

DEDICATED TO PROFESSOR IWO BIAŁYŃICKI-BIRULA ON HIS 90TH BIRTHDAY

— \diamond —

Factorization with a Logarithmic Energy Spectrum of a Central Potential

F. GLEISBERG^a AND W.P. SCHLEICH^{a,b,*}^a*Institut für Quantenphysik and Center for Integrated Quantum Science and Technology (IQST), Universität Ulm, D-89069 Ulm, Germany*^b*Hagler Institute for Advanced Study at Texas A & M University, Texas A & M AgriLife Research, Institute for Quantum Studies and Engineering (IQSE) and Department of Physics and Astronomy, Texas A & M University, College Station, Texas 77843-4242, USA*

Published: 14.06.2023

Doi: [10.12693/APhysPolA.143.S112](https://doi.org/10.12693/APhysPolA.143.S112)*e-mail: wolfgang.schleich@uni-ulm.de

We propose a method to factor numbers based on two interacting bosonic atoms in a central potential, where the single-particle spectrum depends logarithmically on the radial quantum numbers of states corresponding to zero angular momentum. Bosons initially prepared in the ground state are excited by a sinusoidally time-dependent interaction into a state characterized by quantum numbers, which represent the factors of the number encoded in the frequency of the perturbation. We also discuss the complete single-particle spectrum as well as the limitations of our method caused by decoherence.

topics: factorization, logarithmic energy spectrum, central potential, cold atoms

1. Introduction

It is well-known that the decomposition of a positive composite integer into a product of prime factors is a difficult problem in number theory since it requires *non-polynomial* time on a classical computer, which makes it attractive for cryptological applications [1]. Indeed, decoding a message encoded by the famous Rivest–Shamir–Adleman (RSA) protocol [2] requires the decomposition of a large semiprime, i.e., an integer composed by two primes, in a reasonable time. Such a decomposition can be easily prevented by choosing larger and larger semiprimes. The topic of prime factorization is intimately connected to Peter Shor because on an ideal quantum computer Shor’s factorizing algorithm [3] takes only *polynomial time* and is therefore expected to break the RSA scheme in the future.

1.1. Factorization based on a central potential with logarithmic spectrum

As an alternative method, we have studied [4–6] the factorization of integers using bosonic atoms in one- and two-dimensional potentials, both with a logarithmic energy spectrum. Our present

theoretical study represents an extension of these thoughts and is motivated by two features: (i) it is possible [7] to create and control almost any kind of potential for the center-of-mass motion of the atom using adiabatic potentials, and (ii) bosons in a spherically symmetric *parabolic* potential as well as in a spherical box provide textbook examples for the thermodynamics of the Bose–Einstein condensation [8, 9]. For this reason, in this article, we numerically construct a *central* potential with a logarithmic energy spectrum and propose a factorization algorithm.

The two bosons originally trapped in the ground state of this potential are excited by a periodic perturbation with a frequency governed by the semiprime we want to factor. At a later time, the bosons are found with a probability of about one-half in a state where the energies of the individual bosons contain the factors of the semiprime. Thus a measurement of these energies provides us with the factors we are looking for.

Many ways to experimentally implement our scheme are offered. The most promising one takes advantage of the fact that the interaction of an atom with an electromagnetic wave, which is far detuned from the atom’s resonance, experiences [10]

a potential for its center-of-mass motion determined by the spatial dependence of the light intensity. Hence, by tailoring the intensity distribution to the predetermined shape of the potential, one creates the desired spectrum. In this way, it was possible to create [11], for example, a potential whose energy eigenvalues are given by prime numbers. Obviously, in the context of factorization, the potential with an energy spectrum given by the *logarithm* of primes is of interest and was proposed in [5].

Malcolm G. Boshier at Los Alamos National Laboratory has kindly informed us [12] that he is presently pursuing our approach to factor numbers. By shaking the one-dimensional potential associated with a logarithmic energy spectrum, he and his team could already excite individual energy states as well as their coherent superposition. Energy measurement is achieved by imaging the atoms and counting the number of nodes and anti-nodes of the energy wave functions.

We emphasize that the spherical symmetry of the unperturbed potential is crucial for the protocol proposed in this article. Among the necessities to experimentally obtain symmetry of this kind is microgravity [13]. Hence, a drop tower, for example, the one in Bremen [14], a sounding rocket in space [15], or the International Space Station [16, 17] could provide such an environment.

Moreover, central to our considerations are *s*-states, i.e., the states of vanishing angular momentum. It is worthwhile mentioning that such states have also played a major role in the studies [18–20] of the unusual dynamics of free wave packets. Indeed, they display focusing or defocusing effects even in the absence of external potentials or position-dependent phase factors, and are the result of the dependence of the Laplacian in the Schrödinger equation on the number of space dimensions. This manifestation of the dimensionality of space in quantum mechanics [21] is the analogue of the violation of Huygens’s principle in electrodynamics.

1.2. Overview

This article is organized as follows. In Sect. 2 we introduce the logarithmic energy spectrum and discuss the distribution of a given energy onto two single-particle states. Moreover, we recall a *one*-dimensional potential giving rise to such a spectrum. We then solve in Sect. 3 the Schrödinger equation in *three* dimensions and show that the *s*-states, i.e., states corresponding to the zero azimuthal quantum number, suffice to determine the central potential with a logarithmic energy spectrum. Moreover, we take into account the boundary condition at the origin and demonstrate that the single-particle *s*-states exhibit an energy spectrum identical to the one introduced in Sect. 2. In Sect. 4, we define the corresponding two-particle states using the bra–ket notation.

Section 5 constitutes the main part of our article. Here we discuss the realization of our factorizing scheme by two bosonic atoms moving in the central potential determined in Sect. 3, and being excited by a time-dependent interaction into the factor state. We derive the solution of the corresponding Schrödinger equation within the rotating wave approximation and demonstrate that after measuring the single-particle energies at random times the factor state is found with a probability of about 1/2. A brief discussion of the limitations of our method completes this section. We conclude with a short summary in Sect. 6.

Central to our proposal is the fact that the energy spectrum of our central potential does not display any accidental degeneracies. For an elementary discussion of this point, we refer to Appendix.

2. Logarithmic spectrum and potential in one dimension

In the present section, we first introduce the logarithmic energy spectrum and discuss its special role in finding factors of an integer. We then turn to the distribution of the given energy onto two subsystems. This discussion constitutes the foundation for our factorization protocol. We conclude by recalling [4, 22] the potential in one space dimension that gives rise to such a spectrum.

2.1. Central idea for factorization

Our scheme is based on the logarithmic energy spectrum

$$E_k(L) \equiv \hbar\omega_0 \ln \left(\frac{k}{L} + 1 \right) \quad (1)$$

with $k = 0, 1, 2, \dots$ and $E_0(L) = 0$. Here, the constant L plays the role of a scaling parameter and $\hbar\omega_0$ is the unit of energy.

