FINDING WITNESSES USING FEWER RANDOM BITS

by

Victor Shoup

Computer Sciences Technical Report #725

November 1987

Finding Witnesses Using Fewer Random Bits

Victor Shoup*
Computer Sciences Department
University of Wisconsin
Madison, WI 53706

Abstract. Let G be a proper subgroup of $\mathbb{Z}_n^*$, the multiplicative group of units modulo n. Many number theoretic algorithms assume that an element in $\mathbb{Z}_n^* - G$ can easily be found. In this context, an element in $\mathbb{Z}_n^* - G$ is often called a "witness." Ankeny's theorem states that, assuming the ERH, the smallest witness is $O(\log^2 n)$. The purpose of this paper is to examine a "randomized" Ankeny's conjecture. Consider the following experiment. Choose $a \in \mathbb{Z}_n$ at random. Examine the elements $a, a+1, \ldots, a+k-1$, where $k = O(\log^c n)$ for some constant c. We would like the probability that none of these are witnesses to be small. The randomized Ankeny conjecture is that this probability is $O(1/n^\alpha)$ for some constant $0 < \alpha < 1$. We show that if the randomized Ankeny conjecture is true, then a deterministic Ankeny conjecture, which allows us to efficiently find witnesses deterministically, is already true. We also prove some partial randomized Ankeny results, which state that we can bound the probability of not finding a witness by $O(1/p^{1/2-\epsilon})$, where p is a prime divisor of n that is "nontrivial" on G.

0. Introduction

The Half-Cost of a Randomized Algorithm

It is customary nowadays to consider problems that are solvable in random polynomial time to be tractable. However, this point of view relies on the availability of a source of independent, uniformly distributed random bits. No such source exists, so the status of problems solvable in random polynomial time is dubious at best. We would like to eliminate the need for random bits—i.e., find deterministic polynomial time algorithms for problems that are currently known only to have random polynomial time algorithms. In lieu of eliminating random bits altogether, we might tackle the intermediate problem of *reducing* the number of random bits.

We are therefore lead to viewing random bits as a scarce resource. Let's restrict our attention to probabilistic Turing machines that either accept or reject their input, such that for any particular input, the probability that the machine accepts is either 0 or $\geq 1/2$. That is, we restrict our attention to probabilistic

* This research was supported by NSF grants DCR-8504485 and DCR-8552596.

Turing machines of the kind that characterize **RP**. Let M be such a machine. Suppose that on input x, the number of random bits used is at most $b(x)$ and that the error probability is $2^{-t(x)}$. We define the *half-cost* of M on input x, denoted $h(x)$, to be the ratio $b(x)/t(x)$. Intuitively, the half-cost measures the number of random bits required to cut in half the probability of making a mistake.

We argue that the half-cost is a good measure of an algorithm's use of random bits. Simply using $b(x)$ as a measure of random bit use is inadequate, since it ignores the effectiveness of the random bits in reducing the error probability. It is important to consider the relationship between the number of random bits and the error probability. The half-cost does this. One nice property of the half-cost is that it does not change if we iterate M to reduce the error probability.

We observe that if the half-cost is nonzero (if it is zero, M is actually deterministic), the best possible half-cost is $O(1)$ and the worst is polynomial in the length of the input. In our quest for better algorithms, as an intermediate step in eliminating random bits altogether, we should strive to minimize the half-cost.

The Subgroup Paradigm

We now consider a collection of number theoretic problems that can be solved in random polynomial time using what we'll call the *subgroup paradigm*. These problems are characterized as follows. Given an integer n as input, a search is conducted for an integer a that lies outside some proper subgroup G of the multiplicative group of units modulo n. Such an integer a is then used in further computations, or is simply used to signal acceptance of the input. Examples include the congruence solving algorithm in [AMM], the problem of finding primitive elements modulo primes p given the prime decomposition of $p-1$, the problem of factoring n given the Euler totient function $\phi(n)$ [M], and the primality tests of Solovay and Strassen [SS] and Miller [M].

Given the abundance of algorithms that employ the subgroup paradigm, we are compelled to take a closer look at it. Let $\mathbb{Z}_n$ be the ring of integers modulo n, $\mathbb{Z}_n^+$ be the set of nonzero elements of $\mathbb{Z}_n$, and $\mathbb{Z}_n^*$ be the multiplicative group of units of $\mathbb{Z}_n$. Let's restrict our attention to membership problems for languages $L \subset \mathbb{Z}$ that can be characterized as follows: for every n there exists a subgroup G of $\mathbb{Z}_n^*$ such that (1) membership in G can be determined in polynomial time, and (2) $n \in L$ if and only if G is a proper subgroup. The set of composite integers is such a language (see [SS] or section 3). An algorithm that employs the subgroup paradigm to recognize L relies on the hypothesis that we can efficiently find an element of $\mathbb{Z}_n^* - G$, assuming G is a proper subgroup of $\mathbb{Z}_n^*$. Actually, it often suffices to simply find an element of $\mathbb{Z}_n^+ - G$. Such an element is often called a "witness," since it testifies to the fact that $n \in L$.

How are witnesses to be found? One approach is to use a version of Ankeny's theorem which states that, assuming the Extended Riemann Hypothesis (ERH), the least element in $\mathbb{Z}_n^* - G$ is $O\left(\log^2 n\right)$ (see [B2]). This gives rise to the following efficient procedure: examine the numbers $1, 2, \ldots, k$, where $k = O\left(\log^2 n\right)$—one of these must be a witness. The problem with this approach is that the ERH has never been proved.

