Improving the Berlekamp algorithm for binomials $x^n - a$

Ryuichi Harasawa Yutaka Sueyoshi Aichi Kudo

Nagasaki University

July 19, 2012

1. Polynomial factorization over finite fields

Polynomial factorization

Input: $f(x) \in \mathbb{F}_q[x]$

Output: pair(s) $(f_i(x), e_i)$ with $f(x) = \prod f_i(x)^{e_i}$
($f_i(x)$: irreducible polynomial)

Application to cryptography

- Construction of extension field:
  $f(x)$: irre. poly./$\mathbb{F}_q$ of degree $n \Rightarrow \mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f(x))$
- Index calculus for solving DLP (on Jacobian group):
  Check if $f(x)$ is $\mathcal{B}$-smooth ($\mathcal{B} (\subset \mathbb{F}_q[x])$: factor base).
  If so, the factorization of $f(x)$ gives a relation to solve DLP.

2. Procedure of factorization

We first perform the square-free factorization.
After the procedure, we factor square-free polynomial(s).

$f(x)$: square-free $\overset{\text{def}}{\iff}$ $f(x)$ has no repeated factors
(i.e., $g(x) \mid f(x)\ (\deg(g(x)) \geq 1) \ \Rightarrow\ g(x)^2 \nmid f(x)$)

Square-free factorization

Input: $f(x) \in \mathbb{F}_q[x]$

Output: $g_i(x)$'s: square-free (possibly $g_i(x) = 1$)
with $f(x) = \prod_{i \geq 1} g_i(x)^i$

3. Overview of square-free factorization

$p = \mathrm{char}\mathbb{F}_q$.
$f(x) = \prod_i g_i(x)^i$, $g_i(x)$: (unknown) square-free poly.
$f'(x)$: the formal derivation of $f(x)$.

Key facts

- $f'(x) = 0 \Rightarrow f(x) = g(x)^p$ $(\exists g(x) \in \mathbb{F}_q[x])$,
  more precisely $f(x) = \sum_j a_{jp}x^{jp} = (\sum_j a_j^{(1/p)}x^j)^p$
- $\gcd(f(x), f'(x)) = \prod_{p\nmid i} g_i(x)^{i-1} \cdot \prod_{p|i} g_i(x)^i$
- $f(x)/\gcd(f(x), f'(x)) = \prod_{p\nmid i} g_i(x)$: square-free

We compute $g_i(x)$'s using the facts repeatedly.
Especially, $\gcd(f(x), f'(x)) = 1 \Longrightarrow f(x)$: square-free.

4. Factorization of square-free polynomial

$f(x)$: square-free polynomial over $\mathbb{F}_q$
Two popular methods to factor square-free poly.:

1. Berlekamp method:
   Using the kernel of the linear mapping, $\pi_q - \mathbf{id}$,
   defined by $g(x) \mapsto (g(x)^q - g(x)) \bmod f(x)$.
2. Cantor/Zassenhaus method:
   Using Distinct-degree & Equal-degree factorizations.

We focus on the Berlekamp method in this talk.

5. Berlekamp algorithm

- Assume that q is odd.
- $f(x) \in \mathbb{F}_q[x]$: square-free polynomial.

We consider the linear mapping $\pi_q - \mathbf{id}$ from $\mathbb{F}_q[x]/(f(x))$ to itself defined by $g(x) \mapsto (g(x)^q - g(x)) \bmod f(x)$.

Step 1: Compute the kernel of $\pi_q - \mathbf{id}$, say $\mathcal{N}$.

Step 2: For a random element $g(x) \in \mathcal{N}$, we find non-trivial factors of $f(x)$ by computing $\gcd(f(x), g(x))$ and $\gcd(f(x), g(x)^{(q-1)/2} - 1)$.

We note that #(irre. factor(s) of $f(x)$) $= \dim_{\mathbb{F}_q} \mathcal{N}$

6. The purpose of this talk

Main theme: The computation of the kernel $\mathcal{N}$
for $f(x) = x^n - a$ deined over $\mathbb{F}_q$ with $p = \mathbf{char}\mathbb{F}_q$.

Previous work: $a = 1 \Rightarrow$ Eugene Prange (1959)
We extend the method to general a.

Assumption on $f(x) = x^n - a$:

- $a \neq 0$ (otherwise, obvious)
- $p \nmid n$ (otherwise, $f(x) = (x^{n/p} - a^{1/p})^p$
and $f(x) \leftarrow x^{n/p} - a^{1/p}$).

