MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 177-194

AVERAGE CASE ERROR ESTIMATES FOR THE STRONG PROBABLE PRIME TEST

IVAN DAMGÅRD, PETER LANDROCK, AND CARL POMERANCE

Dedicated to the memory of D. H. Lehmer

ABSTRACT. Consider a procedure that chooses k-bit odd numbers independently and from the uniform distribution, subjects each number to t independent iterations of the strong probable prime test (Miller-Rabin test) with randomly chosen bases, and outputs the first number found that passes all t tests. Let $p_{k,t}$ denote the probability that this procedure returns a composite number. We obtain numerical upper bounds for $p_{k,t}$ for various choices of k, t and obtain clean explicit functions that bound $p_{k,t}$ for certain infinite classes of k, t. For example, we show $p_{100,10} \leq 2^{-44}$, $p_{300,5} \leq 2^{-60}$, $p_{600,1} \leq 2^{-75}$, and $p_{k,1} \leq k^2 4^{2-\sqrt{k}}$ for all $k \geq 2$. In addition, we characterize the worst-case numbers with unusually many "false witnesses" and give an upper bound on their distribution that is probably close to best possible.

1. INTRODUCTION

Let $n > 1$ be odd and write $n - 1 = 2^s u$, where u is odd. If n is prime and $n \nmid a$, then either

$$(1.1) \qquad a^u \equiv 1 \bmod n \qquad \text{or} \qquad a^{2^i u} \equiv -1 \bmod n \quad \text{for some } i < s.$$

If this should hold for some pair n, a we say n is a *strong probable prime base* a. This concept was introduced by Selfridge in the mid 1970s; a variant was used by Miller in his ERH-conditional primality test, and Rabin used it in his probabilistic "primality" test. Often called now the *Miller-Rabin test*, we use the more descriptive *strong probable prime test.*

Note that though (1.1) always occurs if n is prime and $n \nmid a$, it may sometimes also occur when n is composite. Let

$$\mathcal{S}(n) = \{a \in [1, n-1] : a^u \equiv 1 \bmod n \text{ or } a^{2^i u} \equiv -1 \bmod n \text{ for some } i < s\}$$

and let $S(n) = |\mathcal{S}(n)|$. It has been shown independently by Rabin [7] and Monier [5] that if n is odd and composite, then $S(n) \leq (n-1)/4$. In fact, if $n \neq 9$ is odd and composite, then $S(n) \leq \varphi(n)/4$, where φ is Euler's function.

Thus, Rabin [7] showed that the strong probable prime test could be made into a probabilistic compositeness test. That is, given an odd composite number n, choose a random integer $a \in [1, n-1]$ and see if $a \in \mathcal{S}(n)$. If not, then

Received by the editor July 27, 1992.
1991 *Mathematics Subject Classification*. Primary 11Y11; Secondary 11A51.
The third author was supported in part by an NSF grant.

you have proved that n is composite. The expected number of iterations to come up with such a proof is of course at most $4/3$.

In practice, though, we may be presented with a large odd number n for which we are not sure if it is prime or composite. Suppose we choose a random number $a \in [1, n-1]$ and see if $a \in \mathcal{S}(n)$. If $a \in \mathcal{S}(n)$, we might choose another number $a' \in [1, n-1]$ and try again. From the Rabin-Monier theorem, we have the following: the probability that an odd composite number n has $a_1, \dots, a_t \in \mathcal{S}(n)$ for $a_1, \dots, a_t$ chosen uniformly and independently from the integers in $[1, n-1]$ is at most 4^{-t}.

Suppose now that the number n is also chosen randomly, say from the set M_k of odd k-bit integers. Say we continue to choose numbers n from M_k until we find one that passes t random strong probable prime tests (and does not fail any). That is, we choose $n \in M_k$ at random, then choose $a_1 \in [1, n-1]$ at random and see if $a_1 \in \mathcal{S}(n)$. If so, we choose $a_2 \in [1, n-1]$ at random and see if $a_2 \in \mathcal{S}(n)$. We continue until some $a_i \notin \mathcal{S}(n)$ for $i \le t$, in which case we discard n and try again, or until we find some n which has $a_1, \dots, a_t \in \mathcal{S}(n)$.

Of course, if n is prime, then n will always have $a_1, \dots, a_t \in \mathcal{S}(n)$. Let $p_{k,t}$ denote the probability that this procedure returns a composite number n.

From the above it may be tempting to say $p_{k,t} \le 4^{-t}$ for all k. But as shown in [2], the reasoning behind such a conclusion from the Rabin-Monier theorem is fallacious. Indeed, if the primes were very sparsely distributed (as they are in M_k for k large), then it might be *more* likely to observe an event with probability 4^{-t} than to observe an event with a lower probability of occurrence (namely that a random number in M_k is prime).

Thus any estimation of $p_{k,t}$ must take into account the distribution of the primes. Moreover, to get a good upper bound for $p_{k,t}$, one must show that the worst-case upper bound for $S(n)/(n-1)$ of $1/4$ for n composite is rather an unusual occurrence. That is, for most n, $S(n)/(n-1)$ is considerably smaller than $1/4$. Thus we shall be concerned with the *average* value of $S(n)/(n-1)$ for n odd and composite, rather than the *worst* (highest) value.

From the results in [3] we have

$$p_{k,1} \le 2^{-(1+o(1))k \ln\ln k/\ln k} \quad \text{for } k \to \infty. \tag{1.2}$$

However, the expression $o(1)$ was not computed explicitly in [3], so this result is computationally useless for finite values of k.

In this paper we present elementary arguments for explicit upper estimates of $p_{k,t}$ for various values of k, t. Numerical estimates are presented in Table 1. One can see in this table that we often have $p_{k,t}$ considerably *smaller* than 4^{-t}. We also can obtain explicit upper bound estimates for $p_{k,t}$ that are valid for all large values of the subscripts. In particular, we show that

$$\begin{aligned}
&p_{k,1} < k^2 4^{2-\sqrt{k}} \quad \text{for} \quad k \ge 2,\\
&p_{k,t} < k^{3/2} 2^t t^{-1/2} 4^{2-\sqrt{tk}} \quad \text{for} \quad t = 2,\ k \ge 88 \quad \text{or} \quad 3 \le t \le k/9,\ k \ge 21,\\
&p_{k,t} < \tfrac{7}{20} k 2^{-5t} + \tfrac{1}{7} k^{15/4} 2^{-k/2-2t} + 12k 2^{-k/4-3t} \quad \text{for} \quad t \ge k/9,\ k \ge 21,\\
&p_{k,t} < \tfrac{1}{7} k^{15/4} 2^{-k/2-2t} \quad \text{for} \quad t \ge k/4,\ k \ge 21.
\end{aligned}$$

The proof of the last two inequalities uses a result of independent interest, namely that the number of Carmichael numbers up to x with just three prime factors is at most $x^{1/2}(\ln x)^{O(1)}$. Previously, all we knew (see [6]) was that there are at most $O(x^{2/3})$ such numbers up to x. (Recall that n is a Carmichael number if n is composite and $a^n \equiv a \bmod n$ for all integers a. The *existence* of Carmichael numbers is what causes us to discard the simple Fermat congruence for (1.1).)

