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

Analogue algorithm for parallel factorization of an exponential number of large integers
II. Optical implementation

Vincenzo Tamma

Received: date / Accepted: date

Abstract We report a detailed analysis of the optical realization [22,31,30,24] of the analogue algorithm described in the first paper of this series [21] for the simultaneous factorization of an exponential number of integers. Such an analogue procedure, which scales exponentially in the context of first order interference, opens up the horizon to polynomial scaling by exploiting multi-particle quantum interference.

Keywords quantum computation · optical interferometry · algorithms · analogue computers · factorization · exponential sums · Gauss sums

1 Introduction

Factorization of a large integer N is a very difficult problem to solve with our current digital computers. Indeed, divisions of N for all its possible trial factors are costly tasks for a digital computer. Shor's algorithm [17,32] is the only algorithm which so far would allow an exponential speed-up in the solution of the factoring problem by employing entanglement between quantum systems [6,12].

Recently different methods for factorization based on exponential sums [16] have led to several important publications [2,20,35,11,36,7,10,19,18,34,14,9,8,13,1,33,4,15]. In the first paper [21] of this series we have described the physical principle for a generic analogue implementation of a novel factorization algorithm based on the analogue measurement of the periodicity in the maxima of Continuous Truncated Exponential Sums (CTES) [22,31,30,24]. Differently from previous factoring methods this algorithm allows the

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

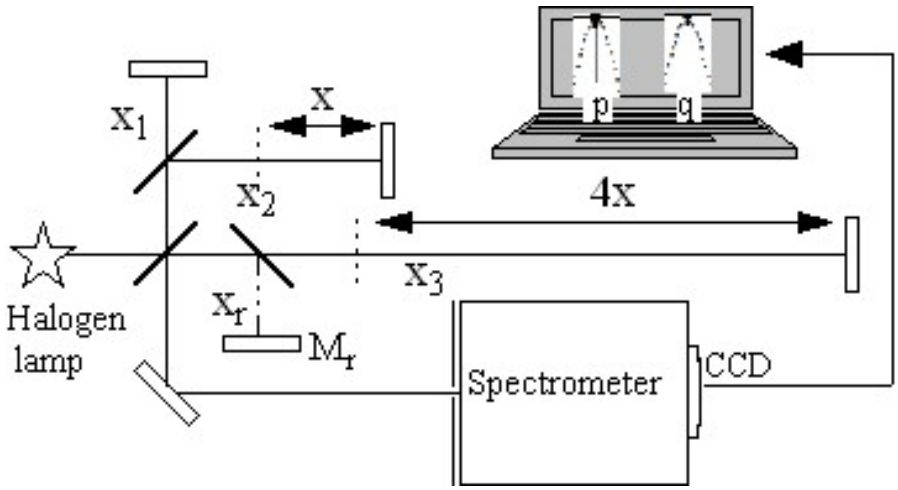

Fig. 1 Example with $M = 3$ interfering paths of an optical computer based on a generalized symmetric Michelson interferometer, a polychromatic source (halogen lamp), M balanced beam splitters, $M + 1$ mirrors, and a spectrometer connected to a CCD camera [30]. The lengths of the M interfering paths are varied with respect to the reference length x_r indicated by thin vertical dashed lines. The length of the m-th optical path reads $x_m = x_r + (m-1)^j x$, with the unit of displacement x, integer order j (we depeict here the case $j = 2$), and $m = 1, 2, ..., M$.

factorization of an exponential number of integers by the analogue implementation of a polynomial number of CTES interferograms where divisions of large numbers are performed by "nature".

Is there an example of a physical system able to compute such a factoring algorithm?

The answer is yes! Divisions occur in a natural way in the wave nature of light. In fact, a wave of wavelength λ propagating over a distance d acquires a phase $\phi = 2\pi d/\lambda$ and therefore naturally performs the ratio d/λ. In contrast to a digital computer, division turns out to be an instantaneous task for such a physical system. A polychromatic source of light, which contains a continuous broad range of wavelengths, allows us to perform in parallel an exponential number of "expensive" divisions to test trial factors simultaneously.

In Section II we will describe how the CTES algorithm can be physically implemented with an "optical computer" based on a polychromatic source, a multi-path Michelson interferometer and a spectrometer. The simultaneous factorization of an exponential number of integers will be demonstrated by suitably rescaling the wavelengths of the output optical CTES interferograms. Section III will detail the experimental realizations with our optical computer of CTES of orders $j = 1, 2, 3$ leading to the factorization of numbers with up to seven digits. Section IV and V will address, respectively, the final remarks as well as possible extensions of our optical algorithm to factoring methods with polynomial scaling.

