EPL, **84** (2008) 40006
doi: 10.1209/0295-5075/84/40006

www.epljournal.org

NMR implementation of factoring large numbers with Gauß sums: Suppression of ghost factors

X. Peng[(a)] and D. Suter[(b)]

Fakultät Physik, Technische Universität Dortmund - 44221 Dortmund, Germany, EU

received 13 July 2008; accepted in final form 6 October 2008
published online 10 November 2008

PACS 03.67.Lx – Quantum computation architectures and implementations
PACS 02.10.De – Algebraic structures and number theory
PACS 82.56.-b – Nuclear magnetic resonance

Abstract – Finding the factors of an integer can be achieved by various experimental techniques, based on an algorithm developed by Schleich *et al.* (*Fortschr. Phys.*, **54** (2006) 856), which uses specific properties of Gauß sums. Experimental limitations usually require truncation of these series, but if the truncation parameter is too small, it is no longer possible to distinguish between factors and so-called "ghost" factors. Here, we discuss two techniques for distinguishing between true factors and ghost factors while keeping the number of terms in the sum constant or only slowly increasing. We experimentally test these modified algorithms in a nuclear spin system, using NMR.

Introduction. – Factorization of large numbers is a computationally hard problem: the computational resources required to accomplish this task increase exponentially with the number of digits [1] for all algorithms discovered until 1994. Then Peter Shor developed an algorithm that can solve the task in polynomial time. This algorithm requires a computational device that operates according to the laws of quantum mechanics, storing information in quantum states and performing logical operations as unitary evolutions under suitable Hamiltonians [2]. Experimental implementations of Shor's factorization algorithm were demonstrated first with nuclear spins as qubits [3], and recently with photonic qubits [4,5].

More recently, another factorization algorithm was proposed by Schleich and co-workers [6–9] which uses properties of Gauß sums. A complete normalized quadratic Gauß sum is defined by

$$\mathcal{A}_N^{l-1}(l)=\frac{1}{l}\sum_{m=0}^{l-1}\exp\left[2\pi i m^2\frac{N}{l}\right], \qquad (1)$$

where N is the integer to be factorized and l is the trial factor. If l is a factor of N, *i.e.*, N/l is an integer, the resulting sum is $|\mathcal{A}_N^{l-1}(l)|=1$. In all other cases, $|\mathcal{A}_N^{l-1}(l)|<1$.

The number of terms that has to be evaluated for the complete Gauß sum of eq. (1) grows as $\sum_{l=1}^{\sqrt{N}} l=\frac{1}{2}\sqrt{N}(\sqrt{N}-1)\propto N$. A factorization algorithm on the basis of eq. (1) is thus computationally very expensive. However, in most cases, a complete evaluation is not necessary. Recent experimental implementations using NMR [10,11], cold atoms [12] and ultra-short laser pulses [13] have successfully demonstrated that it is usually possible to truncate the sums after a relatively small number of terms. We write the corresponding truncated sums as

$$\mathcal{A}_N^{M}(l)=\frac{1}{M+1}\sum_{m=0}^{M}\exp\left[2\pi i m^2\frac{N}{l}\right], \qquad (2)$$

with a constant truncation parameter M for each argument l, instead of the upper limit $l-1$ in the complete Gauß sum of eq. (1). Accordingly, only $M\sqrt{N}$ terms have to be added, greatly improving the efficiency and precision of the experiments. However, the truncation of the Gauß sum weakens the discrimination of the factors from non-factors, resulting in the appearance of "ghost" factors, whose Gauß sums are close to unity. The requirement of suppressing these "ghost" factors thus sets a lower limit on the choice of the truncation parameter M.

[(a)] Present address: Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China - Hefei, Anhui 230026, PRC; E-mail: xhpeng@ustc.edu.cn

[(b)] E-mail: dieter.suter@uni-dortmund.de

The choice of an optimal truncation parameter M was discussed in a recent paper by Stefanák *et al.* [14]. They found an upper bound on the truncation parameter $M \sim \sqrt[4]{N}$, which represents a sufficient and necessary condition for the success of the Gauß sum factorization scheme. Here, we experimentally explore this issue, using liquid-state NMR for the evaluation of the Gauß sums. Furthermore, we demonstrate additional possible ways of reducing the truncation parameter M, while keeping excellent contrast between factors and non-factors.

