Quantum Information and Computation, Vol. 7, No. 5&6 (2007) 522–550

SHARP PROBABILITY ESTIMATES FOR SHOR'S ORDER-FINDING ALGORITHM

P. S. BOURDON
Mathematics Department, Washington and Lee University
Lexington, Virginia 24450, USA

H. T. WILLIAMS
Department of Physics and Engineering, Washington and Lee University
Lexington, Virginia 24450, USA

Received September 2, 2006
Revised December 30, 2006

Let N be a (large) positive integer, let b be an integer satisfying $1 < b < N$ that is relatively prime to N, and let r be the order of b modulo N. Finally, let QC be a quantum computer whose input register has the size specified in Shor's original description of his order-finding algorithm. In this paper, we analyze the probability that a single run of the quantum component of the algorithm yields useful information—a nontrivial divisor of the order sought. We prove that when Shor's algorithm is implemented on QC, then the probability P of obtaining a (nontrivial) divisor of r exceeds .7 whenever $N \geq 2^{11}$ and $r \geq 40$, and we establish that .7736 is an asymptotic lower bound for P. When N is not a power of an odd prime, Gerjuoy has shown that P exceeds 90 percent for N and r sufficiently large. We give easily checked conditions on N and r for this 90 percent threshold to hold, and we establish an asymptotic lower bound for P of $2\mathrm{Si}(4\pi)/\pi \approx .9499$ in this situation. More generally, for any nonnegative integer q, we show that when QC(q) is a quantum computer whose input register has q more qubits than does QC, and Shor's algorithm is run on QC(q), then an asymptotic lower bound on P is $2\mathrm{Si}(2^{q+2}\pi)/\pi$ (if N is not a power of an odd prime). Our arguments are elementary and our lower bounds on P are carefully justified.

Keywords:

Communicated by: R Jozsa & R Laflamme

1 Introduction

In this Introduction, we assume readers are familiar with Shor's algorithm for finding the order of an integer b relative to a larger integer N to which b is relatively prime. The algorithm is reviewed in the next section.

The goal of Shor's algorithm is to find the least positive integer r such that $b^r \equiv 1 \pmod N$; that is, to find the order of b modulo N. In [1, 2], Shor describes an efficient algorithm to accomplish this task that runs on a quantum computer whose input register has n qubits, where n is chosen to be the unique positive integer such that $N^2 \leq 2^n < 2N^2$. The final quantum-computational step in Shor's algorithm is measurement of the input register in the computational basis. One obtains an n-bit integer y, and the key calculation at this point is the probability that y satisfies

$$\left|y - \frac{s2^n}{r}\right| \leq \frac{1}{2} \text{ for some } s \in \{1, 2, \ldots r-1\}. \tag{1}$$

Lower bounds for this probability, for sufficiently large N and r, are typically given at around 40 percent along with $4/\pi^2$ as an asymptotic lower bound (see, e.g., [2, p. 1500], [3], [4, p. 58], [5, Chapter 3]). We find a precise formula for the probability P that y belongs to

$$S := \left\{\text{nint}\left(\frac{s2^n}{r}\right) : s = 1, 2, 3, \ldots, r-1\right\},$$

and thereby satisfies (1). Here, *nint* is the nearest-integer function. We use our probability formula to show that the integer y obtained by Shor's quantum computation will belong to S with probability exceeding 70%, as long as $N \geq 2^{11}$ and $r \geq 40$. Moreover, we show that

$$\frac{2}{\pi^2}(-2 + \pi\text{Si}(\pi)) \approx 0.7737$$

provides an asymptotic lower bound for P. Here Si is the sine-integral function $\text{Si}(x) = \int_0^x \frac{\sin t}{t}\, dt$. Note that we may assume both r and N are large; otherwise, there is no reason to resort to quantum computation to find r.

Efficient order-finding leads to efficient methods for factoring composite integers (see, e.g., [6, §5.3.2]). Interest in the factoring problem is especially great for composite integers of the form pq, where p and q large distinct primes—the ability to factor such integers would allow one to read information encoded via the RSA cryptography system (see, e.g, [7]). In fact, order-finding itself permits decryption of RSA encoded messages (see, e.g., [8, Appendix A]).

When N is not a power of a prime, Gerjuoy ([7]) shows that Shor's algorithm (input register having n qubits where $N^2 \leq 2^n < 2N^2$) succeeds in finding a divisor of r with probability exceeding 90%, given N and r are sufficiently large. (Here and in the sequel, by "divisor of r" we mean a divisor exceeding 1.) The key lemma for Gerjuoy's work is that $r < N/2$ whenever N is not a power of a prime. (See [7, Appendix B] for an elementary proof of this fact in case $N = pq$, where p and q are distinct odd primes; we provide a general proof in Section 5 below.) This lemma allows Gerjuoy to establish that Shor's algorithm finds a divisor of r whenever the integer y observed at the conclusion of quantum computation belongs to

$$\tilde{S} := \left\{y : \left|y - \frac{s2^n}{r}\right| \leq 2 \text{ for some } s \in \{1, 2, \ldots, r-1\}\right\}.$$

In Section 5 of this paper, we apply our methods to find a precise formula for the probability $\tilde{P}$ that y belongs to $\tilde{S}$. We then use the formula to describe conditions on r and N that will ensure $\tilde{P}$ exceeds 90% and we show that

$$\frac{2\text{Si}(4\pi)}{\pi} \approx 0.9499$$

is an asymptotic lower bound for $\tilde{P}$.

In the final section of this paper, we extend our results to the case where the quantum computer "QC(q)" implementing Shor's algorithm has $n+q$ qubits in its input register, where

q is a nonnegative integer and where, just as before, $N^2 \leq 2^n < 2N^2$. Again assuming that N is not a power of a prime (so that Gerjuoy's lemma applies), we establish that when Shor's algorithm is run on QC(q), an asymptotic lower bound on the probability of finding a divisor of r is

$$\frac{2\text{Si}(2^{2+q}\pi)}{\pi},$$

a quantity which we show exceeds $1 - \frac{1}{\pi^2 2^{q+1}}$. When $q = 3$, our asymptotic bound is greater than 0.993. Also, when $q = 3$, we give easily checked conditions on r and N that will ensure the probability of success exceeds 99 percent.

We remark that phase-estimation analysis as it is described in [8], which served as the basis for its treatment in [6, Chapter 5] (see in particular the paragraph containing (5.44) on page 227), assures that the 99 percent threshold is reached when $q = 5$ (N not a power of a prime), or when $q = 7$ (N arbitrary).

2 Preliminaries

Our probability analysis depends on some elementary number theory; specifically, the following two lemmas. In these lemmas, r is a positive integer exceeding 1.

Lemma 1 *Suppose that t is a positive integer less than r which is relatively prime to r and that k is a nonnegative integer; then* $\{(kr+s)t \pmod r : s = 1, 2, \ldots r-1\} = \{1, 2, \ldots, r-1\}$.

Proof: Define $f : \{1, 2, \ldots, r-1\} \to \{1, 2, \ldots, r-1\}$ by

$$f(s) = (kr + s)t \ (\text{mod } r) = st \ (\text{mod } r).$$

To prove the lemma, it suffices to show f is one-to-one. Suppose $f(s_1) = f(s_2)$, then

$$(s_1 - s_2)t \equiv 0 \ (\text{mod } r).$$

Since t is relatively prime to r, the preceding equation shows that r must divide $s_1 - s_2$, but since $|s_1 - s_2| < r$, we must have $s_1 - s_2 = 0$. Hence f is one-to-one, as desired. □

Lemma 2 *Suppose that 2^n exceeds r and $r = 2^{\tilde{k}} r'$, where $\tilde{k}$ is a nonnegative integer and r' is a positive odd integer exceeding* 1*. Then there exists an integer q and a positive integer t less than r', relatively prime to r', such that*

$$\frac{2^n}{r} = q + \frac{t}{r'}.$$

Proof: Note $2^n/r = 2^{n-\tilde{k}}/r'$. Let q be the integer quotient that results when $2^{n-\tilde{k}}$ is divided by r' and let t be the remainder:

$$\frac{2^{n-\tilde{k}}}{r'} = q + t/r'.$$

It follows that $2^{n-\tilde{k}} = qr' + t$, and this equation shows that if t and r' had a common divisor exceeding 1 (necessarily odd since r' is odd), then that common divisor would be a odd number greater than 1 dividing $2^{n-\tilde{k}}$, which is absurd. The lemma follows. □

Let $\mathbf{Z}^+$ denote the set of positive integers. For the remainder of this paper, b and N denote elements of $\mathbf{Z}^+$ such that $1 < b < N$ and b is relatively prime to N. Let r be the *order* of b modulo N: $b^r \equiv 1 \pmod N$ and r is the least positive integer for which this equation holds. It is easy to show such an r exists and that $r < N$.[a] Also, since $1 < b < N$, r must be greater than 1. We now describe Shor's quantum algorithm, which is designed to compute the order r of b.

We focus on the transformations and measurements of the input and output registers of the machine implementing the algorithm, ignoring any work-register activity. The machine has input register having n qubits, where n is the least positive integer such that $N^2 \leq 2^n$. Its output register will have n_0 qubits, where n_0 is the least positive integer for which $N \leq 2^{n_0}$. (It's easy to check that either $n = 2n_0$ or $n = 2n_0 - 1$.) Note that the size of the output register allows it to hold any of the r integers in the set $\{b^x \pmod N) : x = 0, 1, 2, \ldots, r-1\}$.

The machine begins in state $|0\rangle_n |0\rangle_{n_0}$. Hadamard gates are applied to each of the n qubits in the input register to put the machine in state

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |0\rangle_{n_0}.$$

Then a unitary transformation that takes

$$|x\rangle_n |0\rangle_{n_0} \quad \text{to} \quad |x\rangle_n |b^x (\text{mod } N)\rangle_{n_0}, x \in \{0, 1, 2, \ldots, 2^n - 1\},$$

is applied, yielding the machine state

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |b^x (\text{mod } N)\rangle_{n_0}. \tag{2}$$

The next step in the algorithm, as described by Shor [2], is the application of the quantum Fourier-transform to the input register. However, to limit the number of summations that appear in our work, we will, at this stage, follow David Mermin [5, Chapter 3] and measure the output register. When this measurement is made on the machine in state (2), we obtain an n_0-bit integer J. Observe that there must be exactly one integer x_0 in $\{0, 1, 2, \ldots, r-1\}$ such that $b^{x_0} \equiv J \pmod N$ and that every $x \in \{0, 1, \ldots, 2^n - 1\}$ such that $b^x \equiv J \pmod N$ has the form $x_0 + kr$ for some integer k in $\{0, 1, 2, \ldots, m-1\}$, where

$$m = \left\lceil \frac{2^n}{r} - \frac{x_0}{r} \right\rceil. \tag{3}$$

(Here, $\lceil w \rceil$ represents the least integer greater than or equal to the real number w; later we use $\lfloor w \rfloor$ to represent that greatest integer less than or equal to w.) For future reference, observe

$$\frac{2^n}{r} - 1 < m < \frac{2^n}{r} + 1. \tag{4}$$

Thus, after measuring J in the output register, the machine's input register is in state

$$\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |kr + x_0\rangle_n. \tag{5}$$

[a] In fact, r must divide $\phi(N)$, where $\phi(N)$ denotes the number of positive integers less than N that are relatively prime to N.

We can think of the input register's state as $1/\sqrt{m}$ times a vector of 0's and 1's, which has 1's in positions $kr + x_0$ for $k \in \{0, 1, 2, \ldots, m-1\}$ and zeros elsewhere. Thus the input register contains values of a periodic $\{0, 1/\sqrt{m}\}$-valued function, having period r. By taking the quantum Fourier-transform of the input register, we (hope to) obtain information about the fundamental frequency $1/r$ and its overtones s/r, $s = 2, 3, \ldots, r-1$. After applying the quantum Fourier-transform, the input register is in state

$$\frac{1}{\sqrt{2^n m}} \sum_{y=0}^{2^n-1} e^{2\pi i x_0 y/2^n} \sum_{k=0}^{m-1} e^{2\pi i k r y/2^n} |y\rangle. \tag{6}$$

Here we are following Mermin [5, Chapter 3], even notationally.

The final step in the quantum-computational part of Shor's algorithm is measurement of the input register, which yields and n-bit integer y. As we discuss in the next section, if the integer $y \in \{0, 1, 2, \ldots, 2^n - 1\}$ measured belongs to

$$S = \left\{ \text{nint}\left(\frac{s2^n}{r}\right) : s = 1, 2, 3, \ldots, r-1 \right\}, \tag{7}$$

then one can use y to find a nontrivial divisor of the order r. Our goal is to find an exact expression for the probability that y belongs to S.

3 An Exact Probability Calculation

For each $s \in \{1, 2, \ldots, r-1\}$, let

$$y_s = \text{nint}\left(\frac{s2^n}{r}\right).$$

We seek to compute

> $P :=$ *the probability that the n-bit integer y observed via measurement of the quantum system in state (6) belongs to* $S = \{y_s : s = 1, 2, \ldots, r-1\}$.

