MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 174
APRIL 1986, PAGES 691–701

Fast Primality Tests for Numbers Less Than $50 \cdot 10^9$

By G. C. Kurtz, Daniel Shanks and H. C. Williams*

Abstract. Consider the doubly infinite set of sequences $A(n)$ given by

$$A(n+3) = rA(n+2) - sA(n+1) + A(n)$$

with $A(-1) = s$, $A(0) = 3$, $A(1) = r$. For a given pair $\{r, s\}$, the "signature" of n is defined to be the sextet

$$A(-n-1),\ A(-n),\ A(-n+1),\ A(n-1),\ A(n),\ A(n+1),$$

each reduced modulo n. Primes have only three types of signatures, depending on how they split in the cubic field generated by $x^3 - rx^2 + sx - 1$. An "acceptable" composite is a composite integer which has the same type of signature as a prime; such integers are very rare. In this paper, a description is given of the results of a computer search for all acceptable composites $\leqslant 50 \cdot 10^9$ in the Perrin sequence ($r = 0, s = -1$). Also, some numbers which are acceptable composites for both the Perrin sequence and the sequence with $r = 1$, $s = 0$ are presented.

1. Introduction. Let $\{r, s\}$ be a pair of rational integers that occur as the coefficients in the cubic function

$$f(x) = x^3 - rx^2 + sx - 1. \tag{1}$$

For a given pair, define the cubic recurrence $A(n)$ for $n = \ldots, -2, -1, 0, 1, 2, \ldots$ by

$$\begin{aligned} &A(-1) = s, \quad A(0) = 3, \quad A(1) = r, \quad \text{and} \\ &A(n+3) = rA(n+2) - sA(n+1) + A(n), \quad \text{or} \\ &A(n) = sA(n+1) - rA(n+2) + A(n+3). \end{aligned} \tag{2}$$

If the discriminant d of $f(x)$ is not zero, one has, explicitly,

$$A(n) = \alpha^n + \beta^n + \gamma^n, \tag{3}$$

where α, β and γ are the three distinct roots of $f(x) = 0$. Four examples that have the smallest discriminants in absolute value ($\neq 0$) are those given by

$$\begin{array}{rcccc} \{r,s\} = & \{0,-1\}, & \{1,0\}, & \{1,-1\}, & \{-1,-2\} \quad \text{for} \\ d = & -23, & -31, & -44, & +49, \end{array} \tag{4}$$

respectively.

In their elaborate [1], Adams and Shanks treat these sequences (2) and their possible use in primality tests. Their treatment is general, but most of the numerical work there concerns the first three cases in (4): $d = -23, -31, -44$. The present note is a sequel to [1] that answers some of the questions raised there. We refer the reader

Received May 31, 1985; revised July 15, 1985.
1980 *Mathematics Subject Classification.* Primary 10A25, 10A35, 10--04.
*Research supported by NSERC of Canada grant #A7649.

to [1] for much material that we do not examine or repeat here. We confine ourselves here to $d = -23$ and -31.

The case $\{0, -1\}$ for $d = -23$ is called *Perrin's sequence* in [1] because of Perrin's 1899 note [2] which examined this $A(n)$ for $n > 0$. We also call it Perrin's sequence here although it does have an earlier history. Specifically, in 1876 Lucas [3] already discussed this $A(n)$ for $n > 0$ and proved that

$$n \mid A(n) \tag{5}$$

if n is a prime, so (5) is a *necessary* condition for primality. If, *in addition*,

$$n \nmid A(m) \quad \text{for every } 0 < m < n, \tag{6}$$

then Lucas showed that (6) and (5) constitute a *sufficient* condition for primality. But (6) is clearly not an efficient test; it has no practical value.

Note that (6) is *not* a necessary condition since, e.g.,

$$223 \mid A(112)$$

is found in [1, p. 298]. Likewise, (5) is *not* a sufficient condition since, e.g.,

$$521^2 = 271441 \mid A(271441)$$

is given in [1, p. 255].

