Shuffling cards, factoring numbers and the quantum baker's map

2005 J. Phys. A: Math. Gen. 38 L597

(http://iopscience.iop.org/0305-4470/38/37/L01)

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

J. Phys. A: Math. Gen. **38** (2005) L597–L605 doi:10.1088/0305-4470/38/37/L01

LETTER TO THE EDITOR

Shuffling cards, factoring numbers and the quantum baker's map

Arul Lakshminarayan

Department of Physics, Indian Institute of Technology Madras, Chennai, 600036, India

Received 2 June 2005, in final form 28 July 2005
Published 31 August 2005
Online at stacks.iop.org/JPhysA/38/L597

Abstract

It is pointed out that an exactly solvable permutation operator, viewed as the quantization of cyclic shifts, is useful in constructing a basis in which to study the quantum baker's map, a paradigm system of quantum chaos. In the basis of this operator the eigenfunctions of the quantum baker's map are compressed by factors of around five or more. We show explicitly its connection to an operator that is closely related to the usual quantum baker's map. This permutation operator has interesting connections to the art of shuffling cards as well as to the quantum factoring algorithm of Shor via the quantum order finding one. Hence we point out that this well-known quantum algorithm makes crucial use of a quantum chaotic operator, or at least one that is close to the quantization of the left-shift, a closeness that we also explore quantitatively.

PACS numbers: 05.45.Mt, 03.67.Lx

(Some figures in this article are in colour only in the electronic version)

A textbook example of a simple fully chaotic system is provided by the model of a baker mixing dough, the baker's map. The classical baker's map [1], T, is the area preserving transformation of the unit square $[0, 1) \times [0, 1)$ onto itself, which takes a phase-space point (q, p) to (q', p') where $(q' = 2q, p' = p/2)$ if $0 \leqslant q < 1/2$ and $(q' = 2q-1, p' = (p+1)/2)$ if $1/2 \leqslant q < 1$. The stretching along the horizontal q direction by a factor of two is compensated exactly by a compression in the vertical p direction. The repeated action of T on the unit square leaves the phase-space mixed, this is well known to be a fully chaotic system that in a mathematically precise sense is as random as a coin toss [2]. The area-preserving property makes this map a model of chaotic two-degree of freedom Hamiltonian systems and the Lyapunov exponent is $\log(2)$ per iteration.

As the classical baker's map is exactly solvable in many ways, including an explicit prescription for finding periodic orbits of any period, its quantization was sought as a simple model of quantum chaos. The baker's map as quantized by Balazs and Voros [3] has many nice features, including simplicity, that make it ideal for this purpose and has been used extensively in studies of quantum chaos and semiclassical methods. It has also been experimentally implemented recently using NMR [4]. The quantum baker's map, in the position representation, that we use here is

$$B = G_N^{(\frac{1}{2},\frac{1}{2})\dagger} \begin{pmatrix} G_{N/2}^{(\frac{1}{2},\frac{1}{2})} & 0 \\ 0 & G_{N/2}^{(\frac{1}{2},\frac{1}{2})} \end{pmatrix}, \tag{1}$$

where

$$(G_N)_{mn}^{(\alpha,\beta)} = \frac{1}{\sqrt{N}} \exp[-2\pi \mathrm{i}(m+\alpha)(n+\beta)/N]. \tag{2}$$

We require that N be an even integer; Saraceno [5] imposed anti-periodic boundary conditions ($\alpha = \beta = 1/2$) that we use. In this case we drop the superscripts indicating these phases. The Hilbert space is finite dimensional, the dimensionality N being the scaled inverse Planck constant ($N = 1/h$), where we have used that the phase-space area is unity. The position and momentum states are denoted as $|q_n\rangle$ and $|p_m\rangle$, where $m, n = 0, \ldots, N-1$ and the transformation function between these bases is the finite Fourier transform G_N given above.

