Factorization with a logarithmic energy spectrum of a central potential

Ferdinand Gleisberg\textsuperscript{1} and Wolfgang P. Schleich\textsuperscript{1,2}

\textsuperscript{1}Institut für Quantenphysik and Center for Integrated Quantum Science and Technology (IQ\textsuperscript{ST}), Universität Ulm, D–89069 Ulm, Germany

\textsuperscript{2}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
Abstract

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 the zero angular momentum states. The bosons initially prepared in the ground state are excited by a sinusoidally time-dependent interaction into a state characterized by the quantum numbers which represent the factors of a number encoded in the frequency of the perturbation. We also discuss the full single-particle spectrum and limitations of our method caused by decoherence.

I. INTRODUCTION

It is well-known that the decomposition of a positive integer into a product of prime factors is a difficult problem in number theory for it requires non-polynomial time on a classical computer making it attractive for cryptological applications. E.g. for decoding a message encoded by the famous RSA protocol decomposition of a large semiprime i.e. a number composed by two primes in a reasonable time is needed. Such a decomposition can easily be prevented by choosing larger and larger semiprimes. If the topic of prime factorization is mentioned somewhere, may be in a discussion or may be in an article, it does not take long until the name Peter Shor appears because on a large ideal quantum computer Shor’s factorizing algorithm takes only polynomial time and is therefore expected to break the RSA scheme in the future.

As an alternative method we have studied the factorization of integers using bosonic atoms in one- and two-dimensional potentials both with a logarithmic energy spectrum. Bosons in a spherically symmetric harmonic potential as well as in a spherical box provide textbook examples for the study of thermodynamics of the Bose–Einstein condensation.

Our present theoretical study is motivated by the possibility to create and control nearly any kind of traps using adiabatic potentials as was stated in Ref. For the presentation of our work we have chosen here a pedagogical approach. We constructed numerically a central potential with a logarithmic energy spectrum. Two bosons originally trapped in the ground state of this potential are excited by a periodic perturbation with a frequency which contains the semiprime we want to factor. After some 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. Then a measurement of these energies provides the factors
we are looking for. The spherical symmetry of the unperturbed potential is crucial for our
protocol. Among the difficulties to realize spherical symmetry experimentally we mention
that here an environment free of gravity is required.

Our article is organized as follows. In Section II we introduce the logarithmic energy
spectrum and discuss the distribution of a given energy onto two single-particle states. In
Section III the Schrödinger equation in three dimensions is solved and it is found that the
s states i.e. the states with zero azimuthal quantum number are sufficient to determine
the potential with a logarithmic energy spectrum. In Section IV we take into account the
boundary condition at the origin and demonstrate that the single-particle s states exhibit
an energy spectrum similar to the one introduced in Section II. Section V discusses the
realization of our factorizing scheme by two bosonic atoms moving in the central potential
determined in Section III moreover, when excited by a time dependent interaction the
bosons achieve a transition into the factor state. In Section VI we present the solution of
the Schrödinger equation within the rotating wave approximation while the calculation can
be found in App. A and B. We mention that after a measurement of the single particle
energies at randomly chosen times the factor state is found with a probability of about one
half. Limitations of our method caused by decoherence are discussed in Section VII followed
by a short summary. An elementary discussion of the absence of accidental degeneracy in
our logarithic spectrum can be found in App. C.

II. MATHEMATICAL TOOLBOX

In the present section we first introduce the logarithmic energy spectrum and discuss its
special role in finding the factors of an integer. We then turn to the distribution of a given
energy onto two subsystems. This discussion constitutes the foundation for our factorization
protocol.

Our factorization scheme is based on a logarithmic energy spectrum of the type

\[ E_k(L) \equiv \hbar \omega_0 \ln \left( \frac{k}{L} + 1 \right), \quad k = 0, 1, 2, \ldots \]  

(1)

with \( E_0(L) = 0 \). 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 \( N = q_1 \cdot q_2 \) we try to distribute the energy

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

onto two subsystems with spectrum (1) and get

\[
E_{\text{total}}(N; L) = \hbar \omega_0 \ln \left( \frac{q_1}{L} \right) + \hbar \omega_0 \ln \left( \frac{q_2}{L} \right)
\]

\[
= E_{q_1-L} + E_{q_2-L}
\]

where we have used Eq. (1). Since the parameter \( L \) appears in the indices of the energies in Eq. (4) it has to be integer. No negative indices are present in Eq. (4) therefore \( N \) must not contain factors \( q_i < L \). Moreover, a factor \( q_i = L \) causes the unwanted case that the total energy (3) may be transferred to one subsystem while the other one is in the ground state \( E_0(L) \) and no factorization takes place. We conclude that we have to remove factors 2, 3, ..., \( L \) what can be done by simple division before our factorization protocol can be applied. However, if \( L \) is chosen to be unity it is easily verified that here the trivial factorization \( N = 1 \times N \) cannot be excluded. Moreover, in Section IV we shall see that \( L \) has to be odd. Therefore, throughout our article we consider the case \( L \geq 3 \). The question of uniqueness of the distribution (3) is easily answered because the fundamental theorem of arithmetics guarantees that the decomposition of the integer \( N \) is unique if both factors, \( q_1 \) and \( q_2 \), respectively, are prime.

