ORDERS OF GAUSS PERIODS IN FINITE FIELDS

Joachim von zur Gathen and Igor Shparlinski

June 17, 1996

Abstract

It is shown that Gauss periods of a special type give an explicit polynomial-time computation of elements of exponentially large multiplicative order in some finite fields. This can be considered as a step towards solving the celebrated problem of finding primitive roots in finite fields in polynomial time.

1 Introduction

One of the most important unsolved problems in the computational theory of finite fields is to design a fast algorithm to construct primitive roots in a finite field $\mathbb{F}_q$ of q elements. All known algorithms for this problem work in two stages:

1. Find a "small" set $\mathcal{M} \subseteq \mathbb{F}_q$ guaranteed to contain a primitive root of $\mathbb{F}_q$.
2. Test all elements of $\mathcal{M}$ for primitivity.

In many cases, we have quite good algorithms for the first stage, especially if one assumes the Extended Riemann Hypothesis (ERH); see Chapter 3 of [16]. Unfortunately, at the current state of the art, the second stage requires the integer factorization of $q-1$ which is not known to be obtainable in polynomial time. It is demonstrated in [17] that we can find a primitive root of $\mathbb{F}_q$ in time $O(q^{1/4+\varepsilon})$ for any $\varepsilon > 0$. Even the ERH cannot help too much here.

On the other hand, for many applications, instead of a primitive root just an element of high multiplicative order is sufficient. Such applications include but are not limited to cryptography, coding theory, pseudo random number generation and combinatorial designs. As a specific example we point out the sparse polynomials interpolation algorithms [1, 19] where instead of a primitive root just an element of large order can be used (after some simple adjustments of the other parameters). Also, it is often enough to solve such a problem for some sufficiently "dense" sequence of fields, rather than for all fields.

In this paper we design, under these two relaxations of the original problem, fast deterministic algorithms.

The work was motivated by and can be considered as a continuation of [2] whose key tool are special Gauss periods over finite fields which are shown to generate *normal bases.* Experimental results indicate that such periods often produce primitive roots and thus generate *primitive normal bases,* or at least have high multiplicative order.

In Section 2 we concentrate on the following special case of a Gauss period in $\mathbb{F}_{q^n}$. Let $r = 2n + 1$ be a prime not dividing q, and let β be a primitive rth root of unity in $\mathbb{F}_{q^{2n}}$. Then

$$\alpha = \beta + \beta^{-1} \in \mathbb{F}_{q^{2n}},$$

where φ is the Euler function, is called a *Gauss period of type* $(n, 2)$ over $\mathbb{F}_q$. It is, in fact, an element of $\mathbb{F}_{q^n}$. We refer to [10] and [2] for the literature of this topic. In Section 3 we consider a more general variant of these Gauss periods.

If we know the minimal polynomial of β over $\mathbb{F}_q$ (i.e., we have factored $x^r - 1$ over $\mathbb{F}_q$), that of α can be determined by linear algebra over $\mathbb{F}_q$, in polynomial time. While a deterministic polynomial time algorithm to factor polynomials over finite fields is not known, there are many efficient (probabilistic and deterministic, unconditional and ERH–dependent) methods. We just mention that $x^r - 1$ can be completely factored over $\mathbb{F}_q$ with the following number of arithmetic operations in $\mathbb{F}_q$:

- $(r \log q)^{O(1)}$ probabilistically,
- $r^{O(1)} q^{1/2} \log q$ deterministically,
- $(r \log q)^{O(1)}$ deterministically under the ERH.

More precise forms of these assertions and further details can be found in [16], Section 1.1. If q is a primitive root modulo the prime r, then the characteristic polynomial of β is $x^{r-1} + \ldots + x + 1$. This can be used in the construction of Theorem 1 below.

In this paper we do not estimate the cost of constructing α (which, as we mentioned above, is fairly small) but rather concentrate on the cost of finding n for which the corresponding α is of large period.

Gauss periods of type (n, k) for $k > 2$ can be defined similarly and are of great interest as well, but unfortunately at the moment we cannot give any lower bounds on their multiplicative order. This remains an interesting open problem.

