Factorizing numbers with the Gauss sum technique: NMR implementations

T. S. Mahesh, Nageswaran Rajendran, Xinhua Peng, and Dieter Suter*
Fachbereich Physik, Universität Dortmund, 44221 Dortmund, Germany
(Received 29 January 2007; published 4 June 2007)

Several physics-based algorithms for factorizing large numbers were recently presented. A notable recent algorthm by Schleich *et al.* uses Gauss sums for distinguishing between factors and nonfactors. We demonstrate two NMR techniques that evaluate Gauss sums and thus implement their algorithm. The first one is based on differential excitation of a single spin magnetization by a cascade of rf pulses. The second method is based on spatial averaging and selective refocusing of magnetization for Gauss sums corresponding to factors. All factors of 16 637 and 52 882 363 are successfully obtained.

DOI: 10.1103/PhysRevA.75.062303 PACS number(s): 03.67.Lx

I. INTRODUCTION

Given an integer, factorizing it or confirming it to be a prime, is an important problem in network and security systems [1]. Using classical computers with finite resources of memory, the factorization time increases exponentially with the size of the number. In 1994, Shor discovered a quantum algorithm for factorization that takes only polynomial time [2]. Shor's algorithm requires a data register that is large enough to encode the number to be factored along with some ancilla qubits. A practical demonstration has been carried out by factorizing the integer "15" [3], using nuclear magnetic resonance. However, quantum computers capable of implementing Shor's algorithm for larger numbers have not been developed so far.

Another physics-based method for factorizing numbers has been proposed recently by Schleich and co-workers [4–6]. The mathematical basis of the technique relies on the properties of Gauss sums [7]. In contrast to Shor's algorithm, it can be implemented on quantum mechanical as well as on classical systems. Accordingly, it does not provide a speed-up over classical methods.

For the physical implementation, it requires an ensemble of two-level systems, which accumulate the individual terms of the Gauss sum. The sum is obtained by measuring the expectation value as an ensemble average. As specific systems for the implementation of this algorithm, atomic systems driven by resonant lasers have been proposed [8–10], and an implementation by nuclear spins $\frac{1}{2}$ was demonstrated by Mehring *et al.* [11].

Like in Mehring's paper, we also use nuclear spins driven by radio-frequency (rf) pulses, but we use two different approaches that demonstrate the flexibility of the Gauss-sum technique and require fewer rf pulses.

II. GAUSS SUMS BY DIFFERENTIAL EXCITATION

A. Principle

The factorization scheme of Schleich *et al.* relies on sums of the form

$$\sum_{m=-\infty}^{\infty} e^{i2\pi m^2 a}, \tag{1}$$

which are known as Gauss sums [14]. Clearly, the series adds to infinity if a is an integer, and to zero otherwise.

Schleich *et al.* used this property for their factorization scheme by evaluating the truncated series

$$A_N^M(j) = \frac{1}{M+1}\sum_{m=0}^{M} \exp[i\phi_m(j)], \tag{2}$$

where $\phi_m(j)=(2\pi m^2\frac{N}{j})$, N is the number to be factored, the integer j is a trial factor, and M is a truncation number. This truncated series adds up to unity if N/j is an integer, i.e., if j is a factor of N. In all other cases, the sum is a small number whose value depends on the truncation number M,

$$A_N^M(j) = \begin{cases} 1, & \text{if } N/j = \text{integer}, \\ \ll 1, & \text{otherwise}. \end{cases}$$

Physical systems that can implement this scheme must be described by complex numbers. As a first example, consider a pendulum with two degrees of freedom. Its excitation can be described by an amplitude and a direction angle, which can be represented by a single complex number. The individual terms of the Gauss sum are realized by resonant momentum transfers to the pendulum, with the direction specified by the phase of the complex number. If N/j is an integer, the momentum transfers all occur in the same direction and therefore keep increasing the amplitude of the pendulum. In all other cases, the direction will vary and the individual momenta interfere destructively.

