Noname manuscript No.
(will be inserted by the editor)

Analogue algorithm for parallel factorization of an exponential number of large integers

I. Theoretical description

Vincenzo Tamma

Received: date / Accepted: date

Abstract We describe a novel analogue algorithm that allows the simultaneous factorization of an exponential number of large integers with a polynomial number of experimental runs. It is the interference-induced periodicity of "factoring" interferograms measured at the output of an analogue computer that allows the selection of the factors of each integer [26,35,34,28]. At the present stage the algorithm manifests an exponential scaling which may be overcome by an extension of this method to correlated qubits emerging from n-order quantum correlations measurements. We describe the conditions for a generic physical system to compute such an analogue algorithm. A particular example given by an "optical computer" based on optical interference will be addressed in the second paper of this series [25].

Keywords quantum computation · interference · algorithms · analogue computers · factorization · exponential sums · Gauss sums

1 Fundamental principle of our work

Multiplying numbers is much easier than the inverse problem of finding the factors of large integers. Indeed, the security of codes relies on the current inability of a fast solution of this problem but is endangered by the well-known Shor's factoring algorithm [21,36,9,7,8,16,15].

Recently, important works about the use of different kinds of exponential sums [20] for factorization purposes have been published [3,24,39,14,40,10,13,23,22,38,18]. Our method differs from the past experimental realizations [12,11,17,2,37,5,19] in three important simultaneous achievements [26,35,34]. First, the division of N by the test factors ℓ is not pre-calculated, but it is performed by the experiment itself.

Institut für Quantenphysik and Center for Integrated Quantum Science and Technology (IQ^{ST}), Universität Ulm, Albert-Einstein-Allee 11, D-89081 Ulm, Germany
Tel.: +49 (731) 50-22781
Fax: +49 (731) 50-23086
E-mail: vincenzo.tamma@uni-ulm.de

Second, several test factors are tested simultaneously. Third, a scaling property inherent in the recorded interferograms allows us to obtain the factors of an exponential number of large integers.

The core of Shor's factoring algorithm stands on the measurement of the periodicity in the dominant maxima of the quantum probability distribution at the output of a quantum computer [15]. In line with Shor's idea, the key behind the algorithm we present in this paper stands in the measurement of the periodicity in the maxima of Continuous Truncated Exponential Sums (CTES) by performing first-order "factoring" interference processes with a physical system. Interestingly, the number n of necessary experimental runs scales logarithmically with respect to the largest integer to be factored. A noteworthy theoretical result at the core of the algorithm is that the periodicity of the resulting n interference patterns as a function of a continuous physical parameter in a given range, when appropriately scaled, allows us to achieve factorization of large numbers by simply looking at the interference maxima at integer values.

The paper is organized in the following way. In section II will be given some mathematical background about CTES in connection with the hyperbolic function. In section III we will describe the factoring algorithm for a generic physical system and the conditions this system must satisfy. We will provide a generalization of the described algorithm in Section IV. Section V and VI will address final remarks and perspectives of extensions to polynomial scaling methods of factorization, respectively.

2 Hyperbolic function, CTES periodicity and factorization

We define a continuous truncated exponential sum (CTES) in the form [26,35,34,28]

$$\mathscr{I}^{(M,j)}(\xi) \equiv |s^{(M,j)}(f(\xi))|^2, \tag{1}$$

where $s^{(M,j)}$ is the modulo-squared value of the generalized curlicue function [1,26, 28]

$$s^{(M,j)}(\zeta) \equiv \left| \frac{1}{M} \sum_{m=1}^{M} \exp\left[2\pi i (m-1)^j \zeta\right] \right|^2 \tag{2}$$

of integer order $j \geq 1$, with $M \geq 2$ interfering terms, and

$$f(\xi) \equiv \frac{1}{\xi} \tag{3}$$

is the hyperbolic function with continuous variable $0 \leq \xi \leq 1$.

In Fig. 1, we represent the modulo squared of the curlicue function $s^{(M,j)} = s^{(M,j)}(\zeta)$ in its dependence on the argument ζ for $M = 3,4,5$ and $j = 1,2,3$. We note that $|s^{(M,j)}|^2$ has, for all the orders j, a dominant maximum at $\zeta = 0$ with $s^{(M,j)}(0) = 1$ and decaying oscillations on the sides. The higher the order j and the truncation parameter M of the curlicue function are, the larger is the number of decaying oscillations on the sides and the sharper is the dominant peak. Moreover, we recognize

from Eq. (2) the periodicity property $s^{(M,j)}(\zeta+1)=s^{(M,j)}(\zeta)$. Therefore, it suffices to consider $s^{(M,j)}=s^{(M,j)}(\zeta)$ in the domain $-1/2\leq\zeta\leq 1/2$. In addition, $|s^{(M,j)}(\zeta)|^2$ is symmetric with respect to $\zeta=0$.

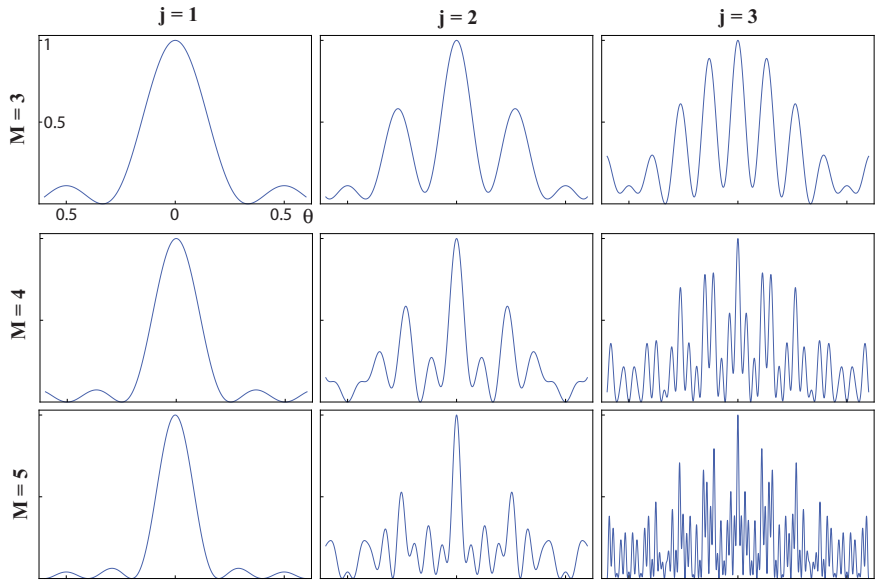

Fig. 1 Modulo-squared value $s_M^{(j)}$ of the generalized curlicue function in its dependence on the argument ζ for the number $M=3,4,5$ of interfering waves (column) and the power $j=1,2,3$ of the phase shift (row). For increasing M the dominant peak becomes narrower, which will make it easier in our algorithm to check if a peak corresponds to a factor or not. Unfortunately, at the same time the number of side maxima increases as well. However, we note that for a fixed j and increasing M the value of the maxima of second order decreases and $s_M^{(j)}$ becomes sharper. On the other hand, for a fixed M but increasing j the value of the maxima of second order increases and $s_M^{(j)}$ becomes wider [28].

The hyperbolic function f in Eq. (3) induces in the function $\mathscr{I}^{(M,j)}$ a notable periodicity. Indeed, the function $\mathscr{I}^{(M,j)}$ is characterized by dominant maxima, which repeat each time f assumes integer values.

Why does such a CTES periodicity matter in factorization?

In order to answer this question we first point out that, as shown in Refs. [26, 34, 28], the factorization problem could be, in principle, solved if we can achieve the complete knowledge of the hyperbolic function f.

Indeed, if we look at f as a function of the new variable ξ_N obtained by the scaling relation

$$\xi_N \equiv N\xi, \tag{4}$$

we obtain

$$f(\xi_N) = \frac{N}{\xi_N}. \tag{5}$$

For each possible value of N, the factors are given by the integer values $\xi_N = \ell$ such that

$$f(\ell) = \frac{N}{\ell} = k, \tag{6}$$

with k a positive integer.

Unfortunately, it is not an easy task to compute the hyperbolic function so that for any given integer N the condition (6) can be verified in order to identify the factors.

