Fast quantum maps

1998 J. Phys. A: Math. Gen. 31 L655

(http://iopscience.iop.org/0305-4470/31/38/001)

J. Phys. A: Math. Gen. **31** (1998) L655–L662. Printed in the UK PII: S0305-4470(98)94324-4

LETTER TO THE EDITOR

Fast quantum maps

G G Athanasiu†‖, E G Floratos‡¶ and S Nicolis§+

† Physics Department, University of Crete and Forth, Heraklion, Crete, Greece
‡ INP, NRCPS 'Demokritos' 15310 Aghia Paraskevi, Athens, Greece
§ CNRS–Laboratoire de Mathématiques et Physique Théorique (UPRES A 6083), Université de Tours, Parc Grandmont, 37200 Tours, France

Received 18 May 1998

Abstract. We develop number theoretic tools that allow us to perform computations relevant for the quantum mechanics over finite fields of arbitrary, odd size, with the same speed-up that is enjoyed by the fast Fourier transform.

Recent developments in non-perturbative string theory, the discovery of D branes [1] and their dynamics, have revealed a new sector of heavy solitonic objects through which distances below string scales can be probed in the weak-coupling regime (non-relativistic limit) [2]. It seems that the most fundamental of these solitonic objects, the D0 branes, have low-energy effective Lagrangian the one-dimensional reduction of a 10d supersymmetric Yang–Mills (YM) system, the so-called SUSY YM quantum mechanics. Indeed a stack of N D0 branes has $SU(N)$ SUSY YM quantum mechanics as its low-energy effective Lagrangian [3, 4] and the target space collective coordinates of the D0 branes become N by N Hermitian matrices functions of time (YM gauge potentials) and their SUSY partners. This implies that a non-commutative geometry setting is emerging for the description of the dynamics of D0 branes [5].

All the above has been lifted to the level of a candidate for the M-theory, (the theory which presumably unifies all known string theories), the famous by now M(atrix) theory [6] Curiously enough, the above picture resembles the (now some years old) $SU(N)$ truncation [7] of the excitations of the supermembrane theory in 11 dimensions [8] in analogy with the bosonic membrane $SU(N)$ truncation [9, 10].

Closer to the D0 picture comes the work of [10], where the discretized membrane and its non-commutative geometry, finite quantum mechanics (FQM) was introduced, as a consistent truncation of the bosonic membrane and its dynamical symmetry: that of the area-preserving diffeomorphism group. In this discretized version of the membrane the elementary excitations' degrees of freedom were assumed to be one-particle states living on the membrane, like particles in discrete phase space $\mathbb{Z}_N \times \mathbb{Z}_N$. A physical analogue system of these elementary excitations was proposed to be the quantum Hall effect of one electron on a magnetic lattice of rational magnetic flux per plaquette. The Hilbert space of these

‖ E-mail address: athanasi@physics.uch.gr
¶ E-mail address: manolis@timaios.nrcps.ariadne-t.gr. On leave of absence from Physics Department, University of Crete.
+ E-mail address: nicolis@celfi.phys.univ-tours.fr

0305-4470/98/380655+08$19.50

elementary excitations is finite-dimensional and the quantum mechanics of linear quantum maps was further developed in [11–13]. The $SU(N)$ matrices of the YM quantum mechanics can be thought of as coherent states of such elementary excitations. The difference with the above-mentioned model of elementary excitations of the membrane is that time is also discrete and the motion of these excitations is typically random and chaotic—a fact which at the quantum level is translated into extended, random wavefunctions for typical eigenstates.

Although we are far from a realistic scenario for the role of these elementary excitations for the quantum dynamics of the SUSY $SU(N)$ quantum mechanics we believe that further technical developments are necessary in order to acquire better understanding of the situation.

On a more mathematical side FQM has been developed so far using representation theory of the modular group $SL(2,\mathbb{Z}_N)$, the linear canonical transormation group of the elementary excitations, for values of N, prime or powers of primes. In this letter we treat the case of general odd integers N, using prime decomposition and the Chinese remainder theorem for the modular group and its representations. The case of integers $N = 2^n$ and general integers will be dealt with elsewhere.

An immediate practical consequence of our work is the possibility to extend the fast Fourier transform for any odd N to the metaplectic representation of the modular group $SL(2,\mathbb{Z}_N)$.

