Eliminating Ghost Factors in Truncated Gauss-Sum Factorization

R. M. Caplan

May 6, 2009

1 Introduction

The factorization of large numbers is very important in cryptography and communications. Computing such large factorizations on a standard computer quickly becomes computationally difficult. Recently, researchers have found ways to use physical systems to factor large numbers by having the physical system compute Truncated Gauss Sums (TGS) [1]. Such systems include collections of ultra-cold atoms (such as Bose-Einstein Condensates) [2] and Nuclear Magnetic Resonance spectroscopy of spin-1/2 atoms [3].

In most of the experimental realizations, the number of terms in the TGS must be kept low for the experiments to work correctly/cheaply. However, in so doing, the TGS exhibits what are known as ghost factors, which are trial factors which can appear as factors in the TGS pattern. As one increases the number of terms in the TGS, the number of ghost factors decreases.

In [4], it was found that in order to suppress all ghost factors for any number N, one needs the number of terms in the TGS to scale as $\sqrt[4]{N}$. Unfortunately, this may be too restrictive for experiments.

In this work we try to find a way to eliminate the ghost factor problem but without requiring the large number of terms in the TGS. Our method relies on doing multiple experiments for nearby numbers to lower the requirements on M. We find that our method does allow one to lower the requires M, but in so doing, increases the total computation needed. However, it is assumed here that for real world experiments, lowering M is more important than lowering the total computational cost (since the computations are being performed by a physical system).

2 Truncated Gauss Sum Factorization and Ghost Factors

Here we review what TGSs are, and how they are used to factor numbers. We also describe the ghost factors and the problems they cause.

The full quadratic Gauss sum is defined as:

$$A_N^{l-1}(l) = \frac{1}{l}\sum_{m=0}^{l-1} \exp\left(2\pi i m^2 \frac{N}{l}\right), \tag{1}$$

where N is the number to be factored, and $l \in [1, \lfloor\sqrt{N}\rfloor]$. The way factors are found using the sum is that if l is a factor of N then all terms become equal to one, so the total Gauss sum yields the value one. Any other value indicates that l is not a factor of N. $|A_N^{l-1}|$ is referred to as the factorization interference pattern. An example interference pattern is shown in Fig. 1. We see that for the full Gauss sum, factors and nonfactors are very easy to differentiate.

The total number of terms that need to be computed and added in the full Gauss sum is:

$$T_{\mathrm{FGS}} = \frac{1}{2}\sqrt{N}(\sqrt{N}-1) = \frac{1}{2}(N-\sqrt{N}) \sim N. \tag{2}$$

In physical experimental computations of Gauss sums, the number of terms in the summation for each trial factor l, corresponds to number of pulses, light fields, or other physical setups. When the number of terms

is too large, the system becomes hard to use (because of such effects such as decoherence), therefore what is used is the truncated Gauss sum which has a fixed number of terms in the sum for all l:

$$A_N^M(l) = \frac{1}{M+1} \sum_{m=0}^{M} \exp\left(2\pi i m^2 \frac{N}{l}\right), \tag{3}$$

where M is the fixed value of terms to sum. The total number of computations is now:

$$T_{\mathrm{TGS}} = M\sqrt{N}. \tag{4}$$

The choice of M is very important because when M is low, one sees what are referred to as 'ghost factors'. Ghost factors are trial factors (values of l) which yield values of $|A_N^M(l)|$ close to 1, which, due to experimental measuring error, may be misinterpreted as being factors of N. Although typically this is easily checked manually, for very large N, this may be enormous numbers of ghost factors which make checking each one undesirable. Therefore one would like to have M as small as possible, while avoiding ghost factors. In Fig. 1 we show the factorization interference patterns for $N = 11223344$ using a full and truncated Gauss sum (with $M = 3$). True factors are demarcated by the vertical blue lines. We see that in this example, the TGS exhibits many ghost factors which could easily be mistaken for true factors.

3 Fourth-Root Optimal Scaling Law

In Ref. [4], the scaling properties of the number of ghost factors versus M was studied in order to find a value for M which guarantees that there will be no ghost factors (as defined by a TGS value over a threshold of $|A_N^M| = 1/\sqrt{2}$) for all N. We summarize their analysis and results here in order to provide a background to our new approach.

