TEXAS STATE UNIVERSITY SAN MARCOS

Department of Computer Science
San Marcos, TX 78666

Report Number TXSTATE-CS-TR-2005-5

Introduction to Quantum Message Space

R. D. Ogden

2005-11-02

Introduction to Quantum Message Space

Technical Report #2, Quantum Computation Study Group,
Department of Computer Science and Engineering,
Texas State University at San Marcos

Prepared by R. D. Ogden
ro01@txstate.edu
Revised November 2, 2005

Abstract

According to Landauer's Principle the annihilation (and presumably the creation) of one bit costs at least kT ln(2) much energy. This seems to imply that serial bit transmission is impossible; however, a complete quantum theory of communication should permit Alice to send Bob a message of arbitrary length, unknown to Bob in advance. One is lead to consider the Hilbert state space $\sum_{n=0}^{\infty}\left(\mathbb{C}^2\right)^{\otimes n}$, where $\mathbb{C}^2$ is conventional qubit space, but the obvious operator which appends a 0 (say) to a string x (i.e., sends $|\ x\rangle$ to $|\ x0\rangle$) is no longer unitary on this space because it is not onto . The remedy proposed in this report is to use ℓ^2 $(FG(2))$ for the quantum message space (QMS), where FG (2) is the free group on the bit symbols {0,1}; the "anti-bits" 0^{-1} and 1^{-1}, represented by 2 and 3 respectively, are introduced, and thus the conservation laws are retained. After developing the basic QMS constructs we describe the message-length observable N, noting that most quantum operators used hitherto in quantum information theory commute with N. In QMS the operation which appends a string to a message is implemented by a right translation operator. We review the harmonic analysis on the free group FG (2) and the decomposition of the right regular representation into irreducible representations of FG (2). This decomposition is implemented by the spectral analysis of the operator A, which is left convolution by $(|\ 0\rangle+|\ 1\rangle+|\ 2\rangle+|\ 3\rangle)/\ 4$. This analysis yields a family of projectors which commute with the extended qubit operations implemented by the right regular representation and therefore can be used to construct quantum operators for quantum computation on QMS.

Index Terms–Quantum information theory, harmonic analysis, free group, Eigenvalues and eigenfunctions, Hilbert spaces, Message systems, Operators (mathematics).

I. INTRODUCTION

In classical communication theory a binary-encoded message source generates bit strings according to the underlying source statistics, those of an ergodic stochastic process. In general, messages of arbitrary length may be generated. Moreover, in classical communication theory it is convenient to conceive of the bits in a message being generated serially one at a time.
In much of quantum computation theory the message length is assumed known; i.e., N-qubits are studied with N, the number of qubits, fixed. The underlying Hilbert space is then a 2^N dimensional complex space with a complete orthogonal set of normalized pure states indexed by the strings of length N. Furthermore, it is often assumed that the "noise" in the quantum communication channel preserves N, but it has been argued that there is no physical necessity for this.
In contrast, quantum message space permits strings of arbitrary length; it contains an orthonormal list (δ_a) of orthonormal state vectors indexed by $a \in 2^*$ = the set of *all* bit strings. The message is then an observable whose value a is a (possibly empty) bit string. If ϱ is the *a priori* state before measurement, the probability that the message received equals a is $\langle \delta_a \mid \varrho(\delta_a) \rangle / \mathrm{Trace}(\varrho)$. When a measurement is made with result a (i.e., a quantum message whose value is a is received), the system state becomes $\langle \delta_a | \varrho(\delta_a) \rangle\ \delta_a \otimes \delta_a^*$, where the operator $\alpha \otimes \beta^*$ is defined by $\alpha \otimes \beta^*(\varphi) = \langle \beta \mid \varphi \rangle\ \alpha$. Let $\mathcal{H}^+$ = Hilbert space generated by $(\delta_a)_{a \in 2^*}$. A state ϱ supported by $\mathcal{H}^+$ represents a "positive" message source; i.e., one whose value is a (possibly empty) string of *0*s and *1*s.
The space $\mathcal{H}^+$ would seem to be a natural candidate for a quantum state space which allows messages of arbitrary length, but it leaves no provision for bit creation. The obvious process of bit creation by appending is implemented by the operator V_b which maps δ_a to δ_{ab}, where $b \in 2$ is a bit; e.g., $V_0(\delta_{001}) = \delta_{0010}$. V_b leaves $\mathcal{H}^+$ invariant and acts as an isometry thereon, but this map is not onto, thence it is not unitary. This is consistent with Landauer's principle[NG]: since at least kT *ln(2)* much energy is required to erase a bit, presumably at least that much energy is needed to create a new bit. Thus it would seem that serial bit generation is not possible in a closed system.

The operations of appending and deleting bits evoke the creation operators (e.g., V_b) and annihilation operators (V_b^*) of quantum field theory. The formal analogues of momentum and position would be the real and imaginary parts of V_b. The empty string is sort of like the vacuum from which everything is created. But the (anti-)commutation relations are disappointing and trivial; with hindsight this is so because 2^* is a free semi-group.

But there is a precedent in atomic physics for evading conservation laws by postulating a new "particle" with the necessary properties for balancing the equations; in such a way the positron and neutrino were first proposed, by Pauli/Dirac and E. Fermi, and sure enough physical evidence turned up that

seemed to confirm their reality, which today is an established fact of physics. In this paper anti-qubits are proposed, which do make the appending of a bit a unitary operation, balanced by effects on anti-qubits and mixtures. But in this case we are ignorant of any physical basis in new particles or fields, but of new *relations* within infinite-dimensional Hilbert spaces suitable for modelling a quantum message space which permits bit generation and messages of arbitrary length unknown in advance.
The basic references for quantum mechanics used in this report are Mackey, "Mathematical Foundations of Quantum Mechanics" [Ma] and the standard reference of Nielsen and Chaung, "Quantum Computation and Quantum Information" [NG]. [PS] is a suggested reference for quantum field theory.
Special thanks to Carl Brannen for a close critical reading and various helpful suggestions.

II. THE FREE GROUP FG(2): ENCODINGS AND CONVENTIONS

A. Strings

2^n refers to the set of integers {0,1,2,3,...,2^n-1}, or the set of bit strings of length n, or the simply the number 2^n, depending on the context. The set of all bit strings $2^* = \cup_{n\geq 0} 2^n$ forms a semigroup with identity under the operation of string concatenation.
When we complete 2^* as a group we get the free group with two generators, *FG(2)* . We will use *0* and *1* for the group generators, and denote 0^{-1} and 1^{-1} by *2* and *3* respectively. The set of generators and their inverses is the alphabet for the free group, so for *FG(2)* this shall be 4 = {0,1,2,3} . 0 and 1 are bits that make up positive messages; 2 and 3 (in this context) are the *anti-bit* values. The free group identity is the empty string Λ . The inverse map on 4 is the map *inv:* $0 \to 2$, $1 \to 3$, $2 \to 0$, $3 \to 1$, $a \to a^{-1}$.
In a free group there are no simplifications possible except that of removing digrams consisting of an alphabet symbol and its inverse: aa^{-1} . In the present context this means that any of the four substrings *02,13,20,31* may be removed from an expression representing a free group element. A string in 4^* which does not contain one of these four substrings is a *reduced word.*