We now recall the basic features of FQM.

The torus phase space has been the simplest prototype for studying classical and quantum chaos [14–17]. Discrete elements of $SL(2,\mathbb{R})$, i.e. elements of the modular group $SL(2,\mathbb{Z})$, are studied on discretizations of the torus with rational coordinates of the same denominator l, $(q,\ p) = (n_1/l, n_2/l) \in \Gamma, n_1, n_2, l \in \mathbb{Z}$ and their periodic trajectories mod 1 are examined studying the periods of elements $\mathcal{A} \in SL(2,\mathbb{Z})$ mod l. The action mod 1 becomes mod l on an equivalent torus, $(n_1, n_2) \in l\Gamma$. The classical motion of such discrete dynamical systems is usually 'maximally' disconnected and chaotic [15, 17].

FQM is the quantization of these discrete linear maps and the corresponding one-timestep evolution operators $U(\mathcal{A})$ are $l \times l$ unitary matrices called *quantum maps*. In the literature [16, 17] these maps are determined semi-classically. In [11, 12] the exact quantization of $SL(2,\mathbb{F}_p)$, where $\mathbb{F}_p$ is the simplest finite field of p elements with p a prime number was studied in detail. In [13] these results were extended to powers of primes, p^n—the group is then $SL(2,\mathbb{Z}_{p^n})$.

The Hilbert space $\mathbb{H}_\Gamma$ of the wavefunctions on the torus $\Gamma = \mathbb{C}/\mathbb{L}$ of complex modulus $\tau = \tau_1 + \mathrm{i}\tau_2$, where $\mathbb{L}$ is the integer lattice $\mathbb{L} = \{m_1 + \tau m_2 | (m_1, m_2) \in \mathbb{Z} \times \mathbb{Z}\}$, is defined as the space of functions of complex argument $z = x + \mathrm{i}y$

$$f(z) = \sum_{n\in\mathbb{Z}} c_n \mathrm{e}^{\mathrm{i}\pi n^2\tau + 2\pi \mathrm{i} n z} \tag{1}$$

with norm [11]

$$\|f\|^2 = \int \mathrm{e}^{-2\pi y^2/\tau_2} |f(z)|^2 \,\mathrm{d}x\,\mathrm{d}y \qquad \tau_2 > 0. \tag{2}$$

Consider the subspace $\mathbb{H}_l(\Gamma)$ of $\mathbb{H}_\Gamma$ with periodic Fourier coefficients $\{c_n\}_{n\in\mathbb{Z}}$ of period l

$$c_n = c_{n+l} \qquad n \in \mathbb{Z},\ l \in \mathbb{N}. \tag{3}$$

The space $\mathbb{H}_l(\Gamma)$ is l-dimensional and there is a discrete Heisenberg group [18], with

generators $\mathcal{S}_{1/l}$ and $\mathcal{T}_1$ acting as [19, 20]

$$\begin{aligned}(\mathcal{S}_{1/l}f)(z) &= \sum_{n\in\mathbb{Z}} c_n \mathrm{e}^{2\pi \mathrm{i}n/l}\mathrm{e}^{2\pi \mathrm{i}nz+\pi \mathrm{i}n^2\tau}\\ (\mathcal{T}_1 f)(z) &= \sum_{n\in\mathbb{Z}} c_{n-1}\mathrm{e}^{2\pi \mathrm{i}nz+\pi \mathrm{i}n^2\tau} \qquad c_n\in\mathbb{C}.\end{aligned} \tag{4}$$

On the l-dimensional subspace of vectors $(c_1,\ldots,c_l)$ the two generators are represented by

$$\begin{aligned}(\mathcal{S}_{1/l})_{n_1,n_2} &= Q_{n_1,n_2} = \omega^{(n_1-1)}\delta_{n_1,n_2}\\ (\mathcal{T}_1)_{n_1,n_2} &= P_{n_1,n_2} = \delta_{n_1-1,n_2}\end{aligned} \tag{5}$$

with $\omega = \exp(2\pi \mathrm{i}/l)$. The Weyl relation becomes

$$QP = \omega PQ \tag{6}$$

and the Heisenberg group elements are

$$\mathcal{J}_{r,s} = \omega^{r\cdot s/2}P^rQ^s. \tag{7}$$

The generators $\mathcal{J}_{r,s}$ satisfy the following composition law:

$$\mathcal{J}_{r,s}\mathcal{J}_{r',s'} = \omega^{(r's-s'r)/2}\mathcal{J}_{r+r',s+s'} \tag{8}$$

and the 'commutation' relations

$$\mathcal{J}_{r,s}\mathcal{J}_{r',s'} = \omega^{r's-s'r}\mathcal{J}_{r',s'}\mathcal{J}_{r,s}. \tag{9}$$