The choice of anti-periodic boundary conditions fully preserves parity symmetry, here called R, which is such that $R|q_n\rangle = |q_{N-n-1}\rangle$. Time-reversal symmetry is also present and implies in the context of the quantum baker's map that an overall phase can be chosen such that the momentum and position representations are complex conjugates: $G_N\phi = \phi^*$, if ϕ is an eigenstate in the position basis. B is an unitary matrix, whose repeated application is the quantum version of the full left-shift of classical chaos. There is a semiclassical trace formula, which, based on the unstable periodic orbits, approximates eigenvalues [6].

Despite the simplicity of the quantum baker's map, its solution in terms of exact spectra continues to be elusive. Recently we showed [7] that for N that are powers of two, it is possible to write approximate analytic formulae for certain classes of states. In particular the Thue–Morse sequence ($\{1, -1, -1, 1, -1, 1, 1, -1, \ldots\}$, where the nth term is the parity of n when expressed in binary, counting n from zero) [8] and its Fourier transform [9] determine to a large extent a class of states we called 'Thue–Morse states'. Similar expressions were also found for families of strongly scarred states. Despite having simple, if approximate, analytic formulae these states were found to be multifractals. Thus we went some way in solving a quantum chaotic system that is nearly generic. A crucial tool used was the Walsh–Hadamard transform [10]. That is, if ϕ is an eigenstate we studied $H_K\phi$, where $H_K = \otimes^K H$, a K-fold tensor product of the Hadamard matrix $H = ((1, 1), (1, -1))/\sqrt{2}$, where $2^K = N$.

We wish to now address the case of general N and arrive at a counterpart of the Walsh–Hadamard transform that will simplify the states of the quantum baker's map. We show that a simple operator, the shift operator, that is exactly solvable, acts as a good zeroth order operator for the quantum baker's map. Therefore its eigenstates form a basis in which the eigenstates of the quantum baker's map appear simple. We study this operator's action in phase space and show how to build a quantum baker's map around this operator. This 'new' quantum baker will then turn out to be very close to the 'usual' quantum baker's map in equation (1).

The shift operator S, by definition, acts on the position basis as $S|q_n\rangle = |q_{2n}\rangle$ or $|q_{2n-N+1}\rangle$ depending on whether $n < N/2$ or otherwise. We note that S is 'almost' B, only there is no momentum cut-off, as $\langle p_m|B|q_n\rangle = \sqrt{2}\langle p_m|q_{2n}\rangle$ for n and m both $\leqslant N/2 - 1$. In fact S is a generalization of what was proposed as the quantum baker's map by Penrose [11] for the case when $N = 2^K$. In this case if the position state $|q_n\rangle$ is denoted in terms of the binary expansion of $n = a_{K-1}a_{K-2}\cdots a_0$ then $S|a_{K-1}a_{K-2}\cdots a_0\rangle = |a_{K-2}a_{K-3}\cdots a_0a_{K-1}\rangle$. It is easy to see that S commutes with the parity operator R. However S does not respect the usual time-reversal symmetry, relevant to the baker's map, namely $G_N^{-1} S^* G_N \neq S^{-1}$. It does respect a 'restricted' time-reversal symmetry in the case when $N = 2^K$, as $\hat{b}^{-1} S^* \hat{b} = S^{-1}$, where $\hat{b}$ is the bit reversal operator defined as $\hat{b}|a_{K-1}a_{K-2}\cdots a_0\rangle = |a_0 a_1 \cdots a_{K-2}a_{K-1}\rangle$. It is useful to rewrite the action of S on the position basis (written simply as $|n\rangle$) as

$$S|n\rangle = |2n \bmod (N-1)\rangle, \tag{3}$$

with the caveat that $S|N-1\rangle = |N-1\rangle$, rather than $|0\rangle$. This is not crucial as it affects only an one-dimensional invariant subspace.

We point to two apparently unrelated contexts in which S has already appeared. Firstly S is closely related to the perfect 'riffle–shuffle' [12] used to randomize a deck of cards, to be more precise the 'out-shuffle'. If for instance $N = 8$ cards were in a deck, it is split into two exact halves and the cards are then interleaved. If the cards were numbered 0, 1, 2, 3, 4, 5, 6, 7, the out-shuffle brings it to 0, 4, 1, 5, 2, 6, 3, 7, which is easily verified to be the action S^{-1}. The *deterministic* chaos of this shuffling process forms the basis of certain card tricks. The perfect shuffle returns the deck to its original state after a few shuffles, we will see below that this is the 'quantum period function' relevant to S.