2 Large-order normal elements

Let A be the set of all integers $a \in \mathbb{N}$ for which Artin's conjecture holds in the following form:

$$\exists C(a), x_0(a) \quad \forall x \geq x_0(a) \qquad \pi_a(x) \geq x/(C(a) \log^2 x), \tag{1}$$

where $\pi_a(x)$ is the number of primes up to x for which a is a primitive root. It is known that A contains the odd powers of all but at most two prime numbers [4], and of all prime numbers under the ERH [5]; many other relevant results can be found in [11]. For any $a \in \mathbb{N}$, clearly $a^2 \notin A$.

Theorem 1. *For any prime power $q = p^k \in A$ and any sufficiently large integer N there is an integer $n = (r-1)/2$ with $N \leq n \leq M$, where $M = 3C(q)N \log N$ and $C(q)$ is as in (1), such that the Gauss period $\alpha = \beta + \beta^{-1} \in \mathbb{F}_{q^n}$, where β is a primitive rth root of unity over $\mathbb{F}_q$, generates a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and has multiplicative order at least*

$$2^{(2n)^{1/2}-2}.$$

For any $\varepsilon > 0$, such an n can found with the following number of bit operations:

- $O(C(q) \exp[(1+\varepsilon) \log^{1/2} M \log^{1/2} \log M])$ *probabilistically,*
- $O(M^{5/4+\varepsilon})$ *deterministically,*

∘ $O(M^{6/5+\varepsilon})$ *deterministically under the ERH.*

Proof. Let R be the set of primes r in the interval $[2N+1, 2M+1]$ for which q is a primitive root. We first estimate $\#R$ from below. More precisely, we show that for N large enough

$$\#R \geq \pi_a(2M+1) - \pi(2N) > \frac{M}{C(q)\log^2(2M)}. \tag{2}$$

Indeed, assume that N is such that $M \geq \max\{4, x_0(q)\}$ so that

$$\frac{2M+1}{\log^2(2M+1)} \geq \frac{2M}{\log^2(2M)}),$$

and

$$3(\log(2N) - 3/2)\log N > 2\log^2(6C(q)N\log N).$$

Then,

$$\frac{\pi_a(2M+1)}{2} \geq \frac{M}{C(q)\log^2(2M)} \geq \frac{3N\log N}{\log^2(6C(q)N\log N)} > \frac{2N}{\log(2N) - 3/2}.$$

We have

$$\frac{2N}{\log(2N) - 3/2} \geq \pi(2N)$$

by [13], (3.4). Therefore $\pi_a(2M+1) - \pi(2N) \geq 0.5\pi_a(2M+1)$ and (2) follows.

It follows from (2) that $\pi_a(2M+1) > \pi(2N)$, hence $R \neq \emptyset$.

For any $r \in [2N+1, 2M+1]$, we test whether $r \in R$ as follows. First, we check if r is prime. Then we factor $r-1$ and check if q is a primitive root modulo r by testing if

$$q^{(r-1)/l} \not\equiv 1 \bmod r$$

for each prime divisor l of $r-1$. The latter can be done in polynomial time. Primality testing and finding the integer factorization of $r-1$ can be both done, for any $\varepsilon > 0$, with the following number of bit operations:

∘ $O(\exp[(1+\varepsilon)\log^{1/2} M \log^{1/2}\log M])$ probabilistically [9],

∘ $O(M^{1/4+\varepsilon})$ deterministically [15],

∘ $O(M^{1/5+\varepsilon})$ deterministically under the ERH [14].

For a probabilistic algorithm, we select r uniformly at random in the interval $[2N+1, 2M+1]$, then the probability of success is at least

$$\frac{\#R}{\#[2N+1,2M+1]} \geq \frac{\pi_a(2M+1)-\pi(2N)}{2M} \geq \frac{1}{2C(q)\log^2(2M)},$$

by (2). For a deterministic algorithm we test all numbers $r \in [2N+1, 2M+1]$.

