AN ABSTRACT OF THE THESIS OF

Paul Arthur Kinion for the degree of Master of Science

in Mathematics presented on May 6, 1982

Title: Uniform Hamiltonian Touring Sequences

Redacted for Privacy

Abstract approved: ____________________

Paul Cull

Sequential machines uniquely determine directed graphs. A path in a sequential machine may be specified by a starting state and an input sequence. A uniform Hamiltonian touring sequence (UHTS) is an input sequence that specifies a Hamiltonian path regardless of the starting state. We present a polynomial time algorithm that determines the existence of a UHTS for a linear sequential machine (LSM) defined over the prime field Z_p.

The problem of whether or not a general graph contains a Hamiltonian path is known to be NP-complete. If we restrict ourselves to directed graphs defined by LSM's then there is a Hamiltonian path if and only if the digraph is strongly connected. This condition is polynomial time testable by determining the rank of the controllability matrix. We show that strong connectedness is not sufficient to guarantee the existence of a UHTS.

Uniform Hamiltonian Touring Sequences

by

Paul A. Kinion

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Master of Science

Completed May 6, 1982

Commencement June 1982

APPROVED

Redacted for Privacy

Professor of Mathematics in charge of major

Redacted for Privacy

Head of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

Date thesis is presented May 6, 1982

Typed by Jane A. Tuor for Paul Arthur Kinion

To Youn Su

ACKNOWLEDGEMENTS

They were the best of times, they were the worst of times. They were the times I got together with Paul Cull to work on this thesis. Without Paul's endless supply of ideas and encouragement, these times, would still be those times. Thank you Paul.

Thank you also to the typist, Jane Tuor. She was given a difficult task and did a fine job.

There are three other people in my life to whom I owe a great deal. Thank you Mom, thank you Dad, and thank you Sis for all your love and support.

TABLE OF CONTENTS

LIST OF DIAGRAMS

UNIFORM HAMILTONIAN TOURING SEQUENCES

I. INTRODUCTION AND DEFINITIONS

Many problems about graphs are hard. No known algorithm for solving any of these problems has polynomial running time. For example, does a given digraph have a path visiting each vertex exactly once. The existence of such a path, called a Hamiltonian path, is a hard problem [see Garey and Johnson p. 199]. Often when a general problem is restricted to special cases, there are polynomial time algorithms. We shall restrict the Hamiltonian path problem by considering a special class of graphs and imposing a "uniform" condition on the paths. We will display a polynomial time algorithm which solves this restricted problem.

In a natural way, a sequential machine defines a digraph. A sequential machine, with a state set X and an input set Y, is defined by a next state function $F: X\times Y\to X$ according to the formula $x_{i+1}= F(x_i,y_i)$. That is F maps the present state and input to the next state. The vertex set for the corresponding digraph is X and there is an edge from x to x' if and only if there is a $y \in Y$ such that $x' = F(x,y)$. A tour through a digraph is a path that visits all vertices at least once. If a digraph defined by the sequential machine F has a tour, it may be specified by a starting state x_0 and an input sequence. Such a sequence is called a touring sequence for x_0. Suppose we start the machine in a state other than x_0 and apply a touring sequence for x_0. In general we no longer have a tour. If an input sequence is a touring sequence for all states in X, we call it a uniform touring sequence (UTS). A UTS must have at least N-1 elements where N is the number of states in X. A UTS with exactly N-1 elements will cause the machine to visit each state exactly once regardless of the starting state. For this reason we call a UTS of length N-1 a uniform Hamiltonian touring sequence (UHTS).

We extend our notion of the next state function in order to describe the action of a machine on an input sequence. Let Y^* denote the set of all finite sequences of elements from the input set Y. The function $\eta\colon X\times Y^*\to X$ is defined recursively by $\eta(x,\{\}) = x$ and

$$\eta(x,\{y\}_{i=0}^{m}) = F(\eta(x,\{y\}_{i=0}^{m-1},y_m)).$$

A linear sequential machine (LSM) defines its next state function by

$$\begin{aligned}(x,\{y\}_{i=0}^{m}) &= A^{m+1}x + A^{m}By_0 + A^{m-1}By_1 + \dots + By_m\\ &= A^{m+1}x + (0,\{y\}_{i=0}^{m}) \text{ where}\end{aligned}$$

A and B are n dimensional matrices defined over the field Z_p. We denote a LSM by the pair [A,B]. The state set X and the input set Y are both the n dimensional vector space whose scalar field is Z_p. Note that there are $N=p^n$

different states. We shall address the problem of determining the existence of UHTS for a LSM and show this problem is polynomial time solvable. That is, the problem may be solved by an algorithm whose running time is bounded by a polynomial in n, the dimension of the state space.

We will use algebraic techniques to determine necessary and sufficient condtions for a LSM to have a UHTS. If a machine has a UHTS we can define an operation *, so that the state set X under * forms a group. In this case, X has a normal subgroup S_0 which allows us to define a "standard form" for the matrix A. This form is used to reduce the number of relevant cases to four.

Strong connectedness is a significant condition to consider when determinig the existence of a UHTS. A set $S \subset X$ is strongly connected by F if and only if for each pair x, $x' \epsilon$ S, there exists an input sequence $\{y\}_{i=0}^{m}$ such that $x' = \eta(x,\{y\}_{i=0}^{m})$ and each intermediate state is in S. In the case where S = X we say F is strongly connected.

Related to strong connectednes is the notion of controllability. If every pair of states in X has a connecting input sequence of the same length, K, F is called K-controllable. A machine is controllable if it is K-controllable for some K. When F = [A,B] we define the controllability matrix to be the n by n^2 matrix $[B \vdots AB \vdots \ldots \vdots A^{n-1}B]$.

II. PRELIMINARY RESULTS

Our first two theorems provide several alternate characterizations of strong connectedness. They are central to many of the arguments proving the correctness of our algorithm. In particular Theorem 2 provides the key to actually constructing a UHTS provided one exists. We conclude this section with two simple results concerning machines that have UHTS's.

Theorem 1: Let [A,B] be a finite state linear sequential machine. Then the following are equivalent.

i) [A,B] is strongly connected.

ii) [A,B] has a UTS.

iii) [A,B] is controllable.

and iv) rank $[B \vdots AB \vdots A^2B \vdots \ldots \vdots A^{n-1}B] = n$

[The equivalence of i, iii, and iv were taken from Cohn].

Proof: i) <=> ii) Clearly if [A,B] has a UTS then [A,B] is strongly connected.

Assume [A,B] is strongly connected. Then for each state $x \in X$, there is an input sequence $T(x)$ such that when [A,B] is started in x and fed $T(x)$, each state is visited at least once. Pick some arbitrary state, say x_1. We will construct the UTS by starting with $T(x_1)$. Pick any other state say x_2. Either $T(x_1)$ causes a complete tour or not. If it does, go on to another state. If it doesn't add $T(\eta(x_2,T(x_1))$ to our UTS. Continue in this manner until all possible starting states are taken care of.

i) <=> iii) if [A,B] is controllable then clearly [A,B] is strongly connected.

Assume [A,B] is strongly connected. Let $\ell(i,j)$ denote the length of the shortest input sequence that takes state i to state j. Since [A,B] is strongly connected, ℓ is defined for every pair of states. Set $L' = \max_{i \varepsilon X} \ell(i,0)$ and $L'' = \max_{j \varepsilon X} \ell(0,j)$. We claim [A,B] is L-controllable where $L = L' + L''$. This follows since a transition from any state i to any other state j can be made via the 0 state. At this point $L - \ell(i,0) - \ell(0,j)$ zero inputs can be introduced to pad out the sequence.

iii) <=> iv) Assume rank $[B \vdots AB \vdots \cdots \vdots A^{n-1}B] = n$. Then for any pair x, $x' \varepsilon X$ there is a vector u such that $x' - A^n x = [B \vdots AB \vdots \cdots \vdots A^{n-1}B]u$.

Let $\begin{pmatrix} y_n \\ y_{n-1} \\ \vdots \\ y_1 \end{pmatrix} = u$. Now $x' - A^n x = [B \vdots AB \vdots \cdots \vdots A^{n-1}B] \begin{pmatrix} y_n \\ y_{n-1} \\ \vdots \\ y_1 \end{pmatrix}$

so $x' - A^n x = A^{n-1}By_1 + By_2 + \cdots + By_n$

$= \eta\ (0, \{y\}_{i=1}^{n})$

and $x' = \eta(x, \{y\}_{i=1}^{n})$. Hence [A,B] is n-controllable.

Assume [A,B] is K-controllable for some integer K. Reversing the previous construction we see that rank $[B \vdots AB \vdots \cdots \vdots A^{K-1}B] = n$. Note that $[B \vdots AB \vdots \cdots \vdots A^{n-1}B] < n$ then for some i<n, rank $[B \vdots AB \vdots \cdots \vdots A^{i-1}B]$ = rank $[B \vdots AB \vdots \cdots \vdots A^{i}B]$. The columns of A^iB can be expressed as linear combinations

of columns in $[B \vdots AB \vdots \cdots \vdots A^{i-1}B]$. Thus $A^{i+1}B$ adds no new linearly independent columns to $[B \vdots AB \vdots \cdots \vdots A^{i}B]$. Continuing in this manner shows

rank $[B \vdots AB \vdots \cdots \vdots A^{i-1}B]$ = rank $[B \vdots AB \vdots \cdots \vdots A^{j}B] < n$ for all $j \geqslant i$. Hence rank $[B \vdots AB \vdots \cdots \vdots A^{K-1}B] = n$ implies rank $[B \vdots AB \vdots \cdots \vdots A^{n-1}B] = n$. ■

The fact that every UHTS is also a UTS gives us the following result.

Corollary 1.1: If a LSM has a UHTS then it is strongly connected.

Theorem 2 [Cull 1980]: A LSM [A,B] is strongly connected if and only if it has a directed Hamiltonain circuit.

Proof: If [A,B] has a directed Hamiltonian circuit then obviously [A,B] is strongly connected. Assume [A,B] is strongly connected. We will demonstrate a permutation on the state set X. From the associated cycles a Hamiltonian circuit can be constructed.

For every $x \in X$, define the successor set $S(x) = \{Ax + By | y \in X\}$. That is S(x) is the set of all states reachable from x in one step. Clearly $S(0) = R(B)$, the range of B, and $S(x) = Ax + R(B)$. Since [A,B] is strongly connected every element is in some successor set. Hence X is partitioned by equal sized successor sets, i.e. the cosets of R(B). Note that distinct successor sets do not overlap. That is if $S(x_1) \cap S(x_2)$ is nonempty then

$S(x_1) = S(x_2)$.

Define $\equiv$ to be the equivalence relation where $x_1 \equiv x_2$ if and only if $S(x_1) = S(x_2)$. Let $E(x)$ denote the equivalence class containing x. We want to show that for all $x \in X$, $|E(x)| = |E(0)|$ where $||$ denotes the number of elements in a set.

Let $q \in E(0)$. Since $0 \in S(0) = S(q)$, there is a y such that $Aq + By = 0$. Hence $Ax = A(x + q) + By \in S(x) \cap S(x + q)$ so $S(x) = S(x + q)$. That is $x \equiv x + q$ for all $q \in E(0)$. This shows that $|E(x)| \geqslant |E(0)|$.

Similarly assume $q' \in E(x)$. Then there is a y' with $Aq' + By' = Ax$. Now $A(x - q') + By = 0$ is in both $S(0)$ and $S(x = q')$. So $0 \equiv x - q'$ for all $q' \in E(x)$ implies $|E(0)| \geqslant |E(x)|$.

