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 $0 = k_0 < k_1 < k_2 < \cdots < k_r = n$.

Example of `irreduc01NR`

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

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

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

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

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

Example of `irreduc01NR`: Iteration 0

$$
\begin{aligned}
w(x) &= 1 + x^{14} + \cdots + x^{145} \\
\widetilde{w}(x) &= 1 + \cdots + x^{131} + x^{145}
\end{aligned}
$$

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

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

OK; next ummatched term: x^{25}

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 $f(x) = \widetilde{f}(x)$, 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 $w(x)\widetilde{w}(x) = f(x)\widetilde{f}(x)$. 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 $w(x) = \widetilde{f}(x)$: $f(x)$ 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	*N/A*	0.192	309.574
100000	30	0/50/10	*N/A*	0.191	1373.840

Computational Complexity of `irreduc01NR`

n	r	# test	# irreduc	CPU time (sec) Range	CPU time (sec) 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	CPU time (sec) 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