Remarkable Phase Oscillations Appearing in the Lattice Dynamics of Einstein-Podolsky-Rosen States

Daniel I. Fivel

Department of Physics, University of Maryland, College Park, Maryland 20742

(Received 13 June 1994)

It is shown that the transformations of Einstein-Podolsky-Rosen states such as those used in communication and cryptography schemes can be described as a hopping motion on a finite phase space lattice associated with a finite Heisenberg group. Quantum mechanical Hamiltonians that generate the hopping are shown to cause phase oscillations characterized by the number-theoretic Legendre symbol.

PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c

The clever trick used in the Einstein-Podolsky-Rosen (EPR) [1] argument is to circumvent the uncertainty principle by getting information about a particle from a measurement made on a partner with which it is perfectly correlated. Two-particle states of this kind are called EPR states or "completely entangled states," and their extraordinary properties have suggested possible applications to communication and cryptography [2,3]. The fact that one can make use of the correlation to obtain information about complementary observables suggests that there is a sense in which the dynamics of a two-particle EPR state is *classical* in spite of the underlying quantum mechanical behavior of its constituent particles. In this paper I am going to explain how this classical behavior is generated and show that some surprising phase alteration patterns accompany it that are associated with number-theoretic quadratic residues.

Entangled states have the property that one can transform a two-partner system by a unitary transformation applied to just one of the partners in such a way that an observer who "acquires" both partners can ascertain what transformation was performed. Moreover, no eavesdropper can obtain information by interception of a partner because it is coded into the quantum mechanical phase relationship between them. Consider, for example, a system of two spin-1/2 particles for which we can construct four orthogonal EPR states

$$\begin{aligned}
|A\rangle &= 2^{-1/2}\{|\uparrow,1\rangle|\downarrow,2\rangle - |\downarrow,1\rangle|\uparrow,2\rangle\},\\
|B\rangle &= 2^{-1/2}\{|\uparrow,1\rangle|\downarrow,2\rangle + |\downarrow,1\rangle|\uparrow,2\rangle\},\\
|C\rangle &= 2^{-1/2}\{|\uparrow,1\rangle|\uparrow,2\rangle - |\downarrow,1\rangle|\downarrow,2\rangle\},\\
|D\rangle &= 2^{-1/2}\{|\uparrow,1\rangle|\uparrow,2\rangle + |\downarrow,1\rangle|\downarrow,2\rangle\}. \qquad (1)
\end{aligned}$$

Observe that these states can be transformed into one another by acting only on particle 2 and using only the two unitary operators σ and τ given by

$$\begin{aligned}
\sigma|\uparrow,2\rangle &= |\uparrow,2\rangle, \qquad \sigma|\downarrow,2\rangle = -|\downarrow,2\rangle,\\
\tau|\uparrow,2\rangle &= |\downarrow,2\rangle, \qquad \tau|\downarrow,2\rangle = |\uparrow,2\rangle, \qquad (2)
\end{aligned}$$

together with their products. This gives us the four transformations on particle 2: $u_1, u_2, u_3, u_4 = I, \sigma, \tau, \sigma\tau$.

Thus suppose "Alice" prepares state $|A\rangle$ and sends particle 2 to "Bob" who applies one of the four u_ν's to that particle. He returns the particle to her and, since she now possesses both particles, she can determine which of the four orthogonal states $|A\rangle, |B\rangle, |C\rangle, |D\rangle$ the two-particle system is in by means of a generalized Stern-Gerlach apparatus. Thus she can deduce which of the four choices of operator Bob made.

Now let us examine the structure of the operators u_ν: The two operators σ and τ used to construct them involve multiplication by a root-of-unity phase (here ± 1) and cycling the spin, respectively. The fact that repeated application of the two operators gives rise to only four states results from the fact that σ and τ generate the ray representation of a four element *group*. The structure of that group is very reminiscent of the group of phase space translations in quantum mechnaics. To see this note the similarity between

$$\sigma\tau = e^{i\pi}\tau\sigma \qquad (3)$$

and the coordinate and momentum translations:

$$e^{i\alpha X}e^{i\beta P} = e^{-i\alpha\beta}e^{i\beta P}e^{i\alpha X}. \qquad (4)$$

In both cases we have a *Heisenberg group*. In the latter case it is the infinite Heisenberg group associated with the translations of a continuum phase space with real-valued coordinate and momentum, whereas in the former it is a finite Heisenberg group associated with translations on the finite two-dimensional lattice in which the "coordinates" and "momenta" are in Z_2, i.e., the field of integers mod(2).

