Verifying Sierpiński and Riesel Numbers in ACL2

John Cowles

Ruben Gamboa

University of Wyoming

cowles@cs.uwyo.edu

ruben@cs.uwyo.edu

k is a **Sierpiński number**:

- k is an odd positive integer
- no prime in this infinite list

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

A **Riesel number** is similar to a Sierpiński number, with -1 replacing $+1$ in the above infinite list.

k is a **Riesel number**:

- k is an odd positive integer
- no prime in this infinite list

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

A **Sierpiński number** is an odd k:
No prime in this list

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

A **Riesel number** is an odd k:
No prime in this list

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

$\mathcal{C}$ is a **cover** for such a k:

- $\mathcal{C}$ is a finite list of positive integers

- each integer, j, in the appropriate infinite list,

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

  has a factor, d, in $\mathcal{C}$, with $1 < d < j$

Given a k and its cover $\mathcal{C}$, use ACL2 to verify that each integer, in the appropriate infinite list, has a smaller factor in $\mathcal{C}$.

Sierpiński and Riesel numbers are not easy to find.

To disqualify an odd positive integer as a Sierpiński number or a Riesel number:

- 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:

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

Both $k = 103$ and $k = 197$ are eliminated by finding a prime in the list no later than $k2^{16} + 1$, leaving 47 and 143 as the only possible Sierpiński numbers less than 200.

$143 \cdot 2^{53} + 1$ is prime.

$47 \cdot 2^{583} + 1$ is prime.

Thus, there are no Sierpiński numbers in the range $1 \leq k \leq 199$.

The situation is similar for Riesel numbers.

W. Sierpiński proved (1960), for

$$k = 155113807464625933 81,$$

every member in the infinite list,

$$k2^1 + 1, k2^2 + 1, k2^3 + 1, \ldots, k2^n + 1, \ldots,$$

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

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

F_5 is the product of two primes:

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

Thus (3 5 17 257 641 65537 6700417) is a cover for $k = 155113807464625933 81$, showing it to be a Sierpiński number.

J. Selfridge proved (1962) that 78557 is a Sierpiński number

- (3 5 7 13 19 37 73) is a cover

Selfridge and Sierpiński conjectured (1967) that 78557 is the smallest Sierpinski number.

The distributed computing project
Seventeen or Bust

- devoted to proving 78557 is the smallest Sierpinski number.
- disqualify every $k < 78557$ by finding an n that makes $k \cdot 2^n + 1$ prime.
- When started in 2002, all but 17 values of k had already been disqualified.
- Currently six values of k remain to be eliminated.

For example, 19249 was eliminated:

- $19249 \cdot 2^{13018586} + 1$ is prime
- 3918990 digits in this prime

H. Riesel showed (1956) 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 is
$k = 1436655830453507930986 57$.

Covers Into ACL2 Proofs

Given an odd positive integer, k, with a Sierpiński cover, $\mathcal{C}$, 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 $\mathcal{C}$, find positive integer b_d and nonnegative integer c_d so that for every nonnegative integer i, d is a factor of $k \cdot 2^{b_d \cdot i + c_d} + 1$.

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

1. For each d in $\mathcal{C}$, 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 $\mathcal{C}$ 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 among $1, 2, \ldots, d-1$. Let b_d be the first 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 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 $k \cdot 2^{b_d \cdot i + c_d} + 1$.

2. For each positive integer n, find d in $\mathcal{C}$ and nonnegative integer i so that $n = b_d \cdot i + c_d$. If such d and i exist, then 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 $\mathcal{C}$. Check for each

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

   that there always is a d in $\mathcal{C}$ 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 $\mathcal{C}$ is an odd prime.

Instead, for each individual k and $\mathcal{C}$, 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
- the cover $\mathcal{C}$ for k

The macros then generate the proof, following the plan just outlined

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))
```

- rightmost numbers form the cover $\mathcal{C} = (3\ 5\ 7\ 13\ 19\ 37\ 73)$

- leftmost numbers are the b_d's: $b_{73} = 9$

- middle numbers are the c_d's: $c_{73} = 3$

A theorem for $d = 73 \in \mathcal{C}$ is

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

Here $b_{73} = 9$ and $c_{73} = 3$.

The proof is by induction.

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 ...)
```

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 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 ...)
```

We are concerned that ACL2 will simply fail for some combination of numbers and their covers.

We have used these macros to generate the proof for each of the 34 Sierpiński and Riesel numbers *with covers* listed in the appendix of our paper.

All of the proofs have gone through automatically.

Note that the appendix essentially contains all the Sierpiński and Riesel numbers known to us.

Some ACL2 verified Sierpiński Numbers

k	$\mathcal{C}$
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)

There are Sierpiński and Riesel numbers with no known covers.

$k = 44745755^4$ and $k = 7341106150007 75^4$ are both Sierpiński number, but no covers are known.

Let $a =$

389684530387388117515931462080888704606697246980 9

and let $k = a^2$. Then k is a Riesel number with no known cover

ACL2 proofs have been constructed for these 3 numbers.