Effect of truncation. – The choice of the truncation parameter M plays a crucial role in the success of the Gauß sum factorization scheme. In the previous experiments, the visibility of the resulting factorization interference pattern was high enough for successful factorization of, *e.g.*, the eight-digit number $N = 52882363$ by logarithmically choosing the truncation parameter $M = \ln N$ [10,11]. However, in some cases, we also observed some "ghost" factors. Like in ref. [14], we define those trial factors for which the absolute value of the truncated Gauß sum is larger than the threshold value $1/\sqrt{2}$ as "ghost" factors.

As Stefanák *et al.* showed [14], this sum behavior for different trial factors is best analyzed by considering the fractional part of $2N/l$,

$$\epsilon(N,l) = \frac{2N}{l} - 2k \qquad (3)$$

with $|\epsilon| \leqslant 1$. Here $2k$ is the closest even integer to $2N/l$. Since $\exp(i2\pi m^2 k) = 1$, the Gauß sum (2) can be rewritten as

$$\mathcal{A}_N^M(l) = s_M(\epsilon) \equiv \frac{1}{M+1}\sum_{m=0}^{M} \exp(i\pi m^2 \epsilon), \qquad (4)$$

where $s_M(\epsilon)$ is the normalized curlicue function, which has the property:

$$s_M(\epsilon) = \begin{cases} 1, & \epsilon = 0, \quad \text{for all factors,} \\ \frac{1}{\sqrt{2}}, & \epsilon = 0.5, \quad \text{for threshold non-factors,} \\ 0, & \epsilon \to 1, \quad \text{for typical non-factors.} \end{cases} \qquad (5)$$

Here three different classes for the trial factors are defined [14]. For the class of the ghost factors, the curlicue function depends on the truncation parameter M:

$$s_M(\epsilon) \xrightarrow{\epsilon \to 0} \begin{cases} 1, & \text{for a small } M, \\ 0, & \text{for a very large } M. \end{cases} \qquad (6)$$

Ghost factors occur when ϵ is very close to zero and the Gauß sum is truncated after too few terms. Figure 1 illustrates this behavior: for a given ϵ, the number of terms M needed to suppress the value of $s_M(\epsilon)$ below the threshold $1/\sqrt{2}$ is $\approx 1/\sqrt{\epsilon}$.

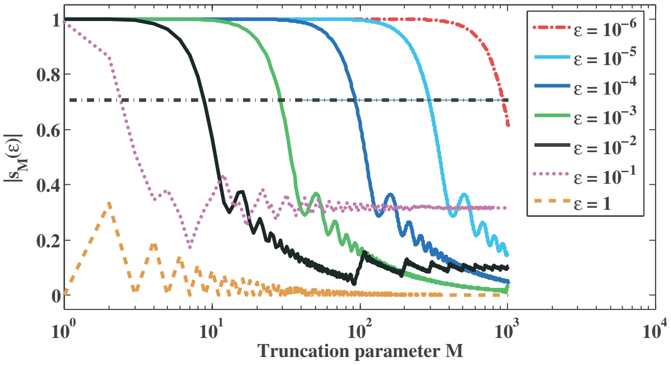
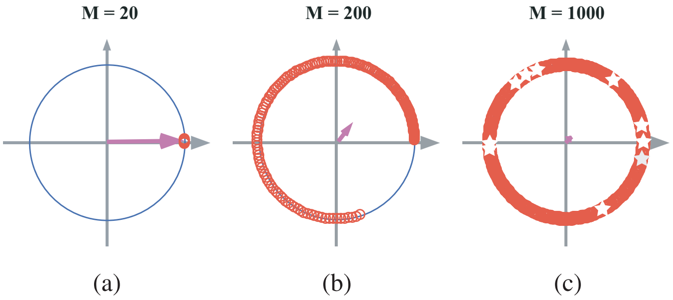


Fig. 1: (Colour on-line) Absolute values $|s_M(\epsilon)|$ of the normalized curlicue function *vs.* the truncation parameter M for different values of ϵ.