If y does belong to S, then Shor [1, 2] explains how to use that information to find a divisor of r (in an efficient way). He depends on a classical result in number theory that states that if y is an integer such that

$$\left| \frac{y}{2^n} - \frac{s}{r} \right| \le \frac{1}{2r^2} \quad \text{for some } s \in \{1, 2, \ldots, r-1\}, \tag{8}$$

then one can obtain, via the continued-fraction expansion of $y/2^n$, a rational number $\frac{\tilde{s}}{\tilde{r}}$, in lowest terms, such that $\frac{\tilde{s}}{\tilde{r}} = \frac{s}{r}$; hence, $r = \frac{s}{\tilde{s}}\tilde{r}$ and $\tilde{r}$ is a divisor of r. If s happens to be relatively prime to r, then the order r is determined. Note that if $y = y_s$ is an element of S, then

$$\left| y - \frac{s2^n}{r} \right| \le \frac{1}{2},$$

so that $|y/2^n - s/r| \le \frac{1}{2\ 2^n} \le \frac{1}{2N^2} < \frac{1}{2r^2}$. Thus observing an integer from S at the conclusion of quantum computation will yield a divisor of r. The probability of finding r itself, as the least common-multiple of divisors found, rises quickly to 1 with the number of different divisors known.

It follows from (6) that the probability $p(y_s)$ that y_s will be observed is

$$p(y_s) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} e^{2\pi ikry_s/2^n}\right|^2, s \in \{1, 2, \ldots, r-1\},$$

which may be rewritten,

$$p(y_s) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} e^{\frac{2\pi ikr}{2^n}\left(y_s - \frac{s2^n}{r}\right)}\right|^2, s \in \{1, 2, \ldots, r-1\}, \tag{9}$$

because $e^{\frac{2\pi ikr}{2^n}\left(y_s - \frac{s2^n}{r}\right)} = e^{2\pi ikry_s/2^n} e^{-2\pi iks} = e^{2\pi ikry_s/2^n}$ for each s. Let

$$\delta_s = y_s - \frac{s2^n}{r}, \tag{10}$$

which allows us to re-express (9) as

$$p(y_s) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} e^{\frac{2\pi ikr\delta_s}{2^n}}\right|^2, s \in \{1, 2, \ldots, r-1\}. \tag{11}$$

Representation (11) of $p(y_s)$ can be simplified by using the formula for the partial sum of a geometric series: $\sum_{l=0}^{m-1} w^l = (1-w^m)/(1-w)$; one obtains that for every $s \in \{1, 2, \ldots, r-1\}$

$$p(y_s) = \frac{1}{2^n m}\frac{\left|1 - e^{\frac{2\pi imr\delta_s}{2^n}}\right|^2}{\left|1 - e^{\frac{2\pi ir\delta_s}{2^n}}\right|^2} = \frac{1}{2^n m}\frac{\sin^2\left(\frac{\pi mr\delta_s}{2^n}\right)}{\sin^2\left(\frac{\pi r\delta_s}{2^n}\right)}. \tag{12}$$

In our calculation of P, unless we indicate otherwise, we will assume only that the number n of qubits in the input register exceeds n_0, the number in the output register. Observe that this ensures that $2^n/r > 2^{n-n_0} \geq 2$. It follows that the set S of (7) consists of $r-1$ distinct elements, and thus

$$P = \sum_{s=1}^{r-1} p(y_s). \tag{13}$$

Also note that there is no ambiguity in the value of $\text{nint}\,(s2^n/r)$ for $s = 1, 2, \ldots, r-1$ because $s2^n/r$ can never be a half-integer.

We consider the simplest case first: $\frac{2^n}{r}$ is an integer. In this case, $y_s = \text{nint}\left(\frac{s2^n}{r}\right) = \frac{s2^n}{r}$ and therefore $\delta_s = 0$ for each s. It follows from (11) that $p(y_s) = \frac{m}{2^n}$ for every s and thus

$$P = (r-1)\frac{m}{2^n}. \tag{14}$$

Using the lower bound on m from (4), we have

$$P > 1 - \frac{1}{r} - \frac{r-1}{2^n}. \tag{15}$$

This exceeds .95 if, e.g., $r > 25$, $n > 15$, and $2^n \geq N^2 > r^2$.

We now address the more challenging, more interesting case: $\frac{2^n}{r}$ is not an integer. Note that in this case, there must be a nonnegative integer $\tilde{k}$ such that

$$r = 2^{\tilde{k}} r', \text{ where } r' \text{ is odd and exceeds 1.} \tag{16}$$

Suppose that $\tilde{k}$ is positive so that r is even. Then appearing in the sum over s in (13) are values of s that are multiples of r': $r', 2r', ..., (2^{\tilde{k}} - 1)r'$. For each of these values, $y_s = \text{nint}\left(\frac{s2^n}{r}\right) = \text{nint}\left(2^{n-\tilde{k}}\frac{s}{r'}\right) = 2^{n-\tilde{k}}\frac{s}{r'}$ and therefore $\delta_s = 0$ for each such s. Thus we have from (11)

Observation 1: The total contribution to P from multiples of r' is $(2^{\tilde{k}} - 1)\frac{m}{2^n}$.

The remaining s values, i.e. those that are not multiples of r', consist of $2^{\tilde{k}}$ sequences, each with $r' - 1$ terms:

$$(1, 2, ..., r'-1), (r'+1, r'+2, ..., 2r'-1), \ldots, \left((2^{\tilde{k}} - 1)r' + 1, (2^{\tilde{k}} - 1)r' + 2, ..., 2^{\tilde{k}}r' - 1\right). \tag{17}$$

We will show that the contribution to P from each sequence is the same.

Note that Observation 1 is valid even if $\tilde{k} = 0$ and that the assertion made in the preceding paragraph is trivially true since there is only one sequence in (17) in this case.

Apply Lemma 2 to represent $\frac{2^n}{r}$ as $q + t/r'$ where q is a positive integer and $t < r'$ is relatively prime to r'. Consider the collection

$$\begin{aligned} S' := \{y_s : s \in \{1, 2, \ldots, r' - 1\}\} &= \left\{\text{nint}\left(\frac{s2^n}{r}\right) : s \in \{1, 2, \ldots, r' - 1\}\right\} \\ &= \left\{\text{nint}\left(sq + \frac{st}{r'}\right) : s \in \{1, 2, \ldots, r' - 1\}\right\}. \end{aligned}$$

Apply Lemma 1 with $k = 0$ to see that $st \not\equiv 0 \pmod{r'}$ for each $s \in \{1, 2, \ldots, r' - 1\}$. Hence, for each such s, $st = q_s r' + j_s$ for some nonnegative integer q_s and some $j_s \in \{1, 2, \ldots, r' - 1\}$. Thus

$$S' = \left\{\text{nint}\left(sq + q_s + \frac{j_s}{r'}\right) : s \in \{1, 2, \ldots, r' - 1\}\right\}. \tag{18}$$

Let $s \in \{1, 2, \ldots, r' - 1\}$. Observe that if

$$j_s \leq \left\lfloor \frac{r'}{2} \right\rfloor, \text{then } y_s = sq + q_s \text{ and } y_s - \frac{s2^n}{r} = -j_s/r'. \tag{19}$$

If

$$j_s \geq \left\lceil \frac{r'}{2} \right\rceil, \text{ then } y_s = sq + q_s + 1 \text{ and } y_s - \frac{s2^n}{r} = \frac{r' - j_s}{r'}. \tag{20}$$

Lemma 1 tells us that as s varies from 1 to $r' - 1$, the integers j_s appearing in the representation $\frac{s2^n}{r} = sq + \frac{st}{r'} = sq + q_s + \frac{j_s}{r'}$ will also vary from 1 to $r' - 1$. Thus, in (18)

$$\left\{\frac{j_s}{r'} : s \in \{1, 2, \ldots, r' - 1\}\right\} = \left\{\frac{1}{r'}, \frac{2}{r'}, \ldots, \frac{r' - 1}{r'}\right\}.$$

Thus Lemma 1 (with $k=0$), combined with observations (19) and (20), yields

$$\left\{\left|y_s - \frac{s2^n}{r}\right| : s = 1, 2, \ldots, r'-1\right\} = \left\{\frac{1}{r'}, \frac{2}{r'}, \ldots, \frac{\lfloor r'/2\rfloor}{r'}\right\} \tag{21}$$

and that for a given $l \in \{1, 2, \ldots \left\lfloor \frac{r'}{2} \right\rfloor\}$, there are exactly two integers s_1 and s_2 in $\{1, 2, 3, \ldots, r'-1\}$ such that $|y_{s_1} - \frac{s_1 2^n}{r}| = l/r'$ and $|y_{s_2} - \frac{s_2 2^n}{r}| = l/r'$.

Now suppose that $r' < r$; in other words, the integer $\tilde{k}$ in (16) is positive. Let k be any integer satisfying $1 \le k \le 2^{\tilde{k}} - 1$. The analysis of the preceding two paragraphs, with Lemma 1 applied as stated, shows that

$$\left\{\left|y_s - \frac{s2^n}{r}\right| : s = kr'+1, kr'+2, \ldots, kr'+r'-1\right\} = \left\{\frac{1}{r'}, \frac{2}{r'}, \ldots, \frac{\lfloor r'/2\rfloor}{r'}\right\}, \tag{22}$$

with each element of the set on the right corresponding to $|y_s - \frac{s2^n}{r}|$ for exactly two values of s in the range $kr'+1$ to $kr'+r'-1$.

Using the definition of δ_s from (10) as well as (21) and (22), we see that for any k with $0 \le k \le 2^{\tilde{k}} - 1$,

$$\{|\delta_{kr'+q}| : q = 1, 2, \ldots, r'-1\} = \left\{\frac{j}{r'} : j = 1, 2, \ldots, \left\lfloor \frac{r'}{2} \right\rfloor\right\} \tag{23}$$

with each member of the set on the right corresponding to $|\delta_{kr'+q}|$ for exactly two values of $q \in \{1, 2, \ldots, r'-1\}$. Thus we have

Observation 2: the contribution to P from from any one of the sequences in (17), which would take the form $\sum_{q=1}^{r'-1} p(y_{kr'+q})$ for some $k \in \{0, 1, \ldots, 2^{\tilde{k}} - 1\}$, is given by

$$\frac{2}{2^n m} \sum_{j=1}^{\left\lfloor \frac{r'}{2} \right\rfloor} \frac{\sin^2\left(\frac{\pi m r(j/r')}{2^n}\right)}{\sin^2\left(\frac{\pi r(j/r')}{2^n}\right)} = \frac{2}{2^n m} \sum_{j=1}^{\left\lfloor \frac{r'}{2} \right\rfloor} \frac{\sin^2\left(\frac{\pi m j}{2^{n-\tilde{k}}}\right)}{\sin^2\left(\frac{\pi j}{2^{n-\tilde{k}}}\right)}, \tag{24}$$

where we have used (12).

Combining Observations 1 and 2 leads us to a final form for the exact probability:

$$P = 2^{\tilde{k}} \frac{2}{2^n m} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m j}{2^{n-\tilde{k}}}\right)}{\sin^2\left(\frac{\pi j}{2^{n-\tilde{k}}}\right)} + (2^{\tilde{k}} - 1)\frac{m}{2^n}. \tag{25}$$

Note that the preceding formula is valid even when $\frac{2^n}{r}$ is an integer, provided we take $r = 2^{\tilde{k}} r'$, where $r' = 1$, and we follow convention and interpret the sum from $j = 1$ to $j = [\frac{r'}{2}] = 0$ to be 0.

4 Lower Bounds on the Probability of Success

In this section, we discuss two different ways of obtaining lower bounds for

$$P = 2^{\tilde{k}} \frac{2}{2^n m} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m j}{2^{n-\tilde{k}}}\right)}{\sin^2\left(\frac{\pi j}{2^{n-\tilde{k}}}\right)} + (2^{\tilde{k}} - 1)\frac{m}{2^n},$$

where $r < N \leq 2^{n_0}$, $2^{\tilde{k}} r' = r$ with $r' \geq 3$ odd (and $\tilde{k} \geq 0$), and $\frac{2^n}{r} - 1 < m < \frac{2^n}{r} + 1$. Our first method of bounding P below uses elementary inequalities based on the Maclaurin series for the sine function and requires only that $n > n_0$. Our second method provides an integral-based underestimate and requires $N^2 \leq 2^n$ (Shor's condition). The lower bounds presented below are rigorously justified in Appendix B.

To derive a series-based lower bound for P, we use the following elementary inequalities:

$$\sin^2 x \leq x^2 \text{ for all } x, \quad \text{and} \quad \sin^2 x \geq \left(x - \frac{x^3}{6}\right)^2 \text{ for, say, } x \in \left[0, \frac{3\pi}{4}\right]. \tag{26}$$

We obtain (see Appendix B)

$$P > \left(1 - \frac{1}{2^{n-n_0}} - \frac{1}{r}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r+1}{r} + \frac{1}{2^{n-n_0-1}} + \frac{1}{2^{2(n-n_0)}}\right)\right) \quad \text{if } \tilde{k} = 0 \ (r, \text{odd}), \tag{27}$$

and

$$\begin{aligned} P \quad > \quad & \left(1 - \frac{1}{2^{n-n_0}} - \frac{1}{r'}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{1}{2^{n-n_0-2}} + \frac{1}{2^{2(n-n_0)-1}}\right)\right) \\ & + \frac{1}{r'} - \frac{1}{2^{\tilde{k}} r'} - \frac{1}{2^{n-n_0}} \quad \text{if } \tilde{k} > 0 \ (r, \text{even}). \end{aligned} \tag{28}$$

Assuming that $n - n_0 \geq 11$ and $r \geq 40$, one can show (Appendix B) that the right-hand side of either (27) or (28) exceeds 0.70. Thus if Shor's algorithm is carried out with an input register having the size described in Shor's original paper, then the probability of finding a divisor of the period sought exceeds 70% (as long as $r \geq 40$ and $N \geq 2^{11}$).