In order to find the factors of a given semiprime $N \equiv pq$, we distribute the total energy

$$E_{\text{total}}(N; L) \equiv \hbar\omega_0 \ln \left(\frac{N}{L^2} \right) \quad (2)$$

onto *two* subsystems, each with the spectrum defined by (1) according to the relation

$$E_{\text{total}}(N; L) = \hbar\omega_0 \ln \left(\frac{p}{L} \right) + \hbar\omega_0 \ln \left(\frac{q}{L} \right) \quad (3)$$

that is

$$E_{\text{total}}(N; L) = E_{p-L}(L) + E_{q-L}(L). \quad (4)$$

Since L appears in the indices of the energies in (4), it has to be an integer. No negative indices are present in (1), therefore N cannot contain the factors $q < L$ and $p < L$.

Moreover, the factor $q = L$ or $p = L$ causes the unwanted case that the total energy given by (3) may be transferred to one of the two subsystems while the other one remains in the ground state

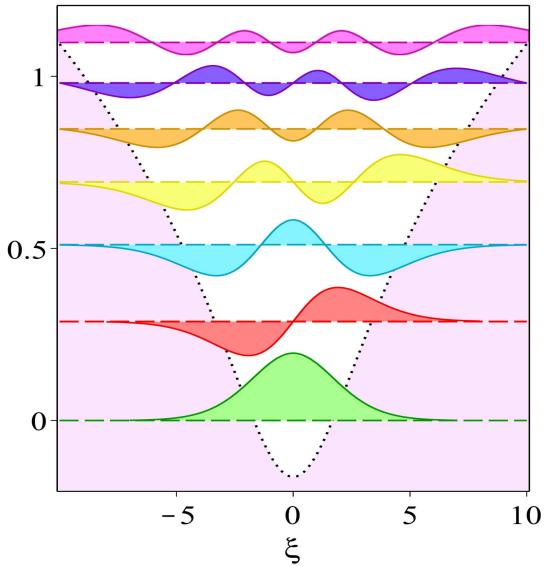


Fig. 1. The one-dimensional potential $V = V(\xi; 3)$ (dotted line) creating a logarithmic energy spectrum for the scaling parameter $L = 3$ as a function of the dimensionless coordinate $\xi \equiv \alpha x$ with $\alpha^2 \equiv \mu\omega_0/\hbar$. This potential is determined [22] numerically by an iteration algorithm based on a perturbation theory using the Hellmann–Feynman theorem, and is designed to obtain a logarithmic dependence of the energy eigenvalues $E_k(L = 3)$ on the quantum number k as given by (1). In the neighborhood of the origin, the potential is approximately harmonic whereas for large values of ξ it is logarithmic. The solid lines depict the numerically determined energy wave functions $u_k = u_k(\xi, 3)$ of the first seven states in their dependence on the dimensionless position. Both, the energies $E_k(3)$, $k = 0, 1, \dots, 6$ (dashed lines) as well as the potential $V = V(\xi; 3)$ are expressed in units of $\hbar\omega_0$.

and no factorization takes place. Hence, we have to remove the factors $2, 3, \dots, L$, which can be done by the division before we start our factorization protocols.

However, if L is chosen to be unity the trivial factorization $N = 1 \times N$ cannot be excluded. Moreover, in Sect. 3 we shall see that L has to be odd. Therefore, throughout our article, we consider the case $L \geq 3$.

The question of the uniqueness of the distribution according to (3) is easily answered because the fundamental theorem of arithmetics guarantees that the decomposition of the integer N is unique if both factors, p and q , are prime.

For our factorization protocol, the two subsystems have to be brought into a state of total energy (3), followed by a measurement of their individual energies which allows us to determine the factors p and q , as described in Sect. 5. In the remainder of our article, we shall concentrate on the factorization of semiprimes.

2.2. The inverse problem

Next, we briefly address the problem of creating such a logarithmic energy spectrum by determining the appropriate potential V in one space dimension denoted by the coordinate x . For the sake of simplicity, we assume a symmetric potential $V(x) = V(-x)$ with $-\infty < x < \infty$, where the time-independent Schrödinger equation for a particle of mass μ reads

$$\left[-\frac{\hbar^2}{2\mu} \frac{d^2}{dx^2} + V(x; L) - E_k(L) \right] u_k(x; L) = 0. \quad (5)$$

Since the eigenvalues $E_k(L)$ depend on the scaling parameter L , the potential $V = V(x; L)$ and the eigenfunctions $u_k = u_k(x; L)$ must also display the same dependence.

Under standard circumstances, the potential $V = V(x; L)$ is given and the eigenvalues must be found. However, now the energy spectrum is prescribed, and we have to determine the potential $V = V(x; L)$ from the Hellmann–Feynman theorem and the iteration algorithm described in the previous article [22]. In Fig. 1 we show the so-obtained potential $V = V(x; L = 3)$ together with the eigenfunctions $u_k = u_k(x; L = 3)$ and energy eigenvalues $E_k(L = 3)$ for $0 \leq k \leq 6$.

We conclude by noting that in [22], we constructed this potential with a logarithmic energy spectrum to obtain wave packets whose auto-correlation function yields the Dirichlet representation of the Riemann zeta function [23]. However, it has also become crucial for our factorization proposals [4–6] in one and two dimensions and plays a crucial role in the present article when we propose an algorithm for three dimensions.

3. Logarithmic energy spectrum in three dimensions

In the present section, we realize the logarithmic spectrum (1) for a particle of mass μ moving in three space dimensions in a central potential $V = V(r)$ that we shall determine. For this purpose, we start from the time-independent Schrödinger equation in three dimensions and concentrate on the radial wave functions. Due to the vanishing boundary condition at the origin, the corresponding eigenfunctions are the odd ones of the symmetric one-dimensional problem in Sect. 2. We conclude by discussing the resulting energy spectrum.

3.1. From three dimensions to one dimension

We start from the Schrödinger equation

$$\left[-\frac{\hbar^2}{2\mu} \Delta + V(r) - E \right] \psi(r, \theta, \varphi) = 0, \quad (6)$$

in spherical coordinates r , θ and φ and employ the ansatz

$$\psi_{j,\ell,m}(r, \theta, \varphi) \equiv R_{j,\ell}(r) Y_\ell^m(\theta, \varphi) \quad (7)$$

for the energy eigenfunctions $\psi_{j,\ell,m}$ that are simultaneous eigenfunctions of the Hamiltonian \hat{H} , the square of the angular momentum \hat{L}^2 and its z -component \hat{L}_z forming a complete set of commuting operators with the eigenvalues $E_{j,\ell}$, $\hbar^2 \ell(\ell+1)$ and $\hbar m$, respectively. The radial quantum number j , as well as the azimuthal quantum number ℓ , takes value $0, 1, 2, \dots$ while the magnetic quantum number m assumes $2\ell+1$ values given by $-\ell \dots \ell$. The functions $Y_\ell^m = Y_\ell^m(\theta, \varphi)$ are the spherical harmonics.