Interestingly, we can exploit the constructive/destructive periodic interference characterizing the CTES function in Eq. (1) as a tool in the distinction between factors and non factors of any given number N. In particular, the rescaled hyperbolic function $f(\xi_N)$ in Eq. (5) corresponds to the rescaled CTES

$$\mathscr{I}^{(M,j)}(\xi_N) = \left| \frac{1}{M} \sum_{m=1}^{M} \exp\left[2\pi i (m-1)^j f(\xi_N)\right] \right|^2 \tag{7}$$

as a function of $\xi_N \equiv N\xi$. The condition (6) leads to total constructive interference in the rescaled CTES function $\mathscr{I}^{(M,j)}(\xi_N)$ in Eq. (7). Indeed, the factors of an arbitrary number N are the integer values ℓ of ξ_N corresponding to dominant maxima in the function $\mathscr{I}^{(M,j)}$.

In Fig. 2 is simulated the rescaled CTES function in Eq. (7), with $M = 3$, $j = 2$, as a function of the variable $\xi_N \in [330.84, 337.21]$ for the factorization of $N = 111547$. We can see that the two factors $\ell = 331, 337$ (represented by stars) correspond to complete constructive interference. On the other hand, for the other test factors (represented by triangles) there is partially destructive interference. Moreover, there are absolute maxima (represented by points) which do not correspond to integer test factors.

In Fig. 3, instead, we have simulated the CTES function in the case of $j = 3$ for the same value of N and M and the same range of values of ξ_N. As expected, it turns out that as the order j of the exponential sum increases, the peaks associated with the absolute maxima become sharper. On the other hand, the values of the second order maxima in the interference pattern increase for larger orders j. In order to suppress such maxima, it is necessary to increase the number of terms M in the sum. Also, in such a case, the first order peaks become increasingly sharper.

If we consider the range of values of ξ_N in Fig. 2 and Fig. 3, the closer a non factor is to a factor, the larger the corresponding value is of the rescaled CTES function. Of course, if we move to integer values of ξ_N farther from the factors there is a larger probability of partial or total destructive interference between the terms in the CTES function. This makes the distinction between factors and non factors easier.

In general, the maximum possible step $\Delta\xi$ between consecutive values of ξ where the CTES has to be computed can not be exactly determined since it depends on the

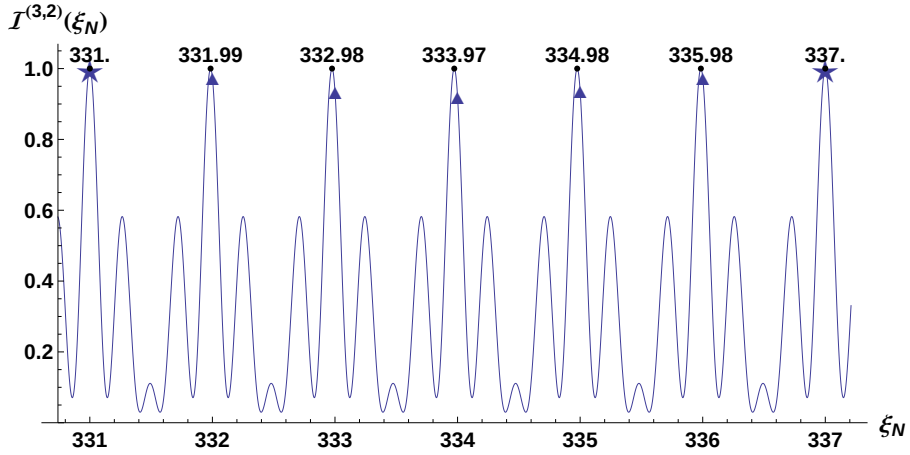

Fig. 2 Rescaled CTES (j=2) function $\mathscr{I}^{(M,j)}(\xi_N)$ in Eq. (7) with $M = 3$ for $N = 111547$, as a function of the variable $\xi_N \equiv N\xi$ in the interval $[330.84, 337.21]$ [35]. We can see that the two factors $\xi_N = 331, 337$, represented by stars, correspond to complete constructive interference, with respect to the other integer trial factors $\xi_N = 332, 333, 334, 335, 336$, represented by triangles, which present partially destructive interference.

value of the factors of the integer $N \leq N_A Amax$ to be factored. However, it can be easily shown [26] that such value is included in the interval

$$N^{-2} < \Delta\xi < 1 \tag{8}$$

if $\xi_N \in [1, \sqrt{N}]$, or the interval

$$\sqrt{N^{-3}} < \Delta\xi < 1 \tag{9}$$

if $\xi_N \in [\sqrt{N}, N]$.

In conclusion, the CTES function in Eq. (1) allows us to extract the information about factors encoded by its periodicity in the dominant maxima. Such a periodicity is imprinted by its functional dependence on the hyperbolic function $f(\xi) \equiv 1/\xi$. We recognize all the values ξ corresponding to an integer value of $f(\xi) \equiv 1/\xi$ as dominant maxima in the interference pattern. When for one of these values of ξ we find, for a given large number N, $\xi_N \equiv N\xi$ be an integer, such an integer is a factor of N.

However, a digital implementation of the CTES function for factoring purposes would rely on performing an exponential number of divisions, which are expensive operations for digital computers. On the other hand, an analogue implementation of such a "factoring" function would rely on the help of "nature" to perform such divisions for us. In the next section, we will describe the prerequisites for a generic physical system to compute a factoring algorithm based on the implementation of CTES interferograms.

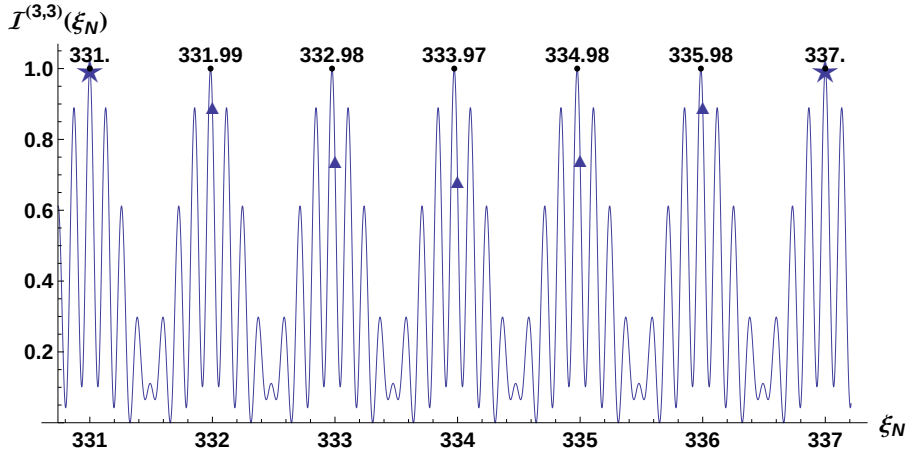

Fig. 3 Rescaled CTES (j=3) function $\mathscr{I}^{(M,j)}(\xi_N)$ in Eq. (7) with $M=3$ for $N=111547$, as a function of the variable $\xi_N \equiv N\xi$ in the interval $[330.84, 337.21]$ [35]. The two factors $\xi_N = 331, 337$, represented by stars, correspond to complete constructive interference, with respect to the other integer trial factors $\xi_N = 332, 333, 334, 335, 336$ in such an interval, represented by triangles. As expected, the peaks associated with the absolute maxima in the case $j=3$ are sharper than the respective peaks in the case $j=2$ represented in Fig. 2. On the other hand, the value of the maxima of second order in the function $\mathscr{I}^{(M,j)}$ increases at the increasing of the order j.

3 Factoring analogue algorithm

In the previous section we have shown how the implementation of the CTES function $\mathscr{I}^{(M,j)}(\xi)$ in Eq. (1) would allow, in principle, the prime number decomposition of arbitrary integers. Now, we want to describe the analogue implementation of the CTES algorithm with a generic physical system that exploits interference. This will lead us to the introduction of a two-dimensional interferogram $I^{(M,j)}(o_\xi; x) \equiv \mathscr{I}^{(M,j)}(\xi)$ as a function of a continuous physical parameter $o_\xi \equiv \xi x$ and a discrete physical parameter x associated with two independent observables O_ξ and O_x, respectively. In the second paper of this series [25] we will give an example of an "optical computer" based on a multi-path Mach Zehnder interferometer, where the physical parameter o_ξ and x will correspond to the wavelengths associated with the spectrum of the optical source and the optical-path unit, respectively.

