Primality Testing with Fewer Random Bits[1]

René Peralta[2]
Computer Science Department; University of Wisconsin—Milwaukee
P. O. Box 784; Milwaukee, WI 53201; USA

Victor Shoup
Department of Computer Science; University of Toronto; Toronto, Ontario M5S 1A4; Canada

Abstract

In the usual formulations of the Miller-Rabin and Solovay-Strassen primality testing algorithms, to test a number n for primality, the algorithm chooses "candidates" $x_1, x_2, \ldots, x_k$ uniformly and independently at random from $\mathbf{Z}_n$, and tests if any are a "witness" to the compositeness of n. For either algorithm, the probability that it errs is at most 2^{-k}.

In this paper, we study the error probabilities of these algorithms when the candidates are instead chosen as $x, x+1, \ldots, x+k-1$, where x is chosen uniformly at random from $\mathbf{Z}_n$. We prove that for $k = \lceil \frac{1}{2} \log_2 n \rceil$, the error probability of the Miller-Rabin test is no more than $n^{-1/2+o(1)}$, which improves on the $n^{-1/4+o(1)}$ bound previously obtained by Bach. We prove similar bounds for the Solovay-Strassen test, but they are not quite as strong; in particular, we only obtain a bound of $n^{-1/2+o(1)}$ if the number of distinct prime factors of n is $o(\log n / \operatorname{loglog} n)$.

1. Introduction

Main Results

Two very well-known primality tests are the *Miller-Rabin* test (Miller 1976, Rabin 1980) and the *Solovay-Strassen* test (Solovay & Strassen 1977). Both of these tests have the following structure. For each (odd) positive integer n, a set $W(n) \subset \mathbf{Z}_n$ is defined with the property that if n is composite, then $\#W(n) \geq n/2$, and if n is prime, then $W(n) = \emptyset$. For composite n, the set $W(n)$ is called the set of *witnesses* to the compositeness of n, and the complementary set $L(n) = \mathbf{Z}_n \backslash W(n)$ is called the set of *liars*.

For both of these tests, the problem of testing whether a given $x \in \mathbf{Z}_n$ is in $W(n)$ has an efficient (deterministic, polynomial-time) algorithm.

To actually use these tests, a probabilistic procedure such as the following is usually employed. Suppose n is to be tested for primality. Choose $x_1, \ldots, x_k$ independently and uniformly at random from $\mathbf{Z}_n$. If any of these x_i's is in $W(n)$, the algorithm says "composite"; otherwise, the algorithm says "prime".

If n is prime, then this probabilistic procedure will say "prime" with certainty. However, if n is composite, the algorithm could erroneously say "prime" with some small probability, bounded by 2^{-k}.

[1]Appeared in *Computational Complexity* 3, pp. 355–367, 1993.
[2]Supported in part by NSF grant CCR-9207204

Our goal in this paper is to analyze the performance of the Miller-Rabin and Solovay-Strassen tests when the above random sequence $x_1, \ldots, x_k$ is replaced by the sequence

$$x, x+1, x+2, \ldots, x+k-1,$$

where the starting value x is chosen at random from $\mathbf{Z}_n$.

For the Miller-Rabin test, we use the notation $W_{MR}(n)$ and $L_{MR}(n)$; likewise, for the Solovay-Strassen test, we use the notation $W_{SS}(n)$ and $L_{SS}(n)$.

We can now state our main results. For the Miller-Rabin test, we obtain the following result.

Theorem 1.1. *Let n be an odd composite integer and let $k = \lceil \frac{1}{2} \log_2 n \rceil$. For a randomly chosen $x \in \mathbf{Z}_n$, the probability that $\{x, x+1, \ldots, x+k-1\} \subset L_{MR}(n)$ is bounded by*

$$n^{-1/2+o(1)}.$$

We do not obtain such a nice result for the Solovay-Strassen test. We can obtain the following probability bound that depends on the number $\omega(n)$ of distinct prime factors in n.