The metaplectic representation of $SL(2,\mathbb{Z}_l)$ is defined by the relation

$$U^{-1}(\mathcal{A})\mathcal{J}_{r,s}U(\mathcal{A}) = \mathcal{J}_{(r,s)\mathcal{A}} \tag{10}$$

where $\mathcal{A}$ is an element of $SL(2,\mathbb{Z}_l)$. In the literature the metaplectic representation of $SL(2,\mathbb{Z}_l)$, (the group of 2×2, integer-valued matrices mod l), is known for $l=p^n$ [21]†

The Weyl–Fourier form of $U(\mathcal{A})$ is [13]

$$U(\mathcal{A}) = \frac{\sigma(1)\sigma(\delta)}{p^n}\sum_{r,s=0}^{p^n-1}\mathrm{e}^{\frac{2\pi \mathrm{i}}{p^n}[br^2+(d-a)rs-cs^2]/2\delta}\mathcal{J}_{r,s} \tag{11}$$

where

$$\begin{aligned}\mathcal{A} &= \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL(2,\mathbb{Z}_{p^n}) \qquad \delta = 2-a-d\\ \sigma(x) &= \frac{1}{\sqrt{p^n}}\sum_{r=0}^{p^n-1}\omega^{xr^2}.\end{aligned} \tag{12}$$

All the operations in the exponent are carried out mod p^n. If $\delta\equiv 0 \bmod p^n$ we use the trick

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix} = \begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix} -c & -d\\ a & b\end{pmatrix} \tag{13}$$

and the fact that $U(\mathcal{A})$ is a representation (cf [13] and below).

We shall now work out some technical details of the representation theory of $SL(2,\mathbb{Z}_N)$ that we need for the factorization of the Heisenberg group and of the metaplectic representation.

We start with the Chinese remainder theorem for numbers [23]. Let $N\in\mathbb{Z}$ be a non-prime, that may be written as a product of two co-prime factors, N_1 and N_2, namely

† The representation theory of the symplectic group $SL(2,\mathbb{F}_{p^n})$, over the finite field $\mathbb{F}_{p^n}$, may be found in [22].

$N = N_1 N_2$. We denote by $N\mathbb{Z}$ the set of all multiples of N. Then any $r \in \mathbb{Z}/N\mathbb{Z}$ may be written uniquely as

$$r = r_1 m_1 n_1 + r_2 m_2 n_2$$

where $r_1 \equiv r \bmod N_1$, $r_2 \equiv r \bmod N_2$, $m_1 = N/N_1$, $m_2 = N/N_2$, $n_1 = m_1^{-1} \bmod N_1$, $n_2 = m_2^{-1} \bmod N_2$.

In other words, we may establish a one-to-one correspondance between the number r and the 2-tuple (r_1, r_2). This defines the *Sino representation* of r. This 2-tuple may be promoted to a bona fide element of a set $\mathcal{V}_N^{(2)}$, whose elements have the following properties, for any two numbers $r, r' \in \mathbb{Z}/N\mathbb{Z}$:

$$r \times r' \leftrightarrow (r_1 r_1^{'} \bmod N_1, r_2 r_2^{'} \bmod N_2)$$

and

$$r + r' \leftrightarrow (r_1 + r_1^{'} \bmod N_1, r_2 + r_2 \bmod N_2).$$

We can immediately generalize this result to the case in which $N = N_1 \times N_2 \times \cdots N_k$ where all pairs of factors are co-prime. The decomposition reads

$$r = r_1 m_1 n_1 + r_2 m_2 n_2 + \cdots + r_k m_k n_k$$

where $m_i = N/N_i$, $n_i \equiv m_i^{-1} \bmod N_i$ and one may similarly establish a one-to-one correspondance between r and the k-tuple $(r_1, r_2, \ldots, r_k)$ element of the set $\mathcal{V}_N^{(k)}$. Furthermore note that $\mathcal{V}_N$ has the property

$$\mathcal{V}_N \leftrightarrow \mathcal{V}_{N_1} \otimes \mathcal{V}_{N_2} \otimes \cdots \otimes \mathcal{V}_{N_k}.$$

