On Swan's theorem for binary pentanomials

David Thomson
Joint with B. Hanson (Toronto) and D. Panario (Carleton)
Special thanks to K. S. Williams

Carleton University
dthomson@math.carleton.ca

WCNT - December 2014

Motivation – Schoolbook construction of finite fields

The complexity of various computations over finite fields depends on the basis representation used.

Let n be a positive integer and let q be a prime power. The finite extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can be constructed by

1. Picking a degree-n irreducible polynomial over $\mathbb{F}_q$.
2. Adjoining one of its roots

The bottleneck.

Equivalently, pick $f \in \mathbb{F}_q[x]$ irreducible. Then

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(f);$$

that is, the elements of $\mathbb{F}_{q^n}$ are the polynomials of degree at most $n-1$ over $\mathbb{F}_q$. Arithmetic is performed (mod f).

The cost of arithmetic using this power basis is* directly related to the number of terms in the modulus f (lower is better).

Obvious. Let $f \in \mathbb{F}_2[x]$. If f has an even number of nonzero terms, then f is reducible.

Swan-Stickelberger

Stickelberger

So, for performing arithmetic over $\mathbb{F}_2$, we prefer polynomials f which have $3, 5, \ldots$ non-zero terms.

Theorem. (Stickelberger) Suppose that f is a monic polynomial of degree n with coefficients in $\mathbb{Z}_p \subset \mathbb{F}$, where $\mathbb{F}$ is a p-adic field. Let $\overline{f} = f \pmod{p}$ and suppose $\overline{f}$ has no repeated roots. If $\overline{f}$ has r irreducible factors over the residue class field, then

$$r \equiv n \pmod 2 \text{ if and only if } D(f) \text{ is a square in } \mathbb{F},$$

where $f(x) = \prod_{i=0}^{n-1}(x - \alpha_i)$ and

$$D(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \prod_{i=0}^{n-1} f'(\alpha_i),$$

is its discriminant.

Swan's contributions (1962)

Corollary. If f is an irreducible polynomial over $\mathbb{F}_2$ with $D(f) \neq 0$ and r is its number of irreducible factors over $\mathbb{F}_2$, let $g \in \mathbb{Z}_2[x]$ such that $g \pmod 2 = f$. Then $n \equiv r \pmod 2$ if and only if $D(g) \equiv 1 \pmod 8$.

Moreover, the discriminant of a trinomial is computable by hand.

Proposition.

$$D(x^n + x^k + 1) = (-1)^{n(n-1)/2} \left(n^{n_1} + (-1)^{n_1+1}(n-k)^{k_1} \right)^d,$$

where $d = \gcd(n, k)$, $n_1 = n/d$ and $k_1 = n/d$.

Swan's Theorem (1962)

Theorem. Let $n > k > 0$. Wlog (considering instead the reverse polynomial), assume precisely one of n, k is odd. If r is the number of irreducible factors of $x^n + x^k + 1 \in \mathbb{F}_2[x]$, then r is even when:

1. n even, k odd, $n \neq 2k$ and $nk/2 \equiv 0, 1 \pmod 4$;
2. n odd, k even, $k \nmid 2n$ and $n \equiv 3, 5 \pmod 8$;
3. n odd, k even, $k | 2n$ and $n \equiv 1, 7 \pmod 8$.

Experiment. (See Seroussi, HFF, Magma) For $n \leq 10,000$ approximately 50% of all degrees n have an irreducible trinomial.

In every case that there is not an irreducible trinomial, we find an irreducible pentanomial.

Pentanomials

Some acknowledgements

Let $f(x) = x^n + x^r + x^s + x^t + 1$.

Personal notes of K. S. Williams provide:

1. A table of congruences of n, r, s, t that conjectures the parity of the number of irreducible factors of f.
2. Most of the following worked example.

And thanks to B. Hanson (UofT) for compiling this work in his Honours project and contributing to many fruitful discussions both then and in some follow-up work.

Example of the table

Here, $f(x) = x^n + x^r + x^s + x^t + 1$ with k irreducible factors.