We will first introduce a CTES "factoring" procedure which takes advantage of a single interferogram $I^{(M,j)}(o_\xi; x)$ associated with a given value of x. We will determine the range $N_{min} \leq N \leq N_{max}$ of factorable numbers N by covering all the trial factors in either the range $[1, \sqrt{N}]$ or $[\sqrt{N}, N]$ with a given range $o_{min} \leq o_\xi \leq o_{max}$ of values of the observable O_ξ [26].

Next, we will show that the CTES "factoring" algorithm can exploit the degree of freedom in the variable x of the analogue function $I^{(M,j)}(o_\xi; x)$ in order to check all the necessary trial factors of an exponential number of large integers N [26]. In par-

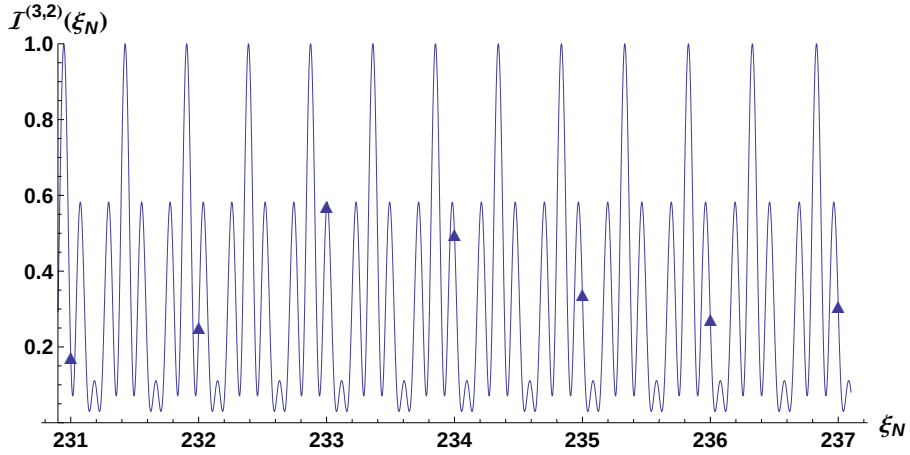

Fig. 4 Rescaled CTES ($j = 2$) function $\mathscr{I}^{(M,j)}(\xi_N)$ in Eq. (7) with $M = 3$ for $N = 111547$, as a function of the variable $\xi_N \equiv N\xi$ in the interval $[230.9, 237.1]$. We can clearly see that all the integer trial factors $\xi_N = 231, 232, 233, 234, 235, 236, 237$ in such a range, represented by triangles, correspond to a relatively small value of the CTES function with respect to the dominant maxima so they can be easily disregarded as possible factors.

ticular, such a procedure is based on the measurement of the periodicity of a number n of interferograms for different suitable values of x. We will interestingly find that the value of n scales logarithmically with respect to the largest number N_{max} to be factored.

3.1 Analogue implementation of the CTES function

We have shown that the implementation of a CTES function in Eq. (1) would allow the factorization, in principle, of arbitrary numbers. Unfortunately, the calculation of such a sum would require an exponential number of divisions associated with the computation of the function $f(\xi)$. On a digital computer, for which division is a rather costly process, such a computation turns out to be very slow. Therefore, it would be more efficient to reproduce the CTES function with an analogue technique in order to solve the problem quickly. More explicitly, an analogue implementation of the CTES algorithm is possible if there is a physical system able to compute divisions for us and then read out the factors by taking advantage of the interference process leading to CTES interferograms.

In particular such a physical system needs to fulfill three main requirements.

First, we assume that the system is characterized by two independent observables O_x and O_ξ. The observable O_x can be tuned to values

$$o_x^{(m,j)} \equiv (m-1)^j x, \tag{10}$$

with j a positive integer and $m = 1, ..., M$. The unit of measurement x can be, in principle, arbitrarily varied. On the other hand, the observable O_ξ assumes a continuous range of values

$$o_\xi \equiv \xi x, \tag{11}$$

where x is the unit of measurement chosen in Eq. (10).

Second, the physical system needs to be able to compute the hyperbolic function in Eq. (3) in the form of ratios between the values of O_x and O_ξ for a given interval of the variable ξ.

Third, the system must be able to exploit interference in order to reproduce the interferogram

$$I^{(M,j)}(o_\xi; x) \equiv \left| \frac{1}{M} \sum_{m=1}^{M} \exp\left[i \frac{o_x^{(m,j)}}{o_\xi} \right] \right|^2 \equiv \mathscr{I}^{(M,j)}(\xi) \tag{12}$$

as a function of $o_\xi \equiv \xi x$. Of course, for a parallel evaluation of the sum for several values of ξ it is necessary that the system contains at the same time the information about all the possible values of the physical observable O_ξ. The corresponding CTES function $\mathscr{I}^{(M,j)}(\xi)$ in Eq. (1) will finally allow us to extract the information about factors.

In particular, for a generic value of the number N to be factored, it is possible to look at the obtained interferogram in Eq. (12) as a function of the rescaled variable in Eq. (4)

$$\xi_N \equiv N\xi = \frac{N}{x} o_\xi, \tag{13}$$

where we use Eq. (11) in the second equality.

Indeed, we obtain the rescaled interferogram

$$I^{(M,j)}(\xi_N; x) \equiv \mathscr{I}^{(M,j)}(\xi_N) \tag{14}$$

corresponding to the rescaled CTES function $\mathscr{I}^{(M,j)}(\xi_N)$ defined in Eq. (7).

Each time there is a dominant maximum at a value of o_ξ for which ξ_N in Eq. (13) is an integer, we find such an integer to be a factor of N.

It is important to point out that the information about the one-dimensional CTES function $\mathscr{I}^{(M,j)}(\xi)$ in Eq. (1) is inferred by the two-dimensional CTES interferogram $I^{(M,j)}(o_\xi; x)$ in Eq. (12) as a function of the physical variable o_ξ and the physical parameter x. Indeed, as becomes clear later, this feature will turn out to be one of the key points to understand the working principle behind the CTES analogue algorithm.

3.2 Factorization with a single interferogram

In this section, we describe the "factoring" procedure based on the use of a single interferogram given by the CTES analogue function $I^{(M,j)}(o_\xi;x)$ in Eq. (12) recorded at a given value of x. We address the question of the interval $N_{min,x} \le N \le N_{max,x}$ of numbers N factorable by covering all the trial factors in either the range $[3,\sqrt{N}]$ [1] or $[\sqrt{N},N]$ with a given range $o_{min} \le o_\xi \le o_{max}$ of values for the observable O_ξ.

In general, for each integer N a generic trial factor ℓ can be checked only if

$$\xi_N = \ell \in [\xi_N^{(min)}, \xi_N^{(max)}] \equiv [\frac{N}{x}o_{min}, \frac{N}{x}o_{max}], \tag{15}$$

where $\xi_N^{(min)}$ and $\xi_N^{(max)}$ are respectively the smallest and largest values that the variable ξ_N in Eq. (13) can assume for the rescaled interferogram $I^{(M,j)}(\xi_N;x)$.

We consider the case in which we want to check all the trial factors $\ell \in [3,\sqrt{N}]$ leading from Eq. (15) to the condition

$$\text{Method (1): } \xi_N = \ell \in [3,\sqrt{N}] \subseteq [\frac{N}{x}o_{min}, \frac{N}{x}o_{max}]. \tag{16}$$

By dividing the upper and lower bounds of each interval respectively by $\sqrt{N}$ and 3 we find

$$1 \in [\frac{N}{3x}o_{min}, \frac{\sqrt{N}}{x}o_{max}], \tag{17}$$

which implies

$$\frac{N}{3x}o_{min} \le 1 \le \frac{\sqrt{N}}{x}o_{max} \tag{18}$$

for each integer N in the interval $N_{min,x} \le N \le N_{max,x}$ to be determined. By squaring the third term in this series of inequalities we obtain the condition

$$x \le x^{(1)} \equiv \frac{3o_{max}^2}{o_{min}}, \tag{19}$$

giving an upper bound to the choice of the parameter x associated with the rescaled interferogram $I^{(M,j)}(\xi_N;x)$ independent of the number N to factorize. From Eq. (18) we also easily obtain [2]

$$N_{max,x}^{(1)} \equiv \left\lfloor \frac{3x}{o_{min}} \right\rfloor$$
$$\text{and}$$
$$N_{min,x}^{(1)} \equiv \left\lceil \frac{x^2}{o_{max}^2} \right\rceil, \tag{20}$$

[1] We are sure that there is at least one factor of N in such interval. The trial factor 2 is obviously excluded since it is easy to recognize if N is an even integer.

