FAST TRACK COMMUNICATION

Factorizing numbers with classical interference: several implementations in optics

A A Rangelov

Department of Physics, Sofia University, James Bourchier 5 blvd., 1164 Sofia, Bulgaria

Received 5 November 2008, in final form 6 November 2008
Published 12 January 2009
Online at stacks.iop.org/JPhysB/42/021002

Abstract
Truncated Fourier, Gauss, Kummer and exponential sums can be used to factorize numbers: for a factor these sums equal unity in absolute value, whereas they nearly vanish for any other number. We show how this factorization algorithm can emerge from superpositions of classical light waves and we present a number of simple implementations in optics.

(Some figures in this article are in colour only in the electronic version)

1. Introduction
Factorization of numbers into their prime factors is a hard non-polynomial problem for classical computers. It was Shor [1] who proposed a quantum algorithm which can solve the problem of factorization of numbers on a quantum computer with a tremendous speedup as compared to a classical computer. A practical demonstration of Shor’s algorithm has been carried out by factorizing the integer 15 [2], using nuclear magnetic resonance. However, quantum computers capable of implementing Shor’s algorithm for larger numbers have not yet been developed.

Several approaches to factorizing numbers based on interference of multiple quantum paths have been proposed [3–11]. Those schemes do not use quantum entanglement and do not capitalize on quantum parallelism. As a consequence, these schemes scale exponentially with the number of digits of the factorized number. This is in contrast to Shor’s algorithm which requires only a polynomial number of operations. Nevertheless, if the interference is implemented in a suitable way in a system, which does the factorization, then one can benefit because nature plays the role of a computer.

As was pointed out by Jones [12] the proposed techniques for factorization based on Gauss sums [6–8] unfortunately do not provide useful methods for factorizing numbers, because a precalculation of the factors is needed for the experiment. In spite of that, Gauss sums would be useful if it is possible to avoid explicit precalculation stages of the algorithms.

Physical systems that can implement the Gauss sums must be described by complex numbers. In the present communication, we investigate how truncated Fourier sum and its generalizations, such as truncated Gauss, Kummer and exponential sums could emerge from superposition of several oscillations. Those sums can be used successfully to factorize numbers. Due to the wide use of interferences and beats in optics, we shall keep our consideration close to optics, and our examples are also in wave optics.

However, the proposed implementation can be extended to virtually any physical system where superposition among several different oscillations appears, from the mechanical pendulum with several degrees of freedom, through the atomic and solid state systems and their analogues in quantum mechanics.

2. Truncated Fourier, Gauss, Kummer and exponential sums
In order to find the factors of a given number \( N \) we use the following truncated sum:

\[
A_N^{(M)}(l) = \frac{1}{M} \sum_{m=1}^{M} \exp\left(-2\pi i m l N / M\right),
\]

where \( k \) is an integer and \( M \) is the number of terms in the sum. The argument \( l \) scans through all integers between \( 1 \) and \( \sqrt{N} \) for possible factors. The capability of the sum of
equation (1) to factor numbers originates from the fact that for an integer factor $q$ of $N$ with $N = ql$, all phases in $A_N^{(M)}(l)$ are integer multiples of $2\pi$. Consequently, the terms add up constructively and yield $A_N^{(M)}(l) = 1$. When $l$ is not a factor, the phases oscillate rapidly with $m$, and $A_N^{(M)}(l)$ takes on small values. In this interference pattern, the larger truncation parameter $M$ leads to better convergence. In principle, already the first several terms of the sum are sufficient to discriminate factors from non-factors. Depending on the coefficient $k$ in equation (1) we distinguish several important cases

- Fourier sum for $k = 1$ [10],
- Gauss sum for $k = 2$ [5–10, 13, 14],
- Kummer sum for $k = 3$ [10],
- exponential sum for $k = m$ [10].

