E_{\pi'^a_{[n]-Z} \in \Pi_{t=0}^{k-1} A_{[n]-Z}} \\ \qquad (\Sigma_{t=0}^{k-1} \beta_i^t h_i(\pi'^s(t), \pi'^a(t)))| \\ BT(Z, \pi'^s(t), \pi'^a(t), \pi'^s(t+1)) \wedge \pi'^s(0) = s \wedge |\pi'| = k\}\} \\ \text{if } \mathbf{k} > \mathbf{0} \wedge \mathbf{i} \notin \mathbf{Z} \\ E_{\pi_i'^a \in \Pi_{t=0}^{k-1} A_i}(min_{\pi'^a_Z \in \Pi_{t=0}^{k-1} A_Z}\{E_{\pi'^a_{[n]-Z-\{i\}} \in \Pi_{t=0}^{k-1} A_{[n]-Z-\{i\}}} \\ \qquad (\Sigma_{t=0}^{k-1} \beta_i^t h_i(\pi'^s(t), \pi'^a(t)))| \\ BT(Z, \pi'^s(t), \pi'^a(t), \pi'^s(t+1)) \wedge \pi'^s(0) = s \wedge |\pi'| = k\}) \\ \text{if } \mathbf{k} = \mathbf{0} \\ 0 \end{cases}$$

For recall,

Theorem 1 *$v_i^{'k}(Z,s) = v_i^k(Z,s)$ and $u_i^{'k}(Z,s) = u_i^k(Z,s)$, $\forall k \geq 0$.*

Proof 1 *For $k = 0$, the result is trivial because value of empty path is defined to be 0. So the maximin path value is 0. Substitute the original function value $v_i^{'k}(Z,s)$ to compute $v_i^{k+1}(Z,s)$ in the dynamic programming definition. Let $i \in Z$, any path of length k th iteration be π and let $\{\pi\}$ be any infinite length probabilistic path starting from state s.*

$$
\begin{aligned}
&E_{a_{[n]-Z}\in A_{[n]-Z}}(h(s,\langle a_i,a_{-i}\rangle)+\beta_i v_i^k(Z,s')|BT(Z,s,\langle a_i,a_{-i}\rangle,s'))\\
&=E_{a_{[n]-Z}\in A_{[n]-Z}}(h(s,\langle a_i,a_{-i}\rangle)+\beta_i E_{\pi^a\in\Pi_{t=0}^{k-1}A_{[n]-Z}}(\Sigma_{t=0}^{k-1}\beta_i^t h_i(\pi^s(t),\pi^a(t))|\\
&\qquad BT(Z,s,\langle a_i,a_{-i}\rangle,s')))\\
&=E_{a_{[n]-Z}\in A_{[n]-Z}}(h(s,\langle a_i,a_{-i}\rangle))+E_{A_{[n]-Z}}(E_{\pi'^a\in\Pi_{t=1}^{k}A_{[n]-Z}}(\\
&\qquad \Sigma_{t=1}^{k}\beta_i^t h_i(\pi'^s(t),\pi'^a(t))|BT(Z,s,\langle a_i,a_{-i}\rangle,s')))\\
&=E_{\pi'^a\in\Pi_{t=0}^{k}A_{[n]-Z}}(h(s,\langle a_i,a_{-i}\rangle))+E_{\pi'^a\in\Pi_{t=0}^{k}A_{[n]-Z}}(\Sigma_{t=1}^{k}\beta_i^t h_i(\pi'^s(t),\pi'^a(t))|\\
&\qquad BT(Z,s,\langle a_i,a_{-i}\rangle,s'))\\
&=E_{\pi'^a\in\Pi_{t=0}^{k}A_{[n]-Z}}(\Sigma_{t=0}^{k}\beta_i^t h_i(\pi'^s(t),\pi'^a(t))|BT(Z,s,\langle a_i,a_{-i}\rangle,s'))
\end{aligned}
\tag{1}
$$

The maximin value would be:

$$
\begin{aligned}
v_i' k(Z,s)=&\, max_{\pi_i'^a\in\Pi_{t=0}^{k}A_i} min_{\pi_{[Z]-\{i\}}'^a\in\Pi_{t=0}^{k}A_{[Z]-\{i\}}}\\
&E_{\pi'^a\in\Pi_{t=0}^{k}A_{[n]-Z}}(\Sigma_{t=0}^{k}\beta_i^t h_i(\pi'^s(t),\pi'^a(t))|BT(Z,s,\langle a_i,a_{-i}\rangle,s'))
\end{aligned}
\tag{2}
$$

When $\{\pi\}$ is the path set corresponding to optimal expected value for length k, $\{\pi'\}$ would be the path set $s\langle a_i,a_{-i}\rangle\pi\in\Pi_{t=0}^{k}A_{[n]-Z}$. Suppose we choose a different path set from s' other than $v_i^k(s',Z)$ if does not correspond to the maximum expected value over player i among the guaranteed values, we can miss a max value path set in general. The proof is similar for $u_i^k(Z,s)$.