We can rewrite the TGS as:

$$A_N^{(M)}(l) = s_M(\rho(N,l)), \tag{5}$$

where $s_M(\tau)$ is called the normalized curlicue function, and is defined as:

$$s_M(\tau) = \frac{1}{M+1} \sum_{m=0}^{M} \exp(i\pi m^2 \tau), \tag{6}$$

and $\rho(N,l)$ is the fractional part of $2N/l$ which we write as:

$$\rho(N,l) = \frac{p}{q} = \frac{2N}{l} - 2k, \tag{7}$$

where $2k$ is the closest integer (up or down) to $2N/l$. We see that $\rho \in [-1,1]$. To see the relationships between these equations, we plot an example case with $M = 3$ and $N = 14123$ in Fig. 2. We also plot the curlicus function as a function of both τ and M. We can see that ghost factors occur for values of $|s_M(\tau)|$ in the central peak near $\tau = 0$. This peak narrows as M is increased, and as $M \to \infty$, it collapses to the value 1 for $\tau = 0$ (which corresponds to true factors). It is shown in Ref. [4] that for large M, $|s_M(\tau)|$ is bounded from above by $1/\sqrt{2}$ (this bound corresponds to the 2 prominent side peaks in $s_M(\tau)$). Therefore, this value is used as the definition of a ghost factor, i.e. any trial factor with $|A| > 1/\sqrt{2}$ is considered a ghost factor. Although experimental error may be more accurate then this, changing the threshold only changes the prefactor on the ghost factor scaling, and so we keep the threshold at $1/\sqrt{2}$.

The advantage of rewriting the TGS in the form of Eq. (5) is that we can analyze $s_M(\tau)$ independent of a specific N and l. We know that ghost factors occur only very close to $\tau = 0$, so by assuming τ to be small, we can approximate the sum $s_M(\tau)$ as an integral:

$$s_M(\tau) \approx \frac{1}{M} \int_0^M du \exp(i\pi m^2 \tau) = \frac{F(M\sqrt{2\tau})}{M\sqrt{2\tau}}, \tag{8}$$