We have shown that X is partitioned into equal sized equivalence classes, say $E(x_1), E(x_2), \ldots, E(x_r)$. Note that $S(E(x_i)) = \bigcup_{x \in E(x_i)} S(x) = S(x_i)$. We claim $S(x_1), S(x_2), \ldots,$ $S(x_r)$ also partition X. This is clear since every state is reachable from some equivalence class. Consequently $|E(x_i)| = |S(0)| = |R(B)|$.

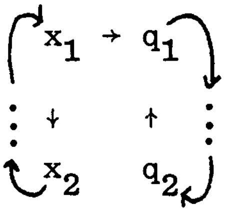
Let $\phi_i: E(x_i) \rightarrow R(B)$ be any bijection. We define a permutation $\pi: X \rightarrow X$ by $\pi(x) = Ax_i + \phi_i(x)$ where $x \in E(x_i)$. Note that $x \in E(x_i)$ if and only if $\pi(x) \in S(x_i)$ since the range of ϕ_i is $R(B)$.

Each x is contained in one and only one equivalence class so π is well defined.

To show π is one to one assume $\pi(x) = \pi(x')$. We have noted $x \equiv x'$ so for some i, $Ax_i + \phi_i(x) = Ax_i + \phi_i(x')$. Since ϕ_i is a bijection, $x = x'$.

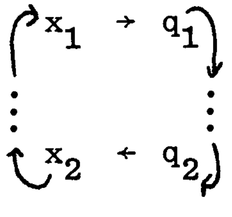
Now π is a one to one mapping over a finite set so π is a permutation on X. Furthermore π decomposes into a set of disjoint cycles. If there is one cycle it is a Hamiltonian circuit. Otherwise cycles may be joined together in the following manner to form the desired circuit.

Since [A,B] is strongly connected, there is a path from one cycle to another. Suppose $q_1 \varepsilon S(x_1)$ as shown.



Since q_1 is also in $S(q_2)$ then $S(x_1) = S(q_2)$. Hence $x_2 \varepsilon S(x_1)$ implies x_2 is a successor of q_2.

We may now form the larger cycle shown here.



Clearly we may continue joining cycles until a Hamiltonian circuit is constructed. ■

Our primary applications of Theorem 2 are the following two corollaries. Under certain conditions a strongly connected subspace will have a Hamiltonian circuit.

Corollary 2.1: Suppose the subspace S is strongly connected by the machine [A,B]. If S is invariant, i.e. if $Ar \varepsilon S$ for all $r \varepsilon S$, then S has a Hamiltonian circuit.

Proof: Since S is strongly connected there is a tour of S starting at 0. That is an input sequence $\{t\}_{i=0}^{j}$ exists giving

$$S = \{0, Bt_0, ABt_0+Bt_1, A^jBt_0 + \dots + Bt_j\}$$

where repetitions may occur. Since S is an invariant subspace $Bt_i \varepsilon S$ for $i = 0,1,\dots,j$.

Assume the dimension of S is m and that $r_1, r_2, \dots, r_m$ is a basis for S. Let Y denote the set of all m tuples over Z_p. Define the isomorphism $\phi: S \rightarrow Y$ by $\phi(\alpha_1 r_1 + \alpha_2 r_2 + \dots + \alpha_m r_m) = (\alpha_1, \alpha_2, \dots, \alpha_m)^T$.

Let $\tilde{A}$ be the matrix whose i^{th} column is $\phi(Ar_i)$. Let $\tilde{B}$ be any m by m matrix whose range is the vector space $\phi((R)(B) \cap S))$. Now $[\tilde{A},\tilde{B}]$ is a strongly connected LSM. By Theorem 2 it has a Hamiltonian circuit. Applying ϕ^{-1} to each state gives a corresponding circuit for S. ∎

Corollary 2.2: Suppose [A,B] is a LSM with an invariant strongly connected subspace S. Assume $z \varepsilon S$ with $Az = z \neq 0$. Let $w_1, w_2, \dots, w_\ell, z$ be a basis for S and define W to be the span of $w_1, w_2, \dots, w_\ell$. Then W has a Hamiltonian circuit mod z. That is there exists an input sequence causing the machine to generate $0 = u_1, u_2, \dots, u_L$, $L = p^\ell$, $u_i \varepsilon S$, the projection of $\{u_1, u_2, \dots, u_{L-1}\}$ onto

W is W, and u_L projects to 0. Specifically u_L is a multiple of z.

Proof: Let P: X→W be the projection map. We claim that for i = 1,2,..., $P(A^iu) = P(A^iP(u))$ when $u \in S$. To see this assume $u = \alpha_1w_1 + \ldots + \alpha_\ell w_\ell + \beta z$. Now

$$\begin{aligned} P(A^iu) &= P(\alpha_1A^iw_1 + \ldots + \alpha_\ell A^iw_\ell + \beta z) \\ &= P(\alpha_1A^iw_1 + \ldots + \alpha_\ell A^iw_\ell) \\ &= P(A^iP(u)). \end{aligned}$$

As in the proof of Corollary 2.1, let Y denote the set of all ℓ tuples over Z_p. Define the isomorphism ϕ: W→Y by $\phi(\alpha_1w_1 + \ldots + \alpha_\ell w_\ell) = (\alpha_1,\ldots,\alpha_\ell)^T$. Define $\tilde{A}$ to be the matrix whose i^{th} column is $\phi(P(AW_i))$. Let $\tilde{B}$ be any ℓ by ℓ matrix whose range is $\phi(P(R(B) \cap S))$.

We claim $\phi(P(A^iu)) = \tilde{A}^i\phi(P(u))$. Again suppose $u = \alpha_1w_1 + \ldots + \alpha_\ell w_\ell + \beta z$. Now

$$\phi(P(Au)) = \phi(P(\alpha_1Aw_1) + \ldots + P(\alpha_\ell AW_\ell)).$$

If $e_1, \ldots, e_\ell$ denotes the standard normal basis then

$$\begin{aligned} \phi(P(Au)) &= \alpha_1\tilde{A}e_1 + \ldots + \alpha_\ell\tilde{A}e_\ell \\ &= \tilde{A}\phi(P(u)). \end{aligned}$$

Note that $\phi(P(A^iu)) = \phi(P(A(A^{i-1}u))) = \tilde{A}\,\phi\,(P(A^{i-1}u))$. Continuing this process gives $\phi(P(A^iu)) = \tilde{A}^i\phi(P(u))$.

Since S is strongly connected it has a tour that starts and ends at 0. So there are inputs y_i such that $S = \{0, By_0, ABy_0 + By_1, \ldots, A^iBy_0 + \ldots + By_j = 0\}$. Now

$Y = \phi(W) = \phi(P(S))$

$= \{0,\phi(P(By_0)),\ \phi(P(ABy_0)) + \phi(P(By_1)),\dots,$

$\phi(P\ A^iBy_0)$ʒ $+ \dots + \phi(P(By_j)) = 0\}.$

Using our first claim,

$Y = \{0,\phi(P(By_0)),\phi(P(AP(By_0))) + \phi(P(By_1)),\dots,$

$\phi(P(A^iP(By_0))) + \dots + \phi(P(By_j)) = 0\}.$

Since $R(\tilde{B}) = \phi(P(R(B)\cap S))$ there are inputs $\tilde{y}_i$ such that $\widetilde{By}_i = \phi(P(By_i))$. This together with our second claim gives $Y = \{0,\widetilde{By}_0,\widetilde{ABy}_0 + \widetilde{By}_1,\dots,\tilde{A}^j\widetilde{By}_0 + \dots + \widetilde{By}_j = 0\}$. Now Y has a tour that starts and ends with 0 so $[\tilde{A},\tilde{B}]$ is strongly connected.

By Theorem 2, $[\tilde{A},\tilde{B}]$ has a Hamiltonian circuit. Let $\{\tilde{t}\}_{i-0}^{L-1}$ where $L = p^{\ell}$ be the associated input sequence. That is $Y = \{0,\widetilde{Bt}_0,\widetilde{ABt}_0 + \widetilde{Bt}_1,\dots,\tilde{A}^{L-1}\widetilde{Bt}_0 + \dots + \widetilde{Bt}_{L-1} = 0\}$. As before let t_i be such that $\phi(P(Bt_i)) = \widetilde{Bt}_i$ with $Bt_i \varepsilon S$. Following the same steps that proved the strong connectedness of $[\tilde{A},\tilde{B}]$ we can show

$\phi^{-1}(Y) = W = P\{0,Bt_0,ABt_0 + Bt_1,\dots,A^{L-1}Bt_0 + \dots + B^{t}{}_{L-1}\}$

and that the last state projects to 0 in W. Since $Bt_i \ \varepsilon\ S$ and S is invariant, all states within the brackets are in S. Hence we have constructed a Hamiltonian circuit mod z. ■

The following lemma provides an important restriction on the type of machine that can have a UHTS.

Lemma 3: Let [A,B] be a LSM with a UHTS. Then A is invertable and there is an integer $K > 0$ such that $A^K = I$.

Proof: Let $\{y\}_{m=0}^{N-2}$ be the UHTS and assume A is not invertable. Now there are distinct vectors x and x' with $Ax = Ax'$. Since the UHTS causes [A,B] to pass through each state regardless of the starting state,

$$X = \{x, Ax + By_0, A^2x + ABy_0 + By_1, \ldots, A^{N-1}x + A^{N-2}By_0 + \ldots + By_{N-2}\}$$

and

$$X = \{x', Ax' + By_0, A^2x' + ABy_0 + By_1, \ldots, A^{N-1}x' + A^{N-2}By_0 + \ldots By_{N-2}\}.$$

The intersection gives

$$X = \{Ax + By_0, A^2x + ABy_0 + By_1, \ldots, A^{N-1}x + A^{N-2}By_0 + \ldots + By_{N-2}\}$$

which contradicts the assumption that X has N elements so A is invertable.

Since there are only a finite number of possible n by n matrices over Z_p, there are a finite number of values for A^i, $i = 1,2,\ldots$. Hence there must be two different powers say i and j such that $A^i = A^j$ with $i > j$. Now $A^{i-j} = I$ where $i-j > 0$. ■

Lemma 4: The existence of a UHTS is preserved under a similarity transform.

Proof: Suppose [A,B] has a UHTS $\{y\}_{m=0}^{N-2}$ and that C is any nonsingular matrix. We claim $\{Cy\}_{m=0}^{N-2}$ is a UHTS for the machine $[CAC^{-1}, CBC^{-1}]$. Starting this machine with an arbitrary state x generates

$\{x, CAC^{-1}x + CBC^{-1}Cy_0, (CAC^{-1})^2x + (CAC^{-1})(CBC^{-1})Cy_0 +$
$CBC^{-1}Cy_1, \ldots, (CAC^{-1})^{N-1}x + (CAC^{-1})^{N-2}(CBC^{-1})Cy_0 + \ldots +$
$CBC^{-1}Cy_{N-2}\}$
$= C\ \{C^{-1}x, AC^{-1}x + By_0, A^2C^{-1}x + ABy_0 + By_1, \ldots, A^{N-1}C^{-1}x +$
$A^{N-2}By_0 + \ldots + By_{N-2}\}$

Since $C^{-1}x \varepsilon X$ and $\{y\}_{m=0}^{N-2}$ is a UHTS for [A,B] then we have generated all X states within the brackets. Now C is non-singular so $CX = X$ and our result is proved. ■

III THE GROUP STRUCTURE

When a machine has a UHTS we associate with each state a specific sequence. The next state function restricted to these sequences define the binary operation *. The state set together with * form a group. We formalize this idea in Theorem 5. It is interesting to note the existence of this group is both a necessary and sufficient condition for a sequential machine to have a UHTS.