It is interesting to note that the above upper bound for $p_{k,t}$ in the range $t \le k/9$ decays by a factor smaller than $1/4$ as t increases by 1, while for $t \ge k/4$, it decays by the factor $1/4$. This confirms the perhaps intuitive concept that $p_{k,t}$ for large t is dominated by the possibility of choosing a worst-case composite number n with about $n/4$ "false witnesses", while for smaller values of t, the probability is dominated by more typical values of n with only a few false witnesses.

In [4], a probability related to $p_{k,1}$ is computed. Consider a procedure which chooses a random pair n, a, where $n \le x$ is an odd number and $1 < a < n-1$ (with the uniform distribution on all such pairs), and accepts n if $a^{n-1} \equiv 1 \bmod n$. Let $P(x)$ denote the probability that this procedure accepts a composite number n. In §7 we show how the numerical estimates for $P(x)$ from [4] can be used to obtain estimates for $p_{k,t}$. Further, these estimates may be used together with the ideas from this paper to get estimates that are sometimes stronger than both those in Table 1 and those in [4]. For this see Table 2.

It is easy to see that the Rabin-Monier theorem implies that $p_{k,t} \le 4^{1-t}p_{k,1}/(1-p_{k,1})$ for every $k \ge 2$, $t \ge 2$. Thus from (1.2) it follows that there is a number k_0 such that $p_{k,t} \le 4^{-t}$ for all $k \ge k_0$, $t \ge 1$. Indeed, if $p_{k,1} \le 1/5$, then $p_{k,t} \le 4^{-t}$ for all $t \ge 1$. It was left as an open question in [2] to determine a numerical value for k_0. From the work in [4] it is possible to show that 200 may be taken as a value for k_0. Using our result that $p_{k,1} \le k^2 4^{2-\sqrt{k}}$, one easily sees that $p_{k,1} \le 1/5$ for each $k \ge 95$, so that 95 may be taken as a value for k_0. From Propositions 1 and 2 below it follows that $p_{k,1} \le 1/5$ for each $k \in \{55, 56, \dots, 94\}$, so that k_0 may be taken as 55. Going further, we find that $p_{k,1} \le 1/4$ and $p_{k,2} \le 1/17$ for each $k \in \{51, 52, 53, 54\}$, so that using $p_{k,t} \le 4^{2-t}p_{k,2}/(1-p_{k,2})$ for $t \ge 3$, we see that k_0 may be taken to be 51. By tightening estimates in this paper and computing $p_{k,1}$ for small values of k, it may now be possible to show that k_0 can be taken to be 2, which we conjecture to be the case.

Thanks are due to Ronald Burthe who brought some minor errors to our attention.

2. Preliminaries

Recall the definition of $S(n)$ from §1. Let $\alpha(n) := S(n)/\varphi(n)$ for $n > 1$, n odd. Thus $\alpha(n) \le 1/4$ for odd composite $n > 9$.

Let $\omega(n)$ denote the number of distinct prime factors of n, and let $\Omega(n)$ denote the number of prime factors of n counted with multiplicity. We shall always let p denote a prime number. By $p^\beta \parallel n$, we mean $p^\beta \mid n$ and $p^{\beta+1} \nmid n$.

Lemma 1. *If $n > 1$ is odd, then*

$$\frac{1}{\alpha(n)} \ge 2^{\omega(n)-1} \prod_{p^\beta \parallel n} p^{\beta-1} \frac{p-1}{(p-1, n-1)} \ge 2^{\Omega(n)-1} \prod_{p \mid n} \frac{p-1}{(p-1, n-1)}.$$

Proof. The second inequality follows immediately from the identity

$$\sum_{p^\beta \| n} (\beta - 1) = \Omega(n) - \omega(n).$$

For the first inequality, by using the well-known formula for $\varphi(n)$ and the definition of $\alpha(n)$, it will suffice to prove

$$S(n) \leq 2^{1-\omega(n)} \prod_{p|n} (p-1, n-1). \tag{2.1}$$

Let $\nu(n)$ be the largest number such that $2^{\nu(n)} \mid p-1$ for each prime $p \mid n$. Suppose the largest odd factor of $n-1$ is u. In [5], Monier showed that

$$S(n) = (1 + 1 + 2^{\omega(n)} + 2^{2\cdot\omega(n)} + \cdots + 2^{(\nu(n)-1)\omega(n)}) \prod_{p|n} (p-1, u). \tag{2.2}$$

Now

$$\prod_{p|n} (p-1, u) \leq 2^{-\nu(n)\omega(n)} \prod_{p|n} (p-1, n-1)$$

and

$$1 + 1 + 2^{\omega(n)} + 2^{2\cdot\omega(n)} + \cdots + 2^{(\nu(n)-1)\omega(n)} \leq 2 \cdot 2^{(\nu(n)-1)\omega(n)}. \tag{2.3}$$

Thus,

$$S(n) \leq 2 \cdot 2^{(\nu(n)-1)\omega(n)} 2^{-\nu(n)\omega(n)} \prod_{p|n} (p-1, n-1) = 2^{1-\omega(n)} \prod_{p|n} (p-1, n-1),$$

which proves (2.1) and the lemma. □

Lemma 2. *If t is a real number with $t \geq 1$, then*

$$\sum_{n=[t]+1}^{\infty} \frac{1}{n^2} < \frac{\pi^2 - 6}{3t}.$$

Proof. Let $m = [t]$, so that $m \geq 1$. Then

$$\begin{aligned} \sum_{n=[t]+1}^{\infty} \frac{1}{n^2} &= \sum_{n=1}^{\infty} \frac{1}{n^2} - \sum_{n=1}^{m} \frac{1}{n^2} = \frac{\pi^2}{6} - \sum_{n=1}^{m} \frac{1}{n^2} \\ &< \frac{m+1}{t} \left(\frac{\pi^2}{6} - \sum_{n=1}^{m} \frac{1}{n^2} \right) = \frac{1}{t} f(m), \end{aligned}$$

say. If k is at least 2, then

$$\begin{aligned} f(k-1) - f(k) &= k \left(\frac{\pi^2}{6} - \sum_{n=1}^{k-1} \frac{1}{n^2} \right) - (k+1) \left(\frac{\pi^2}{6} - \sum_{n=1}^{k} \frac{1}{n^2} \right) \\ &= -\frac{\pi^2}{6} + \frac{k}{k^2} + \sum_{n=1}^{k} \frac{1}{n^2} = -\frac{\pi^2}{6} + \sum_{n=1}^{k} \frac{1}{n^2} + \int_k^{\infty} \frac{dx}{x^2} \\ &> -\frac{\pi^2}{6} + \sum_{n=1}^{\infty} \frac{1}{n^2} = 0. \end{aligned}$$

Thus the sequence $f(1), f(2), \ldots$ is decreasing and the above estimate gives

$$\sum_{n=[t]+1}^{\infty} \frac{1}{n^2} < \frac{1}{t} f(1) = \frac{2}{t}\left(\frac{\pi^2}{6} - 1\right),$$

which proves the lemma. □

3. A simple estimate

Recalling the definition of $\alpha(n)$ from §2, we let C_m denote the set of odd, composite integers n with $\alpha(n) > 2^{-m}$. Thus if $m = 1$, we have $C_m = \varnothing$, and if $m = 2$, we have $C_m = \{9\}$.

