Perfect Numbers in ACL2

John Cowles

Ruben Gamboa

University of Wyoming

perfect number n:

- n is a positive integer
- n equals the sum of all positive integer **proper** divisors of n.
  - k is **proper divisor** of n iff $k < n$ and $k \mid n$.
- $n = \sum_{\substack{k=1 \\ k|n}}^{n-1} k$
- Examples
  - $6 = 1 + 2 + 3$ is perfect
  - $12 \neq 1 + 2 + 3 + 4 + 6$ is **not** perfect

- The smallest perfect numbers:
  - $6 = 2 \cdot 3$
  - $28 = 4 \cdot 7$
  - $496 = 16 \cdot 31$
  - $8128 = 64 \cdot 127$

- Each first factor, $2, 4, 16, 64$, is a power of 2.

- Each second factor, $3, 7, 31, 127$, has the form $2^k - 1$.

- Each second factor, $3, 7, 31, 127$, is a **prime**.

The Greek Euclid proved:

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**.

- Every new Mersenne prime leads to a new perfect number.

Wikipedia:

- Less than 50 Mersenne primes are known.
- Largest known Mersenne prime is $2^{57,885,161} - 1$.
- Largest known perfect number, with over 34 million digits,

$$2^{57,885,160}(2^{57,885,161} - 1)$$

- Not known if there are infinitely many Mersenne primes.
- Not known if there are infinitely many perfect numbers.

- If there are only **finitely** many perfect numbers, then clearly the series below, of the reciprocals of all perfect numbers, converges.

- $$\sum_{\text{perfect } n} \frac{1}{n} = \frac{1}{6} + \frac{1}{28} + \frac{1}{496} + \frac{1}{8128} + \cdots$$

- An ACL2 theory of perfect numbers is used to state and prove, in ACL2(r):

  - Even if there are **infinitely** many perfect numbers, the series converges.

All perfect numbers built from Mersenne primes are even.

The Swiss Euler proved every **even** perfect number is built from some Mersenne prime:

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

No **odd** perfect numbers are known.

Euler also proved

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.*

The ACL2 Theory

- For positive integer n, the function $\sigma(n)$ has many useful properties.

- $\sigma(n)$ denotes the sum of **all** (including n) positive integer divisors of n.

- $\sigma(n) = \sum_{\substack{k=1 \\ k|n}}^{n} k$

- Reformulate definition of perfect number in terms of σ:

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

The ACL2 Theory

Some properties of σ 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 $\gcd(p^k, \sigma(p^k)) = 1$

The ACL2 Theory

$n = 2^i(2^{i+1} - 1)$ is an even perfect number

- the exponent i is computed by an ACL2 term
  - `(cdr (odd-2^i n))`
  - returns the largest value of i such that 2^i divides n

The ACL2 Theory

$n = p^i m^2$ is an odd perfect number

- the prime p and exponent i are 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)))`