Another approach is to use randomization. Assuming we can generate a "random" sequence

$a_1, a_2, \ldots, a_k$ of elements from $\mathbb{Z}_n$, the probability that all of these lie in G is at most 2^{-k}. To see this, note that $|G| \leq \phi(n)/2 < n/2$, and so the probability that a randomly chosen element from $\mathbb{Z}_n$ lies in G is at most 1/2. This approach will, with very high probability, quickly find an element in $\mathbb{Z}_n^+ - G$. It will also quickly find an element in $\mathbb{Z}_n^* - G$. This follows from the fact that $\phi(n) = \Omega(n/\log\log n)$ (see [HW], p. 267). The problem with this approach is that it uses many random bits, and in fact uses them in a possibly suboptimal way. The half-cost of an algorithm using this approach could be as bad as $\Omega(\log n)$.

The Randomized Ankeny's Conjecture

Our goal is to minimize the half-cost of randomized algorithms that use the subgroup paradigm. To this end, we examine a "randomized" Ankeny's conjecture. Consider the following experiment. Choose $a \in \mathbb{Z}_n$ at random. Examine the elements $a, a+1, \ldots, a+k-1$, where $k = O(\log^c n)$ for some constant c. We would like the probability that none of these are witnesses to be small. The randomized Ankeny conjecture is that this probability is $O(1/n^\alpha)$ for some constant $0 < \alpha < 1$. If the randomized Ankeny conjecture is true, then randomized algorithms that use the subgroup paradigm can be modified so that they have an optimal half-cost, i.e. $O(1)$. It has been shown in [B1] that when n is prime, the probability of not finding a witness using such a procedure is $O\left(1/n^{1/2-\epsilon}\right)$ for all $\epsilon > 0$. Thus, the focus of this paper is composite n.

We have two main results:

(1) We show that if the randomized Ankeny conjecture is true, then a deterministic Ankeny conjecture, which allows us to efficiently find witnesses deterministically, is already true.

(2) We prove a partial randomized Ankeny result, the usefulness of which depends on the factorization of n and the structure of G. This result states that we can bound the probability of not finding an element in $\mathbb{Z}_n^+ - G$ by $2\log p/\sqrt{p}$ where p is a prime divisor of n that is "nontrivial" on G (see section 2 for the technical definition of "nontrivial"). We also prove an analogous result for finding elements in $\mathbb{Z}_n^* - G$.

These results are discussed in sections 1 and 2, respectively. Section 3 sketches some applications of the results in section 2, including a half-cost analysis of the Solovay-Strassen prime test, which is an improvement of the error bound of Kranakis [K]. Section 4 discusses some open questions.

1. Negative Results

Let G be a proper subgroup of $\mathbb{Z}_n^*$. Suppose we perform the following experiment: choose $a \in \mathbb{Z}_n$ at random and examine $a, a+1, \ldots, a+k-1$, where $k = O(\log^c n)$ for some constant c. We want to know the probability that none of these are in $\mathbb{Z}_n^+ - G$ (or better, $\mathbb{Z}_n^* - G$). We would like this to be $O(1/n^\alpha)$ for some $0 < \alpha < 1$. It turns out that if we can make the probability this small, we can in fact reduce it to zero by looking at longer (but still polynomial bounded) sequences. We begin with some definitions to make things more concise.

Let n be an integer, G a subgroup of $\mathbb{Z}_n^*$, and k a positive integer. Define $P(n, k, G)$ to be the fraction of $a \in \mathbb{Z}_n$ such that none of $a, a+1, \ldots, a+k-1$ are in $\mathbb{Z}_n - G$. We similarly define $P^+(n, k, G)$ and $P^*(n, k, G)$

by replacing $\mathbb{Z}_n - G$ by $\mathbb{Z}_n^+ - G$ and $\mathbb{Z}_n^* - G$, respectively. We then define $P(n,k) = \max_G P(n,k,G)$, where G ranges over all proper subgroups of $\mathbb{Z}_n^*$. $P^+(n,k)$ and $P^*(n,k)$ are defined similarly by replacing $P(n,k,G)$ by $P^+(n,k,G)$ and $P^*(n,k,G)$, respectively.

We know formally define three randomized Ankeny conjectures: RA, RA$^+$, and RA*.

Randomized Ankeny Conjecture (RA). There exist positive numbers b and c, and $0 < \alpha < 1$ such that

$$P\left(n, \lfloor b(\log n)^c \rfloor\right) = O\left(\frac{1}{n^\alpha}\right).$$

We define RA$^+$ and RA* by replacing P by P^+ and P^*, respectively. In each of these definitions, we can replace $O(1/n^\alpha)$ by $o(1/n^\alpha)$, since $1/n^\alpha = o\left(1/n^{\alpha/2}\right)$. Also note that RA $\leftrightarrow$ RA$^+$. This is because

$$P\left(n, \lfloor b(\log n)^c \rfloor\right) \leq P^+\left(n, \lfloor b(\log n)^c \rfloor\right) \leq P\left(n, \lfloor b(\log n)^c \rfloor\right) + b(\log n)^c/n$$

We know define three analogous deterministic Ankeny conjectures: SA, SA$^+$, and SA*.