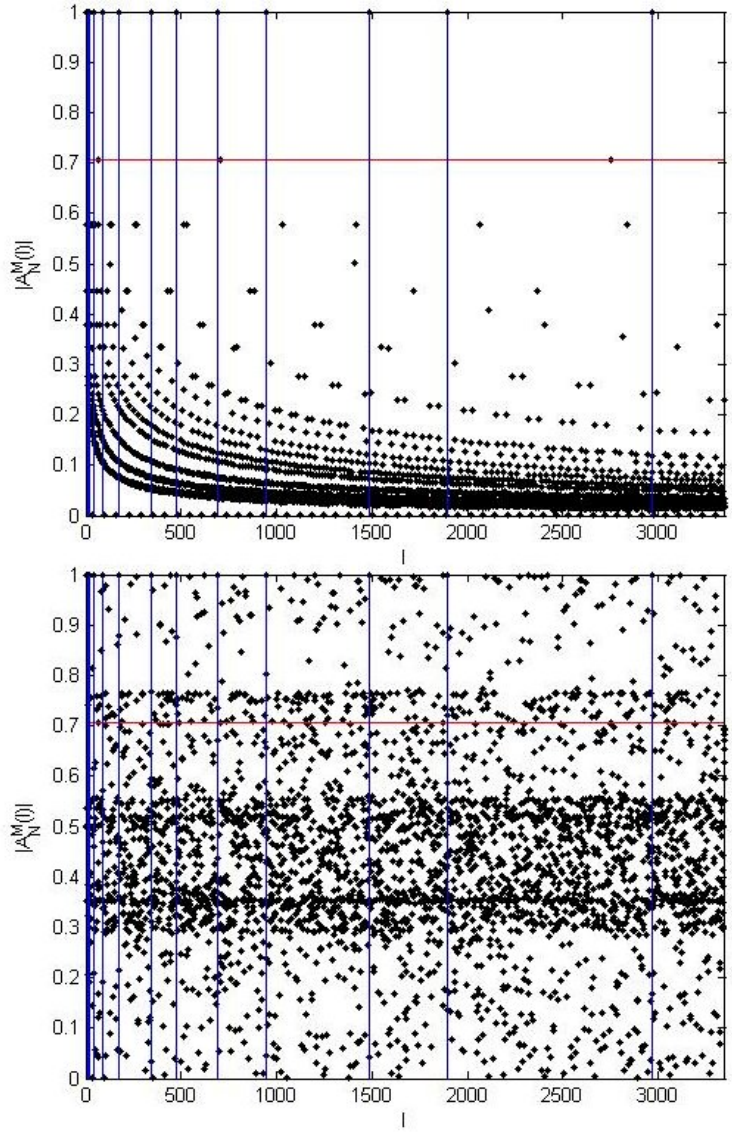

Figure 1: Comparison between the factorization interference pattern of $N = 11223344$ of the full Gauss sum (top) and a truncated Gauss sum with $M = 3$ (bottom). True factors are marked by the vertical blue lines. We can clearly see how the TGS results in ghost factors, which appear to the eye as true factors of N.

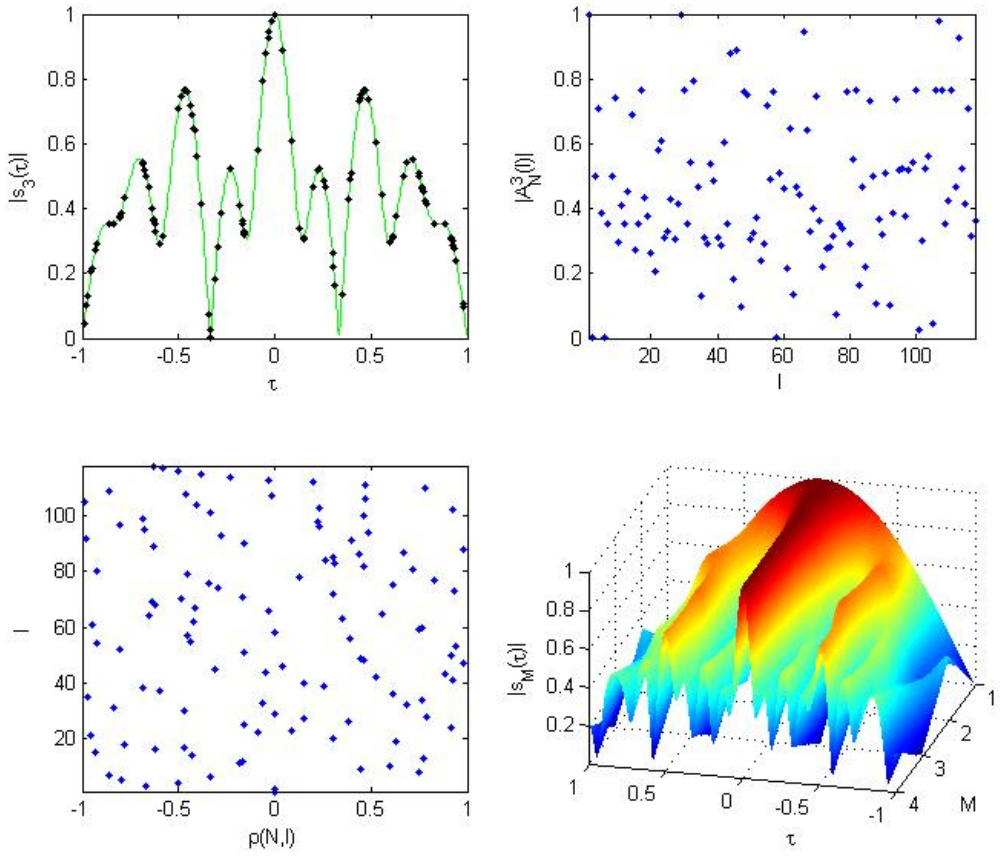

Figure 2: An example of the normalized curlicus function (top left), TGS (top right) and the fractional part of $2N/l$ (bottom left) for $N = 14123$ and $M = 3$. To see the relation between the functions, one can follow the fractional part up to the curlicus function, and then trace it over to the TGS. It is apparent that ghost factors occur for small values of *tau* in the central peak of the curlicus function. This peak diminishes as one increases M as can be seen in the surf plot of $|s_M(\tau)|$ (bottom right).