Theorem 5 has several corollaries pertaining to properties of *, the matrix A, and the structure of the state set. In particular the UHTS defines a normal subgroup S_0 and a vector v in a natural way. The existence of S_0 and v are two conditions our algorithm tests for.

Theorem 5: The LSM [A,B] has a UHTS, $\{y\}_{m=o}^{N-2}$, if and only if X can be ordered by $x_i = \eta(0,\{y\}_{m=0}^{i-1})$ and (X,*) is a group with * defined by $x_i * x_j = A^j x_i + x_j$.

Note the correspondence between x_i and the sequence $\{y\}_{m=0}^{i-1}$.

Proof: Assume $\{y\}_{m=0}^{N-2}$ is a UHTS and set $x_i = \eta(0,\{y\}_{m=0}^{i-1}) = A^{i-1}By_0 + A^{i-2}By_1 + \ldots + By_{i-1}$.

Now all states are ordered and

$$\begin{aligned} x_i * x_j &= A^j x_i + x_j \\ &= A^j x_i + \eta(0,\{y\}_{m=0}^{j-1} \\ &= \eta(x_i,\{y\}_{m=0}^{j-1}). \end{aligned}$$

To show * is associative consider

$$\begin{aligned}(x_i * x_j)*x_k &= \eta(x_i * x_j,\{y\}_{m=0}^{k-1})\\ &= \eta(\eta(x_i,\{y\}_{m=0}^{j-1}),\{y\}_{m=0}^{k-1})\\ &= \eta(x_i,\{y_0,\ldots,y_{j-1},y_0,\ldots,y_{k-1}\})\\ &= x_i * \eta(0,\{y_0,\ldots,y_{j-1},y_0,\ldots,y_{k-1}\})\\ &= x_i * \eta(\eta(0,\{y\}_{m=0}^{j-1}),\{y\}_{m=0}^{k-1})\\ &= x_i * \eta(x_j,\{y\}_{m=0}^{k-1})\\ &= x_i * (x_j * x_k)\end{aligned}$$

The state $x_0 = 0$ is the identity. Clearly $x_i * x_0 = A^0 x_i + x_0 = x_i$ and $x_0 * x_i = A^i x_0 + x_i = x_i$.

To show that each state has an inverse let x_i be an arbitrary element of X. Since $\{y\}_{m=0}^{N-2}$ is a UHTS, all states must be visited when the machine is started at x_i. In particular 0 must be visited. Now there is an $r \leqslant N - 1$ such that $\eta(x_i,\{y\}_{m=0}^{r-1}) = 0$. So $x_i * x_r = 0$ making x_r the right inverse of x_i.

The existance of a left inverse of x_i arises from the claim that $x_j * x_i = x_k * x_i$ if and only if $x_j = x_k$. This is clear since A has full rank. Now $x_i \neq x_j$ implies $A^i x_j \neq A^i x_k$ so $A^i x_j + x_i = x_j * x_i \neq x_k * x_i = A^i x_k + x_i$. Because $x * x_i$ takes on a different value for each $x \in X$, there exists an $x_\ell \in X$ such that $x_\ell * x_i = 0$ making x_ℓ the left inverse of x_i.

We can easily see that $x_r = x_\ell$ by considering $(x_\ell * x_i) * x_r = x_\ell * (x_i * x_r)$. Now $0 * x_r = x_\ell * 0$ so $x_r = x_\ell$. Hence $(X,*)$ is a group.

To prove sufficiency assume X can be ordered by $x_i = \eta(0,\{y\}_{m=0}^{i-1})$ and (X,*) is a group with * defined as above. Let x be an arbitrary element of X. To demonstrate $\{y\}_{m=0}^{N-2}$ is a UHTS it suffices to show

$$\eta(x,\{y\}_{m=0}^{i-1}) = \eta(x,\{y\}_{m=0}^{j-1}) \text{ if and only if } i = j.$$

That is $x * x_i = x * x_j$ if and only if $i = j$. This is clear by multiplying on the left with the inverse of x. ■

For each corollary of Theorem 5 we hypothesize that the LSM [A,B] has the UHTS $\{y\}_{m=0}^{N-2}$ and that the state set is ordered as before. Recall from Lemma 3 that some power of A is the identity matrix. We denote the smallest positive power by K. That is $A^K = I$ and $A^i \neq I$ for $0 < i < K$.

Corollary 5.1: If $x_i * x_j = x_\ell$ the $\ell \equiv i + j \bmod K$.

Proof: Let x be any state in X. Now

$$\begin{aligned} x * (x_i * x_j) &= x * x_\ell \\ &= A^\ell x + x_\ell \\ &= A^\ell x + (x_i * x_j). \end{aligned}$$

Since * is associative this also equals

$$\begin{aligned} (x * x_i) * x_j &= A^j(x * x_i) + x_j \\ &= A^j(A^i x + x_i) + x_j \\ &= A^{i+j}x + A^j x_i + x_j \\ &= A^{i+j}x + (x_i * x_j). \end{aligned}$$

Hence $A^\ell x = A^{i+j}x$ for all $x \varepsilon X$ so $A^\ell = A^{i+j}$ giving $\ell \equiv i+j \bmod K$. ■

Definition 5.2: We construct the sets S_0, $S_1,\ldots,S_{K-1}$ so that each set contains every K^{th} element of X. That is

$$\begin{aligned}
S_0 &= \{x_0,x_K,\ldots,x_{sK},x_{sK+K}\} \\
S_1 &= \{x_1,x_{K+1},\ldots,x_{sK+1},x_{sK+K+1}\} \\
\vdots &\qquad\qquad\quad \vdots \\
S_r &= \{x_r,x_{K+r},\ldots,x_{sK+r},x_{N-1}\} \\
S_{r+1} &= \{x_{r+1},x_{K+r+1},\ldots x_{sK+r+1}\ \} \\
\vdots &\qquad\qquad\qquad \vdots \\
S_{K-1} &= \{x_{K-1},x_{2K-1},\ldots,x_{sK+K-1}\}.
\end{aligned}$$

We shall see in the next corollary that in fact each set contains the same number of states. However at this point we can only say $|S_i| \leqslant |S_0|$ for $0 \leqslant i < K$.

Corollary 5.3: S_0 is a normal subgroup of (X,*) and S_i is a coset for i = 1,2,..., K - 1.

Proof: Let x_{iK} and x_{jK} be elements of S_0. Suppose $x_\ell = x_{iK} * x_{jK}$ then $\ell = (iK + jK) \bmod K = 0$. Now ℓ is a multiple of K so $x_\ell \in S_0$. Hence S_0 is closed under *.

Let $x_j = x_{iK}^{-1}$. Now $x_j * x_{iK} = 0 = x_0$ so $(j + ik) \bmod K = 0$. This implies j is a multiple of K so $x_j \in S_0$. Therefore S_0 is a subgroup of (X,*).

Let $x_i * x_{jK}$ be an element of the left coset $x_i * S_0$ where $0 \leqslant i < K$. Suppose $x_\ell = x_i * x_{jK}$ then $\ell = (i + jK) \bmod K = i$. Hence there is a positive integer m such that $\ell = i + mK$ so $x_\ell \in S_i$. Now $x_i * S_0 \quad S_i$. We will show equality by an order argument. Clearly $|x_i * S_0| = |S_0|$ and we have just shown $|x_i * S_0| \leqslant |S_i|$.

Now $| S_0 | = | x_i * S_0 | \leqslant | S_i | \leqslant | S_0 |$ implies $| x_i * S_0 | = | S_i |$ so $x_i * S_0 = S_i$.

Similarly if we let $x_{jK} * x_i$ be an element of the right coset $S_0 * x_i$ where $0 \leqslant i < K$, we find that $S_0 * x_i \subset S_i$. As before $| S_0 | = | S_0 * x_i | \leqslant | S_i | \leqslant | S_0 |$ so $S_0 * x_i = S_i$.

Since $x_i * S_0 = S_0 * x_i = S_i$, then S_0 is a normal subgroup of $(X,*)$ and S_i is a coset for $i = 0,\ldots,K-1$. ■

Corollary 5.4: There is an integer k such that $K = p^k$.

Proof: Since X is partitioned by equal sized cosets we have

$$N = p^n = | X | = K | S_0 | .$$

Now K divides p^n and p is prime so K is a power of p. For the remainder of this paper, k will denote this power. ■

Our next corollary provides some of the methodology required to put A into the "standard form" used in Theorem 6.

Corollary 5.5: S_0 is an $n - k$ dimensional invariant subspace of X and $S_i = x_i + S_0$ for $i = 0,1,\ldots,K - 1$.

Proof: Note that if $x_{jK} \varepsilon S_0$ then for all $x \varepsilon X$, $x * x_{jK} = A^{jK}x + x_{jK} = x + x_{jK}$. So $S_i = x_i * S_0 = x_i + S_0$ for $i = 0,1,\ldots,K - 1$. This also says that $*$ restricted to S_0 is simply vector addition. Hence S_0 is a subspace of X. By Corollary 5.4, $p^n = p^k | S_0 |$ so $| S_0 | = p^{n-k}$, i.e. the dimension of S_0 is $n - k$.

To show $AS_0 = S_0$, let x_{jK} be any element of S_0. By

Corollary 5.3, $S_0 * x_1 = S_1$ so $x_{jk} * x_1 = Ax_{jK} + x_1 \varepsilon S_1$. We have just shown that $S_1 = x_1 + S_0$ so $Ax_{jK} \varepsilon S_0$. Hence $AS_0 \subset S_0$. Since A is invertable $|AS_0| = |S_0|$ so $AS_0 = S_0$. ■

Throughout we denote x_1 by v. We define $v^0 = 0$ and for $i > 0$, $v^i = v * v * \ldots * v$ i times.

Corollary 5.6: For $i = 0,1,\ldots,N - 2, v^i \varepsilon S_{i \bmod K}$.

Proof: Since $(S_0,*)$ is a normal subgroup, $\{S_0,S_1,\ldots, S_{K-1}\}$ is the quotient group under the operation

$$\begin{aligned} S_i * S_j &= (x_i * x_j) * S_0 \\ &= (x_i * x_j) + S_0 \\ &= x_\ell + S_0 \text{ where } \ell \equiv i + j \bmod K. \end{aligned}$$

Consider

$$\begin{aligned} S_1^i &= (v * S_0)^i \\ &= v^i * S_0 \\ &= (x_1 * \ldots * x_1) + S_0 \\ &= x_\ell + S_0 \text{ where } \ell \equiv \bmod K. \end{aligned}$$

Now $v^i + S_0 = S_{i \bmod K}$ so $v^i \varepsilon S_{i \bmod K}$. ■

We have defined $S_0,S_1,\ldots,S_{K-1}$, so that the UHTS causes the machine to visit cosets consecutively. That is it moves from S_i to S_{i+1} and from S_{K-1} to S_0. This property together with the invariance of S_0 allows us to prove an interesting result concerning the elements of the UHTS.

Corollary 5.7: $By_i \varepsilon S_1$ for $i = 0,1,\ldots,N - 2$. That is $By_i \equiv v \bmod S_0$.

