Physics of Factorization

M. Revzen, A. Mann and J. Zak
Department of Physics, Technion - Israel Institue of Technology,
Haifa 32000, Israel

Abstract

The N *distinct* prime numbers that make up a composite number M allow 2^{N-1} bi partioning into two relatively prime factors. Each such pair defines a pair of conjugate representations. These pairs of conjugate representations, each of which spans the M dimensional space are the familiar complete sets of Zak transforms (J. Zak, Phys. Rev. Let.**19**, 1385 (1967)) which are the most natural representations for periodic systems. Here we show their relevance to factorizations. An example is provided for the manifestation of the factorization.

PACS Numbers 03.65.-w

Shor's discovery [1] of an algorithm for factorization with quantum computers is considered one of the benchmarks in the developement of quantum information theory. In the following we hope to initiate a study of the physics of factorization, i.e. the interrelation between factorization and physical representations. Our study shows that a finite dimensional kq representation (i.e. the Zak transform) [2] can be viewed as a member in a set of pairs of conjugate representations each spanning the same finite dimensional phase space. Members of the set (Fourier transform is counted as one such member) relate to the factorization of the number M which is the space dimensionality. Thus we have a correspondence between the set of Zak transforms in M dimensional space and the factorization of M. To achieve self containment we shall review some of our earlier results [3], which are based on a general theory of quantum mechanics in finite phase plane [4] that was developed by Schwinger [5]. In Schwinger's study the finiteness of phase space is realized by applying boundary conditions to the coordinate x of the considered wave functions $\psi(x)$, *and* to their Fourier transform $F(p)$:

$$\psi(x+Mc)=\psi(x);\ F(p+\frac{2\pi}{c})=F(p), \tag{1}$$

where M is an integer and c is constant. (We refer to c as the scaling constant.) As a consequence of these boundary conditions, the coordinate x and the momentum p are quantized ($\hbar=1$) and they assume the following discrete values

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

Thus Eq.(1) implies ([5]) an M dimensional vector space. In our study the operators $\hat{x}$ and $\hat{p}$ are replaced by the exponential operators $\tau(c)$ and $T(c)$ defined by,

$$\tau(Mc)=e^{ix\frac{2\pi}{Mc}}, \qquad T(c)=\ e^{ipc}. \tag{3}$$

We now assume that M is factorizable to

$$M=M_1^nM_2^m\ldots M_{N-1}^rM_N^s, \tag{4}$$

with the $M_i\neq M_j$, $(i\neq j)$ prime numbers, while $n,m,...,r,s$ are positive integers, i.e., M is made of N distinct prime numbers. We now consider the partitioning of this product into two factors,

$$M=M_aM_{\tilde{a}}. \tag{5}$$

Here M_a incorporates one part of the above N factors while $M_{\tilde{a}}$ contains the other part. We note that this assures that the two numbers M_a and $M_{\tilde{a}}$ are relative prime, i.e. the equation

$$sM_a\ -\ tM_{\tilde{a}}\ =\ 0\ [Mod\ M] \tag{6}$$

has only the trivial solution for the integers $[s,\ t]$, viz $t = M_a,\ s = M_{\tilde{a}}$. We further define the two lengths,

$$a = M_a c\ , \quad \tilde{a} = M_{\tilde{a}} c\ . \tag{7}$$

An example of one such partitioning for the M given in Eq.(4) is

$$M_a = M_1^n \text{ and } M_b = M_2^m \dots M_N^s. \tag{8}$$

Next we define two kq-representations based on the two complete sets of commuting operators [2]

$$\tau(a) = e^{i\hat{x}\frac{2\pi}{a}}, \quad T(a) = e^{i\hat{p}a} \tag{9}$$
$$\tau(\tilde{a}) = e^{ix\frac{2\pi}{\tilde{a}}}, \quad T(\tilde{a}) = e^{ip\tilde{a}}. \tag{10}$$

