Counting Perfect Polynomials

Enrique Treviño

joint work with U. Caner Cengiz and Paul Pollack

49th West Coast Number Theory
December 18, 2017

LAKE FOREST
COLLEGE

Caner

(a) Caner Cengiz

(b) Paul Pollack

Perfect Numbers

n is perfect if n is the sum of its proper divisors, i.e.

$$n = \sum_{\substack{d|n \\ d \neq n}} d$$

Examples:

$$\begin{aligned} 6 &= 1 + 2 + 3 \\ 28 &= 1 + 2 + 4 + 7 + 14 \\ 496 &= 1 + 2 + 4 + 8 + 16 + 31 + 31 \cdot 2 + 31 \cdot 4 + 31 \cdot 8 \\ 2^{p-1}(2^p - 1) &= 1 + 2 + 4 + \cdots + 2^{p-1} + (2^p - 1)\left(1 + 2 + 4 + \cdots + 2^{p-2}\right) \end{aligned}$$

for $2^p - 1$ prime (i.e., a Mersenne prime).

Polynomials Mod 2

- A polynomial mod 2 is one of the form

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

  where $a_i \in \{0, 1\}$.
- We consider the operation mod 2, i.e., $1 + 1 = 0, 0 + 1 = 1 + 0 = 1, 0 + 0 = 0$.
- For example

$$x^2 + 1 = x^2 + 2x + 1 = (x + 1)^2.$$

Perfect Polynomials Mod 2

- Let $\sigma(P)$ be the sum of the divisors of a polynomial P in mod 2.
- A polynomial is said to be perfect mod 2 if $\sigma(P) = P$.
- $x^2 + x = x(x+1)$, so

  $$\sigma(x^2 + x) = 1 + x + (x + 1) + x^2 + x = x^2 + x.$$

  So $x^2 + x$ is perfect.
- $$\sigma(x^2 + 1) = 1 + (1 + x) + (1 + x^2) = 1 + x + x^2,$$

  so $x^2 + 1$ is not perfect.

Family of perfect polynomials

Let $P(x) = (x(x+1))^{2^n-1}$. We'll show $\sigma(P) = P$.

- $$1 + x + x^2 + \cdots + x^{2^n-1} = \frac{x^{2^n} - 1}{x - 1} = \frac{x^{2^n} + 1}{x + 1} = (x+1)^{2^n-1}.$$
- $$1 + (1+x) + \cdots + (1+x)^{2^n-1} = \frac{(1+x)^{2^n} - 1}{x} = \frac{1 + x^{2^n} - 1}{x} = x^{2^n-1}.$$
- $$\sigma(P) = \sigma(x^{2^n-1})\sigma((x+1)^{2^n-1}) = (x+1)^{2^n-1} \cdot x^{2^n-1} = P.$$

Weirdo Perfects

Degree	Factorization into Irreducibles
5	$T(T+1)^2(T^2+T+1)$
	$T^2(T+1)(T^2+T+1)$
11	$T(T+1)^2(T^2+T+1)^2(T^4+T+1)$
	$T^2(T+1)(T^2+T+1)^2(T^4+T+1)$
	$T^3(T+1)^4(T^4+T^3+1)$
	$T^4(T+1)^3(T^4+T^3+T^2+T+1)$
15	$T^3(T+1)^6(T^3+T+1)(T^3+T^2+1)$
	$T^6(T+1)^3(T^3+T+1)(T^3+T^2+1)$
16	$T^4(T+1)^4(T^4+T^3+1)(T^4+T^3+T^2+T+1)$
20	$T^4(T+1)^6(T^3+T+1)(T^3+T^2+1)(T^4+T^3+T^2+T+1)$
	$T^6(T+1)^4(T^3+T+1)(T^3+T^2+1)(T^4+T^3+1)$

Figure: Perfect numbers not in the infinite family. Found by Canaday in 1941

Even and Odd Perfects

- We say that P is an even perfect if $x(x+1)|P$ and P is perfect.
- We say that P is odd otherwise.

Conjecture

All perfect polynomials are EVEN.

