Journal of Physical Mathematics
ISSN: 2090-0902

Sowa, J Phys Math 2016, 7:2
http://dx.doi.org/10.4172/2090-0902.1000180

Research Article Open Access

The Quantum Sieve of Eratosthenes

Sowa A*

Department of Mathematics and Statistics, University of Saskatchewan, Canada

Abstract

We introduce and examine quantum states of a special kind, referred to as E-states, whose properties are both structurally and functionally analogous to the sieve of Eratosthenes. More broadly, the concept of an E-state is related to a certain noncommutative extension of the Dirichlet ring, also discussed here for the first time. Furthermore, we demonstrate that E-states can be implemented on a universal quantum computer and, as a particular application, we construct an algorithm which implements the Dirichlet multiplication of sequences on a quantum computer. We also discuss the potential applicability of E-states to the problem of integer factorization although, we haste to add, we are not aware at present of the possibility of using this approach to obtain algorithms of sub-exponential complexity.

Keywords: Quantum sieve; Quantum algorithm for Dirichlet multiplication (convolution); Integer factorization

Introduction

Quantum parallelism is a phenomenon that Nature herself seems to be suggesting as a means to getting around repetitive chores of forbidding duration. It is the cornerstone of most if not all interesting quantum computing schemas and the main factor responsible for computational speedups of some quantum algorithms, e.g. Shor's pioneering integer factorization algorithm, [1]. Arguably, quantum parallelism may be so distinct a feature of quantum algorithms that the efficiency some of them provide will remain unachievable within the Church-Turing'ian model of computation [2,3].

In this article we explore possible advantages of some quantum structures deemed analogous to the classical sieve of Eratosthenes. The main idea is to set a bipartite quantum system in a state of the form $\Sigma a_{lk}|l\rangle\ k\rangle$ with amplitudes a_{lk} nonzero only if $k|l$ (i.e. l can be divided by k without remainder). We refer to such states as Eratosthenian states or, simply, E-states. If we were skilled in the art of creating E-states with good control they could be used for efficient integer factorization. Suppose we wanted to find a divisor K of N, where N is a number with $n\sim\log N$ bits (in binary representation). All we would have to do is implement an E-state with only a polynomial in n quantity of comparable-magnitude amplitudes $a_{lk}\neq 0$, including $a_{Nk}\neq 0$. If such a state were created we would be able to find the factor K of N with only a polynomial in n number of trials. Note that for a construction of such a state K need not be known *a priori*. Instead, it would suffice to ensure that the state is an E-state and that its nonzero amplitudes would have the first index concentrated near N, which is much more generalist a description. The challenge is to find ways of implementing such states. In Section 3 we propose several ways of implementing E-states on a quantum computer. Unfortunately all the methods we have found thus far result in a number of nonzero amplitudes that is exponential in n. However, it is not clear if this should be inevitable. Is there a fundamental constraint preventing successful realization of E-states with amplitudes concentrated in small areas of interest? For now this is an open question. A sceptic might argue that perhaps the whole idea should be dismissed as backward, given that a superior algorithm is already known—namely, the algorithm of Shor. However, we take an opposing view. Indeed, we find the concept to be intriguing for at least these three reasons: First, we do not exclude the possibility that future research could bring a discovery of a method enabling construction of very rarefied E-states with only a polynomial in n number of nonzero amplitudes placed in targeted places. Alternatively, in time we may be able to understand the fundamental reasons why this is impossible or intractable, e.g. by finding arguments for uncomputability of such states or at least a revealing constraint on the required physical resources. Second, as demonstrated in subsection 3.4, the concept of E-states enables implementation of the Dirichlet multiplication on a quantum computer. This new algorithm is interesting in its own right. Third, as shown in Subsection 2.2 the set of E-matrices (a notion slightly more general than that of E-states, the latter necessarily requiring normalization) forms a noncommutative ring, which extends the classical Dirichlet ring. We feel that an occurrence of a fundamental and, to our knowledge, entirely new algebraic structure further strengthens the case for E-states.

It is one of the conclusions reached in this paper that the algebra of the Dirichlet polynomials — i.e. objects of the type $\sum a_n n^{-s}, s\in\mathbb{C}$, where the sum is finite — may be handled by a quantum computer. This extends our earlier work in which we demonstrated that the Dirichlet polynomials may be efficiently manipulated on a classical computer. In both cases the manipulation of Dirichlet polynomials is enabled by their matrix representation (which also extends to the infinite Dirichlet series). This fact has numerous practical applications [4-6].

Eratosthenian Matrices and Eratosthenian Quantum States

E-matrices

Consider a matrix $A=[a_{nk}]$, and either $n,k\in\{1,2\ldots N\}$ or both indices run over the entire set of positive integers $\mathbb{N}$. We will say that A is Eratosthenian (an E-matrix for short) if and only if.

$$a_{nk}\neq 0\Rightarrow k\,|\,n.$$

When written explicitly an E-matrix assumes the form

***Corresponding author:** Sowa A, Associate Professor, Department of Mathematics and Statistics, University of Saskatchewan, Canada, Tel: 154445354154; E-mail: sowa@math.usask.ca