A.2 Correctness of Arbitrary Precision Nash Equilibria Verification[?]

Proposition 1 Though this result is not directly used in the proof of Theorem **??**, we take advantage of this subsection to explain how one can prove it. Indeed, Proposition 1 relies on the same Lemmas than the ones used for the proof of Theorem **??**. For recall,

Proposition 1 *1.* $\lim_{k\to\infty} v_i^k(Z,s)=v_i(Z,s)$

2. $\lim_{k\to\infty} u_i^k(Z,s)=u_i(Z,s)$

Lemma 1 *1.* $\forall k\in\mathbb{N}, |v_i(\{\pi\})-v_i(\{\pi|_k\})|\le e_i(k)$.

2. $\lim_{k\to\infty} v_i(\{\pi|_k\})=v_i(\{\pi\})$.

Lemma 2 *Let $\{\pi\}$ be a probabilistic path set s.t. $v_i(\{\pi\})$ is minimum in* $\mathsf{Path}(s,Z,i,\sigma)$*, let $\{\{\bar\pi_k\}\}_{k\in\mathbb{N}}$ be a sequence of finite path, s.t. $\forall k$, $v_i(\{\bar\pi_k\})$ is minimum in* $\mathsf{Path}_k(s,Z,i,\sigma)$*, then $v_i(\{\pi|_k\})-v_i(\{\bar\pi_k\})\le 2e_i(k)$.*

Lemma 3 *$\forall s\in S$ and strategy σ we have:*
$\lim_{k\to\infty} v_i^k(Z,s,\sigma|_k)=v_i(Z,s,\sigma)$.

Lemma 4 *$\forall s \in S$ and $\forall k \in \mathbb{N}$, we have:*
$|v_i^k(Z,s) - v_i(Z,s)| < E_i(k)$.

Lemma 5 *$\forall s \in S$ and $\forall k \in \mathbb{N}$, we have:*
$|u_i^k(Z,s) - u_i(Z,s)| < E_i(k)$.

As written in the paper, apart Lemma 1, Lemmas 2 to 5, as well as the proposition, are very similar from the results established in [**?**]. For that reason, we do not reproduce their proof here and we refer to the text and [**?**] for more details. Proof of Lemma 1 is given below.

We now present the proof of Theorem **??**. For recall,

Theorem 2 *Let $\mathcal{G} = (S, s_0, A, T, P, H, \beta)$ be an n player game, $\epsilon > 0$ and $\delta > 0$ and $Z \subset [n]$ be the set of Byzantine players, for each player $i \in [n]$ let*

1. $M_i = max\{|h_i(s,a)| | s \in S \text{ and } a \in A\}$
2. $E_i(k) = 5\beta_i^k \frac{M_i}{1-\beta_i}$
3. $\Delta_i(k) = max\{v_i^k(Z \cup \{i\}, \mathsf{f}(s)) - u_i^k(Z,s) | s \in O\}$
4. $\epsilon_1(i,k) = \Delta_i(k) - 2E_i(k)$
5. $\epsilon_2(i,k) = \Delta_i(k) + 2E_i(k)$,

and let k_i be the minimum numbers of steps such that $4E_i(k_i) < \delta$,

1. *if $\forall i \in [n]$, $\epsilon \geq \epsilon_2(i,k_i) > 0$ then $\mathcal{M}_{|gz}$ is ϵ-Nash-equilibrium,*
2. *if $\exists i \in [n]$, $0 < \epsilon \leq \epsilon_1(i,k_i)$ then $\mathcal{M}_{|gz}$ is not ϵ-Nash-equilibrium,*
3. *if $\forall i \in [n]$, $\epsilon_1(i,k_i) < \epsilon$ and $\exists j \in [n]$ s.t. $\epsilon < \epsilon_2(j,k_j)$ then $\mathcal{M}_{|gz}$ is $(\epsilon + \delta)$-Nash-equilibrium.*

Proof 2 *In order to prove the convergence of the value function, we want to bound the value difference by a more convenient function. For that purpose, we define $e_i(k) = \beta_i^k \frac{M_i}{1-\beta_i}$ and prove Lemma 1.*

Lemma 1 1. $\forall k \in \mathbb{N}, |v_i(\{\pi\}) - v_i(\{\pi|_k\})| \leq e_i(k)$.

