Physics Letters A 379 (2015) 2556–2560

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Factorization with a logarithmic energy spectrum of a two-dimensional potential

F. Gleisberg [a,*], M. Volpp [a], W.P. Schleich [a,b]

[a] Institut für Quantenphysik and Center for Integrated Quantum Science and Technology, (IQ^{ST}), Universität Ulm, D-89069 Ulm, Germany
[b] Texas A & M University Institute for Advanced Study (TIAS), Institute for Quantum Studies and Engineering (IQSE) and Department of Physics and Astronomy, Texas A & M University, College Station, TX 77843-4242, USA

ARTICLE INFO

Article history:
Received 11 May 2015
Accepted 27 May 2015
Available online 29 May 2015
Communicated by V.M. Agranovich

Keywords:
Number theory
Trapped particle
Factorization protocol

ABSTRACT

We propose a method to factor numbers using a single particle caught in a separable two-dimensional potential with a logarithmic energy spectrum. The particle initially prepared in the ground state is excited with high probability by a sinusoidally time-dependent perturbation into a state whose two quantum numbers represent the factors of a number encoded in the frequency of the perturbation. We discuss the limitations of our method arising from off-resonant transitions and from decoherence.

1. Introduction

The logarithms introduced by John Napier (1550–1617) were used extensively to facilitate tedious calculations.

Even in the last century the slide-rule with its logarithmic scale was an indispensable tool for any physicist but got eventually replaced by the electronic pocket calculator. In this Letter we employ logarithms to find the prime factors p and q of a given number $N = p \times q$ using the quantum dynamics of a single atom moving in a two-dimensional potential.

This potential is designed as to obtain a logarithmic energy spectrum in the two vibrational motions. An excitation with an energy determined by the number to be factored provides us by a measurement of one of the energies of the two motions with the factors. We propose an excitation mechanism which leads us exclusively to the states that contain the factors, that is to the factor states. Moreover, we discuss the limitations of our method.

The problem of factorization is crucial to the security of communication and Peter Shor's celebrated quantum algorithm [1] has triggered interest in alternative methods [2–5]. In a recent article [2] we have proposed a factorization scheme based on two interacting atoms in a one-dimensional trap with a logarithmic energy spectrum. The present Letter is different in three major aspects: (i) We replace the *two* atoms moving in *one* space dimension by a *single* particle in *two* dimensions, (ii) we propose an excitation mechanism which is easier to realize experimentally, and (iii) we consider an energy spectrum which contains a scaling parameter and allows us to eliminate in the outcome of the measurement trivial factors such as unity and the number to be factored.

Our Letter is organized as follows: In Section 2 we introduce the logarithmic spectrum together with the addition formula of the energies which is at the heart of our factorization scheme. We dedicate Section 3 to the realization of such an energy spectrum by the motion of a quantum particle in an appropriate two-dimensional potential and summarize our factorization protocol based on the measurement of the energy of one of the motions. Sections 4 and 5 discuss the dynamics governed by the Schrödinger equation. In particular, we show that the system of differential equations for the probability amplitudes to be in the energy eigenstates reduces to a two-level problem involving the ground state and the factor state only. Since our factorization scheme is based on Rabi oscillations we estimate the interaction time in Section 6 and analyze the influence of perturbations such as off-resonance transitions and decoherence in Section 7. We summarize our results in Section 8 and provide a brief outlook.

2. Addition theorem of energies and factorization

Energy spectra composed of logarithms of either natural numbers or of prime numbers have been studied in [2,6–8]. Our factorization scheme is based on a logarithmic energy spectrum of the type

* Corresponding author.
E-mail address: ferdinand.gleisberg@uni-ulm.de (F. Gleisberg).
URL: http://www.uni-ulm.de/nawi/institut-fuer-quantenphysik.html (W.P. Schleich).

http://dx.doi.org/10.1016/j.physleta.2015.05.038
0375-9601/

$$E_\ell(L) \equiv \hbar\omega_0 \ln\left(\frac{1}{L}\,\ell + 1\right), \tag{1}$$

where the choice of the quantum numbers $\ell = 0, 1, 2, \ldots$ implies a vanishing ground state energy $E_0(L)$. Moreover, we have introduced the unit of energy $\hbar\omega_0$. The argument L indicates the dependence of the spectrum on the constant L which plays the role of a scaling parameter.

