

A Test for the Irreducibility of  
Lacunary 0-1 Polynomials

**Douglas B. Meade**

meade@math.sc.edu

**Michael Filaseta**

filaseta@math.sc.edu

University of South Carolina

16 July 1998

## Abstract

The computational complexities of traditional algorithms for the irreducibility of a polynomial depend at best polynomially on the degree of the polynomial. The authors have used ideas of Ljunggren (1960) and Schinzel (1969) to develop a significantly improved algorithm in the case of 0-1 polynomials, an algorithm with a computational complexity that depends logarithmically on the degree of the polynomial (but somewhat poorly on the number of non-zero terms). This talk will provide an overview of the algorithm, including its implementation (in Maple), and a discussion of its performance.

A WWW-based interface to this algorithm can be found at:

<http://www.math.sc.edu/~filaseta/irreduc.html>

# Problem Description & Background

## Problem

- Determine if a 0-1 polynomial is irreducible (over the integers)?

## Objective

- Find a general irreducibility algorithm that has a better dependence on the degree of the polynomial

## Computational Performance of irreduc

$M$	$r$	# test	# irreduc	CPU time (sec)	
				Range	Mean
100	10	50	37	0.090 – 2.980	0.584
200	10	50	33	0.120 – 23.240	4.692
300	10	50	35	1.260 – 111.780	20.663
400	10	30	22	4.660 – 205.290	48.145
500	10	30	23	20.730 – 366.820	72.717
1000	10	10	9	67.370 – 1071.180	475.771
10000	10	1	1	89.105 hrs	89.105 hrs

## 0-1 Polynomials

Define  $S$  to be the set of 0-1 polynomials which do not vanish at the origin, *i.e.*,

$$S := \left\{ \sum_{j=0}^t \epsilon_j x^j : t \in \mathbb{Z}^+, \epsilon_j \in \{0, 1\} \text{ for each } j, \epsilon_0 = 1 \right\}$$

### Example

- Is  $f(x) = 1 + x^{14} + x^{81} + x^{92} + x^{120} + x^{145}$  reducible?
- If so, what is the factorization?

## Definitions

- **(ir)reducible**

(ir)reducible over the integers

- **reciprocal** of  $f(x) \in S$

$$\tilde{f}(x) := x^{\deg f} f(1/x)$$

- **non-reciprocal part** of  $f(x) \in S$

$f(x)$  with monic reciprocal irreducible factors removed

- **norm** of  $f(x) \in S$

$$\|f\|^2 := \# \text{ of non-zero terms in } f(x)$$

# Theoretical Basis

## Lemma

Let  $f(x) \in S$ . If  $f(x) = g(x)h(x)$  where  $g(x)$  and  $h(x)$  are monic polynomials in  $\mathbb{Z}[x]$ , then the polynomial  $g(x)\tilde{h}(x)$  is in  $S$  and has the same number of coefficients being 1 as  $f(x)$ .

## Usage:

Define  $w(x) := g(x)\tilde{h}(x)$ .

Then:

- $w(x) \in S$
- $w(x)\tilde{w}(x) = f(x)\tilde{f}(x)$
- $\|w(x)\| = \|f(x)\|$

## Example of irreduc01NR

Is  $f(x) = 1 + x^{14} + x^{81} + x^{92} + x^{120} + x^{145}$  irreducible?

$$\tilde{f}(x) = 1 + x^{25} + x^{53} + x^{64} + x^{131} + x^{145}$$

$$\begin{aligned} f(x)\tilde{f}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &\quad + x^{81} + x^{92} + x^{106} + x^{117} + x^{120} + x^{131} + x^{134} \\ &\quad + 6x^{145} + \dots \end{aligned}$$

We seek  $w(x) \in S$  with:

- $w(x) \neq f(x)$  and  $w(x) \neq \tilde{f}(x)$ ,
- $w(x)\tilde{w}(x) = f(x)\tilde{f}(x)$ , and
- $\|w\|^2 = \|f\|^2 = 6$ .