To strengthen and simplify these tests, [1] proceeds as follows: First, unlike [3] and [2], $A(n)$ is also extended backwards for $n = 0, -1, -2, \ldots$, as we give it in (2). Next, (5) is rewritten as

$$A(n) \equiv A(1) \pmod{n}$$

and then generalized to

$$A(-n) \equiv A(-1), \qquad A(n) \equiv A(1), \pmod{n}. \tag{7}$$

This double test is valid for every prime n and any $A(n)$ in (2). It strengthens the single test (5); e.g., 271441, which is the *smallest* composite that satisfies (5), fails to satisfy the left side of (7). Next, [1] gives a simple $O(\log n)$ algorithm for computing the sextet:

$$A(-n-1),\ A(-n),\ A(-n+1),\ A(n-1),\ A(n),\ A(n+1) \pmod{n}. \tag{8}$$

This is called the *signature* of n. It enables us to make the double test (7) very quickly. The four additional numbers in (8) contain further useful information.

Every prime $n = p$ will have *exactly one* out of only three possible types of prime signatures. These are the *S signature*:

$$A(-2),\ A(-1),\ A(0),\ A(0),\ A(1),\ A(2), \pmod{n}$$

which we may give explicitly as

$$s^2 - 2r,\ s, 3, 3,\ r,\ r^2 - 2s, \pmod{n}, \tag{9}$$

the *I signature*:

$$r,\ s,\ D',\ D,\ r,\ s, \pmod{n}, \tag{10}$$

and the *Q signature*:

$$A,\ s,\ B,\ B,\ r,\ C, \pmod{n}, \tag{11}$$

where A, B, C, D', and D must satisfy certain specific congruences. For example, in Perrin's sequence, $p = 23$ and 59 have an S signature, $p = 3$ and 13 have an I

signature, and $p = 5$ and 7 have a Q signature. We call these three types of primes S primes, I primes, and Q primes, respectively. Of course, all three signatures contain

(12) $\qquad$ ———, s, ———, ———, r, ———

since all primes satisfy (7).

We note that an S prime also satisfies

(13) $$(d/p) \neq -1,$$

so in Perrin's sequence, with $d = -23$, every S prime satisfies

(13a) $$p \equiv 0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16 \text{ or } 18 \pmod{23}.$$

For any $A(n)$, we say that n has an *acceptable signature* for that $A(n)$ if it has an S signature, (9) and (13); or an I signature (10); or a Q signature (11). Clearly, that is not a *complete* definition since we have not stated (here) what the aforementioned congruences are for A, B, ... They are given in [1], but luckily, in our results below, we *do not need these congruences* so, for brevity, we do not repeat them here. Of course, the immediate question is this: Given an $A(n)$, does any *composite* n have an acceptable signature? For the Perrin sequence the answer is "yes". In [1], we saw that

(14) $$T_1 = 27664033 = 3037 \cdot 9109$$

satisfies (9) and (13a), and therefore has an S signature. We call a composite an *acceptable composite* if it has an acceptable signature. We learn below that (14) is the smallest acceptable composite for the Perrin sequence.

We knew, a priori, that composites with acceptable signatures must be *very rare*. Four reasons for this were given in [1, Section 4]. There are two different sieves defined there that can sieve out large classes of composite n that cannot satisfy (12) and, *ipso facto*, cannot be acceptable composites. Indeed, we used these sieves in the computations described in Section 5 below to determine *all* acceptable composites $\leqslant 50 \times 10^9$ in Perrin's sequence. We found:

Fact 1. Up to 50×10^9 there are only 55 acceptable composites for Perrin's sequence. That is, up to that limit, only one composite out of about 870 million composites is acceptable. This confirms the characterization in the title of [1]: these are strong primality tests.

In fact, our results are even stronger, but to understand them we must first understand S primes.

2. The S Primes and S Composites. The S primes play a very special role in the cubic fields generated by (1). We have

(15) They are the primes p that split completely in the cubic fields so that we have

(15a) $$x^3 - rx^2 + sx - 1 \equiv (x - a)(x - b)(x - c) \pmod{p}.$$

Equivalently, we have

(16) $$A(n) \bmod p \text{ has a period that divides } p - 1.$$

We also have

(17) For all discriminants d not equal to a square, such as our $d = -23$, -31 and -44 above, the S primes have an asymptotic density of $1/6$.

