Finite cyclic quantum state machines: a topological perspective

2001 J. Phys. A: Math. Gen. 34 5731

(http://iopscience.iop.org/0305-4470/34/28/309)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **34** (2001) 5731–5743 PII: S0305-4470(01)18976-6

Finite cyclic quantum state machines: a topological perspective

A D Parks

Quantum Processing Group, Systems Research and Technology Department, Naval Surface Warfare Center, Dahlgren, VA, USA

Received 10 November 2000
Published 6 July 2001
Online at stacks.iop.org/JPhysA/34/5731

Abstract

Finite cyclic quantum state machines (FCQSMs) are characterized by free actions of finite cyclic groups upon odd-dimensional spheres. This provides for a covering space representation for all such machines. FCQSM simulation, as well as simple, quotient, and split FCQSMs are defined within this context. The notions of dynamical and process symmetries for FCQSMs are introduced and it is shown that although all FCQSMs obey a weak version of a FCQSM symmetry principle, only those which adhere to a strong version of this principle can simulate special FCQSMs defined by their dynamical symmetries. Finally, a simulation complexity index and an induced topological complexity index are defined for FCQSMs and an order relation is developed in terms of these indices which serves as a more precise statement of the weak version of the FCQSM symmetry principle. These indices are also shown to be related to FCQSMs which do not conform to the strong version of the FCQSM symmetry principle.

PACS numbers: 03.65.Bz, 02.40.Re, 89.70.+c

1. Introduction

Since the discovery of Shor's quantum factoring algorithm [1] much research has been devoted to the theoretical illumination of the properties and limitations of the quantum computer. Soon after Shor's announcement of his breakthrough discovery, Lloyd [2] identified linear algebraic conditions necessary for quantum computation and briefly discussed the evolution of cyclic quantum computers in this context. More recently, Malyshev [3], Moore *et al* [4], and Gudder [5] have studied quantum grammars and quantum automata. There, Gudder introduced the notion of a quantum state machine (QSM) using a traditional state and transition function formalism that was appropriately modified for quantum mechanical systems. Gudder's QSM is a simple quantum mechanical system which has no input or output and evolves from one state to another in equally spaced time steps.

0305-4470/01/285731+13$30.00

The purpose of this paper is to study the properties of finite cyclic quantum state machines (FCQSMs). These machines are the special class of QSMs which evolve in finite-dimensional Hilbert spaces and return to their initial states after a finite number of equally spaced evolutionary time steps. This research differs from its predecessors in that it is performed from an algebraic topological perspective. In particular, FCQSMs are characterized in terms of the covering spaces that result from the free actions of finite cyclic groups upon odd-dimensional spheres. This characterization enables a natural definition for *FCQSM simulation*, as well as for *simple*, *quotient*, and *split FCQSMs*. In addition, it provides a basis for discussing the symmetries of FCQSMs in terms of the automorphism group for the acting cyclic group (i.e. the FCQSMs *group of dynamical symmetries*) and the group of covering space homeomorphisms (i.e. the FCQSMs *group of process symmetries*). These symmetries are shown to obey a weak version of a FCQSM symmetry principle. It is also shown that not all FCQSMs adhere to a strong version of the FCQSM symmetry principle. Only those machines which obey a strong version of this principle can simulate FCQSMs defined by their groups of dynamical symmetries. Finally, the notions of *simulation complexity* and of *induced topological complexity* are introduced and their relationships to both versions of the FCQSM symmetry principle are determined.

It should be mentioned that due to the range of mathematical concepts used here, it is not practical to make this paper self-contained. Readers who are not familiar with certain of these concepts are invited to consult any of the many excellent mathematics texts which treat them (e.g. [6–11]).

2. A covering space model for FCQSMs

Consider a quantum system with normalized states $|\psi\rangle$ belonging to the $(n+1)$-dimensional Hilbert space $\boldsymbol{C}^{n+1}$ and defined by the set $\mathcal{H} = \left\{|\psi\rangle \in \boldsymbol{C}^{n+1} : \langle\psi|\psi\rangle = 1\right\}$, where $\boldsymbol{C}$ is the set of complex numbers and $n \geqslant 1$. As is well known, the set of states $\mathcal{H}$ is homeomorphic to the $(2n+1)$-dimensional (unit) sphere S^{2n+1}. Let $f : \mathcal{H} \to S^{2n+1}$ be this homeomorphism. Also consider a unitary evolution operator $\hat{U}(\Delta t)$ on $\mathcal{H}$ for a fixed time step Δt such that for some positive integer $m \geqslant 2$ and any $|\psi_0\rangle \in \mathcal{H}$: (i) $\hat{U}^k(\Delta t)|\psi_0\rangle \neq |\psi_0\rangle$ for $1 \leqslant k < m$; and (ii) $\hat{U}^m(\Delta t)|\psi_0\rangle = |\psi_0\rangle$. The sequential application of $\hat{U}(\Delta t)$ m times to $|\psi_0\rangle$ produces the following (closed) cycle of length m in $\mathcal{H}$ which represents the dynamic evolution of a FCQSM in $\mathcal{H}$:

$$|\psi_0\rangle \overset{\hat{U}}{\to} |\psi_1\rangle \overset{\hat{U}}{\to} |\psi_2\rangle \overset{\hat{U}}{\to} \cdots \overset{\hat{U}}{\to} |\psi_{m-1}\rangle \overset{\hat{U}}{\to} |\psi_m\rangle = |\psi_0\rangle. \tag{1}$$

Thus, in general, for $k \geqslant 1$,

$$\hat{U}^k(\Delta t)|\psi_0\rangle = \hat{U}^{k \bmod m}(\Delta t)|\psi_0\rangle = |\psi_{k \bmod m}\rangle.$$

Since $\hat{U}(\Delta t)$ is an element of the group of all unitary transformations on $\mathcal{H}$, it generates the cyclic group $\langle\hat{U}(\Delta t)\rangle$. Because $\hat{U}^m(\Delta t)|\psi_0\rangle = |\psi_0\rangle$ implies $\hat{U}^m(\Delta t) = \hat{I}$, where $\hat{I}$ is the group identity operator, $\langle\hat{U}(\Delta t)\rangle$ is a finite cyclic group of order m. Therefore, we have shown the following:

Lemma 1. *$\langle\hat{U}(\Delta t)\rangle$ is a group that is isomorphic to the cyclic group $\mathbb{Z}_m$ of order m.*