Using these relations it is now possible to establish that

$$SL(2, \mathbb{Z}_N) = SL(2, \mathbb{Z}_{N_1}) \times SL(2, \mathbb{Z}_{N_2}) \times \cdots \times SL(2, \mathbb{Z}_{N_k}). \tag{14}$$

Indeed, consider the case $k = 2$ and an element of $SL(2, \mathbb{Z}_N)$ of the form

$$\mathcal{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow \begin{pmatrix} (a_1, a_2) & (b_1, b_2) \\ (c_1, c_2) & (d_1, d_2) \end{pmatrix}. \tag{15}$$

It will now be shown that this element is an element of the set $SL(2, \mathbb{Z}_{N_1}) \times SL(2, \mathbb{Z}_{N_2})$ Consider a generic element of $SL(2, \mathbb{Z}_{N_1})$. It may be written as

$$\mathcal{A}_1 = \begin{pmatrix} (a_1, 1) & (b_1, 0) \\ (c_1, 0) & (d_1, 1) \end{pmatrix}. \tag{16}$$

Take now a generic element of $SL(2, \mathbb{Z}_{N_2})$, that may be written

$$\mathcal{A}_2 = \begin{pmatrix} (1, a_2) & (0, b_2) \\ (0, c_2) & (1, d_2) \end{pmatrix}. \tag{17}$$

It is straightforward to check that $\mathcal{A}_1 \cdot \mathcal{A}_2 = \mathcal{A}$. Using the Chinese remainder theorem for numbers we know that the decomposition is unique.

Let us close with the remark that the matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \tag{18}$$

with $a^2 + b^2 \equiv 1 \bmod N$ generate the group $O_2(N) \lhd SL(2, \mathbb{Z}_N)$. Once more it is possible to show that

$$O_2(N) = O_2(N_1) \times O_2(N_2) \tag{19}$$

namely

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} (a_1, 1) & (b_1, 0) \\ (-b_1, 0) & (a_1, 1) \end{pmatrix} \begin{pmatrix} (1, a_2) & (0, b_2) \\ (0, -b_2) & (1, a_2) \end{pmatrix}. \tag{20}$$

In the following we discuss the implications of the factorization of $SL(2, \mathbb{Z}_N)$ (cf previous discussion) for the metaplectic representation. We begin with the factorization of the Heisenberg group $\mathfrak{h}(N = N_1 N_2)$ (cf the work of Schwinger in [18]).

Indeed, using the Chinese remainder theorem and the commutation relations of the $\mathcal{J}_{r,s}$, we find

$$\begin{aligned} \mathcal{J}_{r,s} &= \mathcal{J}_{r_1 m_1 n_1 + r_2 m_2 n_2, s_1 m_1 n_1 + s_2 m_2 n_2} \\ &= \mathcal{J}_{r_1 m_1 n_1, s_1 m_1 n_1} \mathcal{J}_{r_2 m_2 n_2, s_2 m_2 n_2} \\ &= \mathcal{J}_{r_2 m_2 n_2, s_2 m_2 n_2} \mathcal{J}_{r_1 m_1 n_1, s_1 m_1 n_1} \end{aligned}$$

since the extra phase factor equals unity.

We shall now use the factorization properties of the Heisenberg group generators, $\mathcal{J}_{r,s}$ to obtain the decomposition of the unitary operator $U(\mathcal{A})$, $\mathcal{A} \in SL(2, \mathbb{Z}_N)$, that governs the time evolution of the quantum system in the case in hand. To do this we recall that the evolution of the generators $\mathcal{J}_{r,s}$ is given by

$$U^{-1}(\mathcal{A}) \mathcal{J}_{r,s} U(\mathcal{A}) = \mathcal{J}_{(r,s)\mathcal{A}}. \tag{21}$$

If $N = N_1 N_2$, then $\mathcal{A} = \mathcal{A}_1 \cdot \mathcal{A}_2$, with $\mathcal{A}_1 \in SL(2, \mathbb{Z}_{N_1})$ and $\mathcal{A}_2 \in SL(2, \mathbb{Z}_{N_2})$. We shall show that $U(\mathcal{A}) = U(\mathcal{A}_1) \cdot U(\mathcal{A}_2)$.

