IOPscience iopscience.iop.org

Home Search Collections Journals About Contact us My IOPscience

Factorizations and physical representations

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2006 J. Phys. A: Math. Gen. 39 5151

(http://iopscience.iop.org/0305-4470/39/18/027)

View the table of contents for this issue, or go to the journal homepage for more

Download details:
IP Address: 171.66.16.104
The article was downloaded on 03/06/2010 at 04:27

Please note that terms and conditions apply.

Institute of Physics Publishing

Journal of Physics A: Mathematical and General

J. Phys. A: Math. Gen. **39** (2006) 5151–5162

doi:10.1088/0305-4470/39/18/027

Factorizations and physical representations

M Revzen[1,2], F C Khanna[2], A Mann[1,2] and J Zak[1]

[1] Department of Physics, Technion—Israel Institute of Technology, Haifa 32000, Israel
[2] Theoretical Physics Institute, Department of Physics, University of Alberta, Edmonton, Alberta T6G 2J1, Canada

E-mail: revzen@physics.technion.ac.il, khanna@phys.ualberta.ca, ady@physics.technion.ac.il and zak@physics.technion.ac.il

Received 20 December 2005, in final form 7 March 2006
Published 19 April 2006
Online at stacks.iop.org/JPhysA/39/5151

Abstract

A Hilbert space in M dimensions is shown explicitly to accommodate representations that reflect the decomposition of M into prime numbers. Representations that exhibit the factorization of M into two relatively prime numbers: the kq representation (Zak J 1970 *Phys. Today* **23** 51), and related representations termed q_1q_2 representations (together with their conjugates) are analysed, as well as a representation that exhibits the complete factorization of M. In this latter representation each quantum number varies in a subspace that is associated with one of the prime numbers that make up M.

PACS numbers: 73.20.Dx, 02.20.Df, 03.65.−w

1. Introduction

Quantum mechanics in a finite-dimensional Hilbert space, which is the main topic of this paper, was originally studied by Weyl [1], whose work allowed him to establish the relationship between the Heisenberg commutation relation and the Schrödinger wave equation. However, it was Schwinger [2] who initiated a systematic study of finite-dimensional quantum mechanics. The recent developments in our understanding of the foundations of quantum mechanics that led, among other things, to the possibility of quantum computers, is responsible for the intensive recent interest in the problem of quantum mechanics in finite-dimensional systems. Thus, e.g., a protocol was developed in a finite-dimensional space that can implement the Fourier transformation in a quantum computer [3]. Other applications are to the problem of definition of conjugate operators and phase operators, e.g. (a very incomplete list) [4–8]. There are many other beautiful applications of finite-dimensional Hilbert spaces. For recent reviews, see, e.g. [9].

Information and computation may be understood in terms of classical physics [10]. However, the extension of these ideas to the quantum domain [11] enriches our understanding of both information theory and quantum mechanics. Thus quantum computers, where entanglement and superposition of states are essential elements, allow computations believed to be intractable on any classical computer. The most often quoted example is Shor's [12] quantum algorithm for factorizing numbers, while there is no known efficient classical algorithm for factoring. In this paper we study the relation of factorizability to quantum physics. Thus we wish to find and characterize physical representations which reflect the prime factorization of M, the dimensionality of the space of the problem. Our study is based on Schwinger's [2] general theory of quantum mechanics in finite-dimensional space in terms of unitary operators.

Schwinger [2] showed that M-dimensional vector spaces allow the construction of two unitary operators, U and V (in his notation), that form a complete operator basis, i.e. they suffice to construct all possible operators of the physical system. This means that if an operator commutes with both U and V it is necessarily a multiple of the unit operator. These operators have a period M, i.e.

$$U^M = V^M = 1, \tag{1}$$

where M is the smallest integer for which this equality holds. The eigenvalues of both U and V are distinct: they are the M roots of unity, i.e. with $|x\rangle$ the eigenfunctions of U,

$$U|x\rangle = \mathrm{e}^{\mathrm{i}(\frac{2\pi}{M})x}|x\rangle, \qquad |x + M\rangle = |x\rangle, \qquad x = 1, \ldots, M.$$

The operator V is defined over these eigenvectors as

$$V|x\rangle = |x - 1\rangle. \tag{2}$$

Schwinger then showed that the absolute value of the overlap between *any* eigenfunction of U, $|x\rangle$ and any one of V, $|p\rangle$, is a constant:

$$|\langle p|x\rangle| = \frac{1}{\sqrt{M}}. \tag{3}$$

Sets of operators whose eigenvectors satisfy equation (3) are called conjugate; the vector bases defined by them are referred [13, 14] to as conjugate vector bases (or mutually unbiased bases). It was further noted by Schwinger [2] that alternative conjugate vector bases may be constructed. For example, we may let $U \to U' = U^n$ for $n < M$ such that it has no common factor with M. U' has, clearly, the same period and eigenvalues as U. The corresponding V' that satisfies the relevant equation, equation (2), was shown to be some power of V.