$\Rightarrow f(x)$: square-free (since $\mathbf{gcd}(f(x), f'(x)) = 1$)

7. The kernel $\mathcal{N}$ of $\pi_q - \mathrm{id}$

- $f(x)$: square-free poly. of degree n to be factored.
- $Q = (q_{ij})_{0 \le i,j \le n-1}$: $n \times n$ matrix with
$$(x^j)^q \equiv \sum_{0 \le i \le n-1} q_{ij} x^i \pmod{f(x)}.$$

$$\Downarrow \quad \pi_q - \mathrm{id} : \ g(x) \mapsto (g(x)^q - g(x)) \bmod f(x)$$

- $Q - I_n$: the matrix representation of $\pi_q - \mathrm{id}$
(I_n: $n \times n$ identity matrix)
$\Rightarrow \mathcal{N}$: the solution space of $(Q - I_n)X = 0$

In order to get $\mathcal{N}$,
I think we generally apply the Gaussian elimination.

8. The computation of $\mathcal{N}$ for $x^n - a$ (1/2)

Let $p = \mathrm{char}\mathbb{F}_q$, $f(x) = x^n - a$ ($p \nmid n$, $a \neq 0$).

Notation

- For $q \bmod n \neq 0$, $\langle q \rangle := \{q^i \bmod n \mid i = 0, 1, 2, \ldots\}$
- $\bar{\alpha} := \{\alpha q^i \bmod n \mid i = 0, 1, 2, \ldots\}$: the orbit containing $\alpha \in \mathbb{Z}/n\mathbb{Z}$ with respect to $\langle q \rangle$. (Let $\ell = \#\bar{\alpha}$.)
- $\alpha_i := \alpha q^i \bmod n$ (note that $\alpha q^\ell \bmod n = \alpha (= \alpha_0)$)
- $T_{\bar{\alpha}} := \{\beta_0 x^{\alpha_0} + \beta_1 x^{\alpha_1} + \cdots + \beta_{\ell-1} x^{\alpha_{\ell-1}} \mid \beta_i \in \mathbb{F}_q\}$ for $\bar{\alpha} = \{\alpha_0, \alpha_1, \ldots, \alpha_{\ell-1}\}$

9. The computation of $\mathcal{N}$ for $x^n - a$ (2/2)

Then we have

- $\mathbb{F}_q[x]/(f(x)) = \bigoplus_{\bar{\alpha}} T_{\bar{\alpha}}$
  ($\bar{\alpha}$ runs over all orbits in $\mathbb{Z}/n\mathbb{Z}$ with respect to $\langle q \rangle$)
- $\pi_q(T_{\bar{\alpha}}) \subseteq T_{\bar{\alpha}}$ $(= \mathrm{id}(T_{\bar{\alpha}}))$ (i.e., $T_{\bar{\alpha}}$: π_q-invariant).
- $\mathcal{N} = \mathrm{Ker}(\pi_q - \mathrm{id})$.

$\Longrightarrow \quad \mathcal{N} = \bigoplus_{\bar{\alpha}} (\mathcal{N} \cap T_{\bar{\alpha}})$

That is, in order to get the karnel $\mathcal{N}$ of $\pi_q - \mathrm{id}$,
it is sufficient to compute $\mathcal{N} \cap T_{\bar{\alpha}}$ for each $\bar{\alpha}$.
$\Rightarrow$ We restrict the domain of $\pi_q - \mathrm{id}$ to the subspace $T_{\bar{\alpha}}$.

10. The computation of $\mathcal{N} \cap T_{\bar{\alpha}}$ (1/2)

For $h(x) = \beta_0 x^{\alpha_0} + \beta_1 x^{\alpha_1} + \cdots + \beta_{\ell-1} x^{\alpha_{\ell-1}}$ in $T_{\bar{\alpha}}$, we consider the equation $(\pi_q - \mathrm{id})(h(x)) = 0$ (equivalently, $h(x)^q \equiv h(x) \pmod{f(x)}$).

$$\Rightarrow \begin{cases} \beta_{\ell-1} = a^{\gamma_{\ell-2}}\beta_{\ell-2} & \leftarrow \text{coefficient of } x^{\ell-1} \\ \beta_{\ell-2} = a^{\gamma_{\ell-3}}\beta_{\ell-3} & \leftarrow \text{coefficient of } x^{\ell-2} \\ \quad\vdots & \quad\vdots \\ \beta_0 = a^{\gamma_{\ell-1}}\beta_{\ell-1} & \leftarrow \text{constant term,} \end{cases}$$

where $q\alpha_i = \gamma_i n + \alpha_{i+1 \bmod \ell}$.