## Example of irreduc01NR: Iteration 0

$$w(x) = 1 + x^{14} + \dots + x^{145}$$

$$\tilde{w}(x) = 1 + \dots + x^{131} + x^{145}$$

$$w(x)\tilde{w}(x) = 1 + x^{14} + x^{131} + 3x^{145} + \dots$$

$$\begin{aligned} f(x)\tilde{f}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &\quad + x^{81} + x^{92} + x^{106} + x^{117} + x^{120} + x^{131} + x^{134} \\ &\quad + 6x^{145} + \dots \end{aligned}$$

OK; next unmatched term:  $x^{25}$

## Example of irreduc01NR: Iteration 1

$$w(x) = 1 + x^{14} + x^{25} + \dots + x^{145}$$

$$\tilde{w}(x) = 1 + \dots + x^{120} + x^{131} + x^{145}$$

$$w(x)\tilde{w}(x) = 1 + x^{14} + x^{25} + x^{120} + x^{131} + x^{134} + 4x^{145} + \dots$$

$$\begin{aligned} f(x)\tilde{f}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &\quad + x^{81} + x^{92} + x^{106} + x^{117} + x^{120} + x^{131} + x^{134} \\ &\quad + 6x^{145} + \dots \end{aligned}$$

OK; next unmatched term:  $x^{39}$

## Example of irreduc01NR: Iteration 2

$$w(x) = 1 + x^{14} + x^{25} + x^{39} + \dots + x^{145}$$

$$\tilde{w}(x) = 1 + \dots + x^{106} + x^{120} + x^{131} + x^{145}$$

$$\begin{aligned} w(x)\tilde{w}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{106} + 2x^{120} + 2x^{131} \\ &= + x^{134} + 5x^{145} + \dots \end{aligned}$$

$$\begin{aligned} f(x)\tilde{f}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &\quad + x^{81} + x^{92} + x^{106} + x^{117} + x^{120} + x^{131} + x^{134} \\ &\quad + 6x^{145} + \dots \end{aligned}$$

Mismatch in  $x^{120}$  &  $x^{131}$ ; backtrack to match  $x^{39}$

## Example of irreduc01NR: Iteration 2 – Attempt 2

$$w(x) = 1 + x^{14} + x^{25} + \dots + x^{106} + x^{145}$$

$$\tilde{w}(x) = 1 + x^{39} + \dots + x^{120} + x^{131} + x^{145}$$

$$\begin{aligned} w(x)\tilde{w}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{106} + x^{120} \\ &= + x^{131} + x^{134} + 5x^{145} + \dots \end{aligned}$$

$$\begin{aligned} f(x)\tilde{f}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &\quad + x^{81} + x^{92} + x^{106} + x^{117} + x^{120} + x^{131} + x^{134} \\ &\quad + 6x^{145} + \dots \end{aligned}$$

OK; next unmatched term:  $x^{67}$

## Example of irreduc01NR: Iteration 3

$$w(x) = 1 + x^{14} + x^{25} + x^{67} + x^{106} + x^{145}$$

$$\tilde{w}(x) = 1 + x^{39} + x^{78} + x^{120} + x^{131} + x^{145}$$

$$\begin{aligned}w(x)\tilde{w}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &= + x^{92} + x^{103} + x^{106} + x^{120} + x^{131} + x^{134} \\ &= + 6x^{145} + \dots\end{aligned}$$

$$\begin{aligned}f(x)\tilde{f}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &\quad + x^{81} + x^{92} + x^{106} + x^{117} + x^{120} + x^{131} + x^{134} \\ &\quad + 6x^{145} + \dots\end{aligned}$$