Secondly, a generalization of S, where the factor 2 is replaced by any integer (coprime to $N-1$) is precisely the operator whose 'phase estimation' leads to the solution of the order-finding problem [13]. The multiplicative order of 2 modulo $N-1$ is the smallest integer r such that $2^r = 1 \bmod (N-1)$, which is the quantum period again as $S^r = 1$. We are guaranteed that such a number exists as Euler's generalization of Fermat's little theorem implies that $\phi(N-1)$ is such that $2^{\phi(N-1)} \equiv 1 \bmod (N-1)$, thus r is either $\phi(N-1)$ or is a divisor of it (here $\phi(n)$ is the Euler totient function, being the number of positive integers less than n and coprime to it). Finding the multiplicative order is the route of the quantum factoring algorithm of Shor. Thus it is interesting that this well-known quantum algorithm makes critical use of an operator that could be thought of as a quantization of the fully chaotic left-shift, or at least nearly, as explained below.

That the classical limit of the unitary operator S is not the baker's map is made clear by studying its action on coherent states. The structure of S in the position basis is that of a permutation, and its action on the momentum basis is found easily:

$$\langle m'|S|m\rangle = \frac{1}{N} \frac{-\sin[\pi(m'+1/2)/N] + (-1)^{m+1}\cos[\pi(m'+1/2)/N]}{\sin[\pi(m-2m'-1/2)/N]}. \tag{4}$$

Thus the momentum representation is also real. More importantly, for a given initial momentum m, there are two momentum values around which the final state is spread, namely $[m/2]$ or $[m/2] \pm N/2$. Thus the action of S on coherent states would roughly be a combination of its actions on position and momentum states and therefore splits an initial state while performing appropriate scaling. Thus S creates 'squeezed cat states' out of coherent ones, taking a state localized at (q, p) to two that are localized at $(2q \bmod 1, p/2)$ and $(2q \bmod 1, (p+1)/2)$. Repeated action by S on an initial coherent state is illustrated in figure 1 and exact revival occurs for the same reason that a deck of cards under the perfect riffle–shuffle reorders.

Using the action of S we can construct a quantum baker's map. The action of choosing the left or right vertical partition is done by the projectors P_1 and $P_2 = I_N - P_1$, where

$$P_1 = \begin{pmatrix} I_{N/2} & 0 \\ 0 & 0 \end{pmatrix}. \tag{5}$$

The action of stretching and compression is implemented by S, which however produces an extra copy, shifted in momentum by one-half. Thus this is in the other horizontal partition that divides momentum into two equal halves. Thus we once again use projectors, now in

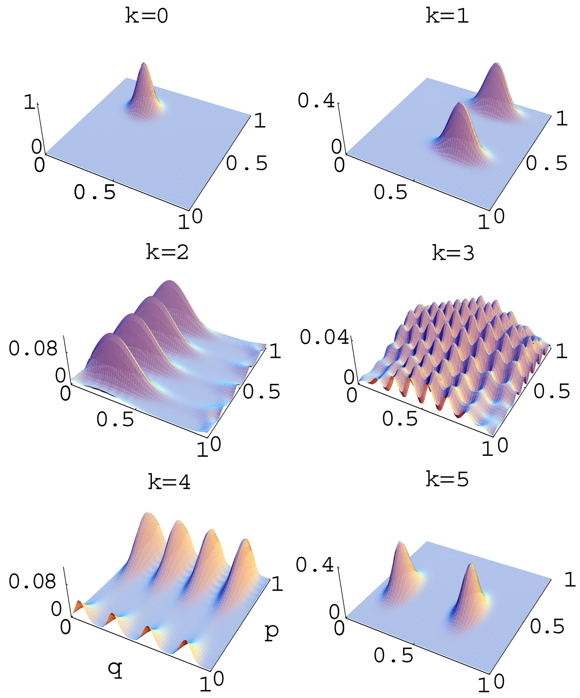

Figure 1. The correlation $|\langle qp|S^k|q_0, p_0\rangle|^2$ as a function of (q, p) for the case of $N = 64$, where $|qp\rangle$ is a toral coherent state localized at (q, p) [5]. Further applying S to the last figure produces the first as in this case S^6 is the identity.

