The Number of Elements in a Subset: A Grover-Kronecker Quantum Algorithm

Shahar Dolev and Itamar Pitowsky

The Edelstein Center, Levi Building,

The Hebrerw University, Givat Ram, Jerusalem, Israel

Boaz Tamir

Department of Philosophy of Science,

Bar-Ilan University, Ramat-Gan, Israel.

Abstract

In a fundamental paper [*Phys. Rev. Lett.* *78*, 325 (1997)] Grover showed how a quantum computer can find a single marked object in a database of size N by using only $O(\sqrt{N})$ queries of the oracle that identifies the object. His result was generalized to the case of finding one object in a subset of marked elements. We consider the following computational problem: A subset of marked elements is given whose number of elements is either M or K, $M < K$, our task is to determine which is the case. We show how to solve this problem with a high probability of success using only iterations of Grover's basic step (and no other algorithm). Let m be the required number of iterations; we prove that under certain restrictions on the sizes of M and K the estimation $m \leq \frac{2\sqrt{N}}{\sqrt{K}-\sqrt{M}}$ obtains. This bound sharpens previous results and is known to be optimal up to a constant factor. Our method involves simultaneous Diophantine approximations, so that Grover's algorithm is conceptualized as an orbit of an ergodic automorphism of the torus. We comment on situations where the algorithm may be slow, and note the similarity between these cases and the problem of small divisors in classical mechanics.

PACS numbers: 03.67.L.x.

Keywords: quantum computation, Grover's algorithm, Diophantine approximation

Consider a quantum register of n qubits, which can have any of the $N = 2^n$ values $|a_j\rangle = |a_1^j\rangle \otimes ... \otimes |a_n^j\rangle$, $a_k^j \in \{0, 1\}$, or any superposition thereof. Our task is to search for one specific element, $|a_j\rangle$ out of these N. At our disposal is an oracle that if given the required value $|a_j\rangle$, will mark it by rotating its phase by π. Should the oracle receive a superposition of the basis elements, it will rotate only the branch of $|a_j\rangle$. Grover [1] demonstrated that by using $O(\sqrt{N})$ calls to the oracle one can find the marked element $|a_j\rangle$ with a very high probability. It was also shown [2] that if one is asked to find any one of K $(1 < K < N)$ marked elements (that is, the oracle will rotate all the K elements), it is possible to reach a high probability of success by calling the oracle $O(\sqrt{N/K})$ times.

In this paper we consider a variant of the algorithm which can solve fast the following problem: We know that there is a subset S of marked elements in the database, and we have an oracle to demarcate them. However, we do not know exactly how many elements there are in S, only that the number is either $|S| = M$ or $|S| = K$ for some $0 \leq M < K \leq N/2$. We shall show that under certain restrictions on the values of M and K and their relations to N we can solve the problem by calling the oracle m times, where $m < \frac{2\sqrt{N}}{\sqrt{K}-\sqrt{M}}$ (theorem 1).

Our result sharpens an earlier work of Nayak and Wu [3], who obtain a solution to the problem with a probability of success $\geq \frac{2}{3}$ after calling the oracle $m \leq O(\sqrt{\frac{N}{K-M}} + \frac{\sqrt{M(N-M)}}{K-M})$ times. The authors apply the counting algorithm of Brassard and his collaborators [4], which involves the elaborate discrete Fourier transform [5] on top of Grover's simpler procedure. By contrast, we simply iterate Grover's rotation, and apply simultaneous Diophantine approximations [6] to calculate the number of iterations that separate the two cases. Mathematically speaking, this means that we conceptualize Grover's algorithm as an orbit of a discrete dynamical process on the torus $\mathbb{T}^2$. Note also that all these upper bounds are optimal (up to a constant factor). This follows from the general lower bound on the complexity of quantum queries [7].