Mismatch in  $x^{103}$ ; backtrack to match  $x^{67}$

## Example of irreduc01NR: Iteration 3 – Attempt 2

$$w(x) = 1 + x^{14} + x^{25} + x^{78} + x^{106} + x^{145}$$

$$\tilde{w}(x) = 1 + x^{39} + x^{67} + x^{120} + x^{131} + x^{145}$$

$$\begin{aligned}w(x)\tilde{w}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &= + x^{81} + x^{92} + x^{117} + x^{120} + x^{131} + x^{134} \\ &= + 6x^{145} + \dots\end{aligned}$$

$$\begin{aligned}f(x)\tilde{f}(x) &= 1 + x^{14} + x^{25} + x^{39} + x^{53} + x^{64} + x^{67} + x^{78} \\ &\quad + x^{81} + x^{92} + x^{106} + x^{117} + x^{120} + x^{131} + x^{134} \\ &\quad + 6x^{145} + \dots\end{aligned}$$

$$\|w\|^2 = 6, w(x) \neq f(x), w(x) \neq \tilde{f}(x) \implies f(x) \text{ is reducible}$$

## Example of irreduc01NR: Conclusion

- $f(x) = 1 + x^{14} + x^{81} + x^{92} + x^{120} + x^{145}$  is reducible
- one factor of  $f(x)$  is  $\gcd(f(x), w(x)) = 1 + x^{14} + x^{53}$
- $f(x) = (1 + x^{14} + x^{53})(1 - x^{39} + x^{67} + x^{92})$

$f(x)$	CPU time (sec)		
	irreduc	irreduc01NR	irreduc01
$1 + x^{14} + x^{81} + x^{92} + x^{120} + x^{145}$	8.24	0.01	0.05

## Comparison of Algorithms

$M$	$r$	# test	Average CPU time (sec)		
			irreduc	irreduc01NR	irreduc01
100	10	50	0.584	0.015	0.041
200	10	50	4.692	0.015	0.039
300	10	50	20.663	0.014	0.043
400	10	30	48.145	0.013	0.048
500	10	30	72.717	0.015	0.057
1000	10	10	475.771	0.014	0.132
10000	10	1/30/30	89.105 hrs	0.013	8.943
50000	30	0/50/10	<i>N/A</i>	0.192	309.574
100000	30	0/50/10	<i>N/A</i>	0.191	1373.840

## Computational Complexity of irreduc01NR

$M$	$r$	# test	# irreduc	CPU time (sec)	
				Range	Mean
$10^{10}$	30	50	50	0.170 – 0.210	0.198
$10^{100}$	30	50	50	0.210 – 0.360	0.261
$10^{100}$	50	50	50	1.170 – 1.800	1.462
$10^{100}$	100	50	50	19.630 – 26.730	23.981
$10^{10^5}$	30	10	10	20.090 – 21.210	20.856
$10^{10^5}$	50	10	10	79.560 – 85.080	82.454
$10^{10^5}$	100	1	?	requires >64MB	N/A

## Computational Complexity of irreduc01

$M$	$r$	# test	# irreduc	CPU time (sec)	
				Range	Mean
20000	10	30	22	0.010 – 54.550	28.796
20000	20	30	26	0.010 – 125.110	46.693
20000	30	30	26	0.010 – 212.180	54.694
20000	40	30	26	0.010 – 130.830	53.728
20000	50	30	28	0.020 – 136.140	59.368
50000	30	10	9	0.010 – 390.780	309.574
100000	30	10	9	0.020 – 2872.090	1373.840
100000	50	10	9	0.020 – 1562.580	1342.016
100000	100	10	9	0.040 – 1642.850	1424.939

# Computational Complexity

irreduc	typical case	cubic in deg $f$
irreduc	worst case	exponential in deg $f$
irreduc01NR	typical case	logarithmic in deg $f$

## Additional Comments

irreduc

- much more general – irreducibility of a multivariate polynomial over an algebraic number field

irreduc01NR

- limited to 0-1 univariate polynomials
- performs best for lacunary polynomials
- complexity is exponential in # of non-zero terms