A simple proof of the $\Omega(\sqrt{n})$ space lower bound for Consensus

Leqi Zhu

Abstract

The proof that at least $\Omega(\sqrt{n})$ registers are needed for any obstruction-free algorithm, where every process decides after taking a finite number of consecutive, uninterrupted steps, solving $n$-process consensus [4] is notorious for its difficulty. We present a simple proof of this result.

A configuration $C$ is $(P,Q)$-bivalent for disjoint sets of processes $P$ and $Q$ if, each process in $P \cup Q$ is poised to write to a register, all processes in $P$ are poised to write to different registers, all processes in $Q$ are poised to write to different registers, and, for some $v \in \{0,1\}$, $C \beta_P$ is $v$-deciding for $P$ while $C \beta_Q$ is $\bar{v}$-deciding for $Q$, where $\beta_P$ and $\beta_Q$ are the block writes by $P$ and $Q$, respectively.

Lemma 1. Suppose that $X,Y_1,\ldots,Y_\ell$ are pairwise disjoint sets of processes and $C$ is a $(X,Y_i)$-bivalent configuration for each $i \in \{1,\ldots,\ell\}$. Suppose that $C \beta_X$ is $v$-deciding for $P$ and $C \beta_{Y_i}$ is $\bar{v}$-deciding for $Y_i$, for each $j \in \{1,\ldots,\ell\}$, for some $v \in \{0,1\}$, where $\beta_X$ and $\beta_{Y_i}$ are the block writes by $X$ and $Y_i$. Then there is a configuration $C'$ reachable from $C$ by a $P$-only execution, a process $p \in X$, and $i \in \{1,\ldots,\ell\}$ such that:

- $p$ is poised to perform a write $\beta_p$ to a register not covered by $Y_i$,
- $C' \beta_p \beta_{Y_i}$ is $v$-univalent for $Y_i$, and
- $C' \beta_{Y_j}$ is $\bar{v}$-deciding for $Y_j$, for all $j \in \{1,\ldots,\ell\}$.

Proof. Let $\alpha$ be a $X$-only execution from $C$ which decides $v$ (this exists since $C \beta_X$ is $v$-deciding for $X$), and let $\alpha'$ be the longest prefix of $\alpha$ such that $C \alpha' \beta_{Y_i}$ is $v$-deciding for all $j \in \{1,\ldots,\ell\}$. Let $\beta_p$ be the next step in $\alpha$ after $\alpha'$, which is by some process $p \in X$. It follows that $C \alpha' \beta_p$ is $v$-valent for $Q_i$, for some $i \in \{1,\ldots,\ell\}$ and $\beta_p$ is a write to a register not covered by $Q_i$. \hfill \Box

Lemma 2. Suppose that, for every configuration $C$ bivalent for a set $U$ of processes with $|U| \geq d$, it is possible to reach, via a $U$-only execution, a $(P,Q)$-bivalent configuration $C'$ with $\min\{|P|,|Q|\} = k$. Then, for every configuration $C$ bivalent for a set $U'$ of processes with $|U'| \geq d + k$, it is possible to reach, via a $U'$-only execution, a $(P',Q')$-bivalent configuration $C'$ with $\min\{|P'|,|Q'|\} = k$ and $\max\{|P'|,|Q'|\} = k + 1$.

Proof. Let $C$ be any configuration which is bivalent for a set $U'$ of processes with $|U'| \geq d + k$. Since $|U'| \geq d + k > d$, it is possible to reach a $(P,Q)$-bivalent configuration $C'$ with $\min\{|P|,|Q|\} = k$. If $\max\{|P|,|Q|\} \geq k + 1$, then we are done. Suppose now that $\max\{|P|,|Q|\} = k$. Without loss of generality, we may assume that $C'$ is bivalent for $U' - Q$. Since $|Q| = k$, $|U' - Q| \geq d$. It follows that we may reach a $(P',Q')$-bivalent configuration $C''$ from $C'$ via a $(U' - Q)$-only execution with $\min\{|P'|,|Q'|\} = k$. If $\max\{|P'|,|Q'|\} \geq k + 1$, then we are done. Suppose now that $\max\{|P'|,|Q'|\} = k$. Without loss of generality, we may assume that $C'' \beta_P$ is $v$-deciding for $P$ and $C'' \beta_Q$ is $\bar{v}$-deciding for $Q$ and $Q'$. The claim now follows by Lemma 1 with $C = C''$, $X = P$, $Y_1 = Q$, and $Y_2 = Q'$. \hfill \Box