Let M_k denote the set of odd k-bit integers. For $k \geq 2$, we have $|M_k| = 2^{k-2}$. We shall be concerned with the proportion in M_k of those odd integers which are also in C_m.

Theorem 1. *If m, k are positive integers with $m + 1 \leq 2\sqrt{k-1}$, then*

$$\frac{|C_m \cap M_k|}{|M_k|} < \frac{8}{3}(\pi^2 - 6) \sum_{j=2}^{m} 2^{m-j-(k-1)/j}.$$

Proof. Note that from Lemma 1, $n \in C_m$ implies $\Omega(n) \leq m$. Let $N(m, k, j)$ denote the set of $n \in C_m \cap M_k$ with $\Omega(n) = j$. Thus,

$$|C_m \cap M_k| = \sum_{j=2}^{m} |N(m, k, j)|. \tag{3.1}$$

Suppose $n \in N(m, k, j)$, where $2 \leq j \leq m$. Let p denote the largest prime factor of n. Since $2^{k-1} < n < 2^k$, we have $p > 2^{(k-1)/j}$. Let $d(p, n) = (p-1)/(p-1, n-1)$. From Lemma 1 and the definition of C_m, we have

$$2^m > \frac{1}{\alpha(n)} \geq 2^{\Omega(n)-1} d(p, n) = 2^{j-1} d(p, n),$$

so that $d(p, n) < 2^{m+1-j}$.

For a given prime $p > 2^{(k-1)/j}$ and integer $d \mid p-1$ with $d < 2^{m+1-j}$, we ask how many $n \in M_k$ there are with $p \mid n$, $d = d(p, n)$, and n composite. This is at most the number of solutions of the system

$$n \equiv 0 \bmod p, \quad n \equiv 1 \bmod \frac{p-1}{d}, \qquad p < n < 2^k,$$

which, by the Chinese Remainder Theorem, is at most

$$\frac{2^k d}{p(p-1)}.$$

We conclude that

$$\begin{aligned} |N(m, k, j)| &\leq \sum_{p > 2^{(k-1)/j}} \sum_{\substack{d \mid p-1 \\ d < 2^{m+1-j}}} \frac{2^k d}{p(p-1)} \\ &= 2^k \sum_{d < 2^{m+1-j}} \sum_{\substack{p > 2^{(k-1)/j} \\ d \mid p-1}} \frac{d}{p(p-1)}. \end{aligned} \tag{3.2}$$

Now, for the inner sum we have

$$\sum_{\substack{p>2^{(k-1)/j}\\ d\mid p-1}} \frac{d}{p(p-1)} < \sum_{ud>2^{(k-1)/j}-1} \frac{d}{(ud+1)ud}$$
$$< \frac{1}{d} \sum_{u>(2^{(k-1)/j}-1)/d} \frac{1}{u^2} < \frac{\pi^2-6}{3} \cdot \frac{1}{2^{(k-1)/j}-1},$$

by Lemma 2. Putting this estimate in (3.2), we get

$$(3.3)\qquad \begin{aligned} |N(m,k,j)| &< 2^k \frac{\pi^2-6}{3} \sum_{d<2^{m+1-j}} \frac{1}{2^{(k-1)/j}-1} \\ &= 2^k \frac{\pi^2-6}{3} \cdot \frac{2^{m+1-j}-1}{2^{(k-1)/j}-1}. \end{aligned}$$

So far we have not used our hypothesis $m+1 \le 2\sqrt{k-1}$. Using this and the inequality $j+(k-1)/j \ge 2\sqrt{k-1}$, which is valid for all $j>0$, we have $m+1 \le j+(k-1)/j$. Thus,

$$\frac{2^{m+1-j}-1}{2^{(k-1)/j}-1} \le \frac{2^{m+1-j}}{2^{(k-1)/j}} = 2 \cdot 2^{m-j-(k-1)/j}.$$

Combining this estimate with (3.3) and (3.1), we have

$$|C_m \cap M_k| < 2^{k+1} \frac{\pi^2-6}{3} \sum_{j=2}^{m} 2^{m-j-(k-1)/j}.$$

Thus, the theorem follows from the fact that $|M_k| = 2^{k-2}$. □

4. First numerical results

In this section we use Theorem 1 and an explicit estimate for the distribution of prime numbers to obtain some quite good numerical estimates for $p_{k,t}$ for various values of k and t.

Let $\pi(x)$ denote the number of primes $p \le x$ and let $\sum'$ denote a sum over composite integers.

Recall the function $S(n)$ from §1 and let $\bar{\alpha}(n) := S(n)/(n-1)$. Thus, $\bar{\alpha}(n) \le \alpha(n)$ for all odd $n > 1$. Using the law of conditional probability, we have for $k \ge 2$

$$(4.1)\qquad \begin{aligned} p_{k,t} &= \left(\sum_{n\in M_k} \bar{\alpha}(n)^t\right)^{-1} \sum_{n\in M_k}{}' \bar{\alpha}(n)^t \le \left(\sum_{p\in M_k} \bar{\alpha}(p)^t\right)^{-1} \sum_{n\in M_k}{}' \bar{\alpha}(n)^t \\ &= (\pi(2^k)-\pi(2^{k-1}))^{-1} \sum_{n\in M_k}{}' \bar{\alpha}(n)^t. \end{aligned}$$

Thus, to get an upper estimate for $p_{k,t}$, it will suffice to find an upper estimate for the final sum in (4.1) and a lower estimate for $\pi(2^k)-\pi(2^{k-1})$.

Proposition 1. *Let* $c = 8(\pi^2 - 6)/3$. *For any integers* k, M, t *with* $3 \le M \le 2\sqrt{k-1} - 1$ *and* $t \ge 1$, *we have*

$$\sum_{n \in M_k}{}' \bar{\alpha}(n)^t \le 2^{k-2-Mt} + c \cdot 2^{k-2+t} \sum_{j=2}^{M} \sum_{\substack{m=j \\ m \ne 2}}^{M} 2^{m(1-t)-j-(k-1)/j}.$$

Proof. First note that the hypothesis implies $k \ge 5$, so we have $C_1 \cap M_k = C_2 \cap M_k = \varnothing$. Thus,

$$\begin{aligned} \sum_{n \in M_k}{}' \bar{\alpha}(n)^t &= \sum_{m=3}^{\infty} \sum_{n \in M_k \cap C_m \setminus C_{m-1}} \bar{\alpha}(n)^t \le \sum_{m=3}^{\infty} \sum_{n \in M_k \cap C_m \setminus C_{m-1}} \alpha(n)^t \\ &\le \sum_{m=3}^{\infty} 2^{-(m-1)t} |M_k \cap C_m \setminus C_{m-1}| \qquad (4.2) \\ &\le 2^{-Mt} |M_k \setminus C_M| + \sum_{m=3}^{M} 2^{-(m-1)t} |M_k \cap C_m|. \end{aligned}$$