Theorem 1.2. *Let n be an odd composite integer and let $k = \lceil \frac{1}{2} \log_2 n \rceil$. For a randomly chosen $x \in \mathbf{Z}_n$, the probability that $\{x, x+1, \ldots, x+k-1\} \subset L_{SS}(n)$ is bounded by*

$$n^{-1/2+o(1)} \cdot (\log n)^{\omega(n)}.$$

In the worst-case, $\omega(n)$ may be asymptotic to $\log n / \operatorname{loglog} n$, in which case this bound is useless ($\log n$ denotes the natural logarithm). However, if $\omega(n) = o(\log n / \operatorname{loglog} n)$, then this bound becomes $n^{-1/2+o(1)}$.

We can obtain a uniform bound (independent of $\omega(n)$) by considering shorter sequences.

Theorem 1.3. *Let n be an odd composite integer and let $k = \left\lceil (\log n)^{\lambda} \right\rceil$, where $0 < \lambda < 1/2$ is any fixed constant. For a randomly chosen $x \in \mathbf{Z}_n$, the probability that $\{x, x+1, \ldots, x+k-1\} \subset L_{SS}(n)$ is bounded by*

$$2^{-(\log n)^{\lambda}} \cdot (1 + o(1)).$$

We can also obtain a uniform bound by considering much longer sequences. If we set $k = \lceil (\log n)^c \rceil$ for constant $c > 2$, then we obtain an error probability for the Solovay-Strassen test of

$$n^{-1/2+1/c+o(1)}.$$

Indeed, if n is divisible by a prime less than $(\log n)^c$, then the algorithm will fail to find a witness with probability $O((\log n)^c / n)$; otherwise, $\omega(n) \leq \log n / c \operatorname{loglog} n$ and the bound follows from Theorem 1.2.

Related Work

Bach (1991) examined the error probability of the Miller-Rabin test using the sequence

$$x, x+1, \ldots, x+k-1,$$

where $x \in \mathbf{Z}_n$ is chosen at random and $k = \lceil \frac{1}{2} \log_2 n \rceil$. Bach proved that the error probability is at most $n^{-1/4+o(1)}$ in this case.

Our Theorem 1.1 is a quantitative improvement of Bach's result, and the techniques we use are closely related to those used by Bach. However, the methods in Bach's paper do not appear to directly yield a similar result for the Solovay-Strassen test, and our results here appear to be the first of their kind in the literature.

Other related results include the work of Bach & Shoup (1990) on factoring polynomials over finite fields, and the work of Karloff & Raghavan (1988) on sorting.

One can view all of these results as solutions to special instances of the problem of "recycling random bits." Along these lines, we mention the general results of Cohen & Wigderson (1989) and Impagliazzo & Zuckermann (1989) which essentially state that the error probability of any probabilistic algorithm can be made exponentially small at the cost of only a constant factor increase in the number of random bits used.

While these general results on recycling random bits are very powerful, we point out that they do not subsume our results, as our algorithms are extremely simple in comparison, and moreover, our results show that the error probability of these primality tests can be significantly reduced without using *any* extra random bits.

2. Jacobi Symbol Sequences

The main tool from number-theory that we shall use is the following lemma concerning the Jacobi symbol.

Lemma 2.1. *Let n be an odd squarefree integer and let k be a positive integer. Let $\epsilon_j \in \{-1, +1\}$ for $0 \leq j < k$. Then for randomly chosen $x \in \mathbf{Z}_n$, the probability that*

$$\left(\frac{x+j}{n}\right) = \epsilon_j \quad (0 \leq j < k)$$

is at most

$$2^{-k} + n^{-1/2} \cdot (k-1)^{\omega(n)}.$$

In particular, if $k \geq \frac{1}{2}\log_2 n$, then this probability is at most

$$n^{-1/2}(\log_2 n)^{\omega(n)}.$$

Proof. Let Q be the probability in question. If $k \geq p$ for some prime p dividing n, then $Q = 0$, so we can assume that $k < p$ for all primes p dividing n.