2 Optical computer for factoring an exponential number of integers

We consider a symmetric Michelson interferometer in free space with $M+1$ paths and a polychromatic source given by a halogen lamp as shown in Fig. 1 for $M=3$. The system includes M balanced beam splitters and $M+1$ mirrors. The lengths

$$x_m \equiv x_r + (m-1)^j x, \tag{1}$$

with $m = 1, 2, ..., M$, are calibrated with respect to the reference path x_r. The integer value j will define the order of the CTES to be experimentally recorded. Here x denotes the optical-path unit of displacement. After the calibration, the reference mirror is blocked. The intensity in the exit port of the interferometer is the result of the interference of the waves in the remaining M arms. Since we deal with a symmetric interferometer consisting of balanced beam splitters, all the interfering beams have, in principle, the same amplitude. Therefore, by normalizing the output intensity with respect to the source intensity, the different interfering optical paths x_m, with $m = 1, 2, ..., M$, lead to the CTES patterns

$$\begin{aligned} I^{(M,j)}(\lambda; x) &\equiv I^{(M,j)}(\frac{\lambda}{x} \equiv \xi) \\ &\equiv \left| \frac{1}{M} \sum_{m=1}^{M} \exp\left[2\pi i (m-1)^j \frac{1}{\xi} \right] \right|^2. \end{aligned} \tag{2}$$

Such interferograms, for each given value of the optical-path unit x, depend only on the dimensionless variable

$$\xi \equiv \frac{\lambda}{x} \tag{3}$$

given by the ratio between the wavelengths of the halogen source and the unit x.

Since x and λ only enter into the spectrum as a ratio $x/\lambda = 1/\xi$ we can easily apply the scaling law

$$I^{(M,j)}(\lambda; x) \equiv I^{(M,j)}(\frac{\lambda}{x} \equiv \xi) = I^{(M,j)}(N\frac{\lambda}{x} \equiv \xi_N; N), \tag{4}$$

with

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

continuous function of the N-dependent dimensionless variable

$$\xi_N \equiv N\frac{\lambda}{x}. \tag{5}$$

This scaling procedure allows us to determine the factors of N as the integer values $\xi_N \equiv N\lambda/x = \ell$ whose corresponding wavelengths λ are associated with dominant maxima in the CTES optical interferograms in Eq. (2).

In the next sections we will describe how this result leads to an optical implementation of the analogue algorithm described in Ref. [21]. The two key physical observables O_ξ and O_x for such an optical computer correspond, respectively, to the source wavelengths with values $o_\xi \equiv \lambda$ in a given range $\lambda_{min} \leq \lambda \leq \lambda_{max}$ and the optical-path relative lengths with values $o_x^{(m,j)} \equiv x_m - x_r = (m-1)^j x$, with $m = 1, 2, ..., M$, for given values of M, j and path unit x.

2.1 Factorization with a single optical interferogram

In this section, we describe the CTES factoring procedure based on the measurement of a single interferogram $I^{(M,j)}(\lambda; x)$ in Eq. (2) recorded at a given value of x. We address the question of the interval $N_{min,x} \leq N \leq N_{max,x}$ of numbers N factorable by covering all the (integer) trial factors ℓ in either the range $[3, \sqrt{N}]$ [1] or $[\sqrt{N}, N]$ with a given selected range $\lambda_{min} \leq \lambda \leq \lambda_{max}$ of wavelengths of the optical source.

In general, for each integer N a trial factor $\ell \leq N$ can be checked only if

$$\xi_N = \ell \in [\xi_N^{(min)}, \xi_N^{(max)}] \equiv [\frac{N}{x}\lambda_{min}, \frac{N}{x}\lambda_{max}], \tag{6}$$

where $\xi_N^{(min)}$ and $\xi_N^{(max)}$ are respectively the smallest and largest values that the variable ξ_N in Eq. (5) can assume for the rescaled interferogram $I^{(M,j)}(\xi_N; x)$ in Eq. (4).

We consider first the case in which we want to check all the trial factors $\ell \in [3, \sqrt{N}]$ leading from Eq. (6) to the condition

$$\text{Method (1): } \xi_N = \ell \in [3, \sqrt{N}] \subseteq [\frac{N}{x}\lambda_{min}, \frac{N}{x}\lambda_{max}]. \tag{7}$$

It is easy to obtain [21] the interval [2]

$$N_{min,x}^{(1)} \equiv \left\lceil \frac{x^2}{\lambda_{max}^2} \right\rceil \leq N \leq N_{max,x}^{(1)} \equiv \left\lfloor \frac{3x}{\lambda_{min}} \right\rfloor \tag{8}$$

of factorable integers in the optical range $\lambda_{min} \leq \lambda \leq \lambda_{max}$ with a single interferogram associated with a given value x satisfying the condition [21]

$$x \leq x^{(1)} \equiv \frac{3\lambda_{max}^2}{\lambda_{min}}. \tag{9}$$

[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.

In the particular case of an interferogram recorded at the maximum possible value $x = x^{(1)}$ in Eq. (9), by considering the largest wavelength range such that $\lambda_{max}/\lambda_{min}$ is an integer, we find the largest but also the only integer

$$N^{(1)} \equiv \frac{9\lambda_{max}^2}{\lambda_{min}^2} \tag{10}$$

factorable by using a single experimental interferogram $I^{(M,j)}(\lambda; x)$.

We consider now the second case in which we want to check all the trial factors $\xi_N = \ell \in [\sqrt{N}, N]$ leading from Eq. (6) to the condition

$$\text{Method (2): } \xi_N = \ell \in [\sqrt{N}, N] \subseteq [\frac{N}{x}\lambda_{min}, \frac{N}{x}\lambda_{max}]. \tag{11}$$

In this case we easily obtain [21] the interval

$$N_{min}^{(2)} \equiv 1 \leq N \leq \left\lfloor \frac{x^2}{\lambda_{min}^2} \right\rfloor \equiv N_{max,x}^{(2)} \tag{12}$$

of factorable numbers for the given optical range $\lambda_{min} \leq \lambda \leq \lambda_{max}$ with a single interferogram associated with a given value x satisfying the condition [21]

$$x \leq x^{(2)} \equiv \lambda_{max}. \tag{13}$$

In particular, for an optical interferogram recorded at the maximum value $x = x^{(2)} \equiv \lambda_{max}$ in Eq. (13) we obtain the largest interval

$$N_{min}^{(2)} \equiv 1 \leq N \leq \left\lfloor \frac{\lambda_{max}^2}{\lambda_{min}^2} \right\rfloor \equiv N_{max}^{(2)} \tag{14}$$

of factorable integers.

