Verifying Sierpiński and Riesel Numbers in ACL2

John R. Cowles Ruben Gamboa
Department of Computer Science
University of Wyoming
Laramie, Wyoming, USA
cowles@cs.uwyo.edu ruben@cs.uwyo.edu

A *Sierpiński number* [4, page 420] and [1], is an odd positive integer, k, such that no positive integer in this infinite list is prime:

$$k2^1+1, k2^2+1, k2^3+1, \ldots, k2^n+1, \ldots. \tag{1}$$

A *Riesel number* [1] is similar to a Sierpiński number, with -1 replacing $+1$ in the above infinite list. Such a number is an odd positive integer, k, so that no positive integer in this infinite list is prime:

$$k2^1-1, k2^2-1, k2^3-1, \ldots, k2^n-1, \ldots.$$

A *cover*, for such a k, is a finite list of positive integers such that each integer, j, in the appropriate infinite list, has a factor, d, in the cover, with $1 < d < j$.

Given a k and its cover, ACL2 is used to systematically verify that each integer, in the appropriate infinite list, has a smaller factor in the cover.

1 Introduction

Sierpiński and Riesel numbers are not easy to find. To disqualify an odd positive integer as a Sierpiński number or a Riesel number, one need only locate a prime in the appropriate infinite list. With four exceptions, $k = 47, 103, 143, 197$, all of the first 100 odd positive integers, $1 \leq k \leq 199$, are disqualified as Sierpiński numbers by finding at least one prime in the first eight elements of the infinite list [3]:

$$k2^1+1, k2^2+1, k2^3+1, \ldots, k2^8+1.$$

Both $k = 103$ and $k = 197$ are eliminated by finding a prime in the list no later than $k2^{16}+1$ [3], leaving 47 and 143 as the only possible Sierpiński numbers less than 200. It turns out that $143 \cdot 2^{53}+1$ and $47 \cdot 2^{583}+1$ are prime [3], eliminating them. Thus, there are no Sierpiński numbers in the range $1 \leq k \leq 199$. The situation is similar for Riesel numbers.

In 1960, W. Sierpiński [7] proved, for

$$k = 15511380746462593381,$$

every member in the infinite list, given by (1), is divisible by one of the prime factors of the first six Fermat numbers. For nonnegative integer, n, the *Fermat number*, F_n, is given by

$$F_n = 2^{2^n}+1.$$

The first five Fermat numbers are prime and F_5 is the product of two primes:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537,$$

Hardin and Schmaltz (Eds): ACL2 2011
EPTCS 70, 2011, pp. 20–27, doi:10.4204/EPTCS.70.2

$$F_5 = 4294967297 = 641 \cdot 6700417.$$

Thus $(3\ 5\ 17\ 257\ 641\ 65537\ 6700417)$ is a cover for $k = 155113807464625933 81$, showing it to be a Sierpiński number. Sierpiński's original proof is described in [8, page 374] and [2].

In 1962, J. Selfridge (unpublished) proved that 78557 is a Sierpiński number by showing that

$$(3\ 5\ 7\ 13\ 19\ 37\ 73)$$

is a cover [6]. Later, in 1967, Selfridge and Sierpiński conjectured that 78557 is the smallest Sierpinski number [6]. The distributed computing project Seventeen or Bust [6] is devoted to proving this conjecture, disqualifying every $k < 78557$, by finding an n that makes $k \cdot 2^n + 1$ prime. For example, $19249 \cdot 2^{13018586} + 1$, a 3918990-digit prime, eliminated 19249 [9]. When this project started in 2002, all but 17 values of k had already been disqualified. Currently six values of k remain to be eliminated.

Earlier, in 1956, but less well known than Sierpiński's work, H. Riesel [5] showed 509203 is a Riesel number with cover $(3\ 5\ 7\ 13\ 17\ 241)$. It is possible for the same odd positive integer to be both a Sierpiński number and a Riesel number. An example [1] is $k = 14366558304535079309 8657$.

2 Covers Into ACL2 Proofs

Given an odd positive integer, k, with a Sierpiński cover, $\mathscr{C}$, here is the process used to verify that k is a Sierpiński number. There is a similar process for verfying Riesel numbers from their covers.