(a) (b) (c)

Fig. 2: (Colour on-line) Distribution of the phases $\phi_m = \pi m^2 \epsilon$ for a fractional part $\epsilon(N,l) = 4 \times 10^{-5}$ for different truncation parameters M: (a) $M = 20$, (b) $M = 200$ and (c) $M = 1000$. The individual terms of the Gauß sums are represented by red circles. The arrows from the origin $(0,0)$ represent the resulting truncated Gauß sums of eq. (2), whose absolute values are, respectively, $|s_{M=20}| \approx 1$, $|s_{M=200}| \approx 0.3155$ and $|s_{M=1000}| \approx 0.0770$. In (c) the white stars on the circle are the random phases created by a randomized procedure: 10 values of m were randomly chosen from the range $[0, M_{max}]$. Their sum is ≈ 0.0023, very close to the origin.

Figure 2 illustrates how ghost factors occur for small ϵ: the three parts of the figure show the distribution of the different terms of a Gauß sum in the complex plane for (a) $M = 20$, (b) 200, and (c) 1000 terms for $\epsilon = 4 \times 10^{-5}$: only in the third case are the phases of the terms sufficiently well distributed that the sum (shown as the blue line) approaches zero.

Randomized selection of terms. – Suppressing all ghost factors of truncated Gauß sums below the threshold $1/\sqrt{2}$, requires $M \sim \sqrt[4]{N}$ [14]. This may still be too large for experimental factorization of large integers, *e.g.*, $M \approx 1000$ for the factorization of a 12-digit integer requires extreme precision in the experimental implementation and may lead to excessive decoherence. However, the number of terms in the sum can be reduced significantly below the $\sqrt[4]{N}$ threshold by a suitable choice of the terms that are evaluated: instead of evaluating all terms with $0 \leqslant m \leqslant M$, we randomly choose a relatively small fraction of the terms with $m \in [0, M \sim \sqrt[4]{N}]$.

As a test of this procedure, we select a "difficult" case, where the conventional procedure requires a large truncation parameter. Such cases occur, *e.g.*, for numbers that are products of neighboring primes. We chose as an experimental example the product of the 100000th and 100001th prime,

$$N = 1689259081189 = 1299709 \times 1299721.$$

In the experiments, we implement the procedure by adding nuclear spin coherence, using the ${}^1\text{H}(I=\frac{1}{2})$ nuclear spins of water, diluted in D_2O. The nuclear system was contolled by suitable radio-frequency (rf) magnetic fields [10]. In the rotating frame, an rf pulse with duration τ, amplitude ω and phase ϕ_m generates the unitary operator

$$U_m = \exp(-i\theta(I_x \cos\phi_m + I_y \sin\phi_m)), \tag{7}$$

where $I_{x,y}$ are the components of the spin angular-momentum operator $\mathbf{I}$. The lower index m indicates that the Hamiltonian is specific for each term in the Gauß sum. The flip angle $\theta = \omega\tau$ represents the absolute value and ϕ_m the phase of a complex number in the series, corresponding to $\phi_m(l) = 2\pi m^2 \frac{N}{l}$ in the Gauß sum. Here $\tau \approx 0.5\,\mu\text{s}$ to guarantee the linear-response range $(M+1)\theta \ll \pi/2$. The sum was realized in the experiment by applying a sequence of $M+1$ rf pulses with small flip angle to the spins, with the phase of each pulse equal to that of the corresponding term of the Gauß sum [10]. A short delay ($5\,\mu$s) was inserted between the pulses. The combined effect of these pulses can be described by the propagator $U(l) = U_M \cdots U_0$.

In the limit of small flip angles, $M\theta \ll 1$, the operators in the exponent approximately commute and the propagator can be approximated by

$$U(l) \approx \exp\left\{-i\theta \sum_{m=0}^{M} [I_x \cos\phi_m(l) + I_y \sin\phi_m(l)]\right\}. \tag{8}$$

If l is a factor of N, then $\phi_m(l) = 2k\pi$ with k integer and all $M+1$ pulses have the same phase ($\phi = 0$). In this case, the combined effect of the pulses is $U(l) \approx e^{-i\theta(M+1)I_x}$. If it is applied to the thermal equilibrium state, it creates transverse magnetization I_y, with an amplitude $\propto \theta(M+1)$. If l is not a factor of N, the individual signals interfere destructively and the resulting transverse magnetization is close to zero. For each experiment, the transverse magnetization generated was recorded as a free induction decay (FID).