Case	$[n]$	$[r], [s], [t]$	$[k]$
0.1	$n \equiv 0[8]$	$r \equiv s \equiv t \equiv 0[2]$	$k \equiv 0[2]$
0.2	$n \equiv 0[8]$	$\{r, s, t\} = \{0[4],\ 0[4],\ 1[2]\}$	$k \equiv 0[2]$
0.3	$n \equiv 0[8]$	$r \equiv s \equiv t \equiv 1[2],\ r \equiv s \equiv t[8]$	$k \equiv 0[2]$
0.4	$n \equiv 0[8]$	$\{r, s, t\} = \{0[4],\ a[8],\ a[8]\}$, a odd	$k \equiv 0[2]$
0.5	$n \equiv 0[8]$	otherwise	$k \equiv 1[2]$
1.1	$n \equiv 1[8]$	any	$k \equiv 1[2]$
2.1	$n \equiv 2[8]$	$r \equiv s \equiv t \equiv 0[2]$	$k \equiv 0[2]$
2.2	$n \equiv 2[8]$	otherwise	$k \equiv 1[2]$

$\vdots$

Case 3.1: $n \equiv 3 \pmod 4$; $r \equiv s \equiv t \equiv 0 \pmod 4$

Compute the discriminant

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (f'(\alpha_i))$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (n\alpha_i^{n-1} + 4r'\alpha_i^{r-1} + 4s'\alpha_i^{s-1} + 4t'\alpha_i^{t-1})$$

Since we need $D(f) \pmod 8$, considering only terms containing one 4.

Expanding,

$$D(f) = (-1)^{\frac{n(n-1)}{2}} n^n (\alpha_1 \cdots \alpha_n)^{n-1} + (-1)^{\frac{n(n-1)}{2}} 4n^{n-1} \times \left(r' \sum_{k=1}^{n} \frac{(\alpha_1 \cdots \alpha_n)^{n-1}}{\alpha_k^{n-r}} + s' \sum_{k=1}^{n} \frac{(\alpha_1 \cdots \alpha_n)^{n-1}}{\alpha_k^{n-s}} + t' \sum_{k=1}^{n} \frac{(\alpha_1 \cdots \alpha_n)^{n-1}}{\alpha_k^{n-t}} \right)$$

$$= \underbrace{(-1)^{\frac{n(n-1)}{2}} n^n (\alpha_1 \cdots \alpha_n)^{n-1}}_{A} + (-1)^{\frac{n(n-1)}{2}} 4n^{n-1} (\alpha_1 \cdots \alpha_n)^{n-1} \times \underbrace{\left(r' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-r}} + s' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-s}} + t' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-t}} \right)}_{B}.$$

Case A.

Expanding,

$$D(f) = (-1)^{\frac{n(n-1)}{2}} n^n (\alpha_1 \cdots \alpha_n)^{n-1} + (-1)^{\frac{n(n-1)}{2}} 4n^{n-1} \times \left(r' \sum_{k=1}^{n} \frac{(\alpha_1 \cdots \alpha_n)^{n-1}}{\alpha_k^{n-r}} + s' \sum_{k=1}^{n} \frac{(\alpha_1 \cdots \alpha_n)^{n-1}}{\alpha_k^{n-s}} + t' \sum_{k=1}^{n} \frac{(\alpha_1 \cdots \alpha_n)^{n-1}}{\alpha_k^{n-t}} \right)$$

$$= \underbrace{(-1)^{\frac{n(n-1)}{2}} n^n (\alpha_1 \cdots \alpha_n)^{n-1}}_{A} + (-1)^{\frac{n(n-1)}{2}} 4n^{n-1} (\alpha_1 \cdots \alpha_n)^{n-1} \times \underbrace{\left(r' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-r}} + s' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-s}} + t' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-t}} \right)}_{B}.$$

Case A. We know $\alpha_1 \cdots \alpha_n \equiv -1 \equiv 7 \pmod 8$ by comparing coefficients. For both $n \equiv 3, 5 \pmod 8$, we find $A \equiv 5 \pmod 8$.