For Perrin's sequence the S primes, and they alone, may be represented as

$$p = a^2 + 23b^2, \tag{18}$$

while for $\{r, s\} = \{1, 0\}$ with $d = -31$ we have

$$p = a^2 + 31b^2. \tag{18a}$$

It is a striking result in [1] that while the S primes have a density of only $1/6$ and while it is easy to construct acceptable composites, such as (14), that have S signatures, *no* acceptable composite was constructed there for Perrin's sequence that has a Q or I signature, even though Q and I primes, taken together, are five times as numerous as the S primes. It was even suggested in [1] that Q or I type acceptable composites may not exist in Perrin's sequence!

We established in Fact 1 that acceptable composites are very rare in this sequence, and a second motivation for the present investigation was to verify that all acceptable composities $\leqslant 50 \cdot 10^9$ have S signatures. That is true; we found

Fact 2. If any $n \leqslant 50 \cdot 10^9$ has a Perrin signature containing

$$\text{\_\_\_\_\_}, -1, \text{\_\_\_\_\_}, \text{\_\_\_\_\_}, 0, \text{\_\_\_\_\_}, \tag{19}$$

this being the appropriate special case of (12), and if its signature is *not* a Perrin S signature:

$$1, -1, 3, 3, 0, 2, \tag{20}$$

then n is a prime; i.e., n is a Q or I prime.

This strong formulation makes it unnecessary in the present paper to repeat all the details of the Q and I signatures. We mentioned this omission in the discussion above after (13a). The minimal test (19) suffices to establish the primality of these numbers.

There are two kinds of S-type acceptable composites constructed in [1]. The Carmichael type is a Carmichael number where each of its prime factors is an S prime. The smallest example is

$$C_1 = 7045248121 = 821 \cdot 1231 \cdot 6971$$

where

$$821 = 27^2 + 23 \cdot 2^2, \quad 1231 = 32^2 + 23 \cdot 3^2, \quad 6971 = 18^2 + 23 \cdot 17^2.$$

It follows from (16) that such a Carmichael number has an S signature, and since it also satisfies (13) it is acceptable.

There are 2163 Carmichael numbers $\leqslant 25 \cdot 10^9$ (see [4]) but only two of them have S primes for each prime divisor. The second is

$$C_2 = 7279379941 = 211 \cdot 3571 \cdot 9661.$$

This great rarity (2 out of 2163) stems from the fact that S primes have an asymptotic density of $1/6$, and, for small primes, the local density is even smaller (only 23 and 59 are S primes for the 24 odd primes < 100) and yet each Carmichael number must have at least three distinct prime divisors.

Next, we generalize the O_i and T_i in [1] and define the *generalized Owings type*. Suppose

$$N = p_1 p_2 \tag{21}$$

for two S primes

$$p_1 = ck + 1 \quad \text{and} \quad p_2 = dk + 1 \tag{22}$$

for which the periods of $A(n) \bmod p_1$ and $A(n) \bmod p_2$ *both* divide k. Then (16) implies that N is an acceptable composite with an S signature. We designate this N as

$$N = (k.cd), \tag{23}$$

where in all our examples below we allow one digit for c and two for d. Thus T_1 in (14) is

$$T_1 = (3036.103)$$

while

$$O_1 = 46672291 = (4830.102)$$

is the second smallest acceptable composite for the Perrin sequence.

If $c = 1$, the requirement that $A(n) \bmod p_1$ have a period dividing k is automatically satisfied. In the O_i type in [1], here designated as $(k.102)$, it was indicated that the probability that the period of $A(n) \bmod p_2$ divides k is $\frac{1}{4}$. Subsequently [5], that probability of $\frac{1}{4}$ was proven rigorously. Therefore, if we have any two primes

$$p_1 = k + 1, \qquad p_2 = 2k + 1,$$

the probability that N is acceptable is $1/144$ since each p must be an S prime.