Proof. $U(\mathcal{A})$ may be written as a linear combination of the generators $\mathcal{J}_{r,s}$ as

$$U(\mathcal{A}) = \frac{\sigma(1)\sigma(\delta)}{N} \sum_{r,s=0}^{N-1} \omega^{(br^2 + (d-a)rs - cs^2)/(2\delta)} \mathcal{J}_{r,s} \tag{22}$$

where

$$\mathcal{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Using the Sino representation, $xr^2 = (x_1, x_2)(r_1^2, r_2^2) = (x_1 r_1^2, x_2 r_2^2) = x_1 r_1^2 n_1 m_1 + x_2 r_2^2 n_2 m_2$ and the double sum is seen to split into the product of two sums

$$\begin{aligned} \frac{1}{N} \sum_{r=0}^{N-1} \omega^{xr^2} &= \frac{1}{N_1 N_2} \sum_{r_1, r_2 = 0}^{N_1 - 1, N_2 - 1} \mathrm{e}^{2\pi \mathrm{i}(x_1 r_1^2 n_1 m_1 + x_2 r_2^2 n_2 m_2)/(N_1 N_2)} \\ &= \left(\frac{1}{N_1} \sum_{r_1=0}^{N_1 - 1} \mathrm{e}^{2\pi \mathrm{i} m_1 x_1 r_1^2 / N_1} \right) \left(\frac{1}{N_2} \sum_{r_1=0}^{N_2 - 1} \mathrm{e}^{2\pi \mathrm{i} m_2 x_2 r_2^2 / N_2} \right) \end{aligned} \tag{23}$$

which leads to the relation

$$\sigma(x) = \sigma(m_1 x_1) \sigma(m_2 x_2). \tag{24}$$

This takes care of the prefactor. The phase is re-arranged as follows:

$$\begin{aligned} \phi \equiv (br^2 + (d-a)rs - cs^2)/(2\delta) &= ((b_1 r_1^2 + (d_1 - a_1) r_1 s_1 - c_1 s_1)/(2\delta_1)) m_1 n_1 \\ &+ ((b_2 r_2^2 + (d_2 - a_2) r_2 s_2 - c_2 s_2)/(2\delta_2)) m_2 n_2 = \phi_1 N_2 m_1 + \phi_2 N_1 m_2. \end{aligned}$$

The upshot of this is that $U(\mathcal{A})$ may be rewritten as

$$\begin{aligned} U(\mathcal{A}) &= \frac{\sigma(m_1\delta_1)\sigma(m_2\delta_2)}{N_1N_2}\sum_{r_1,r_2=0}^{N_1-1,N_2-1}\omega_{N_1}^{m_1\phi_1}\omega_{N_2}^{m_2\phi_2}\mathcal{J}_{r_1m_1n_1,s_1,m_1,n_1}\mathcal{J}_{r_2m_2n_2,s_2m_2n_2} \\ &= \frac{\sigma(m_1\delta_1)}{N_1}\sum_{r_1=0}^{N_1-1}\omega_{N_1}^{m_1\phi_1}\mathcal{J}_{r_1m_1n_1,s_1m_1n_1}\frac{\sigma(m_2\delta_2)}{N_2}\sum_{r_2=0}^{N_2-1}\omega_{N_2}^{m_2\phi_2}\mathcal{J}_{r_2m_2n_2,s_2m_2n_2} \\ &= U(\mathcal{A}_1)\cdot U(\mathcal{A}_2). \end{aligned}$$

As a consequence $U(\mathcal{A}_1)$ and $U(\mathcal{A}_2)$ commute. Now we establish an isomorphism between $U(\mathcal{A}_1)$ and $U(\mathcal{A}_2)$ with $U_1(\mathcal{A}_1)$ and $U_2(\mathcal{A}_2)$, where U_1 and U_2 are the metaplectic representations of dimension N_1 and N_2 respectively. Indeed we shall exhibit a permutation matrix R with the properties

$$\begin{aligned} &RPR^{\mathrm{T}} = P_1\otimes P_2 \\ &RQR^{\mathrm{T}} = Q_1\otimes Q_2 \\ &R\mathcal{J}_{r,s}R^{\mathrm{T}} = \mathcal{J}_{r_1,s_1}\otimes\mathcal{J}_{r_2,s_2} \\ &RU(\mathcal{A})R^{\mathrm{T}} = U_1(g_1)\otimes U_2(g_2) \end{aligned}$$

where P and Q (P_i, Q_i,$i=1,2$) are the generators of the Heisenberg group $\mathfrak{h}(N)$ (resp. $\mathfrak{h}(N_i)$).