We have

$$\begin{aligned} nQ &\leq 2^{-k} \sum_{x \bmod n} \prod_{j=0}^{k-1} (1 + \epsilon_j (x+j \mid n)) \\ &= 2^{-k} \sum_{x \bmod n} \sum_f \delta_f \left(\frac{f(x)}{n}\right), \end{aligned}$$

where the sum on f ranges over all 2^k polynomials $f(t)$ dividing $t(t+1)\cdots(t+k-1)$, and each δ_f is ± 1. Rearranging terms, expanding the Jacobi symbol in terms of Legendre symbols, and applying the Chinese Remainder Theorem, one finds that

$$nQ \leq 2^{-k} \sum_{f} \prod_{p|n} \left| \sum_{x \bmod p} \left(\frac{f(x)}{p} \right) \right|,$$

where the product is over all primes p dividing n.

The term corresponding to $f(t) = 1$ contributes $2^{-k}n$ to the right-hand side. For the terms corresponding to $f(t) \neq 1$, the polynomial $f(t)$ is squarefree modulo each prime p dividing n, and using well-known character sum estimates (see Lidl & Niederreiter 1983, Theorem 5.51), we can bound the contribution from all of these terms by

$$\prod_{p|n} (k-1)\sqrt{p} = (k-1)^{\omega(n)} n^{1/2}.$$

Therefore,

$$nQ \leq 2^{-k}n + (k-1)^{\omega(n)} n^{1/2},$$

and dividing through by n, the first statement of the lemma follows. The second statement follows from the first by a simple calculation. □

3. Analysis of the Miller-Rabin Test

In this section, we give a proof of Theorem 1.1.

For the reader's convenience, we state here the witness set for the Miller-Rabin test.

Let n be an odd number, and let $n - 1 = 2^h m$ where m is odd. Then $x \in \mathbf{Z}_n$ is in $W_{MR}(n)$ if $x \neq 0$ and one of the following conditions hold:

1. $x^{n-1} \not\equiv 1 \pmod{n}$.
2. There exists an ℓ, with $1 \leq \ell \leq h$, such that

   $$x^{n-1} \equiv x^{(n-1)/2} \equiv \cdots \equiv x^{(n-1)/2^{\ell-1}} \equiv 1 \pmod{n},$$

   and $x^{(n-1)/2^\ell} \not\equiv \pm 1 \pmod{n}$.

Suppose now that n is an odd composite number for which a Miller-Rabin witness is sought. Let k be as in Theorem 1.1. Let

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

be the prime factorization of n, and, as above, let

$$n - 1 = 2^h m \quad (m \text{ odd}).$$

For $1 \leq i \leq r$, let

$$p_i - 1 = 2^{h_i} m_i \quad (m_i \text{ odd}).$$

Let

$$h^* = \min\left(\{h_i : 1 \leq i \leq r\} \cup \{h\}\right).$$

Lemma 3.1. *If $x \in \mathbf{Z}_n$ is a nonzero liar for the Miller-Rabin test, then the following conditions hold.*

1. *For* $h^* \le \ell \le h$,

$$x^{2^\ell m} \equiv 1 \pmod{n}.$$

2.

$$x^{2^{h^*-1}m} \equiv \pm 1 \pmod{n}.$$

Proof. If $h^* = h$, then the lemma is clear from the definition of the Miller-Rabin test.

Now suppose that $h^* < h$, so that $h^* = h_{i_0}$ for some $i_0 \in \{1, \ldots, r\}$. Since $x^{2^h m} \equiv 1 \pmod{p_{i_0}^{e_{i_0}}}$, the m-th power map must annihilate the image of x in the Sylow q-group of $G = (\mathbf{Z}_{p_{i_0}^{e_{i_0}}})^*$ for all odd primes q dividing the order of G. Furthermore, for $h^* \le \ell \le h$, the 2^ℓ-th power map annihilates the Sylow 2-group of G. It therefore follows that $x^{2^\ell m} \equiv 1 \pmod{p_{i_0}^{e_{i_0}}}$ for $h^* \le \ell \le h$. As x is a Miller-Rabin liar, this same congruence must hold modulo n.