The use of quadratic phases to factor numbers (Gauss sum) has the advantage of fewer terms needed in the sum to distinguish factors from non-factors compared to the linear phase (Fourier sum), which is because of high quasi-randomness for the quadratic phase [10]. In the very same way the Kummer sum, and sums with nonlinear phases of higher order, has an advantage compared to the Gauss sum [10].

Now we consider a system with $M$ different oscillation modes, with frequencies $\omega_m$, phases $\phi_m$ and amplitudes $E_{0m}$

$$E_m(t) = E_{0m} \exp(i\omega_m t + i\phi_m).$$  \hspace{1cm} (3)

Using the superposition principle we can write the resulting oscillation as the sum of all oscillations

$$E(t) = \sum_{m=1}^{M} E_m(t) = \sum_{m=1}^{M} E_{0m} \exp(i\omega_m t + i\phi_m).$$  \hspace{1cm} (4)

In the sum of equation (4) we can vary the parameters $E_{0m}$, $\omega_m$, $\phi_m$ and the time $t$. In the following several sections we will show how truncated Fourier, Gauss, Kummer and exponential sums could emerge when we fix three of the parameters for all oscillations, while changing the fourth parameter.

3. Factorization using differences in time delay (interferometry)

3.1. Mach–Zehnder interferometer

First we consider the case when the parameters $E_{0m}$, $\omega_m$, $\phi_m$ are equal for all oscillations in equation (3),

$$E_{0m} = E_0, \quad \omega_m = \omega, \quad \phi_m = 0.$$  \hspace{1cm} (5)

thus the only parameter that is left not fixed in equation (3) is the time $t$. This can easily be realized in optics by interferometry, where the individual oscillations describe the electric field for the different arms of the interferometer as shown in figure 1.

**Figure 1.** Four arms Mach–Zehnder interferometer that can be used to factorize numbers by using Fourier, Gauss, Kummer or exponential sums. The four arms correspond to four terms in the sum. Repeating the procedure for doubling the arm, in principle, one can increase the terms in the sum as much as needed to distinguish factors from non-factors.

From figure 1 and equation (4) we see that we have the following sums of electric fields in the detector:

$$E = E_0 \sum_{m=1}^{M} \exp(i\phi_m),$$  \hspace{1cm} (8)

where $\phi_m$ is the phase accumulated in the $m$ arm of the interferometer due to the difference in travel time through each arm.

Suppose that each arm of the interferometer is with length $L$, the wavelength of the light that we use in the vacuum is $\lambda$, and the corresponding frequency is $\omega$, let the index of refraction in each arm of the interferometer be different and denoted as $n_m$. Then the phase $\phi_m$ for the beam that travels through the $m$th arm of the interferometer is given as

$$\phi_m = t_m \omega = \frac{L}{c_m} \omega,$$  \hspace{1cm} (9)

here $t_m$ is the time that light travels in the $m$th arm of the interferometer to pass length $L$ and $c_m$ is the speed of light in that arm. The refraction index in the arm $m$ of the interferometer is

$$n_m = \frac{c}{c_m},$$  \hspace{1cm} (10)

thus

$$\phi_m = \omega \frac{L}{c} n_m = \frac{2\pi}{\lambda} n_m L,$$  \hspace{1cm} (11)

then the electric filed in the detector is

$$E = E_0 \sum_{m=1}^{M} \exp\left(2\pi i \frac{L}{\lambda} n_m \right).$$  \hspace{1cm} (12)

Now, if the index of reflection in the $m$ arm of the interferometer is

$$n_m = a + bm^k,$$  \hspace{1cm} (13)

then

$$E = E_0 \exp\left(2\pi i \frac{aL}{\lambda} \right) \sum_{m=1}^{M} \exp\left(2\pi im^k \frac{bL}{\lambda} \right).$$  \hspace{1cm} (14)
The detector registers the intensity,

$$I \sim |E|^2 = \left| \sum_{m=1}^{M} \exp \left( \frac{2\pi im^k bL}{\lambda} \right) \right|^2.$$  

(15)

Various $k$ give us a different type of truncated sum (see equation (2)). The number that we want to factorize is $bL$, the trial factors are $\lambda$. Each time when the trial factor $\lambda$ is a factor of $bL$ we will observe a maximum signal in the detector. The number of the terms in the sum can be controlled by doubling the elements in the interferometer, figure 1. The numbers that could be factorized in this way are of order $L/\lambda \sim \frac{1m}{1000\mu m} = 10^6$.