Proof: Since $x_i \varepsilon S_{i \bmod K}$, $x_i = v^i + u_1$ where

$u_1 \varepsilon S_0$. Also there is a $u_2 \varepsilon S_0$ such that $x_{i+1} = Ax_i + By_i = v^{i+1} + u_2$. Now $Av^i + Au_1 + By_i = v^{i+1} + U_2 = Av^i + v + u_2$. Hence $By_i = v + u_2 - Au_1$. Since S_0 is an invariant subspace, $u_2 - Au_1 \varepsilon S_0$ so $By_i \varepsilon S_1$. ■

S_0 has several properties as we have already shown. Unfortunately strong connectedness is not one of them as Example 1 demonstrates. For now we can prove a slighlty weaker result. It will be used to prove Corollary 6.1 which states that S_0 is necessarily strongly connected except for one case.

Corollary 5.8: S_o is strongly connected by B and v^K. that is, is $u_1, u_2 \varepsilon S_0$ then there exists an input sequence $\{t_i\}_{i=0}^m$ and a scalar α such that $u_2 - \alpha v^K =$

$$\eta(u_1, \{t_i\}_{i=0}^m) \text{ and}$$

$$\eta(u_1, \{t_i\}_{i=0}^j \varepsilon S_0 \text{ for } j = 0, 1, \ldots, m.$$

Proof: Since $\{y_i\}_{i=0}^{N-2}$ is a UHTS there exists an $m \leqslant N - 2$ such that $u_2 = \eta(u_1, \{y_i\}_{i=0}^m)$. Recall that the UHTS causes the machine to move from coset to successive coset. Since $u_2 \varepsilon S_0$, $m + 1$ must be a multiple of K. Now $u_2 = A^{m+1}u_1 + A^m By_0 + \ldots + ABy_{m-1} + By_m$. Since $By_i \equiv v \bmod S_0$ there are inputs t_i such that $By_i = v + Bt_i$ with $Bt_t \varepsilon S_0$. Substituting $u_2 = A^{m+1}u_1 + A^m(v + t_0) + \ldots + v + t_m$

$$= A^{m+1}u_1 + A^m t_0 + \ldots + t_m + (A^m + \ldots + I)v$$

It remains to show that $(A^m + \ldots + I)v$ is a multiple of v^K. Since there is an α such that $\alpha K = m + 1$,

$$\begin{aligned}(A^m + \dots + I)v &= A^{(\alpha-1)K}(A^{K-1}+ \dots + I) + \\ &\quad A^{(\alpha-2)K}(A^{K-1}+ \dots + I)+ \dots + (A^{K-1}+ \dots + I) \\ &= [A^{(\alpha-1)K}(A^{K-1}+ \dots + I) + A^{(\alpha-2)K}(A^{K-1}+ \dots + \\ &\quad I)+ \dots + (A^{K-1}+ \dots + I)]v \\ &= \alpha v^K \text{ since } Av^K = v^K. \blacksquare\end{aligned}$$

Before concluding this section we introduce the subspace V. It allows us to express X as the direct sum of S_0 and V which in turn leads to the "standard form" of A. This property is crucial to the proof of Theorem 6 which defines the cases our algorithm needs to consider. V is the set of all linear combinations of $v, v^2, \dots, v^k$. We will show that V may serve as a set of coset leaders for the decomposition of X with respect to S_0.

We use $\langle u_1, u_2, \dots, u_r\rangle$ to denote the span of the vectors $u_1, u_2, \dots, u_r$. The symbol $\oplus$ stands for direct sum. In our situation, $X = S_0 \oplus V$ means every state x has a unique representation u + w where $u \in S_0$ and $w \in V$.

Corollary 5.9: Let $V = \langle v, v^2, \dots, v^k\rangle$. Then dimension V = k and $X = S_0 \oplus V$.

Proof: Let ℓ be the largest integer such that $v, v^2, \dots, v^\ell$ are linearly independent modulo S_0. To say a set is l.i. mod S_0 means if a linear combination is in S_0, then the coefficients are all 0. We claim that for

$i = o,1,\ldots,K-1$ there are vectors $u_i \in S_0$ and scalars $\alpha_{1,i},\alpha_{2,i},\ldots,\alpha_{\ell,i}$ such that $v^i = \alpha_{1,i}v + \alpha_{2,i}v^2 + \ldots + \alpha_{\ell,i}v^\ell + u_i$.

This is obvious for $i \leqslant \ell$ and by our definition of ℓ it is true for $\ell + 1$ as well. Proceeding inductively assume $v^m = \alpha_1 v + \alpha_2 v^2 + \ldots + \alpha_\ell v^\ell + u$ where $m > \ell + 1$. Now

$$\begin{aligned} v^{m+1} &= v^m * v = Av^m + v \\ &= A(\alpha_1 v + \alpha_2 v^2 + \ldots + \alpha_\ell v^\ell) + Au + v \\ &= v + \alpha_1 Av + \alpha_2 Av^2 + \ldots + \alpha_\ell Av^\ell + Au \\ &= (1 - \alpha_1 - \alpha_2 - \ldots - \alpha_\ell)v + (\alpha_1 Av + \alpha_1 v) \\ &\quad + (\alpha_2 Av^2 + \alpha_2 v) + \ldots + (\alpha_\ell Av^\ell + \alpha_\ell v) + Au \\ &= (1 - \alpha_1 - \alpha_2 - \ldots \alpha_\ell)v + \alpha_1 v^2 + \alpha_2 v^3 + \ldots + \\ &\quad \alpha_\ell v^{\ell+1} + Au. \end{aligned}$$

Since the claim is true for $\ell + 1$ and $Au \in S_0$ then the claim is true for $m + 1$.

Since $0,v,v^2,\ldots,v^{K-1}$ are all distinct mod S_0 then $\ell \geqslant k$ and $\dim V = k$. Recall the dimension of S_0 is $n - k$ and we have shown $S_0 \quad V = \{0\}$ so $X = S_0 \oplus V$. ■

Note that $\langle v,v^2,\ldots,v^k\rangle = \langle v,Av,\ldots,A^{k-1}v\rangle$.

IV STANDARD FORM

We have shown that the existence of a UHTS implies the existence of two subspaces, S_0 and V. S_0 is invariant and almost strongly connected. We can think of A as a linear transformation on the state set with respect to the standard normal basis. The invariance of S_0 and the structure of V allows us to define the block matrix $\widehat{A}$ which represents the same transformation with respect to a different basis. $\widehat{A}$ is in what we call "standard form" and contains a companion matrix in one of its blocks. Using standard results about characteristic and minimal polynomials we show that k can only take on the values 0, 1, or 2. As a corrolary we show that in all but one case S_0 must be strongly connected.

Theorem 6: Assume the LSM [A,B] has a UHTS. Then $k = 0$, 1, or 2 and in the case $k = 2, p = 2$.

Proof: Assume $k \neq 0$. The matrix A uniquely determines a linear mapping $T:X \to X$ defined by $T(e_i) = Ae_i$ where $\{e_1, e_2, \ldots, e_n\}$ is the standard normal basis for X. Let $\{r_1, r_2, \ldots, r_{n-k}, v, Av, \ldots, A^{k-1}v\}$ be a basis for X. We define $\widehat{A} = \{a_{ij}\}$ to be the unique matrix that represents T with respect to this basis. Since S_0 is invariant,

$$Ar_1 \quad = a_{1,}r_1 + a_{2,}r_2 + \cdots + {}_{n-k,}r_{n-k}$$

$$Ar_{n-k} \quad = a_{1n-k}r_1 + a_{2n-k}r_2 + \cdots + a_{n-kn-k}r_{n-k}.$$

Also

$$Av = 0 + Av$$

$$A(Av) = 0 + 0 + A^2v$$

$$A(A^{k-2}v) = 0 + \ldots + 0 + A^{k-1}v$$

$$A(A^{k-1}v) = a_{1n}r_1 + 1_{2n}r_2 + \ldots + a_{nn}A^{k-1}v.$$

Hence $\tilde{A} = $

$$\left|\begin{array}{ccc|cccc} a_{11} & \cdots & a_{1n-k} & 0 & \cdots & 0 & a_{1n} \\ a_{21} & \cdots & a_{2n-k} & 0 & \cdots & 0 & a_2n \\ & & & & & & \vdots \\ a_{n-k1} & \cdots & a_{n-kb-k} & 0 & \cdots & 0 & \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 & \\ 0 & \cdots & 0 & 1 & & 0 & \vdots \\ & & & & \ddots & & \\ 0 & \cdots & 0 & 0 & & 1 & a_{nn} \end{array}\right|$$

We say that the block matrix $\tilde{A} = \left(\begin{array}{c|c} S & W \\ \hline O & U \end{array}\right)$ is in standard form.

Note that U is a companion matrix.

Since A and $\tilde{A}$ represent the same linear transformation T, $\tilde{A} = CAC^{-1}$ where $C^{-1} = [r_1 \vdots r_2 \vdots \cdots \vdots r_{n-k} \vdots v \vdots Av \vdots \ldots \vdots A^{k-1}v]$. Note that Cv = e_{n-k+1}.

By Corollary 5.6 $0, v, v^2, \ldots, v^{K-1}$ are all distinct mod S_0. That is, not only are the elements distinct but the difference of any two is not in S_0. Hence $C0, Cv, Cv^2, \ldots, Cv^{K-1} = 0, Cv, C(A + I)C^{-1}Cv, \ldots, C(A^{K-2} + \ldots + I)C^{-1}Cv = 0, e_{n-k+1}, (\tilde{A} + I)e_{n-k+1}, \ldots, (\tilde{A}^{K-2} + \ldots + I)e_{n-k+1}$ are all distinct mod CS_0. Since $CS_0 = \langle e_1, \ldots, e_{n-k}\rangle$, $0, e_1, (U + I)e_1, \ldots, (U^{K-2} + \ldots + I)e_1$ are all distinct. In particular, $U + I$, $U^2 + U + I, \ldots, U^{K-2} + \ldots + I$, are all nonzero matrices.

Since $\tilde{A}^K = I$, $U^K = I$. Applying the binomial theorem, $U^K - I = (U - I)^K = 0$ since $K = p^k$. Note that U is a companion matrix so its minimal polynomial equals its characteristic polynomial [See Harrison p. 14]. Now the minimal polynomial divides $(U - I)^K$ and has degree k so $(U - I)^k = 0$.

Let $L = p^\ell$ be such that $p^\ell > k$ and $p^{\ell-1} \leqslant k$. Now $(U - L)^L = U^L - I = (U - I)(U^{L-1} + \ldots + I)$ so $(U - I)^{L-1} = U^{L-1} + \ldots + I$. Since $L - 1 \geqslant k$, $U^{L-1} + \ldots + I = 0$. This implies $L - 1 > K - 2$ so $L > K - 1$. Also $p^{\ell-1} \leqslant k$ implies $L \leqslant pk$. Combining these inequalities gives $p^k - 1 < pk$ or equivalently $p^{k-1} \leqslant k$. Recall this was derived assuming $k \neq 0$. Clearly $k = 1$ satisfies this inequality for all primes. However if $k = 2$ then p must be 2. If $k > 2$ then $p^{k-1} > k$. ■

Corollary 6.1: S_0 is necessarily strongly connected unless $k = 1$ and $p = 2$.

Proof: The case where $k = 0$ is trivial since $S_0 = X$.

Assume $k = 1$ and $p \neq 2$. By the proof of Theorem 6, A is similar to a matrix in standard form $\left(\begin{array}{c|c} S & w \\ \hline 0\ldots0 & 1 \end{array}\right)$.