where $u = \sqrt{2\tau}m$ and F is the Fresnel integral:

$$F(x) = \int_0^x du \exp\left(i\frac{\pi}{2}u^2\right). \tag{9}$$

We can define the input for the Fresnel integral as:

$$\alpha(\eta) \equiv M\sqrt{2\tau}, \tag{10}$$

where η is the threshold value (which we set to $1/\sqrt{2}$). We can now compute the number of terms needed to suppress all ghost factors past the value η, denoted M_0, by solving:

$$\frac{|F(\alpha(\eta))|}{\alpha(\eta)} = \eta, \tag{11}$$

Using $\eta = 1/\sqrt{2}$ yields:

$$\alpha(1/\sqrt{2}) \approx 1.318. \tag{12}$$

Solving Eq. (10) yields:

$$M_0 \approx \frac{1.318}{\sqrt{2\rho(N,l)}}.$$

This gives us the minimum number of M needed to suppress all ghost factors for a trial factor l. The maximum of M_0 occurs when ρ is minimized, which occurs when l is largest, i.e. $l = \sqrt{N}$. When $l = \sqrt{N}$, $\rho(N, \sqrt{N}) \approx 2/\sqrt{N}$, and then we have:

$$M_0 \approx 0.6590\sqrt[4]{N}. \tag{13}$$

In Ref. [4] it is proven that this scaling is both sufficient and necessary to eliminate all ghost factors in the TGS. The total computations needed is now:

$$T_{\text{TGS}}^{M_0} = M_0\sqrt{N} \approx 0.659\sqrt[4]{N}\sqrt{N} = 0.659N^{3/4}. \tag{14}$$

Thus we see that by using the TGS over the FGS, we save a bit in computations, but not that much. Also, since a high M value makes experiments difficult or impossible, requiring $M \sim \sqrt[4]{N}$ may be too restrictive.

4 New Approach: Multiple Experiments

Here we describe our method to eliminate the problem of ghost factors while using a lower value of M. The idea hinges upon the assumption that while there may be experimental error in the value of $|A_N^{(M)}(l)|$, there is none in l itself. I.e., we assume that one can distinguish between the values of the TGS for different ls. We then show that by running more then one experiment, one can identify the ghost factors and distinguish them from the true factors. Also, by using multiple experiments, one gets nearly-ghost-free factorization of nearby numbers automatically.

We first notice how $\rho(N, l)$ changes with changing N for a fixed l (we assume N is large enough so that k is equal for both values of ρ):

$$\rho(N+1, l) - \rho(N, l) = \frac{2(N+1)}{l} - 2k - \frac{2N}{l} - 2k = \frac{2}{l}. \tag{15}$$

As we saw in Fig. 2, one can transverse the central peak of $|s_M(\tau)|$ by moving the value of τ, which in the TGS is $\rho(N, l)$. Our method assumes that while it is difficult to know $|A_N^{(M)}(l)|$ exactly from the experiments, the **movement** of $|A_N^{(M)}(l)|$ for a trial factor is much easier to see. Since $s_M(\tau)$ is symmetric about 0, one should always see a rise and fall of the value of $|A_N^{(M)}(l)|$ as one changes N if l is a factor of N or of a nearby number. The maximum of this curve will be where l is a factor. An example of this is shown in Fig. 3.