We shall refer to the first pair, associated with Eq. (9), as the "a" set and to the second, Eq. (10), as the "$\tilde{a}$" set.(Thus, e.g., the "a" set has its q coordinate: $q = gc,\ \ g = 1, \dots, M_a$, while the set "$\tilde{a}$" has its Q coordinates $Q = g'c\ \ g' = 1, \dots, M_{\tilde{a}}$.) We have

$$[\tau(a), T(a)] = [\tau(\tilde{a}), T(\tilde{a})] = 0, \tag{11}$$

but

$$T(a)\,\tau(\tilde{a}) = \tau(\tilde{a})\,T(a)\ \exp(i2\pi\frac{M_a}{M_{\tilde{a}}}),$$
$$T(\tilde{a})\,\tau(a) = \tau(a)\,T(\tilde{a})\ \exp(i2\pi\frac{M_{\tilde{a}}}{M_a}). \tag{12}$$

It therefore follows that the operators $T(a)$ and $\tau(a)$ and their powers form a set of M commuting operators. The same holds for the operators $T(\tilde{a})$ and $\tau(\tilde{a})$. This means that the operators in Eqs. (9,10) together with their products lead to M^2 distinct operators which replace the M^2 operators in Eq.(3). (Note: a Zak transform may be defined for arbitrary "a"'s (unrelated to $\tilde{a}$) but only when the two factors M_a and $M_{\tilde{a}}$ of Eq. (5) are relatively prime the two sets form a conjugate pair as is discussed below. We study this case only.)

We now consider the complete sets of eigenvectors of each of the two commuting sets of operators in Eq.(9,10):

$$\tau(a)|k,q\rangle = e^{iq\frac{2\pi}{a}}|k,q\rangle; \ \ T(a)|k,q\rangle = e^{ika}|k,q\rangle, \tag{13}$$
$$\tau(\tilde{a})|K,Q\rangle = e^{iQ\frac{2\pi}{\tilde{a}}}|K,Q\rangle; \ \ T(\tilde{a})|K,Q\rangle = e^{iK\tilde{a}}|K,Q\rangle. \tag{14}$$

Here $|k,q\rangle$ and $|K,Q\rangle$ are, respectively, the eigenvectors of the pairs of commuting operators $\tau(a)$, $T(a)$ and $\tau(\tilde{a})$, $T(\tilde{a})$ in Eqs.(9,10). In Eq.(13,14) the variables $k, q,\ K$ and Q assume the following values [2],

$$\begin{aligned} k = \frac{2\pi}{Mc} f,\ f &= 1, \ldots, M_{\tilde{a}},;\ q = gc,\ g = 1, \ldots, M_a && (15) \\ K = \frac{2\pi}{Mc} \bar{f},\ \bar{f} &= 1, \ldots, M_a,;\ Q = \bar{g}c,\ \bar{g} = 1, \ldots, M_{\tilde{a}}. && (16) \end{aligned}$$

Note that for a given M, Eq. (4), M_a implies $M_{\tilde{a}}$ so we may distinguish distinct Zak transforms by an extra label for which we, conveniently, choose the letter "a". Thus e.g., the Zak transform of Eq. (13) is written as $|k, q; a\rangle$ while its mate, Eq. (14), is written as $|K, Q; \tilde{a}\rangle$. This extra label is somewhat analogous to the characterization of irreducible representations via the values of the appripriate Casimir operator, [7], in as much as it does not relate to an eigenvlues but to the representation as a whole.

We now evaluate $\langle a; k, q|K, Q; a\rangle$. To this end we use, [2], that the x-represenatoion of the eigenfunctions of the "a" set operators (cf. Eq. (13) is given by,

$$\langle x|k, q; a\rangle = \frac{1}{M_{\tilde{a}}} \sum_{s=1}^{M_{\tilde{a}}} e^{iksa} \Delta(x - q - sa), \tag{17}$$

