

**A New Irreducibility Test
for Lacunary 0,1 Polynomials**

Douglas B. Meade

meade@math.sc.edu

University of South Carolina

16 March 2001

Linguistics Professor:

It's an interesting fact that, in English, a double negative forms a positive. In some languages though, such as Russian, a double negative is still a negative. However, there is no language in which a double positive can form a negative.

Student:

Yeah, right!

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.

This talk will provide an overview of the algorithm, including its implementation (in Maple), and a discussion of its performance.

The work in this talk is currently available in the IMI Preprint series; the URL is:

<http://www.math.sc.edu/~imip/01papers/0106.pdf>

A WWW-based interface to a Maple implementation of this algorithm can be found at:

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

Computational Performance of Maple's irreduc

n	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

Definitions for 0,1 Polynomials

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

$$S_r := \left\{ \sum_{j=0}^r x^{a_j} : a_j \in \mathbb{Z}, 0 = a_0 < a_1 < a_2 < \cdots < a_r \right\}$$

<i>(ir)reducible:</i>	(ir)reducible over \mathbb{Z}
<i>reciprocal of $f(x)$:</i>	$\tilde{f}(x) := x^{\deg f} f(1/x)$
<i>norm of $f(x)$:</i>	$\ f\ ^2 := \#$ of non-zero terms
<i>non-reciprocal part of $f(x)$:</i>	$f(x)$ with monic reciprocal irreducible factors removed

The Main Theorem

There is an algorithm for determining whether the non-reciprocal part of $f(x) = \sum_{j=0}^r x^{d_j}$, with $0 = d_0 < d_1 < d_2 < \cdots < d_r = n$, $r \geq 2$, and $n \geq 2$, is irreducible that runs in time

$$\ll 2^r r \log r \log n.$$

Furthermore, if the non-reciprocal part of $f(x)$ is reducible, then the algorithm determines a non-trivial factor of $f(x)$ expressed in the form

$$\gcd(f(x), w(x))$$

where $w(x) = \sum_{j=0}^r x^{k_j} \in \mathbb{Z}[x]$, for some integers k_j satisfying $0 = k_0 < k_1 < k_2 < \cdots < k_r = n$.

Theoretical Basis: Lemma 1

Let r be a positive integer, and let $f(x) \in S_r$.
Then the non-reciprocal part of $f(x)$ is reducible

if and only if

there is a $w(x) \in S_r$ satisfying

$$w(x) \neq f(x)$$

$$w(x) \neq \tilde{f}(x)$$

$$w(x)\tilde{w}(x) = f(x)\tilde{f}(x)$$

Theoretical Basis: Lemma 2

Let $f(x) \in S$ be reciprocal. Then $f(x)$ is not divisible by a non-reciprocal polynomial in $\mathbb{Z}[x]$.

Example: $F(x) := x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1$

- $\tilde{F}(x) = F(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$
i.e., $F(x)$ has non-reciprocal (irreducible) factors
- $F(x) \notin S$

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 irred01NR: Iteration 2

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

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

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

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

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

Example of irreduc01NR: Iteration 2 – Attempt 2

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

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

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

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

OK; next unmatched term: x^{67}

Example of irreduc01NR: Iteration 3

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

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

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

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

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

Example of irreduc01NR: Iteration 3 – Attempt 2

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

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

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

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

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

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

Algorithm for irreduc01NR

Step NR1 *Check if $f(x)$ is reciprocal.*

If $f(x) = \tilde{f}(x)$, then $f(x)$ is not irreducible; non-reciprocal part of $f(x)$ is 1; STOP.

Step NR2 *Construct the factoring tree for $f(x)$.*

The factoring tree for $f(x)$ is the binary tree with all possible $w(x) \in S_r$ with $w(x)\tilde{w}(x) = f(x)\tilde{f}(x)$. Note: at most $2^r - 1$ nodes and at most 2^{r-1} endnodes on level r .

Step NR3 *Check polynomials associated with endnodes on level r .*

Case 1: No endnodes or all endnodes correspond to $w(x) = f(x)$ or $w(x) = \tilde{f}(x)$: $f(x)$ is irreducible; STOP.

Case 2: There is an endnode corresponding to $w(x)$ that satisfies all conditions of Lemma 2: $f(x)$ is reducible with a factor $\gcd(f(x), w(x))$; STOP.

Complexity of irreduc01NR: Worst Case

Step NR1 *Check if $f(x)$ is reciprocal.*

$\ll r$ comparisons $\times \log n$ bit ops/comparison

Step NR2 *Construct the factoring tree for $f(x)$.*

$\ll \sum_{\ell=1}^{r-1} 2^\ell r \log r \log n$

$\ll 2^r r \log r \log n$

Step NR3 *Check polynomials associated with endnodes on level r .*

Case 1: $\ll 2 \times 2^{r-1}$ nodes $\times r \log r$ terms $\times \log n$ bit ops per comparison

Case 2: $\ll r$ terms $\times \log n$ bit ops per exponent

Comparison of Algorithms

n	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

n	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

n	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

At dinner yesterday, I tried to cut
myself a slice of prime rib but it
was only divisible by itself and one.

— Chris Lipe, The Top5 List, 9 March 2001