[2] We recall that for any real number y the ceiling $\lceil y \rceil$ is the smallest integer larger than x, while the floor $\lfloor y \rfloor$ is the largest integer lower than y.

defining the interval of factorable numbers with a single interferogram associated with a given value x in Eq. (19) in the range $o_{min} \leq o_{\xi} \leq o_{max}$.

In the particular case of an interferogram recorded at the maximum possible value $x = x^{(1)}$ in Eq. (19), the condition (18) reads

$$\frac{N}{3x^{(1)}} o_{min} = \frac{\sqrt{N}}{x^{(1)}} o_{max} = 1.$$

If o_{max}/o_{min} is an integer, we find the largest but also the only integer

$$N^{(1)} \equiv \frac{9o_{max}^2}{o_{min}^2} \tag{21}$$

factorable by using a single experimental interferogram $I^{(M,j)}(o_{\xi};x)$ in Eq. (12) recorded for the value $x = x^1$.

We consider now the second method in which we want to check all the trial factors $\xi_N = \ell \in [\sqrt{N}, N]$ leading from Eq. (15) to the condition

$$\text{Method (2): } \xi_N = \ell \in [\sqrt{N}, N] \subseteq [\frac{N}{x} o_{min}, \frac{N}{x} o_{max}]. \tag{22}$$

By dividing the lower bound and the upper bound of each interval by $\sqrt{N}$ and N, respectively, we find

$$1 \in [\frac{\sqrt{N}}{x} o_{min}, \frac{o_{max}}{x}], \tag{23}$$

which implies

$$1 \geq \frac{\sqrt{N}}{x} o_{min} \leq \frac{o_{max}}{x} \geq 1 \tag{24}$$

for each integer N in the interval $N_{min,x} \leq N \leq N_{max,x}$ to be determined. From the last inequality in Eq. (24) we obtain the condition

$$x \leq x^{(2)} \equiv o_{max}. \tag{25}$$

From Eq. (24) we also easily obtain

$$N_{max,x}^{(2)} \equiv \left\lfloor \frac{x^2}{o_{min}^2} \right\rfloor$$
$$\text{and}$$
$$N_{min}^{(2)} \equiv 1, \tag{26}$$

defining the interval of factorable numbers with a single interferogram associated with the generic value x in Eq. (25) for the given range $o_{min} \leq o_{\xi} \leq o_{max}$.

We consider now the case of a single interferogram recorded at the maximum value $x = x^{(2)} \equiv o_{max}$ in Eq. (25) leading to the largest interval

$$N_{min}^{(2)} \equiv 1 \leq N \leq N_{max}^{(2)} \equiv \left\lfloor \frac{o_{max}^2}{o_{min}^2} \right\rfloor \tag{27}$$

of factorable integers.

We finally demonstrate that with a single interferogram it is possible to factorize a number

$$\Delta N \sim N_{max} \sim \frac{o_{max}^2}{o_{min}^2} \sim 2^{n_{max}}$$

of integers exponential with respect to the number of binary digits n_{max} associeted with N_{max}. However, in general, the largest factorable integer N_{max} is limited by the value o_{max}/o_{min} associated with the physical system. For this reason, in the next section we will describe a factorization procedure which takes advantage of several interferograms $I^{(M,j)}(o_\xi;x)$ in Eq. (12) at different values x in order to factor numbers exploiting a limited fixed range of values o_ξ of a physical observable O_ξ. In such a method, the maximum factorable number N_{max} will depend only on the largest value achievable for the parameter x.

3.3 Factorization with a sequence of interferograms

So far we have restricted ourselves to a factorization method involving a single interferogram $I^{(M,j)}(o_\xi;x)$ in Eq. (12) defined at a fixed value of the parameter x. However, the remarkable scaling property $\xi_N \equiv No_\xi/x$ characterizing the function $I^{(M,j)}(o_\xi;x)$ allows us to vary the physical values of both o_ξ and x. This implies that we can, in principle, change arbitrarily both the number N we are looking at and the relative trial factors to check by simply varying these two physical "knobs".

In particular, we seek to address the question of the largest number N_{max} that can be factored by measuring several interferograms $I^{(M,j)}(o_\xi;x)$ corresponding to different values of x in a fixed domain $o_{min} \le o_\xi \le o_{max}$ of the variable o_ξ.

3.3.1 Factorization of a single integer N

We consider first the case of a single generic large integer N to be factored. The scaling property $\xi_N \equiv No_\xi/x$, written as $N \equiv \xi_N x/o_\xi$, implies that, in principle, there is no limit to the largest possible value of N if we can vary the unit x up to arbitrary large values. Of course, in practice, the maximum achievable value of x is limited by the particular physical system we are using. We now demonstrate that the number n of values of x, for which the "factoring" interferogram $I^{(M,j)}(o_\xi;x)$ in Eq. (12) must be recorded, scales logarithmically with respect to the value of N.

It should first be pointed out that a single interferogram registered at a given value x allows us to check only the trial factors

$$\xi_N = \ell \in [\xi_N^{(min)}, \xi_N^{(max)}] \equiv [\frac{N}{x}o_{min}, \frac{N}{x}o_{max}], \tag{28}$$

which, in general, for the fixed domain $o_{min} \le o_\xi \le o_{max}$ of values o_ξ, may correspond only to a subset of the total range $3 \le \ell \le \sqrt{N}$ or $\sqrt{N} \le \ell \le N$ of values $\xi_N = \ell$ we would need to cover in order to factor a generic integer N. For this reason, we

consider a suitable sequence of values $x = x_i$, with $i = 0, 1, ..., n-1$. Each interferogram registered at the value $x = x_i$, with $i = 0, 1, ..., n-1$, allows us from Eq. (28) to cover all the trial factors

$$\xi_N = \ell \in [\xi_{N,i}, \xi_{N,i+1}] \equiv [\frac{N}{x_i} o_{min}, \frac{N}{x_i} o_{max}], \tag{29}$$

with $i = 0, 1, ..., n-1$, where

$$\xi_{N,i+1} \equiv \frac{N}{x_i} o_{max} \equiv \frac{N}{x_{i+1}} o_{min} \tag{30}$$

satisfies the condition for consecutive intervals.

This implies that the sequence x_i, with $i = 0, ..., n-1$, associated with the n interferograms is defined by the condition

$$x_{i+1} \equiv \frac{x_i}{c} < x_i, \tag{31}$$

with

$$c \equiv \frac{\xi_{N,i+1}}{\xi_{N,i}} = \frac{o_{max}}{o_{min}} > 1 \tag{32}$$

and, from Eq. (29),

$$\frac{x_0}{o_{min}} \equiv \frac{N}{\xi_{N,0}}. \tag{33}$$

From Eq. (32) we obtain

$$\xi_{N,n} = c^n \xi_{N,0}, \tag{34}$$

leading to the number

$$n \equiv log_c \frac{\xi_{N,n}}{\xi_{N,0}} \tag{35}$$

of interferograms necessary to cover all the trial factors

$$\xi_N = \ell \in [\xi_{N,0}, \xi_{N,n}] \equiv [\frac{N o_{min}}{x_0}, \frac{N o_{min}}{x_0} \, c^n]. \tag{36}$$

We deduce that the value x_0 for the first interferogram as well as the total number n of interferograms $I^{(M,j)}(o_\xi; x)$ depend on the integer N to be factored and on the associated interval $[\xi_{N,0}, \xi_{N,n}]$ of trial factors to be checked. In particular, factorization can be achieved for a generic integer N only if

$$\text{Method } (1): \tag{37}$$
$$\xi_N = \ell \in [3, \sqrt{N}] \subseteq [\xi_{N,0}, \xi_{N,n}] \equiv [\frac{N o_{min}}{x_0}, \frac{N o_{min}}{x_0} \, c^n]$$

or

$$\text{Method } (2): \tag{38}$$
$$\xi_N = \ell \in [\sqrt{N}, N] \subseteq [\xi_{N,0}, \xi_{N,n}] \equiv [\frac{No_{min}}{x_0}, \frac{No_{min}}{x_0}\ c^n].$$

Let us consider first the method (1). The lowest trial factor 3 to be checked leads to the condition

$$\xi_{N,0} \equiv \frac{No_{min}}{x_0} \leq 3, \tag{39}$$

implying

$$\frac{x_0}{o_{min}} \geq \frac{x_{0N}^{(1)}}{o_{min}} \equiv \frac{N}{3}. \tag{40}$$

In an analogous way, the value $\sqrt{N}$ of the largest trial factor to be checked in Eq. (37) determines the condition

$$\xi_{N,n} \equiv \frac{No_{min}}{x_0}\ c^n \geq \sqrt{N}. \tag{41}$$

This, together with Eq. (40), implies the minimum number

$$\begin{aligned} n_{N,x_0}^{(1)} &\equiv \left\lceil log_c \frac{x_0}{o_{min}\sqrt{N}} \right\rceil \\ &\leq \left\lceil log_c \frac{\sqrt{N}}{3} \right\rceil \equiv n_{N,min}^{(1)} \end{aligned} \tag{42}$$

of necessary interferograms $I^{(M,j)}(o_\xi; x_i)$, with $i = 0, 1, ..., n-1$, to factor a generic integer N with the method (1).