We first consider the following two problems: (i) How can a nonvanishing energy

$$E(m\cdot n; L) \equiv \hbar\omega_0 \ln\left(\frac{m\cdot n}{L^2}\right) \tag{2}$$

determined by the product of the two integers m and n be distributed onto two energies of the spectrum (1), and (ii) under which condition is this energy decomposition unique?

The answer to the first question emerges by writing the energy (2) as

$$E(m\cdot n; L) = E_{m-L}(L) + E_{n-L}(L) \tag{3}$$

and comparing it with (1). This addition theorem shows (i) that the scaling parameter L has to be integer, and (ii) that m and n must obey $m, n \geq L$ and $m\cdot n > L^2$.

We now address the second question. The fundamental theorem of arithmetics [9] guarantees that the factors m and n of the product $m\cdot n$ are unique if they are prime. Therefore, at first glance it appears sufficient that the integers m, n are chosen prime. But there is one more possibility of distributing the energy $E(m\cdot n; L)$. Indeed, the relation

$$E(m\cdot n; L) = E_0(L) + E_k(L) \tag{4}$$

with $E_0(L) = 0$ and positive *integer* $k \equiv m\cdot n/L - L$ is valid only if the scaling parameter L is a factor of $m\cdot n$. This possibility is always present for $L = 1$ and has been discussed already in [2,6]. Therefore, throughout our Letter we consider the case $L \geq 2$.

To summarize, the distribution of the energy $E(m\cdot n; L)$ can take place if m, $n \geq L$ with $m\cdot n > L^2$, and it is unique if (i) m, n are prime and (ii) L is *not* a factor of $m\cdot n$. These results are demonstrated in Fig. 1 for the scaling parameter $L = 2$ and $m = 3$ and $n = 5$ and have important consequences for our factorization scheme.

Let the two energies $E_{m-L}(L)$ and $E_{n-L}(L)$ in the addition theorem (3) correspond to the energies of the two degrees of freedom of a particle moving in two dimensions. When we excite the particle from the ground state into a state with total energy $E(m\cdot n; L)$ and provided L is not a factor of $m\cdot n$ we only find the individual energies $E_{m-L}(L)$ and $E_{n-L}(L)$. However, if one of the quantum numbers $m - L$ or $n - L$, or both are negative the corresponding energy does not occur in the spectrum (1). Hence, this excitation cannot take place.

This feature suggests that we can find the prime factors p and q $(p < q)$ of an integer N by an iterative method that tests if a transition from the ground state occurs for a given L. Since in this case (2) and (3) read

$$E_{p-L}(L) + E_{q-L}(L) = \hbar\omega_0 \ln\left(\frac{N}{L^2}\right) \equiv E(p\cdot q; L) \tag{5}$$

we arrive at the following algorithm: When L was chosen by accident larger than p no transition occurs and L has to be lowered. If still no transition occurs it has to be decreased further. If the transition occurs it must be increased. This algorithm converges after a number of steps given by $\ln N$.

However, there is a problem in this scheme. A transition requires a nonvanishing interaction time which is shown in Section 6 to scale with $\sqrt{N}$. Fortunately after this time we find the factors directly by a measurement of the energy and no iteration scheme is necessary.