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

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

of integers exponential with respect to the number of binary digits n_{max} associated with N_{max}. However, in general, the largest factorable integer N_{max} is limited by the value $\lambda_{max}/\lambda_{min}$ associated with the optical spectrum of the interferometer source. For this reason in the next section we will describe a factorization procedure which takes advantage of several optical interferograms $I^{(M,j)}(\lambda; x)$ in Eq. (2) at different values x in order to factor numbers within a limited given range of wavelengths λ. In such a method the maximum factorable number N_{max} will depend on the largest value achievable for the path-unit x.

2.2 Factorization with a sequence of optical interferograms

So far we have restricted ourselves to a factorization method involving a single optical interferogram $I^{(M,j)}(\lambda;x)$ in Eq. (2) defined at a fixed value of the parameter x. However, the remarkable scaling property $\xi_N \equiv N\lambda/x$ characterizing the function $I^{(M,j)}(\lambda;x)$ allows us to consider not only an entire continuous range of wavelengths λ associated with the source but also different discrete values of the unit x characterizing the optical paths in the interferometer.

We determine how the number n of experimental interferograms recorded at different values of x depends on the given range $N_{min} \leq N \leq N_{max}$ of numbers to be factored.

We first point out that a single interferogram registered at a given value x allows us to check for each given integer N only the trial factors

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

In general, for the fixed domain $\lambda_{min} \leq \lambda \leq \lambda_{max}$ of values λ, these trial factors may correspond only to a subset of the total range $3 \leq \ell \leq \sqrt{N}$ or $\sqrt{N} \leq \ell \leq N$ of integer 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 n (to be determined) 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. (15) to cover all the trial factors

$$\xi_N = \ell \in [\xi_{N,i}, \xi_{N,i+1}] \equiv [\frac{N}{x_i}\lambda_{min}, \frac{N}{x_i}\lambda_{max}], \tag{16}$$

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

$$\xi_{N,i+1} \equiv \frac{N}{x_i}\lambda_{max} \equiv \frac{N}{x_{i+1}}\lambda_{min} \tag{17}$$

satisfies the condition for consecutive intervals. This implies that the sequence x_i, with $i = 0, ..., n-1$, defining the n interferograms to be recorded, follows the iterative formula

$$x_{i+1} \equiv \frac{x_i}{c} < x_i, \tag{18}$$

with

$$c \equiv \frac{\xi_{N,i+1}}{\xi_{N,i}} = \frac{\lambda_{max}}{\lambda_{min}} > 1. \tag{19}$$

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

$$\text{Method (1):} \tag{20}$$
$$\xi_N = \ell \in [3, \sqrt{N}] \subseteq [\xi_{N,0}, \xi_{N,n}] \equiv [\frac{N\lambda_{min}}{x_0}, \frac{N\lambda_{min}}{x_0}\ c^n]$$

or the condition

$$\text{Method (2):} \tag{21}$$
$$\xi_N = \ell \in [\sqrt{N}, N] \subseteq [\xi_{N,0}, \xi_{N,n}] \equiv [\frac{N\lambda_{min}}{x_0}, \frac{N\lambda_{min}}{x_0}\ c^n]$$

for the total interval $[\xi_{N,0}, \xi_{N,n}]$ of trial factors covered by the n interferograms.

In the factorization method (1) the interferograms $I^{(M,j)}(\lambda; x)$ are measured at the values $x = x_i$, with $i = 0, 1, ..., n-1$, defined by Eq. (18) with

$$\frac{x_0}{\lambda_{min}} \geq \frac{x_0^{(1)}}{\lambda_{min}} \equiv \frac{N_{max}}{3}. \tag{22}$$

From Ref. [21] we also obtain the minimum number

$$\begin{aligned} n_{x_0}^{(1)} &\equiv \left\lceil log_c\ \frac{x_0}{\lambda_{min}\sqrt{N_{min}}} \right\rceil \\ &\geq \left\lceil log_c\ \frac{N_{max}}{3\sqrt{N_{min}}} \right\rceil \equiv n_{min}^{(1)} \end{aligned} \tag{23}$$

of interferograms necessary to factor all the integers N in any given interval $N_{min} \leq N \leq N_{max}$.

We consider now the method (2) associated with the condition in Eq. (21). In such a case, the interferograms $I^{(M,j)}(\lambda; x)$ are recorded at the values $x = x_i$, with $i = 0, 1, ..., n-1$, defined by Eq. (18) with

$$\frac{x_0}{\lambda_{min}} \geq \frac{x_0^{(2)}}{\lambda_{min}} \equiv \sqrt{N_{max}}. \tag{24}$$

We also easily obtain [21] the minimum number

$$n_{x_0}^{(2)} \equiv \left\lceil log_c \frac{x_0}{\lambda_{min}} \right\rceil \geq \left\lceil log_c \sqrt{N_{max}} \right\rceil \equiv n_{min}^{(2)} \tag{25}$$

of interferograms necessary to factor all the integers N in any given interval $N_{min} \leq N \leq N_{max}$.