In [1], we listed C_1 and C_2 and there is only one more C_i less than $50 \cdot 10^9$. In [1] we listed all seven $O_i = (k.102) \leqslant 25 \cdot 10^9$ and there are five more $\leqslant 50 \cdot 10^9$. In [1] we listed all five $T_i = (k.103) \leqslant 10^9$ and there are nine more $\leqslant 50 \cdot 10^9$. There are 25 additional $(k.cd)$ with $.cd \neq .102$ or $.103$ that are less than $50 \cdot 10^9$. None of these were given in [1]; the smallest is

$$517697641 = 6311 \cdot 82031 = (6310.113).$$

These $3 + 12 + 14 + 25$ acceptable composites $\leqslant 50 \cdot 10^9$ comprise 54 out of the 55 composites referred to in Fact 1.

All 55 are listed in Table 1. The only new type is found in #38. It is

$$N = 24306384961 = 19 \cdot 53 \cdot 79 \cdot 89 \cdot 3433. \tag{24}$$

This N has an S signature (20) and satisfies (13). It is, in fact, a Carmichael number, but it is doubly fortuitous that it satisfies (13) and (20). While 3433 is an S prime, the four small factors are all Q primes, see [1, p. 298]. Therefore, the periods of $A(n) \bmod p$ do *not* divide $p - 1$. The four periods are 180, 1404, 3120, and 3960, respectively, and so it is just luck that these four periods all divide $N - 1$ and that N thereby has an S signature. Further, Q primes satisfy $(d/p) = -1$, not (13), and it was only because we have an even number of Q factors that (13) is satisfied.

No doubt other new (and freakish) types will occur beyond $50 \cdot 10^9$, but the main point in this section is that all acceptables $\leqslant 50 \cdot 10^9$ have S signatures. Therefore, Perrin's sequence gives us a very easy, efficient and elegant *sufficient* test for all Q and I primes $\leqslant 50 \cdot 10^9$. These comprise 5/6 of all primes $\leqslant 50 \cdot 10^9$.

TABLE 1

#	Composite	Factorization	(k.cd)	In [1]
1	27664033	(3037)(9109)	(3036.103)	T_1
2	46672291	(4831)(9661)	(4830.102)	O_1
3	102690901	(5851)(17551)	(5850.103)	T_2
4	130944133	(6607)(19819)	(6606.103)	T_3
5	517697641	(6311)(82031)	(6310.113)	
6	545670533	(13487)(40459)	(13486.103)	T_4
7	801123451	(8951)(89501)	(8950.110)	
8	855073301	(16883)(50647)	(16882.103)	T_5
9	970355431	(22027)(44053)	(22026.102)	O_2
10	1235188597	(17573)(70289)	(17572.104)	
11	3273820903	(40459)(80917)	(40458.102)	O_6
12	3841324339	(25303)(151813)	(25302.106)	
13	3924969689	(25577)(153457)	(25576.106)	
14	4982970241	(26681)(186761)	(26680.107)	
15	5130186571	(50647)(101293)	(50646.102)	O_7
16	5242624003	(51199)(102397)	(51198.102)	O_8
17	6335800411	(33941)(186671)	(16970.211)	
18	7045248121	(821)(1231)(6971)	carmichael	C_1
19	7279379941	(211)(3571)(9661)	carmichael	C_2
20	7825642579	(55949)(139871)	(27974.205)	
21	8118449281	(52021)(156061)	(52020.103)	
22	8236954057	(30253)(272269)	(30252.109)	
23	9085378147	(47659)(190633)	(47658.104)	
24	10563944161	(59341)(178021)	(59340.103)	
25	11821223041	(62773)(188317)	(62772.103)	
26	12883213201	(42901)(300301)	(42900.107)	
27	13677931541	(67523)(202567)	(67522.103)	
28	13955714701	(44651)(312551)	(44650.107)	
29	14735895301	(85837)(171673)	(85836.102)	O_9
30	15391036351	(48661)(316291)	(24330.213)	
31	16283099827	(63803)(255209)	(63802.104)	
32	17044925633	(75377)(226129)	(75376.103)	
33	18301178501	(55229)(331369)	(55228.106)	
34	18321066191	(55259)(331549)	(55258.106)	
35	19267579361	(80141)(240421)	(80140.103)	
36	19862784913	(53269)(372877)	(53268.107)	
37	20913703903	(102259)(204517)	(102258.102)	O_{10}
38	24306384961	(19)(53)(79)(89)(3433)	carmichael *	
39	24918616339	(49919)(499181)	(49918.110)	
40	26448696913	(61469)(430277)	(61468.107)	
41	27811217611	(149161)(186451)	(37290.405)	
42	28427760433	(75403)(377011)	(75402.105)	
43	30713796101	(101183)(303547)	(101182.103)	
44	33209126521	(50543)(657047)	(50542.113)	
45	33996510721	(106453)(319357)	(106452.103)	
46	36056194453	(134269)(268537)	(134268.102)	
47	39283248493	(125353)(313381)	(62676.205)	
48	39675460001	(115001)(345001)	(115000.103)	
49	43234580143	(223)(5107)(37963)	carmichael	
50	43522383061	(147517)(295033)	(147516.102)	
51	46353274003	(152239)(304477)	(152238.102)	
52	46690026571	(152791)(305581)	(152790.102)	
53	46713465109	(65167)(716827)	(65166.111)	
54	47529840403	(154159)(308317)	(154158.102)	
55	47813279821	(89269)(535609)	(89268.106)	