Lemma 3. Suppose that, for every configuration $C$ bivalent for a set $U$ of processes with $|U| \geq d$, it is possible to reach, via a $U$-only execution, a $(P,Q)$-bivalent configuration $C'$ with $\min\{|P|,|Q|\} = k$. Then, for every configuration $C$ bivalent for a set $U'$ of processes with $|U'| \geq d + 2k + 1$, it is possible to reach, via a $U'$-only execution, a $(P',Q')$-bivalent configuration $C'$ with $\min\{|P'|,|Q'|\} = k + 1$.

Proof. Let $C$ be any configuration which is bivalent for a set $U'$ of processes with $|U'| \geq d + 2k + 1$. Since $|U'| \geq d + 2k + 1 > d + k$, it is possible to reach a $(P,Q)$-bivalent configuration $C'$ with $\min\{|P|,|Q|\} = k$ and $\max\{|P|,|Q|\} = k + 1$. Without loss of generality, we may assume that $C'$ is bivalent for $U' - Q$.\hfill \Box
Since \(|U' - Q| \geq |U'| - \max\{|P|, |Q|\} \geq d + k\), it is possible to reach, via a \((U' - Q)\)-only execution, a \((P', Q')\)-bivalent configuration \(C''\) in which \(\min\{|P'|, |Q'|\} = k\) and \(\max\{|P'|, |Q'|\} = k + 1\). Without loss of generality, we may assume that \(|Q'| = k + 1\). There are two cases to consider.

Case 1: \(C''\) is bivalent for \(U' - Q'\). Since \(|U' - Q'| \geq d + k\), by the same argument as before, it is possible to reach, via a \((U' - Q')\)-only execution, a \((P'', Q'')\)-bivalent configuration \(C'''\) in which \(\min\{|P''|, |Q''|\} = k\) and \(\max\{|P''|, |Q''|\} = k + 1\). Without loss of generality, we may assume that \(|Q''| = k + 1\). If \(C'''\) \(\beta_{Q'}\) is \(\nu\)-deciding for \(Q'\) and \(C'''\) \(\alpha_{Q''}\) is \(\pi\)-deciding for \(Q''\), then we are done. Otherwise, we are done by Lemma 1 with \(C = C'''\), \(X = P'', Y_1 = Q''\), and \(Y_2 = Q''\).

Case 2: \(C''\) is univalent for \(U' - Q'\). Since \(Q\) and \(P'\) are disjoint and \(C''\) is univalent for \(Q \cup P' \subseteq U' - Q'\), we may assume that \(Q\) and \(P'\) both cover the same \(k\) registers. By Lemma 1 with \(C = C''\), \(X = Q', Y_1 = Q\), and \(Y_2 = P'\) we can reach, via a \(Q'\)-only execution, a configuration \(C''\) which is, without loss of generality, \((P' \cup \{p\}, Q)\)-bivalent, for some \(p \in Q'\). If \(C''\) is bivalent for \(U' - (P' \cup \{p\})\), then we are done by Case 1. Otherwise, \(C''\) is univalent for \(U' - (P' \cup \{p\})\). Since \(|U' - (P' \cup Q \cup \{p\})| \geq d\), we can find a process \(z \in U' - (P' \cup Q \cup \{p\})\). Run \(z\) until it is poised to write a register not covered by \(P' \cup \{p\}\). Since \(C''\) is univalent for \(Q \cup \{z\}\), the resulting configuration is \((P' \cup \{p\}, Q \cup \{z\})\)-bivalent.