Note that as r and $n - n_0$ approach ∞ in our lower bound formula (27) for odd r, we get an asymptotic lower bound on P of $(1 - \pi^2/36) \approx 0.726$. A sharper asymptotic bound is provided by

$$P \geq \frac{1 - \frac{\pi^2}{4N^2}}{1 + \frac{1}{N}} \left(\frac{2}{\pi^2} \int_{1/r'}^{\frac{1}{2} + \frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\, dx\right) - \frac{3}{N} + \frac{1}{r'} - \frac{1}{2^{\tilde{k}} r'}, \tag{29}$$

an inequality proved to be valid in Appendix B (assuming $N^2 \leq 2^n$). By letting r' and N approach infinity, we obtain

$$\frac{2}{\pi^2} \int_0^{1/2} \frac{\sin^2(\pi x)}{x^2}\, dx = \frac{2}{\pi^2}(-2 + \pi Si(\pi)) \approx 0.7737$$

as an asymptotic lower bound for P.

Consider the function $F(N, \tilde{k}, r')$ defined by the right-hand side of (29). It is clear that if either of $\tilde{k}$ or N increases, so does F. Additionally, the partial derivative of F with respect to r' is positive (whenever N exceeds, say 9) and thus F increases in r' as well. F exceeds 0.75 when $N = 2^{11}, r' = 75$, and $\tilde{k} = 0$. Thus if one uses a classical computer to check that the order r of b modulo N doesn't have the form $2^{\tilde{k}} c$ where c is an odd number satisfying $1 \leq c \leq 73$, and $\tilde{k}$ is a nonnegative integer for which $2^{\tilde{k}} c < N$, then one can be over 75% certain of success. Note there are fewer than $37 \log_2(N)$ numbers to check so that the checking may easily be done on a classical computer. The 0.77 success-rate threshold is reached by, e.g. $N = 2^{15}$, $r' = 447$.

5 Order-finding when N is not a power of a prime

In this section, we assume that N is not a power of a prime, that b is an integer satisfying $1 < b < N$ which is relatively prime to N, and that r is the order of b modulo N. In this situation, Gerjuoy ([7]) has shown that Shor's algorithm succeeds in finding a divisor of r with probability on the order of 90% (given that N and r are sufficiently large). As we mentioned in the Introduction, the key to Gerjuoy's work is his use of the following lemma:

Lemma 3 (Gerjuoy) *If N is not a power of a prime and b is relatively prime to N, then the order r of b modulo N must satisfy*

$$r < \frac{N}{2}.$$

Gerjuoy [7, Appendix B] provides an elementary proof of the preceding lemma in case $N = pq$, where p and q are distinct odd primes. The general result may be established as follows. The collection of all integers less than N and relatively prime to N forms a group under multiplication modulo N. This group, denoted $(\mathbf{Z}/N\mathbf{Z})^\times$, contains $\phi(N)$ elements, where ϕ is the Euler ϕ function. A well-known number-theory result (see, e.g., [9, Proposition 4.1.3]) shows that $(\mathbf{Z}/N\mathbf{Z})^\times$ contains an element having order $\phi(N)$ modulo N if and only if N is 2 or 4 or has the form p^j or $2p^j$, where p is an odd prime and $j \in \mathbf{Z}^+$. Thus if N is a not a power of a prime, then either

(i) $(\mathbf{Z}/N\mathbf{Z})^\times$ contains no element of order $\phi(N)$, or

(ii) $N = 2p^j$ for some positive integer j and some odd prime p.

Suppose that (i) holds, that $b \in (\mathbf{Z}/N\mathbf{Z})^\times$, and that b has order r modulo N. Since the order r of b must divide the number of elements in $(\mathbf{Z}/N\mathbf{Z})^\times$ ([10, p. 43]) and since $r \neq \phi(N)$, we must have $\phi(N) = kr$ for some integer $k \geq 2$. Hence

$$r = \phi(N)/k \leq \phi(N)/2 < N/2,$$

as desired. Suppose that (*ii*) holds. Then $(\mathbf{Z}/N\mathbf{Z})^\times$ does contain elements of order $\phi(N)$; however, an easy calculation shows $\phi(2p^j) = p^j - p^{j-1}$, which is less than $N/2$. Thus in case (ii) holds, all elements of $(\mathbf{Z}/N\mathbf{Z})^\times$ have order less than $N/2$, which completes the proof of the lemma.

Gerjuoy [7] explains how Lemma 3 shows that a divisor of r may be extracted from the integer y observed at the conclusion of Shor's quantum computation *for a larger collection of y's than those contained in the set S of integers nearest $s2^n/r$,* $s = 1, 2, \ldots, r-1$. Specifically, he shows that if one observes an integer y satisfying

$$\left| y - \frac{s2^n}{r} \right| \leq 2 \ \text{ for some } s \in \{1, 2, \ldots r-1\}, \tag{30}$$

then one can obtain a divisor of r. To see why this is so, recall from (8) that the real goal of the computation is to find an integer y satisfying

$$\left| \frac{y}{2^n} - \frac{s}{r} \right| \leq \frac{1}{2r^2} \ \text{ for some } s \in \{1, 2, \ldots, r-1\}. \tag{31}$$

Note that if (30) holds and Lemma 3 applies (so that $2r < N$), then

$$\left|\frac{y}{2^n} - \frac{s}{r}\right| \leq \frac{2}{2^n} \leq \frac{2}{N^2} < \frac{2}{(2r)^2} = \frac{1}{2r^2},$$

so that knowledge of y means knowledge of a divisor of r.

Thus, given that N is not a prime power, Gerjuoy establishes that Shor's computation is successful provided the integer observed belongs to

$$\tilde{S} = \left\{ y : \left| y - \frac{s2^n}{r} \right| \leq 2 : s = 1, 2, \ldots, r-1 \right\}.$$

Observe that the gap between successive values of $s2^n/r$ exceeds $2^n/r \geq N^2/(N/2) = 2N$ so that the set of integers satisfying $\left|y - \frac{s2^n}{r}\right| \leq 2$ will be disjoint from those satisfying $\left|y - \frac{s'2^n}{r}\right| \leq 2$, given $s' \neq s$.

We now describe the elements of $\tilde{S}$ relative to the nearest integers y_s (introduced earlier) and calculate the exact probability that the integer y observed at the end of the Shor computation will belong to $\tilde{S}$.

Recall that for each $s \in \{1, 2, \ldots, r-1\}$, $y_s = \text{nint}\,(s2^n/r)$. Note that if $y_s < s2^n/r$, then $\tilde{S}$ will contain, in addition to y_s, the integers $y_s + 1$, $y_s + 2$, and $y_s - 1$. Similarly, if $y_s > s2^n/r$, then $\tilde{S}$ will contain $y_s, y_s + 1$, $y_s - 1$, and $y_s - 2$. Finally, if $s2^n/r$ is an integer (so that in the notation of Section 3, $s = kr'$ for some k satisfying $1 \leq k \leq 2^{\tilde{k}} - 1$), then $\tilde{S}$ will contain $y_s - 2, y_s - 1, y_s, y_s + 1, y_s + 2$. We have computed the probability P that the integer observed belongs to set $\{y_s : s = 1, 2, \ldots, r-1\}$, where $y_s = \text{nint}\,(s2^n/r)$. Similar methods will allow us to compute the probability that integers of the form $y_s + h$, $h \in \{-2, -1, 1, 2\}$ will be observed. In fact, we compute the probability that $y_s + h$ is observed for any integer h, but in this section will focus only the $|h| \leq 2$ case. Let $h \in \{-2, -1, 1, 2\}$ and $s \in \{1, 2, \ldots, r-1\}$ be arbitrary. Substituting $y_s + h$ for y_s in (9) and using the definition of δ_s in (10), we obtain the probability $p(y_s + h)$ that $y_s + h$ will be observed:

$$p(y_s + h) = \frac{1}{2^n m} \left| \sum_{k=0}^{m-1} e^{\frac{2\pi i k r (h+\delta_s)}{2^n}} \right|^2 = \frac{1}{2^n m} \frac{\sin^2\left(\frac{\pi m r (h+\delta_s)}{2^n}\right)}{\sin^2\left(\frac{\pi r (h+\delta_s)}{2^n}\right)}, s \in \{1, 2, \ldots, r-1\}, \tag{32}$$

which should be compared to (11) and (12).

Let $P_h = \sum_{s=1}^{r-1} p(y_s + h)$. We compute P_h just as we did P:

$$\begin{aligned} P_h &= \sum_{s=1}^{r-1} p(y_s + h) \\ &= \sum_{k=0}^{2^{\tilde{k}}-1} \left(\sum_{q=1}^{r'-1} p(y_{kr'+q} + h) \right) + \sum_{k=1}^{2^{\tilde{k}}-1} p(y_{kr'} + h) \\ &= \sum_{k=0}^{2^{\tilde{k}}-1} \left(\sum_{q=1}^{r'-1} \frac{1}{2^n m} \frac{\sin^2\left(\frac{\pi m r (h+\delta_{kr'+q})}{2^n}\right)}{\sin^2\left(\frac{\pi r (h+\delta_{kr'+q})}{2^n}\right)} \right) + \frac{2^{\tilde{k}} - 1}{2^n m} \frac{\sin^2\left(\frac{\pi m r h}{2^n}\right)}{\sin^2\left(\frac{\pi r h}{2^n}\right)}, \end{aligned}$$

where we have used (32) to obtain the final equality above. Recall from (19), (20), and (23) that $\{\delta_{kr'+q} : q = 1, 2, \ldots r'-1\} = \{j/r' : j = 1, 2, \ldots, \lfloor r'/2 \rfloor\} \cup \{-j/r' : j = 1, 2, \ldots, \lfloor r'/2 \rfloor\}$. Thus, we can say

$$P_h = \sum_{k=0}^{2^{\tilde{k}}-1} \frac{1}{2^n m} \left(\sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r(h+j/r')}{2^n}\right)}{\sin^2\left(\frac{\pi r(h+j/r')}{2^n}\right)} + \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r(h-j/r')}{2^n}\right)}{\sin^2\left(\frac{\pi r(h-j/r')}{2^n}\right)} \right) + \frac{2^{\tilde{k}}-1}{2^n m} \frac{\sin^2\left(\frac{\pi m r h}{2^n}\right)}{\sin^2\left(\frac{\pi r h}{2^n}\right)}$$

Observe that P_h is an even function of h, i.e., $P_h = P_{-h}$. Thus we can say that the probability of observing an integer in $\tilde{S}$ is

$$P + 2P_1 + Pt, \tag{33}$$

where Pt is the probability that the following integers are observed: (a) $y_s + 2$, given $s2^n/r > y_s$, or (b) $y_s - 2$, given $s2^n/r < y_s$, or (c) both $y_s + 2$ and $y_s - 2$, given $s2^n/r$ is an integer. We have

$$Pt = 2 \sum_{k=0}^{2^{\tilde{k}}-1} \frac{1}{2^n m} \left(\sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r(2-j/r')}{2^n}\right)}{\sin^2\left(\frac{\pi r(2-j/r')}{2^n}\right)} \right) + 2 \frac{2^{\tilde{k}}-1}{2^n m} \frac{\sin^2\left(\frac{\pi m r 2}{2^n}\right)}{\sin^2\left(\frac{\pi r 2}{2^n}\right)}.$$

Using our formulas for P, P_1, and Pt, and doing a bit of rearranging, we obtain the following as the probability that an element of $\tilde{S}$ will be observed:

$$\begin{aligned} \tilde{P} &= 2^{\tilde{k}} \frac{2}{2^n m} \sum_{h=-2}^{1} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r(j/r'+h)}{2^n}\right)}{\sin^2\left(\frac{\pi r(j/r'+h)}{2^n}\right)} + (2^{\tilde{k}}-1)\frac{m}{2^n} \\ &\quad + 2\frac{2^{\tilde{k}}-1}{2^n m} \frac{\sin^2\left(\frac{\pi m r 1}{2^n}\right)}{\sin^2\left(\frac{\pi r 1}{2^n}\right)} + 2\frac{2^{\tilde{k}}-1}{2^n m} \frac{\sin^2\left(\frac{\pi m r 2}{2^n}\right)}{\sin^2\left(\frac{\pi r 2}{2^n}\right)} \end{aligned} \tag{34}$$

In Appendix A, we present a numerical calculation illustrating the correctness of our formula for $\tilde{P}$. In Appendix B, we obtain the following lower bound for $\tilde{P}$:

$$\begin{aligned} \tilde{P} &\geq \frac{\left(1 - \frac{\pi^2}{N^2}\right)\left(1 - \frac{\pi^2}{16N^2}\right)}{1 + \frac{1}{2N}} \sum_{h=-2}^{1} \left(\frac{2}{\pi^2} \int_0^{\frac{1}{2} - \frac{1}{2r'}} \frac{\sin^2(\pi x)}{(x+h)^2}\, dx \right) - \frac{1}{r'} \\ &\quad - \frac{7}{2N} - \frac{16}{\pi N\left(1 - \frac{1}{2N}\right)} - \frac{1}{2^{\tilde{k}} r'}. \end{aligned} \tag{35}$$

As r' and N approach infinity, we obtain an asymptotic lower bound of

$$\sum_{h=-2}^{1} \left(\frac{2}{\pi^2} \int_0^{\frac{1}{2}} \frac{\sin^2(\pi x)}{(x+h)^2}\, dx \right) = \frac{2\mathrm{Si}(4\pi)}{\pi} \approx 0.9499. \tag{36}$$

Clearly, the quantity on the right-hand side of (35) increases as any one of r', N, or $\tilde{k}$ increases. This quantity exceeds 0.90 when $N = 2^{16}, r' = 59$, and $\tilde{k} = 0$. Thus if one uses a classical computer to check that the order r of b modulo N doesn't have the form $2^{\tilde{k}}c$ where c is an odd number satisfying $1 \leq c \leq 57$, and $\tilde{k}$ is a nonnegative integer for which $2^{\tilde{k}}c < N$, then one can be over 90% certain of success. Note there are fewer than $29\log_2(N)$ numbers to check so that the checking may easily be done on a classical computer. The 0.94 success-rate threshold is reached by, e.g. $N = 2^{16}$, $r' = 299$.