For our factorization protocol the subsystems have to be brought into a state with total energy (3) followed by a measurement of the energies of the subsystems which easily allows the determination of the factors \( q_i \) as is described in Sect. VI. In the remainder of our article we shall concentrate on the factorization of semiprimes.

III. FROM THREE DIMENSIONS TO ONE DIMENSION

In the present section we realize the subsystem with spectrum (1) by a particle of mass \( \mu \) moving in three dimensions in a central potential \( V(r) \) which we shall determine.

We start with the Schrödinger equation in spherical polar coordinates

\[
\left[ -\frac{\hbar^2}{2\mu} \Delta + V(r) - E \right] \varphi(r, \Theta, \Phi) = 0
\]

(5)
and consider the wave functions
\[ \varphi_{k,\ell,m}(r, \Theta, \Phi) \equiv R_{k,\ell}(r) Y_{\ell}^m(\Theta, \Phi) \] (6)
which are simultaneous eigenfunctions of the Hamiltonian \( \hat{H} \), the square of the angular momentum \( \hat{L}^2 \), and its z-component \( \hat{L}_z \) which form a complete commuting set of operators with eigenvalues \( E_{k,\ell} \), \( \hbar^2 \ell(\ell+1) \) and \( \hbar m \), respectively. The radial quantum number \( k \) as well as the azimuthal quantum number \( \ell \) takes values \( 0, 1, 2, \ldots \) while the magnetic quantum number \( m \) takes the \( 2\ell + 1 \) values \(-\ell \ldots \ell\). The functions \( Y_{\ell}^m(\Theta, \Phi) \) are the spherical harmonics. In what follows we shall use a short-hand notation for the three quantum numbers \( k \equiv (k, \ell, m) \).

Because the solution of Eq. (5) can be found in most textbooks we jump directly to the radial equation valid in the region \( r \geq 0 \)
\[ \left[ -\frac{\hbar^2}{2\mu} \frac{d^2}{dr^2} + \frac{\hbar^2 \ell(\ell+1)}{2\mu r^2} + V(r) - E_{k,\ell} \right] R_{k,\ell}(r) = 0 \] (7)
with the condition that \( R_{k,\ell}(r) \) has to be square integrable and finite at the origin \( r = 0 \). We consider \( s \) states (\( \ell = 0 \)) and set
\[ R_{k,0}(r) = \frac{u_{k,0}(r)}{r} \] (8)
with the boundary condition
\[ u_{k,0}(0) = 0. \] (9)
Moreover, we write the cartesian coordinate \( x \) for the variable \( r \) and assume a symmetric potential \( V(x) = V(-x) \) where now \( -\infty < x < \infty \). With these modifications it is easy to change Eq. (7) into the equation
\[ \left[ -\frac{\hbar^2}{2\mu} \frac{d^2}{dx^2} + V(x; L) - E_k(L) \right] u_k(x; L) = 0 \] (10)
where for the moment we do not take into account the boundary conditions (9) and omit the \( s \) state index \( \ell = 0 \). This is the well-known Schrödinger equation for a particle of mass \( \mu \) moving in the one-dimensional potential \( V(x; L) \) with wave functions \( u_k(x; L) \) which are even (odd) for even (odd) indices \( k \). Here we have changed our notation in order to emphasize that the energies \( E_k(L) \) (11), the potential \( V(x; L) \), and the wave functions \( u_k(x; L) \) depend on the scaling parameter \( L \). Our iteration algorithm to determine the potential \( V(x; L) \) from...
the single particle spectrum (1) is based on the Hellmann-Feynman theorem and is described in a previous article.\cite{11} In Fig. 1 we show $V(x; L = 3)$ together with the eigenfunctions $u_k(x; L)$ for $0 \leq k \leq 6$.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{figure1.png}
\caption{One-dimensional potential $V(\xi; L)$ (dotted line) creating a logarithmic energy spectrum for a scaling parameter $L = 3$ as a function of dimensionless coordinates $\xi \equiv \alpha x$ with $\alpha^2 \equiv \mu \omega_0 / \hbar$. This potential is determined 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 $E_k(L)$ on the quantum number $k$ as given in Eq. (1). In the neighborhood of the origin the potential is approximately harmonic whereas for large values of $\xi$ it is logarithmic. In solid lines we depict the numerically determined energy wave functions of the first 7 states in their dependence on the dimensionless position. Both, the energies $E_k(L)$, $k = 0, 1, \ldots 6$ (dashed lines) as well as the potential $V(\xi; L)$ are shown in units of $\hbar \omega_0$.}
\end{figure}