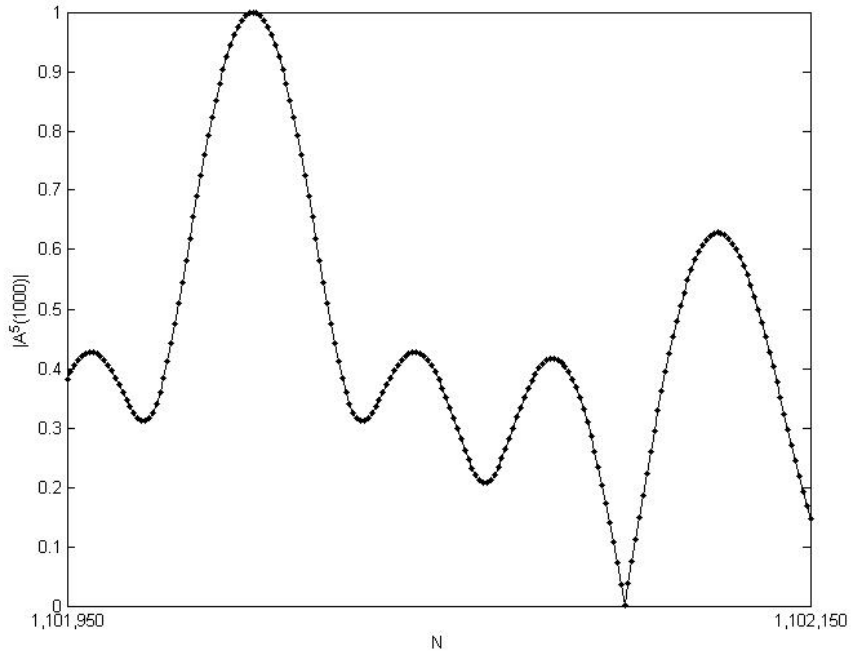

Figure 3: Movement of $|A_N^{(M)}(l)|$ for $N \in [1101950, 1102150]$, $M = 5$, and $l = 1000$. We see that there is a maximum at $N = 1101000$ where l is a factor.

We want to run numerous experiments with the same value of M with varying values of N and look at the $|A_N^{(M)}(l)|$ vs. N curves for each ghost factor l and determine where l is a factor by finding the maximum. From [4], we know that ghost factors are real factors of nearby N, in which case we should observe them reach a maximum either before or after the chosen N.

In order for this method to work, one needs to run enough experiments to be able to notice the maximum in the curve. For low values of l, one only needs to run a few experiments even for very low M, but for larger l one needs to run more. We can quantify the number of experiments needed using the previous continuous approximations of $s_M(\tau)$.

For each ghost factor we want to test $\lfloor K/2 \rfloor$ values to the right and left of N so that we guarantee that the number that l is a factor of is an observed maximum.

To do this, we need to find out how far in τ we need to transverse to cover the distance in the central peak of $|s_M(\tau)|$ from the symmetric intersection points of $|s_M(\tau)| = \eta$, where we will once again take $\eta = 1/\sqrt{2}$.

From Eq. (10) we can compute the width of the central peak of $|s_M(\tau)|$ between the intersections of τ and$|s_M(\tau)| = \eta$ as:

$$2\tau_0 = \frac{\alpha^2(\eta)}{M^2}. \tag{16}$$

Since we know from Eq. (15) that as one varies N, ρ changes by $2/l$, after K experiments we will have moved τ by $2K/l$. Therefore we can compute the required value of K for any ghost factor l as:

$$K = \frac{l\alpha^2(\eta)}{2M^2}. \tag{17}$$

The worst case scenario is when l is the largest possible value ($\sqrt{N}$), in which case we have (for the threshold

of $\eta = 1/\sqrt{2}$):

$$K_{\max} = 0.8686\frac{\sqrt{N}}{M^2} \approx \frac{\sqrt{N}}{M^2}. \tag{18}$$

In Fig. 4 we show this relationship for $N = 10^{13}$. What we see is that for a single experiment, we need

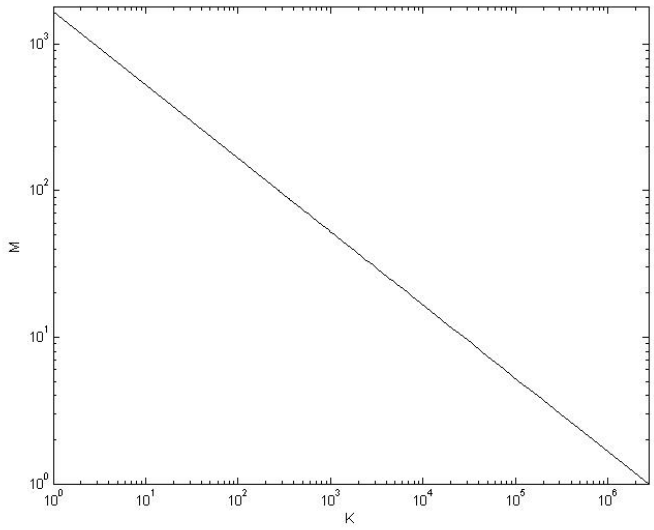

Figure 4: Relationship between number of terms in TGS (M) and number of experiments (K) needed to suppress and/or identify all ghost factors for $N = 10^{13}$.