This proves the first assertion of the lemma. The second assertion follows from the first and the definition of the Miller-Rabin test. $\square$

Before continuing, we define three sets of indices $A, B, C \subset \{1, \ldots, r\}$:

$$\begin{aligned} A &= \{i : e_i > 1\}; \\ B &= \{i : e_i = 1 \text{ and } h_i > h^*\}; \\ C &= \{i : e_i = 1 \text{ and } h_i = h^*\}. \end{aligned}$$

We will also use the following notation: for a subset $S \subset \{1, \ldots, r\}$, define

$$n(S) = \prod_{i \in S} p_i^{e_i}.$$

Lemma 3.2. *Suppose that for* $x \in \mathbf{Z}_n$, $x, x+1, \ldots, x+k-1$ *are all nonzero liars for the Miller-Rabin test. Then the following conditions hold.*

MR-1:

$$\forall i \in A : x^{p_i - 1} \equiv 1 \pmod{p_i^{e_i}}.$$

MR-2:

$$\forall i \in B : (x + j \mid p_i) = 1 \quad (0 \le j < k).$$

MR-3: *(a)*

$$\forall i, i' \in C : (x + j \mid p_i) \cdot (x + j \mid p_{i'}) = 1 \quad (0 \le j < k).$$

(b) Moreover, if $A \cup B \neq \emptyset$, *then*

$$\forall i \in C : (x + j \mid p_i) \equiv (x + j)^{2^{h^*-1}m} \pmod{n(A \cup B)} \quad (0 \le j < k).$$

Proof. To prove MR-1, let $i \in A$. Then $x^{n-1} \equiv 1 \pmod{p_i^{e_i}}$. Since $p_i \nmid n-1$, the $(n-1)$-st power map is injective on the Sylow p_i-group of $(\mathbf{Z}_{p_i^{e_i}})^*$. Therefore, the image of x in this group must be 1. This implies that $x^{p_i - 1} \equiv 1 \pmod{p_i^{e_i}}$. This proves MR-1.

To prove MR-2, let $i \in B$. By Lemma 3.1,

$$(x+j)^{2^{h^*}m} \equiv 1 \pmod{p_i} \quad (0 \leq j < k).$$

From the fact that $h_i > h^*$, and by considering the Sylow 2-group of $\mathbf{Z}_{p_i}^*$, it follows that

$$(x+j \mid p_i) = 1 \quad (0 \leq j < k).$$

This proves MR-2.

Now consider MR-3. By Lemma 3.1,

$$(x+j)^{2^{h^*-1}m} \equiv \pm 1 \pmod{n} \quad (0 \leq j < k).$$

It follows that for any fixed value of j, with $0 \leq j < k$, the Legendre symbols

$$(x+j \mid p_i) \quad (i \in C)$$

have the same value. Moreover, if $A \cup B \neq \emptyset$, then this common value must equal $(x+j)^{2^{h^*-1}m}$ modulo $n(A \cup B)$. This proves MR-3. $\square$

We are now ready to prove Theorem 1.1. For a randomly chosen $x \in \mathbf{Z}_n$, the probability that $x, x+1, \ldots, x+k-1$ are all nonzero liars is bounded by

$$\Pr[\text{MR-1} \wedge \text{MR-2} \wedge \text{MR-3}].$$

The events MR-1 and MR-2 are independent, and so this probability is equal to

$$\Pr[\text{MR-1}] \cdot \Pr[\text{MR-2}] \cdot \Pr[\text{MR-3} \mid \text{MR-1} \wedge \text{MR-2}].$$

It is trivial to prove that

$$\Pr[\text{MR-1}] \leq \prod_{i \in A} \frac{1}{p_i^{e_i - 1}}. \tag{3.1}$$

A direct application of Lemma 2.1 to each of the individual moduli p_i, where $i \in B$, yields

$$\Pr[\text{MR-2}] \leq \prod_{i \in B} \frac{\log_2 p_i}{p_i^{1/2}}. \tag{3.2}$$

Finally, we shall prove that

$$\Pr[\text{MR-3} \mid \text{MR-1} \wedge \text{MR-2}] \leq (\log_2 n)^2 \cdot \prod_{i \in C} \frac{\log_2 p_i}{p_i^{1/2}}. \tag{3.3}$$