Our aim in this paper is to expand Schwinger's analysis and stress its relation to factorization of M, the dimensionality of the space. A different approach to this factorization and an interesting application to defining a correlation measure for M-dimensional entangled density matrices may be found in [15]. We choose to consider a specific example of the M-dimensional space, namely M points on a line, i.e., we consider discretized and truncated spatial coordinate x and its conjugate momentum p as our M-dimensional space. This may be realized by imposing boundary conditions on the spatial coordinate, x, of the wavefunctions under study, $\psi(\mathrm{x})$, and on their Fourier transforms, $F(p)$ (we take $\hbar = 1$) [16]:

$$\psi(x + Mc) = \psi(x), \qquad F\left(p + \frac{2\pi}{c}\right) = F(p).$$

Here M is an integer—it is the dimensionality of the Hilbert space, and we term c the 'quantization length'. As a consequence of the above boundary conditions we have that the values of the spatial coordinate, x, and the values of the momentum, p, are discrete and finite:

$$x = sc, \qquad s = 1, \ldots, M, \qquad p = \frac{2\pi}{Mc}t, \qquad t = 1, \ldots, M.$$

In this case we may replace the operators x and p by the unitary operators

$$\tau(M) = \mathrm{e}^{\mathrm{i}(\frac{2\pi}{Mc})x}, \qquad T(c) = \mathrm{e}^{\mathrm{i}pc}. \tag{4}$$

These operators satisfy the basic commutator relation

$$\tau(M)T(c) = T(c)\tau(M)\,\mathrm{e}^{-\mathrm{i}\frac{2\pi}{M}}. \tag{5}$$

They exhibit the dimensionality (i.e. periodicity) automatically (cf equation (1)):

$$[\tau(M)]^M = [T(c)]^M = 1, \tag{6}$$

and we may associate Schwinger's operator U with $\tau(M)$ and his V with $T(c)$ (henceforth $c = 1$).

For our analysis it is convenient to represent the number M in terms of prime numbers, P_j,

$$M = \prod_{j=1}^{N} P_j^{n_j}, \qquad P_j \neq P_i, \quad j \neq i, \tag{7}$$

where the n_j are integers, and more concisely we denote $P_j^{n_j}$ by m_j, i.e.

$$M = \prod_{j=1}^{N} m_j. \tag{8}$$

We find thus that the greatest common divisor (gcd) among the $m_j s$ is 1:

$$\gcd(m_j, m_i) = 1, \quad \forall j \neq i, \tag{9}$$

i.e. distinct $m_i s$ are relatively prime. Our aim is to construct representations that reflect explicitly this factorization of M. In our study of the kq representation [17–19] the above was used to show that the number of kq representations, $\chi(M)$, having conjugate representations that can be accommodated in the M-dimensional space, is simply related to the number of distinct primes, N, that appear in M (cf equation (8)):

$$\chi(M) = 2^{N-1}. \tag{10}$$

It should be noted that the familiar finite-dimensional Fourier representation is included in this counting. This is reviewed in section 2. In section 3 we consider a novel representation, closely related to the kq representation that we call q_1q_2 representation [19]. Here the relation between the number of representations follows much the same reasoning as for the kq representation. In section 4 we develop a representation that exhibits explicitly the number of prime numbers that comprise M (cf equation (8)). It is in this section that the central point of this paper is presented, i.e. we exhibit the inter-relation between the dimensionality of the space under investigation and representations that reflect its prime number constituents. For the analysis in this section we note that what was required above was less restrictive than having all the involved numbers relatively prime, i.e. that among every pair of them equation (9) holds. What is required is that the numbers are relatively prime numbers [mod M]. This is defined as follows [18–20]: two numbers M_1, M_2 such that their product $M_1M_2 = M$ are said to be relatively prime [mod M] if the equation,

$$tM_1 + sM_2 = 0 \text{ [mod } M] \tag{11}$$

has, for the integers $[s, t]$, only the trivial solution, viz $s = M_1, t = M_2$. (Note: from their definition $s = 1, \ldots, M_1$ and $t = 1, \ldots, M_2$.) This does *not* preclude a nontrivial common divisor for M_1 and M_2. This more relaxed requirement allows representations, presented in this section, wherein every prime number that makes up the dimensionality, M, can be associated with a subspace which may be labelled by an appropriate quantum number. In section 5 we note the relation between the number of conjugate kq representations (which is the same as the number of possible q_1q_2 (or k_1k_2) representations) and the number of solutions to the equation $x^2 = 1$ [mod M], which is used in number theory to factorize a given integer M into two relatively prime factors. The last section, section 6, is devoted to some conclusions and discussion.

2. The kq representation and factorization

Schwinger [2] noted that U and V, with their powers and products, generate M^2 operators which allow expressing all operators in terms of them. We shall study space dimensionalities, Ms, which are not prime numbers, i.e. $N > 1$ in equation (8). We now briefly review our previous results [18, 19] to introduce a somewhat different notation that is convenient for our later generalization: consider bi-partitioning the product that represents M (equation (8)) into two factors,

$$M = M_1M_2. \tag{12}$$

Here M_1 incorporates one part of the N factors of equation (8) and M_2 contains the other part. Our way of bi-partitioning implies that the two numbers, M_1 and M_2, are relatively prime, viz. $\gcd(M_1, M_2) = 1$. We now introduce

$$L_1 = \frac{M}{M_1}, \qquad L_2 = \frac{M}{M_2}.$$

In the case at hand we simply have $L_1 = M_2$, $L_2 = M_1$; however, in section 4 this definition will prove very useful. L_1 and L_2 are also relatively prime mod M, cf equation (11), i.e. the equation