Most of the entries in Table 1 are $(k.cd)$ examples. Let us note that they are easy to factor. Given such an N, compute

$$X_m = \sqrt{4mN}$$

for $m = 2, 3, 4$ out to a moderate limit until X_m is nearly an integer; e.g., for #5 in the table

$$X_{13} = \sqrt{52 \cdot 517697641} \approx 164074.000$$

so $m = 13 = c \times d$. Then, a short calculation gives its factors.

3. Perrin's Sequence and Secundo. We have just seen that Perrin's sequence gives us a simple, sufficient test for the (approximately) 1763 million Q and I primes $< 50 \cdot 10^9$. For the (approximately) 352 million S primes $< 50 \cdot 10^9$ the test is not quite sufficient since there are the 55 composites listed in Table 1. An *inelegant* but *practical* test for the S primes is obvious: Any $n < 50 \cdot 10^9$ that has a Perrin signature (20) and is not listed in Table 1 is an S prime. (We need not even check that (13a) holds.) Probably we could even reduce the algorithm a little; e.g., if we already knew, by a preliminary test, that n had no proper divisor < 225 we could delete the three composites in Table 1 divisible by 19, 211 or 223 for a table-lookup.

Now consider the second $A(n)$ listed in (4), that with $\{r, s\} = \{1, 0\}$ and $d = -31$. As we shall see in the next section, there is more than one $\{r, s\}$ having $d = -31$, and more than one with $d = -23$. It is desirable to have a name for $\{1, 0\}$ and we will call it Secundo. We have not examined Secundo for all $n \leqslant 50 \cdot 10^9$—we would be pleased if one of our readers would undertake that. Nonetheless, it seems probable that Secundo would be somewhat similar to Perrin as stated in Facts 1 and 2 above.

As regards the number of acceptable composites in these two sequences, we do know this: if we go out to

$$n \leqslant 250 \cdot 10^{12}, \tag{25}$$

which is 5000 times as large as $50 \cdot 10^9$, Perrin has 736 acceptable composites of type $(k.102)$ or $(k.103)$ while Secundo has 753—nearly equal. But, for some unknown reason, Secundo starts much more slowly: up to $50 \cdot 10^9$ Perrin has 26 while Secundo has only 7. So, up to $50 \cdot 10^9$, Secundo appears to be an even stronger test than Perrin. As regards Fact 2, it is quite possible that all composites acceptable for Secundo that are $< 50 \cdot 10^9$ have S signatures also, but we do not know that for a fact.

Now, returning to sufficient tests for S primes, we can also use

Fact 3. None of the 55 composites in Table 1 has an acceptable signature for Secundo; in fact, it does not even have a signature containing

$$\text{\_\_\_\_\_}, 0, \text{\_\_\_\_\_}, \text{\_\_\_\_\_}, 1, \text{\_\_\_\_\_}. \tag{26}$$

Put it another way: No composite $\leqslant 50 \cdot 10^9$ is acceptable for both Perrin and Secundo. How far out is this true? What is the smallest composite acceptable in both sequences? We do not know the answer unequivocally but it probably is

$$2277740968903 = 1067179 \cdot 2134357 \tag{27}$$

which exceeds two trillion. We obtain that supposition from the following argument.