$$\Rightarrow \beta_0 = a^{\gamma_{\ell-1}}\beta_{\ell-1} = a^{\gamma_{\ell-1}}(a^{\gamma_{\ell-2}}\beta_{\ell-2}) = \cdots = a^{\gamma_0+\gamma_1+\cdots+\gamma_{\ell-1}}\beta_0$$

11. The computation of $\mathcal{N} \cap T_{\bar{\alpha}}$ (2/2)

We get the relation $\beta_0 = a^{\gamma_0+\gamma_1+\cdots+\gamma_{\ell-1}}\beta_0$, which implies

$$\mathcal{N} \cap T_{\bar{\alpha}} = \begin{cases} \{\beta(x^{\alpha_0} + a^{\gamma_0}x^{\alpha_1} + a^{\gamma_0+\gamma_1}x^{\alpha_2} + \cdots + a^{\gamma_0+\gamma_1+\cdots+\gamma_{\ell-2}}x^{\alpha_{\ell-1}}) \mid \beta \in \mathbb{F}_q\} \\ \qquad \text{(if } a^{\gamma_0+\gamma_1+\cdots+\gamma_{\ell-1}} = 1\text{)}, \\ \{0\} \quad \text{(otherwise)}. \end{cases}$$

Complexity

$\tilde{O}(n \log q)$ bit operations + $O(n \log q)$ operations in $\mathbb{F}_q$
(cf. $O(n^{2.376})$ operations in $\mathbb{F}_q$ for the improved Gaussian elimination using the Coppersmith-Winograd fast matrix multiplication).

12. Example: $f(x) = x^{22} - 2$ defined over $\mathbb{F}_5$ (1/5)

We consider $q = 5$, $f(x) = x^{22} - 2$ ($n = 22, a = 2$).
$\Rightarrow \mathbb{Z}/22\mathbb{Z}$ is decomposed into six orbits with respect to $\langle 5 \rangle$:

$\overline{0} = \{0\}$, $\overline{1} = \{1, 5, 3, 15, 9\}$, $\overline{2} = \{2, 10, 6, 8, 18\}$,
$\overline{4} = \{4, 20, 12, 16, 14\}$, $\overline{7} = \{7, 13, 21, 17, 19\}$,
$\overline{11} = \{11\}$.

For each orbit $\overline{\alpha}$,
we compute the subspace $\mathcal{N}$ by considering $\mathcal{N} \cap T_{\overline{\alpha}}$
(recall that $\mathcal{N}$ is the kernel of the mapping
$g(x) \mapsto (g(x)^q - g(x)) \bmod f(x)$).

13. Example: $f(x) = x^{22} - 2$ defined over $\mathbb{F}_5$ (2/5)

- [The case of $\overline{\mathbf{0}} = \{\mathbf{0}\}$ $(\ell = 1)$]

$$\begin{array}{rcccl} & & (q \cdot \alpha_i & = & \gamma_i \cdot n + \alpha_{i+1}) \\ 5 \cdot \alpha_0 & = & 5 \cdot 0 & = & \underline{0} \cdot 22 + 0 \quad \rightarrow \quad \underline{\gamma_0 = 0}, \ \alpha_1 = 0 = \alpha_0 \end{array}$$

So, we have $a^{\gamma_0} = 2^0 = 1$ in $\mathbb{F}_5$.

$$\begin{array}{rcl} \Rightarrow \quad \mathcal{N} \cap T_{\overline{0}} & = & \{\beta x^{\alpha_0} \mid \beta \in \mathbb{F}_5\} \\ & = & \{\beta \cdot 1 \mid \beta \in \mathbb{F}_5\} \\ & = & \mathbb{F}_5 \end{array}$$