Received April 08, 2016; **Accepted** June 22, 2016; **Published** June 27, 2016

Citation: Sowa A (2016) The Quantum Sieve of Eratosthenes. J Phys Math 7: 180. doi:10.4172/2090-0902.1000180

$$E=\begin{bmatrix} a_{11} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ a_{21} & a_{22} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ a_{31} & \cdot & a_{33} & \cdot & \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ a_{41} & a_{42} & \cdot & a_{44} & \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ a_{51} & \cdot & \cdot & \cdot & a_{55} & \cdot & \cdot & \cdot & \dots & \cdot \\ a_{61} & a_{62} & a_{63} & \cdot & \cdot & a_{66} & \cdot & \cdot & \dots & \cdot \\ a_{71} & \cdot & \cdot & \cdot & \cdot & \cdot & a_{77} & \cdot & \dots & \cdot \\ a_{81} & a_{82} & \cdot & a_{84} & \cdot & \cdot & \cdot & a_{88} & \dots & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \cdot \\ a_{N1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & a_{NN} \end{bmatrix} \tag{1}$$

where the entries represented by centred dots are necessarily zeros, and only if $k|n$ the entry a_{nk} may be nonzero. If an E-matrix E is N-by-N, we write $E\in\mathcal{E}_N$ and if it is infinite, extending indefinitely to the right and down, we write $E\in\mathcal{E}_\infty$. Note that the number of nonzero elements in the n'th row of an E -matrix is at most $d(n)$ (i.e. the number of divisors of n). For $E\in\mathcal{E}_N$ the overall number of nonzero entries is at most $\sigma(N)=d(1)+d(2)+\ldots+d(N)=O(N\log N)$, [7].

It is demonstrated in Subsection 2.2 that every $\mathcal{E}_N$, $N\in\{2,3,4\ldots\}\cup\{\infty\}$, is a ring with respect to the regular matrix addition and multiplication. We also point out that every $\mathcal{E}_N$ contains a nontrivial commutative subring. To see this we introduce the following definition. Namely, we say that an E-matrix is a Dirichletian matrix (D-matrix for short) if $a_{nk}=\alpha_{n/k}$ for a sequence$[\alpha_1, \alpha_2\ldots]$ which may be finite or infinite. We let $\mathcal{D}_N$, $N\in\{2,3,4\ldots\}\cup\{\infty\}$ denote the set of all N-by-N D-matrices. It is easily seen that $\mathcal{D}_N$ is a commutative subring of $\mathcal{E}_N$. Also, it is known, see [6], that $\mathcal{D}_\infty$ is isomorphic to the Dirichlet ring, i.e. the ring of infinite sequences with component-wise addition and the Dirichlet multiplication[1]

$$(\alpha\star\beta)_n=\sum_{d:d|n}\alpha_{n/d}\beta_d. \tag{2}$$

Therefore, $\mathcal{E}_\infty$ furnishes a noncommutative extension of the Dirichlet ring.

E-matrices form a noncommutative ring

Readers who are interested only in the quantum-computing applications of E-matrices may skip this subsection.

Theorem 2.1: *Let $N\in\{2,3,4\ldots\}\cup\{\infty\}$. $\mathcal{E}_N$ is a ring with respect to the operations of matrix addition and multiplication. The ring has a unity given by the identity matrix I. For $A,B\in\mathcal{E}_N$, $AB=I$ if and only if $BA=I$. Moreover, $A\in\mathcal{E}_N$ has an inverse (in $\mathcal{E}_N$) if and only if all the diagonal entries of A are nonzero.*

Proof: It is obvious that $\mathcal{E}_N$ is a group with respect to matrix addition. Furthermore, the identity matrix clearly is the unit of multiplication. Next, we verify that the product of two E matrices is an E-matrix. Indeed, for $A,B\in\mathcal{E}_N$ let $[c_{nk}]=C=AB$. We have

$$c_{nk}=\sum_l a_{nl}b_{lk}=\sum_{d:d|n}a_{nd}b_{dk}=\sum_{d:k|d|n}a_{nd}b_{dk}. \tag{3}$$

(Here,$k|d|n$ is used as shorthand for: $k|d$ & $d|n$.) Thus, for the right-hand side sum to be nonzero at least one of the terms must be nonzero, which implies $k|n$, i.e. C is an E-matrix.

It follows from (3) that if $A,B\in\mathcal{E}_N$ and $AB=I$, then $a_{nn}b_{nn}=1$. Thus, for a matrix $A\in\mathcal{E}_N$ to have a left or right inverse in $\mathcal{E}_N$ it is necessary that all its diagonal entries be nonzero. Next, let $A=[a_{nk}]\in\mathcal{E}_N$ and $a_{nn}\neq0$ for all n. We will construct $B\in\mathcal{E}_N$ such that $AB=I$. Indeed, suppose:

$$\delta_{nk}=\sum_{d:k|d|n}a_{nd}b_{dk}, \tag{4}$$

Where $\delta_{nk}\in\{0,1\}$ is the Kronecker delta. This determines the diagonal entries of B, namely, $b_{nn}=1/a_{nn}$ for all n. In addition, if $k|n$, $k<n$, then (4) implies:

$$b_{nk}=-\frac{1}{a_{nn}}\sum_{d:d<n,k|d|n}a_{nd}b_{dk}. \tag{5}$$

Note that (5) determines b_{nk} via b_{mk} $(k|m)$ with $m<n$. This furnishes a recurrence formula for the off-diagonal entries of B that is the right inverse of A. If A is finite it is clear that B is also the left inverse, i.e. $BA=I$. Therefore, in the rest of the proof we assume that A is infinite. We will find its left inverse $C\in\mathcal{E}_N$, i.e. $CA=I$. As before, assume:

$$\delta_{nk}=\sum_{d:k|d|n}c_{nd}a_{dk}. \tag{6}$$

It follows that $c_{nn}=1/a_{nn}$ for all n. Furthermore, if $k<n$, $k|n$, (6) implies:

$$c_{nk}=-\frac{1}{a_{kk}}\sum_{d:d>k,k|d|n}c_{nd}a_{dk}. \tag{7}$$

This gives recurrence for c_{nk} if the indices are suitably ordered. Namely, if $l|m$ and $k|n$ we say $(m,l)\prec(n,k)$ if either $m<n$ or $m=n$ and $l>k$. Observe that in (7) c_{nk} is determined via c_{nl} with $(n,l)\prec(n,k)$. Thus construction by recurrence yields C such that $CA=I$. Finally, note that $C=CI=CAB=IB=B$, i.e. the left and the right inverses of A are equal. This completes the proof.