If $(k.102)$ is acceptable for Perrin, the probability that it is also acceptable for Secundo is $1/144$. We computed all acceptable $(k.102)$ for Perrin that are $< 250 \cdot 10^{12}$. (That is quite easy to do.) There are 428 of them. Therefore, we expect that about 3 of them will be found among the 416 examples for Secundo. There are, in fact, exactly four coincidences:

$$\begin{array}{l} 2277740968903, \\ 41012029710541, \\ 173536465910671, \\ 198789706573921, \end{array} \tag{28}$$

the first of which is (27).

If $(k.103)$ is acceptable for Perrin, the probability that it is acceptable for Secundo is only $1/324 = 1/6 \cdot 6 \cdot 9$. So, among the 308 $(k.103) < 250 \cdot 10^{12}$ acceptable for Perrin, we should expect that about one will be found among the 337 examples for Secundo. There is exactly one:

$$197529618183301 = 8114383 \cdot 24343147. \tag{29}$$

Incidentally, the ratio of 308 $(k.103)$ to 428 $(k.102)$ in Perrin is close to the predicted ratio in [1, p. 273]:

$$\frac{308}{428} = 0.720 \approx \frac{8}{9}\sqrt{\frac{2}{3}} = 0.726. \tag{30}$$

Now, other $(k.cd)$, as seen in Table 1, occur less frequently than $(k.102)$ and $(k.103)$, and their corresponding probabilities of being acceptable in Secundo are much smaller; e.g., the $(k.213)$ in #30 would have a probability of only $1/24336$. So, it is perhaps unlikely that any such composite will be smaller than that in (27) and that is true also for the rarer Carmichael type. Thus, it is fairly probable that (27) is the smallest example.

An exercise for any computer-loving reader: Find the smallest Carmichael number of the form:

$$N = (6m + 1)(12m + 1)(18m + 1)$$

that is acceptable for both Perrin and Secundo. See [1, p. 274].

4. Other $A(n)$. To sum up at this point: Perrin is a sufficient test for all primes < 27664033 and for all Q and I primes (5/6 of the primes) $< 50 \cdot 10^9$. Our main question is whether we can extend, or even delete, this last bound. Perrin and Secundo, taken together, are sufficient for all primes $< 50 \cdot 10^9$ and perhaps for all primes < 2277740968903. If both sequences are free from Q- and I-type acceptable composites, then they would suffice for 35/36ths of all primes; i.e., for all primes except those that are S in both sequences.

One can envisage adding a third $A(n)$ and presumably the three would suffice up to, say, 10^{18} or 10^{19}, etc. We are not seriously pursuing that program here but we should make some comments about a third $A(n)$, a fourth, etc.

First, we should avoid any $A(n)$ that has a square discriminant such as $\{-1, -2\}$ with $d = 49$. These cyclic cubic fields have an S prime density of $1/3$, not $1/6$, and therefore will have a much larger number of acceptable composites. Such $A(n)$ may well be of theoretical interest but we will avoid them here.

Obviously, we should avoid any (1) which is not irreducible since these offer no cubic field whatsoever.

An interesting type of $A(n)$ we should avoid arose in a discussion with William Adams. Suppose $\{r, s\}$ is some $A(n)$. Then by

(31) $$\{r, s\}_m \quad \text{we mean} \quad \{A(m), A(-m)\}.$$

Therefore, $\{r, s\}_1$ is the original $A(n)$ whereas (31) is the subsequence

(32) $$\ldots A(-2m),\ A(-m),\ A(0),\ A(m),\ A(2m), \ldots.$$

It is easily seen that (31) and $\{r, s\}$ have the same cubic field. If d is the polynomial discriminant of (1) then that for (31) is some square multiple of d:

(33) $$d_m = (s_m)^2 d.$$

Consider Perrin $= \{0, -1\}$. Then, one finds that

(34) $$s_m = 1 \quad \text{for } m = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 9$$

so there are no less than 12 $A(n)$ for which (1) has the discriminant -23. In contrast,

$$s_{\pm 6} = 5, \quad s_{\pm 7} = 8, \quad s_{\pm 8} = 7, \quad s_{\pm 10} = 19,$$

and s_m grows rapidly for larger m.