B. The Free Group

The free group on two elements *FG(2)* is the subset of 4^* consisting of all reduced words. The group operation is string concatenation followed by reduction, Λ is the identity element and the inverse of the reduced word is the string

of the inverse alphabet symbols, in reverse order.
$FG(2)_n = FG(2) \cap 4^n$ = all reduced words of length n. The group operations on *FG(2)* are simply
$x \cdot y = reduce\ (x\ y)$. If $x = x_0 \ldots x_{n-1}$ then x^{-1}=inv(x_{n-1})...inv(x_0) .
Example: 03221211·3300123=032210123=$(103230012)^{-1}$.
The mathematical significance of the free group *FG(2)* is given any group G and pair of elements *a* and *b*, then there is a unique homomorphism from *FG(2)* onto the subgroup of G generated by {*a*,*b*} which sends 0 to *a* and 1 to *b*. The significance for quantum communication theory may be due to its being the natural mathematical structure which allows for bit generation as a unitary operation.
Note we have the inclusions $2^n \subset FG(2)_n \subset 4^n$.

C. Definition Of Quantum Message Space (QMS)

A quantum message space is a Hilbert space $\mathcal{H}$ together with an orthonormal basis $(\delta_a)_{a \in FG(2)}$ indexed by the elements of the free group $FG(2)$ on the two bit values {0,1}. The basis induces a unique atomic spectral measure M mapping subsets $A \subseteq FG(2)$ to orthogonal projectors:

$$M(A) = \sum_{a \in A} \delta_a \otimes \delta_a^*, \ A \subseteq \mathrm{FG}(2) \tag{1}$$

The elements of $FG(2)$, the reduced strings, are the outcome of measurements of the discrete observable determined by M. Thus the measured message is a reduced substring on {0,1,2,3} . Strings of 0s and 1s are reduced; such strings might be called *positive* messages.
Let $(\varphi,\psi) \to \langle \varphi \mid \psi \rangle$ denote the inner product on $\mathcal{H}$, anti-linear in φ. Any quantum state ϱ in message space can be interpreted as a message source. It induces a probability distribution on the messages, $x \in$ *FG(2)* having weight $\langle \delta_x | \varrho(\delta_x) \rangle$/Trace($\varrho$)=probability that the message "received" is x. If the outcome of the measurement is message x then the *a posteriori* state is the pure state $\langle \delta_x | \varrho(\delta_x) \rangle \delta_x \otimes \delta_x^*$.
The *message source entropy* in the quantum message space is

$$\sum_{x \in FG(2)} \eta(\langle \delta_x \mid \varrho\,(\delta_x) \rangle\,/\mathrm{Trace}(\varrho)), \text{where } \eta(p) = -p\ln(p), 0 < p \leq 1, \eta(0) = 0$$

This entropy depends on the choice of the particular basis (δ_a) ; it is not the same as the von Neumann entropy = Trace($\eta(\varrho)$), but as shown in appendix A the von Neumann entropy is a lower bound for the source entropy with respect to (δ_a).

1) **Message Length Observable:**

The message length $\#x$ is an important observable which we denote by N. Formally, we equate N with the unbounded self-adjoint operator

$$N = \sum_{n=0}^{\infty} nM\left(FG(2)_n\right) \tag{2}$$

The *average message length* of the quantum message source ϱ is $\sum_{x\in \mathrm{FG}(2)} \#x \ \langle \delta_x | \varrho\left(\delta_x\right)\rangle / \operatorname{Trace}(\varrho) \ = \operatorname{Trace}(N\varrho)$, which may be infinite.
Note that $\#FG(2)_0 = 1$, and for $n>0$, $\#FG(2)_n = 4 \cdot 3^{n-1}$.
Thus the positive semi-definite operator Nhas the property that the multiplicity of an eigenvalue grows exponentially with $t$he size of the eigenvalue.

After a measurement of N (but not of the message itself) the state becomes $M(FG(2)_n)\varrho M\left(FG(2)_n\right)$,
where n is the result of the measurement. In the *aposteriori* state the observable N has the definite value n. A state ϑ wherein the message has definite length n has the property that $\vartheta N = n\vartheta$, and therefore $N\vartheta = \vartheta N = \vartheta N \vartheta$. It follows that

$$\vartheta = \sum_{x,y\in FG(2)_n} \langle \delta_x | \vartheta\left(\delta_y\right)\rangle \, \delta_x \otimes \delta_y^*. \tag{3}$$

If ϑ is also a positive message state, $\vartheta = \sum_{x,y\in 2^n} \langle \delta_x | \vartheta\left(\delta_y\right)\rangle \, \delta_x \otimes \delta_y^*.$

In particular, an *extended* n*-qubit* is a pure stateof the form $\psi \otimes \psi^* in$ which N has the definite value $n: \ N(\psi) = n\psi$.
A conventional n-qubit is a (normally normalized) pure state in which $\psi \in \operatorname{Span}\left\{\delta_x : \ x \in 2^n\right\}$. Such a state represents a positive n-bit message.

It is interesting to explore the dynamics of a quantum system with Hamiltonian $H = h\nu N$. Here h is Planck$'s$ constant and $\nu > 0$ is some positive constant frequency. The energy eigenvalues are $nh\nu$ for$n = 0, 1, 2, \ldots$ and for $n > 0$ the eigenvalue $nh\nu$ has multiplicity $\#\mathrm{FG}(2)_n = 4 \cdot 3^{n-1}$.

The dynamical unitary operator $U_t \ = \exp(-2\pi i \ N\nu t)$ has period $1/\nu$.
Let $\psi = \sum_{n=0}^{\infty} \psi_n$, where $\psi_n = M\left(FG(2)_n\right)(\psi)$ is the orthogonal projection of ψ to the space of messages of length n. Then the time evolution is given by a Fourier series

$$U_t(\psi) = \sum_{n=0}^{\infty} \psi_n e^{-2\pi \mathrm{i} n\nu t}, \ U_t(\psi) \otimes U_t(\psi)^* = \sum_{n=0}^{\infty} \psi_n \otimes \psi_n^* + \sum_{m<n} 2\mathrm{Re}(e^{2\pi \mathrm{i}(m-n)\nu t} \ \psi_n \otimes \psi_m^*) \tag{4}$$

Following time t the reception of a message before its contents or even its length is known changes the state to the mixed state $\sum_{n=0}^{\infty} \psi_n \otimes \psi_n^*$, which is independent of t. If the message length is known to be precisely k then the state becomes the pure state $\psi_k \otimes \psi_k^*$. The mixed state $\sum_{n=0}^{\infty} \psi_n \otimes \psi_n^*$

represents the component of the state simutaneously measurable with the message length. Note that within this dynamical model it is stationary in time.