Strong Ankeny Conjecture (SA). There exist positive numbers b and c such that

$$P\left(n, \lfloor b(\log n)^c \rfloor\right) = 0 \quad \text{for all sufficiently large } n.$$

Again, we define SA$^+$ and SA* by replacing P by P^+ and P^*, respectively. Note that SA $\leftrightarrow$ SA$^+$, since $P\left(n, \lfloor b(\log n)^c \rfloor\right) = 0$ implies that $P^+\left(n, \lfloor 2b(\log n)^c \rfloor\right) = 0$. Also note that SA $\rightarrow$ $PRIMES \in P$.

Proposition 1.1. RA$^+$ $\rightarrow$ SA$^+$. In particular, $P\left(n, \lfloor b(\log n)^c \rfloor\right) = o(1/n^\alpha)$ implies that $P\left(n, \left\lfloor b(\log n)^{c+1} \right\rfloor\right) = 0$ for all sufficiently large n.

Proof. Assume $P\left(n, \left\lfloor b(\log n)^{c+1} \right\rfloor\right) > 0$ infinitely often. We want to show that $P\left(n, \lfloor b(\log n)^c \rfloor\right)$ is not $o(1/n^\alpha)$. Now, there are infinitely many integers n_0 with a proper subgroup $G_0 < \mathbb{Z}_{n_0}^*$ such that $P(n_0, k_0, G_0) > 0$, where $k_0 = \left\lfloor b(\log n_0)^{c+1} \right\rfloor$. For each such sufficiently large n_0, we cook up an n_1 such that $P\left(n_1, \lfloor b(\log n_1)^c \rfloor\right) > D/n_1^\alpha$, where D is a constant.

There is a constant A such that for any $x > 1$ there is a prime p satisfying $x \leq p \leq Ax$ (see [HW], p. 343). Let x be defined by $(\log n_0)^{c+1} = (\log(n_0 A x))^c$, and notice that $x \rightarrow \infty$ as $n_0 \rightarrow \infty$. Let p be the least prime $\geq x$. For n_0 sufficiently large, $x \leq p \leq Ax$. Put $n_1 = n_0 p$. Now,

$$\begin{aligned}(\log n_0)^{c+1} &= (\log(n_0 A x))^c \\ &\geq (\log n_1)^c\end{aligned}$$

Also,

$$\begin{aligned}(\log n_0)^{c+1} &= (\log(n_0 A x))^c \\ &\leq (\log n_0 A p)^c \quad . \\ &\leq O\left((\log n_1)^c\right)\end{aligned}$$

Hence, there is a constant B such that for sufficiently large n_0,

$$(\log n_1)^c \leq (\log n_0)^{c+1} \leq B(\log n_1)^c.$$

Let $\delta > 0$. Then we have

$$\begin{aligned} n_0 &\leq \exp\left(B^{1/(c+1)}(\log n_1)^{c/(c+1)}\right) \\ &= n_1{}^{B^{1/(c+1)}(\log n_1)^{-1/(c+1)}} \\ &< n_1^\delta \quad \text{for sufficiently large } n_0. \end{aligned}$$

We can set $\delta = 1/2$ so that $n_0 p > n_0^2$, i.e. $p > n_0$. It follows that $\gcd(p, n_0) = 1$, and by Chinese Remaindering, $\mathbb{Z}_{n_1} \cong \mathbb{Z}_{n_0} \times \mathbb{Z}_p$. We define the subgroup $G_1 = G_0 \times \mathbb{Z}_p^*$. Put $k_1 = \lfloor b(\log n_1)^c \rfloor$, and note that $k_1 \leq k_0$. By the Chinese Remainder isomorphism, it is easy to see that $P(n_1, k_1, G_1) = P(n_0, k_1, G_0)P(p, k_1, \mathbb{Z}_p^*)$. Since $k_1 \leq k_0$, $P(n_0, k_1, G_0)$ is nonzero. Therefore, $P(n_0, k_1, G_0) \geq 1/n_0$. Also, $P(p, k_1, \mathbb{Z}_p^*) = (p - k_1)/p$, since there are only k_1 elements $a \in \mathbb{Z}_p$ such that one of $a, a+1, \ldots,$ or $a + k_1 - 1$ are not in $\mathbb{Z}_p^*$. It follows that $P(n_1, k_1, G_1)$ is at least

$$\left(\frac{1}{n_0}\right)\left(\frac{p - k_1}{p}\right).$$

Since $(p - k_1)/p \to 1$ as $p \to \infty$, for sufficiently large n_0, we have $P(n_1, k_1) > D/n_0$ for some constant D. Now put $\delta = \alpha$ and we obtain $P(n_1, k_1) > D/n_1^\alpha$. ■

A similar result holds relating RA* and SA*.

Proposition 1.2. RA* → SA*. In particular, $P^*\left(n, \lfloor b(\log n)^c \rfloor\right) = o(1/n^\alpha)$ implies that $P^*\left(n, \lfloor b(\log n)^{c+1} \rfloor\right) = 0$ for all sufficiently large n.