The ACL2 Theory

$n = p^i m^2$ is an odd perfect number

- m is computed by the ACL2 term

- ```
  (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))))))
  ```
  ```

The ACL2 Theory

$n = p^i m^2$ is an odd perfect number

The three 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 $n = p^i m^2$.

The ACL2 Theory

ACL2 verifies each of the three theorems.

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

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

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.

The ACL2 Theory

ACL2 verifies a result of B. Hornfeck

- 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:

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 that the series, of the reciprocals of all perfect numbers, converges.

ACL2(r) is based on Nonstandard Analysis

Rigorous foundations for reasoning about real, complex, infinitesimal, and infinite quantities

- Two versions of the **reals**

  1. Standard Reals: ${}^{st}\mathbb{R}$

  2. HyperReals: ${}^{\star}\mathbb{R}$

- Standard Reals: ${}^{\mathrm{st}}\mathbb{R}$
  - The unique **complete** ordered field.

    . . . . . .

    Every nonempty subset of ${}^{\mathrm{st}}\mathbb{R}$ that is bounded above has a **least upper bound**
  - **No** non-zero infinitesimal elements
  - **No** infinite elements

- HyperReals: ${}^{\star}\mathbb{R}$
  - ${}^{\star}\mathbb{R}$ is a proper field extension of ${}^{\mathrm{st}}\mathbb{R}$

    $$ {}^{\mathrm{st}}\mathbb{R} \subsetneqq {}^{\star}\mathbb{R} $$
  - **Has** non-zero infinitesimal elements
  - **Has** infinite elements

- $x \in {}^{\star}\mathbb{R}$ is **infinitesimal**:
  For all positive $r \in {}^{\mathrm{st}}\mathbb{R}$, $(|x| < r)$

  0 is the only infinitesimal in ${}^{\mathrm{st}}\mathbb{R}$

- $x \in {}^{\star}\mathbb{R}$ is **finite**:
  For some $r \in {}^{\mathrm{st}}\mathbb{R}$, $(|x| < r)$

- $x \in {}^{\star}\mathbb{R}$ is **infinite**:
  For all $r \in {}^{\mathrm{st}}\mathbb{R}$, $(|x| > r)$

- $x, y \in {}^{\star}\mathbb{R}$ are **infinitely close**, $x \approx y$:
  $x - y$ is infinitesimal

- $\mathfrak{n}_{\infty}$ is an infinite positive integer constant.

Every (partial) function

$$f : {}^{\mathsf{st}}\mathbb{R}^n \longmapsto {}^{\mathsf{st}}\mathbb{R}^k$$

has an extension

$$^\star f : {}^\star\mathbb{R}^n \longmapsto {}^\star\mathbb{R}^k$$

such that

- For $x_1, \cdots, x_n \in {}^{\mathsf{st}}\mathbb{R}$
  ${}^\star f(x_1, \cdots, x_n) = f(x_1, \cdots, x_n)$

- Every first-order statement about f true in ${}^{\mathsf{st}}\mathbb{R}$ is true about ${}^\star f$ in ${}^\star\mathbb{R}$

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

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

Any (partial) function

$$f : {}^{\mathsf{st}}\mathbb{R}^n \longmapsto {}^{\mathsf{st}}\mathbb{R}^k$$

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 $(\forall^{\mathsf{st}} x)$ for $(\forall x \in {}^{\mathsf{st}}\mathbb{R})$
  i.e. "for all **standard** x"

  Use $(\exists^{\mathsf{st}} x)$ for $(\exists x \in {}^{\mathsf{st}}\mathbb{R})$
  i.e. "there is some **standard** x"

- $(\forall x)[\sin^2(x) + \cos^2(x) = 1]$ is true in ${}^{\mathsf{st}}\mathbb{R}$
  becomes $(\forall^{\mathsf{st}} x)[\sin^2(x) + \cos^2(x) = 1]$
  (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 are viewed as 0-ary functions.

Thus

- Elements of ${}^{\mathrm{st}}\mathbb{R}$ are classical

  $2, 4, -1$ are classical

- Elements of ${}^{\star}\mathbb{R} - {}^{\mathrm{st}}\mathbb{R}$ are **not** classical

  The infinite positive integer constant, $\mathfrak{n}_\infty$, is not classical

Functions defined using the nonstandard concepts of infinitesimal, finite, infinite, and infinitely close are not classical.

The real series $\sum_{i=0}^{\infty} f(i)$ converges.
Three proposed definitions:

1. `(defun-sk Series-Converges-Traditional-Standard ()`

$$(\exists^{\mathsf{st}} L)(\forall^{\mathsf{st}} \epsilon > 0)(\exists^{\mathsf{st}}\ \mathsf{int}\ M > 0)(\forall^{\mathsf{st}}\ \mathsf{int}\ n)$$
$$(n > M \Rightarrow |\sum_{i=0}^{n} f(i) - L| < \epsilon)$$

`)`

2. `(defun-sk Series-Converges-Traditional-Hyper ()`

$$(\exists L)(\forall \epsilon > 0)(\exists\ \mathsf{int}\ M > 0)(\forall\ \mathsf{int}\ n)$$
$$(n > M \Rightarrow |\sum_{i=0}^{n} f(i) - L| < \epsilon)$$

`)`

3. `(defun-sk Series-Converges-Infinitesimal ()`

$(\exists^{\mathsf{st}} L)(\forall\ \mathsf{infinite\ int}\ n > 0)(\sum_{i=0}^{n} f(i) \approx L)$
`)`

For **classical** f, ACL2(r) verifies these three definitions are equivalent

For classical f, with **nonnegative** range, these definitions are equivalent to this nonstandard definition:

- `(defun`
  `Series-Converges-Nonstandard ( )`
  $$\sum_{i=0}^{\mathfrak{n}_\infty} f(i) \text{ is finite}$$
)

  Recall $\mathfrak{n}_\infty$ is an infinite positive integer constant.

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

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

by showing this sum is finite:

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

Recall $\mathfrak{n}_\infty$ is an infinite positive integer constant.

Show both summands on the right side 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 $2^i(2^{i+1} - 1) \geq 2^i$, $\dfrac{1}{2^i(2^{i+1} - 1)} \leq \dfrac{1}{2^i}$.

Induction on n verifies $\sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$.

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

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

By Theorem 3, odd perfect numbers, k, have the form $k = p^i m^2$.

Since $p^i m^2 \geq m^2$, $\dfrac{1}{p^i m^2} \leq \dfrac{1}{m^2}$.

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 $n = \mathfrak{n}_\infty$:

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

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:

- 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.