We have finally demonstrated that the number n of experimental runs necessary for factorizing any given range of numbers $N_{min} \leq N \leq N_{max}$, with $N_{min} \geq 1$, using a selected wavelength spectrum $[\lambda_{min}, \lambda_{max}]$, scales logarithmically with respect to either $N_{max}/\sqrt{N_{min}}$ (method (1)) or $\sqrt{N_{max}}$ (method (2)). The described algorithm allows the factorization of a number

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

of integers exponential with respect to the number n_{max} of binary digits of N_{max} by using a polynomial number of interferograms if

$$c \equiv \frac{\lambda_{max}}{\lambda_{min}} \geq 2.$$

On the other hand, the parameter x_0 for the first interferometer scales exponentially with respect with n_{max}.

3 Experimental realizations

We now turn to the experimental implementation of our factoring technique. The experimental setup consists of a symmetric Michelson interferometer with M interfering paths of which we have given an example for $M = 3$ in Fig. 1. Each mirror is mounted on a single axis translation stage. Each stage consists of a $5mm$ manual travel stage, a $50mm$ step motor with 58200 steps for each mm, and a $20\mu m$ piezoelectric and feedback control stage. The resolution of the piezoelectric element is $10\,nm$. The polychromatic source of the interferometer is given by a halogen lamp while a He-Ne laser expanded by lenses is used for the alignment. The interference pattern at the output port of the interferometer is measured by a spectrometer as a continuous function of the wavelengths λ associated with the polychromatic source. In the experiments we will consider the visible spectrum. The spectrometer, with resolution $0.01\,nm$, is characterized by a grating composed by 2400 elements for each mm and by a 2048-pixel CCD array with an accuracy of $0.005 - 0.006\,nm$.

Calibrating the optical paths given by Eq. (1) with a suitable accuracy is one of the most challenging tasks in this experiment. We first determine when all path lengths x_m are equal to x_r, by measuring the polychromatic two-path interference between the m^{th} beam and the reference beam, for each $m = 1, 2, ..., M$, with the mirror M_r tilted by a small angle with respect to all the other mirrors. In particular, the interference fringe associated with two equal paths is completely bright [3] for all the wavelengths of the polychromatic source ("white light condition"). We calibrate the m^{th} path until such a fringe is in correspondence to the entrance slit of the spectrometer. Then we block the mirror M_r and translate each mirror M_m, using the piezoelectric translators together with the step motors, so that Eq. (1) is satisfied. The optical interferometer is now prepared to record the CTES factoring interferogram in Eq. (2) for the chosen values of x, j and M.

In the next sections we will show experimental demonstrations of our factoring method with CTES interferograms of different orders $j = 1, 2, 3$ and numbers of interfering optical paths $M = 2, 3$. We will show how it is possible to select factors of different numbers for a given experimental interferogram recorded at a particular value of the path unit x. Such demonstrations can be easily extended for the generic implementation of the factoring algorithm described in section 2.2 which allows us to check all the possible trial factors of any integer less than N_{max} with only a polynomial number of CTES interferograms recorded, for example, in the optical range $400\,nm \leq \lambda \leq 800\,nm$ ($\lambda_{max}/\lambda_{min} = 2$).

[3] The fringe can also be completely dark if an extra π shift emerges from the number of beam splitters and mirrors present in the two paths.

3.1 Experimental results for $j = 2$ and $M = 3$

After having described the experimental preparation, we can focus now on the actual measurement of the CTES optical interferogram $I^{(M,j)}(\lambda; x)$ in Eq. (2). In this section, we will consider the case of $M = 3$ interfering phase terms with a quadratic dependence ($j = 2$) on m leading to Continuous Truncated Gauss Sum (CTGS) interferograms.

In Fig. 2 we give an experimental proof of principle for the factorization of $N = 207911$. The recorded CTGS interferogram measured for the unit of displacement $x = N\,nm$ in the wavelength range $450.173\,nm \leq \lambda \leq 461.934\,nm$ is scaled according to the corresponding auxiliary variable $\xi_N = \lambda/nm$ in Eq. (5). Thereby, the integer values of ξ_N are also integer values of wavelengths measured in nm. All the trial factors $\xi_N = \ell$ of N corresponding to the wavelengths $\lambda = \ell\,nm$ are represented by vertical lines. Only the trial factors $\ell = 451$ and $\ell = 461$, represented by continuous lines, correspond to the brightest integer wavelengths and therefore are the factors of N. Instead, all the other integer wavelengths, represented by dashed lines, are not associated with dominant local maxima and consequently are not factors. It is interesting to note that in the wavelength range in Fig. 2 the closer a non factor is to a factor, the higher is the corresponding value of intensity. Therefore, we can expect that when non factors are far away from factors, it is generally much easier to recognize that the associated wavelengths do not correspond to dominant local maxima, as we have shown in Ref. [21]. In conclusion, we have demonstrated that the factors of $N = 207911$ correspond to the dominant maxima at integer wavelengths of the recorded interferogram.