It is enough to prove that the matrix R has the property

$$R\boldsymbol{e}_k = \boldsymbol{e}_{k_1}\otimes\boldsymbol{e}_{k_2} \tag{25}$$

where $\boldsymbol{e}_k$ ($\boldsymbol{e}_{k_i}$,$i=1,2$) are the eigenvectors of P (resp. P_i, $i=1,2$) and the indices run as $k=1,\ldots,N$, $k_i=1,\ldots,N_i$, $i=1,2$. The other properties indeed are consequences of this.

We start with an explicit form for the eigenvectors of P

$$\boldsymbol{e}_{k,l} = \frac{\omega^{k(l-1)}}{\sqrt{N}} \qquad k,l=1,\ldots,N. \tag{26}$$

Using the Sino representation we find

$$\frac{\omega_N^{k_1(j_1-1)m_1n_1+k_2(j_2-1)m_2n_2}}{\sqrt{N_1N_2}} = \frac{\omega_{N_1}^{k_1(j_1-1)m_1}}{\sqrt{N_1}}\frac{\omega_{N_2}^{k_2(j_2-1)m_2}}{\sqrt{N_2}}. \tag{27}$$

In order to construct the matrix R, we compare the r.h.s. of equations (25), (27). The indices j_1 and j_2, in equation (27), from the Sino decomposition of j, run from 1 to N_1 (resp. N_2) and the corresponding values of j fill up an $N_1\times N_2$ array. On the other hand, the r.h.s. of equation (25) defines, through the tensor product, a decomposition of j into indices j_1 and j_2 and defines another $N_1\times N_2$ array, that is related to the previous one by a permutation matrix, namely R. Specifically, if we denote the Sino decomposition array by

$$\{j_1,\, j_2\} \tag{28}$$

the matrix R, with rows indexed by i and columns indexed by j, has elements equal to 1 when $\{j_1,\, j_2\}=i$ and zero otherwise. This construction is straightforwardly generalized to more than two co-prime factors of N (cf the book by Schroeder in [23]). The stationary eigenvalue problem for the unitary evolution operator U is reduced to that corresponding to each individual factor of the tensor decomposition of the matrix U (e.g. in the case where

N_1 and N_2 are powers of primes of the type $4k+1$ explicit expressions are known for the eigenvectors and eigenvalues [12, 13]).

The matrix R is used in (classical) fast Fourier algorithms to reduce the number of operations from $O(N^2)$ to $O(N \log N)$ [23]).

By construction, therefore, the property in equation (25) holds and this implies the decomposition of the P operator. The decomposition of the Q operator follows immediately, since it is diagonal in this basis and the operations may be carried out element by element. From these both the decomposition of the $\mathcal{J}_{r,s}$ and $U(\mathcal{A})$ follow since (as may be checked) $RR^{\mathrm{T}} = I$. □

We close with the following remarks. The case $N = 2^n$ cannot be studied by the methods developed here and new ideas are required. This case is, of course, particularly interesting for computational reasons. Indeed, all existing fast Fourier algorithms are given for $N = 2^n$. For powers of primes a similar speed-up of operations may also be obtained (cf Schroeder in [23]). On the other hand, what we have achieved here is the construction of fast algorithms for *any odd* N and for *any quantum map* that is a metaplectic representation of $SL(2, \mathbb{Z}_N)$.

It would be interesting to implement such maps by quantum gates, as already proposed for the quantum Fourier transform [24].