Let us next examine the generalization to entangled states of particles with higher spin. It will turn out to simplify matters (without limiting our insight) if we restrict the spin to be $(p-1)/2$ where p is a *prime* number. This is because, as we shall see, the relevant Heisenberg group will involve the integers mod(p) which form a *field* Z_p. This makes it possible to perform any necessary matrix multiplications and inversions in the unencumbered way that we do with real numbers. Each of the two particles in our entangled state will thus be assumed to inhabit a Hilbert space of dimension p, and the two-particle Hilbert space will be of dimension p^2. Our generalization now takes the following form: Let

$|j\rangle$, $j = 0, 1, \ldots, p-1$, be a basis in $\mathcal{H}_p$ of particle 2. Let the unitary matrices σ, τ of U_p be defined by

$$\sigma|j\rangle = \omega^j|j\rangle, \qquad \tau|j\rangle = |j+1\rangle, \quad \text{mod}(p), \qquad \omega = e^{2\pi i/p}. \tag{5}$$

Then the required u_ν's to be applied by Bob to particle 2 are the p^2 operators $u(\mathbf{j})$, where $\mathbf{j} = (j,k)$ with $j,k = 0, 1, \ldots, p-1$ and

$$u(\mathbf{j}) = e^{-i\pi jk/p}\sigma^j\tau^k. \tag{6}$$

From the familiar character identity

$$\sum_{n=0}^{p-1} e^{2\pi i n/p} = \delta_{n0}, \tag{7}$$

where the Kronecker symbol is understood mod(p), one obtains the orthogonality property:

$$\text{Tr}\{u^\dagger(\mathbf{j})u(\mathbf{j}')\} = p\delta_{\mathbf{j}\mathbf{j}'} \text{ or } \text{Tr}\{u(\mathbf{j})\} = p\delta_{\mathbf{j}\mathbf{0}}, \tag{8}$$

and in view of this (see Appendix A) the entangled states they generate will be mutually orthogonal. The operators also obey the Heisenberg group relation:

$$u(\mathbf{j})u(\mathbf{j}') = e^{i\pi\mathbf{j}\times\mathbf{j}'/p}u(\mathbf{j}+\mathbf{j}'), \quad \mathbf{j}\times\mathbf{j}' \equiv jk' - kj', \tag{9}$$

so that we can think of the p^2 states as corresponding to a $p \times p$ lattice phase space in which coordinate and momentum are in the field $\mathcal{Z}_p$ of integers mod(p). We call this lattice $\mathcal{L}_p$.

The fact that the entangled states have a lattice phase space structure suggests that we next consider the possibility of *dynamically inducing an entangled state to "hop" around on that lattice*. Thus we seek a quantum mechanical Hamiltonian that will cause the two particles to evolve in such a way that at a discrete set of times $t = 0, 1, 2, \ldots$ the entangled state will be found on one of the lattice sites.

The states of the lattice are generated by the actions of the u_ν on a fiducial state, and so we need only consider what happens to these operators when the two particles evolve under some specified time evolution. If the time evolution operators for the two partners are $V_1(t), V_2(t)$, respectively, then it is shown in Appendix A that the u_ν operators evolve according to

$$u_\nu \rightarrow V_2 u_\nu V_1. \tag{10}$$

Note that the trace orthogonality of the u_ν's is preserved for any choice of V_1, V_2 but to preserve the Heisenberg group structure we must require $V_2 = V_1^{-1}$. Thus the two particles evolve as they would if they were antiparticles of one another. The time evolution at the discrete times $t = 0, 1, \ldots$ then produces a sequence of unitary similarity transformations on the u_ν's. However, this is *not* sufficient to insure that the u_ν's are transformed into *other* u_ν's, i.e., to insure that the states simply hop from one site in $\mathcal{L}_p$ to another. To achieve this we must have

$$U(t)u(\mathbf{j})U^{-1}(t) = u(\mathbf{j}(t)), \qquad t = 0, 1, 2, \ldots, \tag{11}$$

where we have put $U = V_2 = V_1^{-1}$ and $\mathbf{j}(t)$ is an orbit on $\mathcal{L}_p$. This imposes a tight constraint on the form of U. For one sees from (9) that for any integer

$$u(\mathbf{j})^n = u(n\mathbf{j}), \tag{12}$$

and hence, if one puts $u(\mathbf{j}') = Uu(\mathbf{j})U^{-1}$, it is easy to check from (9) that for any integers n_1, n_2 we must have

$$(n_1\mathbf{j}_1 + n_2\mathbf{j}_2)' = n_1\mathbf{j}_1' + n_2\mathbf{j}_2', \qquad \mathbf{j}_1' \times \mathbf{j}_2' = \mathbf{j}_1 \times \mathbf{j}_2. \tag{13}$$

In other words, we must have

$$Uu(\mathbf{j})U^{-1} = u(\mathcal{M}\mathbf{j}), \tag{14}$$

in which $\mathcal{M}$ is a linear transformation with integer coefficients mod(p) that leaves the cross product invariant mod(p). Thus $\mathcal{M}$ is a member of the group $\text{SL}_2(\mathcal{Z}_p)$.

