CTES Factorization Algorithm

Vincenzo Tamma[1,2], Heyi Zhang[1], Xuehua He[1], Augusto Garuccio[2], and Yanhua Shih[1]

[1] Department of Physics, University of Maryland, Baltimore County, Baltimore, Maryland 21250, USA
tammav1@umbc.edu

[2] Dipartimento Interateneo di Fisica, Università degli Studi di Bari, 70100 Bari, Italy

Abstract. We introduce a new factorization algorithm, based on the analogue determination of the periodicity of a single generalized continuous truncated exponential sum (CTES) interferogram. We demonstrate that this algorithm allows, in principle, to factorize arbitrary numbers exploiting a remarking rescaling property of the recorded CTES interference pattern. Such an interferogram can be realized taking advantage of multi-path optical interference, using a polychromatic light source and a spectrometer. The resulting interference pattern, when observed as a function of wavelength, contains the information about all factors of any arbitrary number N. This information is encoded in the location of the maxima of the interferogram.

Keywords: Factorization algorithm, interference, continuous truncated exponential sums, Gauss sums, cryptography.

1 Introduction

To find the factors of a large integer number N is a rather difficult problem in computation theory. Indeed, the security of codes relies on this fact. The most celebrated algorithm for factorization is Shor's algorithm, which takes advantage of quantum systems [1]. In the present paper we present a new factorization algorithm, in which both number theory and a physical process allow to solve the problem of factorization. Such an algorithm has a similar working principle with respect to Shor's case: factorization by exploiting the periodicity of a known function, which, in our case, is a generalized truncated continuous exponential sum (CTES), as a function of a continuous variable.

2 Main Challenge in Factorization

In order to develop an effective factorization algorithm, it is important to understand what is the main challenge in factorization that this algorithm needs to overcome. We want to show that such a challenge consists in the computation of the ratio

$$f(\xi) \doteq \frac{1}{\xi}, \tag{1}$$

A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): QuantumCom 2009, LNICST 36, pp. 303–310, 2010.

as a function of the continuous parameter ξ, with $0 < \xi < 1/\sqrt{N_{min}}$, where N_{min} is the smallest number to be factored. In fact, once we know such a function, we have information about all the possible functions N/ξ associated with all the possible numbers $N > N_{min}$ that we want to factorize. We need simply to look at f as a function of the new variable, obtained by the scaling relation:

$$\xi_N \doteq N\xi, \tag{2}$$

with $0 < \xi_N < N/\sqrt{N_{min}} > \sqrt{N}$. In this way we obtain:

$$f(\xi_N) = \frac{N}{\xi_N}. \tag{3}$$

For each possible N, the factors are given by the values $\xi_N = l$, where l is a trial factor, such that

$$f(l) = \frac{N}{l} = k, \tag{4}$$

with k positive integer. In terms of computation, the introduction of ξ_N involves the multiplication of each possible value of ξ by the constant value N, for each number N we want to factorize. This means that no division operations are required once we know the function $f(\xi)$ in Eq. (1).

We have demonstrated that the factorization process turns out to be very fast in terms of computations if we know the function $f(\xi)$ in Eq. (1). Unfortunately, determining if Eq. (4) is satisfied is not an easy task. In fact, there are trial factors l for which $f(l)$ is very close to an integer. In the next section we will show how the constructive/destructive periodical interference associated with a generalized continuous truncated exponential sum (CTES) allows an easy distinction between factors and non factors. Such an approach is substantially different respect to the usual factorization approach using truncated exponential sums [2,3,4,10,11,7,8], which experimental realizations [12,13,18,14,15,17] present a precalculation of the ratio between N and l[19].

3 New Factorization Algorithm by Exploiting the Periodicity of a CTES

We want to show that the function $f(\xi)$, in Eq. (1), and so all the possible functions $f(\xi_N)$, can be extracted by determining the periodicity of the modulo squared of the generalized continuous truncated exponential sum (CTES) $\mathcal{C}^{(M,j)}(\xi)$, defined as:

$$|\mathcal{C}^{(M,j)}(\xi)|^2 \doteq |\frac{1}{M}\sum_{m=1}^{M} \exp\left[\phi_{m,j}(\xi)\right]|^2, \tag{5}$$

with the phase terms $\phi_{m,j}(\xi)$ given by:

$$\phi_{m,j}(\xi) = 2\pi i(m-1)^j f(\xi). \tag{6}$$

In particular, for each possible number N to factorize, the CTES in Eq. (5) can be rescaled in the following way:

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

The factors of an arbitrary number N are the integer values $\xi_N = l$, which correspond to dominant maxima of such a rescaled sum.