References

[1] Polchinski J 1995 *Phys. Rev. Lett.* **75** 4724
[2] Douglas M R, Kabat D, Pouliot P and Shenker S 1997 *Nucl. Phys.* B **485** 85
[3] Witten E 1995 *Nucl. Phys.* B **443** 85
[4] Witten E 1996 *Nucl. Phys.* B **460** 355
Polchinski J, Chaudhuri S and Johnson C V 1996 Notes on D-branes *Preprint* hep-th/9602052
Bachas C 1997 (Half) A lecture on D-branes *Preprint* hep-th/9701019
[5] Connes A, Douglas M R and Schwartz A 1998 *JHEP* **2** 3
[6] Banks T, Fischler W, Shenker S and Susskind L 1997 *Phys. Rev.* D **55** 5112
[7] de Wit B, Hoppe J and Nicolai H 1998 *Nucl. Phys.* B **305** 545
[8] Townsend P K 1995 *Phys. Lett.* B **350**
[9] Goldstone J unpublished
Hoppe J 1982 Quantum theory of a relativistic surface *PhD Thesis* in 1986 *Constraint Theory and Relativistic Dynamics (Camridge, MA: MIT)* ed G Longhi *et al* (Florence: World Scientific)
[10] Floratos E G 1989 *Phys. Lett.* B **228** 335
Fairlie D B and Zachos C K 1989 *Phys. Lett.* B **224** 101
Floratos E G and Iliopoulos J 1988 *Phys. Lett.* **201** 237
[11] Balian R and Itzykson C 1986 *C. R. Acad. Sci., Paris* **303** 773
[12] Athanasiu G G and Floratos E G 1994 *Nucl. Phys.* B **425** 343
[13] Athanasiu G G, Floratos E G and Nicolis S 1996 *J. Phys. A: Math. Gen.* **29** 6737
[14] Arnold V I 1978 *Mathematical Methods of Classical Mechanics* (*Springer Graduate Texts in Mathematics 60*) (New York: Springer)
Arnold V I and Avez A 1968 *Ergodic Problems of Classical Mechanics* (New York: Benjamin)
[15] Vivaldi F 1992 *Nonlinearity* **5** 133
[16] Hannay J and Berry M V 1980 *Physica* **1D** 267
Berry M V 1987 *Proc. R. Soc.* A **473** 183
Keating J P 1994 *J. Phys. A: Math. Gen.* **27** 6605
[17] Balazs N L and Voros A 1986 *Phys. Rep.* C **143** 109
Chirikov B V, Izrailev F M and Shepelyansky D 1988 *Physica* **33D** 77
Ford J, Mantica G and Ristow G H 1991 *Physica* **50D** 493
Leboeuf P and Voros A 1993 *Quantum Chaos* ed G Casati and B V Chirikov (Cambridge: Cambridge University Press)
[18] Weyl H 1931 *The Theory of Groups and Quantum Mechanics* (New York: Dover)

Schwinger J 1960 *Proc. Natl Acad. Sci.* **46** 257
Schwinger J 1960 *Proc. Natl Acad. Sci.* **46** 544
Schwinger J 1960 *Proc. Natl Acad. Sci.* **46** 883
Santhanam T S and Tekumalla A R 1976 *Found. Phys.* **6** 583
Stovicek P and Tolar J 1984 *Rep. Math. Phys.* **20** 157
[19] Cartier P 1966 Quantum mechanical commutation relations and theta functions *Proc. Symp. Pure Mathematics 9 Algebraic–Discontinuous Groups* (Providence, RI: American Mathematical Society)
[20] Mumford D 1986 *Tata Lectures on Theta I–III* (New York: Birkhäuser)
[21] Tanaka S 1966 *Osaka J. Math.* **3** 229
[22] Tanaka S 1967 *Osaka J. Math.* **4** 65
[23] Schroeder M R S 1997 *Number Theory in Science and Communication (Springer Series in Information Sciences)* 3rd edn (New York: Springer)
Tolimieri R, An M and Lu C 1997 *Mathematics of Multidimensional Fourier Transform Algorithms* 2nd edn (New York: Springer)
[24] Shor P W 1994 Algorithms for quantum computation: Discrete logarithms and factoring *Proc. IEEE Computer Society* (New York: IEEE Computer Society) p 124
See also Polynomial–time algorithms for prime factorization and discrete logarithms on a quantum computer *Preprint* quant-ph/9508027
Beckman D, Chari A N, Devabhaktuni S and Preskill J 1996 Efficient networks for quantum factoring *Preprint* quant-ph/9602016