An experimental proof of principle for the factorization of multiple numbers is given in Fig. 3 where the CTGS optical interferogram is measured in the wavelength interval $[451.784\,nm, 463.522\,nm]$, using this time the displacement unit $x = 523426.8\,nm$. We give an example for the factorization of two numbers, $N = 1308567 = 1131 \times 1157$ and $N' = 1306349 = 1133 \times 1153$. We only consider the wavelength interval $[460.36\,nm, 463.24\,nm]$ shown in the center of Fig. 3. We start with the seven-digit number $N = 1308567 = 1131 \times 1157$ and present on the bottom of Fig. 3 an axis with the variable ξ_N rescaled according to Eq. (5). We clearly identify the factor 1157 by the maximum being located at an integer, as shown by the inset. Moreover, we use the same interferogram to factor the number $N' = 1306349 = 1133 \times 1153$. For this purpose we show on the top the rescaled variable $\xi_{N'}$. Again we can identify the factor 1153 by the maximum being located at an integer. This demonstrates that the accuracy in our experiment allows us to factor numbers with values up to $N_{max} \sim 10^6$ by tilting the wavelength axis in order to obtain the auxiliary variable ξ_N associated with a generic number $N < N_{max}$ to factor.

We have demonstrated that the CTES algorithm is optically computable for different values of the unit of displacement x. As expected, the obtained results point out that the maximum number factorable with the recorded interferogram increases with the value of the unit x. The upper limit for the value

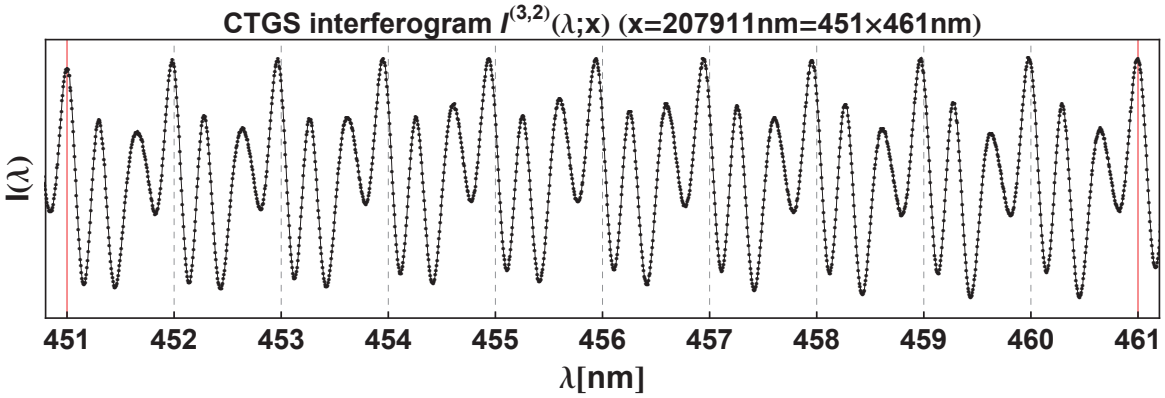

Fig. 2 Experimental realization of the CTGS ($j = 2$) interferogram $I(\lambda) = I^{(M,j)}(\lambda; x)$ in Eq. (2) for $M = 3$ and unit of displacement $x = 207911\,nm$, in the wavelength range $450.173\,nm \leq \lambda \leq 461.934\,nm$ [22]. The dots represent the measured values, and the curve is obtained by joining these experimental points. Only the trial factors $\ell = 451$ and $\ell = 461$, represented by continuous vertical lines, correspond to the brightest integer wavelengths and therefore are the factors of N. Instead, all the other integer wavelengths, represented by dashed vertical lines, are not associated with local maxima and consequently are not factors.

of x is determined by the coherence length associated with the experimental conditions.

3.2 Experimental results for $j = 2$ and $M = 2$

We now consider the case of the CTES optical interferogram $I^{(M,j)}(\lambda; x)$ in Eq. (2) for $M = 2$ and unit of displacement $x = N\,nm$, with $N = 207911$. In this case, since we have only two interfering terms associated with $m = 1, 2$, the value of the order j is not significant anymore. We have experimentally recorded such an interferogram in the wavelength range $450.173 \leq \lambda \leq 461.934$ (see Fig. 4). Again we can distinguish the factors 451 and 461 as the brightest integer wavelengths in the pattern.

It is interesting to compare the obtained interferogram for $M = 2$ interfering terms in Fig. 4 with the one for $M = 3$ terms in Fig. 2. In the case of $M = 2$ the secondary peaks disappear and the dominant peaks are wider [21].

3.3 Experimental results for $j = 1, 3$ and $M = 3$

We now consider the case of $M = 3$ interfering phase terms and $x = 207911\,nm$ for two different orders $j = 1, 3$ of the CTES. In Fig. 5 is represented the recorded interferogram for $j = 1$ corresponding to a Continuous Truncated Fourier Sum (CTFS). Instead, in Fig. 6 is shown the measured Continuous Truncated Kummer Sum (CTKS) interferogram corresponding to $j = 3$. In both pattern we can recognize the factors 451 and 461 as the brightest integer wavelengths.

Comparing the interferograms in Figs. 5, 2, 6, we can note that peaks of higher order appear as the order j increases and at the same time the dominant peaks important for factorization become sharper [21].