Note that states with quantum numbers $\ell > 0$ were not needed for the determination of the potential $V(x; L)$. Some aspects of the full spectrum $E_{k,\ell}(L)$, however, are discussed in App. C.
IV. ENERGY SPECTRUM OF s STATES

We continue to limit ourselves to s states only and suppress the index $\ell = 0$. In the last section the potential $V(x, L)$ and the functions $u_k(x, L)$ were determined numerically and displayed in Fig. [1]. The three-dimensional potential $V(r; L)$ as well as the eigenfunctions $u_k(r; L)$ follow simply by replacing the coordinate $x$ by $r$ in either of them, where now only the region $r \geq 0$ is considered. Figure 2 shows the potential $V(r; L)$ with position vector $r$ in the $x$-$y$ plane. Here in three dimensions only odd solutions $u_k(x; L)$ of Eq. (10) can satisfy

\[ E_{2j+1}(L) = \hbar \omega_0 \ln \left( \frac{2j + 1}{L} + 1 \right) \]  

FIG. 2. Three-dimensional potential $V(r; L = 3)$ in units of $\hbar \omega_0$ creating the logarithmic energy spectrum Eq. (12) with scaling parameter $K = 2$ as a function of the dimensionless coordinates $\xi = \alpha x$ and $\eta = \alpha y$ plotted in the plane $z = 0$.

the boundary condition (9). Therefore, energies $E_k(L)$ as well as eigenfunctions $u_k(x; L)$ with even index $k$ which were present in one dimension in Eq. (10) do not appear anymore in three dimensions.

We will show now that the remaining spectrum $E_k(L)$ has indeed the form of Eq. (11) and therefore guarantees the validity of the results of Section II which we need for our factorization procedure. We rewrite the energies with odd radial quantum numbers $k = 2j+1$
with \( j = 0, 1, 2, 3 \ldots \) and shift them by \(-\hbar \omega_0 \ln(1/L + 1)\). It is easy to verify that the new spectrum is identical with single particle spectrum (1)

\[
E_{3d}^j(K) = \hbar \omega_0 \ln \left( \frac{j + 1}{K} \right)
\]

except that \( L \) has to be replaced by a new scaling parameter

\[
K = \frac{L + 1}{2}.
\]

In order that \( K \) is a positive integer the parameter \( L \) has to be odd. All the statements made in Section II referring to the scaling length \( L \) remain valid here provided \( L \) is replaced by \( K \). The eigenfunctions \( v_j(r; K) \) belonging to \( E_{3d}^j(K) \) are

\[
v_j(r; K) \equiv u_{2j+1}(r; L).
\]

Figure 3 shows the radial functions

\[
R_j(r) = \frac{v_j(r; K)}{r}
\]

for indices \( k = 0, \ldots 5 \) together with the potential \( V(r; L = 3) \) and the energy levels \( E_{j}^{3d}(K = 2) \) (12). To simplify the notation we pass over to the bra-ket formalism. The single-particle Schrödinger equation for the \( s \) states reads

\[
\hat{H}(K) |j\rangle = E_{3d}^j(K) |j\rangle \quad j = 0, 1, 2, \ldots
\]

where the quantum numbers \( \ell = m = 0 \) are suppressed. The hamiltonian \( \hat{H}(K) \) is characterized by the parameter \( K \) (13).

The Schrödinger equation for two non-interacting bosons is

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

with

\[
\hat{H}_{1,2}(K) = \hat{H}_1(K) + \hat{H}_2(K)
\]

\[
E_{m,n}(K) = E_{m}^{3d}(K) + E_{n}^{3d}(K)
\]

in accordance with Eqs. (12 and 13). Note that bosonic two-particle states are defined by

\[
|m,n\rangle_B \equiv \frac{1}{\sqrt{2}} \left( |m,n\rangle + |n,m\rangle \right),
\]

\[
|m,m\rangle_B \equiv |m,m\rangle.
\]
FIG. 3. Central potential $V(\rho; L = 3)$ creating the logarithmic energy spectrum $E_{3d}^3(K = 2)$ in units of $\hbar\omega_0$ as function of the dimensionless radius $\rho \equiv \alpha r$ together with the corresponding radial functions $R_j(\rho)$ of the first 6 states in their dependence on the dimensionless radius. Note that the energies have been shifted in order that the ground state has an energy zero here.