The map $\theta : \langle\hat{U}(\Delta t)\rangle \times \mathcal{H} \to \mathcal{H}$ defined by $\theta\left(\hat{U}^k(\Delta t), |\psi\rangle\right) = \hat{U}^k(\Delta t)|\psi\rangle$, $1 \leqslant k \leqslant m$, obviously describes the dynamics of FCQSMs discussed above. Note that there also exists a map $\varphi = f \circ \theta \circ (\alpha \times f)^{-1}$ such that the diagram

$$\begin{array}{ccc} \langle \hat{U}(\Delta t)\rangle \times \mathcal{H} & \xrightarrow{\theta} & \mathcal{H} \\ \downarrow (\alpha \times f) & & \downarrow f \\ \mathbb{Z}_m \times S^{2n+1} & \xrightarrow{\varphi} & S^{2n+1} \end{array}$$

commutes. Here $\alpha : \langle \hat{U}(\Delta t)\rangle \to \mathbb{Z}_m$ is the group isomorphism of lemma 1. Since α and f are bijective, then so is $(\alpha \times f)$ and its inverse $(\alpha \times f)^{-1}$ exists. Thus, φ is equivalent to θ in the sense that φ also describes the dynamics of FCQSMs because α, f, and $(\alpha \times f)$ merely 'relabel' group elements and states in a manner that preserves the group properties of $\langle \hat{U}(\Delta t)\rangle$ and the topological properties of $\mathcal{H}$. It is therefore useful to characterize the dynamics of FCQSMs using only the properties of φ and refer to each such machine as an (m, n)-FCQSM. Here m and n denote the order of $\mathbb{Z}_m$ and dimension of S^{2n+1}, respectively, and the machine is said to be '*defined by* $\mathbb{Z}_m$' (the role of φ is understood). This is the approach that is followed in this paper.

Lemma 2. *The map φ defines a continuous free left $\mathbb{Z}_m$ -action on S^{2n+1}.*

Proof. This can be shown to be true by first observing that θ defines $\mathcal{H}$ as a $\langle \hat{U}(\Delta t)\rangle$-space because: (1) $\langle \hat{U}(\Delta t)\rangle$ acts (from the left) on $\mathcal{H}$ (i.e. $\hat{U}^m(\Delta t) = \hat{I}$ is the identity element for $\langle \hat{U}(\Delta t)\rangle$ so that $\hat{I}|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$; and for all $|\psi\rangle \in \mathcal{H}$ and $\hat{u}$, $\hat{v} \in \langle \hat{U}(\Delta t)\rangle$, $\hat{u}(\hat{v}|\psi\rangle) = (\hat{u}\hat{v})|\psi\rangle$); and (2) $\theta_{\hat{u}}(|\psi\rangle) \equiv \theta(\hat{u}, |\psi\rangle) = \hat{u}|\psi\rangle$ is continuous for every $\hat{u} \in \langle \hat{U}(\Delta t)\rangle$ since $\mathcal{H}$ is of finite dimension and $\hat{u}$ is a bounded operator. By definition, this action is a free action because $\hat{U}^k(\Delta t)|\psi\rangle \neq |\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$ and all $\hat{U}^k(\Delta t) \in \langle \hat{U}(\Delta t)\rangle$, $1 \leqslant k \leqslant m-1$. Since φ preserves the group and topological properties of θ, it follows that φ also defines S^{2n+1} as a $\mathbb{Z}_m$-space and that the associated action is also a free action. □

Let $S^{2n+1}/\mathbb{Z}_m$ be the quotient space generated by the action φ and $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ be the induced canonical projection. The next theorem is a consequence of an additional property of the action defined by φ.

Theorem 3. *$p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ is a covering.*

Proof. The assertion is true because the action defined by φ is a properly discontinuous action, i.e. $\mathbb{Z}_m$ is a finite group acting freely on the (compact) Hausdorff space S^{2n+1}. □

This result provides a concise topological representation for an (m, n)-FCQSM. Every point in the base space $S^{2n+1}/\mathbb{Z}_m$ represents a process cycle for the associated FCQSM. In addition, the (necessarily continuous) map p provides an equivalence classification of states according to the process cycle to which they belong. The (discrete) fibres $F_x = p^{-1}(x)$ for every process cycle $x \in S^{2n+1}/\mathbb{Z}_m$ are equipotent sets of m points in S^{2n+1} which are the states of the associated cycle given by (1). Observe that $(m, 1)$-FCQSMs are *qubit machines*, i.e. finite cyclic processes in two-dimensional Hilbert spaces. It is noteworthy that base spaces $S^3/\mathbb{Z}_m$ for qubit machines are represented by the classical *Lens spaces* of algebraic topology ([12–14]).

The following properties for $S^{2n+1}/\mathbb{Z}_m$ and S^{2n+1} are noted for future reference: (1) they are path connected spaces; (2) they are connected spaces (because path connected implies connected); and (3) they are locally path connected spaces (since they are both $(2n+1)$-manifolds). Also, it is well established that for $n \geqslant 1$, S^{2n+1} is a simply connected space because it is path connected and $\pi_1(S^{2n+1}) \approx 1$, where $\pi_1(S^{2n+1})$ is the fundamental group for S^{2n+1} (the base point is suppressed for notational simplicity) and 1 denotes the trivial group ('$\approx$' means 'is isomorphic to'). Thus, $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ is a *universal covering*.

3. Quotient machines, split machines, and FCQSM simulations

An (m, n)-FCQSM is said to *simulate* an (m', n)-FCQSM (i.e. the (m, n)-FCQSM cycles emulate those of the (m', n)-FCQSM) if there exists a continuous surjective map $r : S^{2n+1}/\mathbb{Z}_{m'} \to S^{2n+1}/\mathbb{Z}_m$ such that the diagram

$$\begin{array}{ccc} & S^{2n+1} & \\ {}^{q}\swarrow & & \searrow^{p} \\ S^{2n+1}/\mathbb{Z}_{m'} & \xrightarrow{r} & S^{2n+1}/\mathbb{Z}_m \end{array} \qquad (2)$$

commutes.

Theorem 4. *Let $\mathcal{M}$ be a FCQSM defined by $\mathbb{Z}_m$. For every non-trivial subgroup of $\mathbb{Z}_m$ there is a FCQSM that is simulated by $\mathcal{M}$.*

Proof. It is known from the theory of covering spaces that the coverings of a base space are classified by the subgroups of its fundamental group. Since S^{2n+1} is simply connected, then—from the theory of covering spaces—$\pi_1(S^{2n+1}/\mathbb{Z}_m) \approx \mathbb{Z}_m$. If G is a non-trivial subgroup of $\mathbb{Z}_m$, then it must be isomorphic to a cyclic group $\mathbb{Z}_{m'}$ because every non-trivial subgroup of a cyclic group is also a cyclic group. Since $S^{2n+1}/\mathbb{Z}_m$ is connected, locally path connected, and has a universal covering space, there exists a covering $r : S^{2n+1}/\mathbb{Z}_{m'} \to S^{2n+1}/\mathbb{Z}_m$. Because $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ is a universal covering, there also exists an (m', n)-FCQSM defined by $G \approx \mathbb{Z}_{m'}$ which is the unique universal covering $q : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_{m'}$ such that $p = r \circ q$. □

Simulations such as these are called $(m, n)\,/(m', n)$ *simulations* and $\mathcal{M}$ is said to be (m', n) *capable* (obviously every (m, n)-FCQSM is (m, n) capable and therefore simulates itself). As an illustration of this result let $\mathcal{M}$ be a $(4, n)$-FCQSM. This machine is defined by the group $\mathbb{Z}_4$ and $G \approx \mathbb{Z}_2$ is a non-trivial proper subgroup of $\mathbb{Z}_4$. According to theorem 4, $\mathcal{M}$ is $(2, n)$ capable and therefore simulates a $(2, n)$-FCQSM via a $(4, n)\,/\,(2, n)$ simulation so that diagram (2) with $m = 4$ and $m' = 2$ must commute.