4 Remarks

We have demonstrated the physical computability of the CTES algorithm using an optical computer characterized by a multi-path Michelson interferometer, a spectrometer and a polychromatic optical source.

Such an optical computer exploits destructive/constructive interference to experimentally compute the CTES optical interferograms

$$I^{(M,j)}(\lambda; x) \equiv I^{(M,j)}(\frac{\lambda}{x} \equiv \xi)$$

in Eq. (2) recorded over the continuous range of wavelengths $\lambda \equiv \xi x$ of the polychromatic source, with x unit of displacement in the optical paths. The wave nature of light allows us to experimentally compute the divisions $f(1/\xi) = x/\lambda$ for all the possible wavelengths $\lambda = \xi x$ in the CTES optical spectrum. The information about such divisions can be extracted by measuring the periodicity in the maxima of the recorded interferogram. Moreover, rescaling such a periodicity according to the relation $\xi_N \equiv N\lambda/x$ allows us to infer information about the divisions $f(\xi_N) = N/\xi_N$ and, thereby, about

the factors of several numbers N. Indeed, for each value of N, the factors are the integer values of $\xi_N \equiv N\lambda/x$ corresponding to dominant maxima of the recorded CTES interferogram.

Furthermore, we have demonstrated that an optical computer can implement prime number decomposition of an exponential number of integers $N_{min} \leq N \leq N_{max}$. In particular, the CTES factorization algorithm takes advantage of a sequence of optical interferograms $I^{(M,j)}(\lambda; x_i)$, with $i = 0, 1, ..., n-1$, where each one is associated with a different value $x = x_i = (\lambda_{min}/\lambda_{max})\, x_{i-1}$ of the unit of displacement in the multi-path interferometer. The number n of interferograms increases polynomially with respect to the logarithm in base $\lambda_{max}/\lambda_{min}$ of the largest number N_{max} to be factored. Therefore, even by exploiting a source with a wavelength bandwidth only in the visible range such that $\lambda_{max}/\lambda_{min} = 2$, it is possible to achieve a logarithmic scaling in base 2.

Finally, we have given a proof of principle demonstration of the physical computability of the CTES algorithm in the visible range. The factors of numbers with up to seven digits were experimentally found by using optical CTES inteferograms of order $j = 1, 2, 3$ with $M = 2, 3$ interfering paths. We have shown, as expected, that by increasing the number M of interfering terms and the order j of the CTES interferogram the dominant peaks become sharper and sharper. This property can be exploited in order to better distinguish factors from non factors.

Our experimental results demonstrate that the CTES algorithm is not just an abstract mathematical tool but is implementable using an optical computer, which exploits the connection between physical phenomena of light interference and number theory for parallel factorization of an exponential number of integers.

5 Towards factoring with polynomial scaling

The described optical algorithm, in contrast to Shor' s method, leads to the factorization of an exponential number of integers by experimentally implementing a single sequence of a polynomial number of interferograms. However, our scheme does not allow the achievement of polynomial scaling in the number of resources as in the Shor's algorithm, which instead takes advantage of entanglement between single-photon qubits in order to achieve such a goal. Indeed, the largest number factorable N_{max} is upper limited either by the value $(\lambda_{max}/\lambda_{min})^2$ or x_0/λ_{min}, depending on the use of a single interferogram or a sequence of interferograms. Moreover, the accuracy in the variable ξ in Eq. (3)

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

associated with the trial factors of N depends on the experimental uncertainties $\Delta\lambda$ and Δx associated with the measurement of the wavelengths λ and the optical path unit x, respectively. The uncertainty $\Delta\xi$ also has to decrease exponentially [21], implying that the unit x defining the CTES interferograms

in Eq. (2) has to grow exponentially. Interferometric configurations based on multiple path-reflections may be used to achieve larger values of x.

An extension of the presented algorithm based on correlation measurements in n^{th} order interferometers may pave the way towards a new algorithm using a polynomial number of resources, thereby avoiding the requirement of exponentially large values for the optical-path unit x. In this case, multi-photon quantum interference [28,5,26,27,29,25,23,3] may serve as a powerful tool to distinguish factors from non factors.

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

References

1. 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
2. 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
3. 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
4. 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
5. Laibacher, S., Tamma, V.: From the physics to the computational complexity of multiboson correlation interference. Phys. Rev. Lett. (2015). In press
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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
12. 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
13. 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
14. 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
15. 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
16. Schleich, W., Maier, H.: Prime Numbers 101: A Primer on Number Theory. Wiley (2014). URL https://books.google.de/books?id=EEiaGQAACAAJ
17. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J.Sci.Statist.Comput. **26**, 1484 (1997)
18. 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
19. 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
20. 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
21. Tamma, V.: Analogue algorithm for parallel factorization of an exponential number of large integers: I. Theoretical description. Quantum Information Processing **11128**, 1190 (2015).
22. Tamma, V.: Theoretical and experimental study of a new algorithm for factoring numbers. Ph.D. thesis, University of Maryland, Baltimore County (2010). ProQuest
23. Tamma, V.: Sampling of bosonic qubits. International Journal of Quantum Information **12**, 1560,017 (2014). DOI 10.1142/S0219749915600175
24. 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
25. 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
26. 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
27. Tamma, V., Laibacher, S.: Multi-boson correlation sampling. Quantum Inf. Process. (2015). In press (invited paper in memory of Dr. H. Brandt)
28. 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
29. 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
30. 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
31. 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