$$sL_1 + tL_2 = 0 \text{ [mod } M] \tag{13}$$

has only the trivial solution for the integers $[s, t]$, namely $s = M_1$, $t = M_2$. This implies that the equation (we take $c = 1$),

$$x = sL_1 + tL_2 \text{ [mod } M], \qquad x = 1, \ldots, M, \qquad s = 1, \ldots, M_1, \qquad t = 1, \ldots, M_2, \tag{14}$$

has a unique solution x for every pair $[s, t]$, with x running over its whole range of M values. We note that, in general, the pair $[s, t]$ that corresponds to $x = 1$ is *not* $[s = 1, t = 1]$. We will now show how to modify equation (14) to attain this simpler relation among the solutions. Let us consider the replacements $s \to s'N_1$ [mod M_1], $t \to t'N_2$ [mod M_2] with N_1 relative prime to L_2 and N_2 relative prime to L_1. Such replacements retain a unique correspondence $s \leftrightarrow s'$ [mod M_1] and $t \leftrightarrow t'$ [mod M_2].[3] In these new variables equation (14) is

$$\begin{aligned} &x = s'N_1L_1 + t'N_2L_2 \text{ [mod } M], \qquad && x = 1, \ldots, M, \\ &s' = 1, \ldots, M_1, && t' = 1, \ldots, M_2. \end{aligned} \tag{15}$$

We may now choose the N_i to assure that the solution $x = 1$ corresponds to the pair $[s' = 1, t' = 1]$ by solving

$$1 = N_1L_1 + N_2L_2 \text{ [mod } M],$$

i.e. [20]

$$N_2 = L_2^{-1} \text{ [mod } M_2] \qquad \text{and} \qquad N_1 = L_1^{-1} \text{ [mod } M_1]. \tag{16}$$

[3] An illustrative example is: $L_1 = 5, L_2 = 3; N_1 = 2, N_2 = 2$ which leads to the correspondences $s = 1, 2, 3 \leftrightarrow s' = 2, 1, 3$; $t = 1, 2, 3, 4, 5 \leftrightarrow t' = 3, 1, 4, 2, 5$.

Now equation (14) can be rewritten with the solution $x = 1$ corresponding to $s = t = 1$ as

$$x = sN_1L_1 + tN_2L_2\,[\text{mod } M]. \tag{17}$$

An alternative presentation of the above which will be useful in later sections is as follows: recalling that L_1 and L_2 are relatively prime [mod M] equation (14) may be regarded as the solution of a set of two congruences,

$$x = s\,[\text{mod } M_1] \qquad x = t\,[\text{mod } M_2]. \tag{18}$$

The solution of these is [20]

$$x = sN_1L_1 + tN_2L_2\,[\text{mod } M]. \tag{19}$$

To define a kq representation, we use the two commuting operators [17, 18]

$$\tau(M_2) = \mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_2})x}, \qquad T(N_1L_1) = \mathrm{e}^{\mathrm{i}pN_1L_1}. \tag{20}$$

Since $N_1L_1 = 1\,[\text{mod } M_1]$, the equation $[\mathrm{e}^{\mathrm{i}pN_1L_1}]^{M_1} = 1$ is a minimal equation (i.e., M_1 is the smallest number for which it is satisfied). Therefore the eigenvalues of $T(N_1L_1)$ are $\mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}k}, k = 1, \ldots, M_1$. (In [18] we used $\mathrm{e}^{\mathrm{i}pM_2}$ instead of the present $T(N_1L_1)$; these two operators have the same eigenvalues and eigenstates, but enumerated differently. The advantage of $T(N_1L_1)$ is that it shifts the eigenvalues of $\tau(M_1)$ (see equation (22)) by unity whereas $\mathrm{e}^{\mathrm{i}pM_2}$ shifts them by M_2.) The common eigenvectors of these operators are given by

$$\tau(M_2)|k_1, q_2\rangle = \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_2}q_2}|k_1, q_2\rangle \qquad T(N_1L_1)|k_1, q_2\rangle = \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}k_1}|k_1, q_2\rangle. \tag{21}$$

They define an M-dimensional kq representation that is associated with the particular factorization $M = M_1M_2$. The indices are always associated with the range of the variable, thus, e.g. $q_2 = 1, \ldots, M_2$. In the following we shall omit, unless clarity requires otherwise, the numerical indices of q and k, i.e. $q_2 \to q, k_1 \to k$, with similar omission for such indices which will be introduced later. It should be noted that in this notation operators of different indices commute as is illustrated in equation (20). To construct the conjugate vector basis [18] we consider the conjugate pair of (commuting) operators:

$$\tau(M_1) = \mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_1})x}, \qquad T(N_2L_2) = \mathrm{e}^{\mathrm{i}pN_2L_2}, \tag{22}$$

and their eigenfunctions

$$\begin{aligned} \tau(M_1)|K_2, Q_1\rangle &= \mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_1})Q_1}|K_2, Q_1\rangle, \qquad && Q_1 = 1, \ldots, M_1, \\ T(N_2L_2)|K_2, Q_1\rangle &= \mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_2})K_2}|K_2, Q_1\rangle, \qquad && K_2 = 1, \ldots, M_2. \end{aligned} \tag{23}$$