Now, let $r \in R$ and $n = (r-1)/2$. Then $\varphi(r) = 2n$. Let $\beta \in \mathbb{F}_{q^{2n}}$ be a primitive rth root of unity, and $\alpha = \beta + \beta^{-1} \in \mathbb{F}_{q^n}$. It generates a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ [2]. Let

$$h = \lfloor r^{1/2} \rfloor - 1, \quad H = \{1, ..., h\} \subseteq \mathbb{F}_r, \quad S = \{\operatorname{ind} a : a \in H\} \subseteq \mathbb{Z}_{r-1},$$

where we identify $\mathbb{F}_r$ with $\{0, \ldots, r-1\}$, and $\operatorname{ind} a$ is the index (or discrete logarithm) of $a \in \mathbb{F}_r$ in base q. Let $U, U' \subseteq S$ be two different subsets of S, and

$$u = \sum_{s \in U} q^s, \quad u' = \sum_{s \in U'} q^s.$$

We claim that $\alpha^u \neq \alpha^{u'}$. This implies that we have at least $2^{\#S} = 2^h$ distinct powers of α, and thus the order of α is at least

$$2^h \geq 2^{(2n)^{1/2}-2}.$$

We may suppose that $U \cap U' = \emptyset$. Assume that $\alpha^u = \alpha^{u'}$. Then

$$\begin{aligned} 0 &= \alpha^u - \alpha^{u'} = \prod_{s \in U} (\beta + \beta^{-1})^{q^s} - \prod_{s \in U'} (\beta + \beta^{-1})^{q^s} \\ &= \beta^{-u} \prod_{s \in U} (\beta^{2q^s} + 1) - \beta^{-u'} \prod_{s \in U'} (\beta^{2q^s} + 1). \end{aligned}$$

Since β is an rth root of unity, we may reduce the exponents modulo r, and with

$$E = \{q^s \text{ rem } r : s \in U\}, \quad E' = \{q^s \text{ rem } r : s \in U'\} \subseteq H,$$

where $(q^s \text{ rem } r) \in \mathbb{N}$ is the positive remainder of q^s on division by r, and

$$e = \sum_{t \in E} t, \quad e' = \sum_{t \in E'} t,$$

we have $E \cap E' = \emptyset$, and

$$0 = \beta^{-e} \prod_{t \in E} \left(\beta^{2t} + 1\right) - \beta^{-e'} \prod_{t \in E'} \left(\beta^{2t} + 1\right).$$

We may assume that $e' \ge e$, and let

$$f(x) = x^{e'-e} \prod_{t \in E} \left(x^{2t} + 1\right) - \prod_{t \in E'} \left(x^{2t} + 1\right) \in \mathbb{F}_q[x].$$

Then $f(\beta) = 0$, and

$$\deg f \le 2e' \le 2 \sum_{i \in H} i = h(h+1) \le r - \sqrt{r} < r - 1.$$

Since q is primitive modulo r, β has degree $r-1$ over $\mathbb{F}_q$, and therefore the polynomial f is zero. If $e' > e$, then $f(0) = -1$. Thus $e' = e$. But then the monomial x^{2t} occurs in f with nonzero coefficient, where $t = \min(E \cup E')$. This contradiction proves the claim. $\square$

We note that under the ERH, from the asymptotic formula for $\pi_a(x)$ of [5], one can get a slightly better estimate for n, namely apparently one can take $M = cN \log\log\log q$, provided that $N > q^C$ with some absolute constants c and C. Unfortunately C does not seems to be effectively computable and it is not clear how to use this better bound in order to design a faster algorithm. On the other hand, all constants occurring in [4] are effective and thus lead to an effective form of (1) for odd powers of all but at most two prime numbers.

3 A denser sequence of large-order elements

In the next theorem we eliminate the condition that q belongs to A and consider a denser sequence of n. The price we pay is losing the property of α being normal and a weaker lower bound. The work [3] addresses the question of whether α is normal over $\mathbb{F}_q$; this is not the case unless r is squarefree, which never happens in our construction.