S is n-1 by n-1, w is a column vector and v corresponds to e_n. Since the existence of a UHTS is preserved under a similarity transform, we will assume A is of this form and $v = e_n$. We may also assume B is of the form

$$\left(\begin{array}{c|c} B_1 & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ \hline 0\ldots0 & 1\end{array}\right)$$

Since S_0 is strongly connected by B and v^p, the rank of $[B_1 \vdots SB_1 \vdots \ldots \vdots S^{p-1}B_1 \vdots \hat{v}] = n - 1$ where $v^p = \begin{pmatrix}\hat{v}\\ 0\end{pmatrix}$. We will prove S_0 is strongly connected by showing $\hat{v}$ is in the column space of $[B_1 \vdots SB_1 \vdots \ldots \vdots S^{p-1}B_1]$. The crux of the argument is the fact that $Av^p = v^p$ and $(S - I)^{p-2} = S^{p-2} + 2S^{p-3} + \ldots + (p-2)S + (p-1)\,I$. To see the second equality, the binomial theorem gives

$$(S - I)^{p-2} = \sum_{i=0}^{p-2} \binom{p-2}{i} S^{p-2-i}(-1)^i. \quad \text{Now}$$

$$\binom{p-2}{i} = (p - 2)(p - 3)\ldots(p - i)(p - i - 1)/i!$$

$$= \frac{(-2)(-3)\ldots(-i)(-i-1)}{(2)\ (3)\ \ldots(i)} = (-1)^i(i + 1)$$

So $(S - I)^{p-2} = \sum_{i=0}^{p-2} (i + 1)S^{p-2-i}$.

We claim $v^p = \begin{pmatrix}(S - I)^{p-2}w\\ 0\end{pmatrix}$. To prove this claim note

$$A^2 = \left(\begin{array}{c|c} S^2 & (S + I)\ w \\ \hline 0 & 1\end{array}\right)$$

$$A^3 = \left(\begin{array}{c|c} S^3 & (S^2 + S + I)\ w \\ \hline 0 & 1\end{array}\right)$$

$$\vdots$$

$$A^{p-1} = \left(\begin{array}{c|c} S^{p-1} & (S^{p-2} + \ldots + I)\ w \\ \hline 0 & 1\end{array}\right)$$

So $v^p = (A^{p-1} + \ldots + I)e_n$

$$= e_n + \begin{pmatrix}w\\ 1\end{pmatrix} + \begin{pmatrix}(S + I)w\\ 1\end{pmatrix} + \ldots + \begin{pmatrix}(S^{p-2} + \ldots + I)w\\ 1\end{pmatrix}$$

$$= \begin{pmatrix} (p - 1)w + (p - 2)Sw + (p - 3)S^2w + \ldots + S^{p-2}w) \\ p \end{pmatrix}$$

$$= \begin{pmatrix} (S - I)^{p-2}w \\ 0 \end{pmatrix}$$

Now $\binom{w}{0} \varepsilon S_0$ so by Corollary 5.8 there are inputs t_i such that

$$w = S^{p-1}B_1t_0 + S^{p-2}B_1t_1 + \ldots + SB_1t_{p-2} + B_1t_{p-1} + \alpha\hat{v}$$

where $\binom{\hat{v}}{0} = v^p$. Since $Av^p = v^p$, $S\hat{v} = \hat{v}$ so $Sw = B_1t_0 + S^{p-1}B_1t_1 + \ldots + S^2B_1t_{p-2} + SB_1t_{p-1} + \alpha\hat{v}$.

Hence

$(S - I)w = B_1(t_0 - t_{p-1}) + SB_1(t_{p-1} - t_{p-2}) + \ldots + S^{p-1}B_1(t_1 - t_0)$. Recall $p \geqslant 3$ so clearly $\hat{v} = (S - I)^{p-3}$ $(S - I)w$ is in the column space of

$$[B_1 \vdots SB_1 \vdots \ldots \vdots S^{p-1}B_1].$$

Suppose $k = 2$ and $p = 2$. As before we may assume

$$A = \left(\begin{array}{c|cc} & 0 & \\ & \vdots & w \\ S & 0 & \\ \hline 0\ldots0 & & \\ 0\ldots0 & & U \end{array}\right)$$

and $v = e_{n-1}$ where U is a 2 by 2 nonsingular companion matrix. That is either $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Since $A^4 = I$, $U^4 = I$. Now $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^4 \neq I$ so we may assume

$$A = \left(\begin{array}{c|cc} & 0 & \\ & \vdots & w \\ S & 0 & \\ \hline 0\ldots0 & 0 & 1 \\ 0\ldots0 & 1 & 0 \end{array}\right).$$

Clearly $Av = e_n$, $A^2v = \begin{pmatrix} w \\ 1 \\ 0 \end{pmatrix}$ and $A^3v = \begin{pmatrix} S\ w \\ 0 \\ 1 \end{pmatrix}$ so $v^4 =$ $(A^3 + A^2 + A + I)v = \begin{pmatrix} (S + I)w \\ 0 \\ 0 \end{pmatrix}$.

Proceeding as before, Corollary 5.8 guarantees the existence of inputs t_i such that

$$\begin{pmatrix} w \\ 0 \\ 0 \end{pmatrix} = A^3Bt_0 + A^2Bt_1 + AB^t{}_2 + Bt_3 + \alpha v^4$$

where $Bt_i \varepsilon S_0$ for $i = 0, 1, 2, 3$. Since $Av^4 = v^4$

$$A\begin{pmatrix} w \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} Sw \\ 0 \\ 0 \end{pmatrix} = Bt_0 + A^3Bt_1 + A^2Bt_2 + ABt_3 + \alpha v^4$$

Since S_0 is invariant each term is in S_0. Now

$$v^4 = \begin{pmatrix} (S + 1)w \\ 0 \\ 0 \end{pmatrix} = A^3B(t_1 + t_0) + A^2B(t_2 + t_1) +$$

$$AB(t_3 + t_2) + B(t_0 + t_3).$$

S_0 is a subspace so again each term is in S_0.

By Corollary 5.8, if u_1 and u_2 are any elements of S_0, there is in input sequence $\{t'\}_{i=0}^3$ taking u_1 to u_1 to $u_2 - \alpha v^4$ without leaving S_0. If $\alpha = 1$ then the sequence $\{(t_0' + t_1 + t_0), (t_1' + t_2 + t_1), (t_2' + t_3 + t_2), (t_3' + t_0 + t_3)\}$ takes u_1 to u_2 without leaving S_0. This is trivial for $\alpha = 0$ so S_0 is strongly connected.

In the case $p = 2$ and $A^2 = I$, S_0 may or may not be strongly connected as shown in Example 1. ■

V KEY THEOREM

We have developed a battery of properties all LSM's with a UHTS must have. Theorem 7 singles out those properties that are both necessary and sufficient. It provides the key to proving the correctness of our algorithm. The proof of Theorem 7 is constructive and depends on Corollaries 2.1 and 2.2.

Theorem 7: The LSM [A,B] has a UHTS if and only if [A,B] is strongly connected and one of the following hold;

1) $A = I$

2) $A = I$, there is a strongly connected invariant subspace S_0 of dimension $n - 1$, and there is a $v \in R(B)$ such that $X = S_0 \oplus \langle v \rangle$

3) $A^2 = I$ and $p = 2$

4) $A^4 = I$, $p = 2$, there is a strongly connected invariant subspace S_0 of dimension $n - 2$, and there is a $v \in R(B)$ such that $X = S_0 \oplus \langle v, Av \rangle$.

Proof: The necessity of these conditions follows from Theorem 6 and Corollaries 1.1, 5.5, 5.9, and 6.1

To prove sufficiency assume [A,B] is strongly connected.

Case 1 ($A = I$): Since $A = I$, the operation * as defined in Theorem 5 is simply vector addition, a group operation. By Theorem 1 (iv) B must have full rank so any ordering on the state space has an associated input sequence which is a UHTS by Theorem 5.

Case 2 ($p \geqslant 3, A^p = I$): We want to show $\langle v \rangle \equiv \{0, v, (A+I)v, \ldots, (A^{p-2} + \ldots + I)v\}$ mod S_0. Since $X = S_0 \oplus V$ there is a scalar α and a $u \in S_0$ such that $(A + I)v = u + (\alpha + 1)v$. Subtracting gives $(A - \alpha I)v = u \in S_0$. Our result becomes more evident by showing $(\lambda - \alpha)$ divides the minimal polynomial of A [See Gantmacher p. 184]. Since $A^p - I = (A - I)^p = 0$, the minimal polynomial of A is of the form $(\lambda - 1)^m$ for some $m \leqslant p$. We may write $(\lambda - 1)^m = f(\lambda)(\lambda - \alpha) + r$ where r is a constant. Substitution in A gives $(A - I)^m = f(A)(A - \alpha I) + rI$. Now $(A - I)^m v = 0 = f(A)u + rv$. Since S_0 is an invariant subspace $f(A)u \in S_0$ so $rv \in S_0$. This can only happen if $r = o$ so $\lambda - \alpha$ divides $(\lambda - 1)^m$ making $\alpha = 1$. Since we assumed $(A + I)v = u + (\alpha + 1)v$, $(A + I)v \equiv 2v$ mod S_0.

We claim $(A^i + \ldots + I)v \equiv (i + 1)v$ mod S_0 and prove it by induction. Consider

$$\begin{aligned} (A^i + \ldots + I)v &= A(A^{i-1} + \ldots + I)v + v \\ &\equiv A(iv) + iv - (i - 1)v \text{ mod } S_0 \\ &\equiv i(A + I)v - (i - 1)v \\ &\equiv 2iv - (i - 1)v \\ &\equiv (i + 1)v. \end{aligned}$$

Hence $\{0, v, (A + I)v, \ldots, (A^{p-2} + \ldots + I)v\}$ can serve as coset leaders for the decomposition of X with respect to S_0. We denote these states by $\{0, v, v^2, \ldots, v^{p-1}\}$.

There are two subcases to consider. In both assume y is such that $v = By$.

Assume $v^p = 0$. Since S_0 is strongly connected, by Corollary 2.1 S_0 has a Hamiltonian circuit say $\{0 = u_0, u_1, \ldots, u_{L-1}, u_L = 0\}$ where $L = p^{n-1}$. For each $i = 0,1,\ldots, L - 1$ there exists a t_i such that $u_{i+1} = Au_i + Bt_i$. The UHTS is illustrated in diagram 1 where the quantities above the arrows represent the inputs used to get to the next state.

To show we have a Hamiltonian tour note that X is partitioned by $\{S_0, S_1, \ldots, S_{p-1}\}$ where $S_i = S_0 + v^i$. Note also that once state u_1 is reached, the diagram has $L - 1$ distinct columns. The elements in the i^{th} column are of the form $v^j + u_i$. It suffices to show that the v^j components within each column are distinct. This is clear since $0, L - 1, 2(L - 1), \ldots (p - 1)(L - 1)$ are distinct modulo p. Hence we have a Hamiltonian tour starting with the 0 state. Note that we started in S_0, moved from S_{i-1} to S_i for $1 \leqslant i < p$ and from S_{p-1} to S_0.

To show this is a uniform tour suppose we start in an arbitrary state x. It suffices to show that $x + S_0$, $Ax + S_1, \ldots, A^{p-1}x + S_{p-1}$ partition X since $A^p = I$. Assume $x \in S_r$. Then there is a $u \in S_0$ such that $x = u + v^r$. Now $A^i x + S_i = A^i u + A^i v^r + v^i + S_0$. Since $AS_0 = S_0$, $A^i u \in S_0$. Also $A^i v^r + v^i = (A^{i+r-1} + \ldots + A^i)v + (A^{i-1} + \ldots + I)v = v^{i+r}$. Now $A^i x + S_i = v^{i+r} + S_0 = S_{(i+r) \bmod p}$ for $i = 0, \ldots, p - 1$. Hence our diagram exhibits a UHTS.