The utility of the covering space representation and of diagram (2) can be seen by observing that the fibre $p^{-1}(x)$ for each process $x \in S^{2n+1}/\mathbb{Z}_4$ contains the 4 states in the associated process cycle and the fibre $q^{-1}(y)$ for each process $y \in S^{2n+1}/\mathbb{Z}_2$ contains the 2 states in its process cycle. Since $r : S^{2n+1}/\mathbb{Z}_2 \to S^{2n+1}/\mathbb{Z}_4$ is also a covering, the fibre $r^{-1}(x)$ for each process $x \in S^{2n+1}/\mathbb{Z}_4$ contains $m/m' = 4/2 = 2$ process cycles for the $(2, n)$-FCQSM. The commutativity of diagram (2) identifies the 4 states of these two $(2, n)$-FCQSM process cycles with the same 4 states in the single $(4, n)$-FCQSM process cycle for every process cycle $x \in S^{2n+1}/\mathbb{Z}_4$. Thus, the set of states for each 4 state cycle is partitioned so that two $(2, n)$-FCQSM processes are required to visit the same 4 states that each $(4, n)$-FCQSM visits in a single process cycle. This is the meaning of $(m, n)\,/(m', n)$ simulation: the states of the process cycles for (m, n)-FCQSMs 'geometrically register' the states of the process cycles for (m', n)-FCQSMs such that each (m, n)-FCQSM cycle 'registers' m/m' (m', n)-FCQSM cycles. This notion is easily quantified as a *simulation ratio* σ defined as the group index

$$\sigma = [\mathbb{Z}_m : \mathbb{Z}_{m'}] \equiv \frac{|\mathbb{Z}_m|}{|\mathbb{Z}_{m'}|} = \frac{m}{m'} \qquad (3)$$

where $|G|$ is the order of group G (recall *Lagrange's index theorem*: if $\mathbb{Z}_{m'}$ is a subgroup of $\mathbb{Z}_m$, then m/m' is a positive integer).

Theorem 5. *For every $(m, n)\,/(m', n)$ simulation for which $m \neq m'$ there exists a short exact sequence*

$$1 \to \mathbb{Z}_{m'} \overset{\iota}{\to} \mathbb{Z}_m \overset{\vartheta}{\to} \mathbb{Z}_\sigma \to 1 \qquad (4)$$

where ι is an injective homomorphism and ϑ is a surmorphism.

Proof. The injective homomorphism ι exists because $\mathbb{Z}_{m'}$ is a subgroup of $\mathbb{Z}_m$. Since every subgroup of an Abelian group is a normal subgroup, there exists a surjective homomorphism $\vartheta : \mathbb{Z}_m \to \mathrm{Im}\,\vartheta$ such that $\mathrm{Im}\,\iota = \ker\vartheta$ and $\mathrm{Im}\,\vartheta \approx \mathbb{Z}_m/\mathbb{Z}_{m'}$. But $\mathbb{Z}_m/\mathbb{Z}_{m'} \approx \mathbb{Z}_\sigma$ because the homomorphic image of a cyclic group is also a cyclic group and *Lagrange's index theorem* requires that $|\mathrm{Im}\,\vartheta| = \sigma$ (a positive integer). The sequence $\mathbb{Z}_{m'} \xrightarrow{\iota} \mathbb{Z}_m \xrightarrow{\vartheta} \mathbb{Z}_\sigma$ is exact at $\mathbb{Z}_m$ because $\mathrm{Im}\,\iota = \ker\vartheta$. The attachment of homomorphisms $1 \to \mathbb{Z}_{m'}$ and $\mathbb{Z}_\sigma \to 1$ to this sequence extends the exactness to $\mathbb{Z}_{m'}$ and $\mathbb{Z}_\sigma$, respectively. □

Observe that the quotient group $\mathbb{Z}_m/\mathbb{Z}_{m'} \approx \mathbb{Z}_\sigma$ in short exact sequence (4) defines a (σ, n)-FCQSM *quotient machine* when $m \neq m'$. Such a quotient machine is called the *σ-machine* induced by the simulation.

Corollary 6. *Every $(m, n)/(m', n)$ simulation for which $m \neq m'$ induces a σ-machine.*

Proof. This is a direct consequence of theorem 5. □

An $(m, n)/(m', n)$ simulation for which $m \neq m'$ splits if, and only if, its short exact sequence (4) splits, i.e. there exists a homomorphism $\psi : \mathbb{Z}_\sigma \to \mathbb{Z}_m$ such that $\vartheta \circ \psi = 1_\sigma$, where $1_\sigma : \mathbb{Z}_\sigma \to \mathbb{Z}_\sigma$ is the identity isomorphism. When sequence (4) splits, then $\mathbb{Z}_m \approx \mathbb{Z}_{m'} \oplus \mathbb{Z}_\sigma$, where $\oplus$ denotes 'direct sum of Abelian groups'. An (m, n)-FCQSM which exhibits a split simulation is a *split FCQSM*. The following result identifies a condition which enables FCQSMs to simulate their induced quotient machines.

