# Perfect Numbers in ACL2

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

A **perfect number** is a positive integer $n$ such that $n$ equals the sum of all positive integer divisors of $n$ that are less than $n$. That is, although $n$ is a divisor of $n$, $n$ is excluded from this sum. Thus $6 = 1+2+3$ is perfect, but $12 \neq 1+2+3+4+6$ is not perfect. An ACL2 theory of perfect numbers is developed and used to prove, in ACL2(r), this bit of mathematical folklore: Even if there are infinitely many perfect numbers, the series below, of the reciprocals of all perfect numbers, converges.

$$\sum_{\text{perfect } n} \frac{1}{n}$$

## 1 Perfect Numbers

The smallest perfect numbers are $6 = 2 \cdot 3 = 2^1(2^2-1)$, $28 = 4 \cdot 7 = 2^2(2^3-1)$, $496 = 16 \cdot 31 = 2^4(2^5-1)$, $8128 = 64 \cdot 127 = 2^6(2^7-1)$. In each of these examples, the second factor, $3, 7, 31, 127$, of the form $2^k - 1$, is a prime. The Greek Euclid proved [2, page 3]:

**Theorem 1** *If $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ is perfect.*

Primes of the form $2^k - 1$ are called **Mersenne primes**. Thus every new Mersenne prime leads to a new perfect number. According to Wikipedia [5], less than 50 Mersenne primes are known. The largest known Mersenne prime is $2^{57,885,161} - 1$, making $2^{57,885,160}(2^{57,885,161} - 1)$ the largest known perfect number, with over 34 million digits. It is not known if there are infinitely many Mersenne primes, nor if there are infinitely many perfect numbers.

All perfect numbers built from Mersenne primes are even. The Swiss Euler proved every **even** perfect number is built from some Mersenne prime [2, page 10]:

**Theorem 2** *If $n$ is an even perfect number, then $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime.*

It is not known if there are any odd perfect numbers, but Euler also proved [6, page 250]:

**Theorem 3** *If $n$ is an odd perfect number, then $n = p^i m^2$, where $p$ is prime and $i$, $p$, $m$ are odd.*

ACL2 is used to verify each of these three theorems.

If there are only finitely many perfect numbers, then clearly the series

$$\sum_{\text{perfect } n} \frac{1}{n}$$

converges. ACL2(r) is used to verify that even if there are **infinitely many perfect numbers**, the series converges.

M. Kaufmann and D. Rager (Eds.): ACL2 Workshop 2015 (ACL2 2015).
EPTCS 192, 2015, pp. 53–59, doi:10.4204/EPTCS.192.5

## 2 The ACL2 Theory

In number theory, for positive integer $n$, $\sigma(n)$ denotes the sum of **all** (including $n$) positive integer divisors of $n$. The function $\sigma(n)$ has many useful properties, so the definition of a perfect number is reformulated in terms of $\sigma$ [2, pages 8–9]:

$$\text{perfect}(n) \text{ if and only if } \sigma(n) = 2n$$

.

These six properties of $\sigma$ are among those formulated and proved in ACL2:

1. $p$ is prime if and only if $\sigma(p) = p+1$.
2. If $p$ is prime, then $\sigma(p^k) = \sum_{i=0}^{k} p^i = \frac{p^{k+1}-1}{p-1}$.
3. If $p$ and $q$ are different primes, then $\sigma(p \cdot q) = \sigma(p) \cdot \sigma(q)$.
4. $\sigma(k \cdot n) \leq \sigma(k) \cdot \sigma(n)$
5. If $\gcd(k,n) = 1$, then $\sigma(k \cdot n) = \sigma(k) \cdot \sigma(n)$.
6. If $p$ is prime, then $\gcd(p^k, \sigma(p^k)) = 1$.

If $n = 2^i(2^{i+1}-1)$ is an even perfect number, then the exponent $i$ is computed by an ACL2 term, `(cdr (odd-2^i n))`, that returns the largest value of $i$ such that $2^i$ divides $n$.

If $n = p^i m^2$ is an odd perfect number, then $p, i, m$ are respectively computed by the ACL2 terms

- ```
  (car (find-pair-with-odd-cdr
         (prime-power-factors n)))
  ```

- ```
  (cdr (find-pair-with-odd-cdr
         (prime-power-factors n)))
  ```

- ```
  (product-pair-lst (pairlis$ (strip-cars
                               (remove1-equal
                                (find-pair-with-odd-cdr
                                 (prime-power-factors n))
                                (prime-power-factors n)))
                              (map-nbr-product
                               1/2
                               (strip-cdrs
                                (remove1-equal
                                 (find-pair-with-odd-cdr
                                  (prime-power-factors n))
                                 (prime-power-factors n))))))
  ```

These terms implement the following computation:

1. Factor $n = \prod_{j=0}^{k} p_j^{e_j}$ into the product of powers of distinct odd primes.
2. Exactly one of the exponents, say $e_0$, will be odd and all the other exponents will be even.
3. $p$ is the prime with the odd exponent and $i$ is the unique odd exponent. So $n = p^i \cdot \prod_{j=1}^{k} p_j^{2f_j}$.
  ```

4. Then $m = \prod_{j=1}^{k} p_j^{f_j}$ and $n = p^i m^2$.

ACL2 is used to verify a result of B. Hornfeck, that different odd perfect numbers, $n_1 = p_1^{i_1} m_1^2 \neq n_2 = p_2^{i_2} m_2^2$ have distinct $m_i$ [6, page 251]:

**Theorem 4** *If $n_1 = p_1^{i_1} m_1^2$ and $n_2 = p_2^{i_2} m_2^2$ are odd perfect numbers and $m_1 = m_2$, then $n_1 = n_2$.*

Theorems 2, 3, and 4 are enough to prove the folklore that the series, of the reciprocals of all perfect numbers, converges.

# 3 ACL2(r)

ACL2(r) [3] is based on **Nonstandard Analysis** [7, 4] which provides rigorous foundations for reasoning about real, complex, infinitesimal, and infinite quantities. There are two versions of the **reals**

1. The **Standard Reals**, ${}^{\mathrm{st}}\mathbb{R}$, is the unique **complete** ordered field. This means that
   - Every nonempty subset of ${}^{\mathrm{st}}\mathbb{R}$ that is bounded above has a **least upper bound**.

   There are no non-zero infinitesimal elements, nor are there are any infinite elements in ${}^{\mathrm{st}}\mathbb{R}$.
2. The **HyperReals**, ${}^{\star}\mathbb{R}$, is a proper field extension of ${}^{\mathrm{st}}\mathbb{R}$: ${}^{\mathrm{st}}\mathbb{R} \subsetneq {}^{\star}\mathbb{R}$. There are non-zero infinitesimal elements and also infinite elements in ${}^{\star}\mathbb{R}$.

Here are some technical definitions.

- $x \in {}^{\star}\mathbb{R}$ is **infinitesimal**: For all positive $r \in {}^{\mathrm{st}}\mathbb{R}$, $(|x| < r)$.
  0 is the only infinitesimal in ${}^{\mathrm{st}}\mathbb{R}$.
  `(i-small x)` in ACL2(r).
- $x \in {}^{\star}\mathbb{R}$ is **finite**: For some $r \in {}^{\mathrm{st}}\mathbb{R}$, $(|x| < r)$.
  `(i-limited x)` in ACL2(r).
- $x \in {}^{\star}\mathbb{R}$ is **infinite**: For all $r \in {}^{\mathrm{st}}\mathbb{R}$, $(|x| > r)$.
  `(i-large x)` in ACL2(r)
- $x, y \in {}^{\star}\mathbb{R}$ are **infinitely close**, $x \approx y$: $x - y$ is infinitesimal.
  `(i-close x y)` in ACL2(r).
- $\mathfrak{n}_\infty$ is an infinite positive integer constant.
  `(i-large-integer)` in ACL2(r).

Every (partial) function $f : {}^{\mathrm{st}}\mathbb{R}^n \longmapsto {}^{\mathrm{st}}\mathbb{R}^k$ has an extension ${}^{\star}f : {}^{\star}\mathbb{R}^n \longmapsto {}^{\star}\mathbb{R}^k$ such that

1. For $x_1, \cdots, x_n \in {}^{\mathrm{st}}\mathbb{R}$, ${}^{\star}f(x_1, \cdots, x_n) = f(x_1, \cdots, x_n)$.
2. Every first-order statement about $f$ true in ${}^{\mathrm{st}}\mathbb{R}$ is true about ${}^{\star}f$ in ${}^{\star}\mathbb{R}$.

   Example.
   $(\forall x)[\sin^2(x) + \cos^2(x) = 1]$ is true in ${}^{\mathrm{st}}\mathbb{R}$.
   $(\forall x)[{}^{\star}\sin^2(x) + {}^{\star}\cos^2(x) = 1]$ is true in ${}^{\star}\mathbb{R}$.

Any (partial) function $f : {}^{\mathrm{st}}\mathbb{R}^n \longmapsto {}^{\mathrm{st}}\mathbb{R}^k$ is said to be **classical**.

- Identify a classical $f$ with its extension ${}^{\star}f$.
  That is, use $f$ for both the original classical function $f$ and its extension ${}^{\star}f$.

- Use $(\forall^{\mathrm{st}} x)$ for $(\forall x \in {}^{\mathrm{st}}\mathbb{R})$, i.e. "for all **standard** $x$."
  Use $(\exists^{\mathrm{st}} x)$ for $(\exists x \in {}^{\mathrm{st}}\mathbb{R})$, i.e. "there is some **standard** $x$."
- "$(\forall x)[\sin^2(x)+\cos^2(x)=1]$ is true in ${}^{\mathrm{st}}\mathbb{R}$" becomes "$(\forall^{\mathrm{st}} x)[\sin^2(x)+\cos^2(x)=1]$ is true in ${}^{\star}\mathbb{R}$."