We consider now the method (2) in Eq. (38). The lowest trial factor $\sqrt{N}$ to be checked leads to the condition

$$\xi_{N,0} \equiv \frac{No_{min}}{x_0} \leq \sqrt{N}, \tag{43}$$

which implies

$$\frac{x_0}{o_{min}} \geq \frac{x_{0N}^{(2)}}{o_{min}} \equiv \sqrt{N}. \tag{44}$$

In an analogous way, the value N of the largest trial factor to be checked in Eq. (38) determines the condition

$$\xi_{N,n} \equiv \frac{No_{min}}{x_0}\ c^n \geq N. \tag{45}$$

This, together with Eq. (44), leads to the minimum number

$$n_{x_0}^{(2)} \equiv \left\lceil log_c \frac{x_0}{o_{min}} \right\rceil \geq \left\lceil log_c \sqrt{N} \right\rceil \equiv n_{N,min}^{(2)} \tag{46}$$

of necessary interferograms $I^{(M,j)}(o_\xi;x_i)$, with $i=0,1,...,n-1$, to factor a generic integer N with the method (2).

This demonstrates that, in principle, the number n of interferograms necessary for factorizing an arbitrary large number N, using a given range $[o_{min},o_{max}]$ of the physical variable o_ξ, scales logarithmically with respect to $\sqrt{N}$ and thereby polynomially with respect to the number of binary digits associated with N. It is important to point out that the narrower the range $o_{min}\leq o_\xi\leq o_{max}$ is, the closer the value of c in Eq. (32) is to 1 and thereby the larger is the value of n in Eq. (35). However, it would be enough to cover a spectrum such that $o_{max}\equiv 2o_{min}$ in order to obtain a scaling that is logarithmic (base 2) and thereby polynomial with respect to the number of binary digits associated with N.

3.3.2 Extension to the factorization of an exponential number of integers

So far we have considered the case of factoring a single number with a sequence of n "factoring" interferograms. However, the scaling property $\xi_N\equiv No_\xi/x$ implies, as pointed out before, that we can exploit the same interferograms in order to factor not only a single integer but any integer in any given range $N_{min}\leq N\leq N_{max}$. We determine how, in such a case, the number n of experimental runs depends on the smallest and the largest number N_{min} and N_{max} that can be factored.

In particular, factorization can be achieved for all values of N, with $N_{min}\leq N\leq N_{max}$, only if for each single value is satisfied either the condition (37) for the method (1) or the condition (38) for the method (2). Let us consider first the method (1) in Eq. (37). The condition in Eq. (39) needs to be satisfied for each $N_{min}\leq N\leq N_{max}$, which implies

$$\frac{N_{max}o_{min}}{x_0}\leq 3$$

leading to

$$\frac{x_0}{o_{min}}\geq\frac{x_0^{(1)}}{o_{min}}\equiv\frac{N_{max}}{3}. \tag{47}$$

In an analogous way, the condition in Eq. (41) needs to hold for each $N_{min}\leq N\leq N_{max}$, leading to

$$\frac{o_{min}}{x_0}\,c^n\geq\frac{1}{\sqrt{N_{min}}}.$$

This, together with Eq. (47), implies the minimum number

$$\begin{aligned} n_{x_0}^{(1)} &\equiv \left\lceil log_c\,\frac{x_0}{o_{min}\sqrt{N_{min}}}\right\rceil \\ &\geq \left\lceil log_c\,\frac{N_{max}}{3\sqrt{N_{min}}}\right\rceil\equiv n_{min}^{(1)} \end{aligned} \tag{48}$$

of necessary interferograms $I^{(M,j)}(o_\xi;x_i)$, with $i=0,1,...,n-1$, to factor all the integers N in any given interval $N_{min}\leq N\leq N_{max}$ with the method (1).

We consider now the method (2) in Eq. (38). The condition (43) needs to be satisfied for each $N_{min} \leq N \leq N_{max}$, which implies

$$\frac{o_{min}}{x_0} \leq \frac{1}{\sqrt{N_{max}}}$$

and thereby

$$\frac{x_0}{o_{min}} \geq \frac{x_0^{(2)}}{o_{min}} \equiv \sqrt{N_{max}}. \tag{49}$$

In an equivalent way, Eq. (50) reads

$$n_{x_0}^{(2)} \equiv \left\lceil log_c \frac{x_0}{o_{min}} \right\rceil \geq \left\lceil log_c \sqrt{N_{max}} \right\rceil \equiv n_{min}^{(2)} \tag{50}$$

of necessary interferograms $I^{(M,j)}(o_\xi; x_i)$, with $i = 0, 1, ..., n-1$, to factor all the integers N in any given interval $N_{min} \leq N \leq N_{max}$ with the method (2).

In conclusion, the described algorithm allows in both method (1) and (2) the factorization of an exponential number

$$\Delta N \equiv N_{max} - N_{min} \sim N_{max} \sim 2^{n_{max}}$$

of integers, with n_{max} number of binary digits of N_{max}, by using a polynomial number of interferograms in a given physical domain $[o_{min}, o_{max}]$. The largest factorable number is upper limited by the condition for x_0/o_{min} in Eq. (47) and Eq. (49).

3.3.3 Example of factorization of $N \leq N_{max} \equiv 64$

We now describe the implementation of our factoring algorithm for $N_{max} \equiv 64$. We consider a generic observable O_ξ with values $o_\xi = \xi x$ in a given range $o_{min} \leq o_\xi \leq o_{max}$ which satisfies the condition

$$c \equiv o_{max}/o_{min} = 2. \tag{51}$$

We consider first the method (1) in Eq. (37). It turns out that any integer in the range $N_{min} \equiv 8 \leq N \leq N_{max} \equiv 64$ can be factored, according to Eq. (48), by exploiting

$$n = n_{min}^{(1)} \equiv \left\lceil log_2 \frac{64}{3\sqrt{8}} \right\rceil = 3$$

interferograms $I(o_\xi; x_i^{(1)}) \equiv I^{(M=3,j=2)}(o_\xi; x_i^{(1)})$ defined by Eq. (12), with $i = 1, 2, 3$, where the value $x = x_0^{(1)}$ associated with the first interferogram satisfies the condition in Eq. (47)

$$\frac{x_0^{(1)}}{o_{min}} \equiv \frac{N_{max}}{3} = \frac{64}{3}. \tag{52}$$

From Eq. (13) we can now determine all the values

$$x = x_i^{(1)} \equiv c^{-i} x_0^{(1)} = \frac{64}{3} \cdot 2^{-i} o_{min}, \tag{53}$$

with $i = 0,1,2$, for each of the $n = 3$ interferograms. We assume that our physical system is able to record such interferograms in the range $o_{min} \leq o_\xi \leq 2o_{min}$. In Fig. 5 we simulate these interferograms, which are able to cover all the trial factors in the interval $[3, \sqrt{N}]$ for any integer in the range $N_{min} \equiv 8 \leq N \leq N_{max} \equiv 64$. An example is given for the factorization of $N = 15, 63$ by rescaling the axis o_ξ as a function of ξ_{15} and ξ_{63} according to Eq. (13). The trial factors are marked, respectively, with continuous lines and dashed lines. We find the factors 3 and 5 of 15 corresponding to maxima of the interferogram $I^{(M,j)}(o_\xi; x_2^{(1)})$. On the other hand the factor 3 of 63 is associated with the maximum of the interferogram $I^{(M,j)}(o_\xi; x_0^{(1)})$, while the factors 7 and 9 emerge from the maxima in the interferogram $I^{(M,j)}(o_\xi; x_1^{(1)})$.