Sketch of proof. The proof is almost identical to the proof of Proposition 1.1. The only difference is that $P^*(n_1, k_1, G_1) \geq P^*(n_0, k_1, G_0)$. This is because for any integer a, $a \bmod n_1 \in \mathbb{Z}_{n_1}^* - G_1$ implies that $a \bmod n_0 \in \mathbb{Z}_{n_0}^* - G_0$. ■

At this point, the reader might complain that we have just set up a "straw man." Indeed, it would be nice to extend the results of this section to a more general setting. For example, instead of considering sequences $a, a+1, \ldots, a+k-1$, we might consider $a, f(a), \ldots, f^{k-1}(a)$, where f is a fixed function chosen from some interesting family of functions.

One interesting case is to let f be any fixed polynomial with integer coefficients. Propositions 1.1 and 1.2 handled the special case $f(x) = x + 1$. It is easily seen that the proof of Proposition 1.2 does not rely on this restriction, and so it generalizes to any fixed polynomial. An open question is whether or not proposition 1.1 can be generalized in a similar manner.

2. Positive Results

In this section, we prove a weak form of the randomized Ankeny conjecture, which is useful in cases where we have some information about the factorization of n and the structure of the subgroup $G < \mathbb{Z}_n^*$. The main results of this section are Propositions 2.1 and 2.6, which deal with witnesses of the form $\mathbb{Z}_n^+ - G$ and $\mathbb{Z}_n^* - G$, respectively.

Suppose p is a prime dividing n, and G is a subgroup of $\mathbb{Z}_n^*$. Split n into coprime factors p^e and m. We say that *p is nontrivial on G* if for some integer y, $y \equiv 1 \pmod{m}$ and $y \bmod n \in \mathbb{Z}_n^* - G$. Otherwise, *$p$ is trivial on G*. By Chinese Remaindering, $\mathbb{Z}_n^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_{p^e}^*$. It is easy to see that p is trivial on G if and only if G is of the form $H \times \mathbb{Z}_{p^e}^*$ where H is a subgroup of $\mathbb{Z}_m^*$. Notice that if G is a proper subgroup of $\mathbb{Z}_n^*$, then at least one prime divisor of n is nontrivial on G.

Proposition 2.1. Let n be an integer, and p be an odd prime dividing n. Let $k = \lceil \log_2 \sqrt{p} \rceil$. Let G be a proper subgroup of $\mathbb{Z}_n^*$. Assume that p is nontrivial on G. Then the fraction of $x \in \mathbb{Z}_n$ such that none of $x, x+1, \ldots, x+k-1$ are in $\mathbb{Z}_n^+ - G$ is less than $2\log p/\sqrt{p}$.

Proof. It will suffice to show that the fraction of $x \in \mathbb{Z}_n$ such that all of $x, \ldots, x+k-1$ are in G is no more that $\log p/\sqrt{p}$. For then the fraction of $x \in \mathbb{Z}_n$ such that $x, \ldots, x+k-1$ are all outside $\mathbb{Z}_n^+ - G$ is no more than $\log p/\sqrt{p} + k/n$, which is easily shown to be less than $2\log p/\sqrt{p}$.

By Chinese Remaindering, we have $\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_{p^e}$. Let h be the natural homomorphism from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*/G$. Define $h_1 \colon \mathbb{Z}_m^* \to \mathbb{Z}_n^*/G$ by $a \mapsto h(a,1)$, and $h_2 \colon \mathbb{Z}_{p^e}^* \to \mathbb{Z}_n^*/G$ by $b \mapsto h(1,b)$. So we have $h(a,b) = h_1(a)h_2(b)$. Furthermore, since p is nontrivial on G, h_2 is nontrivial, i.e. $h_2(b) \neq 1$ for some b.

Let $x \in \mathbb{Z}_m$. For $y \in \mathbb{Z}_{p^e}$, let $B(y)$ be the condition that if $z = (x,y)$ then $z, z+1, \ldots,$ and $z+k-1$ are all in G. Let α be the fraction of all $y \in \mathbb{Z}_{p^e}$ satisfying $B(y)$. We will show that $\alpha \leq \log p/\sqrt{p}$. Since this holds for all choices of $x \in \mathbb{Z}_m$, the result will follow.

Suppose that $x + j - 1 \notin \mathbb{Z}_m^*$ for some $j = 1, \ldots, k$. Then $z \notin \mathbb{Z}_n^*$ for any choice of y. In this case $\alpha = 0$. Otherwise, let $\gamma_j = h_1(x+j-1)$ for $j = 1, \ldots, k$. We want to know the fraction of $y \in \mathbb{Z}_{p^e}$ such that $y+j-1$ is a unit and $h_2(y+j-1) = \gamma_j^{-1}$ for $j = 1, \ldots, k$. If γ_j^{-1} is not in the range of h_2 for some j, there are no such y, and again $\alpha = 0$.

Otherwise, let K be the kernel of h_2. Choose $\xi_1, \ldots, \xi_k \in \mathbb{Z}_{p^e}^*$ such that $h_2(\xi_j) = \gamma_j^{-1}$. Then $B(y)$ is equivalent to the condition that $y+j-1 \in \xi_j K$ for $j = 1, \ldots, k$. Let $q = [\mathbb{Z}_{p^e}^* : K]$. We know that $q \neq 1$ and $q \mid \phi(p^e) = (p-1)p^{e-1}$. If q does not divide $p-1$, then we must have $q \geq p$. But in this case, the fraction of y satisfying $y \in \xi_1 K$ is already no more than $1/p$, and so $\alpha \leq 1/p \leq \log p/\sqrt{p}$.