First we shall briefly repeat the algorithm [2] of finding an element of a set $S \subset \{1, 2, ..., N\}$, such that $|S| = K$. Let us denote

$$|\alpha\rangle_K \equiv \frac{1}{\sqrt{N-K}} \sum_{i \notin S} |a_i\rangle \qquad |\beta\rangle_K \equiv \frac{1}{\sqrt{K}} \sum_{i \in S} |a_i\rangle \tag{1}$$

Now, write the initial state of the register $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |a_i\rangle$ as a sum of the two vectors in Eq (1) $|\psi\rangle = \sqrt{\frac{N-K}{N}}\,|\alpha\rangle_K + \sqrt{\frac{K}{N}}\,|\beta\rangle_K$, or

$$|\psi\rangle = \cos\frac{\theta_K}{2}\,|\alpha\rangle_K + \sin\frac{\theta_K}{2}\,|\beta\rangle_K\,, \quad \frac{\theta_K}{2} = \sin^{-1}\sqrt{\frac{K}{N}} \tag{2}$$

Each step in Grover's algorithm transforms the present state of the register $|\psi'\rangle$ to a new state $G\,|\psi'\rangle$ by rotating $|\psi'\rangle$ in the plane spanned by $|\alpha\rangle_K$ and $|\beta\rangle_K$ by the angle θ_K. To do that the oracle is asked first to reflect $|\psi'\rangle$ around $|\alpha\rangle_K$ (by introducing a minus sign to the $|\beta\rangle_K$ component), subsequently we reflect the result about $|\psi\rangle$. Thus, after m iterations the state is

$$G^m\,|\psi\rangle = \cos(m\theta_K + \frac{\theta_K}{2})\,|\alpha\rangle_K + \sin(m\theta_K + \frac{\theta_K}{2})\,|\beta\rangle_K \tag{3}$$

All that is left to do is choose m that will bring $G^m\,|\psi\rangle$ as close as possible to $|\beta\rangle_K$, in other words, we look for an integer m which will satisfy $\sin(m + \frac{1}{2})\theta_K \approx 1$. In case $N \gg K$ it follows from the definition of θ_K that m is of the order of magnitude of $\sqrt{\frac{N}{K}}$.

In our problem we are given integers $M < K < N$, and we are told in advance that there is a subset $S \subset \{0, ..., N\}$ of marked elements that contains either M or K elements but we do not know which is the case. We wish to find out whether $|S| = M$ or $|S| = K$. Note that in the classical world the piece of information "there are either M or K marked elements in a database" does not reduce much the complexity of the search, and the expected number of calls of the oracle is $O(N)$. In the quantum world, on the other hand, this hint can allow us sometimes to harness Grover's algorithm and reduce the complexity.

We can always represent the initial state $|\psi\rangle$ as

$$|\psi\rangle = \cos\frac{\theta_M}{2}\,|\alpha\rangle_M + \sin\frac{\theta_M}{2}\,|\beta\rangle_M = \cos\frac{\theta_K}{2}\,|\alpha\rangle_K + \sin\frac{\theta_K}{2}\,|\beta\rangle_K \tag{4}$$

With $\sin\frac{\theta_M}{2} = \sqrt{\frac{M}{N}}$ and $\sin\frac{\theta_K}{2} = \sqrt{\frac{K}{N}}$. Our purpose is to compute the number of iterations m needed to bring M marked elements to their minimal possible magnitude, while at the same time to bring K marked elements to their maximal possible magnitude. That is, if $|S| = M$ the rotation G will operate in the plane spanned by $|\alpha\rangle_M$ and $|\beta\rangle_M$, and $G^m(|\psi\rangle)$ will approach $|\alpha\rangle_M$, the vector of $N - M$ *unmarked* elements. However, if $|S| = K$ the rotation G operates in the plane spanned by $|\alpha\rangle_K$ and $|\beta\rangle_K$ while $G^m(|\psi\rangle)$ will approach $|\beta\rangle_K$, the vector of K *marked* elements. We do not know in advance which is the case, but if such an integer m is found, and G has been iterated m times, all that is left for us to do is measure the quantum register. If the result is one of the elements of S (which we check by another query of the oracle) then it is clear with high probability that $|S| = K$, otherwise, $|S| = M$. As usual, the probability of success can be further increased by repeating the process.