We have thus established that associated with the quantum mechanical transformation U there must be a linear transformation $\mathcal{M}$ on the finite two-dimensional lattice $\mathcal{L}_p$ of integers mod(p), and we note that $\text{SL}_2(\mathcal{Z}_p)$ is just the $\mathcal{L}_p$ analog of a symplectic (canonical) transformation. In other words, for a sequence of times $t = 0, 1, 2, \ldots$ there will be a "classical orbit"

$$\mathbf{j} \rightarrow \mathbf{j}(t) = \mathcal{M}(t)\mathbf{j} \tag{15}$$

on the two-dimensional phase space lattice of integers mod(p) associated with the orbit of the quantum mechanical state under the time evolution operator $U(t)$.

An elegant relationship between the quantum evolution described by U and the classical evolution described by the corresponding $\mathcal{M}$ is obtained when we actually determine the explicit form of $U = U_\mathcal{M}$ that satisfies (14) for various choices of $\mathcal{M}$. One may guess this form from our experience with X, P in quantum mechanics, namely, that *quadratic* forms in X, P generate linear transformations of the operators. By the completeness of the $u(\mathbf{j})$'s over the p^2-dimensional vector space of $p \times p$ matrices, we know that $U_\mathcal{M}$ can be expressed as a linear combination of them. We are thus led to try linear combinations in which the coefficients are phases constructed by exponentiating quadratic forms $\tilde{\mathbf{j}}\mathcal{Q}\mathbf{j}$, in which $\mathcal{Q}$ is a two-by-two matrix and the tilde indicates a row vector. Indeed we find that for each $\mathcal{M}$ there will be a two-by-two matrix $\mathcal{Q}_\mathcal{M}$ such that

$$U_\mathcal{M} = \sum_{\mathbf{j}} \exp\{(\pi i/2p)\tilde{\mathbf{j}}\mathcal{Q}_\mathcal{M}\mathbf{j}\}\, u(\mathbf{j}), \tag{16}$$

or possibly a degenerate form of this in which the double sum reduces to a simple sum.

A straightforward approach to the determination of the relationship between $\mathcal{Q}_\mathcal{M}$ and $\mathcal{M}$ exploits the fact that the group $\text{SL}_2(\mathcal{Z}_p)$ is generated [4] by ρ, χ with

$$\rho = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \chi = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{17}$$

One readily verifies that the corresponding U_ρ and U_χ will be degenerate forms of (16). Specifically, making

use of (7), one obtains a formula for any powers of the generators:

$$U_{\rho^m} = \sum_{j=0}^{p-1} e^{-\pi i m j^2/p} u(j,0), \qquad U_{\chi^m} = \sum_{k=0}^{p-1} e^{\pi i m k^2/p} u(0,k), \quad m = 1,2,\ldots . \tag{18}$$

Thus one might, in principle, find a $U_{\mathcal{M}}$ for any $\mathcal{M}$ by decomposing it into a product of powers of ρ and χ and use (18). However, simpler and more instructive methods are available as indicated in Appendix B.

Since our primary purpose here is to clarify the relationship between the quantum dynamics determined by U and the associated classical motion on the lattice determined by $\mathcal{M}$, it will suffice to focus on the simplest example, namely, the dynamical process obtained by iterating one of the group generators (17). The corresponding quadratic form gives us the lattice analog of free-particle motion because the associated quadratic form is one that behaves like the free-particle Hamiltonian P^2. It will turn out to simplify matters if we consider a sequence of even numbers and examine

$$U(2t) = (U_\rho)^{2t}, \qquad t = 0,1,\ldots . \tag{19}$$

In quantum mechanics the solution of the Schrödinger equation entails the explicit computation of the time evolution operator. In the case of (19) this means that we must *explicity* compute the right side for any choice of t. Now we note that it follows from (13) that U_{ρ^m} must coincide with $(U_\rho)^m$ *up to a phase*. Hence (19) can be written

$$U(2t) = e^{i\psi(t)} U_{\rho^{2t}}, \tag{20}$$

in which we have an explicit formula for $U_{\rho^{2t}}$ from (18) with $m = 2t$, and so "solving the Schrödinger equation" reduces to determining the phase $e^{i\psi(t)}$. As we shall now see this phase turns out to be extraordinarily interesting.