Theorem 7. *Every split FCQSM simulates an induced σ-machine.*

Proof. Let $\mathcal{M}$ be an (m, n)-FCQSM. If $\mathcal{M}$ is a split machine, then it exhibits a split simulation. Thus, short exact sequence (4) splits and $\mathbb{Z}_m \approx \mathbb{Z}_{m'} \oplus \mathbb{Z}_\sigma$. This implies that $\mathbb{Z}_\sigma \approx \{1\} \oplus \mathbb{Z}_\sigma \subset \mathbb{Z}_m$ (where $\subset$ means 'is a subgroup of' and 1 is the identity element for $\mathbb{Z}_{m'}$). From theorem 4, $\mathcal{M}$ must simulate the machine defined by $\mathbb{Z}_\sigma$. The fact that this machine is an induced σ-machine completes the proof. □

Thus, for a split simulation, there are two commutative diagrams of the form given by diagram (2) which can be joined at their common covering $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ to yield the following single diagram:

$$\begin{array}{ccccc} & & S^{2n+1} & & \\ & \overset{q}{\swarrow} & \downarrow^{p} & \overset{s}{\searrow} & \\ S^{2n+1}/\mathbb{Z}_{m'} & \xrightarrow{r} & S^{2n+1}/\mathbb{Z}_m & \xleftarrow{t} & S^{2n+1}/\mathbb{Z}_\sigma. \end{array} \tag{5}$$

Lemma 8. *Diagram (5) commutes.*

Proof. For any $x \in S^{2n+1}$, $p(x) = r \circ q(x)$ and $p(x) = t \circ s(x)$. Thus, $r \circ q(x) = t \circ s(x)$. □

Indeed, such a commutative diagram exists for any two machines simulated by a FCQSM (it is easy to see that similar more complicated commutative diagrams exist for any subset of machines simulated by a FCQSM).

The next lemma guarantees the existence of FCQSMs which satisfy the condition specified by theorem 7. Let $\|a, b\|$ be the *greatest common divisor* of a and b.

Lemma 9. *Any FCQSM defined by $\mathbb{Z}_m$ for which $m = m'\sigma$ such that $\sigma \neq 1$ and $\|m', \sigma\| = 1$ is a split FCQSM.*

Proof. Let $\mathcal{M}$ be a FCQSM defined by $\mathbb{Z}_m$ with $m = m'\sigma$ such that $\sigma \neq 1$ and $\|m', \sigma\| = 1$. Then (from the theory of finite cyclic groups) $\mathbb{Z}_m \approx \mathbb{Z}_{m'\sigma} \approx \mathbb{Z}_{m'} \oplus \mathbb{Z}_\sigma$ so that $\mathbb{Z}_{m'} \approx \mathbb{Z}_{m'} \oplus \{1\} \subset \mathbb{Z}_m$ (where 1 is the identity element for $\mathbb{Z}_\sigma$). Therefore, $\mathcal{M}$ exhibits an $(m, n)\,/\,(m', n)$ simulation for which $m \neq m'$ so that the associated short exact sequence (4) exists with $\operatorname{Im} \iota = \mathbb{Z}_{m'} \oplus \{1\}$ and $\operatorname{Im} \vartheta = \mathbb{Z}_\sigma \approx \mathbb{Z}_m / \mathbb{Z}_{m'}$. Since exactness requires $\operatorname{Im} \iota = \ker \vartheta$, the homomorphism ϑ in this sequence is such that its restriction $\vartheta\ (\{1\} \oplus \mathbb{Z}_\sigma)$ is an isomorphism upon $\mathbb{Z}_\sigma$ (here 1 is the identity element for $\mathbb{Z}_{m'}$). Let the isomorphism $\omega : \{1\} \oplus \mathbb{Z}_\sigma \to \mathbb{Z}_\sigma$ be this restriction of homomorphism ϑ. Since $\mathbb{Z}_\sigma \approx \{1\} \oplus \mathbb{Z}_\sigma \subset \mathbb{Z}_m$ (so that $\mathcal{M}$ simulates the induced σ-machine), then choose the homomorphism $\psi : \mathbb{Z}_\sigma \to \mathbb{Z}_m$ to be $\psi = \omega^{-1}$. Clearly, this choice yields $\vartheta \circ \psi = \vartheta \circ \omega^{-1} = 1_\sigma$ and the short exact sequence splits. Thus, $\mathcal{M}$ exhibits a split simulation and $\mathcal{M}$ is a split FCQSM. □

Recall that a normal series of a group G is a chain of normal subgroups

$$G \supset G' \supset G'' \supset \cdots \supset 1$$

where the length λ of the series is the number of strict inclusions '$\supset$' (here '$X \supset Y$' means Y is a proper subgroup of X). The series is non-trivial if $\lambda > 1$. An (m_1, n)-FCQSM has a *simulation series* if $\mathbb{Z}_{m_1}$ has a non-trivial normal series (every subgroup of $\mathbb{Z}_{m_1}$ is normal) and the simulation series is said to be defined by $\mathbb{Z}_{m_1}$'s normal series. It is easy to see from theorem 4 that if an (m_1, n)-FCQSM has a simulation series defined by the normal series

$$\mathbb{Z}_{m_1} \supset \mathbb{Z}_{m_2} \supset \cdots \supset \mathbb{Z}_{m_k} \supset 1$$

then there is a commutative diagram given by

$$\begin{array}{ccccccc} & & & S^{2n+1} & & & \\ & \overset{p_1}{\swarrow} & \overset{p_2}{\swarrow} & & \cdots & \overset{p_k}{\searrow} & \\ S^{2n+1}/\mathbb{Z}_{m_1} & \overset{r_2}{\leftarrow} & S^{2n+1}/\mathbb{Z}_{m_2} & \overset{r_3}{\leftarrow} & \cdots & \overset{r_k}{\leftarrow} & S^{2n+1}/\mathbb{Z}_{m_k}. \end{array}$$

Thus, each set of m_i states that comprise the cycles for the machine defined by $\mathbb{Z}_{m_i}$ is partitioned into smaller cycle sets of m_j states by each machine defined by $\mathbb{Z}_{m_j}$, $i + 1 \leqslant j \leqslant k$, and the greater j is the more refined the partition. The simulation ratio sequence associated with this simulation series is the $(k-1)$-tuple $\left(\frac{m_1}{m_2}, \frac{m_2}{m_3}, \ldots, \frac{m_{k-1}}{m_k}\right)$. The $(4, n)\,/\,(2, n)$ simulation discussed above is a simple example of a simulation series where the normal series defined by $\mathbb{Z}_4$ is

$$\mathbb{Z}_4 \supset \mathbb{Z}_2 \supset 1$$

and the simulation ratio sequence is the 1-tuple (2).

Note that any two machines in the simulation series defined by $\mathbb{Z}_{m_j}$ and $\mathbb{Z}_{m_l}$, $1 \leqslant j < l \leqslant k$, has a commutative diagram of the form of diagram (2) because $r : S^{2n+1}/\mathbb{Z}_{m_l} \to S^{2n+1}/\mathbb{Z}_{m_j}$ with $r = r_{j+1} \circ r_{j+2} \circ \cdots \circ r_l$ is a covering such that $p_j = r \circ p_l$. Similarly, a diagram analogous to that of diagram (5) also exists for a simulation series.