Otherwise, assume that $q \mid p-1$. Since $K = \{t^q : t \in \mathbb{Z}_{p^e}^*\}$, $B(y)$ is equivalent to the condition that there exist $t_1, \ldots, t_k \in \mathbb{Z}_{p^e}^*$ such that $y+j-1 = \xi_1 t_i^q$ for $j = 1, \ldots, k$. So we have reduced the problem to the following:

CLAIM. Let p be an odd prime, and let $q \mid p-1$, $q \neq 1$. Put $k = \lceil \log_2 \sqrt{p} \rceil$. Let $e > 0$. Let

$\xi_1, \xi_2, \ldots, \xi_k \in \mathbb{Z}^*_{p^e}$. Then the fraction of y in $\mathbb{Z}_{p^e}$ such that there exist $t_1, t_2, \ldots, t_k \in \mathbb{Z}^*_{p^e}$ which satisfy $y = \xi_1 t_1^q, y+1 = \xi_2 t_2^q, \ldots, y+k-1 = \xi_k t_k^q$ is at most $\log p/\sqrt{p}$.

Lemmas 2.2 to 2.5 will establish this claim, and complete the proof. ■

The following lemma, which is really the key to this result, is proved in [B1].

Lemma 2.2. Let p be an odd prime, $q \mid p-1$, $q \neq 1$, $2 \leq k \leq p$. Let $\xi_1, \xi_2, \ldots, \xi_k$ be integers relatively prime to p. Then the number of distinct solutions mod p in $x, y_1, \ldots, y_k$ to the system of equations

$$\begin{aligned} x &\equiv \xi_1 y_1^q \pmod p \\ x+1 &\equiv \xi_2 y_2^q \pmod p \\ &\vdots \\ x+k-1 &\equiv \xi_k y_k^q \pmod p \end{aligned}$$

is at most $p + q^k(k-1)\sqrt{p}$.

We now give a "power raising" lemma which relates the number of solutions to a system of polynomial equations mod p and mod p^e.

Lemma 2.3. Let p be a prime number. Let $f_1, f_2, \ldots, f_m \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ where $m \leq n$. Let $J(x_1, \ldots, x_n)$ be the matrix

$$\begin{pmatrix} \partial f_1/\partial x_1 & \ldots & \partial f_1/\partial x_n \\ \vdots & & \vdots \\ \partial f_m/\partial x_1 & \ldots & \partial f_m/\partial x_n \end{pmatrix}$$

Assume the following "nonsingularity" condition: For any $a_1, \ldots, a_n \in \mathbb{Z}$, if

$$f_i(a_1, \ldots, a_n) \equiv 0 \pmod p \quad (i = 1, \ldots, m)$$

then the rows of $J(a_1, \ldots, a_n)$ are linearly independent mod p.

Now, let N_e be the number of distinct solutions mod p^e in $x_1, \ldots, x_n$ to the system of equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &\equiv 0 \pmod{p^e} \\ &\vdots \\ f_m(x_1, \ldots, x_n) &\equiv 0 \pmod{p^e}. \end{aligned}$$

Then $N_{e+1} = p^{n-m} N_e$, and hence $N_e = p^{(e-1)(n-m)} N_1$.

Proof. Suppose $a_1, \ldots, a_n$ satisfy $f_i(a_1, \ldots, a_n) \equiv 0 \pmod{p^{e+1}}$, for $i = 1, \ldots, m$, where $0 \leq a_j < p^{e+1}$. Let's write $a_j = b_j + h_j p^e$, where $0 \leq h_j < p$ and $0 \leq b_j < p^e$. Then $b_1, \ldots, b_n$ satisfy $f_i(b_1, \ldots, b_n) \equiv 0$

(mod p^e), for $i = 1, \ldots, m$, We will show that for each such solution $b_1, \ldots, b_n$ mod p^e, we can choose $h_1, \ldots, h_n$ in exactly p^{n-m} ways to yield a solution $a_1, \ldots, a_n$ mod p^{e+1}. This will establish the result.

Use Taylor's formula to write

$$\begin{aligned} f_i\left(b_1 + h_1 p^e, \ldots, b_n + h_n p^e\right) &= f_i\left(b_1, \ldots, b_n\right) + h_1 p^e \frac{\partial f_i}{\partial x_1}\left(b_1, \ldots, b_n\right) \\ &\quad + \cdots + h_n p^e \frac{\partial f_i}{\partial x_n}\left(b_1, \ldots, b_n\right) \\ &\quad + \text{higher order terms} \\ &\equiv f_i\left(b_1, \ldots, b_n\right) + h_1 p^e \frac{\partial f_i}{\partial x_1}\left(b_1, \ldots, b_n\right) \\ &\quad + \cdots + h_n p^e \frac{\partial f_i}{\partial x_n}\left(b_1, \ldots, b_n\right) \pmod{p^{e+1}} \end{aligned}$$

Now let's set this quantity equal to zero mod p^{e+1} and divide through by p^e, to obtain

$$f_i\left(b_1, \ldots, b_n\right)/p^e + h_1 \frac{\partial f_i}{\partial x_1}\left(b_1, \ldots, b_n\right) + \cdots + h_n \frac{\partial f_i}{\partial x_n}\left(b_1, \ldots, b_n\right) \equiv 0 \pmod{p}$$