  "$(\forall x)[{}^{\star}\sin^2(x)+{}^{\star}\cos^2(x)=1]$ is true in ${}^{\star}\mathbb{R}$" becomes "$(\forall x)[\sin^2(x)+\cos^2(x)=1]$ is true in ${}^{\star}\mathbb{R}$."

Numeric constants, $c$, are viewed as 0-ary functions, $c : {}^{\mathrm{st}}\mathbb{R}^0 \longmapsto {}^{\mathrm{st}}\mathbb{R}$ or $c : {}^{\star}\mathbb{R}^0 \longmapsto {}^{\star}\mathbb{R}$. Thus, elements of ${}^{\mathrm{st}}\mathbb{R}$, such as $2, 4, -1$, are classical. But elements of ${}^{\star}\mathbb{R} - {}^{\mathrm{st}}\mathbb{R}$, such as the infinite positive integer $\mathfrak{n}_\infty$, are not classical. Functions defined using the nonstandard concepts of infinitesimal, finite, infinite, and infinitely close are not classical.

Let $f$ be a (partial) unary function, whose domain includes the **nonnegative** integers, into the reals. Here are three possible definitions for the real series $\sum_{i=0}^{\infty} f(i)$ converges. The first two are versions of Weierstrass' traditional definition that the real series converges. One version for the standard reals, another version for the hyperreals.

1. `(defun-sk Series-Converges-Traditional-Standard ( )`
   $(\exists^{\mathrm{st}} L)(\forall^{\mathrm{st}} \varepsilon > 0)(\exists^{\mathrm{st}} \text{ integer } M > 0)(\forall^{\mathrm{st}} \text{ integer } n)(n > M \Rightarrow |\sum_{i=0}^{n} f(i) - L| < \varepsilon)$
   `)`
2. `(defun-sk Series-Converges-Traditional-Hyper ( )`
   $(\exists L)(\forall \varepsilon > 0)(\exists \text{ integer } M > 0)(\forall \text{ integer } n)(n > M \Rightarrow |\sum_{i=0}^{n} f(i) - L| < \varepsilon)$
   `)`
3. `(defun-sk Series-Converges-Infinitesimal ( )`
   $(\exists^{\mathrm{st}} L)(\forall \text{ infinite integer } n > 0)(\sum_{i=0}^{n} f(i) \approx L)$
   `)`

For **classical** $f$, ACL2(r) verifies these three definitions are equivalent. ACL2(r) also verifies for classical $f$, with **nonnegative** range, these definitions are equivalent to this nonstandard definition [1]:

- `(defun Series-Converges-Nonstandard ( )`
  $\sum_{i=0}^{\mathfrak{n}_\infty} f(i)$ is finite
  `)`
  Recall that the upper limit, $\mathfrak{n}_\infty$, on this $\sum_{i=0}^{\mathfrak{n}_\infty} f(i)$, is an infinite positive integer constant.

## 4 The Series Converges

Use the definition, `Series-Converges-Nonstandard`, to verify, in ACL2(r), the convergence of

$$\sum_{\mathrm{perfect}(k)} \frac{1}{k} = \sum_{\substack{k=1 \\ \mathrm{perfect}(k)}}^{\infty} \frac{1}{k}$$

by showing this sum is finite:

$$\sum_{\substack{k=1 \\ \mathrm{perfect}(k)}}^{\mathfrak{n}_\infty} \frac{1}{k}$$

Recall $\mathfrak{n}_\infty$ is an infinite positive integer constant.
Verify the previous sum is finite by showing both of the summands on the right side below are finite.

$$\sum_{\substack{k=1\\ \text{perfect}(k)}}^{\mathfrak{n}_\infty} \frac{1}{k} \;=\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ \text{even}(k)}}^{\mathfrak{n}_\infty} \frac{1}{k} \;+\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ \text{odd}(k)}}^{\mathfrak{n}_\infty} \frac{1}{k}$$

By Theorem 2, even perfect numbers, $k$, have the form $k = 2^i(2^{i+1}-1)$. Since $2^i(2^{i+1}-1) \geq 2^i$, $\frac{1}{2^i(2^{i+1}-1)} \leq \frac{1}{2^i}$. Induction on $n$ verifies $\sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$. Thus for any positive integer, $n$, including $n = \mathfrak{n}_\infty$:

$$0 \;\leq\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ \text{even}(k)}}^{n} \frac{1}{k} \;=\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ k=2^i(2^{i+1}-1)}}^{n} \frac{1}{2^i(2^{i+1}-1)} \;\leq\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ k=2^i(2^{i+1}-1)}}^{n} \frac{1}{2^i} \;\leq\; \sum_{i=0}^{n} \frac{1}{2^i} \;=\; 2 - \frac{1}{2^n} \;<\; 2$$