14. Example: $f(x) = x^{22} - 2$ defined over $\mathbb{F}_5$ (3/5)

- [The case of $\overline{1} = \{1, 5, 3, 15, 9\}$ $(\ell = 5)$]

$$
\begin{cases}
 & (q \cdot \alpha_i & = & \gamma_i \cdot n + \alpha_{i+1}) & & \\
5 \cdot \alpha_0 & = 5 \cdot 1 & = & \underline{0} \cdot 22 + 5 & \rightarrow & \underline{\gamma_0 = 0}, \ \alpha_1 = 5 \\
5 \cdot \alpha_1 & = 5 \cdot 5 & = & \underline{1} \cdot 22 + 3 & \rightarrow & \underline{\gamma_1 = 1}, \ \alpha_2 = 3 \\
5 \cdot \alpha_2 & = 5 \cdot 3 & = & \underline{0} \cdot 22 + 15 & \rightarrow & \underline{\gamma_2 = 0}, \ \alpha_3 = 15 \\
5 \cdot \alpha_3 & = 5 \cdot 15 & = & \underline{3} \cdot 22 + 9 & \rightarrow & \underline{\gamma_3 = 3}, \ \alpha_4 = 9 \\
5 \cdot \alpha_4 & = 5 \cdot 9 & = & \underline{2} \cdot 22 + 1 & \rightarrow & \underline{\gamma_4 = 2}, \ \alpha_5 = 1 = \alpha_0
\end{cases}
$$

So, we have

$a^{\gamma_0+\gamma_1+\gamma_2+\gamma_3+\gamma_4} = 2^{0+1+0+3+2} = 2^6 = -1 \neq 1$ in $\mathbb{F}_5$.

$\Rightarrow \mathcal{N} \cap T_1^- = \{0\}$

15. Example: $f(x) = x^{22} - 2$ defined over $\mathbb{F}_5$ (4/5)

- [The case of $\overline{2} = \{2, 10, 6, 8, 18\}$ $(\ell = 5)$]

$$\begin{cases} 5 \cdot \alpha_0 = 5 \cdot 2 = \underline{0} \cdot 22 + 10 \rightarrow \underline{\gamma_0 = 0}, \ \alpha_1 = 10 \\ 5 \cdot \alpha_1 = 5 \cdot 10 = \underline{2} \cdot 22 + 6 \rightarrow \underline{\gamma_1 = 2}, \ \alpha_2 = 6 \\ 5 \cdot \alpha_2 = 5 \cdot 6 = \underline{1} \cdot 22 + 8 \rightarrow \underline{\gamma_2 = 1}, \ \alpha_3 = 8 \\ 5 \cdot \alpha_3 = 5 \cdot 8 = \underline{1} \cdot 22 + 18 \rightarrow \underline{\gamma_3 = 1}, \ \alpha_4 = 18 \\ 5 \cdot \alpha_4 = 5 \cdot 18 = \underline{4} \cdot 22 + 2 \rightarrow \underline{\gamma_4 = 4}, \ \alpha_5 = 2 = \alpha_0 \end{cases}$$

So, we have

$a^{\gamma_0+\gamma_1+\gamma_2+\gamma_3+\gamma_4} = 2^{0+2+1+1+4} = 2^8 = 1$ in $\mathbb{F}_5$.

$$\begin{aligned} \Rightarrow \ \mathcal{N} \cap T_{\overline{2}} &= \{\beta(x^{\alpha_0} + a^{\gamma_0} x^{\alpha_1} + a^{\gamma_0+\gamma_1} x^{\alpha_2} \\ &\quad + a^{\gamma_0+\gamma_1+\gamma_2} x^{\alpha_3} + a^{\gamma_0+\gamma_1+\gamma_2+\gamma_3} x^{\alpha_4}) \mid \beta \in \mathbb{F}_5\} \\ &= \{\beta(x^2 + x^{10} + 4x^6 + 3x^8 + x^{18}) \mid \beta \in \mathbb{F}_5\} \end{aligned}$$

16. Example: $f(x) = x^{22} - 2$ defined over $\mathbb{F}_5$ (5/5)

Performing the same procedure as the previous one for the remainder orbits, we obtain

- $\mathcal{N} \cap T_4^- = \{\beta(x^{20} + 4x^{16} + 2x^{14} + x^{12} + x^4) \mid \beta \in \mathbb{F}_5\}$
- $\mathcal{N} \cap T_7^- = \mathcal{N} \cap T_{11}^- = \{0\}$.

From the computations above, we obtain the results:

- $\{1,\ x^{18} + x^{10} + 3x^8 + 4x^6 + x^2,\ x^{20} + 4x^{16} + 2x^{14} + x^{12} + x^4\}$ forms an $\mathbb{F}_5$-basis of $\mathcal{N}$;
- #(irre. factors of $f(x)$) $= \dim_{\mathbb{F}_5} \mathcal{N} = 3$.