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

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

where $N \equiv p \cdot q$ is semi-prime then according to Eqs. (4 and 12) the bosons are in the state $|p-K, q-K\rangle_B$ we call factor state. 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. In the remainder of the article we suppress the scaling parameter $K$ as well as the suffix $B$ and the superscript 3d in order to simplify the notation.

V. TIME DEPENDENT PERTURBATION

In the present section we describe how the factorization protocol of Section II can be realized with two interacting identical bosons placed in a three-dimensional potential shown in Fig. 2 with single particle spectrum (12) which does not show degeneracy for $s$ states. We prepare the two bosons in the ground state $|0, 0\rangle$ and at $t = 0$ a perturbation

$$\delta V(r_1, r_2; t) = \gamma \sin(\omega_{ext} t) w(r_1, r_2)$$

(22)
is switched on. The frequency $\omega_{\text{ext}}$ is chosen later in a way suitable for the factorization procedure.

The movement of the two-particle ket $|\Psi(t)\rangle$ is now governed by the Schrödinger equation in three dimensions

$$i\hbar \frac{d}{dt}|\Psi(t)\rangle = [\hat{H}_{1,2} + \delta V(t)]|\Psi(t)\rangle$$  \hspace{1cm} (23)

with the unperturbed stationary equations

$$\hat{H}_{1,2} |\mathbf{k}_1, \mathbf{k}_2 \rangle = E_{\mathbf{k}_1, \mathbf{k}_2} |\mathbf{k}_1, \mathbf{k}_2 \rangle.$$  \hspace{1cm} (24)

We substitute the expansion of the solution $|\Psi(t)\rangle$ into the two-particle eigenkets $|\mathbf{k}_1, \mathbf{k}_2 \rangle$ of the unperturbed Hamiltonian $\hat{H}_{1,2}$

$$|\Psi(t)\rangle = \sum_{\mathbf{k}_1, \mathbf{k}_2} b_{\mathbf{k}_1, \mathbf{k}_2}(t)e^{-iE_{\mathbf{k}_1, \mathbf{k}_2}t/\hbar} |\mathbf{k}_1, \mathbf{k}_2 \rangle$$  \hspace{1cm} (25)

into Eq. (23) and arrive at the coupled system

$$i\hbar \dot{b}_{\mathbf{k}_1, \mathbf{k}_2}(t) = \gamma \sin(\omega_{\text{ext}} t) \sum_{\mathbf{k}_1', \mathbf{k}_2'} e^{i(E_{\mathbf{k}_1, \mathbf{k}_2} - E_{\mathbf{k}_1', \mathbf{k}_2'}) t/\hbar} W_{\mathbf{k}_1, \mathbf{k}_2; \mathbf{k}_1', \mathbf{k}_2'} b_{\mathbf{k}_1', \mathbf{k}_2'}(t)$$  \hspace{1cm} (26)

$$b_{\mathbf{k}_1, \mathbf{k}_2}(0) = 1 \quad \text{for} \quad k_1 + k_2 + \ell_1 + \ell_2 = 0 \quad \text{and} \quad b_{\mathbf{k}_1, \mathbf{k}_2}(0) = 0 \quad \text{otherwise}$$

which has to be solved for the probability amplitudes $b_{\mathbf{k}_1, \mathbf{k}_2}(t)$. Here the indices $\mathbf{k}_1$ etc. represent the triple of quantum numbers: $\mathbf{k}_1 \equiv (k_1, \ell_1, m_1)$ introduced in Section III. The eigenkets $|\mathbf{k}_1, \mathbf{k}_2 \rangle$ of $\hat{H}_{1,2}$, the amplitudes $b_{\mathbf{k}_1, \mathbf{k}_2}(t)$, and the matrix elements

$$W_{\mathbf{k}_1, \mathbf{k}_2; \mathbf{k}_1', \mathbf{k}_2'} \equiv \langle \mathbf{k}_1, \mathbf{k}_2 | w(\mathbf{r}_1, \mathbf{r}_2) | \mathbf{k}_1', \mathbf{k}_2' \rangle$$  \hspace{1cm} (27)

are 'bosonic' ones in the sense of Eq. (20) and are built out of the eigenkets $|\mathbf{k}_1, \mathbf{k}_2 \rangle$ of $\hat{H}_{1,2}$ and the spacial part $w$ of the perturbation $\delta \hat{V}$. Moreover, in the summation in Eqs. (25) and (26) the same states must not be counted twice.