The *existence* of such an integer m follows from the theorem of Kronecker on simultaneous Diophantine approximations [6] : *let* $\xi_1, \xi_2, ..., \xi_r$ *be irrational numbers which are linearly independent over the rationals, and let* $\eta_1, \eta_2, ..., \eta_r$ *be any real numbers, and* $\varepsilon > 0$ *real. Then there are integers* $p_1, p_2, ..., p_r$ *and an integer* l *such that*

$$|l\xi_j - \eta_j - p_j| < \varepsilon \quad j = 1, 2, ..., r \tag{5}$$

In our case $r = 2$, and we wish to find an *odd* integer $l = 2m + 1$ which approximates $\xi_1 = \frac{\theta_M}{4\pi}$ to $\eta_1 = 0$, and $\xi_2 = \frac{\theta_K}{4\pi}$ to $\eta_2 = \frac{1}{4}$ [8]. Only in rare cases such ξ_1 or ξ_2 are rationals, or dependent over the rationals [9]. The trouble is that it is very hard to obtain a universal bound on the minimal number l that satisfy Eq (5). In the general case of arbitrary ξ_j's and η_j's no such universal bound exists. In our more specific case, when we consider all M, K, and N, it is an open problem.

Luckily, there is an interesting range of values of M and K for which a small odd l does exist. Remember that the quantum algorithm gains advantage over the classical one only when the number of iterations $m = \frac{l-1}{2}$ is smaller than the average classical search of $O(N)$ steps. Denote $\gamma = \frac{\theta_K}{\theta_M} = \frac{\sin^{-1}(\sqrt{\frac{K}{N}})}{\sin^{-1}(\sqrt{\frac{M}{N}})}$. Our main result is

Theorem 1 ***a****. If* $M < K < \frac{N}{2}$ *satisfy* $\sqrt{K} < 16(\gamma-1)^2\sqrt{N}$ *then there are natural numbers* l *and* p*, such that* l *is odd, and* $l \leq \frac{4\sqrt{N}}{\sqrt{K}-\sqrt{M}}$*, and*

$$\left| l(\frac{\theta_K}{4\pi}) - p - \frac{1}{4} \right| < 2(\gamma - 1) \qquad \left| l(\frac{\theta_M}{4\pi}) - p \right| < (\gamma - 1) \tag{6}$$

b*. Let* $\varepsilon > 0$ *and consider the cases where* $K < (1+\frac{\varepsilon}{2\sqrt{2}})^2 M$*. Then the inequality* $(\gamma-1) < \frac{\varepsilon}{2}$ *is satisfied, so that* $\left|l(\frac{\theta_K}{4\pi}) - p - \frac{1}{4}\right| < \varepsilon$*, and also* $\left|l(\frac{\theta_M}{4\pi}) - p\right| < \varepsilon$*.*

The proof of the theorem is given towards the end of the paper. The theorem allows us to solve the problem even when the size of ε is not excessively small. Suppose that we have iterated the algorithm $m = \frac{l-1}{2}$ times, $m < \frac{2\sqrt{N}}{\sqrt{K}-\sqrt{M}}$, then ε determines the probability of getting the wrong result after measuring the quantum register. The probability of getting the wrong result in case there are K elements in S (that is, obtaining an unmarked element in the measurement) is the square of the coefficient of $|\alpha\rangle_K$ in $G^m(|\psi\rangle)$, that is, $\cos^2(m\theta_K + \frac{\theta_K}{2}) = \cos^2(\frac{l\theta_K}{2}) < \sin^2(2\pi\varepsilon)$. Similarly, the probability of getting a marked element in case $|S| = M$ is $\sin^2(m\theta_M + \frac{\theta_M}{2}) = \sin^2(\frac{l\theta_M}{2}) < \sin^2(2\pi\varepsilon)$. Even if we take $\sin^2(2\pi\varepsilon) = \frac{1}{4}$, that is $\varepsilon = \frac{1}{12}$, then a few repetitions of the algorithm will give the correct answer with overwhelming probability.