More generallyif ϱ is an arbitrary state
($i.e.,$ positive operator on $\mathcal{H}$ with finite positive trace) then

$$\varrho = \sum_{n=0}^{\infty} \varrho_{\mathrm{nn}} + \sum_{m \neq n} \varrho_{\mathrm{mn}} \text{ , where } \varrho_{\mathrm{mn}} = M\left(FG(2)_m\right) \varrho M\left(FG(2)_n\right) \tag{5}$$

The first sum in (5) represents the component of ϱ which is co-measurable with N. Moreover, the expansion (5) is orthogonal with respect to the Hilbert-Schmidt inner product $(A, B) \rightarrow \mathrm{Trace}(A^* B)$, so

$$\mathrm{Trace}\left(\varrho^2\right) = \sum_{n=0}^{\infty} \mathrm{Trace}\left(\varrho_{\mathrm{nn}}^2\right) + \sum_{m \neq n} \mathrm{Trace}(M\left(FG(2)_m\right) \varrho \, M\left(FG(2)_n\right) \varrho) \, .$$

This last expression suggests defining an *index of co-measurability* with respect to N by

$$index(N, \varrho) = \frac{\sum_{n=0}^{\infty} \mathrm{Trace}\left(\varrho_{\mathrm{nn}}^2\right)}{\mathrm{Trace}\left(\varrho^2\right)} \tag{6}$$

Apparently, it is customary in quantum computation to assume that the number of bits is conserved, so that transitions from a message to a message of greater length is impossible; such states are precisely those of index 1. This index gives a measure of the extent this assumption is correct. In particular, there are states in QMS which allow transitions which change the message length.

2) jth Qubit Observable:

What is the value of a particular bit (or extended bit)? If we consider the jth extended bit of a message its value can be $0, 1, 2, 3,$ or -1 representing the case where the message length is not more than j, so the jth bit is not defined. Formally,

$$X_j = (-1) M\left(\cup_{k \leq j} FG(2)_k\right) + \sum_{b=0}^{3} b M\left(\{x \in FG(2) : \#x > j \text{ and } x_j = b\}\right) \tag{7}$$

Each vector of the form δ_{yaz} where $y, z \in FG(2)$ and $\#y = j$ is an eigenvectorofX_j for the eigenvalue $a \in 4$; the corresponding state is such that the measurement of the jth extended bit always yields a. Observe that the operators $\left(X_j\right)_{j \geq 0}$ together with N determine the atomic measure M completely since we know the message if we know the length and the value of the extended qubit at every position less than the length. Finally, the jth qubit is represented by the observable

$$Q_j = -M\left(\{x : \#x \leq j \text{ or } x_j \in \{2,3\}\right)+\sum_{b=0}^{1} bM\left(\{x \in FG(2) : \#x > j \text{ and } x_j = b\}\right) \tag{8}$$

3) Quantum Message Source:

The component of state ϱ that is co-measurable with N is the state ϱ_N . The states ϱ and ϱ_N are identical as message-generating sources, since

$$\text{for } x \in FG(2)_n, \langle \delta_x | \varrho\left(\delta_x\right)\rangle = \langle \delta_x | \varrho_n\left(\delta_x\right)\rangle = \langle \delta_x | \varrho_N\left(\delta_x\right)\rangle \ .$$

Now every quantum state is also an observable because it is *a* self-adjoint operator $\varrho = \sum_r rE_r$ where the orthogonal sum is over $r \in$ spectrum(ϱ). The possible measured values are the elements r. If we measure ϱ while in the state ϱ the probability that the outcome is r equals $m_r\ r/\text{Trace}(\varrho)$, where m_r is the multiplicity of r as an eigenvalue of ϱ. The *a posteriori* state is rE_r and further measurements of ϱ always yield r with no change of state. In the special case that ϱ is *a* pure state $\psi \otimes \psi^*$ the measurement always yields $|\psi|^2$ with probability one. As we have seen in this case $\varrho_N = \sum_{n=0}^{\infty} \psi_n \otimes \psi_n^*$, and this is always *a* mixed state unless ψ is an eigenvector of N. Now if we measure $\psi \otimes \psi^*$ the result is $|\psi|^2$ with probability

$$index(N,\psi \otimes \psi^*) = \sum_{n=0}^{\infty} |\psi_n|^4 \ / \ |\psi|^4 < 1 \text{ in general.}$$

4) Some Examples;

.According to results in [KB] the maximum entropy probability measure on $FG(2)$ with *a* fixed average message length μ is given by w(x) = $(1-p)\ p^n / \#FG(2)_n$ where n = #x and $p = \frac{\mu}{1+\mu}$. Let $\psi = \sum_{\text{x}\epsilon\text{FG}(2)} \sqrt{w(x)}\delta_x$. As *a* message source the pure state $\psi \otimes \psi^*$ is such that the probability of receiving x is $w(x)$.

Now consider the highly mixed state $\sigma = \sum_x w(x)\delta_x \otimes \delta_x^*$. As *a* message source σ induces the same probability distribution on the messages as $\psi \otimes \psi^*$.The entropy of this distribution is log(3/p) p/(1-p) + log(4/3) - log(1-p); as $\mu \to \infty$ the entropy is asymptotic to log(3)μ .

But the von Neumann entropy for $\psi \otimes \psi^*$ is zero because it is *a* pure state, whereas the von Neumann entropy of σ equals the source entropy.

D. Positive Messages

Let $\mathcal{H}^+$ be the Hilbert space spanned by $\{\delta_y : y\epsilon 2^*\}$. $\mathcal{H}^+$is the positive message state space of ordinary bit-string messages. The orthogonal projector onto $\mathcal{H}^+$ is $M(2^*)$ as in (1) above.The operator $N^+ = M(2^*)\, NM(2^*)$ has many properties analogous to those of N.
The state change wrought by a test for positivity with no information about the outcome changes ϱ to $M(2^*)\,\varrho\, M(2^*)+(I - M(2^*))\,\varrho(I - M(2^*))$ and the trace is preserved, but a state change from ϱ to $M(2^*)\ \varrho M(2^*)$ which occurs when the test result is affirmative will of course provide information and reduce the trace of the state.

Multiplication in$FG(2)$ restricted to 2^* is merely concatenation of bit strings. The multiplication derived from the concatenation product of basis vectors indexed by multi-qubits extends to a product on $\mathcal{H}^+$ which is the completionof the tensor algebra on the two-dimensional Hilbert space spanned by the reference qubits$|0\rangle$ and$|1\rangle$. In quantum computationδ_y is often $w$ritten as $|y\rangle$ (ket form) and δ_y^* as $\langle y|$ (bra form) so for example $\delta_{1101} \otimes \delta_{1101}^*$may be written more compactly as $|1101\rangle\langle 1101|$.

Here is a sample computation :

$$(-1|0\rangle{+}3|00\rangle{-}i|10\rangle){*}(|\Lambda\rangle{+}\ |1\rangle{+}|01\rangle) = \ -|0\rangle{+}3|00\rangle{-}i|10\rangle{-}|01\rangle{+}2|001\rangle\ -i|101\rangle\ +3|0001\rangle\ -i|1001\rangle$$

This multiplication is precisely convolution on $FG(2)$. The QMS $\mathcal{H}$ is the extension of $\mathcal{H}^+$ analogous to the extension of the semigroup 2^* to the group $FG(2)$.