Corollary 2.1: *The ring $\mathcal{E}_N$, $N\in\{2,3,4\ldots\}\cup\{\infty\}$, is not local.*

Proof: In light of Theorem 2.1 we see that the set of non-invertible elements in $\mathcal{E}_N$ $(N>2)$ or $\mathcal{E}_\infty$ is not additively closed. Indeed, the sum of two E matrices each with some zeros on the diagonal can yield a matrix whose all diagonal entries are all nonzero. The claim then follows from Theorem 7.1.1 in [8].

Remark 1: Note that the set of all matrices in $\mathcal{E}_N$ (or $\mathcal{E}_\infty$) with a zero column (resp. zero row) is a left (resp. right) ideal. The fact that a ring is not local means that the set of non-invertible elements is not a two-sided ideal. Moreover, neither of the rings has a largest proper left or right ideal, [8].

Remark 2: Note that the recurrence formulas (5) or (7) yield the inverse matrix by filling up consecutively increasing blocks. This can be viewed alternatively in the following way. A matrix $A\in\mathcal{E}_N$ has a block structure as follows:

$$A=\begin{bmatrix} & & 0 \\ & \tilde{A} & \vdots \\ & & 0 \\ a_{N1}\ldots a_{N,N-1} & & a_{NN} \end{bmatrix}, \text{with } \tilde{A}\in\mathcal{E}_{N-1} \text{ and } a_{Nk}\neq0\Rightarrow k\mid N.$$

Suppose $\det A=\prod_n a_{nn}\neq0$, and let us look for A^{-1} in the form,

$$\begin{bmatrix} & & 0 \\ & \tilde{A}^{-1} & \vdots \\ & & 0 \\ x_1\ldots x_{N-1} & & x_N \end{bmatrix}, \quad \text{and } x_k\neq0\Rightarrow k\mid N.$$

In such a case $A^{-1}A=I$ is equivalent to the following set of constraints:

$$\sum_{k:n|k|N}x_k a_{kn}=\delta_{nN} \quad \text{for all } n \text{ such that } n\mid N. \tag{8}$$

[1]Note that $\mathcal{D}_N$ with N finite inherit the Dirichlet multiplication with obvious modifications. These are the only objects that one can hope to implement numerically.

Let $X=[x_1,\ldots x_d,\ldots x_N]$ be the vector whose entries are x_d with $d|N$ in the natural order. Observe that (8) has the form $XM=[0,\ldots 1]$ *where M is a suitable upper triangular d(N)-by-d(N) matrix, and* $\det M=\prod_{n|N} a_{nn}\neq 0$. *Therefore* $X=[0,\ldots 1]M^{-1}$ is the unique solution of (8).

Quantum E-states

Consider a pair of quantum systems which, when in isolation, have the dynamics determined by the Hamiltonians $H_i:\mathcal{H}_i\to\mathcal{H}_i$ (i=A,B), where $\mathcal{H}_i$ represent the respective Hilbert-spaces of states. Let $H_i|n_i\rangle=E_n^i|n_i\rangle$ denote the eigenbasis induced by H_i, i.e. $H_i|n_i\rangle=E_n^i|n_i\rangle$. For our purposes it is necessary to assume that $E_n^i\neq E_n^i$, so that all the eigenspaces of H_i are 1-dimensional. When the mutual isolation of the quantum systems at hand is violated, the pair need to be considered as a composite (more specifically, *bi-partite*) system. Now, the individual states no longer hold any meaning and are superseded by a composite state $|\Psi\rangle\in\mathcal{H}_A\otimes\mathcal{H}_B$ whose dynamics, in the simplest possible case[2], is determined by the composite system Hamiltonian,

$$H_{comp}=H_A\otimes I_B+I_A\otimes H_B:\mathcal{H}_A\otimes\mathcal{H}_B\to\mathcal{H}_A\otimes\mathcal{H}_B. \tag{9}$$

Suppose the composite system is initialized in the state,

$$|\Psi_E\rangle=\sum_{(n,k)\in\mathbb{N}^2} a_{nk}|n_A\rangle|k_B\rangle, \tag{10}$$

Where $E=[a_{nk}]$ is an E-matrix with the Hilbert-Schmidt norm $\|E\|_{H-S}=\|\Psi_E\|=\left(\sum|a_{nk}|^2\right)^{1/2}=1$. The Schrödinger dynamics $i|\dot{\Psi}\rangle=H_{comp}|\Psi\rangle$ with the initial condition $\Psi(0)=\Psi_E$ amounts to a separable evolution of the coefficients and so $|\Psi(t)\rangle=\sum a_{nk}(t)|n_A\rangle|k_B\rangle$, where $a_{nk}(t)=a_{nk}\exp[i(E_N^A+E_k^B)t]$. This means that if $|\Psi(t)\rangle$ is represented in the $|n_A\rangle|k_B\rangle$ basis via an E-matrix at one time, it will remain to be represented by an E-matrix for all times. It is therefore justifiable to call an evolving state as this an *E-state*. Since time evolution of the phase factors is inconsequential for the discussion that follows we will make no further reference to it.