momentum space, to excise the extra copy and complete the action. The full quantum baker built around S is then written as

$$B_S = \sqrt{2} G_N^{-1}(P_1 G_N S P_1 + P_2 G_N S P_2). \tag{6}$$

The factor of $\sqrt{2}$ is essential to restore unitarity after the projecting actions. This is not yet another quantum baker's map since closer inspection shows that it is indeed very close to the usual baker's map in equation (1). This is seen on rewriting B_S as

$$B_S = G_N^{-1} \begin{pmatrix} G_{N/2}^{(\frac{1}{2},\frac{1}{4})} & 0 \\ 0 & \mathrm{i} G_{N/2}^{(\frac{1}{2},\frac{3}{4})} \end{pmatrix} \tag{7}$$

That the usual quantum baker's map is capable of generalizations, including arbitrary phases as boundary conditions and relative phases between the two blocks in the mixed representation is well-known [3], though not all of these 'decorated' baker's maps respect the symmetries of parity and time-reversal. The operator B_S, however, shows the explicit relationship between a quantum baker's map and the solvable operator S, whose action on the position basis is practically the doubling map restricted to the integers. It may be emphasized that even in B_S we are using anti-periodic boundary conditions, the phases of $1/4$ and $3/4$ in the $G_{N/2}$ blocks (as well as the factor of $\mathrm{i} = \sqrt{-1}$) are a direct consequence of the primitive structure in equation (6). That the operator obeys parity symmetry follows from the fact that R_N commutes with G_N and on verifying that

$$R_{N/2} G_{N/2}^{(\frac{1}{2},\frac{1}{4})} = \mathrm{i} G_{N/2}^{(\frac{1}{2},\frac{3}{4})} R_{N/2}. \tag{8}$$

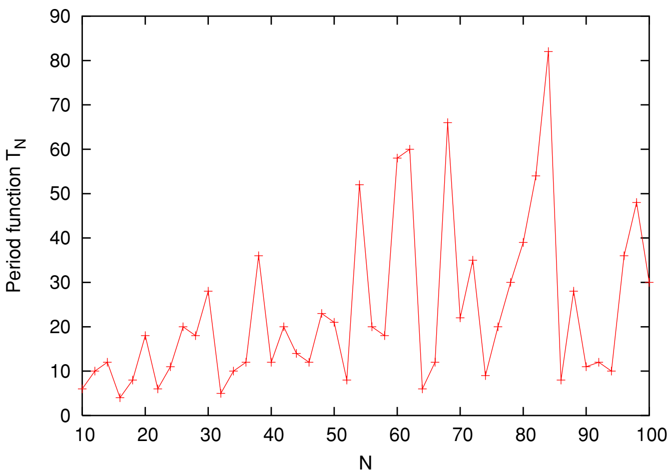

Figure 2. The quantum period function T_N which is the multiplicative order of 2 modulo $N-1$.

However it does not obey the time-reversal symmetry obeyed by the usual quantum baker's map. This follows from the preferential treatment of the position basis, in which S is a permutation, whereas in the momentum basis it is not. In the following we use S as an intermediate operator towards simplifying states of the usual baker's map B of equation (1). While doing so we will also compare the case of the operator B_S wherein there is a more explicit relationship; however a more detailed study of the spectra of B_S and related operators is itself postponed.