1. For each d in $\mathscr{C}$, find positive integer b_d and nonnegative integer c_d so that for every nonnegative integer i, d is a factor of $k \cdot 2^{b_d \cdot i + c_d} + 1$.

   In practice, every d in $\mathscr{C}$ is an odd prime smaller than k.

   (a) Search for positive integer b such that d is a factor of $2^b - 1$. Since d is an odd prime, it turns out that such a b will always exist[1] among $1, 2, \ldots, d-1$. Let b_d be the first[2] such b.

   (b) Search for nonnegative integer c such that d is a factor of $k \cdot 2^c + 1$. If such a c exists, then one exists among $0, 1, \ldots, b_d - 1$. Let c_d be the first[3] such c, if it exists.

   (c) Assuming c_d exists, use induction on i, to prove that for every nonnegative integer i, d is a factor of $k \cdot 2^{b_d \cdot i + c_d} + 1$.

   The base case, when $i = 0$, follows from 1b above.

   The induction step, going from $i = j$ to $i = j + 1$, follows from 1a above:

   $$k2^{b_d(j+1)+c_d} + 1 = [k2^{b_d j + c_d} \cdot (2^{b_d} - 1)] + [k2^{b_d j + c_d} + 1] \tag{2}$$

   By 1a, d is a factor of the left summand of (2) and d is a factor of the right summand by the induction hypothesis.

2. For each positive integer n, find d in $\mathscr{C}$ and nonnegative integer i so that $n = b_d \cdot i + c_d$. If such d and i exist, then, by 1c, d is a factor of $k \cdot 2^{b_d \cdot i + c_d} + 1 = k \cdot 2^n + 1$.

   To ensure that such d and i exist for every positive n, only a finite number of cases need be considered: Let ℓ be the least common multiple of all the b_d's found for the d's in $\mathscr{C}$. Check for each

   $$n \in \{0, 1, 2, \ldots, \ell - 1\},$$

[1] For the mathematically literate: The well-known Fermat's Little Theorem ensures the claimed existence.

[2] Thus, being mathematically precise, b_d is just the order of 2 in the multiplicative group of the integers modulo d.

[3] If d does not divide k, then $2^{c_d} \equiv -(1/k) \pmod{d}$, so c_d is the *discrete logarithm*, base 2, of $-(1/k)$ in the integers modulo d.

that there always is a d in $\mathscr{C}$ that satisfies the equation

$$\mathrm{mod}\,(n, b_d) = c_d.$$

This process has not been formally verified in ACL2. For example, we don't bother to check that every member of $\mathscr{C}$ is an odd prime. Instead, for each individual k and $\mathscr{C}$, ACL2 events are generated that would prove k is a Sierpiński number, if all the events succeed. If some of the events fail, then, as usual when using ACL2, further study of the failure is required, in the hope of taking corrective action. The generation of these events is controlled by the macros `verify-sierpinski` and `verify-riesel`. These macros take three arguments: the name of a witness function that will find a factor for a given $k2^n \pm 1$, the number k that is a Sierpiński or Riesel number, and the cover $\mathscr{C}$ for k. The macros then generate the proof, following the plan outlined in this section.

For each d in $\mathscr{C}$, b_d and c_d from 1a and 1b, are computed. They are needed to define the witness function and to state the theorems mentioned in 1c, which are then proved. For example, the proof that 78557 is a Sierpiński number defines this witness function:

```
(DEFUN WITNESS (N)
 (IF (INTEGERP N)
     (COND ((EQUAL (MOD N 2) 0) 3)
           ((EQUAL (MOD N 4) 1) 5)
           ((EQUAL (MOD N 3) 1) 7)
           ((EQUAL (MOD N 12) 11) 13)
           ((EQUAL (MOD N 18) 15) 19)
           ((EQUAL (MOD N 36) 27) 37)
           ((EQUAL (MOD N 9) 3) 73))
     0))
```

The rightmost numbers, in this definition, form the cover, the corresponding b_d's are the leftmost numbers, and the middle numbers are the c_d's. So $\mathscr{C} = (3\ 5\ 7\ 13\ 19\ 37\ 73)$, $b_{73} = 9$, and $c_{73} = 3$.