Quantum measurements and integer factorization

Suppose an E-state $|\Psi(E)\rangle$ has been prepared in such a way that $a_{nk}\neq 0\Rightarrow k|n$. Suppose we wish to factor a specific integer N. A measurement of the composite system energy returns a pair $((n,k))$ where with probability one $k|n$. However, the probability of drawing such a pair is exactly $|a_{nk}|^2$. This means that if all $|a_{nk}|$ have comparable magnitude, we need at least $\sigma(N)=O(N\log N)$ trials to find a specific pair — the number of trials is exponential in log N or exponential in the number of bits used to represent N. This would change if we were able to prepare the system in an E-state concentrated on the components of the form $|n_A\rangle|k_B\rangle$ where $k|n$. This is, of course, a hard problem. We discuss it from the point of view of quantum computing in Section 3.

E-states on a quantum computer

In this section we consider two different approaches to the construction of an E-state on a quantum computer. The first method relies upon the quantum multiplication circuit, while the second utilizes a quantum gate implementation of a specific arithmetic function. In both cases the resulting state is a superposition of a pure E-state with some additional "artefact" state components. However, as explained below, the pure E-state components are separated from the artefact components by their index range. Thus pure components can be separated a posteriori by a rudimentary classical observation or, alternatively, enhanced via the procedure known as amplitude amplification, [9].

The departure point for both constructions is the known process for creating an equal superposition state, see e.g. [10]. This is obtained by an application of the single qubit Hadamard gates to the ground state:

$$\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle=H^{\otimes n}|0\rangle. \tag{11}$$

An E-state from quantum multiplication

We will demonstrate how to prepare an E-state on a quantum computer with a quantum random access memory consisting of two registers. We let $|x\rangle$ $|y$ denote the state of the registers, where it is understood that $|x\rangle=|x_1,x_2,x_3,..x_n\rangle$ is an n-qubit representation and, similarly, $|y\rangle=|y_1,y_2,y_3,..y_n\rangle$. Well known are quantum computing implementations of certain basic arithmetical operations, see e.g. [11,12] including addition and multiplication. We will make use of the multiplication circuit, implementing $|x\rangle=|x_1,x_2,x_3,..x_n\rangle$

$$|x\rangle|y\rangle\mapsto|x\rangle|x.y\rangle$$

Where $x.y$ denotes the product of two integers. (Here, multiplication may be effectively replaced by multiplication mod 2^{2n}.) However, since multiplication by zeros is not interesting we introduce a modification. Namely, we first add 1 to both x and y, effectively using

$$|x\rangle|y\rangle\mapsto|x+1\rangle|(x+1)(y+1)\rangle \tag{12}$$

Note that $|x\rangle\mapsto|x+1\rangle$ is unitary, and implementable as simplified addition, as long as the register is by one qubit larger that the maximal value of x. Similarly, unitarity implies that $|x+1\rangle|(x+1)(y+1)\rangle$ cannot fall off the register range. Therefore, the second register should have at least $M=2^{2n}$ qubits. We will now combine (11) with (12) to create an E-state. Indeed, in step one we set both registers in the equal superposition states:

$$|0\rangle|0\rangle\mapsto\frac{1}{2^n}\sum_{x=0}^{2^n-1}|x\rangle\sum_{y=0}^{2^n-1}|y\rangle\mapsto\frac{1}{2^n}\sum_{x=1}^{2^n}\sum_{y=1}^{2^n}|x\rangle|x\cdot y\rangle=:|\Psi_{out}\rangle. \tag{13}$$

The output state is very similar to an E-state except for some artefacts. The artefacts can be effectively dealt with either by treating them as a tolerable nuisance, and doing nothing until the quantum information is accessed, or else countermanding them via an application of the Grover's search (amplitude amplification). We illustrate the procedure by an example with n=2, and M=n^2=4. Note that the first register must support n+1=3 qubits. The end state in this case has the form (here c=1/4):

	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$	$\|4\rangle$	$\|5\rangle$	$\|6\rangle$	$\|7\rangle$	$\|8\rangle$	$\|9\rangle$	$\|10\rangle$	$\|11\rangle$	$\|12\rangle$	$\|13\rangle$	$\|14\rangle$	$\|15\rangle$
$\|1\rangle$	·	c	c	c	c	·	·	·	·	·	·	·	·	·	·	·
$\|2\rangle$	·	·	c	·	c	·	c	·	c	·	·	·	·	·	·	·
$\|3\rangle$	·	·	·	c	·	·	c	·	·	c	·	·	c	·	·	·
$\|4\rangle$	c	·	·	·	c	·	·	·	c	·	·	·	c	·	·	·

Note that not shown are rows corresponding to the states $|5\rangle$,$|6\rangle$,$|7\rangle$ or $|0\rangle$ on the first register—these rows contain only zero entries. Furthermore, note that the submatrix corresponding to values $|1\rangle$,$|2\rangle$,$|3\rangle$,$|4\rangle$ on the second register is the transpose of an E-matrix[3]. We also note that a measurement on both registers returns a pair of integers (a,b) where, $a|b$. (In the example at hand the special pair (4,0) signifies (4,16)). Note that those components of the output state that correspond to values other than $|1\rangle$,$|2\rangle$,$|3\rangle$,$|4\rangle$ on the second register cannot be erased, because such an operation would not be unitary. However, the resulting state contains an E-state as a separable component. Summarizing, the

[2]An example of this type of a quantum system is a decoupled spin-pair in an NMR experiment.