A critical aspect of the algorithm is the generation of the phases ϕ_m. This has been discussed in detail in the papers of Schleich *et al.* [4,8–10]. Among the simple solutions, which are directly applicable to implementations by spectroscopy, is a sudden frequency shift by $\Delta\omega$ for a time τ, in such a way that $\phi_m=\Delta\omega\tau$.

B. NMR implementation

For the experimental realization, we choose a different system, which is easier to realize: an ensemble of spins $I=\frac{1}{2}$, which is excited by rf pulses. The Hamiltonian describing the interaction with the rf field is

*Corresponding author. Electronic address: dieter.suter@physik.uni-dortmund.de

 ©2007 The American Physical Society

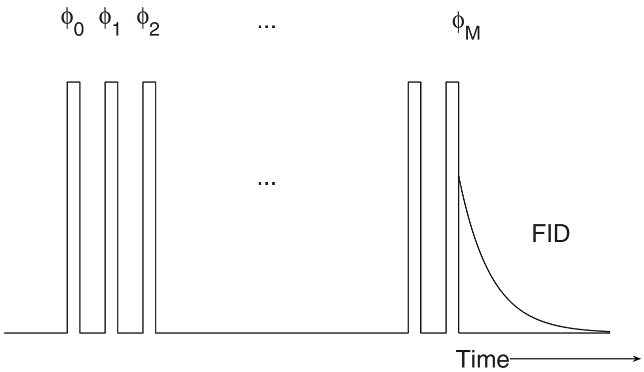

FIG. 1. Pulse sequence for the differential excitation method.

$$\mathcal{H}_m^{\text{eff}} = \omega[I_x \cos \phi_m(j) + I_y \sin \phi_m(j)], \quad (3)$$

where $I_{x,y}$ are the components of the spin angular momentum operator $\mathbf{I}$, ω is the strength of the rf field, and the phase angles $\phi_m(j)$ are equal to the phases of the corresponding terms in the Gauss sum.

If the rf field is applied for a duration τ, it rotates the spins by an angle $\theta = \omega\tau$ around an axis in the xy plane, which is oriented at an angle $\phi_m(j)$ from the x direction. In close analogy to the mechanical pendulum, the effect of the individual rotations adds coherently and reaches a maximum if the rotation axes are the same (i.e., if j factors N). In all other cases, the orientation of the rotation axis is essentially random and the small rotations cancel on average.

Formally, we describe the effect of a single pulse by the propagator

$$U_m(j) = \exp(-i\mathcal{H}_m^{\text{eff}}\tau). \quad (4)$$

As shown in Fig. 1, the Gauss sum is evaluated by applying a sequence of $M+1$ pulses, all with identical flip angle θ but variable phase ϕ_m to the spin system. The combined effect of such a sequence of pulses is given by the propagator

$$U(j) = U_M \cdots U_0 = \prod_{m=M}^{0} \exp\{-i\theta[I_x \cos \phi_m(j) + I_y \sin \phi_m(j)]\}, \quad (5)$$

where $\theta = \omega\tau$. If j is a factor, $\phi_m(j) = 2n\pi$ (with n integer) and therefore the pulses add coherently. The resulting net propagator is then

$$U(j) = \exp[-i(M+1)\theta I_x]. \quad (6)$$

As long as the total rotation angle $\theta(M+1)$ remains small compared to $\pi/2$, the signal observed in the NMR spectrometer is proportional to the angle and can be taken as a measure of the overall rotation. This implies that the individual rotation angles are small, $\theta \ll 1$. Under this condition, the individual terms in Eq. (5) approximately commute and the operator product can be evaluated also for nonfactors. Like in the mechanical analog, the individual contributions then do not add coherently and therefore the effective transverse magnetization remains close to zero.