3.2. Pulse train

Now we consider a train of pulses, where the delay of the $m$ pulse compared to the first pulse is given as

$$t_m = m^k \tau,$$  

(16)

here $m$ takes the values $m = 1, 2, 3, \ldots, M$, while $\tau$ can be set as a unit of time.

We consider the case when all pulses have equal amplitudes $E_{0m} = E_0$ and equal frequencies $\omega_m = \omega$. Then the electric field for the $m$ pulse is given by equation (3) and reads

$$E_m = E_0 \exp(\imath \omega_m t_1) = E_0 \exp(\imath \omega m^k \tau + \imath \varphi_m).$$  

(17)

Let us make a different pathway for every pulse in such a way that all pulses hit the same detector at the same time, this is equivalent to making $\varphi_m = 0$ at the place where all pulses collide. Then the intensity that the detector registers is a result from the superposition among all electric fields, e.g. the sum from equation (4):

$$I \sim |E|^2 = \left| \sum_{m=1}^{M} E_m \right|^2 = \left| E_0 \sum_{m=1}^{M} \exp(2\pi m^k \nu \tau) \right|^2.$$  

(18)

where $\nu = \omega/2\pi$. If one chooses the frequency $\nu$ as the number that we want to factorize ($N$) and $1/\tau$ as a trail factor ($l$), then equation (18) reduces to the sum from equation (1).

4. Factorization using differences in frequencies (beats)

If we now consider a system that exhibits several oscillations with the same amplitude $E_0$ and the same initial phases ($\varphi_m = 0$), but with different frequencies $\omega_m$, then the individual oscillations (3) are described by

$$E_m(t) = E_0 \exp(\imath \omega_m t),$$  

(19)

$$\omega_m = m^k \omega_0,$$  

(20)

the resulting oscillation (4) is

$$E(t) = \sum_{m=1}^{N} E_0 \exp(-2\pi i m^k \nu_0 t),$$  

(21)

where $\nu_0 = \omega_0/(2\pi)$. We will observe beats when $t\nu_0$ is an integer which could be used to find the factors of the number $\nu_0$. One physical realization of the above idea could be a light with several high-harmonic generated frequencies $[15, 16]$, chosen in the way that they present, for example, the odd terms in the Fourier sum

$$\omega_0, 3\omega_0, 5\omega_0, 7\omega_0, \ldots$$  

(22)

then in the detector the time of the detection plays the role of the test factors and whenever there is a beat we observe a maximum of the signal, thus this time is a real factor.

5. Factorization using Faraday effect

The last parameter that we can vary in equation (3) is the amplitude of the individual oscillation. For example, if we work with laser light we can use the different polarization orientations of the electric field. The electric field is a vector in the polarization plane, which can be described by the complex electrical field.

Let us consider the case when we have a linearly polarized light pulse, which is split into several parts and each part passes different pathways through Faraday cells as shown in figure 2.

Applying different Faraday rotation angles $\varphi_m$ on each pathway and collecting all of the light at the same place (at the detector) the resulting electric field is the superposition

$$E = \frac{E_0}{M} \sum_{m=1}^{M} \exp(\imath \varphi_m).$$  

(23)

where $E_0$ is the electrical field amplitude of the initial beam. The relation between the angle of polarization rotation due to the Faraday effect $\varphi_m$ and the magnetic field $B_m$ in a diamagnetic material [17] is

$$\varphi_m = 2\pi bL B_m,$$  

(24)

where $L$ is the length of each pathway and $2\pi b$ is the Verdet constant for the material [17]. For the amplitude of the resulting electric field we have

$$E = \frac{E_0}{M} \sum_{m=1}^{M} \exp(2\pi ibL B_m).$$  

(25)

If we now have a magnetic field $B_m$ for the $m$th Faraday cell, which is given as
\[ B_m = B_0 m^k, \quad (26) \]

then the intensity in the detector is

\[ I \sim |E|^2 = \left| E_0 \sum_{n=1}^{M} \exp(2\pi i m^k bL B_0) \right|^2. \quad (27) \]

Here the number that we want to factorize is \( bL \), the trial factors are \( 1/B_0 \).