The theorem, from 1c, for $d = 73$ is

```
(DEFTHM WITNESS-LEMMA-73
 (IMPLIES (AND (INTEGERP N)
               (>= N 0))
          (DIVIDES 73
                   (+ 1
                      (* 78557
                         (EXPT 2
                               (+ 3
                                  (* 9 N)))))))
 :HINTS ...)
```

Four properties are proved about the witness function, establishing 78557 is a Sierpiński number:

```
(DEFTHM WITNESS-NATP
 (AND (INTEGERP (WITNESS N))
      (<= 0 (WITNESS N)))
 :HINTS ...)
```

```
(DEFTHM WITNESS-GT-1
 (IMPLIES (INTEGERP N)
          (< 1 (WITNESS N)))
 :HINTS ...)

(DEFTHM WITNESS-LT-SIERPINSKI
 (IMPLIES (AND (INTEGERP N)
               (<= 0 N))
          (< (WITNESS N)
             (+ 1 (* 78557 (EXPT 2 N))))))

(DEFTHM WITNESS-DIVIDES-SIERPINSKI-SEQUENCE
 (IMPLIES (AND (INTEGERP N)
               (<= 0 N))
          (DIVIDES (WITNESS N)
                   (+ 1 (* 78557 (EXPT 2 N)))))
 :HINTS ...)
```

As suggested above in 2, these properties can be proved by showing every integer is "covered" by one of the cases given in the COND-expression used in the definition of the witness function.

```
(DEFTHM WITNESS-COVER-ALL-CASES
 (IMPLIES (INTEGERP N)
          (OR (EQUAL (MOD N 2) 0)
              (EQUAL (MOD N 4) 1)
              (EQUAL (MOD N 3) 1)
              (EQUAL (MOD N 12) 11)
              (EQUAL (MOD N 18) 15)
              (EQUAL (MOD N 36) 27)
              (EQUAL (MOD N 9) 3)))
 :RULE-CLASSES NIL
 :HINTS ...)
```

To prove this, we first demonstrate that these cases are exhaustive when n is replaced by $\mathrm{mod}\,(n,36)$ (where 36 is the least common multiple of all the moduli above). This can be checked, essentially, by computation.

```
(DEFTHM WITNESS-COVER-ALL-CASES-MOD-36
 (IMPLIES (INTEGERP N)
          (OR (EQUAL (MOD (MOD N 36) 2) 0)
              (EQUAL (MOD (MOD N 36) 4) 1)
              (EQUAL (MOD (MOD N 36) 3) 1)
              (EQUAL (MOD (MOD N 36) 12) 11)
              (EQUAL (MOD (MOD N 36) 18) 15)
              (EQUAL (MOD (MOD N 36) 36) 27)
              (EQUAL (MOD (MOD N 36) 9) 3)))
 :RULE-CLASSES NIL
 :HINTS ...)
```

The actual modular equivalences that need to be proved depend on both the number 78557 and its cover. Although the theorem that is being proved is obviously true, there does not appear to be a way to prove it once and for all in ACL2, not even using `encapsulate`. Instead, a pair of theorems very much like the ones we have described needs to be proved from scratch for each different Sierpiński or Riesel number. As experienced ACL2 users, we are concerned that ACL2 will simply fail to prove this theorem for some combination of numbers and their covers. However, we have used these macros to generate the proof for each of the Sierpiński and Riesel numbers *with covers* listed in the appendix, and all of the proofs have gone through automatically. Note that the appendix essentially[4] contains all the Sierpiński and Riesel numbers known to us.

3 Numbers Without Covers

There are odd positive integers, shown to be Sierpiński (or Riesel) numbers, that have no known covers. ACL2 proofs have been constructed for these numbers.

For example [1], $k = 4008735125781478102999926000625$ is a Sierpiński number, but no (complete) cover is known. For all positive integer, n, if $\mod(n,4) \neq 2$, then $k \cdot 2^n + 1$ has a factor among the members of $(3\ 17\ 97\ 241\ 257\ 673)$. To show k is a Sierpiński number, a factor of $k \cdot 2^n + 1$ must be found for all positive integer, n, such that $\mod(n,4) = 2$. Such a factor is constructed using these facts:

- $k = 44745755^4$ is a fourth power
- $4x^4 + 1 = (2x^2 + 2x + 1) \cdot (2x^2 - 2x + 1)$