By Theorem 3, odd perfect numbers, $k$, have the form $k = p^i m^2$. Since $p^i m^2 \geq m^2$, $\frac{1}{p^i m^2} \leq \frac{1}{m^2}$. By Theorem 4, no square, $m^2$, appears more than once in

$$\sum_{\substack{k=1\\ \text{perfect}(k)\\ k=p^i m^2}}^{n} \frac{1}{m^2}$$

Induction on $n$ verifies $\sum_{m=1}^{n} \frac{1}{m^2} \leq 2 - \frac{1}{n}$, Thus for any positive integer, $n$, including $n = \mathfrak{n}_\infty$:

$$0 \;\leq\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ \text{odd}(k)}}^{n} \frac{1}{k} \;=\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ k=p^i m^2}}^{n} \frac{1}{p^i m^2} \;\leq\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ k=p^i m^2}}^{n} \frac{1}{m^2} \;\leq\; \sum_{m=1}^{n} \frac{1}{m^2} \;\leq\; 2 - \frac{1}{n} \;<\; 2$$

Therefore, for any positive integer, $n$, including $n = \mathfrak{n}_\infty$:

$$0 \;\leq\; \sum_{\substack{k=1\\ \text{perfect}(k)}}^{n} \frac{1}{k} \;=\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ \text{even}(k)}}^{n} \frac{1}{k} \;+\; \sum_{\substack{k=1\\ \text{perfect}(k)\\ \text{odd}(k)}}^{n} \frac{1}{k} \;<\; 2+2=4$$

and

$$\sum_{\substack{k=1\\ \text{perfect}(k)}}^{\mathfrak{n}_\infty} \frac{1}{k} \text{ is finite.}$$

The heart of this proof is that the partial sums

$$\sum_{\substack{k=1\\ \text{perfect}(k)}}^{n} \frac{1}{k}$$

are bounded above (by 4). This can be stated and carried out entirely in ACL2. The **Reals** and ACL2(r) are required to formally state and prove the series converges.

# A ACL2(r) Books

## A.1 prime-fac.lisp

Unique Prime Factorization Theorem for Positive Integers.
An ACL2 book as well as an ACL2(r) book.

## A.2 perfect.lisp

Perfect Positive Integers.
An ACL2 book as well as an ACL2(r) book.
Over 500 events, incrementally built Summer 2013 – Spring 2015.

## A.3 series1.lisp

The CLASSICAL series, Ser1, converges (to a STANDARD real L).

## A.4 series1a.lisp

The CLASSICAL NONNEGATIVE series, Ser1a, converges (to a STANDARD real L).

## A.5 sumlist-1.lisp

Some nice events from sumlist.lisp plus additional events.

## A.6 sum-recip-e-perfect.lisp

The sum of the RECIPROCALS of the EVEN PERFECT positive integers converges.

## A.7 sum-recip-o-perfect.lisp

The sum of the RECIPROCALS of the ODD PERFECT positive integers converges.

## A.8 sum-recip-perfect.lisp

The sum of the RECIPROCALS of the PERFECT positive integers converges.

# References

[1] John Cowles & Ruben Gamboa (2014): *Equivalence of the Traditional and Non-Standard Definitions of Concepts from Real Analysis*. In Freek Verbeek & Julien Schmaltz, editors: *Proceedings of the Twelfth International Workshop of the ACL2 Theorem Prover and its Applications (ACL2-2014)*, Vienna, Austria, pp. 89–100, doi:10.4204/EPTCS.152.8.

[2] William Dunham (1999): *Euler: The Master of Us All*. Mathematical Association of America.

[3] Ruben Gamboa (1999): *Mechanically Verifying Real-Valued Algorithms in ACL2*. Ph.D. thesis, University of Texas at Austin.

[4] Edward Nelson (1977): *Internal Set Theory: A New Approach to Nonstandard Analysis*. *Bulletin of the American Mathematical Society* 83, pp. 1165–1198, doi:10.1090/S0002-9904-1977-14398-X.

[5] (2015): *Perfect Number: From Wikipedia, the free encyclopedia*. Available at `en.wikipedia.org/wiki/Perfect_number`.

[6] Paul Pollack (2009): *Not Always Buried Deep: A Second Course in Elementary Number Theory*. American Mathmatical Society.

[7] Abraham Robinson (1966): *Non-Standard Analysis*. North-Holland Publishing Co.