From Theorem 1 and the above estimate we have

$$\begin{aligned} \sum_{n \in M_k}{}' \bar{\alpha}(n)^t &\le 2^{k-2-Mt} + c \cdot 2^{k-2} \sum_{m=3}^{M} \sum_{j=2}^{m} 2^{-(m-1)t+m-j-(k-1)/j} \\ &= 2^{k-2-Mt} + c \cdot 2^{k-2+t} \sum_{j=2}^{M} \sum_{\substack{m=j \\ m \ne 2}}^{M} 2^{m(1-t)-j-(k-1)/j}, \end{aligned}$$

which proves the proposition. □

Proposition 2. *For* k *an integer at least* 21, *we have*

$$\pi(2^k) - \pi(2^{k-1}) > (0.71867)\frac{2^k}{k}.$$

Proof. Let $\theta(x) = \sum_{p \le x} \ln p$. We have

$$\pi(x) - \pi\left(\frac{x}{2}\right) \ge \frac{1}{\ln x} \sum_{x/2 < p \le x} \ln p = \frac{1}{\ln x}\left(\theta(x) - \theta\left(\frac{x}{2}\right)\right). \qquad (4.3)$$

From [8] we have

$$\begin{aligned} \theta(x) &< 1.0011x \quad \text{for } x > 0, \\ \theta(x) &> 0.9987x \quad \text{for } x \ge 1155901. \end{aligned}$$

Thus, for $x \ge 1155901$, we have

$$\theta(x) - \theta\left(\frac{x}{2}\right) > 0.9987x - \frac{1}{2}(1.0011)x = 0.49815x.$$

Thus, from (4.3) we have

$$\pi(x) - \pi\left(\frac{x}{2}\right) > 0.49815\frac{x}{\ln x}$$

for $x \ge 1155901$. In particular, if $k \ge 21$, then

$$\pi(2^k) - \pi(2^{k-1}) > 0.49815\frac{2^k}{k \ln 2} > 0.71867\frac{2^k}{k},$$

which proves the proposition. □

TABLE 1. Lower bounds for $-\lg p_{k,t}$

$k\backslash t$	1	2	3	4	5	6	7	8	9	10
100	5	14	20	25	29	33	36	39	41	44
150	8	20	28	34	39	43	47	51	54	57
200	11	25	34	41	47	52	57	61	65	69
250	14	29	39	47	54	60	65	70	75	79
300	16	33	44	53	60	67	73	78	83	88
350	19	37	48	58	66	73	80	86	91	97
400	21	40	53	63	72	80	87	93	99	105
450	23	43	57	68	77	85	93	100	106	112
500	25	46	61	72	82	91	99	106	113	119
550	27	49	64	76	87	96	104	112	119	126
600	29	52	68	80	91	101	110	118	125	132

The numbers in Table 1 were computed from (4.1), Proposition 1, and Proposition 2, using the optimal value of the free parameter M. If j is the entry corresponding to k and t in Table 1, then we are asserting that $p_{k,t} \le 2^{-j}$.

5. GENERAL INEQUALITIES FOR $p_{k,t}$

It is the purpose of this section to obtain clean upper-bound inequalities for $p_{k,t}$ that are valid for all k or all large k. We begin with the following.

Theorem 2. *For $k \ge 2$ we have $p_{k,1} < k^2 4^{2-\sqrt{k}}$.*

Proof. From (4.1) we have for $k \ge 2$ that

$$p_{k,1} \le (\pi(2^k) - \pi(2^{k-1}))^{-1} \sum_{n \in M_k}{}' \bar{\alpha}(n). \tag{5.1}$$

Using $\sum_{m=j}^{M} 2^{m(1-t)} = M + 1 - j$ for $t = 1$, we obtain from Proposition 1 that

$$\sum_{n \in M_k}{}' \bar{\alpha}(n) \le 2^{k-2-M} + c \cdot 2^{k-1} \sum_{j=2}^{M} (M + 1 - j) 2^{-j-(k-1)/j} \tag{5.2}$$

for any integer M with $3 \le M \le 2\sqrt{k-1} - 1$. Note that for any j we have

$$j + \frac{k-1}{j} \ge 2\sqrt{k-1}.$$

Assume $k \ge 5$ and let $M = [2\sqrt{k-1} - 1]$. We get from the above that

$$\begin{aligned} \sum_{n \in M_k}{}' \bar{\alpha}(n) &\le 2^{k-2-M} + c \cdot 2^{k-1-2\sqrt{k-1}} \sum_{j=2}^{M} (M + 1 - j) \\ &= 2^{k-2-M} + cM(M-1) 2^{k-2-2\sqrt{k-1}} \\ &< 2^{k-2\sqrt{k-1}} + \tfrac{1}{4} c (2\sqrt{k-1} - 1)(2\sqrt{k-1} - 2) 2^{k-2\sqrt{k-1}} \\ &< ck 2^{k-2\sqrt{k-1}}. \end{aligned} \tag{5.3}$$

Using $\sqrt{k} < \sqrt{k-1} + 1/(2\sqrt{k-1})$, we have for $k \ge 2$ that

$$2^{-2\sqrt{k-1}} < 2^{-2\sqrt{k}+1/\sqrt{k-1}}. \tag{5.4}$$

Suppose now that $k \ge 42$. Then from (5.3) and (5.4) we have

$$\sum_{n\in M_k}{}' \bar{\alpha}(n) < ck2^{1/\sqrt{41}}2^{k-2\sqrt{k}}.$$

Using this and Proposition 2 in (5.1), we have for $k \ge 42$ that

$$p_{k,1} < \frac{2^{1/\sqrt{41}}c}{0.71867}k^2 2^{-2\sqrt{k}} < k^2 4^{2-\sqrt{k}},$$

which proves the theorem for $k \ge 42$. But $k^2 4^{2-\sqrt{k}} > 1$ for $k \le 63$, so the theorem is trivially true for $k \le 63$. □

Remark. With a little more careful estimation of the sum on the right side of (5.2) we can show $p_{k,1} = O(k^{3/2}4^{-\sqrt{k}})$ with an explicit O-constant.