with a similar equation for the "$|K, Q; \tilde{a}\rangle$" set. $\Delta(x)$ is 1 when x is a multiple of Mc, and it vanishes otherwise. (We note in passing that the set $|x\rangle$ may be viewed as an "a" set with $M_a = M$, and $M_{\tilde{a}} = 1$ i.e. it may be written as $|k = \frac{2\pi}{a}, q; a = M\rangle$, since this coincides with the complete set associated with the commuting operators, (cf. Eq. (13)) $\tau(Mc)$ and $T(Mc)$, the latter being unity in our M dimensional space while "q" spans the whole space. Its mate involves the eigenfunctions of the momentum operator, and, equivalently, forms the eigenfunctions of $\tau(c)$ and $T(c)$, Eq. (14). This pair of conjugate represenations are then the "familar" Fourier represenations as is further clarified below.) With these we may write (the extra label, "a", for the states is understood, and will be put explicitly only if required),

$$\begin{aligned} \langle k, q|K, Q\rangle &= \sum_{x=c}^{Mc} \langle kq|x\rangle\langle x|KQ\rangle && (18) \\ &= \frac{1}{\sqrt{M_a M_{\tilde{a}}}} \sum_{s=1}^{M_{\tilde{a}}} \sum_{t=1}^{M_a} \exp(-iksa + iKt\tilde{a}) \Delta(Q + t\tilde{a} - q - sa) && (19) \end{aligned}$$

recalling that $a = M_a c$ and $\tilde{a} = M_{\tilde{a}} c$ (Eq.(7)), the above expression does not vanish only for

$$tM_{\tilde{a}} - sM_a = \frac{q - Q}{c} \equiv r \ [\text{Mod } M]. \tag{20}$$

For M_a and $M_{\tilde{a}}$ relatively prime (Eq. (8)), then the Eq. (20) has a unique pair $[s, t]$ for each $r = 1, \ldots M$. In this case [3, 5],

$$\langle k, q|K, Q\rangle = \frac{1}{\sqrt{M_a M_{\tilde{a}}}} \exp(-iksa + iKt\tilde{a}) \Delta(Q + t\tilde{a} - q - sa), \tag{21}$$

where $\Delta(x)$ does *not* vanish only when $x = 0 \pmod{Mc}$. (Note: for the special case with $a = Mc$ (hence $\tilde{a} = c$) Eq. (21) gives for the right hand side since, in this case, the set $|k, q\rangle$ is independent of k: in this finite dimensional phase space the operator $\exp(ipMc) = 1$. Similarly, for its mate, the set $|K, Q\rangle$ is independent of Q: the operator $\exp(ix\frac{2\pi}{c}$ is unity for all Q. Thus

$$\frac{1}{\sqrt{M}}\exp(iKt)\Delta(Q - q + t) \;=\; \frac{1}{\sqrt{M}}\exp(iKq),$$

i.e. this is the "familiar" Fourier representation (we have not included an irrelevant overall phase factor)).
We note that

$$2^{(N-1)} \;=\; \text{number of bi partitioning of Eq. (4)} \tag{22}$$

of an arbitrary M (given by Eq. (4)) to such conjugate pairs (where N is the number of *distinct* prime factors making the number M. This follows from the fact that 2^N is the number of bi partitions of N distinct items whose relative ordering is immaterial and that we need only half of these (since we are free to label either as an "a" or "$\tilde{a}$" set). We note that whenever a factor, say M_j^n occurs (in M_a or $M_{\tilde{a}}$) it is considered only once as representing the prime number M_j. Thus our label "a" for the sets of conjugate pairs has N distinct values. We reiterate that Eq. (21) implies that $|\langle a; k, q|K, Q; \tilde{a}\rangle|$ does not depend on q and Q nor on k and K. One has to keep in mind, however, that s and t in the phase in Eq.(21) are determined by r in Eq.(20). The result Eq. (21) shows that when the system is in the eigenstate $|K, Q; a\rangle$ of the commuting operators $T(\tilde{a})$ and $\tau(\tilde{a})$ [see Eq.(13),14)], the probability of measuring k and q does not depend on k and q. The same can be said about measuring K and Q in the eigenstate $|k, q; a\rangle$. We can therefore claim that the two sets of commuting operators in Eq.(7) are conjugate [3, 6]. An important property of conjugate operators is as follows [3]. When the "a" set operators in Eq.(7) operate on the eigenvectors of the "$\tilde{a}$" set, the eigenvalues of these eigenvectors are shifted. Let us first find the eigenvalues of the vectors $T(a)|K, Q; \tilde{a}\rangle$. We have, by using the first equation in Eq. (12), and Eq.(9)

$$\tau(\tilde{a})T(a)|K, Q; \tilde{a}\rangle = e^{i(Q-a)\frac{2\pi}{\tilde{a}}}T(a)|K, Q; \tilde{a}\rangle.$$