4. Dynamical and process symmetries for FCQSMs

This section is concerned with identifying algebraic representations for the *dynamical* and *process symmetries* associated with FCQSMs. In particular, it is assumed that the 'dynamics' of an (m, n)-FCQSM are abstractly represented by the group $\mathbb{Z}_m$ and that the 'global result of the associated processing performed by these dynamics' is abstractly represented by the covering $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$. It is then reasonable to use the automorphisms of $\mathbb{Z}_m$ and the associated covering space automorphisms as distinct dynamical and process symmetries, respectively. The two groups generated by these automorphisms provide useful algebraic descriptions of the dynamical and process symmetries for FCQSMs. The significance of their inter-relationship is discussed in the next section within the context of a FCQSM symmetry principle.

Consider first the dynamical symmetry and recall that a group automorphism for $\mathbb{Z}_m$ is an isomorphism $\beta : \mathbb{Z}_m \to \mathbb{Z}_m$. Let each such isomorphism represent a distinct dynamical symmetry for an (m, n)-FCQSM. The set of all such isomorphisms under the binary operation of composition is the group of dynamical symmetries $\text{Aut}(\mathbb{Z}_m)$ for the machine and $|\text{Aut}(\mathbb{Z}_m)|$ is its order. Although $\text{Aut}(G)$ is not generally known for an arbitrary group G, certain properties for $\text{Aut}(\mathbb{Z}_m)$ are well established.The fundamental properties of $\text{Aut}(\mathbb{Z}_m)$ that are useful for the discussions below are cited here for convenience as the following theorems:

Theorem 10. $\text{Aut}(\mathbb{Z}_m)$ *is an Abelian group of order* $\phi(m)$*, where* ϕ *is the Euler totient.*

The *Euler totient* is defined as: $\phi(1) = 1$ and for $m > 1$, then $\phi(m)$ is the number of integers ℓ such that $1 \leqslant \ell < m$ and $\|\ell, m\| = 1$.

Theorem 11. *For* $m > 2$, $|\text{Aut}(\mathbb{Z}_m)|$ *is never odd.*

Theorem 12. *If* $m = 2^k$*, then* $\text{Aut}(\mathbb{Z}_m) \approx \begin{cases} 1 & \text{when} \quad k = 1 \\ \mathbb{Z}_2 & \text{when} \quad k = 2. \end{cases}$

Theorem 13. *If* m *is an odd prime, then* $\text{Aut}(\mathbb{Z}_m) \approx \mathbb{Z}_{m-1}$.

An automorphism for the covering $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ is a homeomorphism $\eta : S^{2n+1} \to S^{2n+1}$ such that the diagram

$$\begin{array}{ccc} S^{2n+1} & \xrightarrow{\eta} & S^{2n+1} \\ p \searrow & & \swarrow p \\ & S^{2n+1}/\mathbb{Z}_m & \end{array}$$

commutes. Hence, η determines an immunity to change in the topological structure of the covering and therefore represents a distinct symmetry for the covering. Let each such homeomorphism represent a distinct process symmetry for the FCQSM associated with the covering. The set of all such homeomorphisms under the binary operation of composition is the group of process symmetries $\text{Cov}(p)$ for the associated FCQSM and $|\text{Cov}(p)|$ is its order.

Unlike the case for the group of dynamical symmetries, the group of process symmetries can be determined directly from the general theory of covering spaces. It is well known from covering space theory that if $\gamma : \tilde{X} \to X$ is a covering such that $\tilde{X}$ is simply connected and locally path connected, then $\text{Cov}(\gamma) \approx \pi_1(X)$, where $\pi_1(X)$ is the fundamental group for the space X (the base point in X is suppressed in $\pi_1(X)$ for notational simplicity). Since $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ is a covering and S^{2n+1} has these properties, then $\text{Cov}(p) \approx \mathbb{Z}_m$ because—as can also be ascertained from covering space theory—$\pi_1\left(S^{2n+1}/\mathbb{Z}_m\right) \approx \mathbb{Z}_m$. The next theorem is an immediate consequence of this.

Theorem 14. *Every FCQSM simulates its group of process symmetries.*

Proof. The assertion is true because $\text{Cov}(p) \approx \mathbb{Z}_m$ and every FCQSM simulates itself. □

5. Symmetry principles for FCQSMs

Liberty is taken in this section to devise two versions of a *FCQSM symmetry principle*. The simpler version which asserts that 'a process is more symmetric than the dynamics which performs it' is the weak version of the principle. The more precise statement that 'the group of dynamical symmetries for a FCQSM is isomorphic to a subgroup of the group of process symmetries for the processes produced by the FCQSM' is the strong version of the principle. Note that the weak version can be interpreted as a statement only about the relative cardinalities of the sets of distinct dynamical and process symmetries. The strong version is a symmetry conservation principle for FCQSMs which asserts that a faithful copy of the group of dynamical symmetries is contained within the group of process symmetries. If a FCQSM adheres to the weak (strong) version of the symmetry principle, then it is *weakly (strongly) symmetric*.

Since $\mathrm{Cov}(p) \approx \mathbb{Z}_m$, then $|\mathrm{Cov}\,(p)| = m$. Also, from theorem 10, $|\mathrm{Aut}\,(\mathbb{Z}_m)| = \phi\,(m) < m$ for $m \geqslant 2$ so that the following order relation is true for any (m, n)-FCQSM:

$$|\mathrm{Aut}\,(\mathbb{Z}_m)| < |\mathrm{Cov}\,(p)| \qquad m \geqslant 2. \tag{6}$$

Thus, the number of dynamical symmetries is always exceeded by the number of process symmetries. This means that every (m, n)-FCQSM conforms to our weak version of the symmetry principle and we have proven that:

Theorem 15. *Every (m, n)-FCQSM is weakly symmetric.*

An obvious consequence of this result is the fact that the group of dynamical symmetries for a FCQSM is never isomorphic to its group of process symmetries.

Application of the strong version of the symmetry principle demands that a strongly symmetric (m, n)-FCQSM satisfies the requirement

$$\mathrm{Aut}\,(\mathbb{Z}_m) \approx S \subset \mathrm{Cov}\,(p) \approx \mathbb{Z}_m \tag{7}$$

(where '$\subset$' means 'is a subgroup of'). If $\mathrm{Aut}(\mathbb{Z}_m) \approx 1$ for some (m, n)-FCQSM $\mathcal{M}$, then $\mathcal{M}$ clearly satisfies requirement (7) and is therefore strongly symmetric. In this case, $\mathcal{M}$ is said to be *dynamically trivial*. Otherwise, $\mathcal{M}$ is dynamically non-trivial.