We consider now the method (2) in Eq. (38). According to Eq. (50), any integer in the range $N_{min} \equiv 1 \leq N \leq N_{max} \equiv 64$ can be factored by exploiting the same number

$$n = n_{min}^{(2)} \equiv \left\lceil log_2 \sqrt{64} \right\rceil = 3$$

of interferograms $I(o_\xi; x_i^{(2)}) \equiv I^{(M=3,j=2)}(o_\xi; x_i^{(2)})$ defined by Eq. (12), with $i = 1,2,3$, where the value $x = x_0^{(2)}$ associated with the first interferogram satisfies the condition in Eq. (49)

$$\frac{x_0^{(2)}}{o_{min}} \equiv \sqrt{N_{max}} = 8. \tag{54}$$

From Eq. (13) we can now determine all the values

$$x = x_i^{(1)} \equiv c^{-i} x_0^{(1)} = 8 \cdot 2^{-i} o_{min}, \tag{55}$$

with $i = 0,1,2$, for each of the $n = 3$ interferograms. We assume that our physical system covers the spectrum $o_{min} \leq o_\xi \leq 2o_{min}$ of values of a given observable O_ξ. In Fig. 6 we simulate such interferograms, which are able to cover all the trial factors in the interval $[\sqrt{N}, N]$ for any integer in the range $N_{min} \equiv 1 \leq N \leq N_{max} \equiv 64$. We again give an example for the factorization of $N = 15, 63$ by rescaling the axis o_ξ as a function of ξ_{15} and ξ_{63} according to Eq. (13). We find that the factor 3 of 15 corresponds to a maximum of the interferogram $I^{(M,j)}(o_\xi; x_0^{(2)})$, while the factor 5 is associated with a maximum of the interferogram $I^{(M,j)}(o_\xi; x_1^{(2)})$. On the other hand the factor 9 of 63 is associated with the maximum of the interferogram $I^{(M,j)}(o_\xi; x_0^{(2)})$.

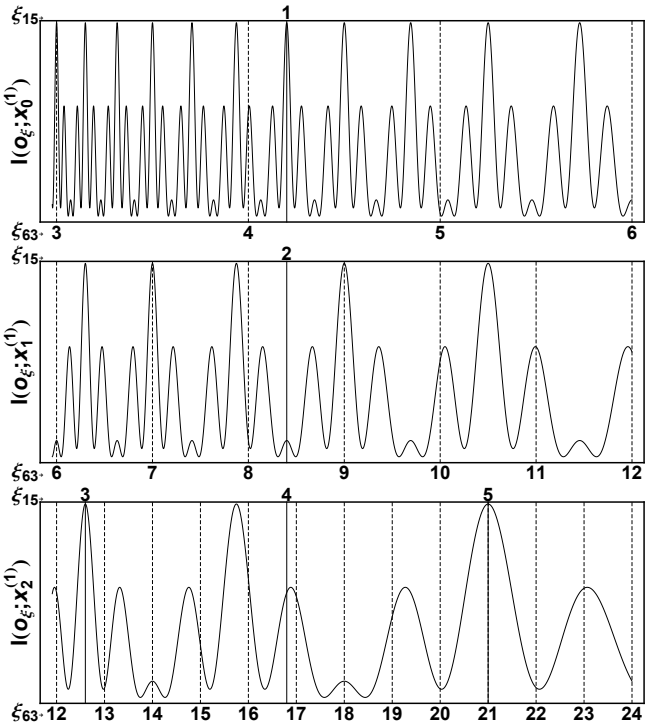

Fig. 5 Factorization of any integer in the range $N_{min} \equiv 8 \leq N \leq N_{max} \equiv 64$ by using the method (1) aimed at checking all the trial factors in the range $[3, \sqrt{N}]$. We exploit $n = 3$ interferograms $I(o_\xi; x_i^{(1)}) \equiv I^{(M=3,j=2)}(o_\xi; x_i^{(1)})$ defined by Eq. (12), with $i = 1,2,3$, where the range of values o_ξ satisfies the condition (51) and the values $x_i^{(1)}$ are given by Eq. (53). We give an example for the factorization of $N = 15,63$ by rescaling the axis o_ξ as a function of ξ_{15} and ξ_{63} according to Eq. (13). The trial factors correspond, respectively, to continuous lines and dashed lines. We find the factors 3 and 5 of 15 corresponding to maxima of the interferogram $I^{(M,j)}(o_\xi; x_2^{(1)})$. On the other hand, the factor 3 of 63 is associated with the maxima of the interferogram $I^{(M,j)}(o_\xi; x_0^{(1)})$, while the factors 7 and 9 emerge from the maxima in the interferogram $I^{(M,j)}(o_\xi; x_1^{(1)})$.

4 Generalization of the CTES algorithm

In this section, we will introduce a generalization of the CTES algorithm. In particular, we generalize the scaling property $\xi_N \equiv N\xi$ defining the new auxiliary variable

$$\xi_{N,s} \equiv s\xi_N \equiv sN\xi, \tag{56}$$

where s is equal to the product of one or more generic prime numbers p_k ($s \equiv \Pi_k p_k$). We can now rescale the CTES function in Eq. (1) as a function of the continuous

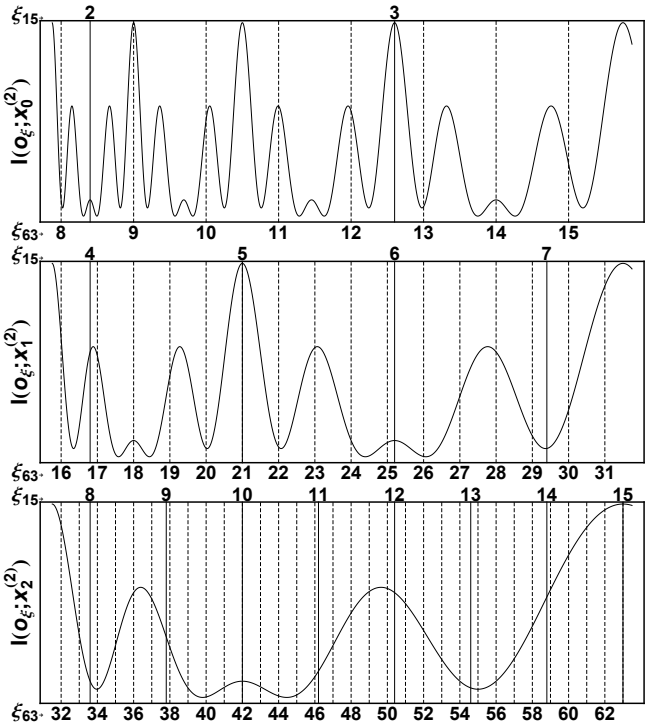

Fig. 6 Factorization of any integer in the range $N_{min} \equiv 1 \leq N \leq N_{max} \equiv 64$ by using the method (2) aimed at checking all the trial factors in the range $[\sqrt{N}, N]$. We exploit $n = 3$ interferograms $I(o_\xi; x_i^{(2)}) \equiv I^{(M=3,j=2)}(o_\xi; x_i^{(2)})$ defined by Eq. (12), with $i = 1,2,3$, where the range of values o_ξ satisfies the condition (51) and the values $x_i^{(2)}$ are given by Eq. (55). We find that the factor 3 of 15 corresponds to a maximum of the interferogram $I^{(M,j)}(o_\xi; x_0^{(2)})$, while the factor 5 is associated with a maxima of the interferogram $I^{(M,j)}(o_\xi; x_1^{(2)})$. On the other hand the factor 9 of 63 is associated with the maximum of the interferogram $I^{(M,j)}(o_\xi; x_0^{(2)})$.

variable $\xi_{N,s}$:

$$\mathscr{I}^{(M,j)}(\xi_{N,s}) = |\frac{1}{M}\sum_{m=1}^{M} \exp\left[2\pi i (m-1)^j \frac{Ns}{\xi_{N,s}}\right]|^2. \tag{57}$$

Let us describe how such a rescaled function allows us to find the factors of a generic number N. If one of the chosen prime numbers p_k that defines the value of s is a factor of N, we have solved the problem. If not, the factors of N are the integer values of $\xi_{N,s}$, different from the prime numbers p_k that correspond to dominant maxima in the rescaled CTES function given by Eq. (57).