32. 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
33. 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
34. 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
35. 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
36. 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

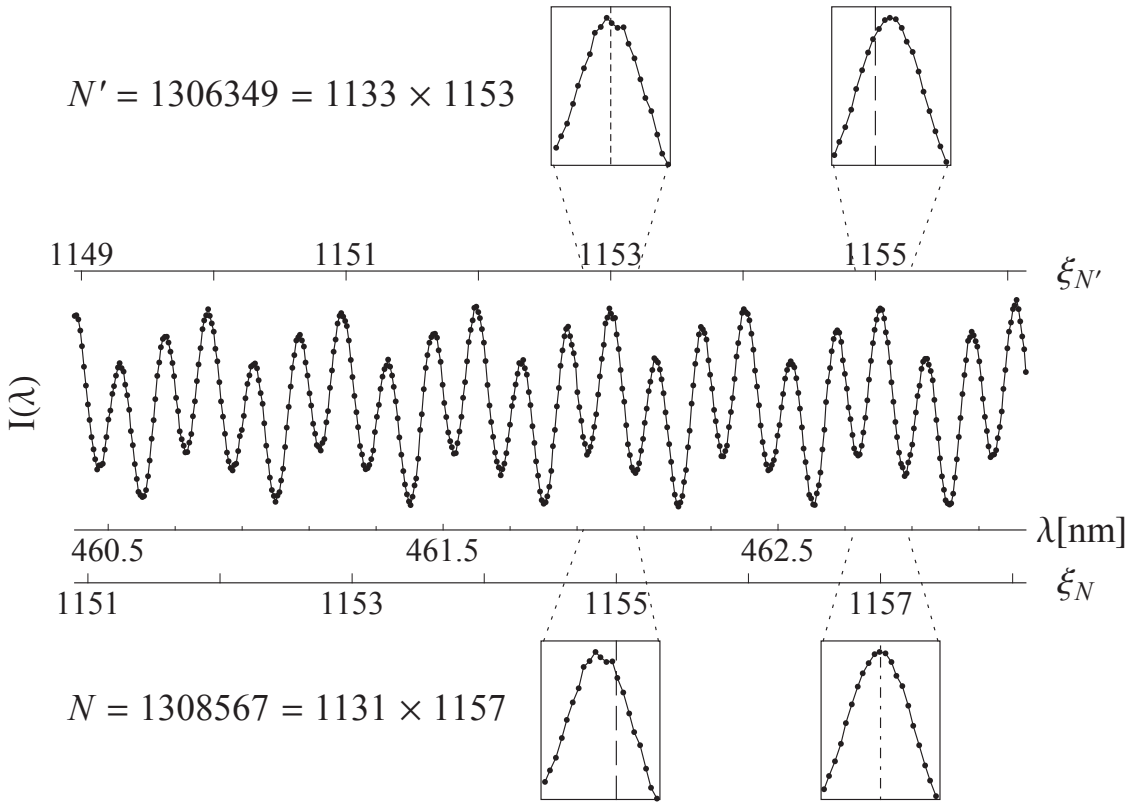

Fig. 3 Experimental realization of the CTGS ($j = 2$) interferogram $I(\lambda) = I^{(M,j)}(\lambda; x)$ in Eq. (2) for $M = 3$ and unit of displacement $x = 523426.8\,nm$, in the wavelength range $460.36\,nm \leq \lambda \leq 463.24\,nm$ (center) [22,30]. The factorization of the two numbers $N = 1308567 = 1131 \times 1157$ (bottom) and $N' = 1306349 = 1133 \times 1153$ (top) is obtained by rescaling the wavelength axis according to Eq. (5). The insets magnify the behavior of the interferogram in the neighborhoods of the two dominant maxima corresponding to the trial factors 1153 ,1155 (this integer is checked as a trial factor for both N and N') and 1157, which are indicated by dotted, dashed, and dashed-dotted lines, respectively. The first dominant maximum in the interferogram points to a factor ($\ell = 1153$) of N' but not of N. On the other hand, the second dominant maxima corresponds to a factor ($\ell = 1157$) of N but not of N'.