**Lemma 4.** Suppose \(C\) is a configuration which is bivalent for a set of processes \(P\) with \(|P| \geq 2\). Then exists \(p, q \in P\) such that there is a \((\{p\}, \{q\})\)-bivalent configuration which is reachable from \(C\) via a \(P\)-only execution.

**Proof.** Let \(C\) be the set of all bivalent configurations reachable from \(C\) via a \(P\)-only history. Among the configurations in \(C\), let \(k\) be the smallest integer such that there is a configuration \(C' \in C\) which is bivalent for a subset \(P'\) of \(P\) with \(|P'| = k\). Let \(P'\) be any subset of \(P\) of size \(k - 1\). If \(P' = \emptyset\), then there is a configuration \(C' \in C\) which is bivalent for a single process \(p\). Let \(q\) be any other process in \(P\). It follows that \(C'\) is a \((\{p\}, \{q\})\)-bivalent configuration. Suppose now that \(P' \neq \emptyset\). Let \(p \in P - P'\). Suppose \(C\) is \(\nu\)-univalent for \(P'\) and \(\pi\)-deciding for \(p\), for some \(v \in \{0, 1\}\). Then \(C\) is a \((\{p\}, \{q\})\)-bivalent configuration for any process \(q \in P'\). Suppose now that \(C\) is \(\nu\)-univalent for \(P'\) and \(p\), for some \(v \in \{0, 1\}\). Since \(C\) is bivalent for \(P\), there is a \(P\)-only execution \(\alpha\) which decides \(\pi\). Let \(\alpha'\) be the longest prefix of \(\alpha\) such that \(C\alpha'\) is \(\nu\)-univalent for \(P'\) and \(p\). Note that \(\alpha' \neq \alpha\) since \(\pi\) is decided in \(\alpha\). Let \(\delta\) be the next step in \(\alpha\) after \(\alpha'\). It follows that \(C\alpha'\delta\) is \(\pi\)-deciding for \(P'\) or \(p\). If \(\delta\) is by a process in \(P'\), then \(C\alpha'\delta\) is \(\nu\)-univalent for \(P'\) since \(C\alpha'\) is \(\nu\)-univalent for \(P'\), so \(C\alpha'\delta\) is \(\pi\)-deciding for \(p\). Otherwise, \(C\alpha'\delta\) is \(\nu\)-univalent for \(p\), since \(C\alpha'\) is \(\nu\)-univalent for \(p\), and thus, by definition of \(\alpha\), \(C\alpha'\delta\) is \(\pi\)-univalent for \(P'\). Picking any process \(q \in P'\), it follows that \(C\alpha'\delta\) is a \((\{p\}, \{q\})\)-bivalent configuration.

**Theorem 1.** Any consensus algorithm using \(r\) register supports at most \(r^2 + r\) processes.

**Proof.** By Lemma 4, for every configuration \(C\) bivalent for a set \(U\) of processes with \(|U| \geq 2\), it is possible to reach, via a \(U\)-only execution, a \((P, Q)\)-bivalent configuration \(C'\) with \(\min\{|P|, |Q|\} = 1\). Combining this with Lemma 3, the number of processes \(T(k)\) needed to obtain a \((P, Q)\)-bivalent configuration with \(\min\{|P|, |Q|\} = k\) satisfies:

\[
T(k) = \begin{cases} 
T(k-1) + 2k - 1 & k > 1 \\
2 & k = 1 
\end{cases}
\]

Thus, \(T(k) = k^2 + 1\). If the system has \(r\) registers, then it is not possible to construct a \((P, Q)\)-bivalent configuration with \(\max\{|P|, |Q|\} = r + 1\). It takes \(r^2 + 1\) processes to construct a \((P, Q)\)-bivalent configuration with \(\min\{|P|, |Q|\} = r\). By Lemma 3, another \(r\) processes are required to reach a \((P', Q')\)-bivalent configuration with \(\max\{|P'|, |Q'|\} = r + 1\). Thus, the system has at most \(r^2 + r\) processes.

**References**