In a general analogue implementation, the auxiliary variable $\xi_{N,s}$ in Eq. (56) is obtained by rescaling the values $o_\xi \equiv \xi x$ of the observable O_ξ according to

$$\xi_{N,s} \equiv \frac{sN}{x} o_\xi . \tag{58}$$

Thereby, the range $[\xi_{N,s}^{(min)}, \xi_{N,s}^{(max)}]$ of trial factors covered by the variable $\xi_{N,s}$ can be equivalent to the interval $[\xi_N^{(min)}, \xi_N^{(max)}]$ of trial factors covered by the variable ξ_N by exploiting a range for the variable o_ξ of the physical observable O_ξ of length $\Delta o = o_{max} - o_{min}$ reduced by a factor s. However, at the same time, each of the values $x = x_i$, with $i = 0, 1, ..., n-1$, increases by the same factor s according to the iteration formula (31) where x_0 in Eq. (49) now reads

$$x_0 \equiv sN_{max} o_{min} / \xi_0, \tag{59}$$

with $\xi_0 \equiv 1, \sqrt{N_{min}}$ depending on the range (37) or (38), respectively, of trial factors we are considering. This implies that the maximum factorable integer N_{max} is upper limited by $x_0/(so_{min})$, where x_{max} is the maximum value physically allowed for the parameter x.

5 Remarks

We have described a novel analogue algorithm based on the experimental measurement of CTES interferograms $I^{(M,j)}(o_\xi; x)$ depending on the continuous argument o_ξ and the discrete parameter x associated with two suitable physical observables O_ξ and O_x, respectively. The domain of factorable integers is determined by the range $o_{min} \le o_\xi \le o_{max}$ of the continuous variable o_ξ and by the maximum value x_{max} allowed by the parameter x .

The largest integer N_{max} factorable with a single CTES interferogram $I^{(M,j)}(o_\xi; x)$ associated with a given value of x and defined in a certain range $o_{min} \le o_\xi \le o_{max}$ is upper limited by the value $(o_{max}/o_{min})^2$. For larger integers N the available physical spectrum of observable values o_ξ may not be enough to cover all the trail factors either in the range $1 \le \xi_N \le \sqrt{N}$ or $\sqrt{N} \le \xi_N \le N$. For this reason, we have introduced an algorithm based on the measurement of n different interferograms $I^{(M,j)}(o_\xi; x_i)$, with $i = 0, 1, ..., n-1$, associated with the respective values $x = x_i$. In this case the largest number factorable is upper limited by the value x_{max}/o_{min}. We have demonstrated that the number n of necessary experimental runs scales logarithmically with respect to the root of the number N we want to factor. Very interestingly our method allows a parallel factorization of an exponential number of large integers with respect to the number of binary digits n_{max} associated with N_{max}. These results are very important in view of the optical implementation of the algorithm described in Ref. [25].

Moreover, we have introduced a generalized CTES procedure defined by the scaling property $\xi_{N,s} \equiv sN\xi$, where $s \equiv \Pi_k p_k$ with p_k generic prime numbers which are non factors of N. We have shown that it is possible to reduce for a factor s the length $\Delta o = o_{max} - o_{min}$ of the range of values o_ξ in which the function $I^{(M,j)}(o_\xi; x)$ is

recorded. In such a case, the maximum factorable integer N_{max} is upper limited by $x_0/(so_{min})$.

In Ref. [25], we describe in detail how an optical computer enables a physical computation of the CTES algorithm for several orders j. In such a case the values o_ξ and x defining the analogue interferogram $I^{(M,j)}(o_\xi;x)$ correspond, respectively, to the wavelengths λ of a polychromatic source and to the unit of displacement defining the optical paths in a generalized Michelson interferometer [35]. Indeed, an experimental proof of the principle of the CTES algorithm has been performed in the case of $j=2$ and $j=3$, leading to the factorization of seven-digit numbers [25,34].

6 Towards a polynomial scaling in the number of physical resources

We point out that any "classical" implementation of the algorithm described so far would lack exponential speed-up. Indeed, the largest number factorable N_{max} is upper limited either by the value $(o_{max}/o_{min})^2$ or x_0/o_{min}, depending on the use of a single interferogram or a sequence of interferograms.

Moreover, the accuracy in the variable ξ in Eq. (11)

$$\Delta\xi = \frac{o_\xi}{x^2}\Delta x + \frac{1}{x}\Delta o_\xi \leq \frac{o_{max}}{x^2}\Delta x + \frac{1}{x}\Delta o_\xi$$

depends on the given experimental indeterminations Δo_ξ and Δx associated with the measurement of the observables O_ξ and O_x, respectively. This shows from Eqs. (8) and (9) that the unit x defining the CTES interferograms in Eq. (12) needs to grow exponentially with respect to the number of bits associated with the largest number N_{max} in the interval of integers to be factored.

The ability to resolve the maxima associated with factors from non factors for larger and larger integers N [26] can be, in general, improved by implementing "factoring" interferograms of either a larger order j or with a larger number M of interfering terms as can be inferred by the relative curlicue functions in Fig. 1.

Ultimately, only a "quantum" system able to encode such physical observables in a qubit representation in line with Shor's algorithm would make it possible to avoid the requirement of exponentially large values for the observable O_x. In particular, a crucial role in our algorithm is played by the hyperbolic function $f(\xi)$ in Eq. (3) emerging from the ratio of the values o_x and o_ξ and characterizing the "factoring" CTES interferograms in Eq. (12). A "qubit" parallel representation of functions analogous to the curlicue function may lead to novel factoring algorithms based on a polynomial number of resources. Moreover, multi-photon quantum interference [32, 6,30,31,33,29,27,4] may serve as an efficient tool to distinguish factors from non factors.

Acknowledgements We thank H. Zhang, X. He, Y.H. Shih and W. P. Schleich for their contributions on this topic and J. Franson, M. Freyberger, A. Garuccio, S. Lomonaco, R. Meyers, T. Pittman and M. H. Rubin for many fruitful discussions.