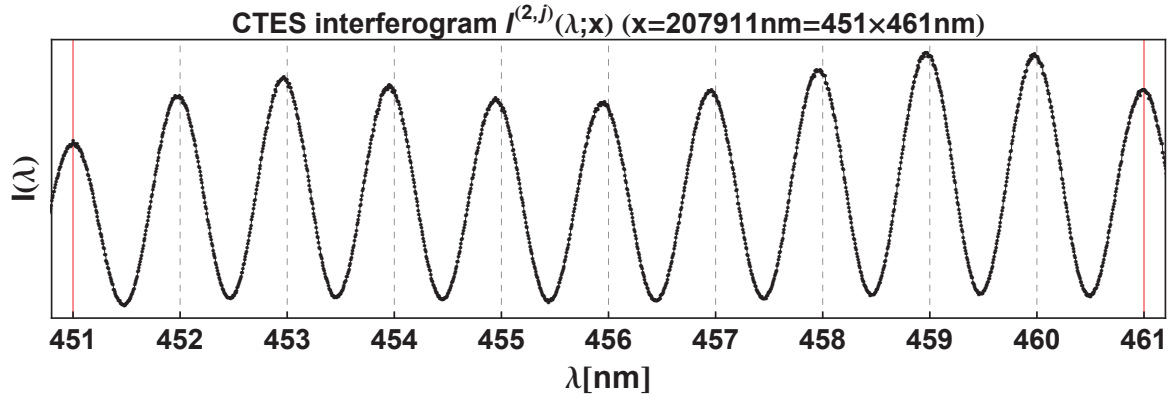

Fig. 4 Experimental realization of the CTES interferogram $I(\lambda) = I^{(M,j)}(\lambda; x)$ in Eq. (2) for $M = 2$, $x = 207911\,nm$, in the wavelength range $450.173\,nm \leq \lambda \leq 461.934\,nm$ [22]. In this case, since there are only two interfering terms associated with $m = 1, 2$, the value of the order j is not significant anymore. Only the trial factors $\ell = 451$ and $\ell = 461$, represented by continuous vertical lines, correspond to the dominant maxima and therefore are the factors of N. Instead, all the other integer wavelengths, represented by dashed vertical lines, are not associated with local maxima and consequently are not factors.

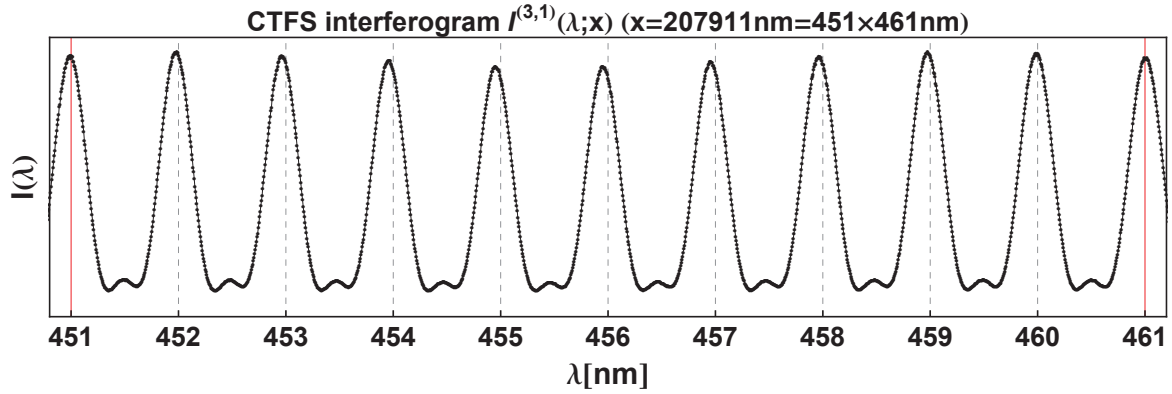

Fig. 5 Experimental realization of the CTFS ($j = 1$) interferogram $I(\lambda) = I^{(M,j)}(\lambda; x)$ in Eq. (2) for $M = 3$ and $x = 207911\,nm$, in the wavelength range $450.173\,nm \leq \lambda \leq 461.934\,nm$ [22]. We recognize the factors $\ell = 451$ and $\ell = 461$ of N, represented by continuous vertical lines, as the dominant maxima with respect to the other trial factors, represented by dashed vertical lines.

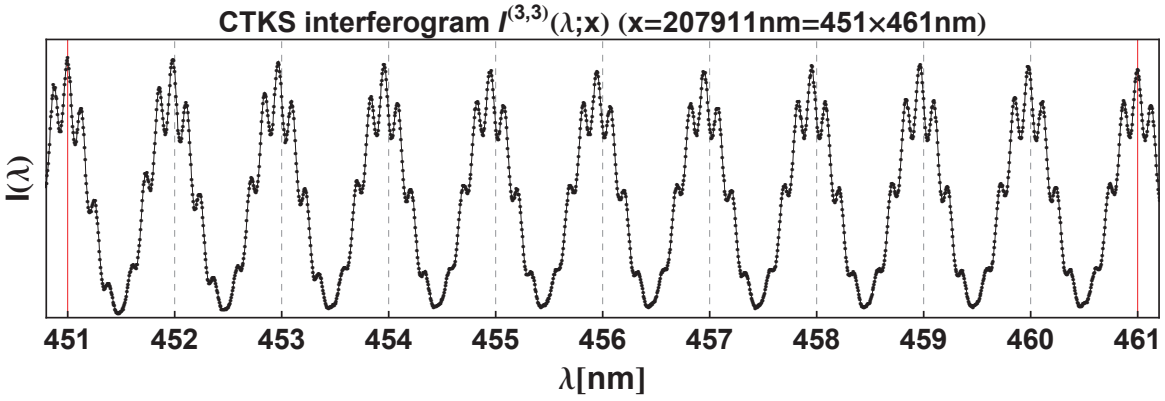

Fig. 6 Experimental realization of the CTKS ($j = 3$) interferogram $I(\lambda) = I^{(M,j)}(\lambda; x)$ in Eq. (2) for $M = 3$ and $x = 207911\,nm$, in the wavelength range $450.173\,nm \leq \lambda \leq 461.934\,nm$ [22]. Only the trial factors $\ell = 451$ and $\ell = 461$, represented by continuous vertical lines, correspond to the brightest integer wavelengths and therefore are the factors of N. Instead, all the other integer wavelengths, represented by dashed vertical lines, are not associated with local maxima and consequently are not factors.