Let $i = 44745755$, so $k = i^4$. Then

$$\begin{aligned} k \cdot 2^{4n+2} + 1 &= 2^2 (i \cdot 2^n)^4 + 1 \\ &= 4(i \cdot 2^n)^4 + 1 \\ &= [2(i \cdot 2^n)^2 + 2(i \cdot 2^n) + 1] \cdot [2(i \cdot 2^n)^2 - 2(i \cdot 2^n) + 1] \end{aligned} \tag{3}$$

The left factor of (3) algebraically reduces to show

$$4004365181040050 \cdot 2^{2\lfloor n/4 \rfloor} + 89491510 \cdot 2^{\lfloor n/4 \rfloor} + 1$$

is a factor of $k \cdot 2^n + 1$, whenever $\mod(n,4) = 2$.

A Riesel number, k, with no known cover, is given in Appendix A. In this example, $k = a^2$ is a square and

$$\begin{aligned} k \cdot 2^{2n} - 1 &= a^2 \cdot 2^{2n} - 1 \\ &= (a2^n)^2 - 1 \\ &= (a2^n + 1) \cdot (a2^n - 1) \end{aligned}$$

shows how to factor $k \cdot 2^m - 1$ when m is even and positive. A (partial) cover, listed in Appendix A, gives a constant factor for each $k \cdot 2^m - 1$, when m is odd and positive.

[4] Given a Sierpiński or Riesel number k and its cover $\mathscr{C}$, infinitely many other examples can be constructed: Let P be the product of the numbers in $\mathscr{C}$ and let i be a positive integer. Then $k + 2 \cdot i \cdot P$ is also a Sierpiński or Riesel number with the same cover.

4 Conclusions

Given a Sierpiński or Riesel number, k, and its cover, we have described ACL2 macros that generate events verifying that each integer, in the appropriate infinite list, has a smaller factor in the cover.

For the few known Sierpiński or Riesel numbers with no known covers, hand-crafted ACL2 proofs have been constructed verifying that each integer, in the appropriate infinite list, has a smaller factor.

References

[1] Michael Filaseta, Carrie Finch & Mark Kozek (2008): *On Powers Associated with Sierpiński Numbers, Riesel Numbers and Polignac's Conjecture*. *Journal of Number Theory* 128, pp. 1916–1940.

[2] Lenny Jones (2011): *When Does Appending the Same Digit Repeatedly on the Right of a Positive Integer Generate a Sequence of Composite Integers?* *American Mathematical Monthly* 118, pp. 153–160.

[3] *Website: The On-Line Encyclopedia of Integer Sequences*. `http://oeis.org/A046067`.

[4] Clifford Pickover (2009): *The Math Book*. Sterling Publishing, New York.

[5] Hans Riesel (1956): *Några Stora Primtal (Swedish: Some Large Primes)*. *Elementa* 39, pp. 258–260.

[6] *Website: Seventeen or Bust*. `www.seventeenorbust.com`. A Distibuted Attack on the Sierpinski Problem.

[7] Waclaw Sierpiński (1960): *Sur un Problème Concernant les Nombres $k \cdot 2^n + 1$*. *Elem. Math.* 15, pp. 73–74. Corrigendum, *ibidem*, 17:85, 1962.

[8] Waclaw Sierpiński (1987): *Elementary Theory of Numbers*. PWN–Polish Scientific Publishers and Elsevier Science Publishers, Warszawa and Amsterdam. Second English edition revised and enlarged by A. Schinzel.

[9] *Website: The Sierpiński Problem: Definition and Status*. `www.prothsearch.net/sierp.html`.

A Sierpiński and Riesel Numbers

Numbers, k, verified with ACL2.

Each k with a cover $\mathscr{C}$ is either mentioned in the References or claimed at various websites. Numbers k without known covers are from [1].