Hence, the h_j of interest are the solutions of

$$J\left(b_1, \ldots, b_n\right) \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} -f_1\left(b_1, \ldots, b_n\right)/p^e \\ \vdots \\ -f_m\left(b_1, \ldots, b_n\right)/p^e \end{pmatrix} \pmod{p}$$

Now, the nonsingularity condition implies that the rows of $J\left(b_1, \ldots, b_n\right)$ are linearly independent. Thus, by Gaussian elimination, there are $n - m$ degrees of freedom, and p^{n-m} solutions. ■

Lemma 2.4. Let p be an odd prime, $e \geq 1$, $q \mid p-1$, $q \neq 1$, $k \geq 1$. Let $\xi_1, \ldots, \xi_k$ be integers relatively prime to p. Let $F(k)$ be the fraction of $x \in \mathbb{Z}_{p^e}$ for which there exist $y_1, \ldots, y_k \in \mathbb{Z}_{p^e}^*$ satisfying

$$\begin{aligned} x &\equiv \xi_1 y_1^q \pmod{p^e} \\ x + 1 &\equiv \xi_2 y_2^q \pmod{p^e} \\ &\vdots \\ x + k - 1 &\equiv \xi_k y_k^q \pmod{p^e}. \end{aligned} \tag{$*$}$$

Then $F(k) \leq q^{-k} + (k-1)/\sqrt{p}$.

Proof. If $k = 1$, the result follows from the fact that one out of every q elements in $\mathbb{Z}_{p^e}^*$ is a q-th residues. If $k > p$, $F(k)$ is zero. Hence we may assume that $2 \leq k \leq p$.

We can use lemmas 2.2 and 2.3 to count the number of solutions to $(*)$. We need to check the nonsingularity condition of lemma 2.3. Let $f_j(x, y_1, \ldots, y_k) = x + j - 1 - \xi_j y_j^q$, for $j = 1, \ldots, k$. Then

$$J(x, y_1, \ldots, y_k) = \begin{pmatrix} 1 & -\xi_1 q y_1^{q-1} & & & \\ 1 & & -\xi_2 q y_2^{q-1} & & \\ \vdots & & & \ddots & \\ 1 & & & & -\xi_k q y_2^{q-1} \end{pmatrix}$$

Assume that $x, y_1, \ldots, y_k$ satisfy $(*)$. Since $k \le p$, at most one y_j can be 0 mod p. From this it is easy to see that the rows of J are linearly independent mod p.

Applying lemmas 2.2 and 2.3, we see that there are at most $p^{e-1}\left(p + q^k(k-1)\sqrt{p}\right)$ solutions to $(*)$. Suppose $x, y_1, \ldots, y_k$ is a solution to $(*)$ such that $y_1, \ldots, y_k \in \mathbb{Z}_{p^e}^*$. Then there are exactly q^k such solutions involving x, namely, $x, \omega^{i_1} y_1, \ldots, \omega^{i_k} y_k$, $0 \le i_j < q$, where ω is a an element of order q in $\mathbb{Z}_{p^e}^*$. Thus the number of $x \in \mathbb{Z}_{p^e}$ for which there exist $y_1, \ldots, y_k \in \mathbb{Z}_{p^e}^*$ satisfying $(*)$ is at most $p^{e-1}\left(pq^{-k} + (k-1)\sqrt{p}\right)$. Divide this by p^e to obtain the result. ■

Lemma 2.5. Notation as in lemma 2.4. Let $k = \lceil \log_q \sqrt{p} \rceil$. We have $F(k) \le \log p/\sqrt{p}$.

Proof. Let $f(x) = q^{-x} + (x-1)/\sqrt{p}$. We know that $F(k)$ is a nonincreasing function, that $F(k) \le f(k)$, and that $f(x)$ is concave up. Hence, it will suffice to show that $f\left(\log_q \sqrt{p}\right), f\left(log_q \sqrt{p} + 1\right) \le \log p/\sqrt{p}$. This is in fact the case for $p \ge 7$, as can be easily checked. For $p = 3$ and $p = 5$, one directly checks that $\log p/\sqrt{p} > 1/2 \ge F(1)$. ■

Lemma 2.5 completes the proof of Proposition 2.1, which deals with witnesses of the form $\mathbb{Z}_n^+ - G$. The natural question to ask next is whether a similar result holds for witnesses of the form $\mathbb{Z}_n^* - G$. To answer this question, we need to know something about the distribution of the units in $\mathbb{Z}_n$. Let $a_1 < a_2 < \cdots$ be the positive integers relatively prime to n. Let $g(n) = \max\{a_{i+1} - a_i\}$. $g(n)$ is known as Jacobsthal's function. Results in [I] imply that $g(n) = O\left(\log^2 n\right)$.

Proposition 2.6. Let n be an integer, and p be an odd prime dividing n. Split n into coprime factors p^e and m. Let $k = g(m)\lceil \log_2 \sqrt{p} \rceil$. Let G be a proper subgroup of $\mathbb{Z}_n^*$. Assume that p is nontrivial on G. Also assume that $k \le p$. Then the fraction of $x \in \mathbb{Z}_n$ such that none of $x, x+1, \ldots, x+k-1$ are in $\mathbb{Z}_n^* - G$ is less than $2\log p/\sqrt{p}$.