The basic commutation relations for our operators are

$$\begin{aligned} T(N_1L_1)\tau(M_1) &= \tau(M_1)T(N_1L_1)\,\mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_1})}, \\ T(N_2L_2)\tau(M_2) &= \tau(M_2)T(N_2L_2)\,\mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_2})}, \end{aligned} \tag{24}$$

with all other operators commuting. Hence we have

$$T(N_1L_1)\tau(M_1)|k, q\rangle = \mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_1})}\,\mathrm{e}^{\mathrm{i}(\frac{2\pi}{M_1})k}\tau(M_1)|k, q\rangle, \tag{25}$$

indicating that $\tau(M_1)|k, q\rangle$ is, up to a phase factor, $|k+1, q\rangle$. In a similar fashion one can show that $T(N_1L_1)|K, Q\rangle$ is, again up to a phase factor, $|K, Q-1\rangle$. The two other operators are also shift operators for the appropriate states. Now, since k is defined mod M_1 and q is defined mod M_2, successive application of either (and both) $\tau(M_1)$, $T(N_2L_2)$ on any one vector $|k, q\rangle$

will generate, *uniquely*, all the vectors in the set $|k, q\rangle$. Thus all the states of one set may be generated by the operators of the other set[4].

Returning to our factorization of M in terms of relative primes, equation (8), we find that only bi-partitionings of the N primes are allowed: P^n may *not* be split by breaking it up into two powers, say P^{n_1} and $P^{n_2}, n = n_1 + n_2$ with one factor in M_1 and the other in M_2, i.e., the bi-partitionings are among the groups of $m_i s$ (equation (8)). Thus the number of kq representations that form a complete operator basis for an M-dimensional physical system equals the number of possible bi-partitionings of M into products of distinct primes that make M (equation (8)), i.e., 2^{N-1} [18].

To conclude this section we give a new derivation for the overlap $\langle kq|KQ\rangle$: recalling our discussion above, we supplement equation (21) with

$$\tau(M_1)|k, q\rangle = |k+1, q\rangle \qquad \text{and} \qquad T(N_2L_2)|k, q\rangle = |k, q-1\rangle, \tag{26}$$

and equation (23) with

$$\tau(M_2)|K, Q\rangle = |K+1, Q\rangle \qquad \text{and} \qquad T(N_1L_1)|K, Q\rangle = |K, Q-1\rangle. \tag{27}$$

These are valid up to phases that are conveniently chosen to be null [2]. We now evaluate $\langle kq|A|KQ\rangle$, where A stands for each of the four operators that generate the complete operator basis for the case under study,

$$\tau(M_1), T(N_1L_1), \tau(M_2) \qquad \text{and} \qquad T(N_2L_2).$$

This leads to the four relations

$$\begin{aligned} &\mathrm{e}^{\mathrm{i}\frac{2\pi}{M_2}q}\langle kq|KQ\rangle = \langle kq|K+1, Q\rangle, &&\mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}Q}\langle kq|KQ\rangle = \langle k-1, q|K, Q\rangle, \\ &\mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}k}\langle kq|KQ\rangle = \langle k, q|K, Q-1\rangle, &&\mathrm{e}^{\mathrm{i}\frac{2\pi}{M_2}K}\langle k, q|KQ\rangle = \langle k, q+1|KQ\rangle. \end{aligned} \tag{28}$$

These are solved by

$$\langle kq|KQ\rangle = \frac{\mathrm{e}^{\mathrm{i}(KqM_1 - kQM_2)\frac{2\pi}{M}}}{\sqrt{M}}, \tag{29}$$

which implies the conjugacy of the two vector bases [13, 14].

3. The q_1q_2 representation

The choice of the two unitary commuting operators $\tau(M_2)$ and $T(N_1L_1)$ (equation (21)) as those that define our vector space basis, i.e. the choice of a kq representation to study the system, is optional. An alternative choice is the two unitary and commuting operators $\tau(M_2)$ and $\tau(M_1)$ [19]. We now discuss such a choice—it leads to the representation that we choose to call the q_1q_2 representation, since its labels may be considered as designating the spatial

[4] It is via this attribute that the necessity of having M_1 and M_2 as relative primes emerges. If M_1 and M_2 have a common factor the $|k, q\rangle$ set defined by $\tau(M_2)$ and $T(N_1L_1)$ is complete. Thus, to have a kq representation what is required is that M is *not* a prime number. To have conjugate kq representations it is necessary that M be factorized into a product of two relative primes. To illustrate this consider an example with $M = 12$ bi-factorized by $M_1 = 2, M_2 = 6$. One can readily check that applying $\tau(M_1)$ and $T(L_2)$ will shift both k and q by multiples of 2 only. In this case we may consider the operator

$$F = \lambda_1 \sum_{k,q=\text{even}} |k, q\rangle\langle k, q| + \lambda_2 \sum_{k,q=\text{odd}} |k, q\rangle\langle k, q|, \quad \lambda_1 \neq \lambda_2.$$

This operator commutes with $\tau(M_2)$ and $T(L_1)$, *and* with $\tau(M_1)$ and $T(L_2)$, while it is *not* a multiple of the unit operator. Hence in cases where the bi-factorization involves numbers which are not relatively prime, one is *not* led to a complete operator basis. Thus the bi-factorization must be without having the same prime (cf equation (8)) occurring in both terms.