On the other hand, perhaps some physical constraint restricts our message measurements to 2^*. Many data-processing operations F in QMS would have as a goal the maximization of Trace(M(2^*) $F(\varrho)$M(2^*))/Trace(ϱ) subject to some bounds on Trace(ϱ). However, the operator F need not preserve states supported by $\mathcal{H}^+$. The positive message observable's spectral measure is M^+ , which is the atomic measure for the observable taking values in $2^*\cup\{(\text{-})\}$, where (-) stands for any fixed thing not in 2^* :

$$M^+(\{a\}) = \delta_a \otimes \delta_a^* \text{ for } a \in 2^*\ , M^+(\{(-)\}) = M\,(FG(2) \sim 2^*\,) = I - M^+\,(2^*\,).$$

Quantum message space contains all the usual spaces for quantum circuits :

$$\text{Span}\,\{\delta_x : x \in 2^n\} = \text{Range}\,(M\,(2^n\,)) \approx \mathbb{C}^{2^n} \approx \mathbb{C}^{\otimes n},\ \text{the space of } n\text{-qubits.}$$

QMS can absorb the tensor product of two such spaces such as $\mathbb{C}^{\otimes k}$ representing k control bits with $\mathbb{C}^{\otimes m}$ data bits. The usual quantum operators of conventional quantum circuit theory can all be extended trivially to $\mathcal{H}^+$; the extensions to $\mathcal{H}$ are not so obvious.

E. Data Processing on Messages

A data-processing operation on states in QMS is implemented by a *quantumoperation*[NC], which in this context means a real linear operator F on the self-adjoint operators of

trace class on $\mathcal{H}$ which is strictly positive and non-trace-increasing. In particular, if ϱ is *a* message state then so is $F(\varrho)$, and $0 < \text{Trace}(F(\varrho)) \leq \text{Trace}(\varrho)$. The information lost by the system(or entropy gained?) is $-\log_2\left(\frac{\text{Trace}(F(\varrho))}{\text{Trace}(\varrho)}\right)$.
If equality holds for all states ϱ then F is trace-preserving;
the interpretation is that the state change $\varrho \rightarrow F(\varrho)$ generates no information, does not increase entropy, and is often reversible. An example of such an operation is $\mathcal{K}(U)(\varrho) = U\varrho U^*$, where U is *a* unitary operator on the QMS $\mathcal{H}$. An example of *a* quantum operation which is not reversible is the measurement of an observable, of *a* projector P say, with 1 as the result of the measurement. We have $\mathcal{Q}(P)(\varrho)=P\varrho P$. If we measure P without changing the entropy of the system *t*he *a posteriori* state *is*

$$\mathcal{T}(P)(\varrho) = \mathcal{Q}(P)(\varrho) + \mathcal{Q}(I-P)(\varrho)$$

Certain*o*ther trace-preserving operations can be built up from orthogonal projectors (P_j) such that $\sum_j P_j = I$ and associated unitary operators (U_j) :

let $\mathcal{T}(U,P)(\varrho) = \sum_j U_j P_j \varrho \mathrm{P}_j U_j^*$, assuming the range of the index j is finite.

If *a* measurement of the index is made with result k the state becomes $P_k \varrho P_k$ and $\mathcal{T}(U,P)(P_k\varrho P_k) = U_k P_k \varrho P_k U_k^*$, so after measuring and knowing the result the operator $\mathcal{T}$ does *a* switch operation, applying $\mathcal{K}(U_k)$ to the *a posteriori* state conditionally. However $\mathcal{T}(U,P)$ may be applied without ever actually getting the result of the measurement.

In the special case when U_j and P_j commute for all j then $\mathcal{T}(U,P) = \mathcal{K}(W)\circ\mathcal{T}(I,P) = \mathcal{T}(I,P)\circ\mathcal{K}(W)$ where $\mathcal{T}(I,P) = \sum_j \mathcal{Q}(P_j)$ is *a* measurement of the outcome j without any definite information about itsvalue.

F. Definite Message States as Registers

1) The Destructive Read Memory Cell:

The cell is in the state δ_b where $b \in \mathit{2}$. We need to read the bit stored, b, and restore it by quantum operations. The cell requires the measurement of whether there is a message or not (i.e., the observable $\delta_\Lambda \otimes \delta_\Lambda^*$) . The unitary operators necessary are the ones which append the bits and which erase them : V_0,V_1,V_2,V_3 , where V_z is the unique unitary operator which maps δ_x to $\delta_{x\cdot z}$.

To read the value of b we may proceed:

1.a.1) Apply V_3 to δ_b to get $V_3(\delta_b)$, which equals δ_Λ if b=1 but equals δ_{03} if b=0 .

1.a.2) Determine if the bit was erased by measuring $\delta_\Lambda \otimes \delta_\Lambda^*$. If the result is 1 then a bit was erased which must have had the value 1; if the result is 0 the state is δ_{03} so b must be 0. In either case the result of measuring $\delta_\Lambda \otimes \delta_\Lambda^*$ is the value of b.

1.a.3) Knowing b, apply V_b to restore the original value of the cell.
The quantum operation for reading the bit is $\mathcal{K}(V_b)\circ\mathcal{Q}(\delta_\Lambda\otimes\delta^*_\Lambda)\circ\mathcal{K}(V_3)$.

To write the value $a\in 2$ to the cell, first erase as before:
1.b.1) Apply V_3 to δ_b to get $V_3(\delta_b)$, which equals δ_Λ if b=1 but equals δ_{03} if b=0 .
1.b.2) Determine if the bit was erased by measuring $\delta_\Lambda\otimes\delta^*_\Lambda$; the result is the value of b.
1.b.3) If b=1 Apply V_a to $\delta_\Lambda$to get δ_a
1.b.4) If b=0 Apply $V_a\circ V_2\circ V_1$ to $\delta_{03}$to get δ_a
The quantum operation for writing the bit is
$\mathcal{K}(V_a)\circ\mathcal{T}((V_2\circ V_1,\mathrm{I}),(\mathrm{I}-\delta_\Lambda\otimes\delta^*_\Lambda,\delta_\Lambda\otimes\delta^*_\Lambda))\circ\mathcal{K}(V_3)$.
Note that in this formulation the value of b does not need to be known.

2) The Shift Register

QMS states can store bit strings of arbitrary length, and the data may be processed rather like shift registers. A message state δ_x stores a bit string $x_0x_1...x_{n-1}\in 2^n$. We can shift bits in and out on the right by the operators $\mathcal{K}(V_a)$, $a\in 4$. We also assume we can measure N, the message length.
To shift in a bit b, $\mathcal{K}(V_b)(\delta_x\otimes\delta^*_x) = \delta_{xb}\otimes\delta_{xb}{}^*$. The length is now $n+1$.
To shift out a bit, suppose $x=ab$, $a\in 2^{n-1}$:
2.b.1) Measure N, and record the result n. This measurement doesn't change the state since we're assuming it is an eigenstate for N.
2.b.2) Erase a 1 by applying V_3 to get $\delta_{ab\,\cdot\,3}$; the state vector is either δ_{a03} or δ_a.
2.b.3) Now measure N again, this time getting the result n' . If $n'\leq n$ leave the state δ_a alone (we know the bit shifted out was a 1); otherwise apply $V_2\circ V_1$to δ_{a03}. In either case the state vector is now δ_a.
The quantum operator for shifting out the bit is

$$\mathcal{K}((n'\leq n)I+\ (n'>n)V_2\circ V_1)\circ Q\left(M\left(2^{n'}\right)\right)\circ\mathcal{K}\left(V_3\right)\circ\mathcal{Q}\left(M\left(2^n\ \right)\right).$$

G. Communication in Quantum Message Space

The classical Shannon model for communication over a channel is summarized by the familiar flow diagram:

message *sent signal* *received signal* *message*
source → encoder/transmitter → channel → decoder/receiver → destination
noise

Rather than over-stretch the analogy with the classical situation, let us describe the steps involved in Alice sending a free-group string, possibly a binary string, to Bob:

0) **Start at the source**.