Assume $v^p \neq 0$. Note that $Av^p = A(A^{p-1} + \ldots + I)v = (I + A^{p-1} + \ldots + A)v = v^p$. We have already shown that

$$\begin{tikzcd}
0 \arrow[r, "y"] & v \arrow[r, "y"] & v^2 \arrow[r, "y"] & \cdots \arrow[r, "y"] & v^{p-1} \arrow[r, "y+t_0"] & v^p + u_1 = u_1
\end{tikzcd}$$

$$\begin{tikzcd}
u_1 \arrow[r, "y+t_1"] & v^1 + u_2 \arrow[r, "y+t_2"] & v^2 + u_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2} + u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
v^{L-1} + u_1 \arrow[r, "y+t_1"] & v^{1+(L-1)} + u_2 \arrow[r, "y+t_2"] & v^{2+(L-1)} + u_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+(L-1)} + u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
v^{2(L-1)} + u_1 \arrow[r, "y+t_1"] & v^{1+2(L-1)} + u_2 \arrow[r, "y+t_2"] & v^{2+2(L-1)} + u_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+2(L-1)} + u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
\vdots & & & & \\
v^{(p-1)(L-1)} + u_1 \arrow[r, "y+t_1"] & v^{1+(p-1)(L-1)} + u_2 \arrow[r, "y+t_2"] & v^{2+(p-1)(L-1)} + u_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+(p-1)(L-1)} + u_{L-1} &
\end{tikzcd}$$

<u>Diagram 1</u>. UHTS for $k=1$, $p>2$, and $v^p = 0$.

$v^p \equiv pv \equiv 0 \bmod S_0$ so $v^p \in S_0$. If $S_0 = \langle v^p \rangle$ then we claim $\{y\}_{i=0}^{p^2-2}$ is a UHTS. Starting this sequence at 0 gives

$$\{0,v,v^2,\ldots,v^p,v^{p+1},\ldots,v^{2p},\ldots,v^{p^2-1}\}$$
$$= \{0,v,v^2,\ldots,v^p + 0,v^p + v,\ldots,2v^p + 0,\ldots,$$
$$(p - 1)v^p + v^{p-1}\}$$

This clearly provides an ordering of the state space which is a group under the operation $v^i * v^j = A^jv^i + v^j$. This group is in fact cyclic with generator v. By Theorem 5 we have a UHTS.

Assume $S_0 \neq v^p$. Then the dimension of S_0 is greater than 1 so $n \geqslant 3$. Since $Av^p = v^p \in S_0$ we may apply Corollary 2.2. Now we have a subspace W of dimension n - 2 with a Hamiltonian circuit mod v^p. Let $\{t\}_{i=0}^{L-1}$, $L = p^{n-2}$, be the associated input sequence giving $\{0 = u_0,u_1,\ldots,u_{L-1},u_L\}$ where U_L projected onto W is 0. That is u_L must be a multiple of v^p so $Au_L = u_L$. The UHTS is illustrated in diagram 2.

Note that
$$\begin{aligned} v^{r+q} &= (A^{r+q-1} + \ldots + I)v \\ &= A^q(A^{r-1} + \ldots + I)v + (A^{q-1} + \ldots + I)v \\ &= A^qv^r + v^q. \end{aligned}$$

Let m be such that $u_L = mv^p$. Now
$$\begin{aligned} v^{i(L-1)} + iu_L &= v^{i(L-1)} + imv^p \\ &= v^{i(L-1)} + v^{imp} \\ &= A^{imp}v^{i(L-1)} + v^{imp} \\ &= v^{i(L-1) + imp} \\ &= v^{i(L-1 + mp)}. \end{aligned}$$

$$0 \xrightarrow{y} v \xrightarrow{y} v^2 \xrightarrow{y} \cdots \xrightarrow{y} v^{p^2-1} \xrightarrow{y+t_0} u_1$$

$$\begin{tikzcd}
u_1 \arrow[r, "y+t_1"] & v+u_2 \quad \cdots \arrow[r, "y+t_{L-2}"] & v(L-2)+ u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
v^{(L-1)}+ u_L+u_1 \arrow[r, "y+t_1"] & v^{1+(L-1)}+ u_L+u_2 \quad \cdots \arrow[r, "y+t_{L-2}"] & v^{L-1(L-1)}+ u_L+u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
v^{2(L-1)}+ 2u_L+u_1 \arrow[r, "y+t_1"] & v^{1+2(L-1)}+ 2u_L+u_2 \quad \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+2(L-1)}+ 2u_L+u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
\vdots & & & \\
v^{(p^2-1)(L-1)}+ (p^2-1)u_L+u_1 \arrow[r, "y+t_1"] & v^{1+(p^2-1)(L-1)}+ (p^2-1)u_L+u_2 \quad \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+(p^2-1)(L-1)}+(p^2-1)u_L+u_{L-1} &
\end{tikzcd}$$

Diagram 2. UHTS for $k=1$, $v^p \neq 0$.

As in the case when $v^p = 0$, after state u_1 is reached we have L - 1 distinct columns. We have a Hamiltonian tour if the elements in each column are distinct. For the r^{th} column assume two elements are the same. That is suppose

$$v^{r+1(L-1)} + iu_L = v^{r+j(L-1)} + ju_L.$$

Then

$$A^r v^{i(L-1)} + v^r + iu_L = A^r v^{j(L-1)} + v^r + ju_L$$

$$A^r v^{i(L-1)} + iu_L = A^r v^{j(L-1)} + ju_L$$

$$v^{i(L-1)} + iu_L = v^{j(L-1)} + ju_L$$

$$v^{i(L-1 + mp)} = v^{j(L-1 + mp)}$$

$$i(L - 1 + mp) \equiv j(L - 1 + mp) \bmod p^2$$

$$(i - j)(p^{n-2} - 1 + mp) \equiv 0 \bmod p^2.$$

We can choose m so that $0 \leqslant m < p$. Recall that $n \geqslant 3$ so p does not divide $(p^{n-2} - 1 + mp)$. Hence p^2 must divide $i - j$. Since each column has only p^2 states, $i = j$. Thus we have a Hamiltonian tour when we start in the 0 state.

Note that if we define S_i as before our tour moves from S_{i-1} to S_i for $0 < i < p$ and from S_{p-1} to S_0. We have already shown in the previous case that for all $x \in X$, $x + S_0$, $Ax + S_1, \ldots, S^{p-1}x + S_{p-1}$ partition X so our tour is uniform.

Case 3 ($p = 2$, $A^2 = I$). By Theorem 1, the rank of [B,AB] is n since [A,B] is strongly connected. Let $b_1, \ldots, b_m$ be such that $b_1, \ldots, b_m, Ab_1, \ldots, Ab_m$ span X. Furthermore we impose the restriction that if any pair b_i, Ab_i are removed we no longer have a spanning set. Now if $Ab_i = b_i$

for $i = 1,\dots,m$ then $m = n$ and $A = I$. Since $A \neq I$ we may assume $Av \neq v$ where $v = b_1$. Set $S = \langle b_2,\dots,b_m,Ab_2,\dots, Ab_m\rangle$. Clearly S is an invariant, strongly connected subspace and $v \notin S$. If $(A + I)v \notin S$ then $X = S\oplus\langle v,Av\rangle$ and we have reduced the problem to case 4.

Assume $(A + I)v = v^2 \in S$ and y is such that $By = v$. Ifn = 2 then clearly $\{y,y,y\}$ is a UHTS since $X = \{0,v, (A + I)v,Av\} = \{0,v,v^2,v^3\}$. Suppose $n > 2$ and that $\{0 = u_0,u_1,\dots,u_{L-1},u_L\}$ be the Hamiltonian circuit mod v^2 guarenteed by Corollary 2.2 where $L = 2^{n-2}$ and $\{t\}_{i=0}^{L-1}$ is the associated input sequence. Diagram 2 with $p = 2$ illustrates a UHTS.

Let $W_0 = \{0,u_1,\dots,u_{L-1}\}$, $W_1 = v + W_0, W_2 = v^2 + W_0$, and $W_3 = v^3 + W_0$. We know that W_0,W_1,W_2, and W_3 partition X. Now the fact that we have a tour starting at 0 is evident if we can show $\{0,v^{L-1} + u_L,v^{2(L-1)},v^{3(L-1)} + u_L\} = \{0,v,v^2,v^3\}$. Recall from Corollary 2.2 that either $u_L = 0$ or $u_L = v^2$. Since $L = p^{n-2}$ and $n > 2$, $L - 1$ is odd. Hence $\{0,L - 1,2(L - 1),3(L - 1)\} \equiv \{0,1,2,3\}$ mod 4. Since $v^4 = 0$, if $u_L = 0$ we have a tour. If $u_L = v^2$, note that $v^i + v^2 = A^2v^i + (A + I)v = v^{i+2}$. Now $\{0,(L - 1) + 2,2(L - 1),3(L - 1) + 2\}$ is also equivalent to $\{0,1,2,3\}$ mod 4 so again we have a tour. Our tour moves from S to $v + S$ and from $v + S$ to S. This tour is uniform if $x + S$ and $Ax + (v + S)$ partition X for all $x \in X$. This is clear if $x \in S$ since S is an invariant subspace. If $x = v + u$,

$u \varepsilon S$ then $x+S = v+S$ and $Ax + v+S = (A+I)v + S = S$. Hence we have demonstrated a UHTS.

Case 4 ($p = 2, A^4=I$): We want to shown that $\{0,v, (A + I)v,(A^2 + A + I)v\} \equiv \langle v,Av\rangle \bmod S_0$. This is clear if $(A^2 + A + I)v \equiv Av \bmod S_0$. We prove our claim by process of elimination. Suppose $(A^2 + A + I)v \varepsilon S_0$. Since S_0 is an invariant subspace then $A(A + I)(A^2 + A + I)v = A(A^3 + I)v = (A + I)v \varepsilon S_0$. This contradicts the hypothesis $X = S_0 \oplus \langle v,Av\rangle$. Suppose $(A^2 + A + I)v = v + u$ where $u \varepsilon S_0$. Then $(A^2 + A)v \varepsilon S_0$ which implies $A^3(A^2 + A)v = (A + I)v \varepsilon S_0$. If $(A^2 + A + I)v = (A + I)v + u$, $u \varepsilon S_0$ then $A^2v \varepsilon S_0$. This implies $v \varepsilon S_0$. The only other possibility is that $(A^2 + A + I)v \equiv Av \bmod S_0$. Now $0,v, (A + I)v, (A^2 + A + I)v$ can serve as coset leaders for the decomposition of X with respect to S_0. As before we denote these states by $0,v,v^2$, and v^3.

We proceed as in case 2. Assume $v^4 = (A^3 + A^2 + A + I)v = 0$. Note that this is the situation of $A^2 = I$. If $n = 2$ then clearly $\{y,y,y\}$ is a UHTS where $v = By$. Otherwise by Corollary 2.1, S_0 has a Hamiltonian circuit say $\{0 = u_0,u_1,\ldots,u_L = 0\}$ where $L = 2^{n-1}$. Let $\{t\}_{i=0}^{L-1}$ be the associated input sequence. The UHTS is shown in diagram 3.