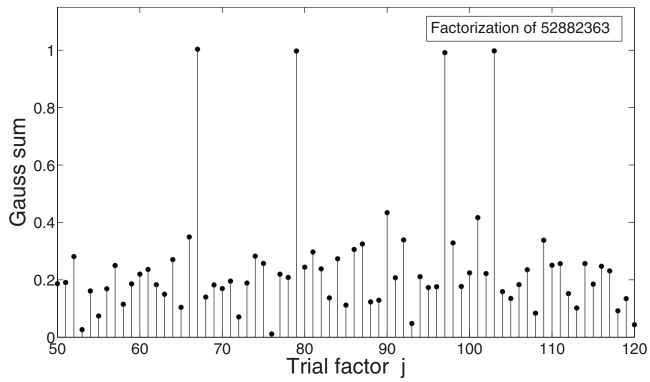

FIG. 2. Factorization of 52 882 363 using the differential excitation method and the truncation number $M=15$.

C. Experimental results

In our experiments, we used the ^{1}H spin of $CHCl_3$ dissolved in Acetone-D_6 as our target system. The experiment was done on a 500 MHz Bruker Avance II+ spectrometer. Initially, the sample was in thermal equilibrium.

Modern NMR spectrometers always rely on direct digital synthesis of the rf signal that is used for excitation and detection. Accordingly, the phase of each pulse is generated digitally. It is thus perfectly possible to implement the frequency-jump method for generating the phases; since the resulting signal is identical to one that is generated by directly programming the phases ϕ_m, we have chosen to compute the phases externally and write them into the pulse program.

The pulse sequence consisted of $(M+1)$ $[\theta]_{\phi_m}$ pulses with the flip angle $\theta = 1°$ and a delay of 5 μs after each pulse, as shown in Fig. 1. Since the reference frame is resonant with the Larmor precession of the spin, the free evolution operators during the delays become unit operators.

At the end of the pulse sequence, we acquired the free induction decay signal, which is proportional to the transverse magnetization. For an accurate determination of its value, we calculated its Fourier transform and integrated over the resonance line. The resulting data were normalized with respect to the reference spectrum (with $\phi_m = 0, \forall m$).

As a first example, we choose to factorize the number $N = 52\,882\,363$. The results are shown in Fig. 2 for trial factors j between 50 and 120. It can be clearly seen that the factors are 67, 79, 97, and 103. The visibility of the data, i.e., the separation between the factors and nonfactors, depends largely on the truncation number M. For this example, we used a relatively small value of $M=15$. For larger values, the relative separation can be increased significantly.

III. GAUSS SUMS BY SPATIAL AVERAGING

Using the principles outlined above, many similar experiments can be conceived that achieve the same objective. As a second example, we choose the case that is summarized in Fig. 3. Here, we also encode the individual terms of the Gauss sum in the phase of rf pulses. In this case, we choose the flip angle θ of the individual pulses such that the total flip angle adds up to