Proof. As in Proposition 2.1, we have $\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_{p^e}$. Let h be the natural homomorphism from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*/G$. Define $h_1 \colon \mathbb{Z}_m^* \to \mathbb{Z}_n^*/G$ by $a \mapsto h(a, 1)$, and $h_2 \colon \mathbb{Z}_{p^e}^* \to \mathbb{Z}_n^*/G$ by $b \mapsto h(1, b)$. So we have $h(a, b) = h_1(a) h_2(b)$. Since p is nontrivial on G, h_2 is nontrivial, i.e. $h_2(b) \ne 1$ for some b.

Let $x \in \mathbb{Z}_m$. For $y \in \mathbb{Z}_{p^e}$, let $B(y)$ be the condition that if $z = (x, y)$ then none of $z, z+1, \ldots,$ and $z + k - 1$ are in $\mathbb{Z}_n^* - G$. Let α be the fraction of all $y \in \mathbb{Z}_{p^e}$ satisfying $B(y)$. We will show that $\alpha < 2\log p/\sqrt{p}$. Since this holds for all choices of $x \in \mathbb{Z}_m$, the result will follow.

By hypotheses, at least $\log_2 \sqrt{p}$ of $x, x+1, \ldots, x+k-1$ are in $\mathbb{Z}_m^*$. Let's call these $x+c_1, \ldots, x+c_l$, where $l = \lceil \log_2 \sqrt{p} \rceil$, and $0 \leq c_j < p$.

Let $\gamma_j = h_1(x+c_j)$ for $j = 1, \ldots, l$. It can be shown that the fraction of $y \in \mathbb{Z}_{p^e}$ such that $y + c_j$ is a unit and $h_2(y+c_j) = \gamma_j^{-1}$ for $j = 1, \ldots, l$, is at most $\log p/\sqrt{p}$. This is just a slight extension of what was shown in Proposition 2.1. Lemmas 2.2 to 2.5 can be modified to handle this extension, and we omit the details.

Furthermore, the fraction of $y \in \mathbb{Z}_{p^e}$ such that $y + c_j$ is not a unit for some $j = 1, \ldots, l$ is no more than l/p. Thus, $\alpha \leq \log p/\sqrt{p} + l/p$. From this, it is easy to show that $\alpha < 2 \log p/\sqrt{p}$. ■

Note that the requirement that $k \leq p$ in Proposition 2.6 is not a practical limitation. If $p < k$, we can efficiently split n into m and p^e. Using the notation in the proof, we can efficiently reduce the problem of finding an element in $\mathbb{Z}_n^* - G$ to the problem of finding an element in $\mathbb{Z}_{p^e}^* - \text{Ker } h_2$. It is not hard to show that one of $1, 2, \ldots, p^2$ must lie in $\mathbb{Z}_{p^e}^* - \text{Ker } h_2$. So we can *deterministically* find a witness simply by examining no more than k^2 numbers.

3. Applications

Applications to Primality Testing

Let n be an odd integer, and let G be the subgroup of $\mathbb{Z}_n^*$ defined by

$$G = \left\{ x \in \mathbb{Z}_n^* : \left(\frac{x}{n}\right) \bmod n = x^{(n-1)/2} \right\}.$$

Here, $\left(\frac{x}{n}\right)$ is the Jacobi symbol. The Solovay-Strassen prime testing algorithm [SS] is based on the fact that n is prime $\leftrightarrow G = \mathbb{Z}_n^*$. A witness to the compositeness of n is any $x \in \mathbb{Z}_n^+ - G$. A possible strategy for searching for a witness is to choose x at random from $\mathbb{Z}_n$, and then test if one of $x, x+1, \ldots, x+k-1$ is a witness, where k is bounded by some polynomial in $\log n$. The following proposition tells us that this strategy has some merit.

Proposition 3.1. Let n be an odd composite integer, and G the subgroup of $\mathbb{Z}_n^*$ defined above. Let p be the largest prime dividing n, and let $k = \lceil \frac{1}{2} \log_2 n \rceil$. Then the fraction of $x \in \mathbb{Z}_n$ such that none of $x, x+1, \ldots, x+k-1$ are in $\mathbb{Z}_n^+ - G$ is no more than $2 \log p/\sqrt{p}$.

Proof. It will suffice to show that all prime divisors p of n are nontrivial on G. Then proposition 2.1 will apply. Let $n = mp^e$ where p does not divide m. By Chinese Remaindering, we can write $\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_{p^e}$. Let g be a generator for $\mathbb{Z}_{p^e}^*$, and let $y = (1, g)$. We will show that $y \notin G$.

Suppose $e > 1$. In this case, we must have $g^{(n-1)/2} \neq \pm 1$ and hence $y^{(n-1)/2} \neq \pm 1$. To see this, note that $g^{(n-1)/2} = \pm 1$ implies that $p^{e-1}(p-1)/2 \mid (n-1)/2$ and hence $p \mid n-1$, which is clearly impossible, since $p \mid n$. We conclude that $y \notin G$.

Suppose $e = 1$ and $m > 2$. In this case, we have $\left(\frac{y}{n}\right) = \left(\frac{1}{m}\right)\left(\frac{g}{p}\right) = 1 \cdot (-1) = -1$. However, $y^{(n-1)/2} = \left(1, g^{(n-1)/2}\right) \neq -1$. Hence, $y \notin G$. ■

We want to compare the half-cost of the probabilistic algorithm based on the strategy described in Proposition 3.1 to the half-cost of the standard Solovay-Strassen algorithm.