Before proving (3.3), we note that (3.1), (3.2), and (3.3) imply that the probability estimate in Theorem 1.1 is bounded by

$$n^{-1/2} \cdot (\log_2 n)^2 \cdot \prod_{p \mid n} \log_2 p.$$

Now, it is proved in Bach (1991) that

$$\prod_{p|n} \log p \leq n^{o(1)}. \tag{3.4}$$

Thus, the probability that $x, x+1, \ldots, x+k-1$ are all nonzero liars is at most $n^{-1/2+o(1)}$. Furthermore, the probability that any of these are zero is $O(\log n/n)$, and Theorem 1.1 is proved.

We now prove (3.3). We can of course assume that $C \neq \emptyset$. We break the proof into two cases.

First, suppose that $\#C = 1$, say $C = \{i_1\}$. Then, as n is composite, $A \cup B \neq \emptyset$. Conditioning on x modulo $n(A \cup B)$, and applying Lemma 2.1 with the modulus p_{i_1}, we obtain

$$\Pr[\text{MR-3(b)} \mid \text{MR-1} \wedge \text{MR-2}] \leq \frac{\log_2 p_{i_1}}{p_{i_1}^{1/2}}.$$

Second, suppose that $\#C \geq 2$. Arbitrarily select $i_1, i_2 \in C$. Then the events MR-3(a) and (MR-1 $\wedge$ MR-2) are independent, and the probability Pr[MR-3(a)] is equal to the probability that the following two events occur:

$$E_1: \quad (x+j \mid p_{i_1} p_{i_2}) = 1 \quad (0 \leq j < k),$$

and

$$E_2: \quad \forall i \in C \backslash \{i_1, i_2\}: (x+j \mid p_i) = (x+j \mid p_{i_1}) \quad (0 \leq j < k).$$

Applying Lemma 2.1 to the composite modulus $p_{i_1} p_{i_2}$, we obtain

$$\Pr[E_1] \leq \frac{(\log_2(p_{i_1} p_{i_2}))^2}{(p_{i_1} p_{i_2})^{1/2}}.$$

Conditioning on x modulo $p_{i_1} p_{i_2}$, and applying Lemma 2.1 to each individual modulus p_i, for all $i \in C \backslash \{i_1, i_2\}$, one sees that

$$\Pr[E_2 \mid E_1] \leq \prod_{\substack{i \in C \\ i \neq i_1, i_2}} \frac{\log_2 p_i}{p_i^{1/2}}.$$

The bound (3.3) then follows by multiplying together these bounds for $\Pr[E_1]$ and $\Pr[E_2 \mid E_1]$.

As an aside, we mention another proof of (3.4). This is equivalent to proving that

$$\sum_{p|n} \operatorname{loglog} p = o(\log n). \tag{3.5}$$

Partition the primes p dividing n into small ones—those with $\log p \leq (\operatorname{loglog} n)^2$, and large ones—those with $\log p > (\operatorname{loglog} n)^2$. As there are at most $O(\log n/ \operatorname{loglog} n)$ distinct primes dividing n, the total contribution of the small primes to (3.5) is $O(\log n \operatorname{log loglog} n/ \operatorname{loglog} n)$, which is $o(\log n)$. As there can be at most $\log n/(\operatorname{loglog} n)^2$ large primes divising n, each contributing a term of at most $\operatorname{loglog} n$ to (3.5), the total contribution of the large primes to (3.5) is $O(\log n/ \operatorname{loglog} n)$, which is $o(\log n)$.

4. Analysis of the Solovay-Strassen Test

In this section, we prove Theorems 1.2 and 1.3.

For the reader's convenience, we state here the witness set for the Solovay-Strassen test. Let n be an odd integer. Then $x \in \mathbf{Z}_n$ is in $W_{SS}(n)$ if

$$\gcd(x,n) > 1 \quad \text{or} \quad \left(\frac{x}{n}\right) \not\equiv x^{(n-1)/2} \pmod{n}.$$

We proceed now to prove Theorem 1.2. At the end of this section, we indicate the modifications needed to prove Theorem 1.3.