Thus the operators of the "a" set, when acting on an eigenstate of its conjugate mate span the whole space in a unique way, with a similar effect for operators of the "$\tilde{a}$" set acting on state of the "a" set. Thus each conjugate pair of the set spans the whole M dimensional space. The total number of such pairs equals $2^{(N-1)}$, where is N the number of distinct prime numbers that make up M. We now consider a "physical" implication of this factorization scheme. A simple illustration of it is gained via the familiar Fourier transform which, from the present vantage point is viewed as "factorizing" the dimensionality M as $M = M \cdot 1$, i.e. in the "a" set we have $M_a = M$ (and, hence, $M_{\tilde{a}} = 1$), in other words it is the familiar x space (of dimension M) and its mate the "$\tilde{a}$" set, the eigenfunctions of $\tau(c)$ and $T(c)$, is here the momentum space (also of dimension M). We consider for this conjugate pair the completely delocalized state $|\psi\rangle$, i.e.

$$\langle x_n|\psi\rangle = \frac{1}{\sqrt{M}}, \quad n = 1, ..., M. \tag{23}$$

This state, expressed in terms of its conjugate set (with $(K_m = \frac{2\pi}{Mc}m)$), is

$$\begin{aligned} \langle K_m|\psi\rangle &= \sum_{n=1}^{M}\langle K_m|x_n\rangle\langle x_n|\psi\rangle \;=\; \frac{1}{M}\sum_n e^{iK_m x_n} \\ &= \frac{1}{M}e^{i(2\pi m/M)}\frac{1-e^{i2\pi m}}{1-e^{i2\pi m/M}} \;=\; m\delta_{K_m,K_M}. \end{aligned} \tag{24}$$

Here $\delta_{n,m}$ is the Kronecker delta.(We have not included an irrelevant overall phase factor.) Thus the state is completely localized in its conjugate set space (p space), we note that we have retrieved the factor 1 in the factorization $M = M \cdot 1$, given above in that the state is localized at a point. Thus for the factorization $M = M \cdot 1$, when we have one member of the pair of conjugate set one dimensional, complete delocalization in the first (the "a"member) leads to complete localization (to one eigenstate) in the the "$\tilde{a}$" set. We now consider an arbitrary pair whose "a" member involves the factor M_a whilst its mate, "$\tilde{a}$", involves the factor $M_{\tilde{a}}$, with, of course, $M = M_a M_{\tilde{a}}$. We take $M_{\tilde{a}} > M_a$. We now consider a completely delocalized state in the "a" set, e.g. a particle spread uniformaly over the coordinates of this member of the set, i.e.,

$$\langle a; k, q|\psi\rangle \;=\; \frac{1}{\sqrt{M}}, \tag{25}$$

and wish to evaluate its value in the "$\tilde{a}$" coordinates, i.e. we seek the value of $\langle a; K, Q|\psi\rangle$ (again deleting the "a" label as implicit in the following),

$$\langle K, Q|\psi\rangle \;=\; \sum_{f,g}^{M_b,M_a}\langle K, Q|k, q\rangle\langle k, q|\psi\rangle, \tag{26}$$

where

$$k \;=\; \frac{2\pi}{Mc}f, \;\; f \;=\; 1, 2 \ldots M_{\tilde{a}}, \; q \;=\; gc, \;\; g \;=\; 1, ...M_a. \tag{27}$$

Substituting Eq. (21) and performing the summation over the index f we get, in complete analogy to Eq. (24) (we do not give an irrelevant, overall phase factor.), that only for $s = M_{\tilde{a}}$ we do get a contribution, which is $M_{\tilde{a}}$. Now since Q is fixed, only one t contributes [8], viz $t = M_a$. This is seen as follows:

$|q-Q| \leq M_{\tilde{a}}c$, as $c \ \leq \ q \ \leq \ M_a c$ and, $c \ \leq \ Q \ \leq \ M_{\tilde{a}}c$, with $M_a \ < \ M_{\tilde{a}}$. Hence Eq.(20) with $s \ = \ M_{\tilde{a}}$ can only be satisfied with $q \ - \ Q \ = \ 0$, hence $t \ = \ M_a$. We have then that for each $Q \ = \ gc, g \ = \ 1, ..M_a$ and $K \ = \ \frac{2\pi}{Mc}f, f \ = \ 1, .., M_a$

$$\langle K, Q|\psi\rangle \ = \ \frac{1}{M_a}, \tag{28}$$

and it vanishes elsewhere (an overall phase factor was not included). This result assures the correct normalization of $|KQ\rangle$, since it implies probability of $\frac{1}{M_a^2}$ and there are M_a^2 non vanishing terms. Thus this result generalizes the result above for the "usual" Fourier decomposition to give that a completely delocalized state in the "a" set ($|k, q>$ representation) is a state which, in the "$\tilde{a}$" set ($|K, Q\rangle$ representation is localized over the square (in phase space) covering M_a^2 spots where M_a is one of the appropriate factors of M.

To summarize, we showed that given a number M that can be factorized into N distinct prime numbers (one that occurs more than once is counted only once) and hence may be bipartitioned into 2^{N-1} products of the form $M \ = \ M_a M_{\tilde{a}}$, allows the definiton of 2^{N-1} Zak transform conjugate pairs. The first such partioning, $M_a = 1, \ M_{\tilde{a}} = M$ leads to the familiar Fourier transform pairs while the next N bipartitioning with M_a being one of counted N primes leads to the appropriate Zak transforms conjugate pairs each with one member having the dimension of the factor. Other partitions yield the other members of Zak transform conjugate pairs. To each such conjugate pair a "physical" manifestation of the factor such as M_a is gained by noting that the localization dimension of a state of one conjugate pair member of M_a^2 is associated with completely delocalization of that state in its conjugate mate representation.

We wish to comment briefly on the choice of the scaling factor c (Eq. (1)). Physically the dimensionality of the phase space was determined by two conditions. The first involves the periodicity in space ,$\psi(x+L) = \psi(x)$, the second involves the periodicity in the Fourier transposed space, $F(p+\frac{2\pi}{c}) = F(p)$. The two requirements may be consistent for the same physical system if $L = Mc$ for some integer M. This integer is the dimensionality of the vector space and the number we factorized in our study. The number of conjugate pairs of Zak transforms depends only on the number of distinct primes (cf. Eq. (4)), viz N , Eq. (22). Thus one may consider varying c, and hence M, in such a way as to preserve the number of primes and thereby retaining the same class of Zak transform pairs that retain the same spatial periodicity. This may be achieved as follows. Rewrite Eq. (4) as

$$Mc \ = \ M_1, \ldots, M_N M_1^{n-1}, \ldots, M_N^{s-1}c \ = \ \bar{M}\bar{c}. \tag{29}$$

With $\bar{M} \ = \ M_1, \ldots, M_N$ and $\bar{c} \ = \ M_1^{n-1}, \ldots, M_N^{s-1}c$. Now the phase space dimensionality is determined by requiring the Fourier transform be periodic

in $\frac{2\pi}{\bar{c}}$. With this, the bi factorization to two relatively prime factors each with its distinct Zak transform label, is into primes of first order only, so we may think of $\bar{c}$ as leading to an irreducible set of Zak transforms.
Further insight into our results and into the conjugacy in general may be gained by an alternative approach to the problem. Thus we consider two distinct Zak transforms, the first charaterized by a length "a" and defined through the two basic commuting operators ($\hbar$=1) [9],

$$exp(ix\frac{2\pi}{a}), \quad exp(ipa),$$

while the second is similarly characterized by a length "b". We now consider a scaling factor c such that