Smallest known Sierpiński number

$k = 78557 = 17 \cdot 4621$, a product of two primes

$\mathscr{C} = (3\ 5\ 7\ 13\ 19\ 37\ 73)$

Smallest known prime Sierpiński number

$k = 271129$

$\mathscr{C} = (3\ 5\ 7\ 13\ 17\ 241)$

More Sierpiński numbers

k	$\mathscr{C}$
271577	(3 5 7 13 17 241)
322523	(3 5 7 13 37 73 109)
327739	(3 5 7 13 17 97 257)
482719	(3 5 7 13 17 241)
575041	(3 5 7 13 17 241)
603713	(3 5 7 13 17 241)
903983	(3 5 7 13 17 241)
934909	(3 5 7 13 19 73 109)
965431	(3 5 7 13 17 241)
1259779	(3 5 7 13 19 73 109)
1290677	(3 5 7 13 19 37 109)
1518781	(3 5 7 13 17 241)
1624097	(3 5 7 13 17 241)
1639459	(3 5 7 13 17 241)
1777613	(3 5 7 13 17 19 109 433)
2131043	(3 5 7 13 17 241)

Smallest Sierpiński number found by Sierpiński

$k = 155113807464625933 81$

$\mathscr{C} = (3\ 5\ 17\ 257\ 641\ 65537\ 6700417)$

Smallest known Riesel number

$k = 509203$

$\mathscr{C} = (3\ 5\ 7\ 13\ 17\ 241)$

More Riesel numbers

k	$\mathscr{C}$
762701	(3 5 7 13 17 241)
777149	(3 5 7 13 19 37 73)
790841	(3 5 7 13 19 37 73)
992077	(3 5 7 13 17 241)

Numbers both Sierpiński and Riesel

$\mathscr{C}_R$ indicates the Riesel number cover and $\mathscr{C}_S$ indicates the Sierpiński number cover.

$k = 143665583045350793098657$

$\mathscr{C}_R = (3\ 5\ 13\ 17\ 97\ 241\ 257)$

$\mathscr{C}_S = (3\ 7\ 11\ 19\ 31\ 37\ 61\ 73\ 109\ 151\ 331\ 1321)$

$k = 47867742232066880047611079$

$\mathscr{C}_R = (3\ 7\ 11\ 19\ 31\ 37\ 41\ 61\ 73\ 109\ 151\ 331)$

$\mathscr{C}_S = (3\ 5\ 13\ 17\ 97\ 241\ 257)$

$k = 878503122374924101526292469$
$\mathscr{C}_R = (3\ 7\ 13\ 19\ 37\ 73\ 97\ 109\ 241\ 257)$
$\mathscr{C}_S = (3\ 5\ 11\ 17\ 31\ 41\ 61\ 151\ 331\ 61681)$

$k = 3872639446526560168555701047$
$\mathscr{C}_R = (3\ 7\ 13\ 19\ 37\ 73\ 97\ 109\ 241\ 673)$
$\mathscr{C}_S = (3\ 5\ 11\ 17\ 31\ 41\ 61\ 151\ 331\ 61681)$

$k = 623506356601958507977841221247$
$\mathscr{C}_R = (3\ 7\ 13\ 19\ 37\ 73\ 97\ 109\ 241\ 673)$
$\mathscr{C}_S = (3\ 5\ 17\ 257\ 641\ 65537\ 6700417)$

Sierpiński numbers without cover

$k = 400873512578147810299992600625 = 44745755^4$
$(3\ 17\ 97\ 241\ 257\ 673)$ is partial cover for $\mod(n,4) \neq 2$.
$4004365181040050 \cdot 2^{2\lfloor n/4 \rfloor} + 89491510 \cdot 2^{\lfloor n/4 \rfloor} + 1$
is a factor of $k \cdot 2^n + 1$, whenever $\mod(n,4) = 2$.

$k = 7341106150007 75^4$
$(3\ 17\ 257\ 641\ 65537\ 6700417)$ is partial cover for $\mod(n,4) \neq 2$.
$10778367901136321929065012012 50 \cdot 2^{2\lfloor n/4 \rfloor} + 1468221230001550 \cdot 2^{\lfloor n/4 \rfloor} + 1$
is a factor of $k \cdot 2^n + 1$, whenever $\mod(n,4) = 2$.

Riesel number without cover

Let $a = 389684530387388117515931462080888704606697246980 9$ and let $k = a^2$.
The list
$(7\ 17\ 31\ 41\ 71\ 97\ 113\ 127\ 151\ 241\ 257\ 281\ 337\ 641\ 673\ 1321\ 14449\ 29191\ 65537\ 6700417)$
is partial cover for odd positve n.
$a \cdot 2^{n/2} + 1$ is a factor of $k \cdot 2^n - 1$, whenever n is positive and even.