Note that $L - 1 = 2^{n-2} - 1$ is odd since $n \geqslant 3$. Now $0,L - 1, 2(L - 1), 3(L - 1)$ are distinct mod 4 so we have a Hamiltonian tour starting at 0. To show it is uniform we

$$\begin{tikzcd}
0 \arrow[r, "y"] & v \arrow[r, "y"] & v^2 \arrow[r, "y"] & v^3 \arrow[r, "y+t_0"] & u_1
\end{tikzcd}$$

$$\begin{tikzcd}
u_1 \arrow[r, "y+t_1"] & v + u_2 \arrow[r, "y+t_2"] & v^2 + u_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2} + u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
v^{(L-1)} + u_1 \arrow[r, "y+t_1"] & v^{1+(L-1)} + u_2 \arrow[r, "y+t_2"] & v^{2+(L-1)} + u_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+(L-1)} + u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
v^{2(L-1)} + u_1 \arrow[r, "y+t_1"] & v^{1+2(L-1)} + u_2 \arrow[r, "y+t_2"] & v^{2+2(L-1)} + u_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+2(L-1)} + u_{L-1} \arrow[r, "y+t_{L-1}+t_0"] & {} \\
v^{3(L-1)} + u_1 \arrow[r, "y+t_1"] & v^{1+3(L-1)} + u_2 \arrow[r, "y+t_2"] & v^{2+3(L-1)} + U_3 \cdots \arrow[r, "y+t_{L-2}"] & v^{L-2+3(L-1)} + u_{L-1} &
\end{tikzcd}$$

<u>Diagram 3</u>. UHTS for $p=2$ and $v^4 = 0$.

need to show $x + S_0, As + S_1, A^2x + S_2, A^3x + S_3$ partition X for all states x. The argument is identical to case 2. Suppose $x \in S_r$. Then there is a $u \in S_0$ such that $x = u + u^r$. Now

$$\begin{aligned} A^ix + S_i &= A^iu + A^iv^r + v^i + S_0 \\ &= A^i(A^{r-1}+\ldots+ I)v + (A^{i-1}+\ldots+ I)v + A^iu + S_0 \\ &= v^{i+r} + S_0 \text{ since } A^iu \in S_0. \end{aligned}$$

Hence all states are visited regardless of the starting state.

Suppose $v^4 \neq 0$. In this case $A^2 \neq I$ and it can be easily shown that $n > 2$. Recall $(A^2 + A + I)v \equiv Av \bmod S_0$ so $(A^2 + I)v \in S_0$. The invariance of S_0 implies $(A^3 + A)v \in S_0$. Now $(A^2 + I)v + (A^3 + A)v = v^4 \in S_0$. Clearly $Av^4 = v^4$. If $n = 3$ and $[A,B]$ is started at 0 then a sequence of seven y's generate $\{0,v,v^2,\ldots,v^7\} = \{0,v,v^2, v^3,v^4,v + v^4,v^2 + v^4,v^3 + v^4\} = X$. This is a UHTS by Theorem 5 since * defined by $v^i * v^j = A^jv^i + v^j = v^{i+j}$ form a cyclic group generated by v.

Assume $n > 3$. By Corollary 2.2 we have a n-3 dimensional subspace W with a Hamiltonian circuit mod v^4. Let $\{0 = u_0,u_1,\ldots,u_L\}$ be the circuit with the associated input sequence $\{t\}_{i=0}^{L-1}$ where $L = 2^{n-3}$. Note that $L - 1$ is odd since $n > 3$. Also u_L is a multiple of v^4 so either $u_L = v^4$ or 0. We claim diagram 4 demonstrates a UHTS.

As in the previous cases after state u_1 is reached we

$$0 \xrightarrow{y} v \xrightarrow{y} v^2 \cdots \xrightarrow{y} v^7 \xrightarrow{y+t_0} u_1$$

$$u_1 \xrightarrow{y+t_1} v + u_2 \xrightarrow{y+t_2} v^2 + u_3 \cdots \xrightarrow{y+t_{L-2}} v^{L-2} + u_{L-1} \xrightarrow{y+t_{L-1}+t_0}$$

$$v^{L-1}+ u_L+u_1 \xrightarrow{y+t_1} v^{1+(L-1)}+ u_L+u_2 \xrightarrow{y+t_2} v^{2+(L-1)}+ u_L+u_3 \cdots \xrightarrow{y+t_{L-2}} v^{L-2+(L-1)}+ u_L+u_{L-1} \xrightarrow{y+t_{L-1}+t_0}$$

$$v^{2(L-1)}+ u_1 \xrightarrow{y+t_1} v^{1+2(L-1)}+ u_2 \xrightarrow{y+t_2} v^{2+2(L-1)}+ u_3 \cdots \xrightarrow{y+t_{L-2}} v^{L-2+2(L-1)}+ u_{L-1} \xrightarrow{y+t_{L-1}+t_0}$$

$$v^{3(L-1)}+ u_L+u_1 \xrightarrow{y+t_1} v^{1+3(L-1)}+ u_L+u_2 \xrightarrow{y+t_2} v^{2+3(L-1)}+ u_L+u_3 \cdots \xrightarrow{y+t_{L-2}} v^{L-2+3(L-1)}+ u_L+u_{L-1} \xrightarrow{y+t_{L-1}+t_0}$$

$$\vdots$$

$$v^{7(L-1)}+ u_L+u_1 \xrightarrow{y+t_1} v^{1+7(L-1)}+ u_L+u_2 \xrightarrow{y+t_2} v^{2+7(L-1)}+ u_L+u_3 \cdots \xrightarrow{y+t_{L-2}} v^{L-2+7(L-1)}+ u_L+u_{L-1}$$

<u>Diagram 4</u>. UHTS for k=2, p=2, and $v^4 \neq 0$.

have $L - 1$ distinct columns. It can be easily verified that since $L - 1$ is odd, $\{0,L - 1,2(L - 1),\ldots,7(L - 1)\} \equiv \{0,1,\ldots,7\}$ mod 8. So if $u_L = 0$ then we have a Hamiltonian tour. This is clear since every element has a distinct representation $v^i + u_j$ where $i \varepsilon \{0,1,\ldots,7\}$ and $j \varepsilon \{0,1,\ldots,L - 1\}$.

If $u = v^4$ then $v^{r+i(L-1)} + u_L = A^4v^{r+1(L-1)} + v^4 = v^{4+r+i(L-1)}$. Now every element has a representation $v^i + u_j$. It remains to show that this representation is unique. That is any two states in a column are distinct. For the r^{th} column assume

$$v^{r+i(L-1)} + iv^4 = v^{r+j(L-1)} + jv^4.$$

Then $v^{r+i(L-1)} + v^{i4} = v^{r+j(L-1)} + v^{j4}$

$$v^{r+i(L-1)+i4} = v^{r+j(L-1)+j4}$$

so $\quad r + i(L - 1 + 4) \equiv r + j(L - 1 + 4)$ mod 8.

Now $\quad i(L - 1 + 4) \equiv j(L - 1 + 4)$ mod 8.

Since $L - 1 + 4$ is odd it has a multiplicative inverse in Z_8 so $i \equiv j$ mod 8. Since there are only eight states in a column, $i = j$. Now we have shown our diagram illustrates a Hamiltonian tour. The fact that it is uniform follows from the same argument used when $v^4 = 0$. ■

We conclude this section with the observation that A can be put in Jordan normal form. A general matrix defined over Z_p may not have its eigenvalues in Z_p since this field is not algebraically closed. We show that 1 is the only eigenvalue for A.

Lemma 8: If $A^K = I$ where K is a power of p then A can be put in Jordan normal form.

Proof: Since $A^K = I$ and K is a power of p, then the binomial theorem gives $A^K - I = (A - I)^K = 0$. Hence the minimal polynomial of A divides $(\lambda - 1)^K$. Now all the eigenvalues of A are 1. In particular all the eigenvalues are in Z_p. Hence A can be put into Jordan normal form [See Jacobson p. 193]. ■

VI THE ALGORITHM

Our algorithm tests for the conditions of Theorem 7. Two of these conditions require a strongly connected invariant subspace. The existence of such a subspace is easily verified when A is in Jordan normal form. Theorem 10 shows the correctness of our algorithm and that it has polynomial running time.

We input A, B, n and the prime p into Algorithm 9. For output we receive a "yes" or "no" depending on whether or not [A,B] has a UHTS. The controllability matrix $[B\ AB\ \ldots\ A^{n-1}B]$ is denoted by C.

ALGORITHM 9:

```
If the rank of $C \neq n$ then no.
Else break up into cases.
    CASE 1: $(A = I)$ then yes.
    CASE 2: $(A^2 = I, p = 2)$ then yes.
    CASE 3: $(A^p = I, p > 2)$ then result of
            SUBROUTINE CASE 3.
    CASE 4: $(A^4 = I, p = 2)$ then result of
            SUBROUTINE CASE 4.
    CASE 5: (none of the above) then no.
```

SUBROUTINE CASE 3: $(A^p = I, p > 2)$

```
Compute $\breve{A} = DAD^{-1}$ where $\breve{A}$ is in Jordan normal form.
If there is a block of size 1 then return yes.
Else set r equal to the number of Jordan blocks.
    Compute $\breve{B} = DB$.
    Compute $P\breve{B}$ where P is the projection matrix that zeros
            out all rows except for the ones correspond-
            ing to the bottom two positions of every
            Jordan block of $\breve{A}$.
    If rank of $P\breve{B} > r$ then return yes.
                      Else return no.
    SUBROUTINE CASE 4:  $(A^4 = I, p = 2)$
Compute  $\tilde{A} = DAD^{-1}$ where A is in Jordan normal form.
If there is a block of size 2 then return yes.
Else set r equal to the number of Jordan blocks.
    If the rank of B = r then return no.
    Else let $J_i$ denote the position of the botton row
            of block i.
        Compute $\tilde{B} = DB$.
        Determine a basis $b_1,\ldots,b_m$ of $R\tilde{B}$ where
                $b_i$, $i = 1,\ldots, r$, is the only basis
                vector with a 1 in the $J_i^{th}$ position.
        Set E equal to the n by m-r matrix whose $i^{th}$
        column is $b_{r+i}$.
        For  i = 1 to r do
            If block i has dimension 3 or 4
            then if $(P_iE)x = e_{J_i-2}$ has a solution where
                $P_i$ is the projection matrix mapping
                to $<e_{J_i-1}, e_{J_i-2}>$
              then return yes.
        End For.
    Return no.
```

Theorem 10: Algorithm 9 is a polynomial time algorithm that correctly determines whether or not the LSM [A,B] has a UHTS.

Proof: The correctness of Algorithm 9 is about immediate from Theorem 7. We need only verify the techniques used in subroutines CASE 3 and CASE 4 for determining the existence of v and S_0.

Both subroutines require that A be put in Jordan normal form. Lemma 8 allows us to do this but also shows that 1 is the only eigenvalue of A. Hence $\tilde{A}$ has 1's along its main diagonal. Now

$$\tilde{A}e_i = \begin{cases} e_i & \text{if i is at the top of a block} \\ e_i + e_{i-1} & \text{otherwise.} \end{cases}$$

Because of this property we say $\tilde{A}$ cycles upward.

We let r denote the number of Jordan blocks in $\tilde{A}$ and J_i is the position of the bottom row of block i. Now [A,B] is strongly connected so the rank of $[\tilde{B}\ \tilde{A}\tilde{B}\ \cdots\ \tilde{A}^{n-1}\tilde{B}]$ equals n. Since $\tilde{A}$ cycles upward there must be linearly independent vectors $b_1,\ldots,b_r$ in the range of $\tilde{B}$ such that b_i has a 1 in the J_i position but a 0 corresponding to the bottom of all other blocks. This is our situation upon entering either subroutine.