In App. A we study the matrix element (27) for the case of a contact interaction between the particles while in App. B we benefit from the rotating wave approximation and reduce the system (26) to the much simpler system (B4) and (B5) of only two differential equations for two probability amplitudes, namely that of the ground state and that of the factor state, respectively. We solve them in then next section.
VI. APPROXIMATE SOLUTION

With the help of the so-called secular or rotating wave approximation (RWA) \[12\] we have reduced the infinite system (26) to only two first-order differential equations with constant coefficients (B4 and B5). App. B presents the calculation. Together with the initial conditions \(b_{0,0}(0) = 1\) and \(b_{p-K,q-K}(0) = 0\) the equations are immediately solved. The resulting probability amplitudes are for the ground state

\[b_{0,0}(t) = \cos(\Omega t)\] (28)

and

\[b_{p-K,q-K}(t) = \sin(\Omega t)\] (29)

for the factor state, respectively, and the so-called Rabi frequency is

\[\Omega = \frac{\gamma}{2h} W_{0,0,p-K,q-K}\] (30)

which is proportional to the interaction matrix element (A4). In Sect. II and IV it was shown that if the bosons are in the factor state \(|p - K, q - K\rangle\) they have a two-particle energy \(\hbar \omega_0 \ln(\frac{N}{K^2})\) with \(N = p \cdot q\) (21).

As mentioned there the factors \(p\) or \(q\) are determined by a measurement of single-particle energies (3) and the factorization protocol has ended successfully.

At time \(t\) the system can be found with probability \(|b_{p-K,q-K}(t)|^2\) in the factor state and at times equal to an odd multiple of \(\pi/(2\Omega)\) with certainty but, unfortunately, the Rabi frequency \(\Omega\) is not known. Instead, we content ourselves with measuring at a time chosen at random from a time interval \([0, T]\) much larger than \(\pi/\Omega\). Utilizing Eq. (29) it is easy to see that the probability to find the factor state is about one half. Then the measurement of a 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 determining so the Rabi frequency (30) was presented in a previous article.[4]

VII. LIMITATIONS

In the present section we shall sketch what prevents our protocol to factor larger and larger semiprimes. According to Ref. [13] there is a high probability for the periodic transition into
the factor state as long as the difference between the energies of this state and of the next
off-resonant state, respectively, is larger than the energy \( \hbar \Omega \) of the Rabi oscillation

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

(31)

Because the Rabi frequency \( \Omega \) defined by Eq. (30) is proportional to the strength \( \gamma \) of the
perturbation (22) this condition can easily be satisfied by choosing \( \gamma \) as small as needed.
Unfortunately, a second condition arises from Section VI where the time of measurement
of the energies of the two bosons was chosen randomly from an interval \([0, T]\). To find
the factor state with a probability of \( \approx \frac{1}{2} \) the length \( T \) of the interval had to fulfill the
condition \( \Omega T \gg 1 \). On the other hand the system has to be free of decoherence during the
time interval \( i.e. T < T_{\text{dec}} \) leading to two inequalities the Rabi frequency has to fulfill

\[
\Omega \gg \frac{1}{T_{\text{dec}}} \quad \text{and} \quad \Omega \ll \frac{\omega_0}{N}.
\]  

(32)

Our aim is to find an upper limit of the number to be factored \( N \). In our articles Ref. 4 and
6 for different experimental situations and models for the spacial part of the interaction an
\( N \)-dependence of the transition matrix element

\[
W_{0,0,p-K,q-K} \propto N^{-1/2}
\]  

(33)

was found in rough approximation and the same is valid, of course, for the Rabi frequency
\( \Omega \) (30). The semiprime \( N \) to be factored therefore has an upper limit

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

(34)

Assuming that according to Eq. (22) the interaction strength \( \gamma \) can be chosen at will this
relation shows that the crucial limiting factor for the magnitude of \( N \) is the decoherence
time \( T_{\text{dec}} \).

VIII. SUMMARY

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 a central potential such that it has a logarithmic energy spectrum. First we calculated numerically a one-dimensional potential from a logarithmic single particle spectrum. Because of the close relationship between three-dimensional spherically symmetric and one-dimensional problems, respectively, the central potential then was easily found. As expected this potential had an energy spectrum with a logarithmic $s$ wave part but with a scaling length different from the one in the one-dimensional spectrum.

In the second part of our work we attacked the problem how to bring the bosons into the factor state. The bosons were excited from their ground state by a periodic time-dependent contact interaction of a frequency which was determined by the number $N$ to be factored. To exclude transitions between non-$s$ states we discussed in extenso the absence of degeneracy. Then we showed within the framework of the well-known rotating wave approximation that the bosons performed a Rabi oscillation between the ground state and the factor state. The latter was found with a probability of about one half when the energies of the bosons were measured at a randomly chosen time. From these the factors of $N$ were easily determined and our factorization protocol has ended successfully.