Let ρ be any state in message space. The sender Alice gets the message from the source by measuring the message observable. The probability that the selected message is z equals $\frac{\langle \delta_z \, | \rho(\delta_z) \rangle}{\mathrm{Tr}(\rho)}$. Note that the source may be *a* message that Alice composed herself by applying the unitary operators V_0 and V_1 in proper order starting with δ_Λ. For example if z $\in FG(2)$ equals 10010 then the composed source would be the pure message state determined by the basis vector $V_0 \circ \; V_1 \circ V_0 \circ \; V_0 \circ V_1 \, (\delta_\Lambda \,) = \delta_z$.

1) Alice gets the message to send .

After this action the state is $\langle \delta_z \, | \rho \, (\delta_z \,) \rangle \, \delta_z \otimes \delta_z^*$ and Alice has the message z to send to Bob. Theprababilityofgettingthismessagefromsource$\rho$is

$$\Pr(z|\rho) = \; \langle \delta_z \, | \rho \, (\delta_z \,) \rangle / \, \mathrm{Tracc}(\rho)$$

2) Alice encodes the message.

By applying a unitary operator G the state is transformed so that its normalized form is $\psi \otimes \psi^*$; $\psi = \mathrm{G}(\delta_z)$ need not be a message basis vector nor even be a multiple qubit (i.e., ψ need not be an eigenvector of *N).*

3) Alice transmits the encoded message over the channel.

The general channel is modelled as a trace-preserving quantum operator $\mathcal{E}$ mapping states on $\mathcal{H}$ to states. $\mathcal{E}$ may have an operator sum decomposition

$$\mathcal{E}(\tau) = \sum_j O(j) \tau O(j)^* \tag{9}$$

where the *O(j)* are bounded operators such that $\sum_j \; O(j)^* \mathrm{O} \; (j) = \; I$

4) The channel transforms the sent signal into the received signal.

The received signal is now

$$\alpha = \; \langle \delta_z \, | \rho \, (\delta_z \,) \rangle \, \mathcal{E} \left(G \, (\delta_z) \otimes G \, (\delta_z)^* \right)$$

5) Bob decodes the received signal .

He does this by applying $G^{-1} = G^*$ to the received signal. The state is now

$$G^* \alpha G = \; \langle \delta_z \, | \rho \, (\delta_z \,) \rangle \, G^* \circ \mathcal{E} \left(G \, (\delta_z) \otimes G \, (\delta_z)^* \right) \circ G, \Pr(\text{received} = \text{sent} | \text{sent} = z) = \langle \delta_z | G^* \alpha G | \delta_z \rangle / \, \mathrm{Trace}(\alpha) \;\; = \Big\langle G$$

6) Bob receives the message.

He does this by measuring the positive message observable M . Suppose the result is w∈FG(2); after this the state becomes $\langle \delta_w | G^* \alpha G | \, \delta_w \rangle \, \delta_w \otimes \delta_w^*$, the probability of this outcome being $\frac{\langle G(\delta_w) \, | \alpha | G(\delta_w) \rangle}{\langle \delta_z \, | \rho(\delta_z \,) \rangle}$.

Clearly, Alice and Bob's objective in choosing an encoding protocol is to maximize the probability that the message Bob receives is the message she sends, (before encoding but after sampling from the source ρ). They use their knowledge of the channel dynamics and [statistical?] knowledge about the initial channel state and the source ρ to design an encoding unitary transformation G which maximizes (as a function of unitary G) the probability that the sent message is the received message.

$$\Pr(\text{received} = \text{sent}|\text{source} = \rho) = \sum_z \Pr(\text{received} = \text{sent}|\text{sent} = z) \Pr(z|\rho) \; = \sum_z \left\langle G\left(\delta_z\right) \middle| \mathcal{E}\left(G\left(\delta_z\right) \otimes G\left(\delta_z\right)^*\right) \middle| \right. \tag{10}$$

If we assume the operator sum form above then

$\Pr(\text{received=sent}|\text{source=}\rho) = \; \sum_{z,j} \Pr(z|\rho) \; |\langle G\left(\delta_z\right)| \, O(j) | G\left(\delta_z\right) \Big\rangle \Big|^2$

Thus Alice and Bob choose G to maximize the above 4^{th} degree form in G, subject to the unitary constraint $G^* \; G = \; I.$

7) Bob passes the message along to its destination and resets the message state.

"Passing the message along" is a classical process. Bob might reset the message state to $\delta_\Lambda \otimes \delta_\Lambda^*$ by applying the operator $R_{w^{-1}}$.

IV. HARMONIC ANALYSIS ON FG(2)

A standard reference for harmonic analysis on finitely generated free groups is [TP]. We also use [Na] for some functional analytic aspects of the argument. The results of this parts are all consequences of results therein. A self-contained development of harmonic analysis of $FG(2)$ which realizes the principal series on L^2[0,1[will be found in [TR3].

The group $FG(2) = \uplus_{n \geq 0} \text{FG}(2)_n$, and so it is countably infinite. With the discrete topology it is a locally compact group whose Haar (translation-invariant measure) is ordinary summation. We define the spaces $\ell^p(\; FG(2))$ as usual:

Let $1 < p < \infty$. For any complex−valued function f on $FG(2)$ define the ℓ^p norm by

$$\|f\|_p = \left(\sum_{x \in \text{FG}(2)} |f(x)|^p \right)^{1/p}$$

and the space ℓ^p(FG(2)) , or ℓ^p for short, is defined by

$$\ell^p(\mathrm{FG}(2)) = \{f : \|f\|_p < \infty\}$$

If $1 < p < \infty$ the spaces ℓ^p and ℓ^q are dual provided $q = p/(p-1)$. The bilinear form $\langle f, g\rangle$ establishes the duality, where

$$\langle f, g\rangle = \sum_{x\in\mathrm{FG}(2)} f(x)g(x) \tag{11}$$

and the sum is absolutely convergent. Note this form is invariant under left and rtight translations of f and g together.

Now define
$\|f\|_\infty = \sup\{ \ |f(x)| : x\in FG(2)\}$

and the space ℓ^∞ as the space of all functions f for which $\|f\|_\infty < \infty$.

Then (11) with $f \in \ell^\infty(FG(2))$ and $g\in \ell^1(FG(2))$ identifies ℓ^∞ with the dual of ℓ^1 [but the dual of ℓ^∞ is much larger than ℓ^1].

We are mainly interested in the Hilbert space $\ell^2(\mathrm{FG}(2))$, with inner product

$$\langle f|g\rangle \ = \ \langle f^*, g\rangle, \ f^* = \text{complex conjugate of } f. \tag{12}$$

The o.n. basis (δ_x) establishes an isomorphism of the QMS $\mathcal{H}$ with $\ell^2(FG(2))$ connecting f(x) with $\langle\delta_x|f\rangle$. We shall use this identification throughout this section. Note $\delta_x(y)$ equals 1 if $x= y$ and equals 0 otherwise.