We first consider SUBROUTINE CASE 3. Suppose $\tilde{A}$ has a block, say the r^{th} one, of size 1. Set $S_0 = \langle b_1, \tilde{A}b_1, \ldots, \tilde{A}^{p-1}b_1, \ldots, b_{r-1}, \ldots, \tilde{A}^{p-1}b_{r-1}\rangle$. Clearly S_0 is a strongly connected, invariant subspace and $X = S_0 \oplus \langle b_r \rangle$. By Theorem 7 we have a UHTS. Suppose all the blocks are of dimension two or more. We need to determine if there is a vector W with a 0 in the J_i^{th} position and a 1 in the J_i-1 spot. Assuming there is such a vector for say i = r then we may define S_0 so that $X = S_0 \oplus \langle b_r \rangle$. If not there is no possibility to have a n-1 dimensional, strongly connected subspace. The projection matrix P zeros out all but the bottom two positions of every block. We know $Pb_1, \ldots, Pb_r$ are linearly independent so the rank of $P\tilde{B}$ is at least r. The existence of w, and a UHTS, depends on whether or not $\tilde{P}B$ has another linearly independent vector in its range.

For SUBROUTINE CASE 4, suppose $\tilde{A}$ has a block, say the r^{th} one, of size 2. Set S_0 equal to the strongly connected invariant subspace $\langle b_1, \tilde{A}b_1, \tilde{A}^2 b_1, \tilde{A}^3 b_1, \ldots, b_{r-1}, \tilde{A}b_{r-1}, \tilde{A}^2 b_{r-1}, \tilde{A}^3 b_{r-1} \rangle$. We will show $X = S_0 \oplus \langle b_r, \tilde{A}b_r \rangle$ by exploiting the property that b_i is the only vector in $\{b_1, \ldots, b_r\}$ with a component in the J_i^{th} position. It is already clear that b_r and $\tilde{A}b_r$ are not in S_0. It remains to show the same for $(\tilde{A} + I)b_r$.

Since $\tilde{A}$ cycles upward, $(A + I)b_r$ has no component in position J_i for $i = 1, \ldots, r$. Now $b_1, (\tilde{A} + I)b_1, (\tilde{A}^2 + I)b_1, (\tilde{A}^3 + I)b_1, \ldots, (\tilde{A}^3 + I)b_{r-1}$ also spans S_0 and $b_1, \ldots, b_{r-1}$ are the only spanning vectors that have components corresponding to the botton of a Jordan block. Assuming $\tilde{A} + I\ b_r$ is in S_0 then it can be written as a linear combination of all the other spanning vectors. Note that $(\tilde{A}^2 + I)(\tilde{A} + I)$ and $(\tilde{A}^3 + I) = (\tilde{A} + I)(\tilde{A}^2 + \tilde{A} + I)$. Now there exists a $u \varepsilon S_0$ such that $(\tilde{A} + I)b_r = (\tilde{A} + I)u$. Let $P = \begin{array}{c|cc} 0 & \multicolumn{2}{c}{0} \\ \hline & 1 & 0 \\ 0 & 0 & 1 \end{array}$ be the projection matrix mapping onto $<e_{n-1},e_n>$, the positions corresponding to the r^{th} Jordan block. Now $P(\tilde{A} + I)b_r = e_{n-1}$. Note that $P\tilde{A} = \tilde{A}P$ since the r^{th} block is two dimensional. Hence $(\tilde{A} + I)Pu = e_{n-1}$. This is only possible if $u \varepsilon S_0$ has a component in the e_n direction which contradicts our construction of S_0. Hence $(\tilde{A} + I)b_r$ is not in S_0. We may not write $X = S_0 \oplus <b_r, Ab_r>$ and apply Theorem 7 to get a UHTS.

Suppose $\tilde{A}$ has no Jordan blocks of size 2. If the rank of $\tilde{B}$ is r then $b_1,\ldots,b_r$ span $R\ \tilde{B}$ and there is no strongly connected invariant subspace of dimension n-2. Hence there is no UHTS. It remains to discuss the case when the rank of $\tilde{B}$ is greater than r. Let $b_{r+1},\ldots,b_m$ be additional basis vectors needed to span $R(\tilde{B})$. The existence of a n-2 dimensional subspace S_0 depends on whether or not $R(\tilde{B})$ has a vector w with a component in the third from the bottom position of some Jordan block. It is also necessary that w has zeros corresponding to the bottom two positions. If such a w exists it must be in $<b_{r+1},\ldots,b_m>$.

For each block i we define P_i to be the projection matrix zeroing out all but the second and third from the bottom positions of block i. That is P_i projects to $<e_{J_i-1}, e_{J_i-2}>$. We set $E = [b_{r+1} \ldots b_m]$. Now w exists if and only if $P_i Ex = e_{J_i-2}$ has a solution for x. If there is a solution then $w = Ex$ and $X = S_0 \oplus <b_i, \tilde{A}b_i>$ where S_0 is the span of $w, b_1, \ldots, b_{i-1}, b_{i+1}, \ldots b_r$ and the products of $\tilde{A}, \tilde{A}^2$, and $\tilde{A}^3$ times these vectors.

We define the size of our problem by n, the dimension of the vector space X and the matrices A and B. The operations performed by Algorithm 9 are determining the rank of a matrix, computing the product of two matrices, solving a system of linear equations, and putting a matrix into Jordan normal form. The standard methods for doing these operations have polynomial running time in n [See Aho, Hopcroft, and Ullman pp. 226-242 for a discussion of the computational complexity of matrix multiplication and solving systems of linear equations].

When Algorithm 9 is to compute the Jordan normal form of A it is already known that 1 is the only eigenvalue of A. The standard methods of reducing A involves finding a maximal linearly independent set of eiginvectors [See Finkbeiner pp. 228-234]. The entire process is a matter of solving order n systems of linear equations. Hence Algorithm 9 has polynomial running time. ■

VII EXAMPLES

The following examples illustrate the conepts we have discussed. Example 1 demonstrates a LSM with a UHTS where S_0 is not strongly connected.

Example 1: $(n = 2, p = 2, k = 1)$

$$A = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, \quad B = \begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}$$

The controllability matrix

$$C = [B\ AB] = \begin{bmatrix}0 & 0 & 0\\1 & 0 & 0\end{bmatrix} \text{ has rank 2 so}$$

[A,B] is strongly connected. However $S_0 = \left\{\begin{matrix}0 & 1\\0, & 0\end{matrix}\right\}$ is not. The sequence $\left\{\begin{matrix}0 & 0 & 0\\1, & 1, & 1\end{matrix}\right\}$ is a UHTS.

Example 2: $(n = 3, p - 3, k = 1)$

$$A = \begin{pmatrix}1 & 1 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}, \quad B = \begin{pmatrix}0 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}$$

This pair has a UHTS where $S_0 = \left\langle \begin{matrix}1\\0\\0\end{matrix}, \begin{matrix}0\\1\\0\end{matrix} \right\rangle$ and $v = \begin{matrix}0\\0\\1\end{matrix}$.

Now $v^3 = (A^2 + A + I)v$

$$= \left[\begin{pmatrix}1 & 2 & 1\\0 & 1 & 2\\0 & 0 & 1\end{pmatrix} + \begin{pmatrix}1 & 1 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix} + \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}\right] \begin{matrix}0\\0\\1\end{matrix} = \begin{matrix}1\\0\\0\end{matrix}.$$

Since v^3 S_0 and $Av^3 = v^3$, Corollary 2.2 guarantees $W = \left\{\begin{matrix}0 & 0 & 0\\0, & 1, & 2\\0 & 0 & 0\end{matrix}\right\}$ has a Hamiltonian circuit mod v^3. The sequence

$$\{e_2, e_2, e_2, e_2\} \text{ generates } \begin{matrix}0 & 0 & 1 & 0\\0, & 1, & 2, & 0\\0 & 0 & 0 & 0\end{matrix}.$$

Using diagram 3 the sequence consisting of eight e_3's followed by $e_3 + e_2$, eight repetitions of the pair $e_3 + e_2$,

$e_3 + 2e_2$, and finishing with $e_3 + e_2$ is a UHTS.

Example 3: $(n = 5, p = 2, k = 2)$

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Following the steps of Algorithm 9 we find this pair is strongly connected and falls into CASE 4: $(A^4 = I, p = 2)$. To put A into Jordan normal form we need to solve

$$(A - I)x = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{matrix} = \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{matrix} .$$

Now e_1 and $e_1 + e_3$ are linearly independent solutions. Next we wish to find solutions to $(A - I)x = e_1$ and $(A - I)y = e_1 + e_3$. The vectors $x = e_2 + e_5$ and $y = e_4$ suffice. The system $(A - I)x = e_2 + e_5$ is inconsistent and $e_4 + e_5$ is a solution to $(A - I)x = e_4$.

We set $D^{-1} = [e_1 + e_3 \quad e_4 \quad e_4 + e_5 \quad e_1 \quad e_2 + e_5]$ and compute $D = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$. Now $DAD^{-1} = \hat{A} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

Since $\hat{A}$ has a block of size 2 and the rank of B is the same as the number of blocks, this system has a UHTS. Now

$$\hat{B} = DB = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} .$$

In this case $X = S_0 \oplus \langle e_5, e_4 + e_5 \rangle$ where

$$S_0 = \left\langle \begin{matrix} 0 & 0 & 1 \\ 0, & 1, & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{matrix} \right\rangle .$$

Example 4: $(n = 3, p = 2, k = 2)$

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

The machines $[A,B_1]$ and $[A,B_2]$ are both strongly connected however $[A,B_2]$ does not have a $n - 2$ strongly connected invariant subspace. The LSM $[A,B_1]$ does however and so it has a UHTS.

VIII CONCLUSION

We have shown that the problem of determining the existence of a UHTS for a LSM is polynomial time solvable. We do not know if there is a polynomial time algorithm to determine if a general sequential machine has a UHTS. One advantage the general case has over the linear case is that the size of the input is defined to be the number of elements in the state space as opposed to its dimension. Even so there may be no polynomial time algorithm in the general case.

In Theorem 1 we have shown that a LSM has a UTS if and only if it is strongly connected. Our proof demonstrates a UTS of length N^2-N and it is clear that any UTS must contain at least N-1 elements. Our work has classified all LSM's that attain this lower bound. However, no LSM has been shown to require N^2-N elements for a UTS. The problem of finding an attainable upper bound for the length of a UTS remains an open question. In fact it is not known if order N^2 inputs are necessary.

Further investigation of the group structure of touring sequences may lead to the solution of these and other problems concerning the theory of sequential machines.

IX BIBLIOGRAPHY

1. Aho, A., Hopcraft, J., and Ullman, J., The Design and Analysis of Computer Algorithms. Reading, MA: Addison-Wesley; 1974.

2. Cohn, M., Controllability in Linear Sequential Networks. IRE Trans. Circuit Theory CT-9, 74-78 (1962).

3. Cull, P., Tours of Graphs, Digraphs, and Sequential Machines. IEEE Trans. Computers C-29, (1980).

4. Finkbeiner II, D.T., Introduction to Matrices and Linear Transformations. San Francisco, CA: W.H. Freeman and Company, third ediction; 1978.

5. Gantmacher, F.R., Matrix Theory. New York, NY: Chelsea Publishing Company, Vol. 1; 1960.

6. Garey, M., and Johnson, D., Computers and Intractability. A Guide to the Theory of NP-completeness. San Francisco, CA: W.H. Freeman and Company; 1979.

7. Harrison, M.A., Lectures on Linear Sequential Machines. New York, NY: Academic Press; 1969.

8. Jacobson, N., Basic Algebra I. San Francisco, CA: W.H. Freeman and Company; 1974.