Correctness proofs for renaming

December 20, 2012

The proofs provided herein are taken from the book "Distributed Computing", by Hagit Attiya and Jennifer Welch, with minor changes.

1 The wait-free algorithm

Lemma 1 No two processes decide on the same name.

Proof: To obtain a contradiction, assume that two processes \( p_i \) and \( p_j \) decide on the same name \( y \). Consider the \texttt{scan} operations they perform in line 4 of their last iteration of the while loop and assume WLOG that the \texttt{scan} operation by \( p_j \) is linearized after that of \( p_i \). Then, from the code and from the linearizability of the snapshot algorithm, \( p_j \) sees \( y \) as \( p_i \)'s suggested value, hence it cannot decide on \( y \).

Lemma 2 The new names are in the range \([1 \ldots 2n - 1]\).

Proof: The rank of a process is at most \( n \). Since a process sees at most \( n - 1 \) values as suggested by other processes, the claim follows.

Lemma 3 Any non-faulty process decides on a name after some finite number of steps.
Proof: To obtain a contradiction, assume the algorithm has an execution $E$ in which some process takes an infinite number of steps and does not decide. We say that such a process is trying. Let $E = E_1E'$ such that, in $E_1$, all trying processes have already updated their value at least once in line 3 and all non-trying processes have either decided or fail-stopped. Let $p_i$ be the trying process with the smallest original name. We prove that $p_i$ decides in $E'$, which is a contradiction.

Let $NF$ ("not free") be the set of suggested names that appear in the snapshot object in the beginning of $E'$ in the segments of non-trying processes. These names will remain taken all throughout $E'$. Let $F = [1 \ldots 2n - 1] \setminus NF$, and assume $F = \{z_1, z_2, \ldots\}$, where $z_1 < z_2 < \cdots$.

Let $E''$ be a suffix of $E'$ in the beginning of which all trying processes have already written a suggestion in line 3 based on a view they received from a scan they have started in $E'$. Since no process performs line 3 for the first time in $E'$, it follows that all these views contain the same set of original names. Hence, each process gets a unique rank in line 6. Let $r$ be the rank of $p_i$’s original name in this view. Then $r$ is the smallest rank among all trying processes.

Consider a trying process $p_j \neq p_i$. When $p_j$ performs a scan in $E'$, it sees every name in $NF$ in use and possibly also some additional suggested names from $F$. Since $p_j$’s rank is bigger than $r$, it follows that, in $E'$, $p_j$ can only suggest names that are bigger than $z_r$. It follows that, in the view returned by the first complete scan performed by $p_i$ in $E''$, none of the names $z_1, \ldots, z_r$ is suggested. Hence $p_i$ eventually decides on $z_r$ in $E''$, a contradiction. ■