coordinates. This representation is closely related to the kq representation. It exists only when M_1 and M_2 are relatively prime, in which case the kq representation has a conjugate KQ representation. The common eigenfunctions of $\tau(M_1)$ and $\tau(M_2)$ are $|q_1, q_2\rangle$. Thus, with

$$\tau(M_1) = \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}x} = \tau(M)^{M_2} \qquad \tau(M_2) = \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_2}x} = \tau(M)^{M_1}, \tag{30}$$

the eigenvector equations are

$$\begin{aligned} \tau(M_1)|q_1, q_2\rangle &= \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}q_1}|q_1, q_2\rangle, \qquad q_1 = 1, \ldots, M_1, \\ \tau(M_2)|q_1, q_2\rangle &= \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_2}q_2}|q_1, q_2\rangle, \qquad q_2 = 1, \ldots, M_2. \end{aligned} \tag{31}$$

These provide an alternative vector basis for the M-dimensional space. The complete operator basis includes, in addition, the unitary operators,

$$T(N_1L_1) \qquad \text{and} \qquad T(N_2L_2).$$

The eigenvector equations for these operators are

$$T(N_1L_1)|k_1, k_2\rangle = \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}k_1}|k_1, k_2\rangle, \qquad T(N_2L_2)|k_1, k_2\rangle = \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_2}k_2}|k_1, k_2\rangle. \tag{32}$$

These, too, span the space and form the conjugate vector basis to $|q_1, q_2\rangle$. A convenient way to demonstrate this is by showing that the absolute value of the overlap of any member of one basis with any member of the other one is independent of either vector [13, 14]. We may get the expression for the overlap $\langle q_1, q_2|k_1, k_2\rangle$ in much the same way that we got equation (29). The result is

$$\langle q_1, q_2|k_1, k_2\rangle = \frac{\mathrm{e}^{\mathrm{i}(q_1k_1M_2+q_2k_2M_1)\frac{2\pi}{M}}}{\sqrt{M}}, \tag{33}$$

assuring that the two vector bases are conjugate.

We now obtain the overlap $\langle x|q_1, q_2\rangle$ where $|x\rangle$ is the eigenvector of $\tau(M)$ with the eigenvalue $\mathrm{e}^{\mathrm{i}\frac{2\pi}{M}x}$. The method is similar to the one we used above for the overlap of the vectors belonging to conjugate vector bases. Thus, since $\tau(M_1) = [\tau(M)]^{M_2}$, we have

$$\langle x|\tau(M_1)|q_1, q_2\rangle = \langle x|q_1, q_2\rangle\, \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}q_1} = \langle x|[\tau(M)]^{M_2}|q_1, q_2\rangle = \mathrm{e}^{\mathrm{i}\frac{2\pi}{M_1}x}\langle x|q_1, q_2\rangle. \tag{34}$$

Using a similar equation with $\tau(M_2)$ replacing $\tau(M_1)$, we obtain

$$x = q_1[\mathrm{mod}\, M_1], \qquad x = q_2[\mathrm{mod}\, M_2]. \tag{35}$$

Noting that $\gcd(M_1, M_2) = 1$ and using the Chinese remainder theorem [20, 21], we have that the unique solution is

$$x = q_1N_1L_1 + q_2N_2L_2[\mathrm{mod}\, M]. \tag{36}$$

Here $N_i = L_i^{-1}\,[\mathrm{mod}\, M_i]$, $i = 1, 2$ (cf equation (16)). Thus we obtain

$$\langle x|q_1, q_2\rangle = \Delta(x - q_1N_1L_1 - q_2N_2L_2), \tag{37}$$

with $\Delta(y) = 1$ when $y = 0\,[\mathrm{mod}\, M]$, and is zero otherwise. The relation for the conjugate vector basis $|k_1, k_2\rangle$ can be handled similarly and we get

$$\langle p|k_1, k_2\rangle = \Delta(p - k_1L_1 - k_2L_2). \tag{38}$$

We now comment briefly on some localization attributes of wavefunctions when described in this representation. We consider a state $|\psi\rangle$ that is smeared over one spatial label but is localized in the other:

$$\langle q_1, q_2|\psi\rangle = \frac{\delta_{q_1,M_1}}{\sqrt{M_2}}. \tag{39}$$

In the k_1k_2 space we have

$$\langle k_1k_2|\psi\rangle = \frac{1}{\sqrt{MM_2}}\Sigma_{q_2}\mathrm{e}^{2\pi\mathrm{i}(\frac{q_2k_2}{M_2})} = \frac{\delta_{k_2,M_2}}{\sqrt{M_1}}. \tag{40}$$

Thus states spread over q_2 and localized in q_1 are, in the conjugate basis, spread in k_1 and localized in k_2, with the localization exhibiting the factorization of M.