[3]The transposition stems from the fact that we adhere to the conventional organization of the quantum circuit operations. A reversal of the order of the registers results in an E-matrix as defined in Section 2.

proposed algorithm for the creation of an approximate E-state consists of the following steps:

- Prepare an initial state according to (11).
- Compute the (shifted) quantum product according to (13). As a result obtain an output state $|\Psi_{out}\rangle=|\Psi_E\rangle+|\Psi_R\rangle$, where $|\Psi_E\rangle$ is (proportional to) an E-state and $|\Psi_R\rangle$ is a remainder.
- Separate $|\Psi_E\rangle$ classically in the following sense: the measurement outcomes that belong in an E-state component are precisely those $|x\rangle|z\rangle$ where z∈{1,2…2^n}
- Optionally, depending on an application, it may be beneficial to engage the generalized Grover's search as a processing step preceding the classical separation. This step provides amplitude amplification, effectively boosting the weight of the $|\Psi_E\rangle$ component and suppressing that of the $|\Psi_R\rangle$.

Remark 1: Note that the probability of an outcome that is an E-state component is $(d(1)+d(2)+\ldots d(2^n))/2^{2n}\sim 2^n\log 2^n/2^{2n}\sim n/2^n$. However, measurements on the full output state provide useful information, and separation of the E-state pointed out in the last step of the algorithm need not always be desirable. We emphasize that the probability of obtaining from measurement any pair $a|b$ is always the same and equal to 2^{-2n}.

Remark 2: The network complexity for multiplication of two registers is of the order n^2. There are several known circuit architectures implementing multiplication. While some implementations rely on the quantum Fourier transform, [12], the classical Vedral-Barenko-Ekert algorithm does not use it, [11]. Even though the latter algorithm demands a greater memory resource, it seems to secure computational stability independent of the input size.

Remark 3: Recall that the Grover search, as well as its various generalizations known as the *amplitude amplification algorithms*, [9], rely on the Grover rotation. To briefly summarize the principle and compute the complexity, we turn attention to $|\Psi_{out}\rangle=|\Psi_E\rangle+|\Psi_R\rangle$. The quantities $a=\langle\Psi_E|\Psi_E\rangle$ and $b=\langle\Psi_R|\Psi_R\rangle$ represent the probabilities of measuring a good component, in the support of $|\Psi_E\rangle$, and a bad component in the support of $|\Psi_R\rangle$. We wish to apply a quantum circuit to $|\Psi_{out}\rangle$ so as to boost the probability of measuring the good component. To this end we use the Grover's rotation:

$$|\Psi\rangle\mapsto G|\Psi\rangle=\left(2|\Psi\rangle\langle\Psi|-I\right)\left(-\frac{2}{a}|\Psi_E\rangle\langle\Psi_E|+I\right)|\Psi\rangle.$$

Grover's rotation is applied k times to $|\Psi_{out}\rangle$ so that $G^k|\Psi_{out}\rangle$ approaches $a^{-1/2}|\Psi_E\rangle$. The value of k depends on the initial partition of energy between $|\Psi_E\rangle$ and $|\Psi_R\rangle$ or, in other words, the ratio of the number of good states to the number of bad states. We have,

$$k=O\left(\sqrt{2^{2n}/\sigma(2^n)}\right)=O\left(\sqrt{2^{2n}/(2^n\log 2^n)}\right)=O(2^{n/2}/\sqrt{n}),$$

i.e. the number of iterations is essentially exponential in n.

An E-state from $f(x)=[N/x]$. x.

This method is based on a quantum implementation of the arithmetic function $f(x)=[N/x].x$, $x\in\mathbb{N}$. (We will not discuss the specific circuit implementation of this function, all reversible classical functions can be converted into quantum computations [13]. We wish to construct an E-state concentrated near the N'th column, where N<2^n. To this end we prepare the state $2^{-n/2}\sum_{x=1}^{2^n}|x\rangle$ on the first register and subsequently implement a two-register operation.

$$2^{-n/2}\sum_{x=1}^{2^n}|x\rangle|0\rangle\mapsto 2^{-n/2}\sum_{x=1}^{2^n}|x\rangle|[N/x]\cdot x\rangle. \qquad (14)$$

The result is a relatively sparse E-state in superposition with an artefact vector. Let us illustrate this with an example for N=6. Selecting n=3, we obtain the following state matrix ($c=1/\sqrt{8}$):

	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$	$\|4\rangle$	$\|5\rangle$	$\|6\rangle$	$\|7\rangle$
$\|0\rangle$	·	·	·	·	·	·	·	·
$\|1\rangle$	·	·	·	·	·	·	c	·
$\|2\rangle$	·	·	·	·	·	·	c	·
$\|3\rangle$	·	·	·	·	·	·	c	·
$\|4\rangle$	·	·	·	·	c	·	·	·
$\|5\rangle$	·	·	·	·	·	c	·	·
$\|6\rangle$	·	·	·	·	·	·	c	·
$\|7\rangle$	c	·	·	·	·	·	·	·
$\|8\rangle$	c	·	·	·	·	·	·	·

Note that the first register requires 4 qubits, and only part of it is shown. The E-state submatrix is indexed by $|1\rangle\ldots\ldots|6\rangle$ on both registers. As before there is some overflow of energy to artefact state components, in this case, $c|7\rangle|0\rangle+c|8\rangle|0\rangle$. As before the artefact components can be separated classically *a posteriori* or suppressed via amplitude amplification [13].

Note that in general a measurement will result in drawing a nontrivial divisor of N with probability $2^{-n}(d(N)-2)$. Again, one may apply the Grover's rotation in order to bring the state close to the state supported on the $d(N)$-2 good components, which requires $k=O(\sqrt{2^n/(d(N)-2)})$ iterations.