Of course, the cubic field discriminant remains -23 for all m. Likewise, for all m, the primes remain distributed into the same sets S, I, and Q. (There would be a minor complication for those primes that divide s_m.) The reader can verify that in Secundo we have

(35) $$s_m = 1 \quad \text{for } m = \pm 1, \pm 2, \pm 3, \text{ and } \pm 5$$

so here we have eight $A(n)$ with $d = -31$.

All these $A(n)$ with $|m| > 1$ should be avoided whether $s_m = 1$ or not. Consider $\{0, -1\}_2 = \text{Perrin}_2$. Since it equals

$$\ldots A(-4),\ A(-2),\ A(0),\ A(2),\ A(4), \ldots$$

every S prime p will have a period that divides $(p - 1)/2$. Whereas, in Perrin, the probability of such a period is only $1/4$. Therefore $\{0, -1\}_2$ should have about four times as many acceptable (k.102) as Perrin has, or, about 1700 examples $< 250 \cdot 10^{12}$. Likewise, $\{0, -1\}_3$ will have nine times as many (k.103) or, about 2700 examples $< 250 \cdot 10^{12}$. And $\{0, -1\}_6$ will have *both* the 1700 (k.102) and the 2700 (k.103).

In Perrin ($m = 1$) or Perrin reversed ($m = -1$) the real x that is a root of (1) is a *fundamental unit* of the cubic field while all $|m| > 1$ will have solutions that are powers x^m of that fundamental unit. Secundo is also a fundamental unit.

The next $A(n)$ in (4) is $\{1, -1\}$ with $d = -44$. This is also a fundamental unit. For the reader's convenience we list the next four with negative discriminants. These also are fundamental.

d	r	s
−59	2	0
−76	3	1
−83	2	−2
−87	2	−1

For $d > 0$, even excluding the cyclic $d = s^2$, there are interesting possibilities since there is a *pair* of fundamental units, and infinitely many units may be selected as one of the units in a fundamental pair. Thus, the five sequences

$$\{4,-5\},\ \{7,6\},\ \{30,-11\},\ \{12,7\},\ \{-2,-3\} \tag{36}$$

all have $d = 257$ and all are fundamental. Although the S, Q and I primes are identical in all five sequences, they will have differing sets of acceptable composites. Thus $\{4,-5\}$, and it alone, has 22 with an S signature. (It is an unusual type, not found in Table 1, since both 2 and 11 are I primes.)

Now return to the Q- and I-type composites. Clearly, we prefer that our $A(n)$ have none. We could not construct such a composite for Perrin and, as stated, one motive for the present paper was to verify that there are none $< 50 \cdot 10^9$. Such composites were constructed for some *other* $A(n)$ in [1, p. 297], in [6] and in Adams' new paper [7]. But, if c is the composite, usually the d of $A(n)$ is $O(c^4)$ and, further, if we attempt to minimize $|d|$, then d usually turns out to be positive. Thus, for any large c so constructed, it is unlikely that d will be small and negative such as -23, $-31, \ldots, -87$.

We do have an amusing "counterexample" for an $A(n)$ that we have already discarded. For $\text{Perrin}_4 = \{2,-3\}$, one finds that 4 is an acceptable composite with an I signature. And this $A(n)$ has $d = -23$, as we saw in (34). But this c is very small (it is hard to find a smaller one) and perhaps this example is exceptional and signifies nothing.

5. Calculations. Here is how we did Perrin to $50 \cdot 10^9$ and thereby obtained Facts 1, 2 and 3. As we mentioned earlier, by using the doubling rule given in [1], it is easy to show that only $O(\log n)$ division and multiplication operations are needed to compute the signature of any given n. However, if one is looking at a large number of n's for which the signature is to be determined, the total amount of computer time required can be prohibitive. Thus, we made use of the results of Section 4 of [1] to sieve out many values of n which could not have an acceptable Perrin signature. In this section we briefly describe how this was done.