Let n and k be as in Theorem 1.2. As in the previous section, let

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

be the factorization of n into primes, letting

$$n - 1 = 2^h m \quad (m \text{ odd}),$$

and for $1 \le i \le r$,

$$p_i - 1 = 2^{h_i} m_i \quad (m_i \text{ odd}).$$

We define four sets of indices, $A, B, C, D \subset \{1, \ldots, r\}$:

$$\begin{aligned} A &= \{i : e_i > 1\}; \\ B &= \{i : e_i = 1 \text{ and } h_i > h\}; \\ C &= \{i : e_i = 1 \text{ and } h_i = h\}; \\ D &= \{i : e_i = 1 \text{ and } h_i < h\}. \end{aligned}$$

Recall the notation $n(S)$ defined just before Lemma 3.2.

Lemma 4.1. *If $x, x+1, \ldots, x+k-1$ are all nonzero liars for the Solovay-Strassen test, then the following conditions hold.*

SS-1:

$$\forall i \in A : x^{p_i - 1} \equiv 1 \pmod{p_i^{e_i}}.$$

SS-2:

$$\forall i \in B : (x + j \mid p_i) = 1 \quad (0 \le j < k).$$

SS-3: *(a)*

$$\forall i, i' \in C : (x + j \mid p_i) \cdot (x + j \mid p_{i'}) = 1 \quad (0 \le j < k).$$

(b) Moreover, if $A \cup B \neq \emptyset$, then

$$\forall i \in C : (x + j \mid p_i) \equiv x^{(n-1)/2} \pmod{n(A \cup B)} \quad (0 \le j < k).$$

Proof. To prove this, one only needs to use the fact that if $(x + j)$ is a nonzero liar, then $(x+j)^{(n-1)/2} \equiv \pm 1 \pmod{n}$. The proof of SS-1 is just the same as the proof of MR-1 in Lemma 3.2. Also, proofs of SS-2 and SS-3 are can be made along the same lines as the proofs MR-2 and MR-3 by considering the Sylow 2-groups of $(\mathbf{Z}_{p_i})^*$ for various values of i. We leave the deatils to the reader. $\square$

Lemma 4.2. *Assume $D \neq \emptyset$. If $x, x+1, \ldots, x+k-1$ are all nonzero liars for the Solovay-Strassen test, then the following conditions hold.*

SS-3′:

$$\forall i \in C : (x + j \mid p_i) = 1 \quad (0 \leq j < k).$$

SS-4:

$$(x + j \mid n(D)) \cdot (x + j \mid n(A \cup B \cup C)) = 1 \quad (0 \leq j < k).$$

Proof. Choose an arbitrary $i_0 \in D$. If $(x + j)$ is a nonzero liar, then it must be the case that

$$(x + j)^{(n-1)/2} \equiv \pm 1 \pmod{n}.$$

As this congruence holds modulo p_{i_0}, and since $h_{i_0} < h$, we must have $(x+j)^{(n-1)/2} \equiv 1 \pmod{p_{i_0}}$.

Therefore, $D \neq \emptyset$ implies that

$$1 = (x + j \mid n) \equiv (x + j)^{(n-1)/2} \pmod{n} \quad (0 \leq j < k).$$

Conditions SS-3′ and SS-4 follow immediately. $\square$

We are now in a position to prove Theorem 1.2. We split the proof into two cases, depending on whether D is empty or not.

First, suppose D is empty. By Lemma 4.1, the error probability is bounded by

$$\Pr[\text{SS-1} \wedge \text{SS-2} \wedge \text{SS-3}],$$

plus the probability that one of $x, x + 1, \ldots, x + k - 1$ is zero, which is negligible. One can now make an argument that is essentially identical to the one used in the proof of Theorem 1.1 to show that

$$\Pr[\text{SS-1} \wedge \text{SS-2} \wedge \text{SS-3}] \leq n^{-1/2+o(1)}.$$

This completes the proof for this first case.