17. Getting factors using the kernel $\mathcal{N}$ (1/2)

We assume that $\dim_{\mathbb{F}_q} \mathcal{N} \geq 2$ and that q is odd.
($\dim_{\mathbb{F}_q} \mathcal{N} = 1 \Rightarrow f(x)$: irreducible)
$g(x)$: random element in $\mathcal{N}$

$$\Rightarrow \quad g(x) \cdot (g(x)^{(q-1)/2} - 1) \cdot (g(x)^{(q-1)/2} + 1)$$
$$= \quad g(x)^q - g(x) \equiv 0 \pmod{f(x)}$$

If $\gcd(f(x), g(x)) \neq 1, f(x)$ or $\gcd(f(x), g(x)^{(q-1)/2} - 1) \neq 1, f(x)$ (or both), then we get a non-trivial factor of $f(x)$.

Repeatedly we perform this procedure
until #(our getting factors of $f(x)$)$= \dim_{\mathbb{F}_q} \mathcal{N}$.

Complexity

$\tilde{O}(n \log q)$ operations in $\mathbb{F}_q$ using a fast polynomial operations.

18. Getting factors using the kernel $\mathcal{N}$ (2/2)

Note that, for $g(x) \in \mathcal{N}$ with $\gcd(f(x), g(x)) = 1$,
$\mathbf{Prob}\{\text{getting non-trivial factors}\} = 1 - (\frac{1}{2})^{\dim_{\mathbb{F}_q} \mathcal{N} - 1} \geq \frac{1}{2}$

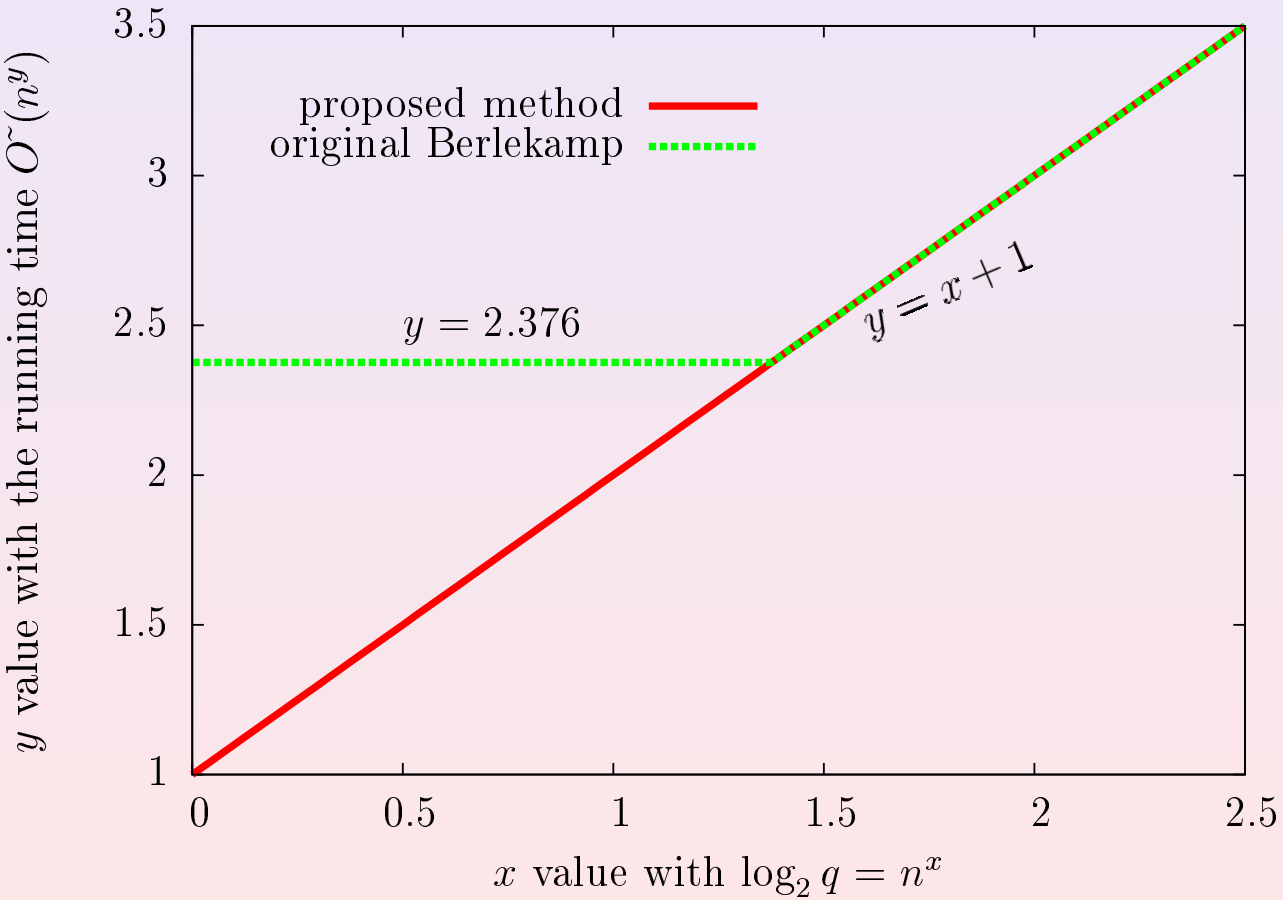
Memo: $f(x) = \prod_{1 \leq i \leq k} f_i(x)$: factorization of $f(x)$.