4. Complete factorization

We now proceed and obtain a representation in which each prime number in the expression for M (cf equation (8)) has characteristics of a degree of freedom [2]. We define

$$L_j \equiv \prod_{k \neq j} P_k^{n_k} = \frac{M}{m_j}, \qquad m_j = P_j^{n_j}. \tag{41}$$

Now consider

$$\tau(m_j) = \tau(M)^{L_j} = U_j = e^{i\frac{2\pi}{m_j}x}, \qquad T(N_j L_j) = T(c)^{N_j L_j} = V_j = e^{iN_j L_j p}. \tag{42}$$

We have clearly

$$U_j^{m_j} = V_j^{m_j} = 1, \tag{43}$$

which defines the dimensionality of the relevant coordinates (see below), and

$$U_i U_j = U_j U_i, \qquad V_i V_j = V_j V_i, \qquad \text{and} \qquad V_i U_j = U_j V_i, \quad \forall i \neq j. \tag{44}$$

However (cf [2])

$$V_i U_i = U_i V_i \, e^{i\frac{2\pi}{m_i}}. \tag{45}$$

We define the N-indexed wavefunction $|q_1, \ldots, q_N\rangle$ as the eigenfunction of the N (commuting) operators $\tau(m_j)$, $j = 1, \ldots N$:

$$\begin{aligned} \tau(m_j)|q_1, \ldots q_j, \ldots, q_N\rangle &\equiv U_j|q_1, \ldots q_j, \ldots, q_N\rangle \\ &= e^{i\frac{2\pi}{m_j}q_j}|q_1, \ldots q_j, \ldots, q_N\rangle, \qquad q_j = 1, \ldots, m_j. \end{aligned} \tag{46}$$

Since the $m_j s$ are relatively prime and the equation $\tau(m_j)^{m_j} = 1$ is a minimal equation, the m_j eigenfunctions of $\tau(m_j)$ are distinct and different for each index j. We now relate this wavefunction to the eigenfunction of $\tau(M)$ by the same procedure that we used above: we establish the correspondence between the M eigenvectors of $\tau(M)$ and those of $\tau(m_j)$. We have N equations of the form

$$\begin{aligned} \langle x|e^{i\frac{2\pi}{m_j}x}|q_1, \ldots q_j, \ldots q_N\rangle &= e^{i\frac{2\pi}{m_j}q_j}\langle x|q_1, \ldots q_j, \ldots q_N\rangle \\ &= \langle x|\left[e^{i\frac{2\pi}{M}x}\right]^{L_j}|q_1, \ldots q_j, \ldots q_N\rangle = e^{i\frac{2\pi}{m_j}x}\langle x|q_1, \ldots q_j, \ldots q_N\rangle. \end{aligned} \tag{47}$$

Thus we must have

$$\begin{aligned} x &= q_1 \,[\mathrm{mod}\, m_1] \\ x &= q_2 \,[\mathrm{mod}\, m_2] \\ &\ldots \\ x &= q_N \,[\mathrm{mod}\, m_N]. \end{aligned} \tag{48}$$

Since $\gcd(m_i, m_j) = 1$, for all $i \neq j$, we have by the Chinese remainder theorem [20, 21] that

$$\langle x|q_1, \ldots q_j, \ldots q_N\rangle = \Delta\left(x - \Sigma_{j=1}^N q_j N_j L_j\right). \tag{49}$$

This associates each of the M values of x with a unique set of the $q_j s$.

The M eigenvectors of the commuting operators $T(N_j L_j)$, $j = 1, \ldots, N$, satisfy

$$T(N_j L_j)|k_1, \ldots, k_j, \ldots, k_N\rangle = e^{i\frac{2\pi}{m_j}k_j}|k_1, \ldots, k_j, \ldots, k_N\rangle, \qquad k_j = 1, \ldots, m_j. \tag{50}$$

By a procedure analogous to that used above to derive equation (49), we get here

$$\langle p|k_1, \ldots, k_N\rangle = \Delta\left(p - \Sigma_{j=1}^N k_j L_j\right). \tag{51}$$

The overlap is evaluated to be

$$\langle k_1 \cdots k_N | q_1 \cdots q_N \rangle = \frac{\mathrm{e}^{\mathrm{i}(\sum_{j=1}^{N} k_j q_j L_j)\frac{2\pi}{M}}}{\sqrt{M}}. \tag{52}$$

In the above, the conjugate vector bases representations $|q_1, \ldots q_j, \ldots q_N\rangle$and $|k_1, \ldots, k_j, \ldots, k_N\rangle$ exhibit the prime numbers constituents of M. Each index j may be viewed as defining a subspace that is associated with the prime P_j. We refer to this representation as the completely factorized representation.

5. Characterization of factorization

In this section we characterize the possible bi-factorizations of M into two relative primes by the roots of an equation implied by the Chinese remainder theorem. In principle one might expect that such a process could be reversed, i.e. by noting the characteristics of the factorizable physical system, given in some space dimensionality M, one may deduce the factors involved. However we address ourselves to the former issue. Thus we will show, in parallel with number theory analysis, that the eigenvalues of unitary operators which form a complete operator basis [2] for a given space dimensionality, M, reflect the factors that make up the number M.