Let $\{A(n)\}$ be any sequence given by (2). For any prime p, we must, at some point, find an m such that

$$A(m) \equiv A(0),\quad A(m+1) \equiv A(1),\quad A(m+2) \equiv A(2) \pmod{p}. \tag{37}$$

The least positive value of m for which (37) holds is called the *period* of p and is denoted by $W(p)$. If p is an S prime, then $W(p) \mid p - 1$; if p is a Q prime, $W(p) \mid p^2 - 1$, and, if p is an I prime, $W(p) \mid p^2 + p + 1$. In [1] it is shown that if

$$mp = kW(p)p + p^n, \tag{38}$$

where $k = 0, 1, 2, \ldots$ and $n = 1, 2, \ldots$, then

$$A(-mp) \equiv A(-1) \quad \text{and} \quad A(mp) \equiv A(1) \pmod{p}. \tag{39}$$

Indeed, we can restrict n to $n \leqslant 1, 2, 3$ for p an S, Q or I prime, respectively. It is also proved in [1] that if $c = mp$ and p is either a Q or an I prime, then (39) can hold *only* for mp given by the form (38). Unfortunately, this result does not hold for p an S prime. A value of m for which (39) is true but (38) is not is called an *outsider*. However, for a given sequence and a given small prime p, it is a relatively

simple matter to determine whether there are any outsiders. For, if there is one, then there must be some outsider $k < W(p) \leqslant p - 1$, and this is easy to determine by a direct search when p is small. For the S primes needed in our work, we determined that there were no outsiders in the Perrin sequence case.

The composites up to $50 \cdot 10^9$ were sieved by running routines written in ASSEMBLER language on an AMDAHL 580 model 5850 Computer. These routines utilize decimal arithmetic as a convenient way of handling any quadruple precision calculations that are necessary. The address of the current segment of composites (represented by 10^6 1-byte flags) is passed to each of these routines.

By a precomputation, we determined, for each of the first 4770 primes (the primes $\leqslant p_{4770} = 46099$), the corresponding period $W(p)$ for the Perrin sequence. These primes have the property that their period can be stored in a single precision word of storage. For each $p \leqslant 46099$, the first sieve routine removes all multiples of p and then restores all multiples of the form $kW(p)p + p^n$ with $n \leqslant 1, 2, 3$ for p an S, Q or I prime, respectively. By using the high-order 4 bits of each flag as the previous state of the current array, this routine remembers not to restore any composite c which has been previously sieved by a different prime p.

Since no integer of the form mp with $m \leqslant 40$ and p a prime can be an acceptable composite [1], our second sieve removes all such integers from our array. After these two sieves had been used, it was necessary to find the signatures for only 0.3% of all integers $\leqslant 50 \cdot 10^9$. Our routines were executed on segments of 10^6 numbers at a time. The average time needed to complete our computations on each segment was about 30 seconds. After all these calculations had been performed, only the 55 composite numbers given above were found to have acceptable Perrin signatures.

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

Department of Mathematics
University of Maryland
College Park, Maryland 20742

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canad R3T 2N2

1. W. ADAMS & D. SHANKS, "Strong primality tests that are not sufficient," *Math. Comp.*, v. 35, 1982, pp. 225–300.

2. R. PERRIN, Item 1484, *L'Intermédiaire des Math.*, v. 6, 1899, pp. 76–77.

3. E. LUCAS, "Sur la recherche des grands nombres premiers," *A. F. Congrès du Clermont-Ferrand*, 1876, pp. 61–68.

4. C. POMERANCE, J. L. SELFRIDGE & S. S. WAGSTAFF, JR., "The pseudoprimes to 25,000,000,000," *Math. Comp.*, v. 35, 1980, pp. 1003–1026.

5. D. SHANKS, "Prime-splitting in associated cubic and quartic fields: Some implications and some techniques." (To appear.)

6. W. ADAMS & D. SHANKS, "Strong primality tests. II–Algebraic identification of the p-adic limits and their implications." (To appear.)

7. W. ADAMS, "Characterizing pseudoprimes for third order linear recurrences." (To appear.)