$$\begin{array}{ccc} \mathbb{F}_q[x]/(f(x)) & \simeq & \mathbb{F}_q[x]/(f_1(x)) \times \cdots \times \mathbb{F}_q[x]/(f_k(x)) \\ \cup & & \cup \\ \mathcal{N} & \simeq & \{(a_1, \ldots, a_k) \mid a_i \in \mathbb{F}_q\} \end{array}$$

For each i, we have $g(x)^{(q-1)/2} \equiv \pm 1 \bmod f_i(x)$.
"not getting a non-trivial factor of $f(x)$
$\iff g(x)^{(q-1)/2} \leftrightarrow (1, 1, \ldots, 1)$ or $(-1, -1, \ldots, -1)$"

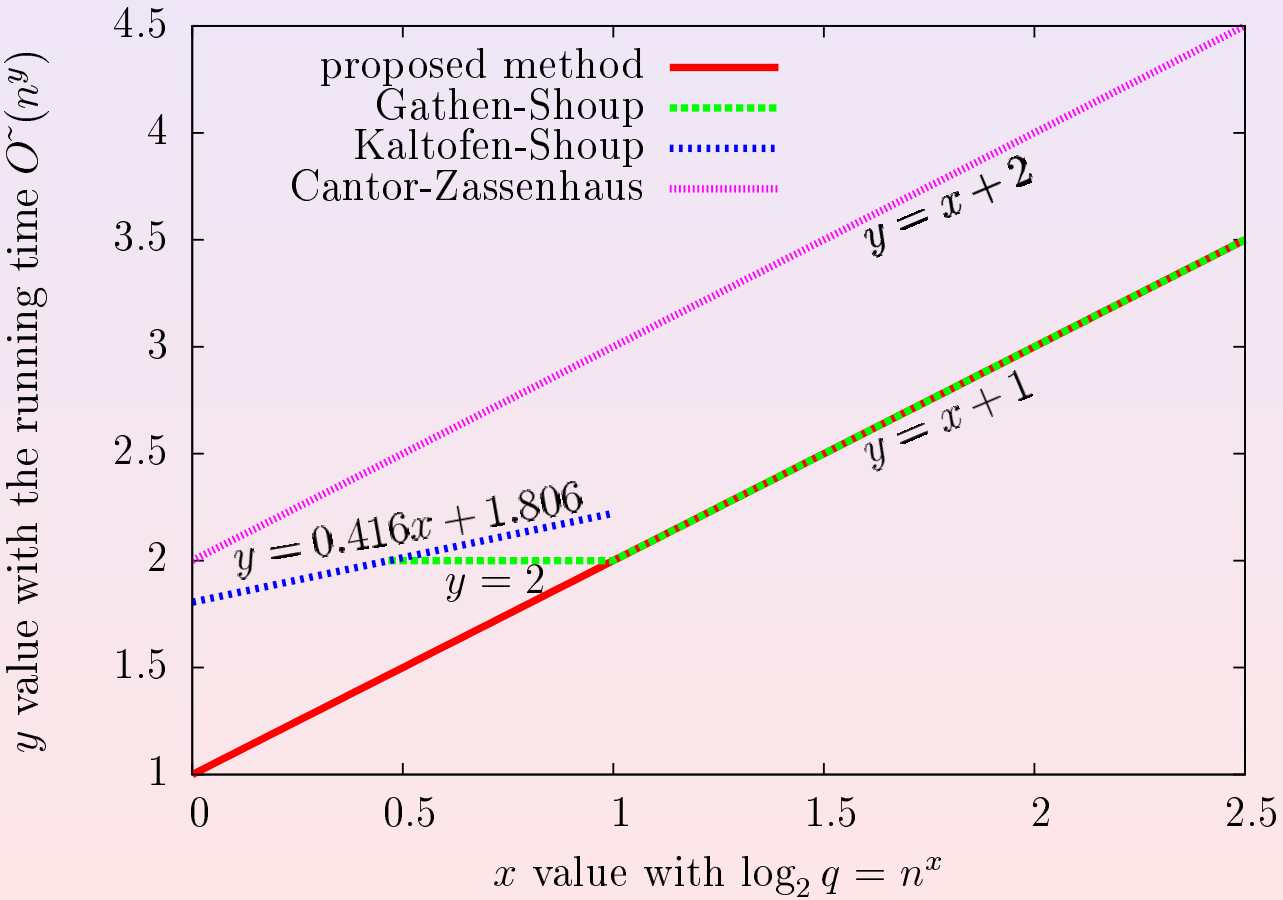
19. Theoretical cost (1/2)