Lemma 16. *An (m, n)-FCQSM is dynamically trivial if, and only if, $m = 2$.*

Proof. ($\Rightarrow$) Suppose an (m, n)-FCQSM is dynamically trivial. Then $\mathrm{Aut}(\mathbb{Z}_m) \approx 1$ and $|\mathrm{Aut}\,(\mathbb{Z}_m)| = 1$. This means that $m \leqslant 2$ because $|\mathrm{Aut}\,(\mathbb{Z}_m)|$ is never odd for $m > 2$ (theorem 11). Since there are no FCQSMs with $m < 2$, then $m = 2$. ($\Leftarrow$) Let $m = 2$. Then, $\mathrm{Aut}(\mathbb{Z}_2) \approx 1$ (theorem 12) so that all $(2, n)$-FCQSMs are dynamically trivial. □

Provided that $\mathrm{Aut}(\mathbb{Z}_m)$ is not isomorphic to the trivial group, when requirement (7) prevails $\mathrm{Aut}(\mathbb{Z}_m)$ must be isomorphic to a cyclic subgroup of $\mathrm{Cov}(p)$ of order $\phi\,(m)$ (theorem 10). In this case, $\mathrm{Aut}(\mathbb{Z}_m) \approx \mathbb{Z}_{\phi(m)}$ defines a $(\phi\,(m)\,, n)$-FCQSM which is simulated by the associated (m, n)-FCQSM (theorem 4) with a simulation ratio defined by the group index

$$[\mathrm{Cov}\,(p) : \mathrm{Aut}\,(\mathbb{Z}_m)] \equiv \frac{|\mathrm{Cov}\,(p)|}{|\mathrm{Aut}\,(\mathbb{Z}_m)|} = \frac{m}{\phi\,(m)}. \tag{8}$$

This special machine defined by $\mathrm{Aut}(\mathbb{Z}_m)$ is referred to as the *ϕ-machine* associated with the (m, n)-FCQSM and we have shown that:

Theorem 17. *A dynamically non-trivial strongly symmetric FCQSM simulates its associated ϕ-machine.*

Thus, the processing performed by strongly symmetric FCQSMs not only conserves their dynamical symmetries, but also 'geometrically registers'—or 'coordinatizes'—these symmetries as states in their process cycles. It is easy to see that the previously discussed $(4, n)$-FCQSMs are dynamically non-trivial strongly symmetric machines. Dynamical non-triviality follows from lemma 16. Since $\mathrm{Aut}(\mathbb{Z}_4) \approx \mathbb{Z}_{\phi(4)} = \mathbb{Z}_2 \subset \mathbb{Z}_4 \approx \mathrm{Cov}\,(p)$ (theorem 12 for $k = 2$), these machines are strongly symmetric and therefore simulate their associated ϕ-machines. As discussed above, each of two pairs of states in every 4 state cycle of the $(4, n)$-FCQSMs simulates (i.e. 'geometrically registers') the dynamical symmetry groups of these machines.

When condition (7) is not satisfied for some FCQSM, then that FCQSM is clearly not strongly symmetric and—by virtue of theorem 15—is said to be *strictly weak*. The next theorem relates ϕ-machine simulation to strictly weak machines and is stated here for the sake of completeness (since it follows directly from the contrapositive of theorem 17, it is stated without proof).

Theorem 18. *If a dynamically non-trivial FCQSM is not capable of simulating its associated ϕ-machine, then it is strictly weak.*

The existence of strictly weak machines is guaranteed by the following theorem.

Theorem 19. *Every (m, n)-FCQSM for which m is odd is strictly weak.*

Proof. If m is odd, then $m > 2$ so that $|\mathrm{Aut}\,(\mathbb{Z}_m)|$ is even (theorem 11) and does not evenly divide m. Thus, $\mathrm{Aut}(\mathbb{Z}_m)$ cannot be isomorphic to a subgroup of $\mathbb{Z}_m \approx \mathrm{Cov}\,(p)$ for the covering $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ and condition (7) cannot be satisfied. □

As an illustration of theorem 19, let $m = 3$ so that the cyclic group $\mathbb{Z}_3$ defines a $(3, n)$-FCQSM with $\mathrm{Cov}(p) \approx \mathbb{Z}_3$. From theorem 13 when $m = 3$, $\mathrm{Aut}(\mathbb{Z}_3) \approx \mathbb{Z}_2$. Since $|\mathrm{Aut}\,(\mathbb{Z}_3)| = 2$ does not evenly divide 3, $\mathrm{Aut}(\mathbb{Z}_3) \approx \mathbb{Z}_2$ cannot be isomorphic to a subgroup of $\mathrm{Cov}(p) \approx \mathbb{Z}_3$. Thus, all $(3, n)$-FCQSMs cannot simulate their ϕ-machines and are therefore strictly weak, i.e. they are only weakly symmetric since $|\mathrm{Aut}\,(\mathbb{Z}_3)| = 2 < 3 = |\mathrm{Cov}\,(p)|$.

The results of this section clearly show that the implication

$$\text{strong FCQSM symmetry} \Rightarrow \text{weak FCQSM symmetry}$$

is valid, but that—in general—its logical converse is not. Indeed, since strictly weak FCQSMs exist, the set of strongly symmetric FCQSMs is properly contained in the set of all (weakly symmetric) FCQSMs.

6. The processing complexity of FCQSMs

This section is concerned with the examination of two intuitively derived quantities which measure the complexity of the processing performed by a FCQSM. The first of these is the *simulation complexity index* $\Omega_{m,n}$ for an (m, n)-FCQSM. This index is a 'capability quantification'—i.e. it is the number of FCQSMs that can be simulated by an (m, n)-FCQSM-and is defined as the number of distinct non-unit factors of the integer m (the subscript n is retained for the sake of notational consistency). Clearly, $\Omega_{m,n}$ counts (up to isomorphism) the number of non-trivial subgroups of $\mathbb{Z}_m$. For example, $\Omega_{10,n} = 3$ because the non-unit factors of 10 are 10, 5, and 2 which correspond to the subgroups $\mathbb{Z}_{10}$, $\mathbb{Z}_5$, and $\mathbb{Z}_2$, respectively. These groups define the machines that a $(10, n)$-FCQSM can simulate.

The larger the $\Omega_{m,n}$ value is for a FCQSM then the more complex the machine is (in the sense of its total simulation capability). An (m, n)-FCQSM which is only (m, n) capable is a *simple* FCQSM and $\Omega_{m,n} = 1$ in this case. Such machines are identified by the following theorem.