We remark that the trig identity $\sin^2(\pi x) = \sin^2(\pi(x+h))$ (for h, an integer) along with some elementary calculus shows that the sum of integrals on the left of (36) equals

$$\frac{2}{\pi^2}\int_0^2 \frac{\sin^2(\pi x)}{x^2}\,dx$$

which via appropriate trig identities and substitutions yields $\frac{2\mathrm{Si}(4\pi)}{\pi}$.

6 Probability Calculations for Larger Computers

Just as in the preceding section, we assume that N is a (large) positive integer that is not a power of a prime, that $b > 1$ is an integer less than N, relatively prime to N, whose order r (modulo N) we seek. Note that Gerjuoy's lemma remains in force: $r < N/2$. Just as before, let n be the positive integer satisfying $N^2 \le 2^n < 2N^2$ so that n is the number of qubits Shor originally specified for the input register of the quantum computer "QC" running his order-finding algorithm. For each nonnegative integer q, let QC(q) be a quantum computer having input register of size $n+q$ qubits. Let

$$\tilde{S}_q = \left\{ y : \left| y - \frac{s2^{n+q}}{r} \right| \le 2^{1+q} \text{ for some } s \in \{1,2,\ldots,r-1\} \right\}.$$

Observe that if $y \in \tilde{S}_q$ then for some $s \in \{1,2,\ldots,r-1\}$,

$$\left| \frac{y}{2^{n+q}} - \frac{s}{r} \right| \le \frac{2}{2^n} \le \frac{2}{N^2} < \frac{2}{(2r)^2} = \frac{1}{2r^2}$$

so that if the integer y, observed at the end of the Shor computation on QC(q), belongs to $\tilde{S}_q$, then the computation will be successful in the sense that a divisor of r (exceeding 1) will be found. Let $\tilde{P}_q$ be the probability that an integer y in $\tilde{S}_q$ is observed. (Note $\tilde{S}_0 = \tilde{S}$ and $\tilde{P}_0 = \tilde{P}$.) Generalizing the computations in the preceding section in the obvious way, we obtain the following analogue of (34):

$$\tilde{P}_q = 2^{\tilde{k}} \frac{2}{2^{n+q}m} \sum_{h=-2^{q+1}}^{2^{q+1}-1} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r'+h)}{2^{n+q}}\right)}{\sin^2\left(\frac{\pi r (j/r'+h)}{2^{n+q}}\right)} + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}} + 2\frac{2^{\tilde{k}}-1}{2^{n+q}m} \sum_{j=1}^{2^{q+1}} \frac{\sin^2\left(\frac{\pi m r j}{2^{n+q}}\right)}{\sin^2\left(\frac{\pi r j}{2^{n+q}}\right)}.$$

The preceding formula yields the following lower-bound for $\tilde{P}_q$ (see Appendix B), which is a generalization of our lower-bound formula (35) for $\tilde{P}$:

$$\tilde{P}_q \ge \frac{\left(1-\left(\frac{\pi}{N}\right)^2\right)\left(1-\left(\frac{\pi}{2^{q+2}N}\right)^2\right)}{1+\frac{1}{2^{q+1}N}} \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{2}{\pi^2} \int_0^{\frac{1}{2}-\frac{1}{2r'}} \frac{\sin^2(\pi x)}{(x+h)^2}\,dx \right) - \frac{1}{r'} - \frac{7}{N2^{q+1}} - \frac{16}{\pi N\left(1-\frac{1}{N2^{q+1}}\right)} - \frac{1}{2^{\tilde{k}}r'}. \quad (37)$$

Fixing q and letting N and r' approach infinity, we obtain

$$\sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{2}{\pi^2} \int_0^{\frac{1}{2}} \frac{\sin^2(\pi x)}{(x+h)^2}\, dx \right) = \frac{2\mathrm{Si}(2^{2+q}\pi)}{\pi}$$

as an asymptotic lower bound for $\tilde{P}_q$. When $q = 3$, we have $\frac{2\mathrm{Si}(32\pi)}{\pi} \approx 0.9937$.

Fix $q = 3$. Clearly, the quantity on the right-hand side of (37) increases as any one of r', N, and $\tilde{k}$ increases. Given $q = 3$, this quantity exceeds 0.99 when $N = 2^{20}, r' = 819$, and $\tilde{k} = 0$. Thus if one uses a classical computer to check that the order r of b modulo N doesn't have the form $2^{\tilde{k}}c$ where c is an odd number satisfying $1 \leq c \leq 817$, and $\tilde{k}$ is a nonnegative integer for which $2^{\tilde{k}}c < N$, then one can be over 99% certain of success in finding a divisor of r on QC(3). Note there are fewer than $409 \log_2(N)$ numbers to check so that the checking may easily be done on a classical computer.

Recall the well-known result $\mathrm{Si}(\infty) = \int_0^\infty \frac{\sin t}{t}\, dt = \frac{\pi}{2}$; thus, given Shor's algorithm runs on QC(q), our asymptotic lower bound $\frac{2\mathrm{Si}(2^{2+q}\pi)}{\pi}$ on the probability of success approaches 1 as $q \to \infty$, as expected. To get a sense of the rapidity of approach to 1, one may use the underestimate

$$\mathrm{Si}(n\pi) \geq \frac{\pi}{2} - \frac{1}{n\pi}, \tag{38}$$

which holds for any positive, even integer n by the following simple argument. For each $j \in \mathbf{Z}^+$, let $s_j = \int_{j\pi}^{(j+1)\pi} \frac{\sin t}{t^3}\, dt$. Note that the sequence (s_j) alternates in sign and $(|s_j|)$ is strictly decreasing. It follows that if n is even, then $\sum_{j=n}^\infty s_j$, which equals $\int_{n\pi}^\infty \sin(t)/t^3\, dt$, is positive. We have for any even integer n,

$$\mathrm{Si}(n\pi) = \frac{\pi}{2} - \int_{n\pi}^\infty \frac{\sin t}{t}\, dt = \frac{\pi}{2} - \frac{1}{n\pi} + 2\int_{n\pi}^\infty \frac{\sin t}{t^3}\, dt \geq \frac{\pi}{2} - \frac{1}{n\pi},$$

where we have obtained the second equality above by twice integrating by parts. Thus, by (38),

$$\frac{2\mathrm{Si}(2^{2+q}\pi)}{\pi} \geq 1 - \frac{1}{\pi^2 2^{1+q}}.$$

The preceding under-estimation is sharp, as the figure below illustrates.

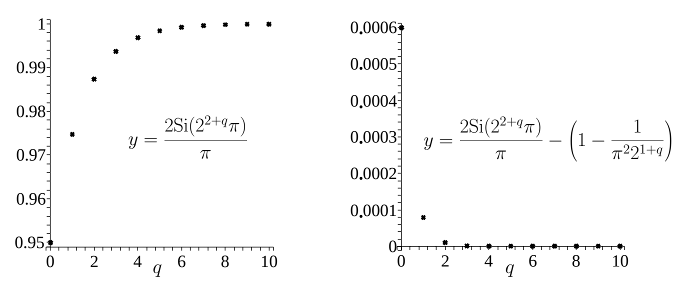

Fig. 1. Left: A plot of our asymptotic lower bounds on the probability of success. Right: $q \mapsto 1 - \frac{1}{\pi^2 2^{1+q}}$ provides a sharp under-estimate for these bounds even for small values of q. Here, q represents the number of qubits added to a "Shor-sized" register.

References

1. P. Shor (1994), *Algorithms for quantum computation: discrete logarithms and factoring*, Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press, pp. 124-134.
2. P. Shor (1997), *Polynomial time algorithms for Prime Factorization and discrete logarithms on a quantum computer*, SIAM J. Computing, 26, pp. 1484-1509.
3. A. Ekert and R. Josza (1996), *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys., 68, pp. 733–753.
4. M. Hirvensalo (2001), *Quantum computing*, Springer (New York).
5. D. Mermin (2006), *Lecture notes on quantum computation*, Cambridge University Press, to appear. (Draft available at http://people.ccmr.cornell.edu/ mermin/qcomp/CS483.html)
6. M. A. Nielsen and I. L. Chuang (2000), *Quantum computing and quantum information*, Cambridge University Press (Cambridge).
7. E. Gerjuoy (2005), *Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers*, Am. J. Phys., 73, pp. 521–540.
8. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca (1998), *Quantum algorithms revisited*, Proc. R. Soc. Lond. A, 454, pp. 339–354.
9. I. Ireland and M. Rosen (1990), *A classical introduction to modern number theory*, Springer-Verlag (New York).
10. I. N. Herstein (1975), *Topics in algebra*, Wiley (New York).

Appendix A: Some Numerical Calculations

To illustrate the correctness of our formula (34) for $\tilde{P}$, we complete a case study here involving small values of N and r: we take $N = 247$ and $b = 4$ so that $r = 18$, which means $\tilde{k} = 1$ and $r' = 9$. We use *Maple* to calculate $\tilde{P}$ two ways.

(1) We use the (inverse) discrete Fourier transform[b] to compute the coordinates, relative to the computational basis, of the state (6), which is the state that results from applying the quantum Fourier transform to the periodic vector (5). We plot the resulting probability amplitudes and sum those corresponding to basis states belonging to

$$\tilde{S} = \left\{ y : \left| y - \frac{s2^n}{r} \right| \leq 2 \text{ for some } s \in \{1, 2, \ldots, r-1\} \right\}.$$

(2) We use our formula (34).

The reader will see that the probabilities calculated by (1) and (2) agree to many decimal places.

Maple Probability Calculation Based on Fourier Coefficients

We suppose $N = 247$ and $b = 4$ so that $r = 18$. Here, the output register will have $n_0 = 8$ qubits and, following Shor, the input register will have $n = 16$ qubits. For simplicity we take $x_0 = 0$ in (5) and create a vector V corresponding to this state. Then we apply `InverseFourierTransform(V)`, plot the resulting probability amplitudes, and sum those

[b] As an operator, the inverse of the discrete Fourier transform is equivalent to what is called the quantum Fourier transform.

corresponding to the possible desired outcomes—those in the $\tilde{S}$. Here's the *Maple* code and output.

```
> Digits:=20:
> with(DiscreteTransforms):
> V:=Vector(2^(16)):  # V will store values of periodic function to which QFT
applied; entries initialized to 0
> m:=ceil(2^(16)/18);
```

$$m := 3641$$

```
> for k from 0 to m-1 do V[k*18+1]:=1/sqrt(m):  od:  #Every 18th value of V
set to 1/srqt(m)
> Z:=InverseFourierTransform(V):
> for k from 0 to 2^16-1 do NZ[k]:=Z[k+1] od:  # Re-index so that NZ[k] is
amplitude of |k> for k = 0..2^{16}-1
> with(plots):
> pointplot({seq([p/2^(16),abs(NZ[p])^2],p=0..2^16-1)});
```

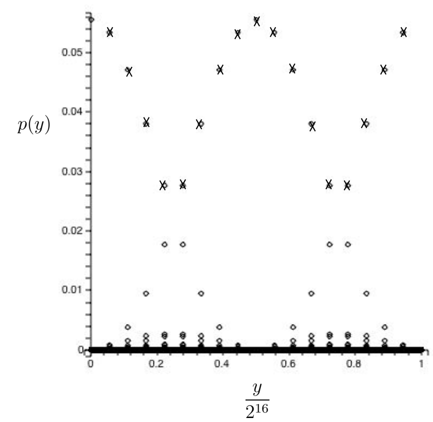

Fig. A.1. The probability that the integer y is observed peaks when $\frac{y}{2^{16}}$ is near an element of $\left\{\frac{s}{18} : s = 0, 1, \ldots, 17\right\}$. Data-points marked with x's have have coordinates $\left(\frac{y_s}{2^{16}}, p(y_s)\right)$, where y_s is the integer nearest $s2^{16}/18$, $s = 1, 2, \ldots, 17$.

```
> for s from 1 to 17 do y[s]:=round(s*2^(16)/18):  od:  #Compute the nearest
integers
> Prob:=0:  #After next loop Prob will be probability of observing an integer
in {y[s]:  s = 1..17}
> for k from 1 to 17 do   Prob:= Prob + abs(NZ[y[k]])^2:  od:
> Prob;
```

$$0.71982482558080545540$$

```
> Prob1:=0:#After next two loops Prob1 will be probability of observing an
integer in {y[s] + 1:  s = 1..17} or {y[s] - 1:  s = 1..17}
> for k from 1 to 17 do  Prob1:= Prob1 + abs(NZ[y[k]+1])^2:  od:
> for k from 1 to 17 do  Prob1:= Prob1 + abs(NZ[y[k]-1])^2:  od:
```

```
> Prob1;
```