the Berlekamp method (original and ours)



20. Theoretical cost (2/2)

Ours and the (improved) Cantor-Zassenhause methods



21. Experimental results (1/9)

For $f(x) = x^n - a$ over $\mathbb{F}_q$, we implement the original/our Berlekamp methods and the Cantor-Zassenhaus method with no improvement.

- 2.8 GHz Pentium G6950 with 1.6 GB RAM;
- The language is C with gcc 4.1.2 compiler;
- We do not use any mathematical library;
- We apply classical methods for polynomial operations;
- We do not perform the square-free factorization.
  $\Leftarrow$ We assume binomials to be square-free (i.e., $\mathbf{char}\mathbb{F}_q \nmid n$).

22. Experimental results (2/9)

Berlekamp method (original / ours)

- For the computation of the kernel $\mathcal{N}$ of the map $g(x) \mapsto g(x)^p - g(x) \bmod f(x)$,
  - original: apply the Gaussian elimination.
  - ours: apply orbits in $\mathbb{Z}/n\mathbb{Z}$ w.r.t. $\langle q \rangle$.
- After getting the kernel $\mathcal{N}$, the both methods perform the same procedure:
  $g(x) \in \mathcal{N} \Rightarrow \gcd(f(x), g(x))$ and $\gcd(g(x)^{(q-1)/2} - 1, f(x))$

23. Experimental results (3/9)

Cantor-Zassenhaus method

- Distinct-degree factorization: separate irre. factors of differing degree
  - $g_1(x) \leftarrow \gcd(f(x),\ x^q - x)$:
    the product of irre. factors of degree 1;
  - $g_2(x) \leftarrow \gcd(f(x)/g_1(x),\ x^{q^2} - x)$:
    the product of irre. factors of degree 2;
  - $g_3(x) \leftarrow \gcd(f(x)/(g_1(x)g_2(x)),\ x^{q^3} - x)$:
    the product of irre. factors of degree 3;
    And so on.
- Equal-degree factorization: separate irre. factors of same degree
  - $h(x)$: a random polynomial
    $\Rightarrow \gcd(h(x), g_i(x))$ and $\gcd(h(x)^{(q^i-1)/2}, g_i(x))$
    $(\deg g_i(x) = i\ell \ \Rightarrow\ \mathbb{F}_q[x]/(g_i(x)) \simeq \oplus_{1\le j\le \ell} \mathbb{F}_{q^i})$.

24. Experimental results (4/9)

Search test polynomials (1/2)

For $f(x) = x^n - a$ over $\mathbb{F}_q$, the factorization pattern depends on the number of roots of $x^n - a$ in $\mathbb{F}_{q^i}$ ($i \geq 1$), say δ_i. Then we see

$$\delta_i = \begin{cases} d_i & (a^{(q^i-1)/d_i} = 1 \text{ with } d_i = \gcd(q^i - 1, n)), \\ 0 & (\text{otherwise}). \end{cases}$$

$\Rightarrow$ the values δ_i's is determined by q, n and the multiplicative order of a (rather than the value of a).

Based on the facts above, we choose test polynomials to be factord.