Theorem 20. *An (m, n)-FCQSM is simple if, and only if, m is prime.*

Proof. ($\Rightarrow$) If $\mathcal{M}$ is a simple (m, n)-FCQSM, then $\mathbb{Z}_m$ has no non-trivial proper subgroups (or else $\mathcal{M}$ would be (m', n) capable for $m' \neq m$) so that 1 and m are the only divisors of m which yield a positive integer group index. Therefore, m is prime. ($\Leftarrow$) If m is prime, then $\mathbb{Z}_m$ has no non-trivial proper subgroups since 1 and m are the only divisors of m. Thus, $\mathcal{M}$ is only (m, n) capable and is a simple FCQSM. □

Although it is not known how to calculate $\Omega_{m,n}$ directly from m, its value can be bounded by recalling that the Euler totient counts the number of integers $1 \leqslant \ell < m$ such that $\|\ell, m\| = 1$. This implies that $m - \phi(m)$ is the maximum number of (non-unit) positive integers $1 < \ell' \leqslant m$ that could divide m so that

$$\Omega_{m,n} \leqslant m - \phi(m) \qquad m \geqslant 2. \tag{9}$$

The use of '$\leqslant$' instead of '$<$' in this inequality is easily shown to be valid by applying it to simple (m, n)-FCQSMs. For this case, it is required by the last theorem that m be prime. Then $\phi(m) = m - 1$ so that inequality (9) yields $\Omega_{m,n} = 1$ (since its value can never be non-positive). The order relation stated as the following lemma will be useful for providing a refined statement of the weak version of the FCQSM symmetry principle.

Lemma 21. $|\mathrm{Aut}(\mathbb{Z}_m)| \leqslant m - \Omega_{m,n} < |\mathrm{Cov}(p)|$.

Proof. Rearranging inequality (9) and using the fact that $|\mathrm{Aut}(\mathbb{Z}_m)| = \phi(m)$ yields

$$|\mathrm{Aut}(\mathbb{Z}_m)| \leqslant m - \Omega_{m,n}.$$

Also, since $1 \leqslant \Omega_{m,n} < m$, then $m - \Omega_{m,n} < m = |\mathrm{Cov}(p)|$. □

In addition to $\Omega_{m,n}$, the algebraic properties of the topologies of the spaces in the covering $p : S^{2n+1} \to S^{2n+1}/\mathbb{Z}_m$ can be used to define the *induced topological complexity index* $\Gamma_{m,n}$ for the (m, n)-FCQSM associated with the covering. This simple index provides a quantification of the topological change induced in S^{2n+1} by the action of the associated (m, n)-FCQSM and is defined as the sum

$$\Gamma_{m,n} = \sum_{j=1}^{\infty} \left\{ \left|\pi_j\left(S^{2n+1}/\mathbb{Z}_m\right)\right| - \left|\pi_j\left(S^{2n+1}\right)\right| \right\}. \tag{10}$$

Here $\pi_j(X)$ is the jth homotopy group for the topological space X (note again that the basepoint in X is suppressed for notational simplicity) and $\left|\pi_j(X)\right|$ is its order. Because $\pi_j(X)$ is an algebraic statement about the $(j+1)$-dimensional 'holes' in space X, then—in a sense—$\sum_{j=1}^{\infty} \left|\pi_j(X)\right|$ is a quantification of the topological complexity of X. Therefore, intuitively, $\Gamma_{m,n}$ is the difference between the complexity induced by the action of an (m, n)-FCQSM (as reflected by the topology of the 'processed' base space $S^{2n+1}/\mathbb{Z}_m$) and the complexity of the 'unprocessed' space of states S^{2n+1}.

Since every covering space is a locally trivial bundle with discrete fibre, it is also a weak fibration. Therefore, the following long exact homotopy sequence exists for every (m, n)-FCQSM:

$$\cdots \to \pi_{j+1}\left(S^{2n+1}/\mathbb{Z}_m\right) \to \pi_j(F) \to \pi_j\left(S^{2n+1}\right) \to \pi_j\left(S^{2n+1}/\mathbb{Z}_m\right) \to \pi_{j-1}(F) \to \cdots \tag{11}$$

where the arrows denote group homomorphisms. As before, the basepoint has been suppressed and F is the fibre for any basepoint (because all fibres are homeomorphic discrete spaces). This long exact sequence can be used to evaluate equation (10) by first noting that since F

is discrete, then, for $j \geqslant 1$, $\pi_j(F)$ is isomorphic to the trivial group, denoted $\pi_j(F) \approx 1$. Substituting this fact into sequence (11) yields the exact sequences

$$1 \to \pi_j\left(S^{2n+1}\right) \to \pi_j\left(S^{2n+1}/\mathbb{Z}_m\right) \to 1 \qquad j \geqslant 2.$$

The exactness of these sequences implies that $\pi_j\left(S^{2n+1}\right) \approx \pi_j\left(S^{2n+1}/\mathbb{Z}_m\right)$ when $j \geqslant 2$. Since isomorphic groups have equal orders, equation (10) reduces to an expression involving only the fundamental groups of the spaces in the covering:

$$\Gamma_{m,n} = \left|\pi_1\left(S^{2n+1}/\mathbb{Z}_m\right)\right| - \left|\pi_1\left(S^{2n+1}\right)\right|.$$

Since $\pi_1\left(S^{2n+1}\right) \approx 1$ for $n \geqslant 1$ and $\pi_1\left(S^{2n+1}/\mathbb{Z}_m\right) \approx \mathbb{Z}_m$ (as noted above), then the last equation gives the final simple result that

$$\Gamma_{m,n} = m - 1. \tag{12}$$

Note that the right-hand side of this equation is independent of the Hilbert space dimension (the subscript n is retained on the left-hand side for the sake of notational consistency) and that the induced topological complexity increases linearly only with the number of distinct states m in a process cycle. Also, observe from equation (12) that the induced topological complexity index is always positively valued for all (m, n)-FCQSMs because $m \geqslant 2$ so that $\Gamma_{m,n} \geqslant 1$.

The following lemma relates the induced topological complexity index to strictly weak FCQSMs.

Lemma 22. *Every dynamically non-trivial (m, n)-FCQSM for which $|\mathrm{Aut}(\mathbb{Z}_m)| = \Gamma_{m,n}$ is strictly weak.*

Proof. Let $\mathcal{M}$ be a dynamically non-trivial (m, n)-FCQSM such that $|\mathrm{Aut}(\mathbb{Z}_m)| = \Gamma_{m,n}$. Since $m > 2$, then $|\mathrm{Aut}(\mathbb{Z}_m)| = \Gamma_{m,n} = m - 1$ is even (theorem 11). Thus, m is odd so that $\mathcal{M}$ is strictly weak (theorem 19). □

A useful relationship between simple FCQSMs and the topological complexity index is identified in the next lemma.