Since the solution of (6) can be found in standard textbooks on quantum mechanics, we jump directly to the radial equation

$$\left[-\frac{\hbar^2}{2\mu r} \frac{d^2}{dr^2} r + \frac{\hbar^2 \ell(\ell+1)}{2\mu r^2} + V(r) - E_{j,\ell} \right] R_{j,\ell}(r) = 0 \quad (8)$$

valid in the region $r \geq 0$ with the condition that $R_{j,\ell} = R_{j,\ell}(r)$ has to be square integrable and finite at the origin $r = 0$.

We consider s -states defined by $\ell = 0$ and set

$$R_{j,0}(r) \equiv \frac{v_{j,0}(r)}{r} \quad (9)$$

with the boundary condition

$$v_{j,0}(0) = 0 \quad (10)$$

at the origin.

3.2. Potential

For the sake of simplicity in the notation, we now suppress the index $\ell = 0$ for the time being. In Sect. 2, we obtained the potential $V = V(x, L)$ and the functions $u_k = u_k(x, L)$ for one space dimension associated with a logarithmic energy spectrum. The three-dimensional potential $V^{(3d)} = V^{(3d)}(r; L)$ as well as the eigenfunctions $v_j(r; L)$ follow by replacing the coordinate x by r in both, where now only the region $r \geq 0$ is considered that is

$$V^{(3d)}(r, L) \equiv V(x = r, L). \quad (11)$$

However, only *odd* solutions $u_k = u_k(x; L)$ of (5) with $k \equiv 2j+1$ can satisfy the boundary condition (10). Therefore, the energies $E_k(L)$ as well as the eigenfunctions $u_k(x; L)$ with *even* index k , which are present in one dimension in (5), do not appear anymore in three dimensions.

Figure 2 shows the potential $V^{(3d)} = V^{(3d)}(r; L)$ for the position vector \mathbf{r} in the x - y plane. We emphasize that states with quantum numbers $\ell > 0$ are not needed to determine V .

3.3. Energy eigenvalues and wave functions of s -states

We now show that the remaining spectrum $E_{2j+1}(L)$ does indeed have the form of (1) and therefore guarantees the validity of the results from

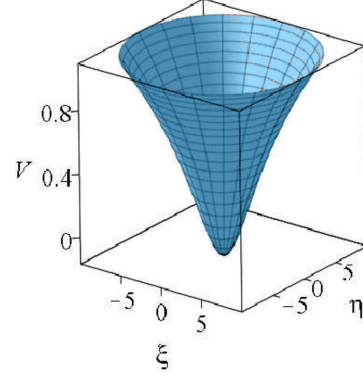


Fig. 2. Three-dimensional potential $V^{(3d)} = V^{(3d)}(r; L = 3)$ in units of $\hbar\omega_0$ creating the logarithmic energy spectrum (13) with the scaling parameter $K = 2$ as a function of the dimensionless coordinates $\xi \equiv \alpha x$ and $\eta \equiv \alpha y$, represented in the plane $z = 0$.

Sect. 2 which are essential for our factorization procedure. For this purpose, we shift the energies

$$E_{2j+1}(L) = \hbar\omega_0 \ln \left(\frac{2j+1}{L} + 1 \right) \quad (12)$$

with $j = 0, 1, 2, 3, \dots$ by a constant amount $\delta E \equiv -\hbar\omega_0 \ln(1/L + 1)$ leading us to new spectrum

$$E_j^{(3d)}(K) = \hbar\omega_0 \ln \left(\frac{j}{K} + 1 \right), \quad (13)$$

which is identical to the single-particle spectrum (1) except that L has to be replaced by the new scaling parameter

$$K \equiv \frac{L+1}{2}. \quad (14)$$

For K to be a positive integer, L has to be odd. All the statements made in Sect. 2 referring to the scaling length L remain valid here provided L is replaced by K .

The eigenfunctions $v_j = v_j(r; K)$ corresponding to $E_j^{(3d)}(K)$ read

$$v_j(r; K) \equiv u_{2j+1}(r; L). \quad (15)$$

Figure 3 shows the radial wave functions

$$R_j(r) \equiv \frac{v_j(r; K)}{r} \quad (16)$$

for indices $j = 0, \dots, 5$ together with the potential $V^{(3d)} = V^{(3d)}(r; K = 2)$ and the energy levels $E_j^{(3d)}(K = 2)$ given by (13).

4. Two-particle bosonic states

So far we have concentrated on a single particle exposed to a central potential giving rise to the logarithmic energy spectrum of (1). We now address the two-particle situation which is central to our factorization scheme.

To simplify the notation we turn to the bra-ket formalism and the time-independent single-particle Schrödinger equation for s -states takes the form ($j = 0, 1, 2, \dots$)

$$\hat{H}(K) |j\rangle = E_j^{(3d)}(K) |j\rangle, \quad (17)$$

where we have suppressed again the quantum numbers $\ell = m = 0$. The Hamiltonian $\hat{H}(K)$ is characterized by the parameter K defined by (14).

The corresponding Schrödinger equation for the two *non-interacting* bosons denoted by 1 and 2 reads

$$\left(\hat{H}_{1,2}(K) - E_{m,n}(K)\right) |m, n\rangle_B = 0, \quad (18)$$

where

$$\hat{H}_{1,2}(K) \equiv \hat{H}_1(K) + \hat{H}_2(K) \quad (19)$$

is the Hamiltonian of both bosons with total energy

$$E_{m,n}(K) \equiv E_m^{(3d)}(K) + E_n^{(3d)}(K), \quad (20)$$

in accordance with (13) and (14).

We note that bosonic two-particle states are defined by

$$|m, n\rangle_B \equiv \frac{1}{\sqrt{2}}(|m, n\rangle + |n, m\rangle), \quad (21)$$

where $|m, m\rangle_B \equiv |m, m\rangle$.

If two identical non-interacting bosons are in a state with energy

$$\hbar\omega_0 \ln\left(\frac{N}{K^2}\right) = E_{p-K}^{(3d)} + E_{q-K}^{(3d)}, \quad (22)$$

where $N \equiv pq$ is semi-prime, then according to (4) and (13) the bosons are in the factor state $|p-K, q-K\rangle_B$. A measurement of the energy of one of the bosons can only result in $\hbar\omega_0 \ln(p/K)$ or $\hbar\omega_0 \ln(q/K)$ and immediately yields the prime factors p and q , respectively.