The experiments were carried out on a 500 MHz Bruker Avance II + NMR spectrometer. Using the standard truncated Gauß sum $\mathcal{A}_N^M(l)$ of eq. (2) with $M = 19$, we obtained experimental results that were indistinguishable from the maximal value of 1 for all trial factors close to the real factors (see upper trace in fig. 3). However, if we use the randomly selected m-values, as few as 10 terms are sufficient to suppress all the non-factors well below the threshold of $1/\sqrt{2}$, as shown in fig. 3 (blue spectra and red dots), while the real factors 1299709 and 1299721 always yielded values close to 1.

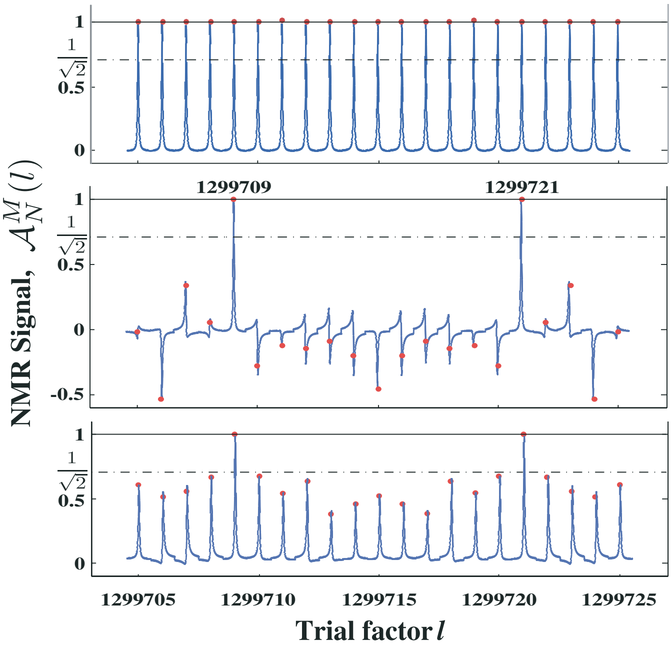


Fig. 3: (Colour on-line) Factorization of $N = 1689259081189$ with $\epsilon_{min} \approx 1.693 \times 10^{-5}$. The upper trace shows the standard truncated Gauß sum with the truncation parameter $M = 19$, the middle trace shows the result of the Monte Carlo procedure with 10 randomly chosen values of m from the range $[0, M_{max} = 1000]$, and the lower trace shows the 5th-order truncated generalized Gauß sum $\mathcal{A}5_N^M$ with the truncation parameter $M = 10$. While all trial factors masked as true factors in the standard truncated procedure (upper trace), the true factors are easily found in the Monte Carlo and generalized Gauß sum procedure.

As the second example, we chose to factorize a 17-digit integer

$$N = 32193216510801043 = 179424673 \times 179424691.$$

Randomly choosing 10 values of m from the range $[0, M_{max} = 5000]$, we experimentally evaluated the partial Gauß sums for the trial factors l between 179424663 and 179424701. The results, shown in fig. 4, clearly show that the factors 179424673 and 179424691 are found and no ghost factors appear.

Generalized Gauß sums. – Truncated generalized Gauß sums can be defined as

$$\mathcal{A}n_N^M(l) = \frac{1}{M+1}\sum_{m=0}^{M} \exp\left[2\pi i m^n \frac{N}{l}\right], \quad n \geqslant 3. \tag{9}$$

In terms of the fractional part $\epsilon(N, L)$ of $2N/l$, they are

$$\mathcal{A}n_N^M(l) = s_M^{(n)}(\epsilon) \equiv \frac{1}{M+1}\sum_{m=0}^{M} \exp\left[\pi i m^n \epsilon\right], \quad n \geqslant 3. \tag{10}$$

The standard case is recovered for $n = 2$. These higher-order generalized Gauß sums can be used for factorization