Second, suppose that D is not empty so that Lemma 4.2 applies. We need to bound the probability

$$\Pr[\text{SS-1} \wedge \text{SS-2} \wedge \text{SS-3}' \wedge \text{SS-4}].$$

The events SS-1, SS-2 and SS-3′ are independent, and it is easy to show by analyzing each $i \in (A \cup B \cup C)$ separately that

$$\Pr[\text{SS-1} \wedge \text{SS-2} \wedge \text{SS-3}'] \leq n_1^{-1/2+o(1)}, \tag{4.1}$$

where $n_1 = n(A \cup B \cup C)$. Now, let $n_2 = n(D)$. Conditioning on x modulo n_1, and applying Lemma 2.1 with modulus n_2, one finds that

$$\Pr[\text{SS-4} \mid \text{SS-1} \wedge \text{SS-2} \wedge \text{SS-3}'] \leq n_2^{-1/2} (\log_2 n_2)^{\omega(n_2)}. \tag{4.2}$$

Multiplying together (4.1) and (4.2), one obtains the probability estimate in Theorem 1.2.

This proves Theorem 1.2.

To prove Theorem 1.3, one retraces the above proof with the smaller value $\lceil (\log n)^\lambda \rceil$ for k. The proof for the case where $D = \emptyset$ goes through in a straightforward fashion and we leave the details to the reader. The interesting case is when $D \neq \emptyset$. Making use of Lemma 2.1 and the estimate $\omega(n_2) \leq (\log n_2 / \operatorname{loglog} n_2)(1 + o(1))$ (see Hardy & Wright 1984, p. 355), the probability in (4.2) can be bounded by

$$\begin{aligned} 2^{-(\log n_2)^\lambda} + n_2^{-1/2} (\log n_2)^{\lambda\, \omega(n_2)} &\leq 2^{-(\log n_2)^\lambda} + \exp[\lambda\, \omega(n_2) \operatorname{loglog} n_2 - \frac{1}{2} \log n_2] \\ &\leq 2^{-(\log n_2)^\lambda} + \exp[\lambda \log n_2 (1 + o(1)) - \frac{1}{2} \log n_2] \\ &\leq 2^{-(\log n_2)^\lambda} (1 + o(1)), \end{aligned}$$

since $\lambda < 1/2$.

5. Conclusion

We have analyzed the performance of both the Miller-Rabin and the Solovay-Strassen test, under the assumption that the search for a witness proceeds by choosing $x \in \mathbf{Z}_n$ at random, and then considering $x, x+1, \ldots$, as candidate witnesses.

Our results for the Miller-Rabin test strengthen those previously obtained by Bach. Our results for the Solovay-Strassen test are new, but unfortunately are not as good as our results for the Miller-Rabin test, as they depend on the number of prime factors of n.

References

E. Bach. Realistic analysis of some randomized algorithms. *J. Comput. Sys. Sci.* **42**, pp. 30–53, 1991.

E. Bach and V. Shoup. Factoring polynomials with fewer random bits. *J. Symb. Comput.* **9**, pp. 229–239, 1990.

A. Cohen and A. Wigderson. Dispersers, deterministic amplifications, and weak random sources. In *30th Annual Symposium on Foundations of Computer Science*, pp. 14–19, 1989.

G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, fifth edition, 1984.

R. Impagliazzo and D. Zuckermann. How to recycle random bits. In *30th Annual Symposium on Foundations of Computer Science*, pp. 248–253, 1989.

H. J. Karloff and P. Raghavan. Randomized algorithms and pseudorandom numbers. In *20th Annual ACM Symposium on Theory of Computing*, pp. 310–321, 1988.

R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, 1983.

G. Miller. Riemann's hypothesis and tests for primality. *J. Comput. Sys. Sci.* **13**, pp. 300–317, 1976.

M. O. Rabin. Probabilistic algorithms for testing primality. *J. of Number Theory* **12**, pp. 128–138, 1980.

R. Solovay and V. Strassen. A fast monte-carlo test for primality. *SIAM J. Comput.* **6**, pp. 84–85, 1977.