5. Factorization algorithm

The present section contains the main results of our article. Here we propose and analyze the realization of the factorization protocol of Sect. 2 by two interacting identical bosons placed in the central potential shown in Fig. 2, with the single-particle spectrum given by (13).

Starting from the corresponding Schrödinger equation, we first derive the equations of motion for the probability amplitudes of the ground state and the relevant excited states. Here we keep all three quantum numbers and denote them by $\mathbf{k} = (j, \ell, m)$. To simplify the notation further, in the remainder of the article, we suppress the scaling parameter K as well as the subscript B and the superscript 3d.

We then derive an explicit expression for the matrix element of the Fermi point interaction [24, 25] and simplify the equations of motion for the resulting probability amplitude with the help of the rotating wave approximation (RWA) [26, 27]. The approximation reduces the equations of motion to

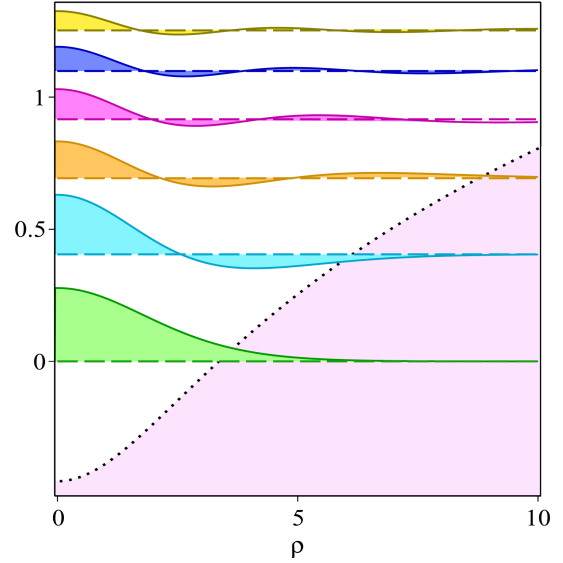


Fig. 3. Central potential $V^{(3d)} = V^{(3d)}(\rho; K = 2)$ represented by a dotted line creating the logarithmic energy spectrum $E_j^{(3d)}(K = 2)$ of (13) in units of $\hbar\omega_0$ as a function of the dimensionless radius $\rho \equiv \alpha r$ together with the corresponding radial functions $R_j = R_j(\rho)$ defined by (16) of the first six states in their dependence on ρ . We shifted the energies to ensure that the ground state has vanishing energy.

a two-level Rabi problem involving the ground state and the factor state. This insight allows us to estimate the probability of success of our factorization scheme. Moreover, we briefly discuss the limitations of our method.

5.1. Coupled set of equations

We prepare two bosons in the ground state $|\mathbf{0}, \mathbf{0}\rangle$ and expose them at $t = 0$ to the perturbation

$$\delta V(\mathbf{r}_1, \mathbf{r}_2; t) \equiv \gamma \sin(\omega_{\text{ext}} t) w(\mathbf{r}_1, \mathbf{r}_2) \quad (23)$$

where γ is a constant and the frequency ω_{ext} is chosen later in a way suitable for the factorization procedure. Moreover, the interaction term w contains the coordinates \mathbf{r}_1 and \mathbf{r}_2 of both particles.

The time evolution of the two-particle state $|\Psi(t)\rangle$ is now governed by the Schrödinger equation

$$i\hbar \frac{d}{dt} |\Psi(t)\rangle = (\hat{H}_{1,2} + \delta V(t)) |\Psi(t)\rangle \quad (24)$$

in three dimensions with the unperturbed stationary states

$$\hat{H}_{1,2} |\mathbf{k}_1, \mathbf{k}_2\rangle = E_{\mathbf{k}_1, \mathbf{k}_2} |\mathbf{k}_1, \mathbf{k}_2\rangle. \quad (25)$$

When we substitute the expansion

$$|\Psi(t)\rangle = \sum_{\mathbf{k}_1, \mathbf{k}_2} b_{\mathbf{k}_1, \mathbf{k}_2}(t) e^{-iE_{\mathbf{k}_1, \mathbf{k}_2} t/\hbar} |\mathbf{k}_1, \mathbf{k}_2\rangle \quad (26)$$

of $|\Psi(t)\rangle$ by the two-particle eigenstates $|\mathbf{k}_1, \mathbf{k}_2\rangle$ of the unperturbed Hamiltonian $\hat{H}_{1,2}$ into (24), we arrive at the coupled system

$$i\hbar \dot{b}_{\mathbf{k}_1, \mathbf{k}_2}(t) = \gamma \sin(\omega_{\text{ext}} t) \sum_{\mathbf{k}'_1, \mathbf{k}'_2} e^{i(E_{\mathbf{k}_1, \mathbf{k}_2} - E_{\mathbf{k}'_1, \mathbf{k}'_2})t/\hbar} W_{\mathbf{k}_1, \mathbf{k}_2; \mathbf{k}'_1, \mathbf{k}'_2} b_{\mathbf{k}'_1, \mathbf{k}'_2}(t) \quad (27)$$

with the initial conditions $b_{\mathbf{k}_1, \mathbf{k}_2}(0) = 1$ for $j_1 + j_2 + \ell_1 + \ell_2 = 0$, and $b_{\mathbf{k}_1, \mathbf{k}_2}(0) = 0$ otherwise, which has to be solved for the probability amplitudes $b_{\mathbf{k}_1, \mathbf{k}_2}(t)$.

We conclude by emphasizing that the eigenstates $|\mathbf{k}_1, \mathbf{k}_2\rangle$ of $\hat{H}_{1,2}$, the amplitudes $b_{\mathbf{k}_1, \mathbf{k}_2}(t)$, and the matrix elements

$$W_{\mathbf{k}_1, \mathbf{k}_2; \mathbf{k}'_1, \mathbf{k}'_2} \equiv \langle \mathbf{k}_1, \mathbf{k}_2 | w(\hat{\mathbf{r}}_1, \hat{\mathbf{r}}_2) | \mathbf{k}'_1, \mathbf{k}'_2 \rangle \quad (28)$$

are ‘‘bosonic’’ ones in the sense of (21) and are built out of the eigenstates $|\mathbf{k}_1, \mathbf{k}_2\rangle$ of $\hat{H}_{1,2}$ and the spacial part w of the perturbation $\delta\hat{V}$ defined by (23). Moreover, in the summation in (26) and (27), the same states must not be counted twice.

5.2. Matrix elements for the contact interaction

Next we derive an explicit expression for the matrix element $W_{\mathbf{k}_1, \mathbf{k}_2; \mathbf{k}'_1, \mathbf{k}'_2}$ (28), assuming the contact interaction

$$w(\mathbf{r}_1, \mathbf{r}_2) \equiv \delta^{(3)}(\mathbf{r}_1 - \mathbf{r}_2). \quad (29)$$

between two particles, providing us with the selection rules of the transitions from the ground state.