The operator S is easily diagonalized. The case $N = 2^K$ is particularly simple, as one sees from the cyclic shifting that $S^K = I_N$, and therefore the possible eigenvalues are ω^l, where $\omega_K = \mathrm{e}^{2\pi\mathrm{i}/K}$ and $0 \leqslant l \leqslant K-1$. The complete set of eigenfunctions can be constructed based on the periodic orbits of the full binary left shift. When K is composite, an arbitrary K-tuple may not produce (on action by S) an invariant subspace of full dimensionality K. Let the number of primitive periodic orbits of period n of the left shift map be denoted as $p(n)$, this is the number of primitive binary n-tuples, where a primitive n-tuple is one that is not a repetition of a shorter string. If K has divisors $d_1, d_2, \ldots, d_M$ (including 1 and K), the dimensionalities of the invariant subspaces are d_i, and there are $p(d_i)$ of them. In these subspaces the eigenfunctions maybe written as

$$|\phi_l\rangle = \frac{1}{\sqrt{d_i}} \sum_{m=0}^{d_i-1} \omega_{d_i}^{lm} S^m \left|\overline{a_{d_i-1} a_{d_i-2} \ldots a_0}\right\rangle. \tag{9}$$

The corresponding eigenvalues $\omega_{d_i}^{-l}$ are $p(d_i)$-fold degenerate. The number of primitive orbits is $p(n) = \sum_{k|n} \mu(n/k) 2^k/n$, where $\mu(n)$ is the Möbius function and the sum is over all the divisors of n. A particularly simple case is when K is prime, as $d_1 = 1$ and $d_2 = K$ are the only possible dimensions and the states in the latter subspace have a degeneracy of $(2^K - 2)/K = (N-2)/K$. Even when K is not prime, the degeneracy increases in the same manner for large N. When N is not a power of 2, the matrix S has nontrivial spectral properties. Since $S^t|n\rangle = |2^t n \bmod (N-1)\rangle$, there exists a time T_N such that $S_N^T = I_N$. This must be the least integer such that $2^T \equiv 1 \bmod (N-1)$, the 'quantum period function' T_N is then simply the multiplicative order defined above, $T_N = \mathrm{ord}_{N-1}(2)$. This is not a simple function and its solution is equivalent to the difficult discrete logarithm problem and thence to the task of factoring numbers. It oscillates wildly with N, as seen in figure 2, going all the way from

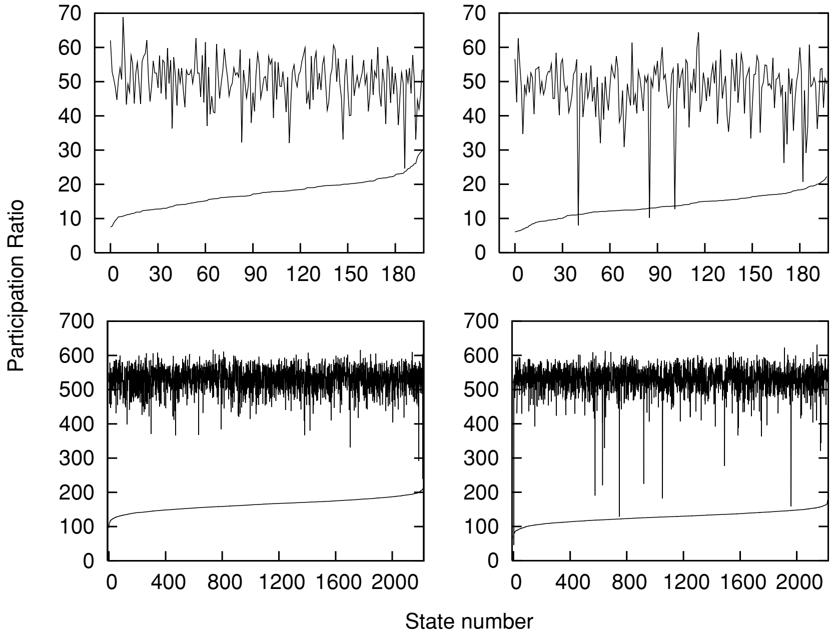

Figure 3. The participation ratio in the position and S-basis of the quantum baker's maps B (left) and B_S (right) when $N = 198$ (top) and $N = 2222$ (bottom). These cases are such that $T_N = N - 2$. In all the figures the lower curve corresponds to the S-basis, and the upper one to the position basis. The states are arranged in increasing order of the participation ratio in the S-basis.