In light of the theorem one can see Grover's algorithm as a discrete dynamical process on the torus $\mathbb{T}^2$: Consider the subset of $\mathbb{T}^2$ given by $D = \{(l\frac{\theta_K}{4\pi} (\bmod 1), l\frac{\theta_M}{4\pi} (\bmod 1))\ ;\ l\ odd\ \}$. If $\frac{\theta_K}{4\pi}$ and $\frac{\theta_M}{4\pi}$ are independent over the rationals, then D is dense in $\mathbb{T}^2$; this is just Kronecker's theorem (with the slight variation that we consider only odd l's). If one thinks of $l = 1, 3, ..$ as a discrete time parameter, then D is a dense orbit of an ergodic dynamical system, and the question is how quickly it will enter a small prescribed neighborhood of $(\frac{1}{4}, 0)$. This question can be generalized to more extensive searches on $\mathbb{T}^r$, for $r \geq 3$ (more on this below); or to questions concerning approximations to other points on the torus, which may be related to the solutions of Diophantine equations; or finally, to questions regarding continuous rather than discrete processes, such as adiabatic computations. We shall come back to this point later.

Here are a few applications of the theorem:

Example 1 *For $K = M + 1$ we need $m = \frac{l-1}{2} < 4\sqrt{(M+1)N}$ iterations of Grover's algorithm to solve the problem up to a probability of error $\sin^2(2\pi\varepsilon)$. To estimate the range for which this is possible note that since $\frac{\sin^{-1}(x_1)}{\sin^{-1}(x_2)} \geq \frac{x_1}{x_2}$ for $0 < x_2 < x_1 < 1$, we have in this case $\gamma - 1 > \sqrt{1 + \frac{1}{M}} - 1 > \frac{1}{3M}$. Therefore, if we choose $\sqrt{\frac{M+1}{N}} < \left(\frac{4}{3M}\right)^2$ then the condition of the theorem: $\sqrt{K} < 16(\gamma - 1)^2\sqrt{N}$ is fulfilled. This means that the range of application of the algorithm for this case is at least $M \lessapprox \sqrt[5]{N}$, and the number of steps is $m \leq O(N^{\frac{3}{5}})$.*

Example 2 *For $K = 2M$ we can increase the database by adding rN artificial elements, out of which rM are marked, so they respond positively to the oracle. As a result we have to separate now between $M' = (r+1)M$ and $K' = (r+2)M$, while the total size of the database increases to $N' = (r+1)N$. We proceed as follows:*

***a**. The condition that $K' < (1 + \frac{\varepsilon}{2\sqrt{2}})^2 M'$ is satisfied if $r + 1 > \sqrt{2}\varepsilon^{-1}$. Let r be the minimal integer that satisfies this inequality.*

***b**. Consider the new angles: $\theta_{M'} = \sin^{-1}(\sqrt{\frac{(r+1)M}{(r+1)N}}) = \theta_M$, and $\theta_{K'} = \sin^{-1}(\sqrt{\frac{(r+2)M}{(r+1)N}})$.*

Therefore $\gamma' - 1 = \frac{\theta_{K'}}{\theta_{M'}} - 1 \geq \sqrt{\frac{(r+2)}{(r+1)}} - 1 > \frac{\varepsilon}{3\sqrt{2}}$. *(We are using once more the fact that* $\frac{\sin^{-1}(x_1)}{\sin^{-1}(x_2)} \geq \frac{x_1}{x_2}$ *for* $0 < x_2 < x_1 < 1$*, and the minimality of* r *from* ***a****).*

c*. Consequently, if we assume* $\sqrt{\frac{M}{N}} < (\frac{2\varepsilon}{3})^2$ *then the condition* $\sqrt{\frac{K'}{N'}} = \sqrt{\frac{(r+2)M}{(r+1)N}} < \frac{8}{9}\varepsilon^2 < 16(\gamma' - 1)^2$ *is fulfilled.*