0.15577667957639559817

```
> Prob2:=0: #After next loop Prob2 will be probability of observing an integer
y[s] + 2 or y[s] - 2, whichever is closer to s2^16/18, s=1..17
> for k from 1 to 17 do   if (round(k*2^(16)/18)< k*2^(16)/18) then Prob2:=Prob2
+abs(NZ[y[k]+2])^2  else Prob2:=Prob2 +abs(NZ[y[k]-2])^2 fi; od:
> Prob2;
```

0.018781342656774252754

```
> Prob + Prob1+Prob2+ abs(NZ[y[9]+2])^2; #Yields probability that observed
integer is in S-tilde; last term needed since both y[9]+2 and y[9]-2 belong
to S-tilde
```

0.89438284786571392115

Probability Calculation Using Formula (34) for $\tilde{P}$

```
> PP:= (k,n,m,rp)-> 2^k*2/(2^n*m)*sum(sum((sin(Pi*m*2^k*rp*(h+j/rp)/2^n)^2
/sin(Pi*2^k*rp*(h + j/rp)/2^n)^2),j=1..floor(rp/2)),h=-2..1) + (2^k - 1)*m/2^n
+ 2*(2^k-1)/(2^n*m)*sin(Pi*m*rp*2^k*1/2^n)^2/sin(Pi*rp*2^k*1/2^n)^2 + 2*(2^k-1)
/(2^n*m)*sin(Pi*m*rp*2^k*2/2^n)^2/sin(Pi*rp*2^k*2/2^n)^2:
> evalf(PP(1,16,3641,9));
```

0.89438284786571368089

Appendix B: Proofs of Lower Bounds for Probability of Success

Lower Bound on P Using Sine Series

Recall our formula (25) for P:

$$P = 2^{\tilde{k}} \frac{2}{2^n m} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m j}{2^{n-\tilde{k}}}\right)}{\sin^2\left(\frac{\pi j}{2^{n-\tilde{k}}}\right)} + (2^{\tilde{k}} - 1)\frac{m}{2^n},$$

where we assume $r < N \leq 2^{n_0}$, $2^{\tilde{k}} r' = r$ with $r' \geq 3$ odd (and $\tilde{k} \geq 0$), $\frac{2^n}{r} - 1 < m < \frac{2^n}{r} + 1$, and $n > n_0$. Recall that n_0 is chosen to be the least positive integer such that $2^{n_0} \geq N$. Observe that $m > 2^n/r - 1$ yields

$$(2^{\tilde{k}} - 1)\frac{m}{2^n} \geq \frac{1}{r'} - \frac{1}{r} - \frac{1}{2^{n-\tilde{k}}} + \frac{1}{2^n} > \frac{1}{r'} - \frac{1}{r} - \frac{1}{2^{n-\tilde{k}}}. \tag{B.1}$$

Also observe that if $j \in \left\{1, 2, \ldots, \left\lfloor \frac{r'}{2} \right\rfloor\right\}$, then our inequalites for m yield

$$0 \leq \frac{\pi m j}{2^{n-\tilde{k}}} = \pi \frac{m r}{2^n}\left(\frac{j}{r'}\right) < \pi\left(1 + \frac{r}{2^n}\right)\left(\frac{1}{2}\right) < \frac{\pi}{2}\left(1 + \frac{1}{2^{n-n_0}}\right) \leq \frac{3\pi}{4}. \tag{B.2}$$

Our goal is to establish the lower bounds (27) and (28). The work is tedious but straightforward.

Using the sine function inequalities (26), the second of which holds by (B.2), as well as

$$(a)\ \ (1-x)^2 \geq 1 - 2x \text{ for } x \in (-\infty, \infty) \ \text{ and } \ (b)\ \ \sum_{j=1}^{k} j^2 = \frac{k(k+1)(2k+1)}{6}, \tag{B.3}$$

we have

$$
\begin{aligned}
P &\geq 2^{\tilde{k}} \frac{2}{2^n m} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\left(\frac{\pi m j}{2^{n-\tilde{k}}} - \left(\frac{\pi m j}{2^{n-\tilde{k}}}\right)^3/6\right)^2}{(\frac{\pi j}{2^{n-\tilde{k}}})^2} + (2^{\tilde{k}}-1)\frac{m}{2^n} \quad \text{(by (26))} \\
&= 2^{\tilde{k}} \frac{2m}{2^n} \sum_{j=1}^{\lfloor r'/2 \rfloor} \left(1 - \left(\frac{\pi m j}{2^{n-\tilde{k}}}\right)^2/6\right)^2 + (2^{\tilde{k}}-1)\frac{m}{2^n} \\
&\geq 2^{\tilde{k}} \frac{2m}{2^n} \sum_{j=1}^{\lfloor r'/2 \rfloor} \left(1 - \left(\frac{\pi m j}{2^{n-\tilde{k}}}\right)^2/3\right) + (2^{\tilde{k}}-1)\frac{m}{2^n} \quad \text{(by } (B.3)(a)) \\
&= 2^{\tilde{k}} \frac{2m}{2^n} \left(\lfloor r'/2 \rfloor - \left(\frac{\pi m}{2^{n-\tilde{k}}}\right)^2 \frac{1}{3} \sum_{j=1}^{\lfloor r'/2 \rfloor} j^2\right) + (2^{\tilde{k}}-1)\frac{m}{2^n} \\
&= 2^{\tilde{k}} \frac{2m}{2^n} \lfloor r'/2 \rfloor \left(1 - \left(\frac{\pi m}{2^{n-\tilde{k}}}\right)^2 \frac{(\lfloor r'/2 \rfloor + 1)(2\lfloor r'/2 \rfloor + 1)}{18}\right) + (2^{\tilde{k}}-1)\frac{m}{2^n}, \quad \text{(B.4)}
\end{aligned}
$$

where we have used (B.3) (b) to obtain the final equality. We continue the calculation, using (B.1), $\frac{2^n}{r} + 1 > m > \frac{2^n}{r} - 1$, and $\lfloor r'/2 \rfloor = \frac{r'}{2} - \frac{1}{2}$, the latter fact holding because r' is odd. We obtain separate underestimates for the cases

(a) $\tilde{k} > 0$ (so that r, which equals $2^{\tilde{k}} r'$, is even), and

(b) $\tilde{k} = 0$ (so that r is odd and $r' = r$).

For $\tilde{k} > 0$, we have

$$
\begin{aligned}
P_{\text{even}} &> \left(\frac{2}{r'} - \frac{1}{2^{n-\tilde{k}-1}}\right)\left(\frac{r'}{2} - \frac{1}{2}\right)\left(1 - \pi^2\left(\frac{1}{r'} + \frac{1}{2^{n-\tilde{k}}}\right)^2 \frac{(r'+1)r'}{36}\right) + \frac{1}{r'} - \frac{1}{r} - \frac{1}{2^{n-\tilde{k}}} \\
&= \left(1 - \frac{r}{2^n} - \frac{1}{r'} + \frac{1}{2^{n-\tilde{k}}}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{r'+1}{2^{n-\tilde{k}-1}} + \frac{r'(r'+1)}{2^{2n-2\tilde{k}}}\right)\right) \\
&\qquad + \frac{1}{r'} - \frac{1}{r} - \frac{1}{2^{n-\tilde{k}}}. \quad \text{(B.5)}
\end{aligned}
$$

For case (b), note that when $\tilde{k} = 0$ the final summand in (B.4) disappears. Thus for $\tilde{k} = 0$, so that $r = r'$, we have

$$
\begin{aligned}
P_{\text{odd}} &> \left(1 - \frac{r}{2^n} - \frac{1}{r} + \frac{1}{2^n}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r+1}{r} + \frac{r+1}{2^{n-1}} + \frac{r(r+1)}{2^{2n}}\right)\right) \\
&> \left(1 - \frac{r}{2^n} - \frac{1}{r}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r+1}{r} + \frac{r+1}{2^{n-1}} + \frac{r(r+1)}{2^{2n}}\right)\right). \quad \text{(B.6)}
\end{aligned}
$$

We analyze P_{odd} first. Recall that $r < N \leq 2^{n_0}$, where r is the order of b modulo N. For now, we just assume $n > n_0$. Note that if 2^{n_0} (or $2^{n_0} - 1$) is substituted into the quantity of

(B.6) for any r appearing in the numerator of a fraction, the effect is to produce a smaller quantity; thus, we have arrived at the advertised lower bound (27) for P when r is odd:

$$P_{\text{odd}} > \left(1 - \frac{1}{2^{n-n_0}} - \frac{1}{r}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r+1}{r} + \frac{1}{2^{n-n_0-1}} + \frac{1}{2^{2(n-n_0)}}\right)\right).$$

We show that $P_{\text{odd}} > .70$ assuming only that the difference $n - n_0 \geq 11$ and $r \geq 41$. Thus if $N \geq 2^{11}$ and $r \geq 40$ is odd, then Shor's algorithm, as it was described in his papers [1, 2], finds a divisor of r with probability at least 70%. Assume $n - n_0 \geq 11$, then

$$P_{\text{odd}} > \left(1 - \frac{1}{2^{11}} - \frac{1}{r}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r+1}{r} + \frac{1}{2^{10}} + \frac{1}{2^{2(11)}}\right)\right).$$

Define $f : [41, \infty) \to \mathbf{R}$ by

$$f(r) = \left(1 - \frac{1}{2^{11}} - \frac{1}{r}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r+1}{r} + \frac{1}{2^{10}} + \frac{1}{2^{22}}\right)\right).$$

It is easy to show that f has positive derivative on $[41, \infty)$ and $f(41) > .70$, which verifies our claims concerning successfully finding a divisor of r in case r is odd.

Now we turn to the case $\tilde{k} > 0$ so that $r = 2^{\tilde{k}} r'$ is even. Using (B.5) along with $\tilde{k} \leq n_0$ and $r < 2^{n_0}$, we obtain the advertised lower bound (28) for P given r is even:

$$\begin{aligned} P_{\text{even}} > & \left(1 - \frac{1}{2^{n-n_0}} - \frac{1}{r'}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{1}{2^{n-n_0-2}} + \frac{1}{2^{2(n-n_0)-1}}\right)\right) \\ & + \frac{1}{r'} - \frac{1}{2^{\tilde{k}} r'} - \frac{1}{2^{n-n_0}}. \end{aligned}$$

We continue to assume that $r \geq 40$ and $n - n_0 \geq 11$. Because $2^{\tilde{k}} r' \geq 40$ we may work with the following four cases (1) $\tilde{k} \geq 4, r' \geq 3$, (2) $\tilde{k} = 3, r' \geq 5$, (3) $\tilde{k} = 2, r' \geq 11$, and (4) $\tilde{k} = 1, r' \geq 21$. We handle these cases separately. Case 1: if we assume that $\tilde{k} \geq 4$, we can say

$$P_{\text{even}} > \left(1 - \frac{1}{2^{11}} - \frac{1}{r'}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{1}{2^9} + \frac{1}{2^{21}}\right)\right) + \frac{1}{r'} - \frac{1}{16r'} - \frac{1}{2^{11}}.$$

Define $f : [3, \infty) \to \mathbf{R}$ by

$$f(r') = \left(1 - \frac{1}{2^{11}} - \frac{1}{r'}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{1}{2^9} + \frac{1}{2^{21}}\right)\right) + \frac{15}{16r'} - \frac{1}{2^{11}}.$$

It is easy to show that f has a global minimum on $[3, \infty)$ at $r_0 := \frac{4194304\pi^2}{9(524288-569\pi^2)} \approx 8.87$ and that $f(r_0) > .72$.

Case 2: For $\tilde{k} = 3$, $r' \geq 5$, we can say $P_{\text{even}} > f(r')$, where $f : [5, \infty) \to \mathbf{R}$ is given by

$$f(r') = \left(1 - \frac{1}{2^{11}} - \frac{1}{r'}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{1}{2^9} + \frac{1}{2^{21}}\right)\right) + \frac{7}{8r'} - \frac{1}{2^{11}}.$$

It is easy to show that f has positive derivative on $[5, \infty)$ and $f(5) > .71$.

Case 3: For $\tilde{k} = 2$, $r' \geq 11$, we can say $P_{\text{even}} > f(r')$, where $f : [11, \infty) \to \mathbf{R}$ is given by

$$f(r') = \left(1 - \frac{1}{2^{11}} - \frac{1}{r'}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{1}{2^9} + \frac{1}{2^{21}}\right)\right) + \frac{3}{4r'} - \frac{1}{2^{11}}.$$

It is easy to show that f has positive derivative on $[11, \infty)$ and $f(11) > .70$.