**ACKNOWLEDGMENTS**

We thank M. A. Efremov and M. Freyberger for stimulating discussions on this topic. WPS 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: Matrix elements of the interaction

In this appendix we study the matrix element (27)

\[ W_{k_1, k_2; k'_1, k'_2} \equiv \langle k_1, k_2 | w(\hat{r}_1, \hat{r}_2) | k'_1, k'_2 \rangle \]  

\[ (A1) \]

assuming a contact interaction between the particles

\[ w(r_1, r_2) = \delta^{(3)}(r_1 - r_2). \]  

\[ (A2) \]
With the help of (A2) the transition matrix element can be represented by the eigenfunctions \( \varphi_k(r) \) introduced in section III:

\[
W_{k_1,k_2;k_1',k_2'} \equiv \int d^3r \varphi_{k_1}(r)^* \varphi_{k_2}(r)^* \varphi_{k_1'}(r) \varphi_{k_2'}(r).
\]  

(A3)

Having in mind that we start our procedure at time \( t = 0 \) with the two particles in the ground state \( |0,0\rangle \) we consider the matrix elements \( W_{0,0,k_1,k_2} \) for a transition into some excited state \( |k_1,k_2\rangle \). It is not difficult to derive the expression

\[
W_{0,0,k_1,k_2} = \frac{1}{4\pi} \int dr r^2 R_{0,0}(r)^2 R_{k_1,\ell_1}(r) R_{k_2,\ell_2}(r) \delta_{\ell_1,\ell_2} \delta_{m_1+m_2,0}.
\]  

(A4)

Here we have substituted Eq. (6) for the eigenfunctions \( \varphi_k(r) \), moreover we applied the well-known orthonormality of the spherical harmonics

\[
\int \int d\Omega Y_{\ell_1}^m(\theta, \varphi) Y_{\ell_2}^n(\theta, \varphi) = \delta_{\ell_1,\ell_2} \delta_{m_1,m_2}
\]  

and the relation for their complex conjugate

\[
Y_{\ell}^{-m}(\theta, \varphi) = Y_{\ell}^m(\theta, \varphi)^*.
\]  

(A5)

(A6)

Note that \( Y_0^0 \equiv 1/\sqrt{4\pi} \).

In the next appendix we use the matrix element (A4) when we return to the system of coupled equations (26) which we shall simplify considerably.

**Appendix B: Rotating wave approximation (RWA)**

In this appendix we put all magnetic quantum numbers \( m_i = 0 \) and omit them henceforth. This assumption will be justified in the calculation below. A single-particle state is now characterized by only two quantum numbers \( k \) and \( \ell \), respectively. We study the sub-system

\[
i\hbar \dot{b}_{0,0,0,0}(t) = \gamma \sin(\omega_{\text{ext}} t) \times \sum_{k_1,k_2,\ell} e^{-i(E_{k_1,\ell}+E_{k_2,\ell})t/\hbar} \times W_{0,0,0,k_1,\ell,k_2,\ell} b_{k_1,\ell;k_2,\ell}(t)
\]  

of the system (26) with the matrix element (A4) and a zero ground state energy of the two bosons.
The essence of the RWA applied to (B1) is simply to keep all terms with constant coefficients on the right hand side and to neglect all oscillating terms. The external frequency $\omega_{\text{ext}}$ is now chosen such that the energy $\hbar \omega_{\text{ext}}$ agrees with the energy
\[ E_{p-K,0;q-K,0} = E_{p-K,0} + E_{q-K,0} = \hbar \omega_0 \ln \left( \frac{N}{K^2} \right) \] (B2)
of the factor state and is determined by the number to be factored $N = p \cdot q$. Consider now the time dependent factors
\[
\frac{1}{2i} \left[ e^{i(E_{p-K,0}+E_{q-K,0})t/\hbar} - e^{-i(E_{p-K,0}+E_{q-K,0})t/\hbar} \right] \
\times e^{-i(E_{k_1,\ell}+E_{k_2,\ell})t/\hbar}
\] (B3)
which appear on the right hand side of (B1). Note here the expanded sinus. Assuming $p \geq q$ only the term with $k_1 = p - K$, $k_2 = q - K$ and $\ell = 0$ survives the application of the RWA and is of amount $(2i)^{-1}$. Appendix C discusses the absence of accidental degeneracy in the single particle spectrum $E_{k,\ell}$ (I) which is demonstrated in Figure 7. None of the terms with $\ell \geq 1$ may therefore lead to additional constant terms in (B3). We note in passing that the $(2\ell + 1)$-fold degeneracy with respect to the magnetic quantum number $m$ is simply unity as was mentioned above.