25. Experimental results (5/9)

Search test polynomials (2/2)

Test polynomial(s) $x^n - a$ over $\mathbb{F}_p$ with $p = 2053$:
$\Rightarrow p - 1 = 2052 = 2^2 \times 3^2 \times 19$

- $a = 29 \Rightarrow \#\langle a \rangle = 171 = 3^2 \times 19$.
  - $n = 1083 \Rightarrow \gcd(n, p-1) > 1$ and $\#\langle a \rangle \nmid \frac{p-1}{\gcd(n,p-1)}$
    There exists no linear factor in $f(x)$ in the case.
  - $n = 1091 \Rightarrow \gcd(n, p-1) = 1$
  - $n = 1110 \Rightarrow \gcd(n, p-1) > 1$ and $\#\langle a \rangle \mid \frac{p-1}{\gcd(n,p-1)}$
    There exist some linear factors in $f(x)$ in the two cases above.
- $a = 1$, $n = 4104 (= 2(p-1))$
  $\Leftarrow$ To characterize the Berlekamp method
  and Cantor-Zassenhaus method

26. Experimental results (6/9)

- Running time for factorning $x^{1083} - 29$ over $\mathbb{F}_{2053}$

mehods		running time (s)
Berlekamp	original	0.075
	ours	0.005
(original) Cantor-Zassenhaus		92.368

- the pattern of factorization
  - 3 irreducible factors of degree 361.
- (ours) $\ll$ (original) for the Berlekamp method.
  $\Leftarrow$ (procedure after getting $\mathcal{N}$) $\ll$ (procedure for getting $\mathcal{N}$).
- (Berlekamp) $\ll$ (Cantor-Zassenhause)
  $\Leftarrow$ $x^{1083} - 29$ has irre. factors of large degree.
  ((procedure for getting $\mathcal{N}$)) $\ll$ (distict-degree factorization))

27. Experimental results (7/9)

- Running time for factorning $x^{1091} - 29$ over $\mathbb{F}_{2053}$

mehods		running time (s)
Berlekamp	original	0.309
	ours	0.235
(original) Cantor-Zassenhaus		223.654

- the pattern of factorization
  - 3 irreducible factors. More precisely,
    - 1 linear factor;
    - 2 irreducible factors of degree 545.
- (ours) $\approx$ (original) for the Berlekamp method.
  $\Leftarrow$ (procedure for getting $\mathcal{N}$) $\ll$ (procedure after getting $\mathcal{N}$).
- (Berlekamp) $\ll$ (Cantor-Zassenhause)
  $\Leftarrow$ $x^{1091} - 29$ has irre. factors of large degree.
  ((procedure for getting $\mathcal{N}$)) $\ll$ (distict-degree factorization))

28. Experimental results (8/9)

- Running time for factorning $x^{1110} - 29$ over $\mathbb{F}_{2053}$

mehods		running time (s)
Berlekamp	original	0.546
	ours	0.474
(original) Cantor-Zassenhaus		14.483

- the pattern of factorization
  - 42 irreducible factors. More precisely,
    - 6 linear factors;
    - 6 irreducible factors of degree 4;
    - 30 irreducible factors of degree 36.
- (ours) $\approx$ (original) for the Berlekamp method.
  $\Leftarrow$ (procedure for getting $\mathcal{N}$) $\ll$ (procedure after getting $\mathcal{N}$).
- (Berlekamp) < (Cantor-Zassenhause) (, not $\ll$)
  $\Leftarrow$ each irre. factor of it does not have so large degree.

29. Experimental results (9/9)

- Running time for factorning $x^{4104} - 1$ over $\mathbb{F}_{2053}$

mehods		running time (s)
Berlekamp	original	11.024
	ours	27.871
(original) Cantor-Zassenhaus		2.362

- the pattern of factorization
  - 3078 irreducible factors. More precisely,
    - $2052\ (= p - 1)$ linear factors;
    - $1026\ (= \frac{p-1}{2})$ irreducible factors of degree 2.
- (Cantor-Zassenhause) < (Berlekamp)
  $\Leftarrow$ each irre. factor of $x^{4104} - 1$ has small degree.
- (original) < (ours) for the Berlekamp method.
  $\Leftarrow$? (I guess I am not good at programing: It is possible not to omit some oblivious procedure(s), for example $1 \times \alpha$.)

30. Future works

- Analysis of other methods for binomials;
  (How much is the complexity reduced ?)
- Combination with other methods;
  (e.g., improved Cantor-Zassenhaus method)
- Extension to more general cases;
  (e.g., trinomial polynomials and large size of base field)
- Does there exist a deterministic polynomial factorization algorithm ?

Thank you!

Theoretical cost