The standard Solovay-Strassen algorithm on input n guesses a number x between 1 and n, which takes $\log_2 n$ random bits. In Solovay and Strassen's analysis of this algorithm, all we can say is that x is a "liar" with probability at most $1/2$. So the half-cost is $O(\log n)$. More recently, Kranakis has shown that if $(n-1)/2$ is odd, the error probability is bounded by $1/2^{r-1}$, where r is the number of distinct prime divisors of n [K]. So the half-cost is $O(\log n/r)$ when restricted to integers n for which $(n-1)/2$ is odd.

The modified Solovay-Strassen algorithm on input n guesses a number x between 1 and n, taking $\log_2 n$ random bits. By Proposition 3.1, x is a "liar" with probability $O\left(1/p^{1/2-\epsilon}\right)$, where p is the largest prime divisor of n. So the half-cost is $O(\log n/\log p)$. This is obviously better than the half-cost yielded by Solovay and Strassen's analysis. In some sense, it is a dual result to Kranakis' result. Kranakis' result states that if n is "very composite," i.e. has many distinct prime factors, then the Solovay-Strassen method has a small error probability. Our result says that if n is "almost prime," i.e. has few prime factors, then the Solovay-Strassen method (modified) has a small error probability. Note, however, that "almost all" integers are "almost prime." So in some sense, our result is better.

Let's look more closely at our result. At worst, we can assume that $p > \frac{1}{4}\log_2 n$; otherwise, we will certainly find a proper divisor of n, and the half-cost will be zero. Therefore, the half-cost is $O\left(\log n/\log\log n\right)$.

Beyond this, we can consider the density of sets of integers n which yield better half-costs. By the density of a set of integers S, we mean $\lim_{N\to\infty} |\{n \leq N : n \in S\}|/N$. It is known (see [HW], p. 356) that the number of prime factors of n is $O(\log\log n)$ on a set of density 1. Therefore, the half-cost is $O(\log\log n)$ on a set of density 1. Compare this to Kranakis' result. If the number of prime factors of n is $O(\log\log n)$, Kranakis' analysis yields a half-cost that is $O(\log n/\log\log n)$. So on a set of density 1, our half-cost is better than Kranakis'. In [KT] it is shown that for any k, the density of integers n such that the largest prime divisor of n is $\leq n^{1/k}$, is no more than $1/k!$. Thus, for any $\epsilon > 0$, the half-cost is $O(1)$ on a set of density $1-\epsilon$.

We should remark that [B1] gives a randomized prime testing algorithm, based on Miller's method, which in fact has a half-cost that is $O(1)$.

Applications to Cryptosystems

Certain algorithms used in cryptosystems use numbers which are the product of two large primes, i.e. $n = pq$ where $p, q \approx n^{1/2}$. Thus, any algorithm which requires finding an $x \in \mathbb{Z}_n^* - G$ can do so with failure probability $O\left(\frac{1}{n^{1/4-\epsilon}}\right)$ by simply randomly choosing x and testing $x, x+1, \ldots, x+k-1$ for membership in G, where $k = \left\lceil \frac{1}{2}\log_2 n \right\rceil$.

4. Open Questions

The obvious question is whether the randomized Ankeny conjecture is true. In section 1, we showed that if it is true, a deterministic Ankeny conjecture is already true. In section 2, we proved a very much weakened randomized Ankeny conjecture. Some conjecture in between should be explored. Once again, consider a proper subgroup G of $\mathbb{Z}_n^*$. Suppose that we restrict our attention to the situation where *all* prime divisors of n are nontrivial on G. The proofs of the results in section 1 don't work in this situation. The proofs of the results in section 2 don't exploit this situation. The subgroup used in the Solovay-Strassen prime test, discussed in section 3, is an example of this situation. This motivates the exploration of a randomized Ankeny conjecture restricted to this case.

Another open question is whether the half-cost of a randomized algorithm, discussed briefly in this paper, has any interesting properties. Pseudo-random number generators are usually analyzed with respect to cryptographic security, making certain intractability assumptions, e.g. that factoring is "hard." However, pseudo-random number generators are used in randomized algorithms. So we should explore connections between intractability assumptions, pseudo-random number generators, and half-costs.

References

[AMM] L. Adleman, K. Manders and G. Miller, "On taking roots in finite fields," *Proc. 1977 FOCS.*

[B1] E. Bach, "Realistic analysis of some randomized algorithms," *Proc. 1987 ACM STOC.*

[B2] E. Bach, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms,* MIT Press (1985).

[HW] G. H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press (1983).

[I] H. Iwaniec, "On the problem of Jacobsthal," *Demonstratio Mathematica* **11**, 1 (1978) 225–231.

[K] E. Kranakis, "Primality tests," Yale University Computer Science Department Report #345 (1984).

[KT] D. Knuth and L. Trabb Pardo, "Analysis of a simple factorization algorithm," *Theoretical Computer Science* **3** (1976) 321–348.

[M] G. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and System Sciences* **13** (1976) 300–317.

[SS] R. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," *SIAM Journal on Computing* **6** (1977) 84–85.