d*. Now, apply the theorem to separate between* M *and* $2M$ *with an error* ε *in a number of steps* m *less than* $\frac{2\sqrt{N'}}{\sqrt{K'} - \sqrt{M'}} < 5(r+1)\sqrt{\frac{N}{M}} \approx 5\sqrt{2}\varepsilon^{-1}\sqrt{\frac{N}{M}}$. *Since* $\varepsilon > \frac{3}{2}\left(\frac{M}{N}\right)^{\frac{1}{4}}$ *we conclude that we need* $m \leq O\left[\left(\frac{N}{M}\right)^{\frac{3}{4}}\right]$ *steps for the separation between* M *and* $2M$*, provided* $\sqrt{M} < (\frac{2\varepsilon}{3})^2\sqrt{N}$*. The same technique will also work for the case* $K = aM$*, with some* $a > 1$*.*

Example 3 *Note that if the conditions of the theorem hold for the triple* M*,* K*,* N *they also hold for* nM*,* nK*,* nN *where* n *is any integer. Also, the angles* θ_M*, and* θ_K *remain the same, and therefore so does the number of iterations required to complete the job, despite the fact that the database has increased* n*-fold. This means that we should take care only of triples* M*,* K*,* N *that do not have a common divisor.*

Example 4 *Suppose that our information is that one of the following cases obtains:* $|S| = M_1$*, or* $|S| = M_2$*, or ...,*$|S| = M_r$*. We can inductively use multiple Diophantine approximations as in Eq (5): First find an odd integer* l *such that* $\sin(l\frac{\theta_{M_j}}{2}) \approx 1$ *for* $1 \leq j \leq [\frac{r}{2}]$*, while* $\sin(l\frac{\theta_{M_j}}{2}) \approx 0$*, for* $[\frac{r}{2}] < j \leq 1$*. If a measurement discovers a marked element then with high probability* $|S| = M_j$ *for some* $1 \leq j \leq [\frac{r}{2}]$*, otherwise it is one of the other cases. Now, divide the resulting set of possibilities into two halves and continue the process. After* $\sim \log_2 r$ *successive Diophantine approximations we are guaranteed to find the answer. The trouble is that the larger* r *is the larger* l *is likely to be, and it is not clear when the process yields better than classical outcomes.*

Example 5 *If* $M = 0$ *and* $K > 0$*, then we are just back with Grover's type algorithm. If* $|S| = 0$ *nothing happens to* $|\psi\rangle$*, and if* $|S| = K$ *we get close to* $|\beta\rangle_K$*.*

Two remarks on the general problem should be made: Firstly, for arbitrary values of M and K the minimal size of the number of iterations m depends on our ability to obtain a *lower bound* on the uniform Diophantine approximation to the quotient $\gamma = \frac{\theta_K}{\theta_M}$. By this we mean finding natural numbers p and q such that $|p\gamma - q|$ is small, *but not too small.* The reason will become clear from the proof below. Intuitively, if $p\frac{\theta_K}{\theta_M}$ stays close to an integer for a long segment of values of p, then the two numbers $\frac{\theta_M}{4\pi}$ and $\frac{\theta_K}{4\pi}$ become hard to separate with a small l. This means that the general separation problem runs into a difficulty similar to the problem of small denominators (or divisors) in classical mechanics [10]. It is likely that a formulation of the algorithm in terms of a continuous adiabatic quantum computer will demonstrate more clearly the relation between our problem and the KAM-type of problems, in the sense that small divisors may show up in the spectral gap. Note also that some of these small divisor problems may be overcome by using the trick in **Example 2**, namely by adding artificial elements to the database and changing the values of θ_K and θ_M.