With these results it is easy to see that (B1) is reduced to the equation
\[
i \hbar \dot{b}_{0,0}(t) = \frac{\gamma}{2i} W_{0,0;p-K,q-K} b_{p-K,q-K}(t)
\] (B4)
where the index $\ell = 0$ present in the matrix elements and in the probability amplitudes is omitted here for convenience. To derive a second equation we select the term with $k_1 = p - K$ and $k_2 = q - K$ from (26) and proceeding like before we get
\[
i \hbar \dot{b}_{p-K,q-K}(t) = -\frac{\gamma}{2i} W_{p-K,q-K;0,0} b_{0,0}(t).
\] (B5)
of the unperturbed $s$ states. Equations (B4 and B5) characterize the dynamics of the two-boson system driven by the periodic perturbation (22) with frequency (B2). Together with the initial conditions $b_{0,0}(0) = 1$ and $b_{p-K,q-K}(0) = 0$ and the symmetry
\[ W_{m,n;0,0} = W_{0,0;m,n} \] (B6)
they are solved in Sect. VI.
FIG. 4. Scaled effective potential (solid line) formed by the angular momentum barrier (dotted) and the potential $V(\rho; L = 3)$ (dashed) which in the quantum case creates the logarithmic energy spectrum \(12\) for a scaling parameter $K = 2$ \(13\) as function of the dimensionless radius $\rho \equiv \alpha_{cl} r$. The horizontal line $E = 0.86 V_0$ denotes the energy of the radial coordinate $r(t)$ of the classical particle moving periodically from the left turning point to the right one and back. Of course, $\Theta(t)$ is not periodic as is the orbit $r(\Theta)$ shown in Fig. 5.

Appendix C: Absence of accidental degeneracy

The energy spectra of any central potential exhibit the $(2\ell+1)$-fold "essential degeneracy" as the energy levels $E_{k,\ell}$ do not depend on the magnetic quantum number $m$. It has been proven long ago that the only potentials that show accidental degeneracy are the Coulomb and the harmonic oscillator one, respectively.\[14\] This is a consequence of the existence of a conserved quantity which does not commute with any member of a complete system of commuting operators of the problem.\[15\] In the Coulomb case this is the well-known Runge-Lenz vector.\[16, 17\] The conserved quantity for the harmonic oscillator problem we shall discuss below. We conclude that in our potential which is neither of both accidental degeneracy is absent. Nevertheless we shall study this problem in more detail here.
1. Trajectory of a classical particle

FIG. 5. Trajectory \( r(\Theta) \) of a classical particle with mass \( \mu \) and energy \( E = 0.86 V_0 \) moving in the effective potential shown in Fig. 4. The trajectory starts at an inner turning point and an angle \( \Theta = 0 \). After having covered five periods it reaches an inner turning point at an angle \( \Theta \approx 11\pi/8 \).

We recall the trajectories of a classical particle in the harmonic oscillator as well as in the Coulomb potential are closed, the latter for negative energies only. Following the textbook \[18\] we calculate the trajectory of a classical particle of mass \( \mu \), energy \( E \) and angular momentum \( J \) moving in the effective potential

\[ V_{\text{eff}}(r) = \frac{J^2}{2\mu r^2} + V_0 v(r) \quad \text{(C1)} \]

with an energy \( E = 0.86 V_0 \) periodically between both turning points as displayed in Fig. 4 while five periods of the trajectory \( r(\Theta) \) are shown in Fig. 5 where the dimensionless radius \( \rho = \alpha_{\text{cl}} r \) with

\[ \alpha_{\text{cl}} = \left( \frac{\mu V_0}{J^2} \right)^{1/2} \quad \text{(C2)} \]

was used.

The potential determined numerically from the spectrum \[11\] and shown in Fig. 2 is denoted by \( v(\rho) \). It is evident that the orbit of the particle does not close but precesses around the force center thus indicating the absence of accidental degeneracy.
2. Energy spectrum

The most direct way to check for degeneracy is simply to calculate the energies $E_{k,\ell}$ for the potential under consideration with radial and azimuthal quantum numbers $k$ and $\ell$, respectively. If two or more of the energies with different indices are equal degeneracy is present otherwise not.

FIG. 6. Lowest scaled energies of the three-dimensional harmonic oscillator. The scheme of levels $E_n = \hbar \omega (n + 3/2)$ shows degeneracy as the principal quantum number $n = 2k + \ell$ depends on both, the radial quantum number $k$ and the azimuthal quantum number $\ell$, respectively. For example the level $n = 2$ is doubly degenerate for the quantum numbers $k = 1, \ell = 0$ and $k = 0, \ell = 2$, respectively.

Before we turn to our potential $v(\rho)$ we recall the situation for the three-dimensional harmonic oscillator where the lowest energy levels are displayed in Fig. 6.