Note first that from (8) taking traces on both sides of (20) will give

$$e^{i\psi(t)} = p^{-1}\mathrm{Tr}[(U_\rho)^{2t}]. \tag{21}$$

If one inserts the left side of (18) for U_ρ (with $m = 1$), there will be a product of sums indexed by $j_1, j_2, \ldots, j_{2t}$ containing $u(j_1 + \cdots + j_{2t}, 0)$, which has zero trace unless the sum of the j's is 0 mod(p). One can then use (7) to pick out this term using a standard trick and obtain

$$\mathrm{Tr}[(U_\rho)^{2t}] = \sum_n [F(n)]^{2t}, \tag{22}$$

where

$$F(n) = \sum_j e^{-i\pi j^2/p} e^{2\pi i n j/p} = S(-2p) e^{i\pi n^2/p},$$
$$S(p) = \sum_n e^{2\pi i n^2/p}, \tag{23}$$

in which the second step results from completion of the square. Thus

$$e^{i\psi(t)} = p^{-1}[S(-2p)]^{2t} S(p/t). \tag{24}$$

The function $S(x)$ is known as a Gaussian sum and such sums are fundamental in the solution of quadratic diophantine equations. We are fortunate that thanks to Gauss (who is reputed to have worked for five years to prove it) [5] we have a beautiful formula for $S(p/t)$ when p is an *odd* prime, namely,

$$S(p/t) = \left(\frac{t}{p}\right)\sqrt{\left(\frac{-1}{p}\right)p}, \tag{25}$$

where the Legendre symbol is defined by

$$\left(\frac{t}{p}\right) = \begin{cases} +1 \text{ if } t \text{ is a square mod} p, \\ -1 \text{ if } t \text{ is not a square mod} p. \end{cases} \tag{26}$$

Now suppose that our $U(t)$ is generated by a Hamiltonian. If we add an arbitrary constant E to that Hamiltonian, it will introduce an extra factor e^{-2iEt} in (24). Hence the argument of the factor $[S(-2p)]^{2t}$ can be "gauged" away along with the t independent factor in (24) which is removed by changing the time origin. Thus up to gauge we have established the extremely surprising fact that

$$e^{i\psi(t)} = t/p, \tag{27}$$

i.e., the time-evolving phase of the "free" EPR state follows a pattern of $+1$'s and -1's in a manner with basic number-theoretic significance. One may observe that, while the notion of "sign" in the usual sense does not exist in the field Z_p, we can give it meaning if, as for real numbers, we define a positive number as one that is the square of something while a negative number is one that is not. Thus the Legendre symbol extends the notion of sign to Z_p. It can also be shown that for $p > 2$ there are just as many squares (quadratic residues) as nonsquares. Thus we have obtained the quite pleasing result that the analog of free-particle motion in the EPR lattice is characterized by a wave function with the Z_p analog of a sign alternating phase.

The computation of the Legendre symbol is facilitated by a factorization law which reduces it to a product of Legendre symbols whose upper members are the prime factors of t. These in turn obey the celebrated and profound Gaussian law of quadratic reciprocity [4] relating q/p to p/q.

It is clear from the above and the discussion in Appendix B that when we come to investigate and classify more general lattice Hamiltonians we will encounter generalized Gaussian sums (theta series) [4,5] and will have to invoke the general theory of quadratic diophantine equations. It thus appears that we have just scratched the surface of fruitful connections between the lattice dynamics of EPR states and one of the richest areas of contemporary mathematics. For example, it will be of utmost interest to ascertain the quantum mechanical significance of the Gaussian law of quadratic reciprocity.

Appendix A.—An entangled state of two particles of spin $J = (N-1)/2$ has the property that a particle may be found with equal likelihood in any state $|x\rangle$ but will be found with certainty in state $|x\rangle$ if its partner is found

in state $|x\rangle^{\mathcal{U}}$, where $\mathcal{U}$ is a one-one map on the N-dimensional Hilbert space $\mathcal{H}_N$ of a particle. It can then be shown [6] that the map $\mathcal{U}$ must be an antiunitary transformation, i.e.,

$$\mathcal{U} = u\mathcal{T}, \tag{28}$$

in which $\mathcal{T}$ may be an arbitrarily selected antiunitary transformation (which we usually choose to be time reversal) and u runs over the unitary transformations on a particle. One may then establish that all of the entangled states are expressible in the form

$$|u\rangle = N^{-1/2}\sum_{j=1}^{N}|j,1\rangle|j,2\rangle^{u\mathcal{T}} \tag{29}$$

and the antiunitarity of $u\mathcal{T}$ enables one to establish that this expression is independent of the choice of the orthogonal basis $|j\rangle$ used. The fact that two-particle Hilbert spaces can be labeled by one-particle operators was first recognized by von Neumann [7] and extensively studied by Herbut and Vujčić [8,9] who refer to the operator u as the "correlation" operator.