Theorem 2. *There is an absolute constant $C > 0$ such that for any prime power q and any sufficiently large $N \ge 2$ there are integers n and r with*

$$N \le n = \varphi(r) \le N + O(N/\log^C N),$$

and such that the Gauss period $\alpha = \beta + \beta^{-1} \in \mathbb{F}_{q^n}$, where β is a primitive rth root of unity over $\mathbb{F}_q$, has multiplicative order at least

$$2^{c_q n^{1/2} - 25}$$

where

$$c_q = 10q^{-12}. \tag{3}$$

For any $\varepsilon > 0$, such n and r can be found with $O(\log^{2+\varepsilon} N)$ bit operations.

Proof. We let p be the characteristic of $\mathbb{F}_q$ and define

$$(l_1, l_2) = \begin{cases} (3,5), & \text{if } p = 2 \text{ or } p \geq 7, \\ (5,7), & \text{if } p = 3, \\ (3,7), & \text{if } p = 5, \end{cases}$$

$$\psi_q = \frac{l_1 l_2}{\varphi(l_1 l_2)} = \begin{cases} 15/8, & \text{if } p = 2 \text{ or } p \geq 7, \\ 35/24, & \text{if } p = 3, \\ 7/4, & \text{if } p = 5. \end{cases}$$

If k_1 and k_2 are positive integers, then

$$l_1^{k_1} l_2^{k_2} = \psi_q \varphi(l_1^{k_1} l_2^{k_2}).$$

Let r_0 be the smallest integer greater than $R = \psi_q N / l_1 l_2$ of the form $r_0 = l_1^{m_1} l_2^{m_2}$, where m_1, m_2 are nonnegative integers. Tijdeman's result [18] on the distribution of numbers containing only a fixed set of primes in their factorization implies that

$$R \leq r_0 \leq R + O(N / \log^C N)$$

with some absolute constant $C > 0$. Thus if we define $r = r_0 l_1 l_2$ and $n = \varphi(r) = \psi_q^{-1} r$, then $N \leq n \leq N + O(N/\log^C N)$.

To estimate the cost, we note that $r_0 = l_1^{m_1} l_2^{m_2} \leq l_1 R$. Therefore, $0 \leq m_i \leq K_i$ for $i = 1, 2$, where

$$K_i = \left\lfloor \frac{\log(l_1 R)}{\log l_i} \right\rfloor.$$

To find r_0, for each

$$k_1 \in \{0, \ldots, K_1\},$$

we compute $k_2 = \lceil \log(R l_1^{-k_1}) / \log l_2 \rceil$, so that

$$l_1^{k_1} l_2^{k_2 - 1} \leq R \leq l_1^{k_1} l_2^{k_2}.$$

For each k_1, this can be done with $O(\log^{1+\varepsilon} N)$ bit operations. From the $K_1 = O(\log N)$ numbers obtained we select the smallest one as r_0.

Let t be the order of q modulo r,

$$h = \left\lfloor (r/2)^{1/2} - t_0 r/t \right\rfloor, \quad S = \{s\colon\ 0 \le s < t \text{ and } 1 \le (q^s \text{ rem } r) \le h\},$$

where as before $(q^s \text{ rem } r) \in \mathbb{N}$ is the positive remainder of q^s on division by r. Let t_0 be the order of q modulo $l_1 l_2$. We define γ_i as the largest power of l_i which divides $q^{t_0} - 1$, for $i = 1, 2$. We need the following inequalities

$$l_1^{\gamma_1} l_2^{\gamma_2} < q^{t_0}, \quad 1 \le t_0 \le \mathrm{lcm}(l_1 - 1, l_2 - 1) \le 12.$$

Korobov [7], Remark after Lemma 1, shows that

$$t \ge t_0 l_1^{-\gamma_1} l_2^{-\gamma_2} r > t_0 q^{-t_0} r \ge 12 q^{-12} r$$

(see also [8], beginning of Section 1). In particular, we see that h is positive for sufficiently large N. Korobov [7], Lemma 2, implies that

$$|\#S - th/r| \le t_0$$

(see also [8], Fact 2). Thus we have $\#S \le th/r + t_0 \le t(2r)^{-1/2}$ and

$$2h\#S \le 2((r/2)^{1/2} - t_0 r/t) \cdot t(2r)^{-1/2} < t.$$

Now we recall that the degree of the minimal polynomial of a primitive rth root of unity β over $\mathbb{F}_q$ equals t. We define $\alpha = \beta + \beta^{-1}$. Since $q^n \equiv 1 \bmod r$, we have $\alpha \in \mathbb{F}_{q^n}$.