Case 4: For $\tilde{k} = 1$, $r' \geq 21$, we can say $P_{\text{even}} > f(r')$, where $f : [21, \infty) \to \mathbf{R}$ is given by

$$f(r') = \left(1 - \frac{1}{2^{11}} - \frac{1}{r'}\right)\left(1 - \frac{\pi^2}{36}\left(\frac{r'+1}{r'} + \frac{1}{2^9} + \frac{1}{2^{21}}\right)\right) + \frac{1}{2r'} - \frac{1}{2^{11}}.$$

It is easy to show that f has positive derivative on $[21, \infty)$ and $f(21) > .70$.

The preceding four cases justify our claims concerning the probability P of success when r is even, and thus, complete our proof that if Shor's algorithm is carried out with an input register having the size described in Shor's original paper, then the probability of finding a divisor of the period sought exceeds 70% (as long as $r \geq 40$ and $N \geq 2^{11}$).

Bounding P Below by an Integral

We provide a lower bound for P in terms of an integral. We start with a representation of P derived from our formula (25) and equation (24):

$$P = 2^{\tilde{k}} \frac{2}{2^n m} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r')}{2^n}\right)}{\sin^2\left(\frac{\pi r (j/r')}{2^n}\right)} + (2^{\tilde{k}} - 1)\frac{m}{2^n}, \tag{B.7}$$

where $r < N \leq 2^{n_0}$, $\frac{2^n}{r} - 1 < m < \frac{2^n}{r} + 1$, and $2^{\tilde{k}} r' = r$ with $\tilde{k}$ a nonnegative integer and $r' \geq 3$ odd. We assume that n satisfies $2^n \geq N^2$. Recall that since r' is odd, $\left\lfloor \frac{r'}{2} \right\rfloor = (r'-1)/2$.

Our approach to finding a integral-based lower bound for P is not the simplest possible one. We use methods here that will be required in our work to underestimate $\tilde{P}_q$ in the final subsection of this appendix.

Lemma B.1 *For* $j \in \{1, 2, \ldots, \left\lfloor \frac{r'}{2} \right\rfloor\}$,

$$\sin^2\left(\frac{\pi m r (j/r')}{2^n}\right) \geq \sin^2\left(\frac{\pi j}{r'} - \frac{\pi j}{2^{n-\tilde{k}}}\right).$$

Proof: Using $2^n/r + 1 \geq m \geq 2^n/r - 1$, we see that the argument of the sine function on the left in the lemma statement satisfies

$$\pi\left(\frac{j}{r'} + \frac{j}{2^{n-\tilde{k}}}\right) \geq \frac{\pi m r (j/r')}{2^n} \geq \pi\left(\frac{j}{r'} - \frac{j}{2^{n-\tilde{k}}}\right). \tag{B.8}$$

Note that the rightmost expression in (B.8) is positive: $\pi j \left(\frac{1}{r'} - \frac{2^{\tilde{k}}}{2^n}\right) = \pi j \left(\frac{2^n - r}{2^n r'}\right) > 0$. The following simple computation shows that leftmost quantity in (B.8) is less than $\pi/2$ for all j between 1 and $\lfloor r'/2 \rfloor = (r'-1)/2$:

Assuming $j \leq \frac{r'-1}{2}$, we have

$$\begin{aligned}
\pi\left(\frac{j}{r'} + \frac{j}{2^{n-\tilde{k}}}\right) &\leq \pi\left(\frac{1}{2} - \frac{1}{2r'} + \frac{r'-1}{2 \cdot 2^{n-\tilde{k}}}\right) \\
&= \frac{\pi}{2} - \frac{\pi}{2}\left(\frac{1}{r'} - \frac{2^{\tilde{k}}(r'-1)}{2^n}\right) \\
&= \frac{\pi}{2} - \frac{\pi}{2}\left(\frac{2^n - r(r'-1)}{2^n r'}\right) \\
&< \frac{\pi}{2},
\end{aligned}$$

where the inequality on the final line follows because the quantity inside parentheses on the penultimate line is positive $(2^n - r(r'-1)) > 2^n - r^2 > 2^n - N^2 \geq 0)$. Thus, because the sine function is increasing on $[0, \pi/2]$, we will obtain an underestimate of $\sin\left(\frac{\pi m r(j/r')}{2^n}\right)$ by replacing $\frac{\pi m r(j/r')}{2^n}$ with $\pi\left(\frac{j}{r'} - \frac{j}{2^{n-\tilde{k}}}\right)$, which yields the lemma. □

Lemma B.2 *For real numbers a and b we have*

$$\sin^2(a \pm b) \geq (\sin^2 a)(1 - b^2) - 2|b||\sin a|.$$

Proof: Using the angle addition formula for the sine function and then

$$(s-t)^2 \geq s^2 - 2st, \tag{B.9}$$

which is valid for all real numbers s and t, we find

$$\begin{aligned}
\sin^2(a \pm b) &\geq (|\sin(a)\cos(b)| - |\sin(b)\cos(a)|)^2 \\
&\geq \sin^2(a)\cos^2(b) - 2|\sin(b)||\sin(a)||\cos(a)\cos(b)| \\
&\geq \sin^2(a)(1 - \sin^2(b)) - 2|\sin(b)||\sin(a)| \\
&\geq \sin^2(a)(1 - b^2) - 2|b||\sin(a)|. \ \square
\end{aligned}$$

Using (B.7), Lemma B.1, and replacing $\sin^2\left(\frac{\pi r(j/r')}{2^n}\right)$ with the larger quantity $\left(\frac{\pi r(j/r')}{2^n}\right)^2$, we have

$$P \geq \left[\frac{2^{\tilde{k}}(2)}{2^n m} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi j}{r'} - \frac{\pi j}{2^{n-\tilde{k}}}\right)}{\left(\frac{\pi r(j/r')}{2^n}\right)^2}\right] + (2^{\tilde{k}} - 1)\frac{m}{2^n}. \tag{B.10}$$

We seek to find an easily computable lower bound for the quantity in square brackets in the preceding inequality; calling this quantity Q, we have

$$\begin{aligned}
Q &= \frac{2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^n}} \left(\frac{1}{r} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi j}{r'} - \frac{\pi j}{2^{n-\tilde{k}}}\right)}{\left(\frac{j}{r'}\right)^2}\right) &\text{(B.11)} \\
&\geq \frac{2}{(\pi^2)\frac{mr}{2^n}} \left(\frac{1}{r'} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi j}{r'}\right)\left(1 - \left(\frac{\pi j}{2^{n-\tilde{k}}}\right)^2\right) - \frac{\pi j}{2^{n-\tilde{k}-1}}\sin\left(\frac{\pi j}{r'}\right)}{\left(\frac{j}{r'}\right)^2}\right) &\text{(B.12)}
\end{aligned}$$

where to obtain (B.12), we have used $\frac{2^{\tilde{k}}}{r} = \frac{1}{r'}$ as well as Lemma B.2 with $a = \frac{\pi j}{r'}$ and $b = \frac{\pi j}{2^{n-\tilde{k}}}$. We continue the calculation, underestimating the quantity on line (B.12) by replacing the first occurrence of $\pi j/2^{n-\tilde{k}}$ with $\frac{\pi r}{2^{n+1}}$, which exceeds its maximum possible value $\pi(r'-1)/2^{n-\tilde{k}+1}$, replacing $\frac{mr}{2^n}$ with $(1 + \frac{r}{2^n})$, and separating the sum:

$$Q \geq \frac{2}{(\pi^2)\left(1 + \frac{r}{2^n}\right)} \left(\frac{1}{r'} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi j}{r'}\right)\left(1 - \left(\frac{\pi r}{2^{n+1}}\right)^2\right)}{\left(\frac{j}{r'}\right)^2} - \frac{1}{r'} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\frac{\pi j}{2^{n-\tilde{k}-1}}\sin\left(\frac{\pi j}{r'}\right)}{\left(\frac{j}{r'}\right)^2}\right) \tag{B.13}$$

We make the subtracted quantity in (B.13) larger by replacing $\sin(\pi j/r')$ with $\pi j/r'$; we also cancel j's and r''s, obtaining

$$Q \geq \frac{2\left(1-\left(\frac{\pi r}{2^{n+1}}\right)^2\right)}{(\pi^2)\left(1+\frac{r}{2^n}\right)}\left(\frac{1}{r'}\sum_{j=1}^{\lfloor r'/2\rfloor}\frac{\sin^2\left(\frac{\pi j}{r'}\right)}{\left(\frac{j}{r'}\right)^2}\right)-\frac{2}{(\pi^2)\left(1+\frac{r}{2^n}\right)}\frac{\pi^2}{2^{n-\tilde{k}-1}}\lfloor r'/2\rfloor$$

We increase the subtracted quantity on the preceding line by replacing $1/(1+r/2^n)$ with 1 and we decrease the initial quantity by viewing the sum in parentheses as a Riemann sum with a left-endpoint selection for the decreasing function $x \mapsto \sin^2(\pi x)/x^2$ on $[\frac{1}{r'}, \frac{1}{2}+\frac{1}{2r'}]$:

$$\begin{aligned} Q &\geq \frac{2\left(1-\left(\frac{\pi r}{2^{n+1}}\right)^2\right)}{(\pi^2)\left(1+\frac{r}{2^n}\right)}\int_{1/r'}^{\frac{1}{2}+\frac{1}{2r'}}\frac{\sin^2(\pi x)}{x^2}\,dx-\frac{2^{\tilde{k}}(r'-1)}{2^{n-1}} \\ &\geq \frac{1-\left(\frac{\pi r}{2^{n+1}}\right)^2}{1+\frac{r}{2^n}}\left(\frac{2}{\pi^2}\int_{1/r'}^{\frac{1}{2}+\frac{1}{2r'}}\frac{\sin^2(\pi x)}{x^2}\,dx\right)-\frac{r}{2^{n-1}}. \end{aligned} \tag{B.14}$$

Thus, starting with (B.10) and using the definition of Q, the underestimate (B.14) for Q, as well as (B.1), we have

$$P \geq \frac{1-\left(\frac{\pi r}{2^{n+1}}\right)^2}{1+\frac{r}{2^n}}\left(\frac{2}{\pi^2}\int_{1/r'}^{\frac{1}{2}+\frac{1}{2r'}}\frac{\sin^2(\pi x)}{x^2}\,dx\right)-\frac{r}{2^{n-1}}+\frac{1}{r'}-\frac{1}{r}-\frac{2^{\tilde{k}}}{2^n}.$$

Because $r < N \leq 2^{n/2}$, we have $\frac{r}{2^n} \leq \frac{1}{N}$; using this as well as $2^{\tilde{k}}/2^n < r/2^n$ and $r = 2^{\tilde{k}}r'$ yields

$$P \geq \frac{1-\frac{\pi^2}{4N^2}}{1+\frac{1}{N}}\left(\frac{2}{\pi^2}\int_{1/r'}^{\frac{1}{2}+\frac{1}{2r'}}\frac{\sin^2(\pi x)}{x^2}\,dx\right)-\frac{3}{N}+\frac{1}{r'}-\frac{1}{2^{\tilde{k}}r'},$$

which is the advertised lower bound (29) on P.

Bounding $\tilde{P}_q$ Below (Including $\tilde{P}_0 = \tilde{P}$)

We derive the lower bound (37) for $\tilde{P}_q$, which upon letting $q = 0$ yields the lower bound (35) for $\tilde{P}$. We depend upon the results of the preceding subsection along with the following three Lemmas.