It follows that the scalar product formula for entangled states can be computed from the corresponding correlation operators by

$$\langle u|v\rangle = N^{-1}\mathrm{Tr}(u^{\dagger}v). \tag{30}$$

In the linear space of N by N matrices one can construct a set of N^2 unitary matrices that are orthonormal in the sense of this inner procuct and may be used as a basis.

If particles 1 and 2 are transformed by unitary operators V_1, V_2, respectively, one sees from the fact that the expression in (29) is invariant to a change of basis that the effect is the same as transforming the correlation operator by

$$u \rightarrow V_2 u V_1^{*}, \text{ where } V^{*} \equiv \mathcal{T}V^{-1}\mathcal{T}^{-1}. \tag{31}$$

If V is a unitary time evolution operator associated with a time-reversal invariant Hamiltonian, then one sees that

$$V^{*}(t) = V(t). \tag{32}$$

Note carefully that while an EPR basis spans the two-particle Hilbert space, *linear combinations of EPR states are not in general EPR states,* so that they themselves form a Riemannian manifold—not a linear subspace—in the two-particle space. Thus one produces new EPR states from old ones by *multiplying* u's rather than by adding them, i.e., from (29) one sees that $v|u\rangle = |vu\rangle$ describes the transformation of an EPR state into another by the action of the unitary operator v on particle 2. To insure that successive untitary transformations keep us within a set of N^2 orthogonal states we must therefore find a finite group with a ray representation consisting of N^2 trace-orthogonal matrices. For prime N one can show [10] that the Heisenberg groups we used are the only possibility.

Appendix B.—Suppose that in (16) we put

$$\mathcal{Q}_{\mathcal{M}} = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix},$$

with integers a, b, c and with the restrictions on the discriminant $\Delta \equiv b^2 - 4ac$:

$$\text{(i)}\ \ \Delta \not\equiv 1(\mathrm{mod}p), \qquad \text{(ii)}\ \ \Delta \equiv 1(\mathrm{mod}4),$$

i.e., b odd. Then it can be shown that $\mathcal{Q}_{\mathcal{M}}$ is related to $\mathcal{M}$ by a Cayley transform:

$$\mathcal{M} = \frac{\nu\mathcal{Q}_{\mathcal{M}} + I}{\nu\mathcal{Q}_{\mathcal{M}} - I}, \qquad \nu = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{33}$$

where the computations in (33) are in Z_p. One sees from (33) how the analog of the canonical structure of quantum mechanics is expressed in the finite lattice phase space of EPR states: If $\mathcal{R}$ is a unimodular matrix, one verifies that $\mathcal{R}^{-1}\nu = \nu\tilde{\mathcal{R}}$ so that (33) continues to hold under the transformation

$$\mathcal{M} \rightarrow \mathcal{R}^{-1}\mathcal{M}\mathcal{R}, \qquad \mathcal{Q}_{\mathcal{M}} \rightarrow \tilde{\mathcal{R}}\mathcal{Q}_{\mathcal{M}}\mathcal{R}. \tag{34}$$

Thus each $U_{\mathcal{M}}$ producing a hopping of EPR states from one lattice site to another will have a counterpart under the canonical transformation $\mathcal{R}$ which, as one sees from its relation to ν, is a finite symplectic transformation of the lattice. Note that $\mathcal{R}$ preserves the discriminant and therefore the two conditions used in deriving (33).

I should like to acknowledge useful conversations with L. Washington and A. Dragt.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] C. H. Bennett, G. Brassard, C. Crêpeau, R. Josza, A. Peres, and W. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).
[4] L. K. Hua, *Introduction to Number Theory* (Springer, New York, 1982), p. 367.
[5] B. Schoeneberg, *Eliptic Modular Functions* (Springer, New York, 1974), p. 218.
[6] D. Fivel, University of Maryland report (unpublished).
[7] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University, Princeton, 1955).
[8] F. Herbut and M. Vujčić, J. Math. Phys. (N.Y.) **8**, 1345 (1967).
[9] F. Herbut and M. Vujčić, in *Fondamenti di meccanica quantistica,* Proceedings of the International School of Physics "Enrico Fermi," Course IL, edited by B. d'Espagnat (Academic Press, New York, 1971).
[10] M. Hall, *Theory of Groups* (MacMillan, London, 1959), p. 51.