Case B.

$$B = \left(r' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-r}} + s' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-s}} + t' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-t}} \right).$$

Here, we notice that $\frac{1}{\alpha_i}$ are roots of the reverse of f; $\hat{f}(x) = x^n f(1/x)$.

Case B.

$$B = \left(r' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-r}} + s' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-s}} + t' \sum_{k=1}^{n} \frac{1}{\alpha_k^{n-t}} \right).$$

Here, we notice that $\frac{1}{\alpha_i}$ are roots of the reverse of f; $\hat{f}(x) = x^n f(1/x)$.

Sums of powers of roots $\Rightarrow$ Newton's formulas.

$$S_{1,i} + a_1 S_{1,i-1} + a_2 S_{1,i-2} + \cdots + a_{i-1} S_{1,1} + i a_i = 0.$$

Using parity arguments (n odd, r, s, t even imply $n-r$, $n-s$, $n-t$ odd, ...), we find $B = 0$.

Putting it together

We have

1. $D(f) = A + 4n^{n-1}B$ with $A \equiv 5 \pmod 8$ and $B = 0$,
2. Thus $D(f) \equiv 5 \pmod 8$,
3. which is not a square,
4. and $n \equiv 3 \pmod 8$ is odd.

Hence, f has an even number of irreducible factors and is always reducible.

How did that work?

Lots of cancellation

Recall the previous case: $n \equiv 3 \pmod 8$, $r, s, t \equiv 0 \pmod 4$. Hence, any product of roots in the discriminant vanished whenever two roots were picked from the x^r, x^s, x^t terms.

We can remove from the table:

1. Cases $0.1, 2.1, 4.1, 6.1$ since the pentanomial is a square,
2. Cases $0.2, 3.1, 5.1, 3.2, 5.2$ by the above.

Remaining cases

Case	$[n]$	$[r], [s], [t]$	$[k]$
0.2	$n \equiv 0[8]$	$\{r, s, t\} = \{0[4],\ 0[4],\ 1[2]\}$	$k \equiv 0[2]$
0.3	$n \equiv 0[8]$	$r \equiv s \equiv t \equiv 1[2],\ r \equiv s \equiv t[8]$	$k \equiv 0[2]$
0.4	$n \equiv 0[8]$	$\{r, s, t\} = \{0[4],\ a[8],\ a[8]\}$, a odd	$k \equiv 0[2]$
0.5	$n \equiv 0[8]$	otherwise	$k \equiv 1[2]$
1.1	$n \equiv 1[8]$	any	$k \equiv 1[2]$
2.2	$n \equiv 2[8]$	otherwise (wrt 2.1)	$k \equiv 1[2]$
3.3	$n \equiv 3[8]$	$r,\ s$ and $t \equiv 0[8]$ or $3[8]$	$k \equiv 0[2]$
3.4	$n \equiv 3[8]$	otherwise	$k \equiv 1[2]$

$\vdots$

And we're stuck.

Case 3.3: $n \equiv r \equiv 3 \pmod 8$, $s, t \equiv 0 \pmod 8$.

The discriminant reduces to:

$$\begin{aligned} D(f) &\equiv 5 \prod_{i=1}^{n} \left(\alpha_i^{n-r} + 1\right) \\ &= \sum_{i=1}^{n} S_{i,n-r}. \\ &= \sum_{k_1<k_2<\cdots<k_i} \left(\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}\right)^{n-r} \end{aligned}$$

But we're not really sure how to compute $\sum_{i=1}^{n} S_{i,n-r}$.

And we're stuck.

Case 3.3: $n \equiv r \equiv 3 \pmod 8$, $s, t \equiv 0 \pmod 8$.

The discriminant reduces to:

$$\begin{aligned} D(f) &\equiv 5 \prod_{i=1}^{n} \left(\alpha_i^{n-r} + 1\right) \\ &= \sum_{i=1}^{n} S_{i,n-r}. \\ &= \sum_{k_1<k_2<\cdots<k_i} \left(\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}\right)^{n-r} \end{aligned}$$

But we're not really sure how to compute $\sum_{i=1}^{n} S_{i,n-r}$. Ideas?