$M \approx \sqrt[4]{N}$ which is the same scaling as in [4]. However, if we want to set $M = 1$ then we need to run $K \approx \sqrt{N}$ experiments! While this is untenable, the region between these extremes is interesting. For example, for a very large $N = 90101019010148987454$, $M_0 \approx 90000$. If we do 100 experiments this number drops to $M \approx 9000$. Therefore, with the relation in Eq. (18) we see that there is some leeway in the M value to identify or eliminate ghost factors by increasing the number of experiments.

An added bonus to this method is that for most values of l we do not need a full $K_{\max}$ to see the true factors of nearby N, and so we have a good chance of correctly factorizing all the nearby numbers within the K range around N automatically (assuming one tracks all l for the multiple experiments instead of just the ghost factors).

As we mentioned previously, the total number of computations needed for the TGS is $T = M\sqrt{N}$. For our method described here, this becomes:

$$T_K = KM\sqrt{N}. \tag{19}$$

We have seen that if we want $K = 1$, we need $M \sim \sqrt[4]{N}$, in which case $T_K \approx N^{3/4}$ as in Eq. (14). If we want to set $M = 1$, we end up needing $T \sim N$ computations, which is the same order as the full Gauss sum! Therefore we see that using our method with multiple experiments ($K > 1$), the total number of computations actually increases. However we need to be aware that while M is a limiting parameter in experiments, the sum computations are not since the physical system computes these. Therefore even though identifying ghost factors using a low M and high number of experiments can increase the total number of computed terms, in practical terms this may not be a problem. The relationship between K and M is not ideal, as for a low constant M, one needs many experiments. However, we feel that this method should be considered, as it may be very useful for expanding the range of numbers a particular M-constrained experiment can factorize.

5 Statistical Considerations

Here we explore the probabilities related to ghost factors, and thier relevance to our method.

We can define a ghost factor counting function as:

$$g(N,M) \equiv \#\left(l = 1, ..., \lfloor\sqrt{N}\rfloor \text{ s.t. } \eta < |A_N^{(M)}(l)| < 1\right) \tag{20}$$

What we would like to do is see what percentage of ghost factors occur for high values of l. Since the number of experiments needed is directly proportional to the l-value of the highest ghost factor, it is useful to see statistically if this value is typically near its maximum ($\sqrt{N}$) or not.

In [4], it was found that, generally, the number of ghost factors scales as:

$$g(N,M) \approx \frac{1}{2}\left(\frac{\alpha}{M}\right)^2 \sqrt{N}. \tag{21}$$

Therefore, the average number of ghost factors per trial factor can be written as:

$$d(M)_{\text{ave}} \approx \frac{1}{2}\left(\frac{\alpha}{M}\right)^2. \tag{22}$$

We show this relationship for 1000 random numbers $N \in [1, 10^8]$ for $M = 15$ in Fig. 5. We see that for

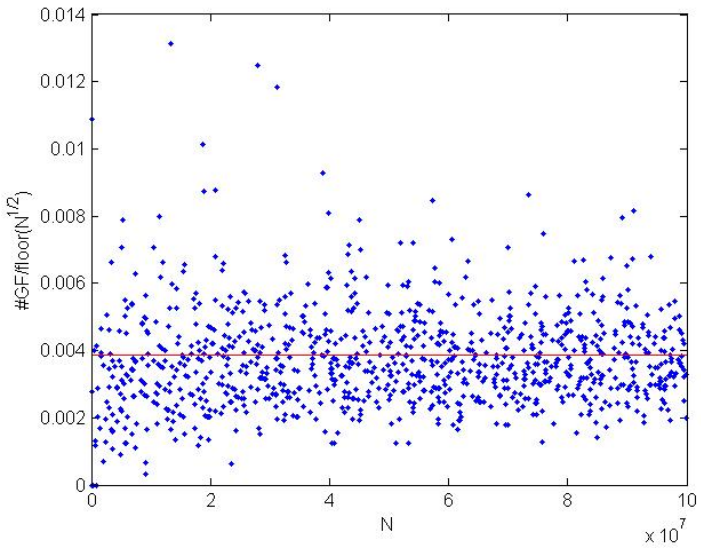

Figure 5: Number of ghost factors per trial factor for 1000 random numbers from $[1, 10^8]$ with $M = 15$. The red line is the prediction given by Eq. (22).