Our analysis above and, in particular, the completely factorized representation as such, allows viewing the N distinct prime constituents of M, equation (8), as N degrees of freedom (cf [2, 14, 22]). Now the relation between $|x\rangle$, the eigenfunction of $\tau(M)$ which deals with the space as a whole (equation (4)), and the eigenfunction $|q_1, \ldots, q_N\rangle$ of the $\tau(m_r)$, that reflects the subspaces, each associated with a particular prime P_r (and dimensionality m_r) is given by equation (49)

$$\langle x | q_1, \ldots q_N \rangle = \Delta(x - q_1 N_1 L_1 - q_2 N_2 L_2 - \cdots - q_N N_N L_N).$$

As was noted in the previous section, this equation brings into our analysis the results of the Chinese remainder theorem [20, 21]. This theorem implies the following

$$\begin{aligned} x &= 1\,[\mathrm{mod}\ M] \Leftrightarrow q_r = 1\,[\mathrm{mod}\ m_r], \qquad \text{for all } r \\ x^2 &= 1\,[\mathrm{mod}\ M] \Leftrightarrow q_r^2 = 1\,[\mathrm{mod}\ m_r], \qquad \text{for all } r. \end{aligned} \tag{53}$$

The equation $x^2 = 1\,[\mathrm{mod}\ M]$ has several solutions. We will henceforth designate the solutions by a_s. We have immediately that, if a_s is a solution, namely $a_s^2 = 1\,[\mathrm{mod}\ M]$, so is $-a_s$, i.e. the solutions appear in pairs.

We now argue that the number of pairs of solutions is 2^{N-1}. Thus we may associate each solution with a conjugate pair of the kq-representation (or equivalently with the $q_1 q_2$ and $k_1 k_2$ representations) that can be accommodated in M dimensions. The trivial solution, $a_s = 1$, is always (i.e. even if M is (power of) prime) present. It corresponds to the trivial factorization, $M = 1 \cdot M$ that we associate with the Fourier representation [18, 19]. We now show that the number of solutions to $x^2 = 1\,[\mathrm{mod}\ M]$ equals 2^{N-1}. The proof is direct: equation (53) implies that

$$x^2 = 1\,[\mathrm{mod}\ M] \Rightarrow q_r = \pm 1\,[\mathrm{mod}\ m_r] \quad \text{for} \quad \mathrm{r} = 1, \ldots, N.$$

This gives 2^N possibilities. But only half of these are distinct since the two solutions $a_s = \pm 1$ give equivalent factorization but in a reverse order (if a_s satisfies $(a_s+1)(a_s-1) = 0\,[\mathrm{mod}\ M]$, then $-a_s$ satisfies $(a_s-1)(a_s+1) = 0\,[\mathrm{mod}\ M]$), and as the order of the factors is immaterial the two lead to one bi-factorization. Note that similar reasoning introduces a factor 1/2 in counting the number of conjugate kq-representations; there this was interpreted as having each distinct bi-factorization leading to a distinct conjugate pair of vector bases—the kq and KQ [18]. Thus 2^{N-1} gives the number of kq conjugate pairs and the number of solutions of $x^2 = 1\,[\mathrm{mod}\ M]$, both expressing the bi-factorization of M into relatively prime numbers.

To clarify the above we now consider, in some detail, a simple example: let $M = 105 = 3 \times 5 \times 7$. Thus we have

$$\begin{aligned} m_1 &= 3, & N_1 &= 2, & L_1 &= 35, \\ m_2 &= 5, & N_2 &= 1, & L_2 &= 21, \\ m_3 &= 7, & N_3 &= 1, & L_3 &= 15. \end{aligned} \tag{54}$$

There are $2^2 = 4$ pairs of (distinct) solutions

$$\begin{aligned} &q_1 = q_2 = q_3 = 1, \Rightarrow a_1 = 1\,[\mathrm{mod}\ 105], \\ &q_1 = q_2 = 1, q_3 = -1, \Rightarrow a_2 = 76\,[\mathrm{mod}\ 105], \\ &q_1 = 1, q_2 = q_3 = -1, \Rightarrow a_3 = 34\,[\mathrm{mod}\ 105], \\ &q_1 = q_3 = 1, q_2 = -1, \Rightarrow a_4 = 64\,[\mathrm{mod}\ 105]. \end{aligned} \tag{55}$$

The four other solutions may be obtained by reversing the signs of the a_s which is obtained by changing the signs of all three q_r in each set. One can readily check that $a_s^2 = 1\,[\mathrm{mod}\ 105]$ in all cases. Now we have that for each s ($s = 2, 3, 4$)

$$(a_s + 1)(a_s - 1) = 0\,[\mathrm{mod}\ 105].$$

Inserting the values of the a_s from $s = 2$ to $s = 4$ (skipping the trivial case of $s = 1$) we get the following expressions for $(a_s + 1)(a_s - 1)$:

$$s = 2 : 5 \times 11(15)(7), \qquad s = 3 : 11(15)(7), \qquad s = 4 : 3 \times 13(21)(5), \tag{56}$$

all evidently zero [mod 105]. We see that every distinct root leads to a distinct bi-factorization. Since the bi-factors must be distinct in every case, so must be the a_s.

To summarize, we have shown that among the eigenstates of the completely factorized representation, those distinguished by $q_j = \pm 1 (j = 1, \ldots N)$ correspond uniquely to the relatively prime bi-factorization of M.

6. Conclusions and discussion

Considerable effort in the study of finite-dimensional quantum mechanics can be traced to the so-called state determination problem (e.g. [8, 14, 15, 22–24] and references therein) namely: what is the minimal set of measurements needed to determine a state? The efficient measurements are expected to be those that are mutually unbiased [24, 25]. These studies specify the mutually conjugate (i.e. mutually unbiased) complete, orthonormal, vector bases that can be accommodated in a finite-dimensional space. Such a characterization has also attractive applications in cryptography [3]. In these studies a dimensionality, M, which is a prime number (or a power of a prime number) allows complete and direct results [24, 25]. In this paper we considered an almost diametrically opposite problem: the dimensionalities of interest are composite numbers (i.e. factorizable into distinct primes and their powers). Among these factors we show how to define *pairs* of conjugate bases. Thereby we, hopefully, provide an approach that will help to understand why a quantum computer can be more efficient in the factorization problem.