A. The Regular Representation

The *left and right regular representations* L and R respectively are defined by

$$L_q f(x) = f\left(q^{-1}x\right) \ , R_q f(x) = f(xq) \text{ where} f\in\ell^p(FG(2)) \text{and } x,q \in FG(2). \tag{13}$$

The binary operation of *convolution* * is defined by

$$f \star g(x) = \sum_{y\cdot z=x} f(y)g(z) \tag{14}$$

L and R define unitary representations of the free group on ℓ^2 which commute with one another. In fact, results in [Na] imply that all operators which commute with R are weak limits of linear combinations of L_q, and conversely. More explicitly, a bounded operator on ℓ^2 which commutes with all R_q is of the form $g \mid\to h*g$ for some unique $h \in \ell^2$ (but not every such h defines a bounded operator on ℓ^2) . The only operators commuting with both L and R are scalar multiples of I, so L (and R) are factor representations of $FG(2)$; in fact, the factor is of von Neumann type II_1 .

The main connection between QMS and harmonic analysis on $FG(2)$ is the observation that the operators V_a which append and remove bits are the operators $R_{a^{-1}}$.

In the context of harmonic analysis on $FG(2)$ the operators $k(\ M) = \sum_{x\in FG(2)}\mathrm{k(x)}\ \delta_x\otimes\delta_x^*$ are the multipliers which map f to $k\,f$. These operators rarely commute with either L or R. The measurements which commute with all V_a commute with R and therefore stem from left convolution operators of the form

$$f \to h * f= \sum_{x\in FG(2)} h(x)L_x(f), \tag{15}$$

where $h(x) = h^\star(x) = h^*\left(x^{-1}\right)$ is such that h*f $\in \ell^2$ whenever f $\in \ell^2$.

In particular the bit-valued observables P (a.k.a. projectors) which commute with R correspond with functions p such that $p^\star\star\ p\ = p$ and where $P\ (\ f\ )\ =\ p^*$f . These observables permit conditional operations which are trace-preserving and which commute with all the operators R_a; i.e., the quantum operations $\mathcal{Q}(\ p\star)$ and $\mathcal{K}(R_a)$ commute, $\forall\ \ a\in FG(2)$.

B. Radial Functions and the Decomposition of the Left Regular Representation into Irreducible Representations

The material in this section is adapted from [TP]; a self-contained technical report[TR3] is forth-coming. As shown in [Na] there is no unique way to do harmonic analysis on a free group with more than one generator, but the technique in [TP] is elegant and of interest here.

A function f on FG(2) is *radial* provided $f(\ x)$ depends only on the message length $\#\ x$. Let K be the vector space of all radial functions with finite support. The functions (μ_n) form an orthogonal basis for K, where $\mu_n(x) = 1/n$ if $\#\ x\ =\ n$, and is 0 otherwise.
Then K turns out to be a commutative algebra under convolution, and in fact it is generated by μ_1. This follows from the formula

$$\mu_1 \star \mu_n = \frac{1}{4}\mu_{n-1} + \frac{3}{4}\mu_{n+1}, n>0. \tag{16}$$

It follows immediately by induction that for any n there is a polynomial $p_n(\lambda)= \sum_{k=0}^{n}p_{\mathrm{nk}}\lambda^k$ such that $\mu_n=p_{\mathrm{n0}}\delta_\Lambda+\ p_{\mathrm{n1}}\mu_1+\ p_{\mathrm{n2}}\mu_1\star\mu_1+...+\ p_{\mathrm{nn}}\mu_1^{\star\mathrm{n}}$. In other words, every function in K is a convolution polynomial in μ_1. The commutative von Neumann algebra generated by $A\ = \mu_1\star$ as an operator on $\ell^2(\ FG(2))$ is maximal Abelian in the von Neumann algebra generated by $(L_a)_{a\in\mathrm{FG(2)}}$. This means it can be used to decompose the left regular representation into irreducible representations of the free group. Note that in general the measurement of A will smear a definite message and scatter its length.

Formula (16) implies that the polynomials p_n satisfy the recursion

$$p_{n+1}(\lambda) = \frac{4}{3}p_n(\lambda) - \frac{1}{3}p_{n-1}(\lambda), \text{for} n > 0; p_0(\lambda) = 1,\ p_1(\lambda) = \lambda. \qquad (17)$$

The spectrum of $\mu_1\star$ considered as a self-adjoint operator on ℓ^2(FG(2)) turns out to be the interval [-$\frac{\sqrt{3}}{2}$,$\frac{\sqrt{3}}{2}$], so λ in (17) may be restricted to that interval. The p_n are orthogonal polynomials with respect to the weight function

$$w(\lambda) = \frac{1}{\pi}\frac{\sqrt{3-4\lambda^2}}{1-\lambda^2}, |\lambda| \le \frac{\sqrt{3}}{2},\ \int_{-\frac{\sqrt{3}}{2}}^{\frac{\sqrt{3}}{2}} p_n(\lambda)p_m(\lambda)w(\lambda)d\lambda = \frac{(n=m)}{\#FG(2)_n} \qquad (18)$$

which equals $\frac{1}{4}3^{1-n}$ if $0< m= n$ and 0 otherwise.
The normalized polynomials $\epsilon_n(\lambda)$=$\sqrt{\#FG(2)_n}p_n(\lambda)$ form an o.n. basis for L^2([-$\frac{\sqrt{3}}{2}$,$\frac{\sqrt{3}}{2}$], $w(\lambda)$ $\mathbf{d}\lambda$). The re-scaled polynomials E_n(x)=$\epsilon_n(\frac{\sqrt{3}}{2}\ x)$, $|\ x|\le 1$, satisfy the recursion formula $E_{n+1}(\ x)$=2 x $E_n(\ x)$ - $E_{n-1}(\ x)$, which is the recursion formula satisfied by the Chebyshev polynomials, so E_n is a linear combination of T_n and U_n; in fact, for n≥1 E_n(x)=(T_n(x)+U_n(x))/$\sqrt{3}$, so $p_0(\lambda)$=1,

$$\forall n > 0\ p_n(\lambda) = \frac{1}{2}3^{-n/2}\left(T_n\left(\frac{2}{\sqrt{3}}\lambda\right) + U_n\left(\frac{2}{\sqrt{3}}\lambda\right)\right) \qquad (19)$$

1) The Poisson Boundary of FG(2)

The Poisson Boundary of the free group is the set Ω of infinite reduced words from the alphabet 4={0,1,2,3}. In other words, Ω is the subset of the infinite product $4^{\mathbb{N}}$ consisting of those infinite strings which contain none of the diagrams 02,13,20,31 . Ω is a closed subset of the compact space $4^{\mathbb{N}}$ and therefore itself compact.
The group $FG(2)$ acts on Ω in a natural way:

$$x \cdot \omega = \mathit{reduce}(x\omega) = \mathit{reduce}\,(x_0 \ldots \mathrm{x}_{n-1}\ \omega_0 \ldots \omega_{n-1})\,\omega_n\omega_{n+1}\ldots. \qquad (20)$$

E.g., 01121032·012231100...= 01121231100...