In Fig. 1, it is represented the modulo squared of the rescaled CTES in Eq. (7), with $M = 3$, $j = 2$, as a function of the variable $\xi_N \in [330.74, 337.21]$, for the factorization of $N = 111547$. We can see that the two factors $l = 331, 337$ (represented by stars) give complete constructive interference. On the other hand, for the other trial factors (represented by triangles), there is partially destructive interference. Moreover, there are absolute maxima (represented by points) which do not correspond to integer trial factors.

We have also represented, in Fig. 2, the modulo squared of the rescaled CTES for the same value of N and M and the same range of values of ξ_N, in the case of $j = 3$. It turns out, as expected, that, as the order j of the exponential sum increases, the peaks associated with the absolute maxima become sharper. On the other hand, increasing the order j, also the values of the second order maxima in the interference pattern increase. In order to suppress such maxima it is necessary to increase the number of terms M in the sum.

In the wavelength range in Fig. 1 and Fig. 2, the more a non factor is near to a factor, the less is the correspondent value of intensity. We analyze now

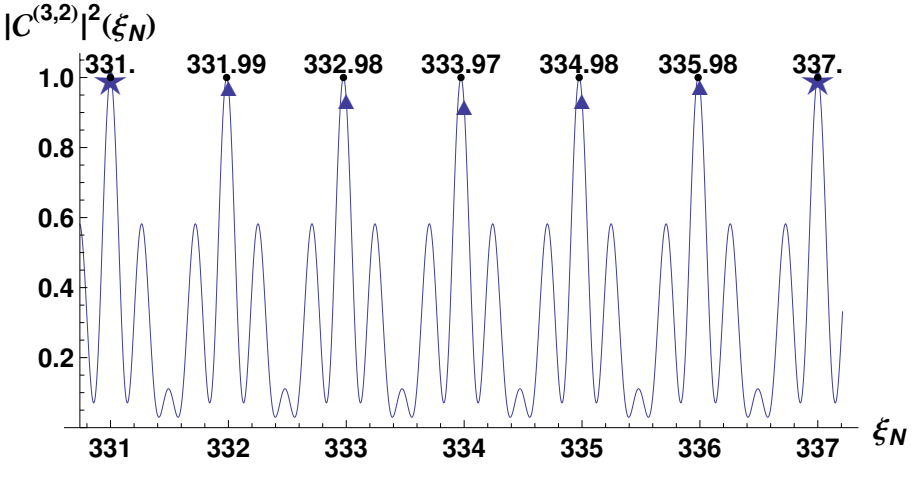

Fig. 1. Modulo squared of the rescaled CTES, in Eq. (7), for $N = 111547$, with $M = 3$ and $j = 2$, as a function of the variable $\xi_N \in [330.74, 337.21]$. We can see that the two factors $l = 331, 337$, represented by stars, give complete constructive interference, despite the other trial factors, represented by triangles, which present partially destructive interference.