Shor's discovery [12] of an algorithm for factorization with quantum computers forms a central step in the development of quantum information theory. The number theoretic basis of the factorization method in Shor's algorithm has been studied extensively [20]. In this paper we give what may be viewed as a study of the physics of factorization, i.e. the inter-relation between the dimensionality of the space under investigation and the representations that reflect its prime number constituents. To this end we elaborate on Schwinger's [2] analysis of unitary operator bases for finite-dimensional Hilbert spaces and show, in what we consider to be a physical language, that a natural representation is available which exhibits the prime number constituents of M. In such a representation each of the N prime numbers present in the prime factorization of M defines a subspace. We give the operator basis acting in such subspaces. We further show that different, when possible, bi-factorizations of M may be viewed as different conjugate pairs of vector bases that may be associated with the kq representations [17, 18], or q_1q_2 and k_1k_2 representations. It was shown that the factorization of the dimensionality of the space as a number is equivalent to the break-up of the space into subspaces. Each subspace is viewed as representing a distinct degree of freedom reflecting a prime number that is among the prime constituents of M.

Acknowledgments

FCK acknowledges the support of NSERC. AM and MR thank the Theoretical Physics Institute at the University of Alberta and the Singapore A^* STAR Temasek Grant 012-104-0040 for partial support. AM and MR thank the National University of Singapore and in particular Professor B-G Englert for kind hospitality and helpful discussions. AM, FCK and MR thank Professor S Sehgal of the University of Alberta for a very helpful discussion. AM acknowledges the hospitality of the Institute for Quantum Information Science at the University of Calgary during the last stages of this work.

References

[1] Weyl H 1950 *Theory of Groups and Quantum Mechanics* (New York: Dover) (reprint)
[2] Schwinger J 1960 *Proc. Natl Acad. Sci.* **46** 570
[3] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[4] Santhanam T S and Tekumalla A R 1975 *Found. Phys.* **6** 583
[5] Pegg D T and Barnett S M 1989 *Phys. Rev.* A **39** 1665
[6] Cannata F and Ferrari L 1991 *Found. Phys. Lett.* **4** 557
Cannata F and Ferrari L 1991 *Found. Phys. Lett.* **4** 569
[7] Schoenhammer K 2002 *Phys. Rev.* A **66** 014101
[8] de la Torre A C and Goyeneche D 2003 *Am. J. Phys.* **71** 49
[9] Vourdas A 2004 *Rep. Prog. Phys.* **67** 267
Vourdas A 2006 *J. Phys. A: Math. Gen.* **39** R65
[10] Szilard L 1929 *Z. Phys.* **53** 840
Shannon C E and Weaver W 1963 *The Mathematical Theory of Communication* (Urbana, IL: University of Illinois Press)
[11] Wiesner S 1983 *SIGACT News* **15** 78
Benioff P A 1982 *Int. J. Theor. Phys.* **21** 177
Feynman R P 1982 *Int. J. Theor. Phys.* **21** 467
Deutsch D 1985 *Proc. R. Soc.* A **400** 97
Landauer R 1991 *Phys. Today* **44** 23
[12] Shor P W 1994 *Proc. 35th Annual Symp. on the Foundations of Computer Science* ed S Goldwasser (Los Alamitos, CA: IEEE Computer Society)
[13] Englert B-G 2005 Private communication
[14] Wootters W K 1987 *Ann. Phys. (NY)* **176** 1
[15] Ellinas D and Floratos E G 1999 *J. Phys. A: Math. Gen.* **32** L63
[16] A physical example is the motion of an electron in a periodic potential and magnetic field: Zak J 1986 *Phys. Lett.* A **116** 195
Zak J 1989 *Phys. Rev.* B **39** 694

[17] Zak J 1967 *Phys. Rev. Lett.* **19** 1385
Zak J 1970 *Phys. Today* **23** 51
[18] Mann A, Revzen M and Zak J 2005 *J. Phys. A: Math. Gen.* **38** L389
[19] Mann A, Revzen M and Zak J 2006 Asher Peres memorial issue *Int. J. Quant. Inf.* **4** 173
[20] Ekert A and Jozsa R 1996 *Rev. Mod. Phys.* **69** 733 (this paper includes an extensive reference list)
[21] Niven I and Zuckerman H S 1972 *An Introduction to the Theory of Numbers* 3rd edn (New York: Wiley)
Schroeder M R 1985 *Number Theory in Science and Communication* 2nd edn (Berlin: Springer)
[22] Leonhardt U 1995 *Phys. Rev. Lett.* **74** 4101
Leonhardt U 1998 *Phys. Rev.* A **53** 2998
[23] Ivanovic I D 1981 *J. Phys. A.: Math. Gen.* **14** 3241
[24] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2001 *Preprint* quant-phys/0103162 v3
[25] Wootters W K and Fields B D 1989 *Ann. Phys. (NY)* **191** 363
Gibbons K S, Hoffman M J and Wootters W K 2004 *Phys. Rev.* A **70** 062101