Needless to say, we are well aware that we should use the *regularized* delta function [24, 25] rather than the delta function of (29) for the zero-range potential. However, in order to bring out most clearly the central points of our factorization algorithm, we resort to the elementary version of (29) of the contact potential and postpone the complete analysis to a future publication.

Due to the delta function in w , the matrix element (28) reduces in position space to

$$W_{\mathbf{k}_1, \mathbf{k}_2; \mathbf{k}'_1, \mathbf{k}'_2} \equiv \int d^3r \psi_{\mathbf{k}_1}^*(\mathbf{r}) \psi_{\mathbf{k}_2}^*(\mathbf{r}) \psi_{\mathbf{k}'_1}(\mathbf{r}) \psi_{\mathbf{k}'_2}(\mathbf{r}). \quad (30)$$

$$i\hbar \dot{b}_{0,0;0,0}(t) = \gamma \sin(\omega_{\text{ext}} t) \sum_{j_1, j_2, \ell} e^{-i(E_{j_1, \ell} + E_{j_2, \ell})t/\hbar} W_{0,0;0,0; j_1, \ell, j_2, \ell} b_{j_1, \ell; j_2, \ell}(t) \quad (34)$$

with the matrix element (31) and vanishing energy of the ground state of the two bosons.

The external frequency ω_{ext} is chosen such that the energy $\hbar\omega_{\text{ext}}$ is identical to the sum

Having in mind that we start our algorithm at time $t=0$ with the two particles in the ground state $|\mathbf{0}, \mathbf{0}\rangle$, we consider the matrix elements $W_{\mathbf{0}, \mathbf{0}; \mathbf{k}_1, \mathbf{k}_2}$ for a transition into the excited state $|\mathbf{k}_1, \mathbf{k}_2\rangle$. With the product ansatz (7) for $\psi_{\mathbf{k}}$, we therefore arrive at the expression

$$W_{\mathbf{0}, \mathbf{0}; \mathbf{k}_1, \mathbf{k}_2} = \frac{1}{4\pi} \int_0^\infty dr r^2 R_{0,0}(r)^2 R_{j_1, \ell_1}(r) \times R_{j_2, \ell_2}(r) \delta_{\ell_1, \ell_2} \delta_{m_1 + m_2, 0}. \quad (31)$$

Here we have applied the well-known orthonormality relation

$$\int d\Omega Y_{\ell_1}^{m_1*}(\theta, \varphi) Y_{\ell_2}^{m_2}(\theta, \varphi) = \delta_{\ell_1, \ell_2} \delta_{m_1, m_2} \quad (32)$$

of the spherical harmonics and the identity

$$Y_\ell^{m*}(\theta, \varphi) = Y_\ell^{-m}(\theta, \varphi) \quad (33)$$

for their complex conjugate together with $Y_0^0 \equiv 1/\sqrt{4\pi}$.

5.3. Encoding the number to be factored and rotating wave approximation

We now employ the expression (31) for the matrix element $W_{\mathbf{0}, \mathbf{0}; \mathbf{k}_1, \mathbf{k}_2}$ to simplify the system of coupled equations (27) considerably. For this purpose, we set the two magnetic quantum numbers $m_1 = m_2 = 0$ and omit them henceforth. This assumption will be justified by the calculation below. The single-particle state is now only characterized by *two* quantum numbers j and ℓ .

Thus we study the set of equations

$$E_{p-K, 0; q-k, 0} = E_{p-K, 0} + E_{q-k, 0} = \hbar\omega_0 \ln\left(\frac{N}{K^2}\right) \quad (35)$$

of the energies of the factor states, and is determined by the number $N = pq$ to be factored.

Next, we address the product

$$\mathcal{E}(t) \equiv \frac{1}{2i} \left(e^{i(E_{p-K, 0} + E_{q-K, 0})t/\hbar} - e^{-i(E_{p-K, 0} + E_{q-K, 0})t/\hbar} \right) e^{-i(E_{j_1, \ell} + E_{j_2, \ell})t/\hbar} \quad (36)$$

of time-dependent factors, which appears on the right-hand side of (34) when we decompose the sine function into the difference of two phase factors.

The essence of RWA, when applied to (34), is to retain only terms with constant coefficients on the right-hand side and to neglect all oscillating terms. Indeed, when we assume that $p \geq q$, only the term with $j_1 \equiv p-K$, $j_2 \equiv q-K$, and $\ell = 0$ survives, providing us with the contribution $(2i)^{-1}$.

The Appendix discusses the possibility of accidental degeneracy in the logarithmic single-particle spectrum $E_{j,\ell}$ given by (1), the absence of which is confirmed therein. None of the terms with $\ell \geq 1$ can therefore lead to additional constant terms in (36).

Within RWA, (34) reduces to the equation

$$i\hbar \dot{b}_{0,0}(t) = \frac{\gamma}{2i} W_{0,0;p-K,q-K} b_{p-K,q-K}(t), \quad (37)$$

where the index $\ell = 0$ is present in the matrix element, and in the probability amplitudes it is omitted here for convenience.

We derive a second equation by selecting the term with $j_1 \equiv p-K$ and $j_2 \equiv q-K$ from (27) and proceeding as before we arrive at the equation of motion

$$i\hbar \dot{b}_{p-K,q-K}(t) = -\frac{\gamma}{2i} W_{p-K,q-K;0,0} b_{0,0}(t). \quad (38)$$

of the unperturbed s -states.

5.4. Factor state and its probability

We note that (37) and (38) characterize the dynamics of a two-boson system driven by the periodic perturbation (23) with energy (35). Together with the initial conditions $b_{0,0}(0) \equiv 1$ and $b_{p-K,q-K}(0) \equiv 0$ as well as the symmetry relation

$$W_{m,n;0,0} = W_{0,0;m,n}, \quad (39)$$

the resulting probability amplitude for the ground state reads

$$b_{0,0}(t) = \cos(\Omega t), \quad (40)$$

whereas for the factor state we find

$$b_{p-K,q-K}(t) = \sin(\Omega t). \quad (41)$$

The Rabi frequency

$$\Omega \equiv \frac{\gamma}{2\hbar} W_{0,0;p-K,q-K} \quad (42)$$

is proportional to the interaction matrix element of (31).

In Sects. 2 and 4 we have shown that if the bosons are in the factor state $|p-K, q-K\rangle$ they have a two-particle energy $\hbar\omega_0 \ln(N/K^2)$ given by (22) with $N = pq$. As mentioned there, the factors p or q are determined by a measurement of the single-particle energies (3), and the factorization protocol has ended successfully.