6. Conclusions

We have shown how the factorization algorithm based on truncated Fourier, Gauss, Kummer or exponential sums emerges naturally from superpositions of classical light waves. We have proposed a number of simple implementations in optics. These implementations can be extended to virtually any physical system where superpositions of several different oscillations appear.

The factorization algorithms discussed in this communication are classical algorithms and thus their complexity scales exponentially with the number of digits. If an extension of this algorithm exists in entangled quantum systems, then a quantum computing parallelism would be involved with an exponential speedup of factorization. The present solutions therefore could be the first step towards an alternative quantum factorization algorithm to the famous Shor algorithm.

Acknowledgments

This work has been supported by the European Commission’s projects CAMEL, EMALI and FASTQUAST, and the Bulgarian NSF Grants Nos 205/06, 301/07 and 428/08. The author is grateful to N Vitanov for stimulating discussions and critical reading of the communication. During the preparation of the communication, the author became aware of a related work by Tamma \textit{et al} (arXiv:0811.1595).

References

[1] Shor P 1994 \\textit{Proc. 35th Annu. Symp. on Foundations of Computer Science} (New York: IEEE Computer Society Press)
[2] Vandersypen L M K, Steffen M, Breyta G, Yannoni C S, Sherwood M H and Chuang I L 2001 \\textit{Nature (London)} 414 834
[3] Clauser J F and Dowling J P 1996 \\textit{Phys. Rev. A} 53 4587
[4] Summhammer J 1997 \\textit{Phys. Rev. A} 56 4324
[5] Merkel W, Averbukh I Sh, Girard B, Paulus G G and Schleich W P 2006 \\textit{Fortschr. Phys.} 54 856
[6] Mahesh T S, Rajendran N, Peng X and Suter D 2007 \\textit{Phys. Rev. A} 75 062303
[7] Mehring M, Muller K, Averbuch I Sh, Merkel W and Schleich W P 2007 \\textit{Phys. Rev. Lett.} 98 120502
[8] Gilowski M, Wendrich T, Muller T, Jentsch Ch, Ertmmer W, Rasel E M and Schleich W P 2008 \\textit{Phys. Rev. Lett.} 100 030201
[9] Sadgrove M, Kumar S and Nakagawa K 2008 \\textit{Phys. Rev. Lett.} 101 180502
[10] Stefanak M, Haase D, Merkel W, Zubairy M S and Schleich W P 2008 \\textit{J. Phys. A: Math. Theor.} 41 304024
[11] Bigourd D, Chatel B, Schleich W and Girard B 2008 \\textit{Phys. Rev. Lett.} 100 030202
[12] Jones J A 2008 \\textit{Phys. Lett. A} 373 5758
[13] Merkel W, Mack H, Schleich W P, Lutz E, Paulus G G and Girard B 2007 \\textit{Phys. Rev. A} 76 023417
[14] Stefanak M, Merkel W, Schleich W P, Haase D and Maier H 2007 \\textit{New J. Phys.} 9 370
[15] Brabec T and Krausz F 2000 \\textit{Rev. Mod. Phys.} 72 545
[16] Gavrila M 1992 \\textit{Atoms in Intense Laser Fields} (Boston, MA: Academic)
[17] Landau L D and Lifschitz E M 1960 \\textit{Course of Theoretical Physics} (Electrodynamics of Continuous Media vol 8) (Oxford: Pergamon)