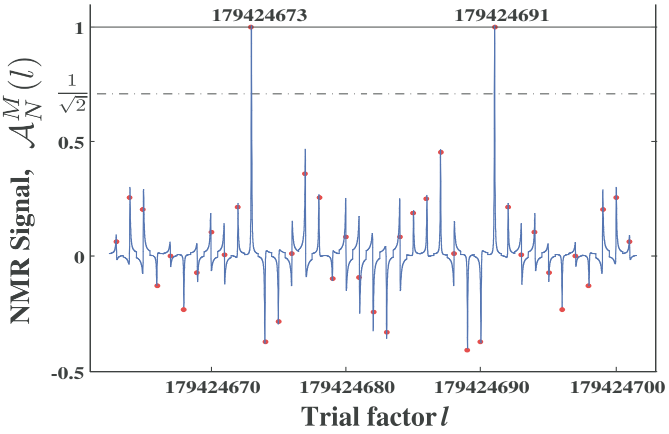


Fig. 4: (Colour on-line) Factorization of $N=32193216510801043$ by the randomized procedure with 10 random phases in $[0, M_{max}=5000]$.

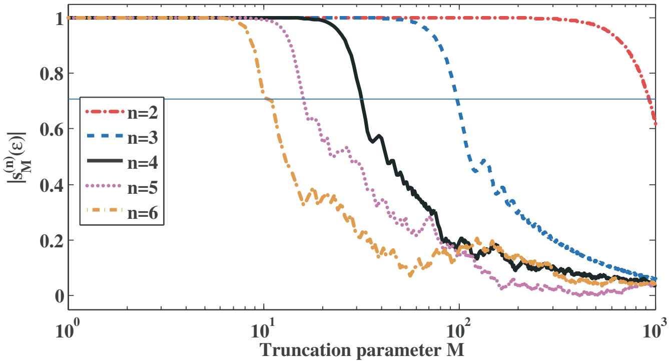


Fig. 5: (Colour on-line) Comparison of the different orders of Gauß sums as a function of the truncation parameter M for a fractional part $\epsilon = 1.0\times 10^{-6}$.

exactly as the second-order function: again, the factors generate constant phases for all terms and thus the maximum of the sum, while non-factors ideally generate sums much smaller than unity. These higher-order generalized Gauß sums can provide higher contrast between factors and non-factors, even for small truncation parameters M. As shown in fig. 5, the higher the order n, the smaller the upper bound of M required to suppress the value of $|s_M^{(n)}|$ below the threshold.

Numerical analysis show that the truncation parameter M required to push all non-factors below the threshold $1/\sqrt{2}$ scales with the order n of the generalized Gauß sum and the size of the number N to be factorized as $M\sim\sqrt[2n]{N}$ [15]. Therefore, to factorize a 12-digit integer, the required value of M decreases from 10^3 to 10 if we use the 6th-order function instead of the quadratic truncated Gauß sum. However the advantage takes the price of the smaller gap between factors and threshold non-factors [15]. The authors also proposed an NMR realization of generalized Gauß sums [16].

We experimentally tested the performance of the higher-order truncated generalized Gauß sums $\mathcal{A}n_N^M$, using the same procedure as for the $n=2$ case. The lower trace of fig. 3 clearly shows that this procedure provides an excellent contrast between factors and non-factors, even for a relatively small number of terms $M=10$.

Conclusion. – Gauß sums [17–19] are ubiquitous in number theory and found many applications, such as Plancherel's theorem on finite groups [20], the Talbot effect of classical optics [21], fractional revivals [22,23], quantum carpets [24] and Josephson junctions [25]. Recently, Gauß sums were also used for factorization, which is related to the proposal of Clauser and Dowling [26] to factor an integer using a familiar Young's N-slit classical interferometer.

In this paper, we presented an experimental investigation on the Gauß sum factorization scheme for large numbers, where ghost factors often appear when the truncation parameter M is relatively small (*e.g.*, $M\sim 15$–20). In these cases, the truncation parameter M must be increased to relatively large numbers, which is undesirable for experimental implementations. To circumvent this increase in the required number of terms, we have introduced a Monte Carlo procedure, where the required number of terms remains roughly constant, and have used higher-order truncated Gauß sums, whose scaling behavior is much more benign than for the second-order function. While we have used a nuclear spin system for the experimental implementation, it should be straightforward to apply this scheme to other (quantum or classical) systems.

* * *

We acknowledge many useful comments from W. Schleich. This work is supported by the DFG through Su 192/19-1.

Additional remark: During the preparation of this paper, we became aware of closely related work [27,28].