Theorem 3. *For k, t integers with $k \ge 21$, $3 \le t \le k/9$ or $k \ge 88$, $t = 2$, we have*

$$p_{k,t} < k^{3/2}\frac{2^t}{\sqrt{t}}4^{2-\sqrt{tk}}.$$

Proof. Assume $k \ge 9$, $t \ge 2$. Using $\sum_{m=j}^{M} 2^{m(1-t)} < 2^{j(1-t)}/(1-2^{1-t})$, we obtain from Proposition 1 that

$$\sum_{n\in M_k}{}' \bar{\alpha}(n)^t \le 2^{k-2-Mt} + c\frac{2^{k-2+t}}{1-2^{1-t}}\sum_{j=2}^{M} 2^{-jt-(k-1)/j} \tag{5.5}$$

for any integer M with $3 \le M \le 2\sqrt{k-1} - 1$. We shall use the inequality

$$jt + \frac{k-1}{j} \ge 2\sqrt{t(k-1)} \quad \text{for all } j > 0.$$

Further, we shall choose $M = \lceil 2\sqrt{(k-1)/t}\rceil$ in (5.5). Thus, to have $M \ge 3$, we must restrict t to $t \le k-1$. Further, for $k \ge 9$ we have

$$M = \left\lceil 2\sqrt{(k-1)/t}\right\rceil \le \left\lceil 2\sqrt{(k-1)/2}\right\rceil \le 2\sqrt{k-1} - 1,$$

so that (5.5) is applicable. Thus, from (5.5) we get

$$\begin{aligned}\sum_{n\in M_k}{}' \bar{\alpha}(n)^t &\le 2^{k-2-Mt} + c\frac{2^{k-2+t}}{1-2^{1-t}}(M-1)2^{-2\sqrt{t(k-1)}} \\ &< 2^{k-2-2\sqrt{t(k-1)}}\left(1 + 2c\sqrt{\frac{k}{t}}\frac{2^t}{1-2^{1-t}}\right).\end{aligned}$$

Now for $k \ge 9$ and $t \ge 2$ we have

$$2c\sqrt{\frac{k}{t}}\frac{2^t}{1-2^{1-t}} \ge 2c\sqrt{\frac{9}{2}}\frac{2^2}{1-2^{-1}} > 350.$$

Thus,

$$\sum_{n\in M_k}{}' \bar{\alpha}(n)^t < 2^{k-2-2\sqrt{t(k-1)}} \frac{351}{350} 2c\sqrt{\frac{k}{t}} \frac{2^t}{1-2^{1-t}}. \tag{5.6}$$

Note that $2^{-2\sqrt{t(k-1)}} < 2^{-2\sqrt{tk}} 2^{\sqrt{t/(k-1)}}$. For $3 \le t \le k/9$, we have

$$\frac{2^{\sqrt{t/(k-1)}}}{1-2^{1-t}} \le \frac{4}{3} 2^{\sqrt{3/26}} < 1.7.$$

For $t = 2$ and $k \ge 88$, we have

$$\frac{2^{\sqrt{t/(k-1)}}}{1-2^{1-t}} = 2^{1+\sqrt{2/(k-1)}} < 2.222.$$

Putting these estimates in (5.6), we get

$$\sum_{n\in M_k}{}' \bar{\alpha}(n)^t < 2^{k-2-2\sqrt{tk}} \frac{351}{350} 4.444c\sqrt{\frac{k}{t}} 2^t$$

for $3 \le t \le (k-1)/2$, $k \ge 9$ and for $t = 2$, $k \ge 88$.

Now using (4.1) and Proposition 2, we get

$$p_{k,t} < \frac{351}{350} \frac{1.111}{0.71867} c k^{3/2} \frac{2^t}{\sqrt{t}} 4^{-\sqrt{tk}}$$

for $3 \le t \le k/9$, $k \ge 21$ and for $t = 2$, $k \ge 88$. Thus, for these values of k, t we have

$$p_{k,t} < k^{3/2} \frac{2^t}{\sqrt{t}} 4^{2-\sqrt{tk}},$$

which proves the theorem. □

Remark. It should be clear from the proof that we have a somewhat stronger, but less clean, inequality that is valid in a wider range for k, t.

We can also use the above methods to estimate $p_{k,t}$ for very large values of t. However, when we do many probable prime tests it is more important to have improved estimates on the distribution of the worst-case numbers, namely the members of C_3. We do this in the next section.

6. The worst-case numbers

In this section we classify the members of C_3, get an improved estimate for $|C_3 \cap M_k|$, and use this to get an estimate for $p_{k,t}$ when t is large.

Theorem 4. *The following numbers comprise* C_3:

(i) $(m+1)(2m+1)$, *where* $m+1$, $2m+1$ *are odd primes,*
(ii) $(m+1)(3m+1)$, *where* $m+1$, $3m+1$ *are primes that are* $3 \bmod 4$,
(iii) $p_1p_2p_3$, *where* p_1, p_2, p_3 *are primes,* $p_1p_2p_3$ *is a Carmichael number, and there is some integer* s *with* $2^s \| p_i - 1$ *for* $i = 1, 2, 3$,
(iv) 9, 25, 49.

Proof. Suppose $m+1$, $2m+1$ are prime and $2^\nu \| m$. If $n=(m+1)(2m+1)$, then (2.2) implies $S(n)=(1+\frac{4^\nu-1}{3})4^{-\nu}m^2$, so that

$$\alpha(n)=\frac{S(n)}{\varphi(n)}=\frac{1+(4^\nu-1)/3}{2\cdot 4^\nu}>\frac{1}{6}.$$

Similarly, if n is in class (ii), then $\nu=1$ and

$$\alpha(n)=\frac{1+(4^\nu-1)/3}{3\cdot 4^\nu}=\frac{1}{6}. \tag{6.1}$$

If n is in class (iii), then

$$\alpha(n)=\frac{1+(8^s-1)/7}{8^s}>\frac{1}{7}.$$

Finally, $\alpha(9)=1/3$, $\alpha(25)=1/5$, $\alpha(49)=1/7$.

It remains to show that C_3 has no other elements. From (2.2) and (2.3) we have

$$S(n)\le 2^{1+(\nu(n)-1)\omega(n)}\prod_{p|n}(p-1\,,u).$$

Say the distinct primes in n are $p_1, p_2, \ldots, p_{\omega(n)}$ and $p_i-1=2^{s_i}u_i$ for each i, where u_i is odd. Then

$$\begin{aligned}\frac{\varphi(n)}{S(n)}&\ge\frac{\prod_{i=1}^{\omega(n)}2^{s_i}u_i}{2^{1+(\nu(n)-1)\omega(n)}\prod_{i=1}^{\omega(n)}(p_i-1\,,u)}\\&=2^{\omega(n)-1}2^{\sum_{i=1}^{\omega(n)}(s_i-\nu(n))}\prod_{i=1}^{\omega(n)}\frac{u_i}{(p_i-1\,,u)}.\end{aligned}\tag{6.2}$$

Thus, a necessary condition for $n\in C_3$ is that the integer on the right of (6.2) is less than 8.

We thus immediately see that $\omega(n)\le 3$. Suppose $\omega(n)=3$. Then, if $n\in C_3$, we see from (6.2) that $s_i=\nu(n)$ for $i=1,2,3$ and $u_i=(p_i-1\,,u)$ for $i=1,2,3$. Thus n is in class (iii).

Suppose $\omega(n)=2$. Suppose $s_1=s_2=\nu(n)$. Since n, having only two distinct prime factors, cannot be a Carmichael number, the final product on the right of (6.2) must be at least 3. Thus, if $n\in C_3$, this product is 3 and n is in class (ii) (and from (6.1) we see that $\nu(n)=1$). If $s_1\ne s_2$ and $n\in C_3$, we must have $|s_1-s_2|=1$, say $s_1=\nu(n)$, $s_2=s_1+1$. We also must have the final product in (6.2) equal to 1, so n is in class (i).