Applying the quantum Fourier transform

Let us briefly examine the effect of an application of the quantum Fourier transform (QFT) to an E-state. In the next subsection we will discuss the topic from a more general point of view, but it is helpful to first focus on the E-state part of $|\Psi_{out}\rangle=|\Psi_E\rangle+|\Psi_R\rangle$ as in (13). As remarked above, $|\Psi_E\rangle$ is separated from the remainder $|\Psi_R\rangle$ by the second register range 1≤z≤2^n. We will refer to the $|\Psi_R\rangle$ term as 'out of bounds' (OOB). Thus,

$$|\Psi_{out}\rangle=\frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{x|z}|x\rangle|z\rangle+OOB=\frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{x=1}^{2^n}\delta_{.|z}(x)|x\rangle|z\rangle+OOB,$$

Where $\delta_{.|z}(x)$=1 if x $|z$ and $\delta_{.|z}(x)$=0 otherwise. Recall, [9], that the n-qubit QFT is defined via

$$|x\rangle\mapsto\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{2\pi ixy/N}|y\rangle,\quad N=2^n,x\in\{0,1,\ldots,N-1\}.$$

Applying the shift $|x\rangle\mapsto|x\text{-}1\rangle$ on the first register, and setting $f_z(x)=\delta_{.|z}(x+1)$ followed by the QFT yield

$$|\Psi_{out}\rangle\mapsto\frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{x=0}^{2^n-1}f_z(x)|x\rangle|z\rangle+OOB\mapsto\frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{k=0}^{2^n-1}\hat{f}_z(k)|k\rangle|z\rangle+OOB,$$

where for all z $\hat{f}_z(k)$ is the discrete Fourier transform of f_z. It is interesting to observe that $\hat{f}_z(0)=2^{-n/2}d(z)$. Therefore, if the output state has been prepared as this, then from among the output states of the form $|0\rangle|z\rangle$, the more highly composite numbers, i.e. those with larger $d(z)$, are more likely to be measured.

The Dirichlet product of state vectors

In recent years there has been a trend in quantum computing to go beyond the realm of discrete algorithms and consider the possibility of manipulating the vectors represented in quantum state amplitudes. A representative example of that trend is reference [14], wherein the

authors address the problem of solving on a quantum computer the linear equation $[\beta_1,\beta_2,\ldots]^T = A[\alpha_1,\alpha_2,\ldots]^T$. Here $|\alpha\rangle=\Sigma\alpha_x|x\rangle$ is regarded as given, A is a classically known matrix, and $|\beta\rangle=\Sigma\ \beta_x|x\rangle$ is to be computed. Of course, prerequisite to this procedure is the possibility of implementing on a register the state $|\alpha\rangle$ with the particular set of amplitudes. One method for accomplishing that is indicated in [15]. We base the following discussion on the possibility of implementing a state

$$|0\rangle \mapsto \sum_{x=1}^{2^n}\alpha_x|x\rangle, \tag{15}$$

where $\{|\alpha_x|^2\}$ is a probability distribution[4] on $\{1,2,\ldots 2^n\}$ With this understood, we will now show how to use the concepts introduced in the preceding paragraphs to describe an implementation of new types of E-states as well as the realization of the Dirichlet multiplication of the amplitude vectors. First, consider a straightforward generalization of (13). Namely,

$$|0\rangle|0\rangle \mapsto \frac{1}{2^n}\sum_{x=1}^{2^n}\alpha_x|x\rangle\sum_{y=1}^{2^n}\beta_y|y\rangle = \frac{1}{2^n}\sum_{x=1}^{2^n}\sum_{y=1}^{2^n}\alpha_x\beta_y|x\rangle|y\rangle \mapsto \frac{1}{2^n}\sum_{x=1}^{2^n}\sum_{y=1}^{2^n}\alpha_x\beta_y|x\rangle|x\cdot y\rangle =: |\Psi_{out}\rangle. \tag{16}$$

Let us examine an example, assuming n=2, and M=n^2=4 (M=4 is the number of qubits required for the second register, and n+1=3 is the number of qubits required for the first register.) In such a case $|\Psi_{out}\rangle$ assumes the form:

	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$	$\|4\rangle$	$\|5\rangle$	$\|6\rangle$	$\|7\rangle$	$\|8\rangle$	$\|9\rangle$	$\|10\rangle$	$\|11\rangle$	$\|12\rangle$	$\|13\rangle$	$\|14\rangle$	$\|15\rangle$
$\|1\rangle$	·	$\alpha_1\beta_1$	$\alpha_1\beta_2$	$\alpha_1\beta_3$	$\alpha_1\beta_4$	·	·	·	·	·	·	·	·	·	·	·
$\|2\rangle$	·	·	$\alpha_2\beta_1$	·	$\alpha_2\beta_2$	·	$\alpha_2\beta_3$	·	$\alpha_2\beta_4$	·	·	·	·	·	·	·
$\|3\rangle$	·	·	·	$\alpha_3\beta_1$	·	·	$\alpha_3\beta_2$	·	·	$\alpha_3\beta_3$	·	·	$\alpha_3\beta_4$	·	·	·
$\|4\rangle$	$\alpha_4\beta_4$	·	·	·	$\alpha_4\beta_1$	·	·	·	$\alpha_4\beta_2$	·	·	·	$\alpha_4\beta_3$	·	·	·

Note that the 4-by-4 submatrix under the registers one-to-four supports an E-state component. In general, we have

$$|\Psi_{out}\rangle = \frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{x|z}\alpha_x\beta_{z/x}|x\rangle|z\rangle + OOB = \frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{x=1}^{2^n}\delta_{x|z}(x)\alpha_x\beta_{z/x}|x\rangle|z\rangle + OOB$$

This is much more general an E-state than that obtained in (13).