What did we know

Theorem (Canaday)

An odd perfect polynomial is a square.

Theorem (Gallardo-Rahavandrainy)

If A is an odd perfect polynomial, then it has at least 5 distinct irreducible factors. Moreover, the number of irreducible factors of A, counted with multiplicity, is at least 12.

What did we prove

Theorem (Cengiz-Enrique-Pollack)

The number of perfect polynomials of norm $\leq x$ is $O_\epsilon(x^{\frac{1}{12}+\epsilon})$ for every $\epsilon > 0$.

The norm of A is $2^{\deg A}$.

Theorem (Cengiz-Enrique-Pollack)

There are no odd perfect polynomials of degree ≤ 200, i.e., there are no odd perfect polynomials of norm $\leq 2^{200} \approx 1.6 \times 10^{60}$.

Theorem (Cengiz-Enrique-Pollack)

If A is a non-splitting perfect polynomial of degree ≤ 200, then A is one of Canaday's polynomials.

Main Tool

Lemma (Fundamental lemma)

Let M be a polynomial which is not perfect, and let $k \geq 2$ be a fixed positive integer. Let $x \geq 10$. Then there exists a constant C_k depending only on k, as well as a set $\mathcal{S}$ depending only on M, k and x, of cardinality bounded by $x^{C_k/\log\log x}$, with the following property: if A is a perfect polynomial of norm $\leq x$ for which

(a) *M is a unitary divisor of A: i.e., $A = MN$ with $\gcd(M, N) = 1$, and*

(b) *$N = A/M$ is k-free, i.e., $P^k \nmid N$ for any irreducible polynomial P,*

then A has a decomposition of the form $M'N'$, where

1. *M' is an element of $\mathcal{S}$,*
2. *M' and N' are unitary divisors of A,*
3. *both factors M' and N' are perfect,*
4. *N' is k-free,*
5. *M is a unitary divisor of M'.*

Algorithm

H.-W. Algorithm

Given a polynomial B and a stopping bound H, with $\deg B \leq H$, the following algorithm (a) outputs only perfect polynomials A of degree $\leq H$ having B as a unitary divisor, and (b) outputs every such A that is indecomposable.

1. *Check if $\sigma(B) = B$. If yes, then output B and break.*
2. *Compute $D = \sigma(B)/\gcd(B, \sigma(B))$.*
3. *If $\gcd(B, D) \neq 1$, break.*
4. *Let P be an irreducible factor of D of largest degree.*
5. *Recursively call the algorithm with inputs BP^k and stopping bound H, for all positive integers k with $\deg(BP^k) \leq H$.*

Note: *indecomposable* means A has no nontrivial factorization as a product of two relatively prime **perfect** polynomials.

Recursion

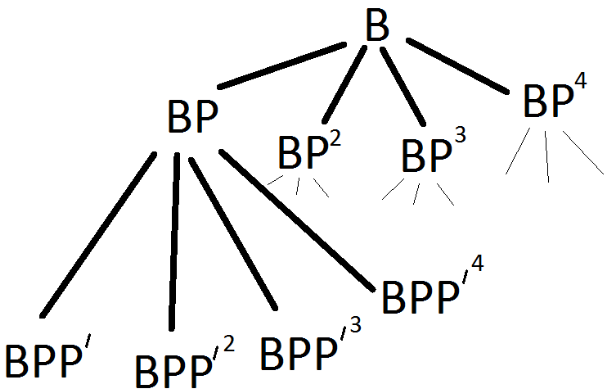

Figure: Recursion for the Algorithm

How did we go so high?

To check odd perfects:

- From the algorithm, we need only check whether P^2 is a unitary divisor for $\deg P \leq 20$.
- Because if A is perfect. It has at least 5 prime divisors and A is a square.

To check even perfects that are not in the infinite family:

- If $P(x)$ is perfect, then $P(x+1)$ is perfect.
- If P is perfect $x|P \Leftrightarrow (x+1)|P$.
- We need only check the algorithm for $x, x^2, \cdots x^{100}$.

Thank you!