At the time t , the system can be found with probability $|b_{p-K,q-K}(t)|^2$ in the factor state, and at the time equal to an odd multiple of $\pi/(2\Omega)$, it is there with 100% certainty. Unfortunately, the Rabi

frequency Ω is not known. Instead, we content ourselves with measuring at a time chosen randomly from a time interval $[0, T]$ much larger than π/Ω . According to (41), the probability to find the factor state is about one-half. Then the measurement of the single-particle energy gives one of the factors while the other one follows from division.

An estimate for a time of measurement by making a guess for the factors p and q and so determining the Rabi frequency (42) was presented in a previous article [4].

5.5. Limitations

In the present section, we briefly address the obstacles that prevent our protocol from factoring larger and larger semiprimes, and in particular, we derive the condition for the largest number N we can factor. Here we address especially limitations due to decoherence.

According to [26], there is a high probability for a *periodic* transition into the factor state as long as the difference between the energies of this state and of the next off-resonant state is larger than the energy $\hbar\Omega$ of the Rabi oscillation. This condition translates into the requirement

$$\hbar\omega_0 \left| \ln\left(\frac{N \pm 1}{K^2}\right) - \ln\left(\frac{N}{K^2}\right) \right| \approx \frac{\hbar\omega_0}{N} \gg \hbar\Omega. \quad (43)$$

Since the Rabi frequency Ω defined by (42) is proportional to the strength γ of the perturbation (23), the inequality (43) can easily be satisfied by choosing γ as small as needed.

Unfortunately, the second condition arises from the fact that we randomly choose the time of measuring the energies of the two bosons from the interval $[0, T]$. To find the factor state with a probability of approximately 1/2, the interval length T has to fulfill the condition $\Omega T \gg 1$.

On the other hand, the system has to be *free of decoherence* during the time interval $T < T_{\text{dec}}$ leading to the two inequalities for the Rabi frequency

$$\Omega \gg \frac{1}{T_{\text{dec}}} \quad (44)$$

and

$$\Omega \ll \frac{\omega_0}{N}. \quad (45)$$

Our aim is now to find an upper limit for the number N to be factored. In [4] and [6] for different experimental situations and models for the spatial part of the interaction, we have found an approximate N -dependence

$$W_{0,0;p-K,q-K} \propto N^{-1/2} \quad (46)$$

of the transition matrix element.

Due to (42) the same scaling holds true, of course, for the Rabi frequency Ω , and the semiprime N to be factored therefore has the upper limit

$$N < \min \left(\left[\frac{\gamma T_{\text{dec}}}{\hbar} \right]^2, \left[\frac{\hbar\omega_0}{\gamma} \right]^2 \right). \quad (47)$$

Assuming that according to (23) the interaction strength γ can be chosen at will, this relation shows that the crucial limiting factor for the magnitude of N is the decoherence time T_{dec} .

6. Conclusions

In the present article, we have proposed a method to find the factors of a semiprime N based on the quantum dynamics of two identical bosonic atoms moving in a spherically symmetric trap whose s -states exhibit a logarithmic single-particle spectrum.

In the first part of our work, we have determined the central potential, which displays such an unusual spectrum. We started by numerically calculating the one-dimensional potential from a logarithmic single-particle spectrum. Taking advantage of the close relationship between three-dimensional spherically symmetric and one-dimensional problems, the central potential was easily found. As expected, it has an energy spectrum with the logarithmic s -wave part, but with a scaling length different from the one in the one-dimensional spectrum.

In the second part, we have attacked the problem of how to force the bosons into the factor state. For this purpose, we excite them from their ground state by a periodic time-dependent contact interaction with a frequency determined by the number N to be factored. To exclude transitions between non- s states, we have discussed *in extenso* the absence of degeneracies.

Then we showed within the framework of the rotating wave approximation that the bosons perform a Rabi oscillation between the ground state and the factor state. The latter emerges with a probability of about one-half when the energies of the bosons are measured at a randomly chosen time. These energies provide us with the factors of N , and our factorization protocol has ended successfully.

Since holographic methods allow us to create almost arbitrary potentials for the center-of-mass motion of atoms and detect them by their fluorescence, an experimental implementation of our factorization scheme is within reach. Indeed, the group of Donatella Cassetari has already used this technique to experimentally realize a potential whose energy eigenvalues are given by the lowest prime numbers. Moreover, the team of Malcolm Boshier even implemented a one-dimensional potential for the logarithmic energy spectrum and observed well-defined excitations of atoms from the ground state to individual energy eigenstates of this potential. Unfortunately, the demonstration of our factorization scheme is still awaiting.

Hence, today's technology already allows us to factor small numbers using this technique. However, three phenomena make the straight-forward application to large composite integers impossible:

(i) decoherence during Rabi oscillations, (ii) scaling of separation between neighboring energy levels with an inverse of the quantum number n requiring increasing accuracy in determining the levels, and (iii) the non-vanishing time for the transition of the two atoms from the ground state to the factor states given by the inverse of the Rabi frequency, which grows with the square root of the number N to be factored.

It is interesting that the same scaling appears in the naive approach towards factoring just trying out all the primes below to the square root of N . Hence, it appears that the RSA scheme is saved by the fact that quantum transitions are not quantum jumps, but rather follow the continuous dynamics given by the Rabi oscillation as dictated by the Schrödinger equation.

Acknowledgments

His classic textbooks *Quantum Electrodynamics* and *Theory of Quanta* co-authored by his wife Zofia and by Marek Cieplak and Jerzy Kamiński, respectively, his seminal work on field quantization without mode functions based on the Wheeler functional, as well as his deep insights into the wave function of the photon, and last not least his entropic uncertainty relations represent only a few of the many outstanding scientific achievements of Professor Iwo Białynicki-Birula.

One of us (W.P.S.) met Iwo exactly 40 years ago at a NATO summer school in Boulder, Colorado, organized by Asim Barut. W.P.S. was immediately impressed by Iwo's unique ability to catch instantly the central point of an argument, his penetrating questions and his love for a good scientific fight, but also by his incredible friendliness. It was therefore only logical that 10 years later Iwo came as the first Humboldt Awardee to the still young *Institute for Quantum Physics at Ulm University*. Over the years we have had a wonderful and extremely productive collaboration, and not only did *we* become close friends but also our families.

We dedicate our article addressing the interface of quantum physics and number theory to our great teacher and fatherly friend Iwo on the occasion of his 90th birthday. We know that this field is dear to his heart, and hope that our little birthday present may find his interest and trigger a discussion leading to a deeper understanding.

Happy Birthday Iwo and many more healthy years filled with fun with physics!

We thank M.G. Boshier, M.A. Efremov and M. Freyberger for stimulating discussions on this topic and M.E.N. Tschaffon for technical assistance. W.P.S. is grateful to the Hagler Institute for Advanced Study at Texas A&M University for a Faculty Fellowship and to Texas A&M University AgriLife Research for its support. The research of the IQST is financially supported by the Ministry of Science, Research and Arts, Baden-Württemberg.