Next, we perform further computation of the output state. We first shift $|x\rangle\mapsto|x\text{-}1\rangle$ on the first register, and then follow by the QFT on the first register. In detail, by letting $f_z=\delta_{x|z}(x+1)\alpha_{x+1}\beta_{z/(x+1)}$ we obtain,

$$|\Psi_{out}\rangle \mapsto \frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{x=0}^{2^n-1}f_z(x)|x\rangle|z\rangle + OOB \mapsto \frac{1}{2^n}\sum_{z=1}^{2^n}\sum_{k=0}^{2^n-1}\hat{f}_z(k)|k\rangle|z\rangle + OOB.$$

Finally, we observe

$$\hat{f}_z(0) = 2^{-n/2}\sum_{x|z}\alpha_x\beta_{z/x} = 2^{-n/2}\,\alpha\star\beta(z),$$

where $\alpha\star\beta$ is the Dirichlet product (convolution) of the sequences α and β Thus, the component of $|\Psi_{out}\rangle$ distinguished by $|0\rangle$ on the first register is

$$|\Psi_D\rangle := 2^{-3n/2}\sum_{z=1}^{2^n}\alpha\star\beta(z)|0\rangle|z\rangle.$$

Note that the example considered in subsection 3.3 is a special case and returns $d(z)=e\star e(z)$, where e=[1,1,1,..]

Summarizing, the amplitudes at $G^k|\Psi_{out}\rangle$ at $|0|z\rangle$ components hold information about $\alpha\star\beta(z)$. This type of information can only be accessed statistically. We point out yet again that the amplitude amplification via the Grover's search algorithm may be engaged to obtain $G^k|\Psi_{out}\rangle\sim|\Psi_D\rangle$. The number of iterations is $k = O(\sqrt{2^{2n}/2^n}) = O(2^{n/2})$.

[4]In fact a harder problem is considered in [15], which is implementation of a state where |αx|2 stems from a discretization of a continuous probability distribution. Also, the reader will note that we have modified the original design by the usual shift of the register index.

Remark: We recall that the known QFT algorithm has $\Theta(n^2)$ complexity. Of course, since the QFT depends on unitary transforms with terms like exp $2\pi i/2^n$ its hardware implementation requires precision (in terns of energy control or ultra-short pulse control, etc.) that is exponential in n. Notably, however, in some applications this difficulty may be overcome by replacing the QFT with the *approximate quantum Fourier transform* (AQFT) introduced in [16]. It is interesting to enquire whether the AQFT might facilitate additional gains also in the task of integer factorization via E-states. However, we do not undertake to address this problem here.

Remarks on E-states of quantum systems in thermal bath

As explained above once an E-state of the form (10) is formed, it will be preserved essentially unchanged in time (except for the unessential phase factors) as long as no measurement is conducted on the composite system. In this section we consider the problem of forming such a state outside the framework of the universal quantum computer. Indeed, one might hope that abandoning the constraint of universality would open more options for achieving such a goal. The approach we consider is based on the thermodynamic equilibrium, and utilizes the results in [17,18].

For simplicity we henceforth assume that $|\Psi_E\rangle$ is effectively finite. The first observation is that an E-state may be reduced to a more standard state via the Schmidt representation. Indeed, let $E=USV^*$ be the SVD decomposition of the matrix $E=[a_{nk}]$ that holds the amplitudes of $|\Psi_E\rangle$. Thus, U and V are unitary matrices while $S=diag[s_1,s_2,s_3,..]$ is a diagonal matrix. Let us define new orthonormal bases for the two subsystems, namely $|e_n^A\rangle = U^*|n_A\rangle$, and $|e_k^B\rangle = V|k_B\rangle$. This gives the Schmidt representation of the E-state

$$|\Psi_E\rangle = \sum s_n|e_n^A\rangle|e_n^B\rangle. \tag{17}$$

We will use these observations to attempt a construction of a quantum system regime in which $|\Psi_E\rangle$ will become its stationary state. The basic concept of adiabatic computing is to switch from the regime that instils $|\Psi_E\rangle$ back to the dynamics governed by the Hamiltonian (9) not disturbing the system state. To this end, one might try to construct an isolated system Hamiltonian for which (17) is a ground state. However, we propose an alternative approach, based on thermodynamic equilibrium at constant temperature. First, we define a Hamiltonian[5] $H_{A-B} = \tilde{H}_A\otimes I_B + I_A\otimes\tilde{H}_B$ where

$$\tilde{H}_A = \sum h_n^A|e_n^A\rangle\langle e_n^A|, \quad and \quad \tilde{H}_B = \sum h_n^B|e_n^B\rangle\langle e_n^B|.$$

Since

$$(H_{A-B}-\nu)|\Psi_E\rangle = \sum(h_n^A + h_n^B - \nu)s_n|e_n^A\rangle|e_n^B\rangle,$$

$|\Psi_E\rangle$is <u>not</u> a stationary state with respect to $H_{A\text{-}B}$, unless the Hamiltonian is completely degenerate $h_n^A = h_n^B = const$. Unfortunately, the completely degenerate Hamiltonian is useless in distinguishing a specific state, since it views any state as stationary. However, consider as an alternative the evolution of the system stabilized by a heat bath at constant temperature T. When the system is in equilibrium, the Helmhotz free energy will be minimized. The Helmholtz free energy is given by:

$$\mathcal{A}[\Psi_E] = \langle\Psi_E|H_{A-B}|\Psi_E\rangle - kT\,S[\rho_A], \quad where\ \rho_A = Tr_B|\Psi_E\rangle\langle\Psi_E|. \tag{18}$$