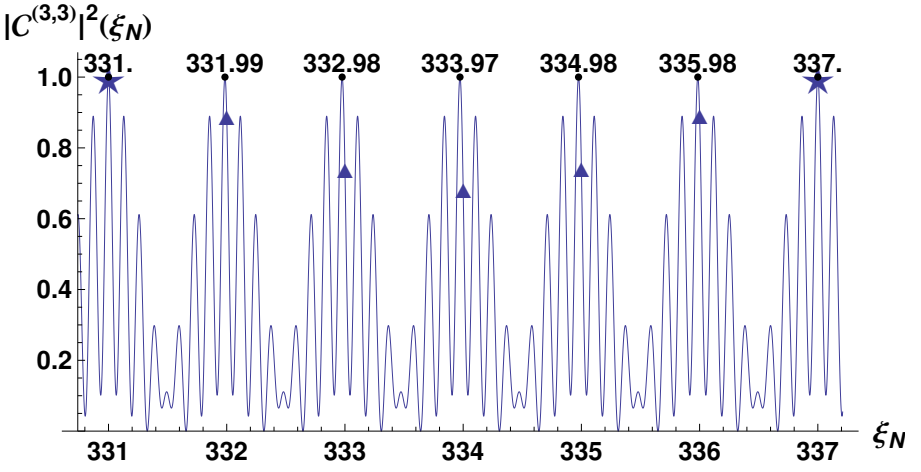

Fig. 2. Modulo squared of the rescaled CTES in Eq. (7), for $N = 111547$, with $M = 3$ and $j = 3$, as a function of the variable $\xi_N \in [330.74, 337.21]$. As expected, the peaks associated with the absolute maxima, in the case $j = 3$, are sharper than the respective peaks, in the case $j = 2$, represented in Fig. 1. On the other hand, increasing the order j, increase the value of the maxima of second order in the interference pattern.

the case of integer wavelengths far from the factors. In Fig. 3, it is shown, for example, a simulation of the interference pattern in the range $[230.9, 237.1]$. We can observe, as expected, that there a is large probability of finding trial factors with associated relatively limited value of intensity. This allows us to speed-up the general selection of the factors among all the possible trial factors, simply disregarding all the value of ξ_N below a suitable threshold value. In this way, the number of trial factors to be considered in order to determine the factors is sensibly reduced.

We gain some insight into the behavior of the function $\mathcal{C}^{(M,j)(\xi)}$, in Eq. (5), as a function of the continuous variable ξ when we represent $f(\xi)$ as

$$f(\xi) = k(\xi) + \frac{1}{2}\tau(\xi), \tag{8}$$

where both the integer k and the continuous parameter τ, which extends from -1 to $+1$, depends on the value of ξ.

When we substitute this representation of $f(\xi)$, in the CTES expression in Eq. (5), we find

$$|\mathcal{C}^{(M,j)}(\xi)|^2 = |s^{(j)}(\tau(\frac{\lambda}{u_N}, N))|^2, \tag{9}$$

where

$$s^{(j)}(\tau) = \frac{1}{M}\sum_{m=1}^{M} \exp\left[\pi i (m-1)^j \tau\right]. \tag{10}$$

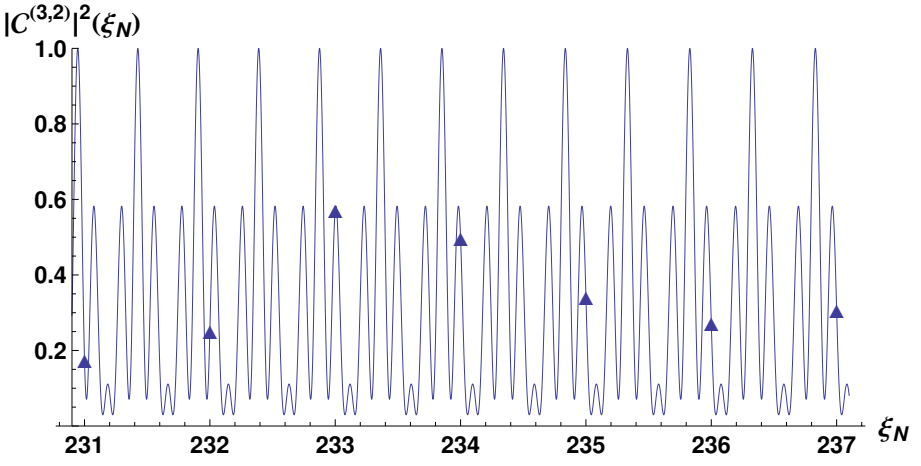

Fig. 3. Modulo squared of the rescaled CTES, in Eq. (7), for $N = 111547$, with $M = 3$ and $j = 2$, as a function of the variable $\xi_N \in [230.9, 237.1]$. We can clearly see that all the integer values of wavelengths in such a range have a relatively limited value of intensity, so that they can be easily disregarded as possible factors.

Hence, the CTES in Eq. (5) is a sequence of the same symmetric function $s^{(j)}$, whose variable τ is determined by Eq. (8). In the case of $j = 0$ this function is closely related to the curlicue function which has a dominant maximum at $\tau = 0$ and oscillations on the sides. The function $s^{(j)}$ repeats periodically for each value ξ such that $f(\xi)$ is equal to an integer k. Consequently the period of repetition of $s^{(j)}$, in the interference pattern, determines the dominant maxima. When a maximum corresponds to an integer value q of $\xi_N = \frac{\xi}{N}$ then q is a factor of N.

