Multiplicative Order of Gauss Periods

Omran Ahmadi[1] Igor Shparlinski[2] Jose Felipe Voloch[3]

[1]CSI, UCD

[2]Macquarie University

[3]University of Texas at Austin

July 17, 2009, $\mathbb{F}_{q^9}$

1, Notations

Some Notations

- $\mathbb{F}_q$ is the finite field with q elements for a prime power q.
- $\mathbb{F}_{q^n}$ is the degree n extension of $\mathbb{F}_q$.
- Generators of $\mathbb{F}_q^*$ are called primitive elements.

2

Open Question

Find an efficient algorithm for constructing primitive elements in finite fields.

- An algorithm is efficient if its running time is $(\log q^n)^{O(1)}$ arithmetic operations in $\mathbb{F}_{q^n}$.
- In many applications (Diffie-Hellman key establishment, pseudorandom bit generations, ...) a primitive element is needed.

3, Main Strategies

1. Find a small subset $S \subset \mathbb{F}_q$ containing a primitive element. (Distribution result) (quite efficient assuming GRH)
2. Test the elements of S to find a primitive element.

4,Testing primitiveness

- (Naive) Compute all the powers of $\alpha \in \mathbb{F}_q$.
- α is primitive iff $\alpha^{(q-1)/d} \neq 1$ for every prime $d|q-1$.
- (Bottleneck) Factorization (Subexponential time algorithm).
- Running time of number field sieve $O(\exp((c+o(1))(\ln q)^{1/3}(\ln \ln q)^{2/3}))$ bit operations.(Best asymptotic running time)

5, Relaxation of Primitive Element Problem

- In many application we need an element of large order.
- Given $\mathbb{F}_q$, it suffices to construct primitive element for $\mathbb{F}_{q^n}$ where n is in the some large subset of the positive integers.

6, Main Idea

- An element of $\mathbb{F}_{q^n}$ which is not in any subfield has minimal polynomial of degree n over $\mathbb{F}_q$.
- If $f(\alpha) = 0$, then $f(\alpha^q) = 0$.
- Powers of an element and its degree are related through its minimal polynomial.
- AKS Deterministic Primality Testing Algorithm

7,Qi Cheng's Result

Theorem (Q. Cheng, 2004)

Let q be a fixed prime power and let N be a positive integer. Then in time polynomial in N an integer $n \in [N, 2qN]$ and $\alpha \in \mathbb{F}_{q^n}$ being of order at least $5.8^{n/\log_q n}$ can be found.

Theorem (Q. Cheng, 2004)

Let q be a fixed prime power and let N be a positive integer. Then in time polynomial in N an integer $n \in [N, N + O(N^{0.77})]$ and $\alpha \in \mathbb{F}_{q^n}$ being of order at least $5.8^{\sqrt{n}}$ can be found.

8, Main Idea and Proof

- Lemma: Let q be a prime power and let $n|q-1$.If $x^n - u \in \mathbb{F}_q[x]$ is an irreducible polynomial over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ is one of its roots, Then for any $a \in \mathbb{F}_q^*$, $\alpha + a$ has order greater than 5.8^n.
- Conjugates of α are $c_1\alpha, c_2\alpha, \ldots, c_n\alpha$ where c_i's are n-th roots of unity in $\mathbb{F}_q$.
- Conjugates of $\alpha + a$ are $c_i\alpha + a$'s.

9, Proof

- Let e_i's be positive integers such that $\sum e_i \leqslant n-1$.
- Take the elements $(\alpha + a)^{\sum e_i q^i} \in \mathbb{F}_{q^n}$.
- $(\alpha + a)^{\sum e_i q^i} = \prod(\alpha + a)^{e_i q^i} = \prod(c_i\alpha + a)^{e_i}$.
- If $\prod(c_i\alpha + a)^{e_i} = \prod(c_i\alpha + a)^{f_i}$, then the degree of $\alpha \leqslant n$.(a contradiction)
- α becomes a root of $\prod(c_i x + a)^{e_i} - \prod(c_i x + a)^{f_i}$.

10, Gauss Periods

Definition

Let $r = 2n + 1$ be a prime number coprime with q and $\beta \in \mathbb{F}_{q^{2n}}$ be a primitive r-th root of unity. Then the element

$$\alpha = \beta + \beta^{-1} \in \mathbb{F}_{q^n} \tag{1}$$

is called a Gauss period of type $(n, 2)$.

Theorem

If q is a primitive root modulo r, and α is a Gauss period, then $NB = \left\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\right\}$ is a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this case, the minimal polynomial of β is of degree $2n$.

11, Orders of Gauss periods

Theorem (I. Shparlinski and J. von zur Gathen, 1998)

Let p be the characteristic of $\mathbb{F}_q$ and let q be a primitive root modulo a prime $r = 2n + 1$ and β be a primitive r-th root of unity in $\mathbb{F}_{q^{2n}}$. Then the multiplicative order of $\alpha = \beta + \beta^{-1}$ is at least

$$2^{\sqrt{2n}}.$$

Theorem (ASV)

With the assumptions as above the multiplicative order of α is at least

$$P(n-1, p-1).$$

$P(m, k)$ is the number of integer partitions of m where no part appears more than k times.

12, Orders of Gauss Periods

Corollary (ASV)

Assuming everything as the last theorem the multiplicative order of α is at least

$$\exp\left(\left(\pi\sqrt{\frac{2(p-1)}{3p}}+o(1)\right)\sqrt{n}\right),$$

as $n \to \infty$.

- When $p > n$, the order of α is at least $13^{\sqrt{n}}$.
- When $p = 2$, the order of α is at least $6.13^{\sqrt{n}}$.

13, Proof

- $\mathfrak{P} = \left\{(u_1, \ldots, u_{n-1}) \mid \sum_{j=1}^{n-1} u_j j = n-1,\ 0 \leqslant u_i's \leqslant p-1\right\}$.
- Let $q^{z_j} \equiv j \pmod{r}$, $0 \leqslant z_j < r$. (q is a primitive root modulo r)
- If $(u_1, \ldots, u_{n-1}), (v_1, \ldots, v_{n-1}) \in \mathfrak{P}$ and $(u_1, \ldots, u_{n-1}) \neq (v_1, \ldots, v_{n-1})$, then $\alpha^{\sum u_i q^{z_i}} \neq \alpha^{\sum v_i q^{z_i}}$.
- $\alpha^{\sum u_i q^{z_i}} = \prod(\beta^{q^{z_i}} + \beta^{-q^{z_i}})^{u_i} = \prod(\beta^i + \beta^{-i})^{u_i} = \beta^{n-1} \prod(\beta^{2i} + 1)^{u_i}$.

14, Applying Polynomial ABC Theorem

- $\alpha^{\sum v_i q^{z_i}} = \beta^{n-1} \prod (\beta^{2i} + 1)^{v_i}$.
- If $\alpha^{\sum u_i q^{z_i}} = \alpha^{\sum v_i q^{z_i}}$, then $\prod (\beta^{2i} + 1)^{u_i} = \prod (\beta^{2i} + 1)^{v_i}$.
- β is of degree $2n$.(A contradiction)

Theorem (Polynomial ABC theorem)

Let A, B, C be nonzero polynomials over $\mathbb{F}_q$ with $A + B + C = 0$ and $\gcd(A, B, C) = 1$. If $\deg A \geqslant \deg \mathrm{rad}\, ABC$, then $A' = 0$.

- Using ABC we can beat GS bound but still unable to beat the partition bound.

Outlook

- Outlook
  - Get similar bound for other types of Gauss periods.
  - Apply polynomial ABC theorem.