REFERENCES

[1] Knuth D. E., *The Art of Computer Programming,* Vol. **2***: Seminumerical Algorithms* (Addison-Wesley, Reading, Mass.) 1998.

[2] Shor P., in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, New York) 1994, p. 124.

[3] Vandersypen L. M. K., Steffen M., Breyta G., Yannoni C. S., Sherwood M. H. and Chuang I. L., *Nature*, **414** (2001) 883.

[4] Lu C.-Y., Browne D. E., Yang T. and Pan J.-W., *Phys. Rev. Lett.*, **99** (2007) 250504.

[5] Lanyon B. P., Weinhold T. J., Langford N. K., Barbieri M., James D. F. V., Gilchrist A. and White A. G., *Phys. Rev. Lett.*, **99** (2007) 250505.

[6] Merkel W., Crasser O., Haug F., Lutz E., Mack H., Freyberger M., Schleich W. P., Averbukh I., Bienert M., Girard B., Maier H. and Paulus G. G., *Int. J. Mod. Phys. B*, **20** (2006) 1893.

[7] Merkel W., Averbukh I. S., Girard B., Paulus G. G. and Schleich W. P., *Fortschr. Phys.*, **54** (2006) 856.

[8] Merkel W., Schleich W. P., Averbukh I. S. and Girard B., *Factorization of numbers with Gauss sums and laser pulses. I. Mathematical Background*, unpublished.

[9] Merkel W., Schleich W. P., Paulus G. G. and Girard B., *Factorization of numbers with laser pulses: II. Engineering a one-photo transition*, unpublished.

[10] Mahesh T. S., Rajendran N., Peng X. and Suter D., *Phys. Rev. A*, **75** (2007) 062303.

[11] Mehring M., Müller K., Averbukh I. S., Merkel W. and Schleich W. P., *Phys. Rev. Lett.*, **98** (2007) 120502.

[12] Gilowski M., Wendrich T., Müller T., Jentsch C., Ertmer W., Rasel E. M. and Schleich W. P., *Phys. Rev. Lett.*, **100** (2008) 030201.

[13] Bigourd D., Chatel B., Schleich W. P. and Girard B., *Phys. Rev. Lett.*, **100** (2008) 030202.

[14] Stefanák M., Merkel W., Schleich W. P., Haase D. and Maier H., *New J. Phys.*, **9** (2007) 370.

[15] Stefanák M., Haase D., Merkel W., Zubairy M. S. and Schleich W. P., *J. Phys. A*, **41** (2008) 304024.

[16] Stefanák M., Merkel W., Mehring M. and Schleich W. P., *NMR implementation of exponential sums for integer factorization,* in *Contemporary Physics, Proceedings of the International Symposium, Islamabad, Pakistan, 26–30 March 2007*, edited by Aslam J., Hussain F. and Riazuddin (World Scientific) 2008, pp. 87–94 .

[17] Lang S., *Algebraic Number Theory* (Addison Wesley, New York) 1970.

[18] Maier H. and Schleich W. P., *Prime Numbers 101: A Primer on Number Theory* (Wiley-VCH, New York) 2007.

[19] Davenport H., *Multiplicative Number Theory* (Springer, New York) 1980.

[20] Yosida K., *Functional Analysis* (Springer Verlag) 1968.

[21] Talbot H. F., *Philos. Mag.*, **9** (1836) 401.

[22] Leichtle C., Averbukh I. S. and Schleich W. P., *Phys. Rev. A*, **54** (1996) 5299.

[23] Leichtle C., Averbukh I. S. and Schleich W. P., *Phys. Rev. Lett.*, **77** (1996) 3999.

[24] Berry M. V., Marzoli I. and Schleich W. P., *Phys. World*, **14** (2001) 39.

[25] Oppenländer J., Häussler C. and Schopohl N., *Phys. Rev. B*, **63** (2000) 024511.

[26] Clauser J. F. and Dowling J. P., *Phys. Rev. A*, **53** (1996) 4587.

[27] Rasel E., in *38th Winter Colloquium on the Physics of Quantum Electronics, Snowbird, US (January 2008)*, to be published in *J. Mod. Opt.*

[28] Weber S., Chatel B. and Girard B., *EPL*, **83** (2008) 34008.