In conclusion, the CTES, in Eq.(5),which is independent from the number N to be factored, allows us to recognize all the values ξ, corresponding to an integer value of $f(\xi)$, as dominant maxima in the interference pattern. The factors of an arbitrary number N are given only by the values ξ such that ξ_N, in Eq. 2, is an integer.

4 Analogue Realization of a CTES with a Multi-path Interferometer and a Spectrometer

We have shown that the implementation of a CTES would allow to factorize, in principle, 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 interesting to reproduce the sum in Eq. (5) with an analogue technique, to solve the problem quickly.

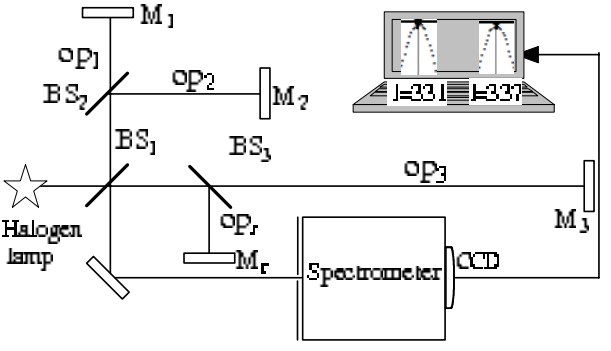

Fig. 4. Experimental setup: generalized symmetric $M+1$-path Michelson interferometer for the realization of truncated exponential sum with truncation parameter $M=3$. Such a setup consists of a polychromatic source (halogen lamp), M balanced beam splitters BS_1, BS_2 and BS_3, the mirrors M_r and M_m, with $m=1,2,3$, and a spectrometer connected to a CCD camera. The $M=3$ interfering paths can be varied respect to the reference path op_r, by moving longitudinally the mirrors M_m, with $m=1,2,3$, respect to the reference mirror M_r, so that the relative difference is given by $op_m \equiv m^j u$, with $u = Nu_N$ where N is the number to factorize.

We introduce an interesting analogue procedure which allows to reproduce the interfering phases terms in Eq. (6). Such a procedure is based on the wave nature of light. In fact the light emitted by a source is characterized by electromagnetic phases of the form $\phi(\lambda) = 2\pi x/\lambda$, which allow to encode the exponential phases $(m-1)^j$ in the optical paths x and the continuous variable ξ, associated with all the possible trial factors, in the wavelengths λ. Moreover, a polychromatic source of light contains a broad range of wavelengths and thereby allows us to test trial factors simultaneously.

In particular, the algorithm described in the previous sections can be implemented, using an $M+1$-path symmetric Michelson interferometer in free space, shown in Fig. 4, for the case $M=3$[1]. The system includes M balanced beam splitters and $M+1$ mirrors. The M interfering paths, whose values op_m, with $m=1,2,..,M$, are measured relative to a reference path op_r. We can encode the phase terms $(m-1)^j$ in Eq. (6), with $m=1,2,3$, in the relative optical paths:

$$op_m^{u,j} \equiv (m-1)^j u, \tag{11}$$

for $m=1,2,3$, with j integer larger than 1, and u suitable unit of length, leading to the interfering phase terms

$$\phi_m(\lambda/u) \equiv 2\pi(m-1)^j/(\lambda/u). \tag{12}$$

For $m=1$ the optical path is equal to the reference path.

[1] The actual experimental results, obtained implementing this procedure, will be presented in an incoming paper [5].

We can use a polychromatic source so that the output interference pattern, measured by a spectrometer connected to a CCD, at the output port of the interferometer, is a continuous function of the wavelengths λ associated with the bandwidth of the source.

Such an intensity pattern $I(\lambda)$ is given by the superposition of the $M = 3$ interfering terms $\exp[i\,\phi_m(\lambda)]$. When we normalize the output intensity respect to the source intensity, we obtain

$$I(\xi) \equiv |\mathcal{C}^{(M,j)}(\xi)|^2, \tag{13}$$

i.e. the modulo squared of the CTGS $\mathcal{C}^{(M,j)}(\xi)$, in Eq. (5), as a function of the dimensionless real parameter

$$\xi \equiv \lambda/u. \tag{14}$$

As stated before, the periodicity of the recorded interferogram in Eq. (13) as a result of a destructive/constructive interference effect, allows us to extract all the information in the function $f(\xi)$, in Eq. (1), necessary to factorize an arbitrary number N, by exploiting the scaling law in Eq. (2).