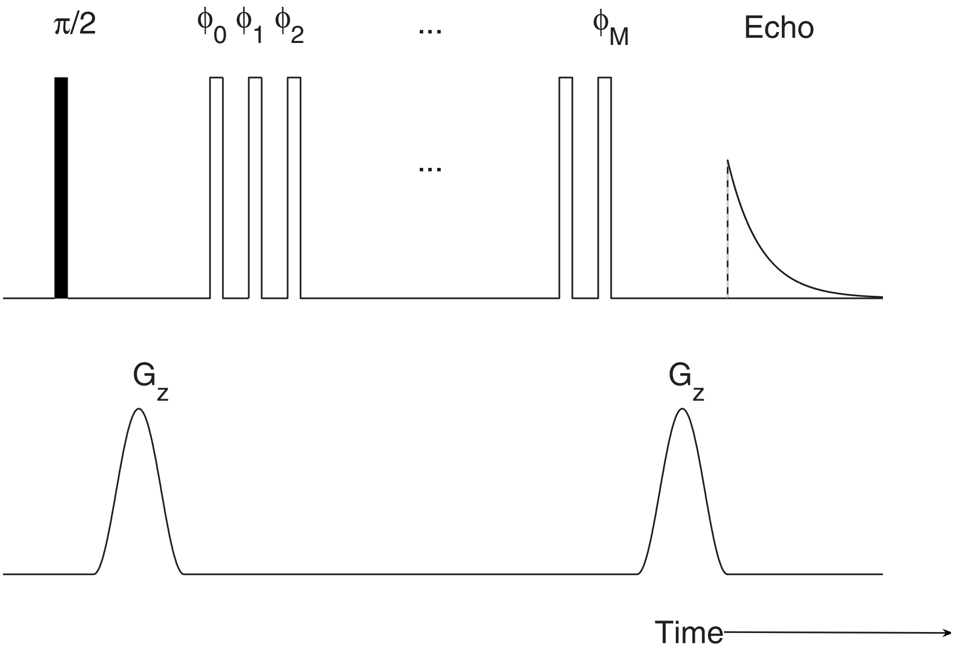

FIG. 3. Pulse sequence for the spatial averaging method. The initial pulse is an rf pulse that creates transverse magnetization. The Gaussian-shaped second pulse is a magnetic field gradient pulse, and the subsequent rectangular pulses are rf pulses with flip angle θ and phase ϕ_m.

$$(M+1)\theta = \pi \tag{7}$$

for factors. [More generally, it may be any angle $(2n+1)\pi$ with n integer.]

This sequence of pulses is applied to a state where transverse magnetization has been dephased by a magnetic field gradient pulse. Starting from thermal equilibrium, where the density operator of the system is proportional to I_z, the excitation pulse creates I_x magnetization. The field-gradient pulse turns this into

$$I_x \xrightarrow{G_z} I_x \cos \alpha_z + I_y \sin \alpha_z, \tag{8}$$

where α_z is the position(z)-dependent dephasing introduced by the gradient

$$\alpha_z = \gamma G_z z T, \tag{9}$$

with γ the gyromagnetic ratio, G_z the field gradient, z the coordinate in the direction of the gradient, and T the duration of the gradient pulse. The total signal, which is the integral of I_x over space, vanishes at this point. For factors j, the combined effect of the pulse sequence is a π rotation, which inverts the accumulated phase, independent of the position z [12],

$$I_x \cos \alpha_z + I_y \sin \alpha_z \xrightarrow{\pi_x} I_x \cos \alpha_z - I_y \sin \alpha_z. \tag{10}$$

When the second field gradient pulse acts on this state, it adds another phase α_z, which is identical to the first. The final state is thus

$$I_x \cos \alpha_z - I_y \sin \alpha_z \xrightarrow{G_z} (I_x \cos \alpha_z + I_y \sin \alpha_z)\cos \alpha_z - (I_y \cos \alpha_z - I_x \sin \alpha_z)\sin \alpha_z = I_x, \tag{11}$$

i.e., the magnetization gets back into phase and an echo is observed. This holds only for terms where j is a factor of N; for the others, the total effect of the sequence of $M+1$ pulses is not a phase reversal, but only a small rotation, which cannot refocus the magnetization. In the experimental implementation, we used this scheme to determine the factors of the number 16 637. Figure 4 shows the experimental results for the trial factors j between 120 and 140, when the sequence is truncated at $M=12$. Again, we can clearly distinguish between the factors (127 and 131) from the nonfactors.

IV. CONCLUSION

Interference between different wave packets is an important feature of quantum mechanics. Schleich *et al.* have used this property to evaluate Gauss sums and show how this can be used to determine if a given number is a factor of another number. Their procedure is related to the proposal of Clauser and Dowling [13] who used optical interferometry for factorization.