Finally, if $n=p^a$ with p prime, then $\alpha(n)=1/p^{a-1}$, so that $n\in C_3$ implies n is in class (iv). □

Theorem 5. *Let $N(x)$ denote the number of Carmichael numbers up to x with exactly three prime factors. Then for all $x\ge 1$ we have*

$$N(x)\le\tfrac{1}{4}x^{1/2}(\ln x)^{11/4}.$$

Proof. A Carmichael number n with three prime factors can be written as pqr with $2<p<q<r$ primes and $[p-1\,,q-1\,,r-1]\mid pqr-1$. Let $g=(p-1\,,q-1\,,r-1)$, and let a, b, c be such that

$$p-1=ga\,,\qquad q-1=gb\,,\qquad r-1=gc.$$

Thus, $a < b < c$, $(a, b, c) = 1$, and

$$a \mid b + c + gbc, \qquad b \mid a + c + gac, \qquad c \mid a + b + gab. \tag{6.3}$$

From (6.3) it easily follows that a, b, c are pairwise coprime. For example, the first relation in (6.3) implies that $(a, b) \mid c$, so that $(a, b, c) = 1$ implies $(a, b) = 1$.

Thus, the relations in (6.3) imply that if a, b, c are given, then g is determined $\bmod abc$.

We now count the number N of quadruples g, a, b, c which satisfy the above conditions and $g^3abc \le x$. Note that $N(x) \le N$. We write $N = N_1 + N_2 + N_3$, where in N_1 we count those quadruples with $g > abc$, in N_2 we count those quadruples with $G < g \le abc$, and in N_3 we count those quadruples with $g \le G$ and $g \le abc$. Here G is a parameter we shall choose later.

If a, b, c are given, then the number of g with $g^3abc \le x$, g in a particular residue class $\bmod abc$, and $g > abc$ is at most $[(x/abc)^{1/3}/abc] \le x^{1/3}/(abc)^{4/3}$. Thus,

$$N_1 \le \sum_{a<b<c} \frac{x^{1/3}}{(abc)^{4/3}} < \frac{1}{6}\zeta\left(\frac{4}{3}\right)^3 x^{1/3}, \tag{6.4}$$

where ζ denotes the Riemann zeta function.

To estimate N_2 note that for each coprime triple a, b, c there is at most one g that satisfies (6.3) and $g \le abc$. Further, if $g > G$ and $g^3abc \le x$, then $abc \le x/G^3$. Thus, N_2 is at most the number of triples a, b, c with $a < b < c$ and $abc \le x/G^3$. Thus,

$$\begin{aligned} N_2 &\le \sum_{1\le a<x^{1/3}/G} \; \sum_{a<b<(x/aG^3)^{1/2}} \; \sum_{b<c\le x/abG^3} 1 \\ &< \sum_a \sum_b \frac{x}{abG^3} < \sum_a \frac{x}{aG^3} \ln\left(\left(\frac{x}{aG^3}\right)^{1/2}\right) \\ &< \frac{x}{2G^3}\left(1 + \ln\left(\frac{x^{1/3}}{G}\right)\right)\ln\left(\frac{x}{G^3}\right) < \frac{x}{6G^3}(\ln x)^2 \end{aligned} \tag{6.5}$$

for $G > e$.

Now we estimate N_3. From (6.3), for g, a, b, c given, there is an integer h with

$$c = \frac{a + b + gab}{h} = \frac{(ga+1)b + a}{h} \tag{6.6}$$

so that

$$h \mid (ga+1)b + a \quad \text{and} \quad h \le ga. \tag{6.7}$$

Note that

$$a + c + gac = (ga+1)c + a = \frac{(ga+1)^2 b + (ga+1)a}{h} + a,$$

so that (6.3) implies $b \mid (ga+1)a + ha$. Since $(b, a) = 1$, we have

$$b \mid ga + 1 + h. \tag{6.8}$$

Also note that

$$b+c+gbc=(gb+1)c+b=(gb+1)\frac{(ga+1)b+a}{h}+b,$$

so that (6.3) implies $a \mid (gb+1)b+hb$, and since $(a, b)=1$, we have

$$a \mid gb+1+h. \tag{6.9}$$

Let j be such that

$$b=\frac{ga+1+h}{j}, \tag{6.10}$$

so that $a<b$ and $h \le ga$ imply $j \le 2g$. We have

$$gb+1+h=g\frac{ga+1+h}{j}+1+h,$$

so that (6.9) implies that $a \mid g+gh+j+jh$; that is,

$$(g+j)(1+h) \equiv 0 \mod a. \tag{6.11}$$

Suppose we are given g, a, j. Let $d=(a, j(g+j))$. Note that (6.10) and (6.11) imply

$$1+h \equiv -ga \mod j, \qquad 1+h \equiv 0 \mod \frac{a}{(a, g+j)}.$$

Thus,

$$1+h \equiv -ga \mod \frac{ja}{d}. \tag{6.12}$$

Indeed,

$$\left[j, \frac{a}{(a, g+j)}\right]=\frac{ja}{(a, g+j)(j, a/(a, g+j))}=\frac{ja}{(j(a, g+j), a)}=\frac{ja}{d}.$$

Now the number of positive integers $h \le ga$ which satisfy (6.12) is at most

$$\left\lceil \frac{ga}{ja/d} \right\rceil=\left\lceil \frac{gd}{j} \right\rceil \le \frac{2gd}{j}, \tag{6.13}$$

since $j \le 2g$ implies $gd/j \ge d/2 \ge 1/2$. Further, if g, a, j, h are given, then b, c are also specified, via (6.6) and (6.10). Thus, by (6.13),

$$\begin{aligned} N_3 &\le \sum_{g \le G} \sum_{j \le 2g} \sum_{a \le x^{1/3}/g} \frac{2g(a, j(j+g))}{j} \\ &\le \sum_{g \le G} \sum_{j \le 2g} \sum_{d \mid j(j+g)} \frac{2gd}{j} \sum_{\substack{a \le x^{1/3}/g \\ d \mid a}} 1 \le 2x^{1/3} \sum_{g \le G} \sum_{j \le 2g} \sum_{d \mid j(j+g)} \frac{1}{j}. \end{aligned} \tag{6.14}$$

Next note that

$$\sum_{d \mid j(j+g)} 1=\tau(j(j+g)) \le \tau(j)\tau(j+g),$$

where $\tau(m)$ denotes the number of divisors of m. Thus, from (6.14),

$$\begin{aligned} N_3 &\le 2x^{1/3} \sum_{g\le G} \sum_{j\le 2g} \frac{\tau(j)\tau(j+g)}{j} \\ &= 2x^{1/3} \sum_{j\le 2G} \frac{\tau(j)}{j} \sum_{j/2\le g\le G} \tau(j+g) \\ &\le 2x^{1/3} \left(\sum_{j\le 2G} \frac{\tau(j)}{j} \right) \left(\sum_{m\le 3G} \tau(m) \right). \end{aligned} \tag{6.15}$$

We have from Lemma 2.6 in [4] and its proof,

$$\sum_{m\le 3G} \tau(m) \le 3G(1+\ln(3G)), \qquad \sum_{j\le 2G} \frac{\tau(j)}{j} \le \frac{1}{2}(2+\ln(2G))^2.$$

Thus, from (6.15) we have

$$N_3 \le 3x^{1/3} G(1+\ln(3G))(2+\ln(2G))^2.$$

We now let $G = x^{1/6}/(\ln x)^{1/4}$. Assume $x > 10^{10}$. Then

$$1+\ln(3G) < \tfrac{1}{4}\ln x, \qquad 2+\ln(2G) < \tfrac{1}{4}\ln x,$$

so that $N_3 \le \frac{3}{64} x^{1/2} (\ln x)^{11/4}$.