Lemma 23. $|\mathrm{Aut}(\mathbb{Z}_m)| = \Gamma_{m,n}$ *if, and only if, m is prime.*

Proof. $(\Rightarrow)$ Let $|\mathrm{Aut}(\mathbb{Z}_m)| = \Gamma_{m,n} = m-1$, where $m \geqslant 2$. Thus, $\phi(m) = m-1$ (theorem 10). This implies that $\|\ell, m\| = 1$ for every $1 \leqslant \ell < m$ so that m must be a prime. $(\Leftarrow)$ Let m be a prime. If $m = 2$, then $|\mathrm{Aut}(\mathbb{Z}_2)| = 2 - 1 = 1 = \Gamma_{2,n}$ (theorem 12). If $m > 2$, then $|\mathrm{Aut}(\mathbb{Z}_m)| = |\mathbb{Z}_{m-1}| = m - 1 = \Gamma_{m,n}$ (theorem 13). □

These last two results show that not only are all dynamically non-trivial simple FCQSMs strictly weak, but also that simple FCQSMs are the only class of FCQSMs which satisfy $|\mathrm{Aut}(\mathbb{Z}_m)| = \Gamma_{m,n}$. In addition, lemmas 23 and 21 can be used to refine the weak version of the FCQSM symmetry principle by including the simulation complexity index and the induced topological complexity index as achievable maximum upper bounds (relative to m) upon the number of distinct dynamical symmetries. This refinement is stated as the final theorem of this paper.

Theorem 24 (Refined weak symmetry principle for FCQSMs). *Every (m, n)-FCQSM conforms to the ordering*

$$|\mathrm{Aut}(\mathbb{Z}_m)| \leqslant m - \Omega_{m,n} \leqslant \Gamma_{m,n} < |\mathrm{Cov}(p)|.$$

Strict equalities hold if, and only if, the machine is simple.

Proof. Since $\Gamma_{m,n} = m - 1$ and $|\mathrm{Cov}\,(p)| = m$, then weak symmetry (inequality (6)) requires that $|\mathrm{Aut}\,(\mathbb{Z}_m)| < \Gamma_{m,n} + 1$ or $|\mathrm{Aut}\,(\mathbb{Z}_m)| - 1 < \Gamma_{m,n}$ so that

$$|\mathrm{Aut}\,(\mathbb{Z}_m)| - 1 < \Gamma_{m,n} < |\mathrm{Cov}\,(p)| \qquad m \geqslant 2.$$

This means that: (i) $|\mathrm{Aut}\,(\mathbb{Z}_m)| < \Gamma_{m,n}$; (ii) $|\mathrm{Aut}\,(\mathbb{Z}_m)| = \Gamma_{m,n}$; or (iii) $\Gamma_{m,n} < |\mathrm{Aut}\,(\mathbb{Z}_m)| \leqslant |\mathrm{Cov}\,(p)|$. Possibility (iii) cannot be true because $|\mathrm{Cov}\,(p)| - \Gamma_{m,n} = 1$ and weak symmetry requires $|\mathrm{Aut}\,(\mathbb{Z}_m)| < |\mathrm{Cov}\,(p)|$. The fact that item (i) is possible (because $\phi\,(m) < m - 1$ can be true) and item (ii) is possible (lemma 23) yields the ordering relation

$$|\mathrm{Aut}\,(\mathbb{Z}_m)| \leqslant \Gamma_{m,n} < |\mathrm{Cov}\,(p)|\,.$$

Observing that $1 \leqslant \Omega_{m,n} < m$ implies that $m - \Omega_{m,n} \leqslant \Gamma_{m,n}$ allows lemma 21 to be used to form the desired ordering. Consider now the following proof of the remaining bi-conditional statement: ($\Rightarrow$) Let $|\mathrm{Aut}\,(\mathbb{Z}_m)| = m - \Omega_{m,n} = \Gamma_{m,n} = m - 1$. This implies that m is prime (lemma 23) and that $\Omega_{m,n} = 1$. Thus, from theorem 20 and the definition of $\Omega_{m,n}$ the associated FCQSM must be simple. ($\Leftarrow$) Let the machine be simple. Then—by definition—$\Omega_{m,n} = 1$ and m must be prime (theorem 20) so that $m - \Omega_{m,n} = m - 1 = \Gamma_{m,n}$. The fact that theorem 23 requires $|\mathrm{Aut}\,(\mathbb{Z}_m)| = \Gamma_{m,n}$ completes the proof. □

7. Concluding remarks

This research has investigated the properties of FCQSMs from an algebraic topological perspective. It has demonstrated that a covering space characterization for all such machines can be obtained using this approach and that this characterization is useful for defining and understanding the notion of FCQSM simulation. This perspective also enabled the establishment of: (1) an order relation which bounds the number of distinct dynamical symmetries for a FCQSM by the values of two complexity indices which are determined entirely by the group structure and topological properties associated with the machine; (2) a symmetry conservation principle for FCQSMs; and (3) a relationship between the violation of this symmetry conservation principle and the two machine complexity indices.

This paper suggests additional theoretical questions related to quantum information processing that might be studied from a similar algebraic topological perspective. These questions include the following: (i) what are the properties of finite QSMs described by other group actions upon odd-dimensional spheres?; (ii) what are the properties of infinite cyclic QSMs?; (iii) is the categorical notion of 'free Abelian group' related to universal quantum computation?; (iv) is there an analogous algebraic topological representation for universal quantum computation?; and—if so—(v) can it be shown that all classical Turing machines can be embedded in this representation?

Acknowledgment

This work was supported in part by a Naval Surface Warfare Center Independent Research Grant.

References

[1] Shor P W 1994 Algorithms for quantum computation: discrete logarithms and factoring *Proc. 35th Symp. on Foundations of Computer Science* pp 124–34
[2] Lloyd S 1994 *J. Mod. Opt.* **41** 2503–20
[3] Malyshev V A 2000 *J. Math. Phys.* **41** 4508–20

[4] Moore C and Crutchfield J P 1997 Quantum automata and quantum grammars *Santa Fe Institute Technical Report* 97-07-062
[5] Gudder S 2000 *Found. Phys.* **30** 301–19
[6] Rotman J J 1988 *An Introduction to Algebraic Topology (Graduate Texts in Mathematics)* (New York: Springer)
[7] Rotman J J 1984 *An Introduction to the Theory of Groups* 3rd edn (Newton, MA: Allyn and Bacon)
[8] Kosniowski C 1980 *A First Course in Algebraic Topology* (Cambridge: Cambridge University Press)
[9] Munkres J R 1984 *Elements of Algebraic Topology* (Menlo Park, CA: Addison-Wesley)
[10] Dubrovin B A, Fomenko A T and Novikov S P 1985 *Modern Geometry-Methods and Applications: Part II. The Geometry and Topology of Manifolds* (New York: Springer)
[11] Geroch R 1985 *Mathematical Physics (Chicago Lectures in Physics)* (Chicago: The University of Chicago Press)
[12] Reidemeister K 1935 *Abh. Math. Semin. Univ. Hamburg* **11** 102–9
[13] Tietze H 1908 *Mh. Math. Phys.* **19** 1–118
[14] Whitehead J H C 1941 *Ann. Math.* **42** 1197–239