Secondly, a remark about the actual value of $l = l(M, K, N)$, the number of iterations needed to complete the task. The proof below is giving a pretty good estimation of l. However, note that this is essentially a different problem. Once a "table" of the values of l is generated for the appropriate M, K, N, it can serve all search problems, no matter what the nature of the objects in the database, and the character of the oracle. Such "table" may allow us to decide what is the best strategy to use. We shall just briefly indicate how to formulate this problem algebraically: Denote $T_l(x) = \cos[l \cos^{-1}(x)]$, then T_l is the l degree Chebyshev's polynomial (of the first kind) [11]. Using Eq (2) we see that $\cos(l\frac{\theta_M}{2}) = T_l(\sqrt{\frac{N-M}{N}})$ and similarly $\cos(l\frac{\theta_K}{2}) = T_l(\sqrt{\frac{N-K}{N}})$. To get rid of the square roots we can use the identity $2T_l^2(x) - 1 = T_{2l}(x) = T_l(2x^2 - 1)$; so that finally our task is to find the smallest odd l such that $T_l(\frac{N-2M}{N}) \approx +1$ while $T_l(\frac{N-2K}{N}) \approx -1$. This observation may also assist in generalizing our result to other values of M, K, and N.

Proof of Theorem 1: Denote $\gamma = \frac{\theta_K}{\theta_M} = \frac{\sin^{-1}(\sqrt{\frac{K}{N}})}{\sin^{-1}(\sqrt{\frac{M}{N}})}$, we take the following three steps

Step 1: If $M < K < \frac{N}{2}$ then

$$0 < \gamma - 1 < \sqrt{2}(\sqrt{K/M} - 1) \tag{7}$$

That $\gamma > 1$ is obvious since $M < K$ and $\sin^{-1}(x)$ is increasing. For the right hand estimation we use the mean value theorem. First note that if $0 < x_2 < x_1 < 1$ then

$$\frac{\sin^{-1}(x_1)}{\sin^{-1}(x_2)} = 1 + \frac{\sin^{-1}(x_1) - \sin^{-1}(x_2)}{\sin^{-1}(x_2) - \sin^{-1}(0)} = 1 + \frac{\sqrt{1 - x_3^2}}{\sqrt{1 - x_4^2}} \frac{x_1 - x_2}{x_2}$$

for some x_3 and x_4 such that $x_1 > x_4 > x_2 > x_3 > 0$. Now, substitute $x_1 = \sqrt{K/N}$ and $x_2 = \sqrt{M/N}$, and remember that $1 - x_3^2 < 1$, and $x_4^2 < \frac{K}{N}$, so that the condition $K < \frac{N}{2}$ entails $\gamma < 1 + \sqrt{2}(\sqrt{K/M} - 1)$.

Step 2: Choose p to be the nearest *odd* integer to $\frac{1}{4(\gamma-1)}$, then $\left|p - \frac{1}{4(\gamma-1)}\right| \le 1$, and also $p \le \frac{1}{2}(\gamma-1)^{-1}$ (assuming $\gamma - 1 \le \frac{1}{4}$). and altogether:

$$\left|p\gamma - p - \frac{1}{4}\right| \le (\gamma - 1) \qquad p \le \frac{1}{2(\gamma-1)} \qquad p\ odd \tag{8}$$

Now, add the condition $\sqrt{\frac{K}{N}} < 16(\gamma-1)^2$. Denote by s the nearest *odd* integer to $\frac{4\pi}{\theta_M}$, then $\left|s - \frac{4\pi}{\theta_M}\right| \le 1$, and put $l = ps$ therefore l is also odd. Then, since $\sin^{-1}(x) \le \frac{\pi}{2}x$ for $0 \le x \le 1$, we have from Eq (8)

$$\left|l\frac{\theta_K}{4\pi} - p - \frac{1}{4}\right| \le \left|p\frac{\theta_K}{\theta_M} - p - \frac{1}{4}\right| + \frac{\theta_K}{4\pi}p\left|s - \frac{4\pi}{\theta_M}\right| < 2(\gamma - 1) \tag{9}$$
$$\left|l\frac{\theta_M}{4\pi} - p\right| = p\frac{\theta_M}{4\pi}\left|s - \frac{4\pi}{\theta_M}\right| < (\gamma - 1)$$