We have from (6.5) that $N_2 < \frac{1}{6}x^{1/2}(\ln x)^{11/4}$. Thus, with (6.4), we have

$$N(x) \le N = N_1 + N_2 + N_3 \le \tfrac{1}{4} x^{1/2} (\ln x)^{11/4} \tag{6.16}$$

for $x > 10^{10}$. (We use $\zeta(4/3) < 1+\int_1^\infty t^{-4/3}\,dt = 4$ and $4^3/6 < \frac{1}{30}x^{1/6}(\ln x)^{11/4}$ for $x > 10^{10}$.) Finally, we note that from the table of Carmichael numbers associated with [6], the inequality of the theorem holds for all x in the remaining range $1 \le x \le 10^{10}$. □

Corollary. *For $k \ge 2$ we have $|C_3 \cap M_k| < \frac{1}{10} k^{11/4} 2^{k/2}$.*

Proof. We consider the four classes of members of C_3 listed in Theorem 4. If $n = (m+1)(2m+1) \le x$ is in class (i), then $2m^2 \le x$. Using that m is even, we have at most $\sqrt{x/8}$ such $n \le x$. If $n = (m+1)(3m+1) \le x$ is in class (ii), then we similarly get at most $\sqrt{x/12}$ such $n \le x$.

Now consider $|C_3 \cap M_k|$ for $k \ge 7$. No member of class (iv) is in M_k. Using the above estimates with $x = 2^k$ and using Theorem 5, we have

$$\begin{aligned} |C_3 \cap M_k| &< \tfrac{1}{\sqrt{8}} 2^{k/2} + \tfrac{1}{\sqrt{12}} 2^{k/2} + \tfrac{1}{4}(\ln 2)^{11/4} k^{11/4} 2^{k/2} \\ &< (0.354 + 0.289 + 0.0913 k^{11/4}) 2^{k/2} < \tfrac{1}{10} k^{11/4} 2^{k/2}, \end{aligned}$$

which proves the corollary for $k \ge 7$. For the remaining values of k it suffices to note that the upper bound in the corollary exceeds $2^{k-2} = |M_k|$. □

We remark that the prime k-tuples conjecture in analytic number theory implies that the number of members of $C_3 \cap M_k$ which are in either of the first two classes of Theorem 4 exceeds $c' k^{-2} 2^{k/2}$ for some positive constant c'. Thus, but for a factor that is $k^{O(1)}$, the above corollary is probably best possible.

The following result complements Theorems 2 and 3.

Theorem 6. *For integers k, t with $k \geq 21$ and $t \geq k/9$ we have*

$$p_{k,t} < \tfrac{7}{20}k2^{-5t} + \tfrac{1}{7}k^{15/4}2^{-k/2-2t} + 12k2^{-k/4-3t}.$$

Proof. By taking $M = 5$ in (4.2), we have

$$\sum_{n \in M_k}{}' \bar{\alpha}(n)^t \leq 2^{-5t}|M_k| + 2^{-2t}|M_k \cap C_3| + 2^{-3t}|M_k \cap C_4| + 2^{-4t}|M_k \cap C_5|.$$

We use Theorem 1 and the corollary to Theorem 5 to get

$$\begin{aligned}\sum_{n \in M_k}{}' \bar{\alpha}(n)^t \leq\ & 2^{k-2-5t} + \tfrac{1}{10}k^{11/4}2^{k/2-2t} \\ & + c2^{k-2-3t}(2^{2-(k-1)/2} + 2^{1-(k-1)/3} + 2^{-(k-1)/4}) \\ & + c2^{k-2-4t}(2^{3-(k-1)/2} + 2^{2-(k-1)/3} + 2^{1-(k-1)/4} + 2^{-(k-1)/5}),\end{aligned}$$

where $c = 8(\pi^2 - 6)/3$. Using $k \geq 21$, we then get from this estimate that

$$\begin{aligned}\sum_{n \in M_k}{}' \bar{\alpha}(n)^t \leq\ & 2^{k-2-5t} + \tfrac{1}{10}k^{11/4}2^{k/2-t} + 1.7c2^{k-2-3t-(k-1)/4} \\ & + 2.7c2^{k-2-4t-(k-1)/5}.\end{aligned}$$

Now using (4.1) and Proposition 2, we have

$$\begin{aligned}p_{k,t} <\ & (0.35)k2^{-5t} + (0.1392)k^{15/4}2^{-k/2-2t} \\ & + (7.26)k2^{-k/4-3t} + (11.2)k2^{-k/5-4t}.\end{aligned} \tag{6.17}$$

For $t \geq k/9$ and $k \geq 21$ the last term above is less than $(4.61)k2^{-k/4-3t}$, which, when put in (6.17), gives the theorem. □

Corollary. *For integers t, k with $t \geq k/4$ and $k \geq 21$ we have $p_{k,t} < \frac{1}{7}k^{15/4}2^{-k/2-2t}$.*

Proof. This result follows immediately from (6.17). □

7. Improved numerical results

In this section we show how the numerical estimates in [4] can be used together with the methods in this paper to get numerical upper estimates for $p_{k,t}$ that are sometimes better than our results above in §4.

In [4], the ratio

$$P(x) = \sum_{\substack{n \leq x \\ n \text{ odd}}}{}' (F(n) - 2) \Bigg/ \sum_{\substack{1 < n \leq x \\ n \text{ odd}}} (F(n) - 2)$$

is estimated from above, where the prime continues to indicate the sum is restricted to composite numbers. Here, $F(n)$ is the number of residues a mod n with $a^{n-1} \equiv 1 \bmod n$.

It is further shown in [4] that

$$\sum_{\substack{1<n\leq x\\ n\ \text{odd}}} (F(n)-2) \geq \frac{x^2}{2(2+\ln x)}$$

for all $x \geq 37$. The argument in [4] proceeds to majorize $P(x)$ by instead majorizing the function

$$\widetilde{P}(x) := \frac{2(2+\ln x)}{x^2} \sum_{\substack{n\leq x\\ n\ \text{odd}}}{}' F(n).$$

Thus, the estimates in [4] actually give upper bounds for the function $\widetilde{P}(x)$. We now show a connection between $\widetilde{P}(2^k)$ and the quantities estimated in Proposition 1.