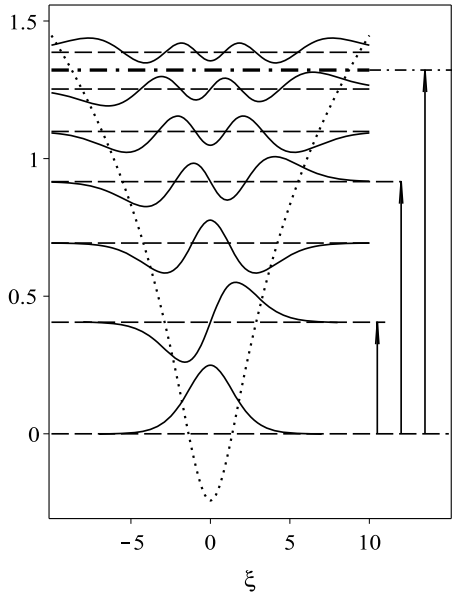

Fig. 1. Scaled one-dimensional potential $V^{(1)}(\xi; L = 2)/\hbar\omega_0$ creating a logarithmic energy spectrum with scaling parameter $L = 2$ as a function of dimensionless coordinate $\xi \equiv \alpha x$ with the trap-specific inverse length $\alpha \equiv (\mu\omega_0/\hbar)^{1/2}$. This potential (dotted line) is determined numerically by an iteration algorithm based on a perturbation theory [8] using the Hellmann–Feynman theorem and is designed to obtain a logarithmic dependence of the energy eigenvalues $E_\ell(L = 2)$ on the quantum number ℓ as given by (1). By solid lines we depict the numerically determined energy wave functions of the first 7 states in their dependence on the dimensionless position. The bold dash-dotted line as well as the long arrow on the right represent the excitation energy $E(3\cdot 5; L = 2) = E_{3-2\,5-2}(L = 2) = E_{1\,3}(L = 2)$ if the number $15 = 3\times 5$ is to be factored, as is expressed by (3) and (9). The two shorter arrows indicate the one-dimensional energies $E_{3-2}(L = 2) = E_1(L = 2)$ and $E_{5-2}(L = 2) = E_3(L = 2)$ which can be seen to sum up to $E_{3-2\,5-2}(L = 2)$. Note that this energy is different from all one-dimensional energies because $L = 2$ is not a factor of the number 15.

3. Energy spectrum of two-dimensional motion

For a given scaling parameter L we can construct numerically a potential $V^{(1)} = V^{(1)}(x; L)$ such that the solutions of the time-independent Schrödinger equation

$$\hat{H}_x^{(1)}\varphi_\ell(x; L) \equiv \left(-\frac{\hbar^2}{2\mu}\frac{d^2}{dx^2} + V^{(1)}(x; L)\right)\varphi_\ell(x; L) = E_\ell(L)\,\varphi_\ell(x; L) \tag{6}$$

for the real-valued energy wave functions φ_ℓ which describes the motion of a non-relativistic particle of mass μ along the x-axis just reproduces the spectrum (1) for the energies $E_\ell(L)$. Here we have indicated by the argument L after the semicolon that the potential $V^{(1)}$ as well as the wave functions φ_ℓ depend on the scaling parameter. Moreover, the superscript denotes the number of dimensions. However, for the sake of simplicity in notation we suppress the superscripts in the energy eigenvalues since a single or a pair of indices already suggests the number of dimensions.

The iteration algorithm to obtain $V^{(1)}$ is based on the Hellmann–Feynman theorem and is described in a previous paper [8]. In Fig. 1 we show $V^{(1)}$ together with the eigenfunctions φ_ℓ for $0 \leq \ell \leq 6$ for the case $L = 2$. No degeneracy is present in this one-dimensional problem.

In this Letter we consider a particle which moves in the x–y plane under the influence of the potential

$$V^{(2)}(x, y; L) \equiv V^{(1)}(x; L) + V^{(1)}(y; L) \tag{7}$$

shown in Fig. 2 for $L = 2$ and formed by the sum of two such potentials each of which displays the logarithmic energy spectrum (1).