$M = 15$, the expected number of ghost factors is approximately $0.004\sqrt{N}$.

We can also see how the number of ghost factors are distributed across the trial factors for a specific M and N. We see that typically, the ghost factors are distributed uniformly across the trail factors as shown in the example of Fig. 6. Since the ghost factors are uniformly (on average) distributed across the trial factors, and we know typically how many ghost factors there are per trial factor, we can determine that the expected number of ghost factors for trial factors 1 to l is:

$$g_l(l,M) \approx \frac{1}{2}\left(\frac{\alpha}{M}\right)^2 l, \tag{23}$$

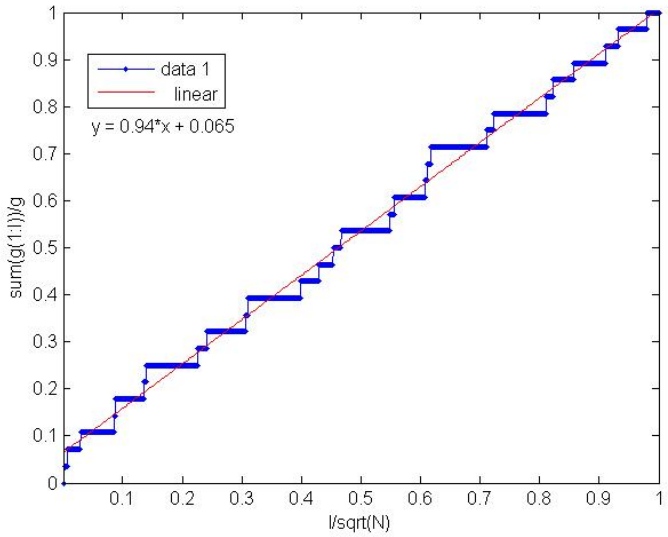

Figure 6: The number of ghost sums from the trial factors 1 to l as a percentage of $\sqrt{N}$ versus the trail factors l per L. Here, $M = 10$ and $N = 12512523$. We see that the distribution is nearly uniform. The red line is a linear fit.

which is simply Eq. (21) for only part of the TGS. Although this does not help our results from above, it does give a nice additional tool. If the number of ghost factors is low enough, it may be justifiable to check them manually with a computer. For experiments where N is too large, and M is too small, and it is infeasible to perform the necessary K experiments to observe the ghost factors, one could possibly do less experiments, (for low l trial factors), and then manually check the higher l values. Thus, for example, one could cut the number of experiments in half, if one can compute half the ghost factors manually.

6 Conclusion

For physical implementations of Gauss sum factorization, the limitation of M may make the elimination of ghost factors impossible for a single experiment. We have shown that if multiple experiments are performed, it is possible to identify the ghost factors, even with lower than optimal M. We also get the benefit of factorizing the nearby N values as well with a very high level of identification of ghost factors.

We also have shown that since the ghost factors are typically uniformly distributed across the trial factors, and the density of ghost factors for any N is constant (with constant M), that if the physical setup cannot perform the necessary K experiments, but can perform slightly less (within a constant factor), one can predict how many ghost factor terms would need to be manually checked to find all factors.

Although our additions do not drastically improve the situation, our hope is that for real world experimental setups, the ideas presented here may be of some use.

References

[1] W. Merkel, I. S. Averbukh, B. Girard, G. G. Paulus and W. P. Schleich. Factorization of numbers with physical systems. *Fortschritte der Physik*, **54** (2006) 856–865.

[2] M. Gilowski, T. Wendrich, T. Muller, Ch. Jentsch, W. Ertmer, E. M. Rasel and W. P. Schleich. Gauss sum factorization with cold atoms. *Physical Review Latters*, **100** (2008) 030201.

[3] T. S. Mahesh, N. Rajendran, X. Peng and D. Suter. Factorizing numbers with the Gauss sum technique: NMR implementations. *Physical Review A*, **75** (2007) 062303.

[4] M. Stefanak, W. Merkel, W. P. Schleich, D. Haase and H. Maier. Factorization with Gauss sums: scaling properties of ghost factors. *New Journal of Physics*, **9** (2007) 370.