Proposition 3. *For* $k \geq 2$ *we have*

$$\sum_{n\in M_k}{}' \bar{\alpha}(n) \leq \frac{2^{k-1}}{2+k\ln 2}\widetilde{P}(2^k) + \frac{k}{4}.$$

Moreover, if k, M, t *are integers with* $3 \leq M \leq 2\sqrt{k-1}-1$ *and* $t \geq 2$, *we have*

$$\sum_{n\in M_k}{}' \bar{\alpha}(n)^t \leq 2^{-M(t-1)} \sum_{n\in M_k}{}' \bar{\alpha}(n) + c\frac{2^{k-2+t}}{1-2^{1-t}} \sum_{j=2}^{M} 2^{-jt-(k-1)/j},$$

where $c = 8(\pi^2-6)/3$.

Proof. The second assertion follows immediately from the proofs of Proposition 1 and (5.5), the only difference being the estimation of

$$\sum_{m=M+1}^{\infty} \sum_{n\in M_k\cap C_m\setminus C_{m-1}} \bar{\alpha}(n)^t = \sum_{n\in M_k\setminus C_M}{}' \bar{\alpha}(n)^t.$$

In Proposition 1 we majorized this expression by $2^{-Mt}|M_k\setminus C_M| \leq 2^{k-2-Mt}$. Now we argue that this expression is at most

$$\sum_{n\in M_k\setminus C_M}{}' \alpha(n)^{t-1}\bar{\alpha}(n) \leq 2^{-M(t-1)} \sum_{n\in M_k\setminus C_M}{}' \bar{\alpha}(n) \leq 2^{-M(t-1)} \sum_{n\in M_k}{}' \bar{\alpha}(n).$$

It remains to show the first inequality in the proposition. We use the fact $S(n) \leq F(n)/2$ if n is odd and divisible by at least two distinct primes. This follows easily from the first inequality in Lemma 1 and the formula (see [1, 5])

$$F(n) = \prod_{p|n}(p-1, n-1).$$

Note that if $n = p^a$, where p is an odd prime, then $S(n) = F(n) = p-1$.

Thus,

$$\begin{aligned}
\sum_{n\in M_k}{}' \bar{\alpha}(n) &= \sum_{n\in M_k}{}' \frac{S(n)}{n-1} \le 2^{1-k} \sum_{n\in M_k}{}' S(n) \\
&\le 2^{-k} \sum_{\substack{n\in M_k \\ \omega(n)>1}}{}' F(n) + 2^{1-k} \sum_{\substack{p^a\in M_k \\ a>1}} S(p^a) \\
&\le 2^{-k} \sum_{\substack{n<2^k \\ n \text{ odd}}}{}' F(n) + 2^{-k} \sum_{\substack{p^a<2^k \\ p>2,\, a>1}} S(p^a) \\
&= 2^{-k} \frac{2^{2k}}{2(2+\ln 2^k)} \widetilde{P}(2^k) + 2^{-k} \sum_{\substack{p^a<2^k \\ p>2,\, a>1}} (p-1) \\
&\le \frac{2^{k-1}}{2+\ln 2^k} \widetilde{P}(2^k) + 2^{-k} k \sum_{2<p<2^{k/2}} (p-1).
\end{aligned}$$

Using

$$\sum_{2<p<2^{k/2}} (p-1) \le 2 \sum_{m<(2^{k/2}-1)/2} m < \frac{2^{k/2}+1}{2} \cdot \frac{2^{k/2}-1}{2} < 2^{k-2},$$

we thus have

$$\sum_{n\in M_k}{}' \bar{\alpha}(n) \le \frac{2^{k-1}}{2+k\ln 2} \widetilde{P}(2^k) + \frac{k}{4}.$$

This completes the proof of Proposition 3. □

It remains now to use (4.1) and Propositions 2 and 3, together with the estimates in [4], to get numerical estimates for $p_{k,t}$. There is a difficulty, however, with using the table from [4] since it gives estimates for $\widetilde{P}(x)$ for x equal to various powers of 10, while in Proposition 3, we need to know an estimate when x is a power of 2. Suppose $2^k \le x$. From the definition of $\widetilde{P}$ we have

$$\widetilde{P}(2^k) \le \frac{2+\ln 2^k}{2+\ln x} \cdot \frac{x^2}{2^{2k}} \widetilde{P}(x) \le \frac{x^2}{2^{2k}} \widetilde{P}(x).$$

Thus, if we have an estimate for $\widetilde{P}(x)$, we can use this to get an estimate for $\widetilde{P}(2^k)$. However, this interpolation formula is too crude. So instead of using the table from [4] and interpolating, we recompute $\widetilde{P}(x)$ using the formulas from [4] for x being various powers of 2 and use these estimates in Proposition 3. Table 2 gives numerical upper bounds for various $p_{k,t}$ using these ideas. If j is the entry in Table 2 corresponding to k, t, then $p_{k,t} \le 2^{-j}$. An entry is italicized if it is an improvement on the corresponding entry in Table 1.

TABLE 2. Lower bounds for $-\lg p_{k,t}$: combined method

$k\backslash t$	1	2	3	4	5	6	7	8	9	10
100	5	14	20	25	29	33	36	39	41	44
150	8	20	28	34	39	43	47	51	54	57
200	11	25	34	41	47	52	57	61	65	69
250	14	29	39	47	54	60	65	70	75	79
300	*19*	33	44	53	60	67	73	78	83	88
350	*28*	*38*	48	58	66	73	80	86	91	97
400	*37*	*46*	*55*	63	72	80	87	93	99	105
450	*46*	*54*	*62*	*70*	*78*	85	93	100	106	112
500	*56*	*63*	*70*	*78*	*85*	*92*	99	106	113	119
550	*65*	*72*	*79*	*86*	*93*	*100*	*107*	*113*	119	126
600	*75*	*82*	*88*	*95*	*102*	*108*	*115*	*121*	*127*	*133*

BIBLIOGRAPHY

1. R. Baillie and S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1391–1417.
2. P. Beuchemin, G. Brassard, C. Crépeau, C. Goutier, and C. Pomerance, *The generation of random numbers that are probably prime*, J. Cryptology **1** (1988), 53–64.
3. P. Erdős and C. Pomerance, *On the number of false witnesses for a composite number*, Math. Comp. **46** (1986), 259–279.
4. S. H. Kim and C. Pomerance, *The probability that a random probable prime is composite*, Math. Comp. **53** (1989), 721–741.
5. L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoret. Comput. Sci. **12** (1980), 97–108.
6. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.
7. M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), 128–138.
8. L. Schoenfeld, *Sharper bounds for the Chebyshev functions* $\theta(x)$ *and* $\psi(x)$. II, Math. Comp. **30** (1976), 337–360; Corrigendum, op cit, 900.

(I. Damgård and P. Landrock) MATEMATISK INSTITUT, NY MUNKEGADE, DK 8000 ÅRHUS C, DENMARK

E-mail address, I. Damgård: ivan@daimi.aau.dk

E-mail address, P. Landrock: Landrock@daimi.aau.dk

(C. Pomerance) DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF GEORGIA, ATHENS, GEORGIA 30602

E-mail address: carl@joe.math.uga.edu