Let $U, U' \subseteq S$ be two different subsets and

$$u = \sum_{s \in U} q^s, \qquad u' = \sum_{s \in U'} q^s.$$

If we assume that $\alpha^u = \alpha^{u'}$, then as in the proof of Theorem 1 we define the sets

$$E = \{q^s \text{ rem } r : s \in U\}, \quad E' = \{q^s \text{ rem } r : s \in U'\} \subseteq \{1, \ldots, h\},$$

and the numbers

$$e = \sum_{t \in E} t, \quad e' = \sum_{t \in E'} t.$$

If, say, $e' \ge e$, then we find that β is a root of the non-zero polynomial

$$f(x) = x^{e'-e} \prod_{t \in E} \left(x^{2t} + 1\right) - \prod_{t \in E'} \left(x^{2t} + 1\right) \in \mathbb{F}_q[x].$$

Furthermore, $\deg f \le 2h\#S < t$; thus our assumption is false.

Therefore, we have at least $2^{\#S}$ distinct powers of α. The claim follows from

$$\begin{aligned} \#S &\ge th/r - t_0 \ge t(2r)^{-1/2} - 2t_0 - t/r \\ &\ge 12(35/48)^{1/2}q^{-12}n^{1/2} - 25 \ge 10q^{-12}n^{1/2} - 25. \quad \square \end{aligned}$$

4 Concluding remarks

The constants in Theorem 2 can be easily refined. We do not do this because we believe that our subexponential lower bound can be essentially improved, perhaps up to $\exp(C(q)m)$ with some $C(q) > 0$.

Our method can produce several more results. For example, it can be shown that if the multiplicative order q modulo $r = 2n + 1$ with $\gcd(r, q) = 1$ is greater than $r^{3/4+\delta}$ with $\delta > 0$, then the construction of Theorem 2 produces an element of order at least

$$\exp(c(q)n^{2\delta}/\log n).$$

This is based on another estimate of Korobov [8]

$$\#S = th/r + O(r^{1/2}\log r)$$

(which can be extracted from the proof of Theorem 3 of that paper). Thus h can be chosen of order $r^{3/2}t^{-1}\log r$, hence $\#S \sim r^{1/2}$. Then one can consider subsets of S with at most $k = \lfloor t/h \rfloor \sim t^2 r^{-3/2}\log^{-1} r$ elements. Accordingly, the order can be estimated from below by

$$\binom{\#S}{k} \ge 2^k \ge 2^{\left(1+o(1)\right)t^2 r^{-3/2}\log^{-1} r}$$

In particular if $r = 2n + 1$ is relatively prime to q and q generates a group of bounded index in the group of units modulo r, the same construction produces α of order at least

$$\exp(c(q)n^{1/2}/\log n)$$

(the logarithmic term can possibly be eliminated). This and several other similar statements which can be obtained within the framework of the method of this paper show that the class of pairs (q, r) which generate elements of large order can be substantially extended.

We also hope that exponentially large lower bounds can be obtained for almost all primes $r = 2n + 1$ if one uses the bound of exponential sums from [6] (instead of Korobov's estimate [8]) and Pappalardi's estimates [12] of the multiplicative orders of a given integer modulo almost all primes.

Finally we note one more interesting question which we believe can be approached by the method of this paper. Given $N > 1$, find a small s (say $s = N^{O(1)}$) such that the Gauss period $\alpha \in \mathbb{F}_{q^n}$ of type $(n, 2)$ over $\mathbb{F}_q$, where $n = sN$, has exponentially large multiplicative order. That is, instead of finding elements of large multiplicative order in a field $\mathbb{F}_{q^n}$ with n close to a given N, now we are looking for a such an element in a not too large extension of a given field $\mathbb{F}_{q^N}$.