For every $x\in FG(2)$, $x\neq \Lambda$, let E_x= {$\omega \in \Omega$: ∀j if # $x>j$ then , ω_j=x_j}. There is a unique Borel probability measure ν on Ω which assigns measure $\frac{1}{4\cdot 3^{\#x-1}}$to E_x. In other words the probability that an infinite reduced word starts with x depends only on the length of x.
The action of $FG(2)$ on Ω does not preserve the measure ν; it transforms it according to

$$\int_\Omega \xi(x\cdot\omega)d\nu = \int_\Omega P(x,\omega)\xi(\omega)d\nu, \text{for all continuous functions } \xi \text{ on } \Omega. \qquad (21)$$

In [TR3] an elementary measure isomorphism between (Ω,ν) and [0,1] with Lebesgue measure is established so in fact all the analysis may be transferred to the unit interval.

2) The Poisson Kernel and the Principal Series

The Poisson Kernel is the function P in the above formula (21); it is given by P(x,ω)=$3^{2N(x,\omega)-\#x}$, where N(x,ω)= k iff ω_j=x_j if $k > j$ but $\omega_k \neq x_k$. This formula implies that the operator π_z(x) on $L^2(\Omega,\nu)$ is unitary whenever Re(z)=$\frac{1}{2}$:

$$\pi_{1/2+it}(x)(\xi)(\omega) = P(x,\omega)^{1/2+it}\xi\left(x^{-1}\cdot\omega\right), \tag{22}$$

where $t \in \mathbb{R}$ and $\xi \in L^2$ (Ω,ν). In fact, $x \to \pi_{1/2+it}$(x) defines a unitary representation of the free group $FG(2)$ on $L^2(\Omega,\nu)$, one of the members of the *principal series* of representaions π_z . When z = 1/2+i t the representation is *irreducible* in that no non-trivial closed Hilbert subspace of $L^2(\Omega,\nu)$ is invariant under all π_z(x). Irreducibility implies that all bounded linear operators on $L^2(\Omega,\nu)$ are limits (in the weak operator topology) of finite linear combinations of $\pi_{1/2+it}$(x), and that all pure states are limits of linear combinations of $\pi_{1/2+it}$(x)(φ), where φ is any non-zero vector (1_Ω say).

3) The Fourier Transform and the Decomposition of the Left Regular Representation

The *Fourier Transform* which decomposes the left regular representation can now be defined. Let

$$K((\lambda,\omega),x) = P(x,\omega)^{1/2+it(\lambda)}, \tag{23}$$

where $x \in FG(2)$, $\omega \in \Omega$, $\lambda \in$ sp(A)=[-$\frac{\sqrt{3}}{2}$,$\frac{\sqrt{3}}{2}$] , and $t(\lambda) = \frac{\cos^{-1}\left(\frac{2}{\sqrt{3}}\lambda\right)}{\ln(3)}$
.
. K is the kernel for the Fourier transform:

$$\mathcal{F}(f)(\lambda,\omega) = \sum_{x\in \mathrm{FG}(2)} K((\lambda,\omega),x)f(x) \tag{24}$$

$$\mathcal{F}:\ell^2\left(FG(2)\right) :\to L^2(\mathrm{sp}(A)\times\Omega, w(\lambda)\mathbf{d}\lambda\otimes d\nu),.$$

$\delta_\Lambda \to 1_{\mathrm{sp}(A)\times\Omega}$
$\delta_y \to K((\lambda,\omega),y)$
$\mu_n \to p_{n\otimes 1_\Omega}$
$\mathcal{F}$ decomposes left convolution operators:
$\mathcal{F}(g*f)(\lambda,\omega) = \sum_y g(y)\pi_{1/2+\mathrm{it}(\lambda)}(y)(\mathcal{F}(f)(\lambda,.))(\omega)$,
or equivalently
$\mathcal{F}\circ(g*)\circ\mathcal{F}^{-1} = \int_{\mathrm{sp}(A)}\sum_y g(y)\pi_{1/2+\mathrm{it}(\lambda)}(y)w(\lambda)d\lambda$

expressing the Fourier-transformed operator as a "direct integral" . In particular,

$$\mathcal{F} \circ L_a \circ \mathcal{F}^{-1} = \int_{\mathrm{sp}(A)} \pi_{1/2+it(\lambda)}(a) w(\lambda) d\lambda$$

decomposes the left regular representation as a direct integral of irreducible representations of the principal series.

Recall that A = left convolution by μ_1=(δ_0+δ_1+δ_2+δ_3)/4 . Then $\mathcal{F}$ diagonalizes all the operators $k(A)$, where k is any bounded Borel function: $\mathcal{F}(k(A)(f))(\lambda,\omega) = k(\lambda)\, \mathcal{F}(f)(\lambda,\omega)$,
or equivalently $\mathcal{F}\circ$k(A)$\circ\mathcal{F}^{-1}$=Mul($k\otimes 1_\Omega$). In particular A is transformed to multiplication by λ on [-$\sqrt{3}/2$,$\sqrt{3}/2$] .
The inverse Fourier transform is given by the kernel :
$K^\top((\lambda,\omega),x)$=$K(x,(\lambda,\omega))^* = P(x,\omega)^{1/2-it(\lambda)}$
$\mathcal{F}^{-1}(\Psi)(x)$=$\int_{\mathrm{sp}(A)} \int_\Omega K^\top\left((\lambda,\omega),x\right)\Psi(\lambda,\omega)d\nu(\omega)w(\lambda)d\lambda$.
Thus the transform is unitary; here is the Plancherel formula:

$$\|f\|_2^2 = f^{*}{*}f(\Lambda) = \int_{\mathrm{sp}(A)} \int_\Omega |\mathcal{F}(f)(\lambda,\omega)|^2 d\nu(\omega)w(\lambda)d\lambda$$

This summary of harmonic analysis on the free group $FG(2)$ indicates that one class of projectors what commute with all R_a are those of the form $f \to g \star f$,where g is a radial function. The Fourier transform of such an operator is of the form Mul($\hat{g}\otimes 1_\Omega$), where $\mathcal{F}(g)$=$\hat{g}\otimes 1_\Omega$. The operator is a projector iff $\hat{g}^2 = \hat{g}$, so $\hat{g} = 1_B$ for some Borel set B $\subseteq$ sp(A) . If follows that

$$g(x) \ = G_n(B) = \int_B \int_\Omega P\left(x^{-1},\omega\right) d\nu(\omega)w(\lambda)d\lambda = \int_B p_n(\lambda)w(\lambda)d\lambda \qquad (25)$$

where $n = \#\, x$, g is a radial function, and $g(\Lambda) = \int_B$w(λ)dλ. Since $g \star \delta_\Lambda = g$, for all $x\in$FG(2) |g(x)|^2/(‖g‖$_2^2$) represents the probability of receiving message x after measuring the projector $g\star$ starting in state δ_Λ. This number is the same for all reduced words of the same length n, given by ($\int_B p_n(\lambda)$w(λ)dλ)^2. Note that this probability is not an additive set function of B, whereas $B\to G_n(B)$ is a signed measure.