Step 3: Let $\varepsilon > 0$. To complete the proof all we have to do is impose the condition $2(\gamma-1) \le \varepsilon$. But then by Eq (7) this will be satisfied if $\sqrt{K} \le (1 + \frac{\varepsilon}{2\sqrt{2}})\sqrt{M}$. To estimate l note that by our definition $p \approx \frac{1}{4(\gamma-1)}$ while $s \approx \frac{4\pi}{\theta_M}$ where $\approx$ indicates equality up to ± 1. Hence, $l = ps \approx \frac{\pi}{\theta_K - \theta_M}$. Using once more the mean value theorem for $\sin^{-1}(x)$ we get $l \le \frac{4\sqrt{N}}{\sqrt{K}-\sqrt{M}}$. ■

Returning to the issue of small denominators, consider how it is avoided in our proof: On the one hand $\gamma - 1$ is small, indeed $\gamma - 1 < \frac{\varepsilon}{2}$ is our basic constraint. On the other hand p is of the order of magnitude of $(\gamma-1)^{-1}$, and $l = ps > p$, so that $\gamma - 1$ cannot be too small. This is the balance that should be struck if we wish to generalize the result to other values of $\gamma = \frac{\theta_K}{\theta_M}$; we have to obtain a uniform Diophantine approximation $|p\gamma - q|$ which is small, but reasonably bounded from below. A further complication is that p has to be odd. General lower bounds of this kind exist for algebraic numbers, but γ is typically transcendental. However, we are dealing with a very special case for which a good lower bound may exist. Also, we can move from a bad case to a better one by adding artificial elements to the database, as in **Example 2**.

Conclusion 1 *Given an oracle that identifies the elements of a subset* $S \subset \{1, 2, ..., N\}$, *and knowledge that either* $|S| = M$ *or* $|S| = K$, *for* $M < K$, *we demonstrated how to decide which is the case by iterating Grover's rotation* $m \le \frac{2\sqrt{N}}{\sqrt{K}-\sqrt{M}}$ *times. The algorithm is working for a certain range of values* M, K, *and* N, *and employs simultaneous Diophantine approximations. This means that we conceive of Grover's algorithm as an orbit of an ergodic* *automorphism of the torus $\mathbb{T}^2$, and ask how quickly it enters a given open subset of $\mathbb{T}^2$. We showed how to apply this process in some special cases, and noted that in other cases the algorithm may be frustrated because of a 'small divisor' type of problem.*

Acknowledgement 1 *We thank Michael Ben-Or and Scott Aaronson for calling our attention to earlier work on the subject. One of us (IP) is grateful for the support of the Israel Science Foundation grant number 879/02.*

---

[1] Grover, L. *Phys. Rev. Lett. 78*, 325 (1997).

[2] Boyer, M. Brassard, G. Høyer, P. and Tapp, A. *Fortsch. Phys. 46*, 493 (1998).

[3] Nayak, A. and Wu, F. *Proc. of STOC'99*, 384 (1999). Also, *quant-ph/9804066.*

[4] Brassard, G. Høyer, P. and Tapp, A. *Proc. of ICALP'98*, 820 (1998). Also, *quant-ph/9805082.*

[5] Shor, P. W. *SIAM J. of Comp. 26*, 1484 (1997).

[6] Hardy, G. H. and Wright, E. M. *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford (1988).

[7] Ambainis, A. *J. of Comp. and System Sci. 64*, 750 (2002). Also, *quant-ph/0002066.*

[8] Kronecker's theorem remains valid when restricted to odd integers l. To see that apply Kronecker's theorem to find integers n and q_j such that $\left|n\xi_j - \frac{1}{2}(\eta_j - \xi_j) - q_j\right| < \frac{\varepsilon}{2}$, and then multiply the inequalities by 2.

[9] Niven, I. *Irrational Numbers*, John Wiley and Sons, New York (1956).

[10] Moser, J. *Stable and Random Motions in Dynamical Systems*, Princeton University Press, Princeton (1973).

[11] Davis, P. J. *Interpolation and Approximation*, Dover, New York (1963).