Lemma B.3 $\sum_{h=1}^{\infty}\frac{1}{(h-\frac{1}{2})^2} \leq 6$

Proof:

$$\sum_{h=1}^{\infty}\frac{1}{(h-\frac{1}{2})^2} = \left(4+\sum_{h=2}^{\infty}\frac{1}{(h-\frac{1}{2})^2}\right) \leq \left(4+\int_{1/2}^{\infty}\frac{1}{x^2}\,dx\right) = 6.\square$$

Lemma B.4 *For every integer h and every nonnegative integer q,*

$$\sin^2\left(\frac{\pi m r(j/r'+h)}{2^{n+q}}\right) \geq \sin^2\left(\frac{\pi m r(j/r')}{2^{n+q}}\right)\left(1-\left(\frac{\pi h r}{2^{n+q}}\right)^2\right)-2\left|\frac{\pi h r}{2^{n+q}}\right|.$$

Proof: Let $W = \sin^2\left(\frac{\pi mr(j/r'+h)}{2^{n+q}}\right)$. We have

$$\begin{aligned} W &\geq \left(\left|\sin\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\cos\left(\frac{\pi hmr}{2^{n+q}}\right)\right| - \left|\sin\left(\frac{\pi hmr}{2^{n+q}}\right)\cos\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\right|\right)^2 \\ &\geq \sin^2\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\cos^2\left(\frac{\pi hmr}{2^{n+q}}\right) - 2\left|\sin\left(\frac{\pi hmr}{2^{n+q}}\right)\right|, \end{aligned}$$

where, to obtain the second inequality, we have used (B.9) as well as

$$\left|\sin\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\cos\left(\frac{\pi hmr}{2^{n+q}}\right)\cos\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\right| \leq 1.$$

We continue the calculation, using $mr/2^{n+q} = 1 + x$, where $-r/2^{n+q} \leq x \leq r/2^{n+q}$:

$$\begin{aligned} W &\geq \sin^2\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\left(1 - \sin^2\left(\pi h(1+x)\right)\right) - 2\left|\sin\left(\pi h(1+x)\right)\right| \\ &\geq \sin^2\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\left(1 - \cos^2(\pi h)\sin^2(\pi hx)\right) - 2\left|\cos(\pi h)\sin(\pi hx)\right| \\ &\geq \sin^2\left(\frac{\pi mr(j/r'))}{2^{n+q}}\right)\left(1 - \left(\frac{\pi hr}{2^{n+q}}\right)^2\right) - 2\left|\frac{\pi hr}{2^{n+q}}\right|, \end{aligned}$$

as desired. □

Lemma B.5 *For every nonzero integer h and odd integer $r' \geq 3$,*

$$\frac{1}{r'}\sum_{j=1}^{\lfloor r'/2 \rfloor}\frac{\sin^2\left(\frac{\pi j}{r'}\right)}{\left(\frac{j}{r'}+h\right)^2} \geq \int_0^{\frac{1}{2}-\frac{1}{2r'}}\frac{\sin^2(\pi x)}{(x+h)^2}\,dx \tag{B.15}$$

Proof: For every integer h, let

$$f_h(x) = \frac{\sin^2(\pi x)}{(x+h)^2}. \tag{B.16}$$

Assume h is a negative integer. As x increases from 0 to $1/2$, $\sin^2(\pi x)$ increases and $(x+h)^2$ decreases (since $h \leq -1$). Thus f_h is an increasing function of x when h is negative. View the left-hand side of (B.15) as a Riemann sum for f_h corresponding to the partition $\mathcal{P} := \left\{[0, \frac{1}{r'}], [\frac{1}{r'}, \frac{2}{r'}], \ldots, \left[\frac{\frac{r'}{2}-\frac{3}{2}}{r'}, \frac{\frac{r'}{2}-\frac{1}{2}}{r'}\right]\right\}$ of $\left[0, \frac{1}{2} - \frac{1}{2r'}\right]$ with right-hand selection points $SP := \{\frac{1}{r'}, \frac{2}{r'}, \ldots, \frac{\frac{r'}{2}-\frac{1}{2}}{r'}\}$. Because, f_h is increasing on $\left[0, \frac{1}{2} - \frac{1}{2r'}\right]$, the Riemann sum overestimates the integral. Hence, (B.15) holds.

Now assume that h is a positive integer. In this case, the function f_h increases up to a maximum occurring at "$x_{\mathrm{m}}(h)$", which is a little less than $1/2$, and then decreases. For example, $x_m(1) \approx 0.4303$ for the function f_1 whose graph appears in Figure B.1. To establish the lemma for positive h we will need to used the following easily verified facts:

(a) For every positive integer h, the point $x_{\mathrm{m}}(h)$ where f_h attains its maximum value on $[0, 1/2]$ exceeds 0.43.

(b) For every positive integer h, there is a positive number $a < 1/4$ such that the graph of f_h is concave up on $[0, a]$ and down on $[a, 1/2]$.

Note that if $r' = 3$, 5, or 7, then the interval of integration on the right of (B.15) is contained in $[0, 0.43]$. Since f_h is increasing on $[0, 0.43]$ for every h, (B.15) holds for $r' = 3, 5, 7$ by the argument applied above for negative values of h. Thus we assume $r' \geq 9$.

For the remainder of the argument j is used to denote an integer in $\{1, 2, \ldots, (r' - 1)/2\}$. Define j_a to be the least positive integer such that $\frac{j_a}{r'} - \frac{1}{2r'} > a$. Because the graph of f_h is concave down on $(a, 1/2]$, for all $j \geq j_a$ the integral

$$\int_{\frac{j}{r'} - \frac{1}{2r'}}^{\frac{j}{r}' + \frac{1}{2r'}} f_h(x)\, dx \tag{B.17}$$

is less than the area $f(j/r')1/r'$ of the trapezoid (pictured in Figure B.1) bounded by the x-axis, the vertical lines $x = \frac{j}{r'} - \frac{1}{2r'}$, $x = \frac{j}{r'} + \frac{1}{2r'}$, and the line tangent to the graph of f_h at $(j/r', f(j/r'))$. It follows that

$$\frac{1}{r'} \sum_{j=j_a}^{(r'-1)/2} f_h\left(\frac{j}{r'}\right) \geq \int_{\frac{j_a}{r'} - \frac{1}{2r'}}^{\frac{1}{2}} f_h(x)\, dx. \tag{B.18}$$

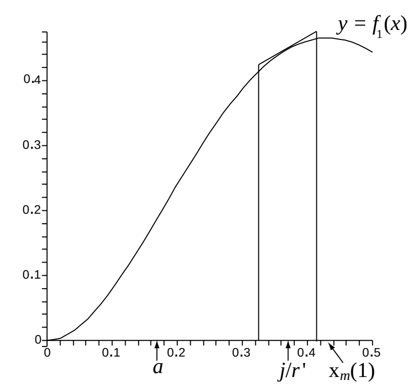

Fig. B.1. The trapezoid pictured has area exceeding the integral of f_1 over $\left[\frac{j}{r'} - \frac{1}{2r'}, \frac{j}{r'} + \frac{1}{2r'}\right]$.

For values of $j < j_a$, note that $\frac{j}{r'} \leq a + \frac{1}{2r'} \leq \frac{1}{4} + \frac{1}{18} < 0.43$ so that f_h is increasing on the interval $\left[\frac{j}{r'} - \frac{1}{r'}, \frac{j}{r'}\right]$. Hence for such a j, the integral

$$\int_{\frac{j}{r'} - \frac{1}{r'}}^{\frac{j}{r'}} f_h(x)\, dx \tag{B.19}$$

is less than $f(j/r')1/r'$. From this it follows that

$$\frac{1}{r'} \sum_{j=1}^{j_a - 1} f_h\left(\frac{j}{r'}\right) \geq \int_0^{\frac{j_a - 1}{r'}} f_h(x)\, dx. \tag{B.20}$$

Combining (B.18) and (B.20) yields

$$\begin{aligned}\frac{1}{r'}\sum_{j=1}^{(r'-1)/2} f_h(\frac{j}{r'}) &> \int_0^{\frac{j_a-1}{r'}} f_h(x)\,dx + \int_{\frac{j_a}{r'}-\frac{1}{2r'}}^{\frac{1}{2}} f_h(x)\,dx \\ &= \int_0^{\frac{1}{2}-\frac{1}{2r'}} f_h(x)\,dx + \left(\int_{\frac{1}{2}-\frac{1}{2r'}}^{\frac{1}{2}} f_h(x)\,dx - \int_{\frac{j_a-1}{r'}}^{\frac{j_a}{r'}-\frac{1}{2r'}} f_h(x)\,dx\right). \quad \text{(B.21)}\end{aligned}$$

We complete the proof of the lemma by establishing that the quantity in parentheses on the right of (B.21) is nonnegative. It suffices to show that the minimum value of f_h on $\left[\frac{1}{2}-\frac{1}{2r'}, \frac{1}{2}\right]$ exceeds the maximum value of f_h on $\left[\frac{j_a-1}{r'}, \frac{j_a}{r'}-\frac{1}{2r'}\right]$. We continue to assume that h is an arbitrary positive integer. Since

$$\frac{j_a}{r'} - \frac{1}{2r'} \le a + \frac{1}{r'} \le \frac{1}{4} + \frac{1}{9} < 0.43, \quad \text{(B.22)}$$

and f_h is increasing on $[0, .43]$, the maximum value of f on $\left[\frac{j_a-1}{r'}, \frac{j_a}{r'}-\frac{1}{2r'}\right]$ is $f_h\left(\frac{j_a}{r'}-\frac{1}{2r'}\right)$. The minimum value of f_h on $\left[\frac{1}{2}-\frac{1}{2r'}, \frac{1}{2}\right]$ occurs either at $L := \frac{1}{2}-\frac{1}{2r'}$ or at 1/2. A computation shows $f_h(1/2) > f_h(1/4+1/9)$; thus by (B.22) and the fact that f_h is increasing on $[0, .43]$, we may conclude $f_h(1/2) > f_h\left(\frac{j_a}{r'}-\frac{1}{2r'}\right)$, as desired. As for L, there are two possibilities, (i) $L \in [x_m(h), 1/2]$ or (ii) $\frac{j_a}{r'}-\frac{1}{2r'} < L < x_m(h)$. In case (i), $f(L) > f_h(1/2) > f_h\left(\frac{j_a}{r'}-\frac{1}{2r'}\right)$ and in case (ii), the desired inequality holds since f_h is increasing on $[0, x_m(h)]$. □

We are now in position to find a lower bound for $\tilde{P}_q$ in terms of integrals of the functions f_h defined by (B.16). We begin with our exact formula for $\tilde{P}_q$ from Section 6, obtaining an underestimate for $\tilde{P}_q$ by dropping the final term in the formula (which is clearly nonnegative):

$$\tilde{P}_q \ge 2^{\tilde{k}}\frac{2}{2^{n+q}m}\sum_{h=-2^{q+1}}^{2^{q+1}-1}\sum_{j=1}^{\lfloor r'/2\rfloor}\frac{\sin^2\left(\frac{\pi m r(j/r'+h)}{2^{n+q}}\right)}{\sin^2\left(\frac{\pi r(j/r'+h)}{2^{n+q}}\right)} + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}}. \quad \text{(B.23)}$$

Using $r < N/2$, $N^2 \le 2^n$ and Lemma B.4, we obtain

$$\sin^2\left(\frac{\pi m r(j/r'+h)}{2^{n+q}}\right) \ge \sin^2\left(\frac{\pi m r(j/r')}{2^{n+q}}\right)\left(1-\left(\frac{\pi h}{2^{q+1}N}\right)^2\right) - \frac{\pi|h|}{2^q N}. \quad \text{(B.24)}$$

Since we are assuming j varies from 1 to $\lfloor r'/2\rfloor$, $\frac{j}{r'} \le \frac{1}{r'}\left\lfloor\frac{r'}{2}\right\rfloor < 1/2$; thus, for every integer h,

$$\frac{|h|}{\left(\frac{j}{r'}+h\right)^2} \le \frac{|h|}{\left(|h|-\frac{1}{2}\right)^2} \le 4. \quad \text{(B.25)}$$

Using (B.24) and (B.23), we have

$$\begin{aligned}\tilde{P}_q &\ge 2^{\tilde{k}}\frac{2}{2^{n+q}m}\sum_{h=-2^{q+1}}^{2^{q+1}-1}\sum_{j=1}^{\lfloor r'/2\rfloor}\frac{\sin^2\left(\frac{\pi m r(j/r')}{2^{n+q}}\right)\left(1-\left(\frac{\pi h}{2^{q+1}N}\right)^2\right)-\frac{\pi|h|}{2^q N}}{\sin^2\left(\frac{\pi r(j/r'+h)}{2^{n+q}}\right)} + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}} \\ &\ge \frac{2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}}\sum_{h=-2^{q+1}}^{2^{q+1}-1}\left(\frac{1}{r}\sum_{j=1}^{\lfloor r'/2\rfloor}\frac{\sin^2\left(\frac{\pi m r(j/r')}{2^{n+q}}\right)\left(1-\left(\frac{\pi h}{2^{q+1}N}\right)^2\right)-\frac{\pi|h|}{2^q N}}{(j/r'+h)^2}\right) + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}}\end{aligned}$$

$$\geq \frac{\left(1-\left(\frac{\pi 2^{q+1}}{2^{q+1}N}\right)^2\right)2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}} \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{1}{r} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r')}{2^{n+q}}\right)}{(j/r'+h)^2} \right) \tag{B.26}$$

$$- \frac{2}{(\pi^2)\frac{mr}{2^{n+q}}} \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{1}{r'} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\frac{\pi|h|}{2^q N}}{(j/r'+h)^2} \right) + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}},$$

where (B.26) follows from the line that precedes it by replacing the first occurrence of h in the numerator with its maximum possible absolute value (namely 2^{q+1}), by separating the sum, and by using $\frac{2^{\tilde{k}}}{r} = \frac{1}{r'}$. Continuing the calculation, we have

$$\tilde{P}_q \geq \frac{\left(1-\left(\frac{\pi}{N}\right)^2\right)2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}} \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{1}{r} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r')}{2^{n+q}}\right)}{(j/r'+h)^2} \right)$$

$$- \frac{2}{(\pi 2^q N)\frac{mr}{2^{n+q}}} \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{1}{r'} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{|h|}{(|h|-1/2)^2} \right) + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}}$$

$$\geq \left(1-\left(\frac{\pi}{N}\right)^2\right) \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left[\frac{2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}} \left(\frac{1}{r} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r')}{2^{n+q}}\right)}{(j/r'+h)^2} \right) \right] \tag{B.27}$$

$$- \frac{2^{q+2} 8 \lfloor r'/2 \rfloor}{(\pi 2^q N r')\frac{mr}{2^{n+q}}} + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}},$$

where (B.25)) provides the final inequality. Using Lemma B.1, with $n+q$ replacing n, we obtain, for $h \in \{-2^{q+1}, \ldots, 2^{q+1}-1\}$, a lower bound on the square-bracketed quantity in (B.27):

$$\frac{2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}} \left(\frac{1}{r} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r')}{2^{n+q}}\right)}{(j/r'+h)^2} \right) \geq \frac{2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}} \left(\frac{1}{r} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi j}{r'} - \frac{\pi j}{2^{n+q-\tilde{k}}}\right)}{(j/r'+h)^2} \right). \tag{B.28}$$