Here, $S[\rho_A]$= -$Tr[\rho_A\log\rho_A]$ is the von Neumann entropy. Note that $S[\rho_A]$= $S[\rho_B]$ because the entropy depends on the nonzero eigenvalues

[5]We emphasize that HA-B is to be distinguished from Hcomp.

of the mixed state which are equal for both subsystems. Also, since $Tr[\rho_A]=1=const$, we may assume without any change to the dynamics that $S(x)= -x \log x+ x$,so that $-S'(x)= \log x$. Now, Ψ_E will be stationary with respect to the functional $\mathcal{A}$ provided it satisfies the Euler-Lagrange equation

$$0 = (H_{A-B} + kT \log \rho_A \otimes I_B - \nu) | \Psi_E \rangle = \sum (h_n^A + h_n^B + kT \log | s_n |^2 - \nu) s_n | e_n^A \rangle | e_n^B \rangle,$$

and this implies:

$$\forall n: \quad h_n^A + h_n^B = \nu - 2kT \log | s_n |. \tag{19}$$

Recall that $\{s_n\}$ is constrained by the fact that Ψ_E is an E-state in the basis $|n_A\rangle|k_B\rangle$, perhaps an E-state with specific features. This imposes a constraint on the energy levels $h_n^A + h_n^B$. Conversely, if the bipartite quantum system is exposed to a constant temperature T regime with the internal energy H_{A-B}, where H_{A-B} is characterised by the precise values of $h_n^A + h_n^B$ obtained via (19), the system will settle in a stationary state of $\mathcal{A}$. Such a state is then expected to be an E-state w.r.t. the $|n_A\rangle|k_B\rangle$ basis. However, the following questions appear to have fundamental significance as regards feasibility of creating an E-state via the proposed process: First, could the SVD data of an Eratosthenian state be known *a priori* and explicitly? Second, even with the assumption that the SVD data are known a priori, would it be possible to build a machine that instils a regime described by (18) with the precise values of $h_n^A + h_n^B$ obtained via (19)?

Discussion and Results

We have discussed novel algebraic and computational structures based on the concept of Eratosthenian matrices (*E*-matrices) and Eratosthenian quantum states (*E*-states). We have observed that *E*-matrices furnish a noncommutative extension of the classical Dirichlet ring. We have also considered the task of initializing and manipulating *E*-states on a quantum computer and introduced an algorithm that implements the Dirichlet product of quantum state vectors. In addition, we have pointed out that if a method was known for efficient initialization of *E* -matrices with targeted narrow supports it would facilitate efficient factorization of integers.

Acknowledgements

I acknowledge the support of the Canadian Foundation for Innovation, grant LOF # 22117. I am grateful to an anonymous reviewer of this work for the suggestion of the relevance of the *approximate quantum Fourier transform*.

References

1. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Computing 26: 1484-1509.
2. Bernstein E, Vazirani U (1997) Quantum Complexity Theory. SIAM J Comput 26: 1411-1473.
3. Jack Copeland B (2004) The Essential Turing. The ideas that gave birth to the computer age. Oxford Press, Clarendon.
4. Sowa A (2011) A fast-transform basis with hysteretic features. IEEE Conference Proceedings: Electrical and Computer Engineering (CCECE) 253-257.
5. Sowa A (2013) The Dirichlet ring and unconditional bases in $L_2[0,2\pi]$ Func. Anal Appl 47: 227-232.
6. Sowa A (2013) Factorizing matrices by Dirichlet multiplication. Lin Alg Appl 438: 2385-2393.
7. Chandrasekharan K (1970) Arithmetical Functions. Springer-Verlag, Berlin.
8. Kasch F (1982) Modules and Rings. Academic Press, London, New York.
9. Brassard G, Høyer P, Mosca M, Tapp A (2002) Quantum Amplitude Amplification and Estimation, in: Conterporary Mathematics 305 Quantum Computation and Information. Amer Math Soc.
10. Nielsen MA, Chuang IL (2000) Quantum Computation and Quantum Communication.Cambridge University Press,United Kingdom.
11. Vedral V, Barenco A, Ekert A (1996) Quantum networks for elementary arithmetic operations. Phys Rev A 54: 147-153.
12. Florio G, Picca D (2004)Quantum implementation of elementary arithmetic operations. Cornell university Library.
13. Rieffel E, Polak W (2011) Quantum Computing. The MIT Press: Cambridge, Massachusetts, London.
14. Harrow AW, Hassidim A, Lloyd S (2009) Quantum algorithm for linear systems of equations. Phys Rev Lett 103: 150502.
15. Grover L, Rudolph T (2002) Creating superpositions that correspond to efficiently integrable probability distributions.Cornell university Library.
16. Barenko A, Ekert A, Suominen KA, Törmä P (1996) Approximate quantum Fourier transform and decoherence. Phys Rev A 54: 139-146.
17. Sowa A (2009) Stationary states in nonlocal type dynamics of composite systems. J Geom Phys 59: 1604-1612.
18. Sowa A (2011) Spectra of nonlocally bound quantum systems. Russ J Math Phys 18: 227-241.

Citation: Sowa A (2016) The Quantum Sieve of Eratosthenes. J Phys Math 7: 180. doi:10.4172/2090-0902.1000180