$\ln(N)/\ln(2)$ when N is a power of 2 to $\phi(N-1) \sim (N-1)\,\mathrm{e}^{-\gamma}/\ln(\ln(N-1))$, where γ is the Euler constant.

The eigenvalues are then T_Nth roots of unity and one set of eigenfunctions are given by

$$|\phi_r\rangle = \frac{1}{\sqrt{T_N}} \sum_{n=0}^{T_N-1} \exp\left(\frac{-2\pi \mathrm{i} r n}{T_N}\right) |2^n \bmod (N-1)\rangle, \tag{10}$$

where $0 \leqslant r \leqslant T_N - 1$. For certain N the period T_N is maximal, that is $T_N = \phi(N-1) = N-2$. Naturally a necessary condition for this is that $N-1$ be prime. In this case apart from the eigenstates with unit eigenvalues, $|0\rangle$ and $|N-1\rangle$, the others are exhaustively given by the above set. If $T_N \neq N-2$, other eigenfunctions can be found based on other subgroups. In general there is degeneracy and the states reside in some appropriate subspace.

If we use the eigenstates of S as a basis for the eigenstates of the quantum baker's map, B, or B_S we find remarkable simplifications, as indeed these operators are 'close' to each other. The crucial difference is that we can solve for the spectrum of S exactly. There are evident similarities of S to the well-studied quantum cat maps [14], where there is a quantum period function that is wildly oscillatory, exactly solvable eigenstates [15] and so on. Here, however, the mathematics is far simpler, involving as it does a scalar multiplier (namely 2) rather than an integer 2×2 matrix.

Let the eigenvectors of S be $|\phi_r\rangle$, we then evaluate the participation ratio (PR) $1/\left(\sum_r |\langle\phi_r|\psi\rangle|^4\right)$, which gives us (roughly) the number of S eigenstates needed to construct the vector $|\psi\rangle$, here chosen to be one of the eigenstates of B. This is the PR in the S-basis, while the PR in the position basis is similarly defined and indicates the delocalization in position. For complex random states random matrix theory predicts a PR of $N/2$. In figure 3,

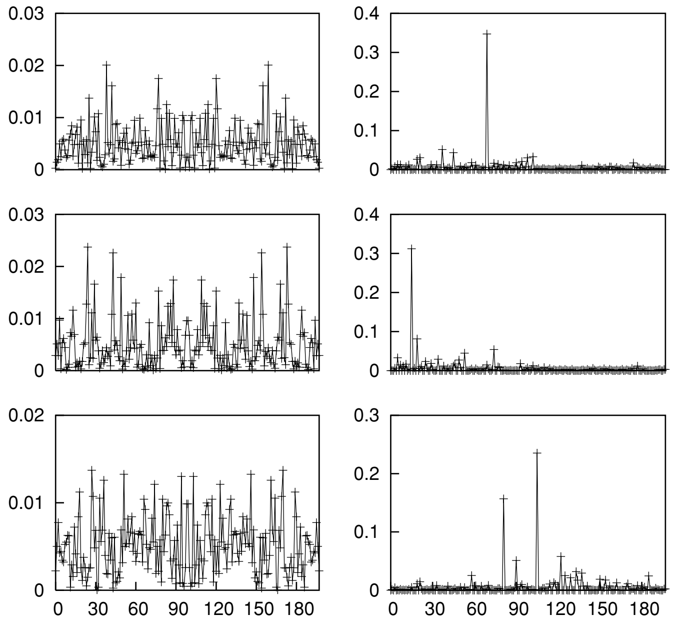

Figure 4. The intensity of three eigenstates of the quantum baker's map ($N = 198$) shown in both the position (left) and in the S-basis (right). The states were chosen for their contrast in the two basis.

we compare the participation ratio of the eigenstates of B and B_S in both the position and the S-basis for a particular case, when the S spectrum is largely non-degenerate. The PR in the position basis is halved to take into account the parity symmetry of the eigenstates, the S-basis already having this symmetry. We note that the S-basis 'simplifies' the states significantly as the PR is smaller by a factor of about five or more.