C. The Harmonic Analysis of a Single Left Translate Operator L_a

Let $a \in FG(2)$, $a \neq \Lambda$. Such a choice defin$\mathcal{F}$es a non-trivial action of the integers $\mathbb{Z}$ on $FG(2)$: $(n, x) \to a^n\cdot x$. Each orbit has a unique reduced word z of minimum length. Therefore, if $z\neq \Lambda$, $z_0\neq$ *inv* ($a_{\#a-1}$)= inverse of last letter of a, and $z_0 \neq a_0$ = first letter of a. Therefore the orbits are in one-to-one correspondence with the set Z of all z satisfying these conditions. Thus there is a unique unitary operator $\mathcal{T}$:ℓ^2(FG(2)) :$\to L^2(\mathbb{T}\times Z)$, where $\mathbb{T}$ is the unit circle with normalized euclidean measure $\frac{d\theta}{2\pi}$, such that $\mathcal{T}(\delta_{a^n\cdot z})(\alpha$,z) =

$\alpha^n \delta_z$. This operator diagonalizes L_a; i.e., $\mathcal{T} \circ L_a \circ \mathcal{T}^{-1} =$ Mul($\zeta \otimes 1_Z$), $\zeta(\alpha)=\alpha$, $\mathcal{T} \circ L_a \circ \mathcal{T}^{-1}(\sum_{n\in\mathbb{Z}} \hat{k}(n)\ L_{a^n})$ = Mul(k$\otimes 1_Z$) for any bounded function k on $\mathbb{T}$ with ordinary Fourier series $\hat{k}(n) = \frac{1}{2\pi}\int_{-\pi}^{\pi}$ k$(e^{\mathrm{i}\theta})e^{-in\theta}d\theta$, and the operator $\sum_{n\in\mathbb{Z}} \hat{k}(n)\ L_{a^n}$ is just convolution with g=$\sum_{n\in\mathbb{Z}} \hat{k}(n)\ \delta_{a^n}$. The functions k which yield projectors in the weakly closed algebra generated by $L_a$and L_a^* are indicator functions of Borel subsets of $\mathbb{T}$.

The case $k = 1_{\{\alpha:|\arg(\alpha)|<\phi\}}$, $\pi \succeq \phi > 0$, determine projectors which are easy to compute, since

$$g\left(a^n\right) = \hat{k}(n) = \frac{1}{2\pi}\int_{-\pi}^{\pi} k\left(e^{\mathrm{i}\theta}\right) e^{-\mathrm{i}n\theta} d\theta = \frac{1}{2\pi}\int_{-\phi}^{\phi} e^{-\mathrm{i}n\theta} d\theta = \sin(n\phi)/(n\pi)$$

if n$\neq$0, and $\hat{k}(0) = \frac{\phi}{\pi} = \|g\|_2^2$ since $k^2 = k$ in this case.

Thus L_a is unitarily equivalent to an infinite sum of bilateral shifts . Of course L_a and all the operators $\sum_{n\in\mathbb{Z}} \hat{k}(n)\ L_{a^n}$ commute with all the operators R_y. Finally, since R_a= V$\circ L_a \circ V^*$, where V is the unitary reflexion operator V(f)(x)=f(x^{-1}), R_a is also unitarily equivalent to an infinite sum of bilateral shifts.

V. DISCUSSION AND CONCLUSIONS

In this report we have developed a mathematical formulation of quantum message space and demonstrated a type of calculus for incorporating simple operations on bits into quantum communication theory and computation. How might quantum message space be implemented physically? Note that since a quantum message space is basically a Hilbert space with a complete orthonormal basis indexed by $FG(2)$, the free group on two elements, the problem is "merely" one of labelling. For example, the energy levels of a harmonic oscillator with one degree of freedom are of the form a n + b, where n = 0,1,2,3,... . One could employ any method for listing the elements of FG(2) to index the eigenstates of the oscillator by FG(2). Of course, in this case since the multiplicity is fixed the amount of energy associated with a message grows exponentially with the message length.

Or consider a hydrogen atom. The bound states are of the form a/n + b , each with multiplicity 2 n + 1 . In principle, FG(2) could label the multitude of energy stationary states. But now the energy levels pile up around 0, and the practical problems of distinguishing bound states when n is very large would make it difficult to send long messages.

In their classic text, Nielsen and Chaung [NC,p.203] speculate:

"...it is by no means clear that the basic assumptions underlying the [finite dimensional] state space and starting conditions [from the computational basis] in the quantum circuit model are justified. Might there be anything to be gained by using systems whose state space is infinite dimensional? Assuming that the starting state...is a computational basis state is also not necessary..."

They go on to suggest that other states, other basic unitary processors, and other measurements might be able to "...perform tasks intractible within the quantum circuit model." We doubt if QMS and the operators we've studied extend the realm of theoretical computability, but they do show how a consistent quantum model of message sources of arbitrary length leads naturally to considerations of alternate models.

APPENDIX: Proof That The Source Entropy $\geq$ Von Neumann Entropy

Let σ be any normalized state, and let (u_k) be an orthonormal basis of eigenvectors for $\sigma = \sum_k \sigma_k u_k \otimes u_k^*$, $\sum\limits_k \sigma_k = 1$ $\forall$ $x \in$ *FG(2)*, $\langle \delta_x \; | \sigma(\delta_x) \rangle = \sum_k \sigma_k |u_{kx}|^2$, where $u_{kx} = \langle \delta_x | u_k \rangle$. Since the function η is convex downward and $\sum_k |u_{kx}|^2 = |\delta_x \; |^2 = 1$, $\eta(\langle \delta_x \; | \sigma(\delta_x) \rangle) \geq \sum_k \eta(\sigma_k) |u_{kx}|^2$. Now sum on x, and we see

source entropy$(\sigma) \geq \sum_x \sum_k \eta(\sigma_k) |u_{kx}|^2 = \sum_k \eta(\sigma_k) \sum_x |u_{kx}|^2 =$
$\sum_k \eta(\sigma_k) = \text{Trace}(\eta(\sigma)) =$ von Neumann entropy(σ).

References

[BEZ] D. Bouwmeester, Artur Ekert, Anton Zeilinger (Eds.), *The Physics of Quantum Information.* New York: Springer-Verlag, 2000.

[Gr] H. S. Green, *Information Theory and Quantum Physics.* New York: Springer-Verlag, 2000 .

[KB] S. Kullback, *Information Theory and Statistics.* New York: Dover Publications, 1968.

[Ma] G. Mackey, *Mathematical Foundations of Quantum Mechanics.*New York: W. A. Benjamin, Inc., 1963 .

[Na] M.A. Naimark, *Normed Rings.* Groningen, The Netherlands: P Noordhoff, Ltd., 1964

[NG] I. Nielsen and Isaac Chaung, *Quantum Computation and Quantum Information.* New York: Cambridge University Press, 2002 .

[PS] Michael E. Peskin, *Introduction to Quantum Field Theory.* New York: HarperCollins, 1995.

[TP] A. Figa-Talamanca and M. Picardello, *Harmonic Analysis on Free Groups.* New York: Marcel-Dekker, Inc., 1983.

[TR3] R. D. Ogden, *Harmonic Analysis in the Free Group with Two Generators.*Technical Report #3, Computer Science Department, Texas State University at San Marcos, to appear.