In fact, we can rescale the obtained intensity pattern for the factorization of an arbitrary number N:

$$I(\xi_N) \equiv |\mathcal{C}^{(M,j)}(\xi_N)|^2, \tag{15}$$

with $|\mathcal{C}^{(M,j)}(\xi_N)|^2$ given by Eq. (7), and ξ_N rescaled variable in Eq. (2).

The presented analogue procedure allows to test all trial factors simultaneously by using a polychromatic source interferometer. The resulting interference pattern, when observed as a function of wavelength, contains the information about all factors of any arbitrary number N. We only have to extract the information from this pattern. The information is encoded in the location of the maxima of the interferogram. When a maximum is at an integer value l of the variable ξ_N in Eq. (2), we have found a factor of $N = p \cdot q$.

5 Conclusion

In the present paper we have introduced a new factorization algorithm, based on the analogue determination of the periodicity of a generalized CTES exploiting a physical interference process. We have demonstrated that the key of such algorithm stands on the destructive/constructive interference associated with the recorded CTES interferogram, which allows to extract all the information about the factors of arbitrary numbers, contained in the experimentally computed ratio $f(\lambda) \doteq u/\lambda \equiv f(\xi) \doteq 1/\xi$, by exploiting the scaling relation in Eq. 2 which defines the variable ξ_N we use for representing f. Such a scaling property of the interferogram allows to rescale the periodicity of the same recorded pattern, in order to factorize, in principle, arbitrary numbers N, looking at the maxima at integer values of the corresponding variable ξ_N.

References

1. Shor, P.: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20-22, pp. 124–134. IEEE Computer Society Press, Los Alamitos (1994)
2. Merkel, W., Wölk, S., Schleich, W.P., Averbukh, I.Sh., Girard, B.: Factorization of numbers with Gauss sums and laser pulses: I. Mathematical background (to be published)
3. Merkel, W., Wölk, S., Schleich, W.P., Averbukh, I.Sh., Girard, B., Paulus, G.G.: Factorization of numbers with Gauss sums and laser pulses: II. Suggestions of implementation (to be published)
4. Merkel, W., Averbukh, I.Sh., Girard, B., Paulus, G.G., Schleich, W.P.: Fortschr. Phys. 54, 856–865 (2006)
5. Tamma, V., Zhang, H., He, X., Garuccio, A., Schleich, W.P., Shih, Y.: Factoring numbers with a single interferogram. Submitted to Nature Photonics
6. Wölk, S., Feiler, C., Schleich, W.P.: J. Mod. Opt. (2009)
7. Clauser, J.F., Dowling, J.P.: Phys. Rev. A 53, 4587–4590 (1996)
8. Summhammer, J.: Phys. Rev. A 56, 4324–4326 (1997)
9. Rangelov, A.A.: J. Phys. B: At. Mol. Opt. Phys. 42, 021002 (2009)
10. Stefanak, M., Merkel, W., Schleich, W.P., Haase, D., Maier, H.: New J. Phys. 9(370), 1–18 (2007)
11. Stefanak, M., Merkel, W., Schleich, W.P., Haase, D., Maier, H.: J. Phys. A: Math. Theor. 41, 304024 (2008)
12. Mehring, M., Müller, K., Averbukh, I.Sh., Merkel, W., Schleich, W.P.: Phys. Rev. Lett. 98, 120502 (2007)
13. Mahesh, T.S., Rajendran, N., Peng, X., Suter, D.: Phys. Rev. A 75, 062303 (2007)
14. Gilowsky, M., Wendrich, T., Muller, T., Jentsch, Ch., Ertmer, W., Rasel, E.M., Schleich, W.P.: Phys. Rev. Lett. 100, 030201 (2008)
15. Bigourd, D., Chatel, B., Schleich, W.P., Girard, B.: Phys. Rev. Lett. 100, 030202 (2008)
16. Sadgrove, M., Kumar, S., Nakagawa, K.: Phys. Rev. Lett. 101, 180502 (2008)
17. Weber, S., Chatel, B., Girard, B.: EPL 83, 34008 (2008)
18. Peng, X., Suter, D.: EPL 84, 40006 (2008)
19. Jones, J.A.: Phys. Lett. A 372, 5758–5759 (2008)