Acknowledgment. This paper was essentially written during two visits by the second author to the University of Paderborn, whose hospitality is gratefully acknowledged. The authors would like to thank Francesco Pappalardi for a useful discussion of the effective computability issues related to Artin's conjecture. The first version of this paper appeared in the Proceeding of the 6th International Symposium on Algorithms and Computation, Cairns, 1995 (Lect. Notes in Comp. Sci., 1995, vol. 1004, pp. 208–215).

References

[1] M. Clausen, A. Dress, J. Grabmeier and M. Karpinski, "On zero testing and interpolation of k-sparse multivariate polynomials over finite field", *Theor. Comp. Sci.*. **84** (1991), 151–164.

[2] S. Gao, J. von zur Gathen and D. Panario, "Gauss periods and fast exponentiation in finite fields", *Proceedings LATIN '95, Springer Lecture Notes in Comp. Sci.*, **911** (1995), 311–322.

[3] J. von zur Gathen and S. Schlink, "Normal bases via general Gauß periods", Technical Report, Department of Mathematics and Computer Science, *Universität–GH Paderborn*, 1996.

[4] D. R. Heath-Brown, "Artin's conjecture for primitive roots", *Quart. J. Math.*, **37** (1986), 27–38.

[5] C. Hooley, "On Artin's conjecture", *J. Reine Angew. Math.*, **225** (1967), 209–220.

[6] S. V. Konyagin and I.E.Shparlinski, "On the distribution of residues of finitely generated multiplicative groups and their applications" *Macquarie Math. Reports*, 95/172C, 1995, 1–70.

[7] N. M. Korobov, "Тригонометрические суммы с показательными функциями и распределение знаков периодических дробей", *Matem. Zametki*, **8** (1970), 641–652. *Matem. Notes*, **8** (1970), 831–837.

[8] N. M. Korobov, "О распределении знаков в периодических дробях", *Matem. Sbornik*, **89** (1972), 654–670. *Mat. USSR-Sb.*, **18** (1972), 659–676.

[9] H. W. Lenstra and C. Pomerance, "A rigorous time bound for factoring integers", *J. Amer. Math. Soc.*, **5** (1992), 483–516.

[10] A. J. Menezes and I. F. Blake and X.H. Gao and R. C. Mullin and S. A. Vanstone and T. Yaghoobian, "Applications of finite fields", *Kluwer Academic Publishers*, Norwell MA, 1993.

[11] W. Narkiewicz, *Classical problems in number theory*, Polish Sci. Publ., Warszawa, 1986.

[12] F. Pappalardi, "On the Order of Finitely Generated Subgroups of $\mathbb{Q}^* \pmod p$ and Divisors of $p-1$", *J. Number Theory*, **57** (1996), 207-222.

[13] J.B. Rosser and L. Schoenfeld, "Approximate functions for some functions of prime numbers ", *Illinois J. Math.* **6** (1962), 64–94.

[14] R. J. Schoof, "Quadratic fields and factorization", *Computational Methods in Number Theory*, Amsterdam, 1984, 235–279.

[15] D. Shanks, "Class number, a theory of factorization and genera", *Proc. Symp. in Pure Math.*, Amer. Math. Soc., Providence, 1971, 415–420.

[16] I. Shparlinski *Computational and algorithmic problems in finite fields*, Kluwer Acad. Publ., Dordrecht, 1992.

[17] I. Shparlinski, "On finding primitive roots in finite fields", *Theor. Comp. Sci.* (to appear).

[18] R. Tijdeman, "On the maximal distance between integers composed of small primes", *Compos. Math.*, **28** (1974), 159–162.

[19] K. Werther, "The complexity of sparse polynomials interpolation over finite fields", *Appl. Algebra in Engin., Commun. and Comp.*, **5** (1994), 91–103.

Joachim von zur Gathen
FB Mathematik-Informatik
Universität-GH Paderborn
33100 Paderborn, Germany
gathen@uni-paderborn.de

Igor Shparlinski
School of MPCE
Macquarie University
Sydney, NSW 2109, Australia
igor@mpce.mq.edu.au