$$a \;=\; M_a c, \;\; \text{and} \;\; b \;=\; M_b c.$$

with M_a, M_b integers. To relate to our problem of *finite* phase space we consider the length Mc with,

$$M \;\;=\;\; M_a M_b.$$

For M_a and M_b relatively prime (i.e. $M_b \equiv M_{\tilde{a}}$) we have that the equation

$$sM_a \;+\; tM_b \;=\; 0 \;[\text{Mod}\; M],$$

has a unique solution: $sM_a \;=\; 0$ [Mod M], $tM_b \;=\; 0$ [Mod M]. In these cases the two Zak transforms are conjugate in the M dimensional space thus defined, and, the factorization of M to N distinct primes, Eq.(4), implies that there are 2^{N-1} distinct relative prime pairs M_a, M_b. Thus we are led to M which is factorized by the 2^{N-1} sets of conjugate Zak transform pairs. These include the pair with $M_a = 1$, $M_b = M$ which is the more familiar Fourier tranform in M dimensions. Here as in all cases, we do not count separately the reverse ordering, viz $M_a = M, M_b = 1$, thereby illustrating the source of -1 in the number, 2^{N-1}, of Zak transform conjugate pairs that factorizes the dimensionality number M.

We summarize our main result by noting that a correspondence was established between the factorization of a number M in terms of N distinct prime numbers and the number of distinct conjugate Zak transform pairs, each spanning an M dimensional space. Thus if M is given in terms of N (distinct) primes (each counted once regardless of the number of times it appears in the factorization), M allows 2^{N-1} bipartitioning to two relative prime factors. This number, 2^{N-1}, is the number of (distinct) conjugate Zak transform pairs, each spanning the M dimensional space. We have given an example where, in a particular Zak transform representation, the constituent factor may be observed: a state that is completely delocalized in the representation of one member of a pair of conjugate Zak transform, is localized (evenly) within the dimensionality that equals the smaller factor that charactarizes the other member of the pair.

References

[1] P. W. Shor, *Proceedings of the 35th Annual Symposium on Foundation of Computer Science*, edited by S. Goldwasser (Los Alamos,CA: IEEE computer society press).

[2] J. Zak, Phys. Rev. lett. **19**, 1385 (1967). J. Zak, Phys. Today **23**, 51 (1970).

[3] A. Mann, M. Revzen and J. Zak, submited for publication.

[4] Quantum mechanics in finite phase plane finds applications in great variety of areas such as quantum Hall effect (e.g. X. G. Wen and Q. Niu , Phys. Rev **B 41**, 9377 (1990)), quantum maps (e.g. P. Leboef, J. Kurchau, M. Feingold and D. P. Arovas, Chaos **2**, 125 (1992)), Landau levels in a magnertic field, von Neumann lattices (e.g. J. Zak, J. Math. Phys. **30**, 1591 (1989)) and quantum computing (e.g. S. D. Barlett, H. de Guise and B. C. Sanders, Phys. Rev. **A 65**, 052316 (2002); For a review see A. Vourdas Rep. Prog. Phys. **67**, 267 (2004).

[5] J. Schwinger, Proc. Natl. Acad. Sci. **46**, 570 (1960).

[6] The Δ (cf. Eq. (10)) in conjuction with M_1 and M_2 being relatively prime implies that $\langle k, q|K, Q\rangle$ is a phase factor. This is studied in a forthcoming book by B-G Englert.

[7] e.g., M. Hamermesh *Group Theory and its Application to Physical Problems*, (Reading, Mass: Addison Wesley, 1962)

[8] The proof that a unique pair of integers [s,t] solves the equation $tM_2 - sM_1 = n - m \equiv r\ [ModM]$ with $M_1M_2 = M$ and M_1 and M_2 relatively prime (cf. Eq. (8) is as follows: suppose that another solution exists with [s',t']. Then by subtraction we have $(t - t')M_2 + (s' - s)M_1 = 0$ which is an impossibility for M_1 and M_2 relatively primes. We are grateful to Prof. R. Aharoni for helpfull comments on this subject.

[9] J. Zak, J. Phys. A **37**, L617, (2004).