2. $\lim_{k\to\infty} v_i(\{\pi|_k\}) = v_i(\{\pi\})$

Proof 3 1. $|v_i(\{\pi|_T\}) - v_i(\{\pi|_k\})| =$

$$|E_{\pi'^a \in \Pi_{t=0}^{k-1} A_{[n]-Z}}(\Sigma_{t=0}^{k-1}\beta_i^t h_i(\pi^s(t), \pi^a(t))) - E_{\pi''^a \in \Pi_{t=0}^{k-1} A_{[n]-Z}\Pi_{t=k}^{T} A_{[n]-Z}}(\Sigma_{t=0}^{T}\beta_i^t h_i(\pi''^s(t), \pi''^a(t)))|$$
$$= |E_{\pi''^a \in \Pi_{t=0}^{k-1} A_{[n]-Z}\Pi_{t=k}^{T} A_{[n]-Z}}(\Sigma_{t=0}^{k-1}\beta_i^t h_i(\pi^s(t), \pi^a(t))) - E_{\pi''^a \in \Pi_{t=0}^{k-1} A_{[n]-Z}\Pi_{t=k}^{T} A_{[n]-Z}}(\Sigma_{t=0}^{T}\beta_i^t h_i(\pi''^s(t), \pi''^a(t)))|$$
$$= |E_{\pi''^a \in \Pi_{t=0}^{k-1} A_{[n]-Z}\Pi_{t=k}^{T} A_{[n]-Z}}(\Sigma_{t=k}^{T}\beta_i^t h_i(\pi''^s(t), \pi''^a(t)))|$$

$\leq |\Sigma_{t=k}^{T} E_{\pi''^a \in \Pi_{t=0}^{k-1} A_{[n]-Z} \Pi_{t=k}^{T} A_{[n]-Z}} (\beta_i^t h_i(\pi''^s(t), \pi''^a(t)))|$ *(Linearity of Expectation)*
$\leq \Sigma_{t=k}^{T} |E_{\pi''^a \in \Pi_{t=0}^{k-1} A_{[n]-Z} \Pi_{t=k}^{T} A_{[n]-Z}} (\beta_i^t h_i(\pi''^s(t), \pi''^a(t)))|$ *(Triangle inequality)*
$\leq \beta_i^k \frac{M_i}{1-\beta_i}$ *(By the choice of* M_i *and* $\lim_{T\to\infty}$*)*
$\leq e_i(k)$

2. $\lim_{k\to\infty} e_i(k) = 0$,
   $\lim_{k\to\infty} |v_i(\{\pi\}) - v_i(\{\pi|_k\})| = 0$ *(by comparison test)*
   $\lim_{k\to\infty} v_i(\{\pi|_k\}) = v_i(\{\pi\})$.

Now we have all the intermediate results to prove Theorem **??**. *By Lemma* **??** *and* **??**, *we have:* $\forall s \in S$, $|v_i^k(Z,s) - v_i(Z,s)| < E_i(k)$ *and* $|u_i^k(Z,s) - u_i(Z,s)| < E_i(k)$. *This implies:*
$v_i(Z \cup \{i\}, s) \leq v_i^k(Z \cup \{i\}, s) + E_i(k)$ *by Lemma* **??**
$v_i(Z \cup \{i\}, s) \geq v_i^k(Z \cup \{i\}, s) - E_i(k)$ *by Lemma* **??**
$u_i(Z, s) \leq u_i^k(Z, s) + E_i(k)$ *by Lemma* **??**
$u_i(Z, s) \geq u_i^k(Z, s) - E_i(k)$ *by Lemma* **??**

Now, we can prove the three following statements:

1. *Using Lemma* **??** *and Lemma* **??**,
   $v_i(Z \cup \{i\}, s) - u_i(Z, s) \leq v_i^k(Z \cup \{i\}, s) + E_i(k) - (u_i^k(Z, s) - E_i(k))$
   $= v_i^k(Z \cup \{i\}, s) - u_i^k(Z, s) + 2E_i(k)$
   $\leq \Delta_i(k) + 2E_i(k)$
   if $\epsilon \geq \epsilon_2(i,k)$ *then* $\Delta_i(k) \leq \epsilon - 2E_i(k)$
   So, $\forall s \in I$,
   $v_i(Z \cup \{i\}, s) - u_i(Z, s) \leq \epsilon$
   M *is* $\epsilon - Nash$.

2. *Similarly,* **??** *and* **??** *can be used to prove*
   $v_i(Z \cup \{i\}, s) - u_i(Z, s) \geq v_i^k(Z \cup \{i\}, s) - E_i(k) - (u_i^k(Z, s) + E_i(k))$
   $= v_i^k(Z \cup \{i\}, s) - u_i^k(Z, s) - 2E_i(k)$
   if $\epsilon \leq \epsilon_1(i,k)$ *then* $\Delta_i(k) \geq \epsilon + 2E_i(k)$
   This implies $\exists Z \in P([n] - \{i\})$ *and* $s \in I$ *s.t.*
   $v_i(Z \cup \{i\}, s) - u_i(Z, s) \geq \epsilon$
   M *is not* $\epsilon - Nash$.

3. *if* $\forall i$, $\epsilon_1(i, k_i) < \epsilon$ *and for some* $j, \epsilon < \epsilon_2(j, k_j)$,
   it is not possible to decide whether M *is* $\epsilon - Nash$. *But, since* $\epsilon_2(j,k_j) - \epsilon_1(i,k_i) = 4E_i(k_i)$ *and* $4E_i(k_i) < \delta$, *we have,*
   $\forall i \in [n]$, $\epsilon + \delta > \epsilon_2(i, k_i)$. *According to the first statement, we have* $(\epsilon + \delta) - Nash$.