Appendix A: Absence of accidental degeneracy in the logarithmic spectrum

The energy spectrum of *any* central potential exhibits the familiar $(2\ell + 1)$ -fold *essential* degeneracy as the energy levels $E_{j,\ell}$ do not depend on the magnetic quantum number m . It has been proven long ago [28] that the only potentials that show *accidental* degeneracy are the Coulomb potential and the harmonic oscillator. This fact is a consequence of the existence of a conserved quantity [29], which does not commute with any member of the complete system of commuting operators of the problem. In the Coulomb case, this constant of the motion is the well-known Runge–Lenz vector [30, 31], whereas, for the harmonic oscillator, we shall discuss it below. Since our central potential leading to the logarithmic energy spectrum is none of the above, accidental degeneracy must be absent. We shall now study this problem in more detail.

A.1: Non-closed trajectory of a classical particle

We recall that the trajectories of a classical particle in the harmonic oscillator as well as in the Coulomb potential are closed, the latter only for negative energies. Following the textbook [32], we calculate the trajectory of a mass μ , energy E , and angular momentum J oscillating in the effective potential

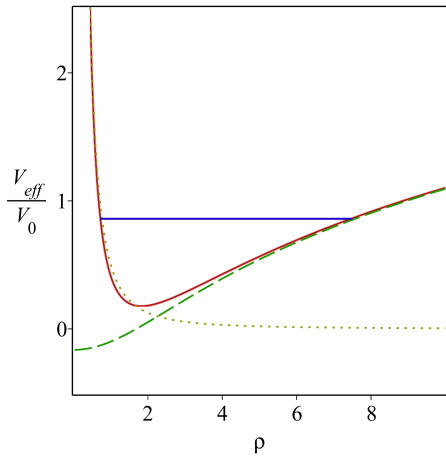


Fig. 4. Scaled effective potential V_{eff} (solid line) formed by the angular momentum barrier (dotted curve) and the potential $V^{(3d)} = V^{(3d)}(r; K = 2)$ (dashed line) which in the quantum case creates the logarithmic energy spectrum given by (13) for the scaling parameter $K = 2$ defined by (14), as a function of the dimensionless radius $\rho \equiv \alpha_{\text{cl}} r$ with $\alpha_{\text{cl}} \equiv (\mu V_0 / J^2)^{1/2}$. The horizontal line denotes the energy $E = 0.86 V_0$ of the radial coordinate $r = r(t)$ of a classical particle moving *periodically* between the left and right turning point. The angle $\theta = \theta(t)$ is *not* periodic, as is the orbit $r = r(\theta)$ shown in Fig. 5.

$$V_{\text{eff}}(r) \equiv \frac{J^2}{2\mu r^2} + V^{(3d)}(r, K) \quad (48)$$

with energy $E = 0.86 V_0$ periodically between the two turning points depicted in Fig. 4.

In Fig. 5 we display five periods of the trajectory $r = r(\theta)$. It is evident that the orbit of the particle precesses around the center of force and does not close, thus indicating the absence of accidental degeneracy.

A.2: Energy spectrum

The most direct way to check for degeneracy is to calculate the energies $E_{j,\ell}$ for the potential under consideration with radial and azimuthal quantum numbers j and ℓ , respectively. If two or more of energies with different indices are equal, degeneracy is present.

Before we get to our potential, we recall the situation for a three-dimensional isotropic harmonic oscillator where the lowest energy levels are displayed in Fig. 6. Indeed, here the energies $E_{j,\ell}$ depend on the combination of both indices j and ℓ on the principal quantum number $n = 2j + \ell$ leading to the degeneracy [33] of levels $E_n = \hbar\omega(n + 3/2)$ demonstrated by the levels with $n = 2, 3, 4$. If the x - and y -axis are oriented along the symmetry axes of the elliptic orbit of the oscillator, then the additional integral of the motion reduces [34] to the scalar function $E_x - E_y$, i.e., a difference between the energies of the motion projections onto the x - and y -axis, respectively.

For our central potential $V^{(3d)} = V^{(3d)}(r, K)$, defined by (11), leading to the logarithmic energy spectrum $E_{j,\ell}(K)$ given by (13), we numerically

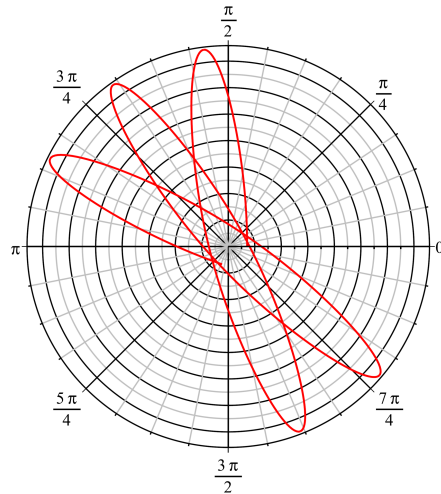


Fig. 5. Trajectory $r = r(\theta)$ of a classical particle with mass μ and energy $E = 0.86 V_0$ moving in the effective potential shown in Fig. 4. The motion starts from an inner turning point at the angle $\theta = 0$. After having covered five periods it reaches again the inner turning point, but now at the angle $\theta \approx 11\pi/8$.

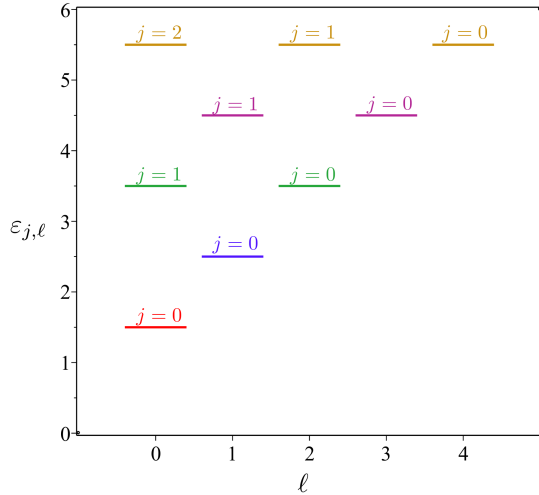


Fig. 6. Lowest dimensionless energies $\varepsilon_{j,\ell} \equiv E_{j,\ell}/(\hbar\omega)$ of an isotropic three-dimensional harmonic oscillator. The levels with the energies $E_n = \hbar\omega(n+3/2)$ show degeneracy as the principal quantum number $n = 2j + \ell$ depends on both the radial quantum number j and the azimuthal quantum number ℓ . For example, the level $n = 2$ is doubly degenerate for pairs of quantum numbers $j = 1, \ell = 0$ and $j = 0, \ell = 2$ leading to the same energy.