The right-hand side of the preceding inequality, with $h = 0$, is identical to Q of (B.11) with $n+q$ replacing n. Thus our work bounding Q below culminating in (B.14) shows

$$\frac{2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}} \left(\frac{1}{r} \sum_{j=1}^{\lfloor r'/2 \rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r')}{2^{n+q}}\right)}{(j/r'+0)^2} \right) \geq \frac{1-\left(\frac{\pi r}{2^{n+q+1}}\right)^2}{1+\frac{r}{2^{n+q}}} \left(\frac{2}{\pi^2} \int_{1/r'}^{\frac{1}{2}+\frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\, dx \right) - \frac{r}{2^{n+q-1}}. \tag{B.29}$$

Thus we have a lower bound for the $h = 0$ summand of (B.27). To bound below the other summands in (B.27), i.e. those corresponding to $h \in \{-2^{q+1}, \ldots, 2^{q+1}-1\} \setminus \{0\}$, we again cycle through the lower bound calculation for Q, (B.11) through (B.14); this time with two substitutions: $n+q$ replacing n and $j/r'+h$ replacing j/r' in the denominator. Underestimate

(B.13) becomes

$$\frac{2\left(1-\left(\frac{\pi r}{2^{n+q+1}}\right)^2\right)}{(\pi^2)\left(1+\frac{r}{2^{n+q}}\right)}\frac{1}{r'}\sum_{j=1}^{\lfloor r'/2\rfloor}\frac{\sin^2\left(\frac{\pi j}{r'}\right)}{\left(\frac{j}{r'}+h\right)^2}-\frac{2}{(\pi^2)\left(1+\frac{r}{2^{n+q}}\right)}\frac{1}{r'}\sum_{j=1}^{\lfloor r'/2\rfloor}\frac{\frac{\pi j}{2^{n+q-\tilde{k}-1}}\sin\left(\frac{\pi j}{r'}\right)}{\left(\frac{j}{r'}+h\right)^2}. \tag{B.30}$$

We make the subtracted quantity in (B.30) larger by replacing $(j/r'+h)^2$ with $(|h|-1/2)^2$, $\sin(\pi j/r')$ with $\pi j/r'$, and we also replace $1/(1+\frac{r}{2^{n+q}})$ with the larger number 1. Thus the subtracted quantity in (B.30) is less than

$$\frac{2}{(\pi^2)}\left(\frac{1}{r'}\sum_{j=1}^{\lfloor r'/2\rfloor}\frac{\frac{\pi j}{2^{n+q-\tilde{k}-1}}\left(\frac{\pi j}{r'}\right)}{\left(|h|-\frac{1}{2}\right)^2}\right) \quad\leq\quad \frac{2}{2^{n+q-\tilde{k}-1}\left(|h|-\frac{1}{2}\right)^2}\left(\frac{1}{r'^2}\sum_{j=1}^{\lfloor r'/2\rfloor}j^2\right).$$

The quantity on the right in parentheses simplifies:

$$\frac{1}{r'^2}\frac{\left\lfloor\frac{r'}{2}\right\rfloor\left(\left\lfloor\frac{r'}{2}\right\rfloor+1\right)\left(2\left\lfloor\frac{r'}{2}\right\rfloor+1\right)}{6}=\frac{(r'-1)(r'+1)}{24r'}\leq\frac{r'+1}{24},$$

where we have used $\left\lfloor\frac{r'}{2}\right\rfloor=\frac{r'-1}{2}$. Thus the subtracted quantity (B.30) is less than or equal to

$$\frac{(r'+1)}{12\cdot 2^{n+q-\tilde{k}-1}\left(|h|-\frac{1}{2}\right)^2}$$

and, by Lemma B.5, the initial quantity in (B.30) is greater than or equal to

$$\frac{2\left(1-\left(\frac{\pi r}{2^{n+q+1}}\right)^2\right)}{(\pi^2)\left(1+\frac{r}{2^{n+q}}\right)}\int_0^{\frac{1}{2}-\frac{1}{2r'}}\frac{\sin^2(\pi x)}{(x+h)^2}\,dx.$$

Using the preceding two observations as well as $2^{\tilde{k}}r'=r$, $r<\frac{N}{2}\leq\frac{2^{n/2}}{2}$, and $r+2^{\tilde{k}}\leq 2r$, we have

$$\begin{aligned}
\text{Quantity}(B.30) \quad &\geq \quad \frac{2\left(1-\left(\frac{\pi r}{2^{n+q+1}}\right)^2\right)}{(\pi^2)\left(1+\frac{r}{2^{n+q}}\right)}\int_0^{\frac{1}{2}-\frac{1}{2r'}}\frac{\sin^2(\pi x)}{(x+h)^2}\,dx-\frac{r+2^{\tilde{k}}}{12\cdot 2^{n+q-1}\left(|h|-\frac{1}{2}\right)^2}\\
&\geq \quad \frac{1-\left(\frac{\pi}{2^{q+2}N}\right)^2}{1+\frac{1}{2^{q+1}N}}\left(\frac{2}{\pi^2}\int_0^{\frac{1}{2}-\frac{1}{2r'}}\frac{\sin^2(\pi x)}{(x+h)^2}\,dx\right)-\frac{1}{12\cdot N2^{q-1}(|h|-1/2)^2}\\
&= \quad C(q,N)\left(\frac{2}{\pi^2}\int_0^{\frac{1}{2}-\frac{1}{2r'}}\frac{\sin^2(\pi x)}{(x+h)^2}\,dx\right)-L(h),
\end{aligned} \tag{B.31}$$

where we have defined

$$C(q,N)=\frac{1-\left(\frac{\pi}{2^{q+2}N}\right)^2}{1+\frac{1}{2^{q+1}N}} \quad\text{and}\quad L(h)=\frac{1}{12\cdot N2^{q-1}(|h|-1/2)^2} \quad \text{for} \quad h\neq 0. \tag{B.32}$$

Notice that for nonzero h, our under-approximating integral from (B.31) has limits from 0 to $\frac{1}{2}-\frac{1}{2r'}$ whereas that for the $h=0$ case has limits from $\frac{1}{r'}$ to $\frac{1}{2}+\frac{1}{2r'}$. To make our final lower-bound formula for $\tilde{P}_q$ simpler, we adjust the under-approximating integral from (B.29) for the $h = 0$ case as follows:

$$\begin{aligned}
\int_{1/r'}^{\frac{1}{2}+\frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\,dx &= \int_{0}^{\frac{1}{2}+\frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\,dx - \int_{0}^{\frac{1}{r'}} \frac{\sin^2(\pi x)}{x^2}\,dx \\
&> \int_{0}^{\frac{1}{2}-\frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\,dx - \frac{\pi^2}{r'},
\end{aligned}$$

where we have used the nonnegativity of the integrand as well as $\sin^2(\pi x)/x^2 \le \pi^2$ to obtain the inequality. Thus (B.29) becomes

$$\begin{aligned}
\frac{2^{\tilde{k}+1}}{(\pi^2)\frac{mr}{2^{n+q}}}\left(\frac{1}{r}\sum_{j=1}^{\lfloor r'/2\rfloor} \frac{\sin^2\left(\frac{\pi m r (j/r')}{2^{n+q}}\right)}{(j/r'+0)^2}\right) &\ge \frac{1-\left(\frac{\pi r}{2^{n+q+1}}\right)^2}{1+\frac{r}{2^{n+q}}}\left(\frac{2}{\pi^2}\int_0^{\frac{1}{2}-\frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\,dx\right) \\
&\quad - \frac{1-\left(\frac{\pi r}{2^{n+q+1}}\right)^2}{1+\frac{r}{2^{n+q}}}\left(\frac{2}{r'}\right) - \frac{r}{2^{n+q-1}} \\
&\ge \frac{1-\left(\frac{\pi}{N2^{q+2}}\right)^2}{1+\frac{1}{N2^{q+1}}}\left(\frac{2}{\pi^2}\int_0^{\frac{1}{2}-\frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\,dx\right) - \frac{2}{r'} - \frac{1}{N2^q} \\
&= C(q,N)\left(\frac{2}{\pi^2}\int_0^{\frac{1}{2}-\frac{1}{2r'}} \frac{\sin^2(\pi x)}{x^2}\,dx\right) - L(0), \qquad \text{(B.33)}
\end{aligned}$$

where $L(0) := \frac{2}{r'} + \frac{1}{N2^q}$.

Using (B.33) to bound below the $h = 0$ term of the sum on line (B.27) and using (B.31) to bound below the terms corresponding to $h \neq 0$, we obtain

$$\begin{aligned}
\tilde{P}_q \ \ge\ & \left(1-\left(\frac{\pi}{N}\right)^2\right)\sum_{h=-2^{q+1}}^{2^{q+1}-1}\left(C(q,N)\left(\frac{2}{\pi^2}\int_0^{\frac{1}{2}-\frac{1}{2r'}} \frac{\sin^2(\pi x)}{(x+h)^2}\,dx\right) - L(h)\right) \qquad \text{(B.34)} \\
& - \frac{2^{q+2}8\lfloor r'/2\rfloor}{(\pi 2^q N r')\frac{mr}{2^{n+q}}} + (2^{\tilde{k}}-1)\frac{m}{2^{n+q}}.
\end{aligned}$$

The preceding inequality will yield the advertised bound (37) for $\tilde{P}_q$ after a few more steps. Using $\frac{1}{r'}\lfloor r'/2\rfloor < 1/2$, $m \ge \frac{2^{n+q}}{r} - 1$, and $r < N/2$, we have

$$\frac{2^{q+2}8\lfloor r'/2\rfloor}{(\pi 2^q N r')\frac{mr}{2^{n+q}}} \le \frac{16}{\pi N\left(1-\frac{1}{N2^{q+1}}\right)}. \qquad \text{(B.35)}$$

Using $2^{\tilde{k}} < r < N/2$ and again using $m \ge \frac{2^{n+q}}{r} - 1$, we get

$$(2^{\tilde{k}}-1)\frac{m}{2^{n+q}} \ge \frac{1}{r'} - \frac{1}{r} - \frac{2^{\tilde{k}}}{2^{n+q}} + \frac{1}{2^{n+q}} > \frac{1}{r'} - \frac{1}{2^{\tilde{k}}r'} - \frac{1}{N2^{q+1}}. \qquad \text{(B.36)}$$

Finally,

$$\sum_{h=-2^{q+1}}^{2^{q+1}-1} L(h) = L(0) + \sum_{\substack{h=-2^{q+1} \\ h\neq 0}}^{2^{q+1}-1} \frac{1}{12\cdot N2^{q-1}(|h|-1/2)^2} \quad \text{(by (B.32))}$$

$$\leq \frac{2}{r'} + \frac{1}{N2^q} + \frac{1}{12 \cdot N2^{q-1}} \left(2 \sum_{h=1}^{\infty} \frac{1}{(|h| - 1/2)^2} \right)$$
$$\leq \frac{2}{r'} + \frac{1}{N2^q} + \frac{1}{N2^{q-1}} = \frac{2}{r'} + \frac{3}{N2^q},$$

where Lemma B.3 provides the final inequality.

Beginning with (B.34) and then using (B.35), (B.36), and $\sum_{h=-2^{q+1}}^{2^{q+1}-1} L(h) \leq \frac{2}{r'} + \frac{3}{N2^q}$, we have

$$\tilde{P}_q \geq \left(1 - \left(\frac{\pi}{N}\right)^2\right) C(q, N) \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{2}{\pi^2} \int_0^{\frac{1}{2} - \frac{1}{2r'}} \frac{\sin^2(\pi x)}{(x+h)^2}\, dx \right) - \left(1 - \left(\frac{\pi}{N}\right)^2\right) \left(\frac{2}{r'} + \frac{3}{N2^q} \right)$$
$$- \frac{16}{\pi N \left(1 - \frac{1}{N2^{q+1}}\right)} + \frac{1}{r'} - \frac{1}{2^{\tilde{k}} r'} - \frac{1}{N2^{q+1}}.$$

Substituting 1 for $\left(1 - \left(\frac{\pi}{N}\right)^2\right)$ the second time it appears on the right of the preceding inequality, simplifying, and using the definition of $C(q, N)$, we arrive at the advertised lower bound on $\tilde{P}_q$:

$$\tilde{P}_q \geq \frac{\left(1 - \left(\frac{\pi}{N}\right)^2\right)\left(1 - \left(\frac{\pi}{2^{q+2}N}\right)^2\right)}{1 + \frac{1}{2^{q+1}N}} \sum_{h=-2^{q+1}}^{2^{q+1}-1} \left(\frac{2}{\pi^2} \int_0^{\frac{1}{2} - \frac{1}{2r'}} \frac{\sin^2(\pi x)}{(x+h)^2}\, dx \right) - \frac{1}{r'}$$
$$- \frac{7}{N2^{q+1}} - \frac{16}{\pi N \left(1 - \frac{1}{N2^{q+1}}\right)} - \frac{1}{2^{\tilde{k}} r'}.$$