We see from the figure that the S-basis simplifies states significantly more in the case of the operator B_S rather than the usual quantum baker's map. At the same time, large dips are seen for the eigenstates of B_S that are not visible for B, indicating perhaps that deviations from RMT (random matrix theory) are larger in the case of the spectra of B_S. To illustrate the simplification, we show in figure 4 three eigenstates of the usual quantum baker's map B, for the case $N = 198$ that are considerably simplified in the S-basis.

We may improve upon the S-basis by making it compliant with time-reversal symmetry. For instance, in the first state (say $|\psi\rangle$) shown in figure 4, the maximum overlap with an S-eigenstate $|\phi_r\rangle$ is $|\langle\phi_r|\psi\rangle|^2 = 0.34$, while the (unnormalized) adapted state $|\phi_r'\rangle = |\phi_r\rangle + G_N^{-1}|\phi_r\rangle^*$ has an overlap of 0.37. This adapted state is such that $G_N|\phi_r'\rangle = |\phi_r'\rangle^*$ as required by time-reversal invariance of the quantum baker's map. An arbitrary phase between $|\phi_r\rangle$ and $G_N^{-1}|\phi_r\rangle^*$ was set as zero after numerically ascertaining that this was the optimal value. Note that the conjugation assumes that the states are in the postion representation.

We remark that this simplification falls significantly short of that achieved by the Hadamard basis for the case when N is a power of 2 [7]. In this case (for the operator B) the Thue–Morse states and many others simplified considerably more in the Hadamard basis, or after a Walsh–Hadamard transform; for instance in the case when $N = 1024$, after the transform the participation ratio of the Thue–Morse state was of the order of 2. While the Thue–Morse sequence (rather its finite truncations) is an eigenstate of S, the Hadamard

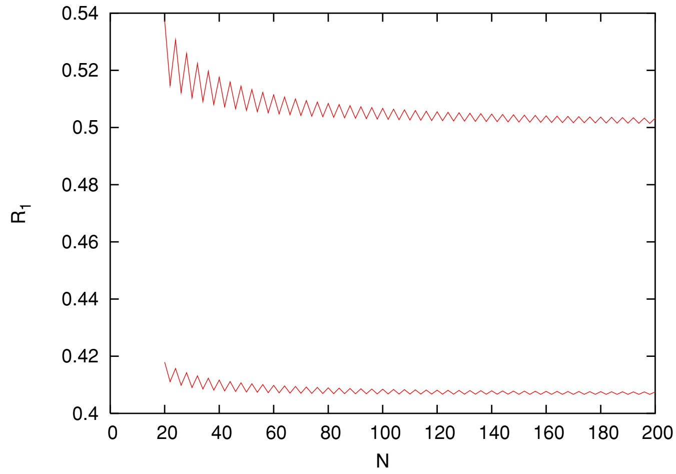

Figure 5. The relative randomness measure R_1 as a function of N, between the operators S and B_S (upper curve), and between S and B (lower curve).

transform itself commutes with S. Due to the degeneracy in the spectrum of S, it appears that the Hadamard transform represents a basis that is more optimal than that provided by the eigenvectors of S. The meaning of this commutation of S and H perhaps in terms of a classical symmetry is not clear to the author.

Finally we remark on the statistical properties of the eigenstates, and on the 'relative randomness', in the sense of Kus and Zyczkowski [16], of S and the operators B and B_S. The usual quantum baker's map eigenstates are nearly generic in the sense that they are close to those that are expected from RMT [17], however there are also known and significant deviations, whose origins may be number-theoretic (such as the multifractal scaling of eigenstates for the case when N are powers of 2 [7]). We find, from results not presented here, that while the eigenstates in the position basis are much closer to the expected Porter–Thomas distribution, the eigenstates in the S-basis deviate considerably, as is to be expected.