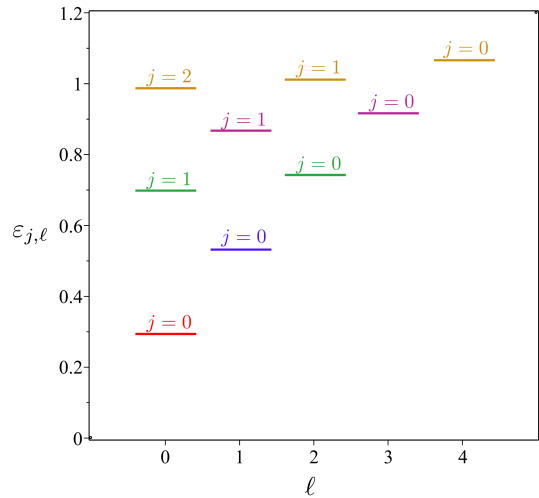


Fig. 7. Scaled energies of a particle with mass μ moving in a three-dimensional potential, leading to a spectrum where the s -state part is given by (13) and the scaling parameter $K = 2$ by (14). Each energy level is characterized by *two* quantum numbers j and ℓ . No principal quantum number can be identified and evidently, no accidental degeneracy is taking place.

solved the radial wave equation (8) and display the lowest energy levels in Fig. 7. At first sight, the scheme resembles that of the harmonic oscillator. However, closer inspection reveals that the levels, which for the harmonic oscillator were degenerate, now differ slightly. We conjecture that higher energy levels behave similarly and that no accidental

degeneracy occurs. We emphasize once more that the $(2\ell + 1)$ -fold *essential* degeneracy with respect to the magnetic quantum number m is caused by the central potential.

References

- [1] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford 1979.
- [2] R.L. Rivest, A. Shamir, L. Adleman, *Commun. ACM* **21**, 120 (1978).
- [3] P.W. Shor, in: *Proc. 35th Annual Symposium on Foundations of Computer Science*, IEEE, 1994 p. 124.
- [4] F. Gleisberg, R. Mack, K. Vogel, W.P. Schleich, *New J. Phys.* **15**, 023037 (2013).
- [5] F. Gleisberg, F. Di Pumpo, G. Wolff, W.P. Schleich, *J. Phys. B* **51**, 035009 (2018).
- [6] F. Gleisberg, M. Volpp, W.P. Schleich, *Phys. Lett. A* **379**, 2556 (2015).
- [7] B.M. Garraway, H. Perrin, *J. Phys. B* **49**, 172001 (2016).
- [8] C.J. Pethick, H. Smith, *Bose-Einstein Condensation in Dilute Gases*, Cambridge University Press, Cambridge 2008.
- [9] S.J. Bereta, L. Madeira, V.S. Bagnato, M.A. Caracanhas, *Am. J. Phys.* **87**, 924 (2019).
- [10] R. Grimm, M. Weidemüller, Y.B. Ovchinnikov, *Adv. Atom. Mol. Opt. Phys.* **42**, 95 (2000).
- [11] D. Cassettari, G. Mussardo, A. Trombettoni, *PNAS Nexus* **2**, 1 (2022).
- [12] M.G. Boshier, private communication, October 2022; M.G. Boshier, “Sensing and Signal Processing with trapped BECs”, talk at the conference *Physics of Quantum Electronics (PQE)*, Snowbird (UT) 2023.
- [13] R.A. Carollo, D.C. Aveline, B. Rhyno, S. Vishveshwara, C. Lannert, J.D. Murphree, E.R. Elliott, J.R. Williams, R.J. Thompson, N. Lundblad, *Nature* **606**, 281 (2022).
- [14] T. van Zoest, N. Gaaloul, Y. Singh et al., *Science* **328**, 1540 (2010).
- [15] D. Becker, M.D. Lachmann, S.T. Seidel et al., *Nature* **562**, 391 (2018).
- [16] D.C. Aveline, J.R. Williams, E.R. Elliott, C. Dutenhoffer, J.R. Kellogg, J.M. Kohel, N.E. Lay, K. Oudrhiri, R.F. Shotwell, N. Yu, R.J. Thompson, *Nature* **582**, 193 (2020).

- [17] N. Gaaloul, M. Meister, R. Corgier, A. Pichery, P. Boegel, W. Herr, H. Ahlers, E. Charron, J.R. Williams, R.J. Thompson, W.P. Schleich, E.M. Rasel, N.P. Bigelow, *Nat. Commun.* **13**, 7889 (2022).
- [18] I. Białyński-Birula, M.A. Cirone, J.P. Dahl, M. Fedorov, W.P. Schleich, *Phys. Rev. Lett.* **89**, 060404 (2002).
- [19] I. Białyński-Birula, M.A. Cirone, J.P. Dahl, R.F. O’Connell, W.P. Schleich, *J. Opt. B* **4**, S393 (2002).
- [20] I. Białyński-Birula, M.A. Cirone, J.P. Dahl, T.H. Seligman, F. Straub, W.P. Schleich, *Fortschritte der Phys.* **50**, 599 (2002).
- [21] M.A. Cirone, J.P. Dahl, M. Fedorov, D. Greenberger, W.P. Schleich, *J. Phys. B* **35**, 191 (2001).
- [22] R. Mack, J.P. Dahl, H. Moya-Cessa, W.T. Strunz, R. Walser, W.P. Schleich, *Phys. Rev. A* **82**, 032119 (2010).
- [23] J. Twamley, G. Milburn, *New J. Phys.* **8**, 328 (2006).
- [24] K. Huang, C.N. Yang, *Phys. Rev.* **105**, 767 (1957).
- [25] Y.N. Demkov, V.N. Ostrovskii, *Zero-range Potentials and their Applications in Atomic Physics*, Plenum Press, New York 1988.
- [26] W.P. Schleich, *Quantum Optics in Phase Space*, VCH-Wiley, Weinheim 2001.
- [27] M.O. Scully, M.S. Zubairy, *Quantum Optics*, Cambridge University Press, Cambridge 1997.
- [28] J. Bertrand, *CR Acad. Sci* **77**, 849 (1873).
- [29] L.D. Landau, E.M. Lifshitz, *Quantum Mechanics: Non-Relativistic Theory*, Vol. 3, Pergamon Press, Oxford 1977.
- [30] C. Runge, W. Lenz, *Vector Analysis*, Vol. 2, Dutton, New York 1919.
- [31] W. Lenz, *Z. Phys.* **24**, 197 (1924).
- [32] H. Goldstein, C. Poole, J. Safko, *Classical Mechanics*, Addison-Wesley, New York 2002.
- [33] C. Cohen-Tannoudji, B. Diu, F. Laloë, *Quantum Mechanics*, Wiley Interscience, New York 1977.
- [34] I.B. Khriplovich, *Theoretical Kaleidoscope*, Lecture Notes in Physics, Vol. 747, Springer, Heidelberg 2008.