In this paper, we discuss specific physical systems that implement such a summation and give experimental examples that determine the factors of a given number. In par-

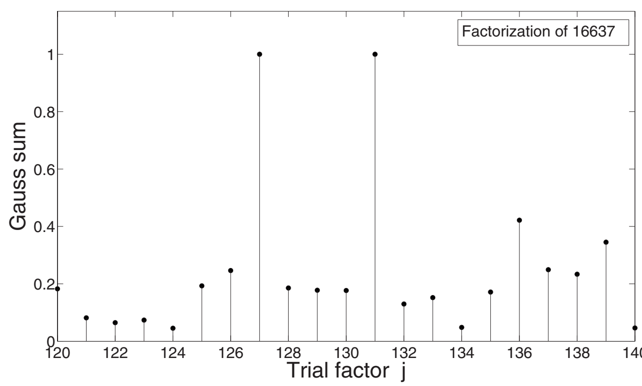

FIG. 4. Factorization of 16 637 using the spatial averaging method with the truncation number $M=12$.

ticular, we show two NMR experiments that calculate Gauss sums and apply them to find the factors of numbers with five and eight decimal digits.

The two techniques differ with respect to the conditions on the flip angles as well as with respect to the required initial condition. We found that the visibility of the resulting scans is quite high, even for small truncation numbers $M \sim 12-15$. For larger numbers, it might be necessary to use larger values of M to obtain sufficient contrast between the factors and nonfactors.

The spin system that we use for the implementation can be completely specified in terms of a two-dimensional Hilbert space. Accordingly, the dynamics of the system can also be described in classical terms and the algorithm may not be considered a quantum algorithm. This fact is also evidenced by the example that we discussed (a classical pendulum). In contrast to Shor's algorithm, this algorithm is no more efficient than known classical algorithms.

ACKNOWLEDGMENTS

This work was initiated by W. Schleich and M. Mehring, who also communicated their papers to the authors. The authors thank Jingfu Zhang for his help in setting up the spectrometer and for useful discussions. The authors gratefully acknowledge financial support from the Alexander von Humboldt Foundation, GK-726 Materials and Quantum Information Processing, and the DFG through Grants Nos. Su192/19-1 and Su192/11-1.

[1] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed. (Springer-Verlag, Berlin, 1994).
[2] P. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, New York, 1994), p. 124.
[3] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature (London) **414**, 833 (2001).
[4] W. Merkel, I. S. Averbukh, B. Girard, G. G. Paulus, and W. P. Schleich, Fortschr. Phys. **54**, 856 (2006).
[5] H. Mack, M. Bienert, F. Haug, F. S. Straub, M. Freyberger, and W. P. Schleich, Phys. Status Solidi B **233**, 403 (2002).
[6] H. Mack, M. Bienert, F. Haug, F. S. Straub, M. Freyberger, and W. P. Schliech, in *Proceedings of the Enrico Fermi Summer School, Course CXLVIII*, edited by P. Mataloni and F. D. Maritini (Elsevier, Amsterdam, 2002), pp. 369–383.
[7] W. Merkel, W. P. Schleich, I. S. Averbukh, and B. Girard (unpublished).
[8] W. Merkel, O. Crasser, F. Haug, E. Lutz, H. Mack, M. Freyberger, and W. P. Schleich, Int. J. Mod. Phys. B **20**, 1893 (2006).
[9] W. Merkel, H. Mack, E. Lutz, W. P. Schleich, G. G. Paulus, and B. Girard, e-print arXiv:quant-ph/0702122.
[10] W. Merkel, W. P. Schleich, G. G. Paulus, and I. S. Averbukh (unpublished).
[11] M. Mehring, K. Müller, I. S. Averbukh, W. Merkel, and W. P. Schleich, e-print arXiv:quant-ph/0609174.
[12] E. L. Hahn, Phys. Rev. **80**, 580 (1950).
[13] J. F. Clauser and J. P. Dowling, Phys. Rev. A **53**, 4587 (1996).
[14] Instead of 2, other exponents could also be used. However, as in the papers of Schleich *et al.*, we will restrict ourselves to 2, which provides efficient randomization.