References

1. Berry, M.: Random renormalization in the semiclassical long-time limit of a precessing spin. Physica D, **33**, 26–33 (1988)
2. Bigourd, D., Chatel, B., Schleich, W.P., Girard, B.: Factorization of Numbers with the Temporal Talbot Effect: Optical Implementation by a Sequence of Shaped Ultrashort Pulses. Phys. Rev. Lett. **100**, 030,202 (2008). DOI 10.1103/PhysRevLett.100.030202. URL http://link.aps.org/doi/10.1103/PhysRevLett.100.030202
3. Clauser, J.F., Dowling, J.P.: Factoring integers with Youngs N-slit interferometer. Physical Review A **53**(6), 45874590 (1996). DOI 10.1103/physreva.53.4587. URL http://dx.doi.org/10.1103/PhysRevA.53.4587
4. D'Angelo, M., Garuccio, A., Tamma, V.: Toward real maximally path-entangled *N*-photon-state sources. Phys. Rev. A **77**, 063,826 (2008). DOI 10.1103/PhysRevA.77.063826. URL http://link.aps.org/doi/10.1103/PhysRevA.77.063826
5. Gilowski, M., Wendrich, T., Müller, T., Jentsch, C., Ertmer, W., Rasel, E.M., Schleich, W.P.: Gauss sum factorization with cold atoms. Phys. Rev. Lett. **100**, 030,201 (2008). DOI 10.1103/PhysRevLett.100.030201. URL http://link.aps.org/doi/10.1103/PhysRevLett.100.030201
6. Laibacher, S., Tamma, V.: From the physics to the computational complexity of multiboson correlation interference. Phys. Rev. Lett. (2015). In press
7. Lanyon, B.P., Weinhold, T.J., Langford, N.K., Barbieri, M., James, D.F.V., Gilchrist, A., White, A.G.: Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement. Phys. Rev. Lett. **99**, 250,505 (2007). DOI 10.1103/PhysRevLett.99.250505. URL http://link.aps.org/doi/10.1103/PhysRevLett.99.250505
8. Lomonaco, S.: Quantum Computation: A Grand Mathematical Challenge for the Twenty-first Century and the Millennium : American Mathematical Society, Short Course, January 17-18, 2000, Washington, DC. No. del 3 in AMS short course lecture notes. American Mathematical Society (2002). URL https://books.google.de/books?id=nIjHCQAAQBAJ
9. Lu, C.Y., Browne, D.E., Yang, T., Pan, J.W.: Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits. Phys. Rev. Lett. **99**, 250,504 (2007). DOI 10.1103/PhysRevLett.99.250504. URL http://link.aps.org/doi/10.1103/PhysRevLett.99.250504
10. Mack, H., Bienert, M., Haug, F., Freyberger, M., Schleich, W.: Wave Packets Can Factorize Numbers. Phys. Stat. Sol. (b) **233**(3), 408415 (2002). DOI 10.1002/1521-3951(200210)233:3⟨408::aid-pssb408⟩3.0.co;2-n. URL http://dx.doi.org/10.1002/1521-3951(200210)233:3<408::AID-PSSB408>3.0.CO;2-N
11. Mahesh, T.S., Rajendran, N., Peng, X., Suter, D.: Factorizing numbers with the Gauss sum technique: NMR implementations. Physical Review A **75**(6), 062,303 (2007). DOI 10.1103/physreva.75.062303. URL http://dx.doi.org/10.1103/PhysRevA.75.062303
12. Mehring, M., Mller, K., Averbukh, I.S., Merkel, W., Schleich, W.P.: NMR Experiment Factors Numbers with Gauss Sums. Phys. Rev. Lett. **98**(12), 120,502 (2007). DOI 10.1103/physrevlett.98.120502. URL http://dx.doi.org/10.1103/PhysRevLett.98.120502
13. Merkel, W., Averbukh, I., Girard, B., Paulus, G., Schleich, W.: Factorization of numbers with physical systems. Fortschritte der Physik **54**(8-10), 856865 (2006). DOI 10.1002/prop.200610315. URL http://dx.doi.org/10.1002/prop.200610315
14. Merkel, W., Wölk, S., Schleich, W.P., Averbukh, I.S., Girard, B., Paulus, G.G.: Factorization of numbers with Gauss sums: II. Suggestions for implementation with chirped laser pulses. New Journal of Physics **13**(10), 103,008 (2011). URL http://stacks.iop.org/1367-2630/13/i=10/a=103008
15. Mermin, N.D.: Quantum Computer Science. Cambridge University Press (2007)
16. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge Series on Information and the Natural Sciences. Cambridge University Press (2000). URL http://books.google.de/books?id=65FqEKQOfP8C
17. Peng, X., Suter, D.: NMR implementation of factoring large numbers with Gauss sums: Suppression of ghost factors. Europhys. Lett. **84**(4), 40,006 (2008). DOI 10.1209/0295-5075/84/40006. URL http://dx.doi.org/10.1209/0295-5075/84/40006
18. Rangelov, A.A.: Factorizing numbers with classical interference: several implementations in optics. Journal of Physics B: Atomic, Molecular and Optical Physics **42**(2), 021,002 (2009). URL http://stacks.iop.org/0953-4075/42/i=2/a=021002

19. Sadgrove, M., Kumar, S., Nakagawa, K.: Enhanced Factoring with a Bose-Einstein Condensate. Phys. Rev. Lett. **101**, 180,502 (2008). DOI 10.1103/PhysRevLett.101.180502. URL http://link.aps.org/doi/10.1103/PhysRevLett.101.180502
20. Schleich, W., Maier, H.: Prime Numbers 101: A Primer on Number Theory. Wiley (2014). URL https://books.google.de/books?id=EEiaGQAACAAJ
21. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J.Sci.Statist.Comput. **26**, 1484 (1997)
22. Stefanak, M., Haase, D., Merkel, W., Zubairy, M.S., Schleich, W.P.: Factorization with exponential sums. Journal of Physics A: Mathematical and Theoretical **41**(30), 304,024 (2008). URL http://stacks.iop.org/1751-8121/41/i=30/a=304024
23. Stefanak, M., Merkel, W., Schleich, W.P., Haase, D., Maier, H.: Factorization with Gauss sums: scaling properties of ghost factors. New Journal of Physics **9**(10), 370 (2007). URL http://stacks.iop.org/1367-2630/9/i=10/a=370
24. Summhammer, J.: Factoring and Fourier transformation with a Mach-Zehnder interferometer. Physical Review A **56**(5), 43244326 (1997). DOI 10.1103/physreva.56.4324. URL http://dx.doi.org/10.1103/PhysRevA.56.4324
25. Tamma, V.: Analogue algorithm for parallel factorization of an exponential number of large integers: II. Optical Implementation. Quantum Information Processing **11128**, 1189 (2015)
26. Tamma, V.: Theoretical and experimental study of a new algorithm for factoring numbers. Ph.D. thesis, University of Maryland, Baltimore County (2010). ProQuest
27. Tamma, V.: Sampling of bosonic qubits. International Journal of Quantum Information **12**, 1560,017 (2014). DOI 10.1142/S0219749915600175
28. Tamma, V., Alley, C.O., Schleich, W.P., Shih, Y.H.: Prime Number Decomposition, the Hyperbolic Function and Multi-Path Michelson Interferometers. Found Phys **42**(1), 111121 (2010). DOI 10.1007/s10701-010-9522-3. URL http://dx.doi.org/10.1007/s10701-010-9522-3
29. Tamma, V., Laibacher, S.: Multiboson correlation interferometry with multimode thermal sources. Phys. Rev. A **90**, 063,836 (2014). DOI 10.1103/PhysRevA.90.063836. URL http://link.aps.org/doi/10.1103/PhysRevA.90.063836
30. Tamma, V., Laibacher, S.: Boson sampling with non-identical single photons. Journal of Modern Optics pp. 1–5 (2015). DOI 10.1080/09500340.2015.1088096. URL http://dx.doi.org/10.1080/09500340.2015.1088096
31. Tamma, V., Laibacher, S.: Multi-boson correlation sampling. Quantum Inf. Process. (2015). In press (invited paper in memory of Dr. H. Brandt)
32. Tamma, V., Laibacher, S.: Multiboson Correlation Interferometry with Arbitrary Single-Photon Pure States. Phys. Rev. Lett. **114**, 243,601 (2015). DOI 10.1103/PhysRevLett.114.243601. URL http://link.aps.org/doi/10.1103/PhysRevLett.114.243601
33. Tamma, V., Seiler, J.: Multipath correlation interference with a thermal source and quantum logic simulations: a fundamental effect in quantum optics (2015). URL http://arxiv.org/abs/1503.07369
34. Tamma, V., Zhang, H., He, X., Garuccio, A., Schleich, W.P., Shih, Y.: Factoring numbers with a single interferogram. Physical Review A **83**(2), 020,304 (2011). DOI 10.1103/physreva.83.020304. URL http://dx.doi.org/10.1103/PhysRevA.83.020304
35. Tamma, V., Zhang, H., He, X., Garuccio, A., Shih, Y.: New factorization algorithm based on a continuous representation of truncated Gauss sums. Journal of Modern Optics **56**(18-19), 2125–2132 (2009). DOI 10.1080/09500340903254700. URL http://dx.doi.org/10.1080/09500340903254700
36. Vandersypen, L.M.K., Steffen, M., Breyta, G., Yannoni, C.S., Sherwood, M.H., Chuang, I.L.: Experimental realization of Shors quantum factoring algorithm using nuclear magnetic resonance. Nature **414**(6866), 883887 (2001). DOI 10.1038/414883a. URL http://dx.doi.org/10.1038/414883a
37. Weber, S., Chatel, B., Girard, B.: Factoring numbers with interfering random waves. Europhys. Lett. **83**(3), 34,008 (2008). DOI 10.1209/0295-5075/83/34008. URL http://dx.doi.org/10.1209/0295-5075/83/34008
38. Wölk, S., Feiler, C., Schleich, W.: Factorization of numbers with truncated Gauss sums at rational arguments. Journal of Modern Optics **56**(18-19), 21182124 (2009). DOI 10.1080/09500340903194625. URL http://dx.doi.org/10.1080/09500340903194625
39. Wölk, S., Merkel, W., Schleich, W.P., Averbukh, I.S., Girard, B.: Factorization of numbers with Gauss sums: I. Mathematical background. New Journal of Physics **13**(10), 103,007 (2011). URL http://stacks.iop.org/1367-2630/13/i=10/a=103007
40. Wölk, S., Schleich, W.P.: Factorization of numbers with Gauss sums: III. Algorithms with entanglement. New Journal of Physics **14**(1), 013,049 (2012). URL http://stacks.iop.org/1367-2630/14/i=1/a=013049