The energies $E_{k,\ell}$ depend on a combination of both indices $k$ and $\ell$ namely on the principal quantum number $n = 2k + \ell$ leading to degeneracy of the levels $E_n = \hbar \omega (n + 3/2)$ as can be checked from levels with $n = 2, 3, 4$ of the figure. If the x- and y-axis are oriented along the symmetry axes of the elliptic orbit of the oscillator then it can be shown that the additional integral of motion reduces to the scalar function $E_x - E_y$, the difference between the energies of the projections of the motion onto the x- and the y-axis, respectively.
FIG. 7. Scaled energies of a particle with mass $\mu$ moving in a three-dimensional potential leading to a spectrum with $s$ state part (12) and scaling parameter $K = 2$ of Eq. (13). Every energy level is characterized by two quantum numbers $k$ and $\ell$, respectively. No principal quantum number can be identified and evidently no accidental degeneracy takes place.

With the help of the potential $v(\rho)$ we solved the radial equation (7) numerically. The lowest energy levels $E_{k,\ell}$ are displayed in Fig. 7. At first sight the scheme of the energies resembles that of the harmonic oscillator potential. But looking more closely we observe that the levels which in the harmonic oscillator scheme of Fig. 6 were degenerate with each other now differ slightly. We conjecture that the higher energy levels behave similarly and no accidental degeneracy is present. 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 $v(\rho)$.

[1] Godfrey H. Hardy and Edwrd M. Wright, *An Introduction to the Theory of Numbers* (Oxford university press, 1979).
[2] Ronald L. Rivest, Adi Shamir and Leonard Adleman, *A method for obtaining digital signatures and public-key cryptosystems* Communications of the ACM 21 (2), 120–126 (1978).

[3] Peter W. Shor “Algorithms for quantum computation: Discrete logarithms and factoring” in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (Ieee 1994) 124–134.

[4] Ferdinand Gleisberg, Rüdiger Mack, Karl Vogel, and Wolfgang P. Schleich “Factorization with a logarithmic energy spectrum,” New Journal of Physics 15 (2), 023037 (2013).

[5] Ferdinand Gleisberg, Fabio Di Pumpo, Gerhard Wolff, and Wolfgang P. Schleich “Prime factorization of arbitrary integers with a logarithmic energy spectrum,” Journal of Physics B: Atomic, Molecular and Optical Physics 51, 035009 (2018).

[6] Ferdinand Gleisberg, Michael Volpp, and Wolfgang P. Schleich “Factorization with a logarithmic energy spectrum of a two-dimensional potential,” Physics Letters A 379, 2556–2560 (2015).

[7] Christopher J. Pethick and Henri Smith, *Bose–Einstein condensation in dilute gases* (Cambridge university press, 2008).

[8] Sálvio J. Bereta, Lucas Madeira, Vanderlei S. Bagnato, and Mônica Caracanhas “Bose–Einstein condensation in spherically symmetric traps,” American Journal of Physics 87, 924–934 (2019).

[9] Barry M. Garraway and Hélène Perrin “Recent developments in trapping and manipulation of atoms with adiabatic potentials” (Journal of Physics B: Atomic, Molecular and Optical Physics) 49, 172001 (2016).

[10] Nathan Lundblad, Thomas Jarvis, and Tiago Correia *Design of a microgravity shell-geometry Bose-Einstein condensate experiment* in “APS Division of Atomic, Molecular and Optical Physics Meeting Abstracts 2017” (APS Meeting Abstracts 2017) 2017, 106.

[11] Rüdiger Mack, Jens Peder Dahl, Hector M. Moya-Cessa, Walter T. Strunz, Reinhold Walser, and Wolfgang P. Schleich “Riemann ζ function from wave-packet dynamics,” Physical Review A 82, 032119 (2010).

[12] Claude Cohen-Tannoudji, Bernhard Diu, and Franck Laloë, *Quantum Mechanics* (Wiley Interscience, New York, 1977).

[13] Wolfgang P. Schleich, *Quantum Optics in Phase Space* (VCH-Wiley, Weinheim, 2001).

[14] Joseph Bertrand, “Théoreme relatif au mouvement d’un point attiré vers un centre fixe,”
Comptes rendus de l’académie des sciences 77, 849–853 (1873).

[15] Lev D. Landau and Evgenii M. Lifshitz, *Quantum mechanics: non-relativistic theory* (Elsevier 2013).

[16] Carl Runge and Wilhelm Lenz *Vector analysis* (Dutton, New York, 1919).

[17] Wilhelm Lenz, “Über den Bewegungsverlauf und die Quantenzustände der gestörten Kepler-bewegung,” Zeitschrift für Physik 24, 197–207 (1924).

[18] Herbert Goldstein, Charles Poole, and John Safko, *Classical mechanics* (AAPT 2002).

[19] Iosif B. Khriplovich, *Theoretical Kaleidoscope* (Springer Science & Business Media, 2007).