To quantitatively compare S and the baker's map operators B and B_S, we study their relative randomness, or degree of noncommutativity, by means of the inner product between the operator S and its image under B (or B_S). Thus define

$$R_1 = |\langle S|BSB^{\dagger}\rangle|/N, \tag{11}$$

where $\langle X|Y\rangle = \mathrm{Tr}(XY^{\dagger})$. It is argued in [16] that this (and related quantities) are small, near zero, if the operators S and B are relatively random, whereas if they commute or anticommute $R_1 = 1$. We show in figure 5 this measure for both the operators B and B_S as a function of N. It is clear that the quantum baker's map B is significantly correlated to the operator S, as the inner product R_1 is around 0.4, and that the operator B_S is more correlated, as the inner product is around 0.5. This is of course reflected in the fact that the eigenstates of B_S are more compressed in the S-basis. It is worthwhile remarking that powers of 2 do not appear to be special for the measure R_1. Also the inner products between S and the baker's map operators themselves behave similarly, as $|\langle S|B\rangle|/N \approx 0.63$ while $|\langle S|B_S\rangle|/N \approx 0.70$.

In conclusion the exactly solvable operator S is a good 'zeroth order' system for the quantum baker's map. This operator is somewhat similar to the semiquantum operators that are obtained on quantizing classical baker's maps after times larger than one [6]. However these operators usually have complicated spectra themselves. We can use S to build a quantum baker's map, which is very close to the usual baker's map, which in turn explains the close relationship between the solvable spectrum of S and that of the quantum baker's map. Using a relative randomness measure it has been shown that indeed the operator S is significantly correlated with the quantum baker's map. While pointing to the evident connection of S to the task of factoring numbers, it is tempting to speculate that the relationship between classically hard computations and their (probably faster) quantum algorithms has a deeper connection to the transition from classical to quantum chaos.

Acknowledgments

I thank the referee for useful suggestions and pointing out [16].

References

[1] Lichtenberg A J and Lieberman M A 1992 *Regular and Chaotic Dynamics* (New York: Springer)
[2] Ornstein D S 1989 *Science* **243** 182
[3] Balazs N L and Voros A 1989 *Ann. Phys., NY* **190** 1
[4] Weinstein Y S, Lloyd S, Emerson J V and Cory D G 2002 *Phys. Rev. Lett.* **89** 157902
[5] Saraceno M 1990 *Ann. Phys., NY* **199** 37
[6] Ozorio de Almeida A M and Saraceno M 1991 *Ann. Phys., NY* **210** 1
Saraceno M and Voros A 1994 *Physica* D **79** 206
[7] Meenakshisundaram N and Lakshminarayan A 2005 *Phys. Rev.* E **71** 065303
[8] Allouche J P and Shallit J 1999 *Sequences and Their Applications, Proc. 1998 SETA Conf.* ed C Ding, T Helleseth and H Niederreiter (Berlin: Springer)
Allouche J P and Shallit J 2003 *Automatic Sequences: Theory, Applications and Generalizations* (Cambridge: Cambridge University Press)
[9] Godreche C and Luck J M 1990 *J. Phys. A: Math. Gen.* **23** 3769
Zaks M A, Pikovsky A S and Kurths J 1999 *J. Phys. A: Math. Gen.* **32** 1523
[10] Schroeder M R 1986 *Number Theory in Science and Communication* (Berlin: Springer)
[11] Penrose O 1970 *Foundations of Statistical Mechanics* (Oxford: Pergamon)
[12] Weisstein E W 'Riffle shuffle' From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/RiffleShuffle.html, and reference therein
[13] Shor P 1994 *Proc. 35th Ann. Symp. on Foundations of Computer Science* (Piscataway, NJ: IEEE)
Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[14] Hannay J H and Berry M V 1980 *Physica* D **1** 267
Keating J P 1991 *Nonlinearity* **4** 309
[15] Eckhardt B 1986 *J. Phys. A: Math. Gen.* **19** 1823
[16] Kus M and Zyczkowski K 1991 *Phys. Rev.* A **44** 956
[17] Haake F 1992 *Quantum Signatures of Chaos* (New York: Springer)