A SIMPLE PROOF OF A THEOREM ON SELF-SYNCHRONIZING AUTOMATA

Dale M. Landi

July 1966

P-3242-1

A SIMPLE PROOF OF A THEOREM ON SELF-SYNCHRONIZING AUTOMATA

Dale M. Landi*

The RAND Corporation, Santa Monica, California

A short proof is offered for verifying that a finite state, completely specified automation is synchronized with probability 1 only if there exists a universal synchronizer for the automation.

---

*Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The RAND Corporation as a courtesy to members of its staff.

A SIMPLE PROOF OF A THEOREM ON SELF-SYNCHRONIZING AUTOMATA

WINOGRAD[3] has shown that a finite state, completely specified automaton will resynchronize itself with probability 1 if and only if there exists a finite sequence of input letters called a universal synchronizer of the automaton. The result is fundamental[1,2] and, as WINOGRAD's proof is unnecessarily long and circuitous, we offer a constructive argument that is more direct.

Following[3], let I* represent the free semigroup with identity generated by a finite input alphabet I, i.e., $I^* = I^0 \cup I^1 \cup \ldots \cup I^k \cup \ldots$, where I^k is the set of all input sequences of length k and $I^0 = \phi$, the identity element. A finite state, completely specified automaton A is a mapping from I* onto some finite output alphabet; the set of states of A, $S = \{s_1, s_2, \ldots, s_M\}$, is finite with state transitions defined on all pairs of the cartesian product $S \times I^*$ by $f(s_m, w) = s_n$, where f is the state transition function, s_m and s_n are in S, and w is in I*. Successive input letters to A are assumed to occur randomly and independently according to some discrete probability law $Pr(I) = \{p_i\}$, with p_i the probability of occurrence of the i^{th} input letter ($p_i > 0$). A subset $E = \{(w_i, w_i')\}$ of $I^* \times I^*$ is called an error set and subsets $C^k_{s_m,(w_i,w_i')}$ of I* are defined by

$$C^k_{s_m,(w_i,w_i')} = \{w \in I^k \mid f(s_m, w_i w) = f(s_m, w_i' w)\},$$

i.e., $C^k_{s_m,(w_i,w_i')}$ is the set of all input sequences w with length k that will synchronize A after an error $w_i \to w_i'$ occurs while A is in state s_m.

An automaton A with input distribution Pr(I) is synchronized with probability 1 with respect to an error set E if and only if for all s_m in S and all (w_i,w_i') in E

$$\lim_{k\to\infty} \Pr\{C^k_{s_m,(w_i,w_i')}\} = 1,$$

where

$$\Pr\{C^k_{s_m,(w_i,w_i')}\} = \sum_{w\in C^k_{s_m,(w_i,w_i')}} \Pr(w) .$$

It will be convenient to extend E to a larger set $\mathcal{E} = EI^*$, i.e., (v_i,v_i') is in $\mathcal{E}$ if and only if there exists a (w_i,w_i') in E and w in I^* such that $(v_i,v_i') = (w_i,w_i')w = (w_iw, w_i'w)$.

A sequence u in I^* is a universal synchronizer of A with respect to E if and only if for all s_m in S and all (v_i,v_i') in $\mathcal{E}$, $f(s_m,v_iu) = f(s_m,v_i'u)$.

<u>THEOREM</u>. A finite state, completely specified automaton A with input distribution Pr(I) is synchronized with probability 1 with respect to an error set E only if and only if there exists a universal synchronizer of A with respect to E.

The first portion of the proof is straightforward and is included here as it appears in Ref. 3 for the sake of completeness.

<u>Proof</u>. If u is a universal synchronizer of A with respect to E and if u has length m and Pr(u) = p, then the probability that u is not a factor of a sequence w with length km is less than or equal to $(1-p)^k$. Hence for all $s \in S$ and all $(w_i,w_i') \in E$,

$$\lim_{k\to\infty} \Pr\left\{C^{km}_{s,(w_i,w_i')}\right\} \geq \lim_{k\to\infty}\left[1 - (1-p)^k\right] = 1.$$

Now, assuming A is synchronized with probability 1, partition $S\times\mathcal{E}$ into $N=1+M(M-1)/2$ equivalence classes,

$$w_t = \{(s_m,v_i,v_i')\epsilon S\times\mathcal{E}\,|\,f(s_m,v_i) = s_\mu,\ f(s_m,v_i') = s_\nu,\ \mu \neq \nu\},$$

one for each unordered, asymmetric pair of states, and one for the remaining triples

$$w_0 = \{(s_m,v_i,v_i')\epsilon S\times\mathcal{E}\,|\,f(s_m,v_i) = f(s_m,v_i')\},\ (t=0,1,\ldots,N).$$

Distinct elements (s_m,v_i,v_i') and (s_n,v_j,v_j') of the same set w_t are indistinguishable with respect to the synchronizing process in that any sequence x in I* that synchronizes A after the error (v_i,v_i') occurs in state s_m also synchronizes A after (v_j,v_j') occurs in state s_n. Since A is synchronized with probability 1, there is at least one synchronizing sequence for every non-empty W_t, call it u_t.

In the remainder of the proof (s_t,v_t,v_t') will be used to denote a representative element of W_t. Construct sequences $z_1, z_2,\ldots, z_N$ as follows:

$$z_0 = u_0 = \phi$$

and

$$z_t = z_{t-1}x_t,\ (t=1,2,\ldots,N),$$

where

$$x_t = \phi \quad \text{if } f(s_t, v_t z_{t-1}) = f(s_t, v_t' z_{t-1}),$$

or

$$x_t = u_{n_i} \quad \text{if } f(s_t, v_t z_{t-1}) \neq f(s_t, v_t' z_{t-1})$$

and

$$(s_t, v_t z_{t-1}, v_t' z_{t-1}) \epsilon W_{n_i} \quad (1 \leq n_i \leq N).$$

Then, $f(s_j, v_j z_t) = f(s_j, v_j' z_t)$ for $j \leq t$, and it follows that $u = z_N$ is a universal synchronizer of A.

REFERENCES

1. Gilbert, E. N., and E. F. Moore, "Variable Length Binary Encodings," Bell Systems Tech. J., Vol. 38, 1959, pp. 933-967.
2. Schutzenberger, M. P., "On the Synchronizing Properties of Certain Prefix Codes," Information and Control, Vol. 7, No. 1, March 1964, pp. 23-26.
3. Winograd, S., Input Error Limiting Automata, IBM Research Report, RC-966, 1963 (also, J. ACM, Vol. 11, 1964, pp. 338-351).