논문 2008-45TC-6-5

선형 요소에 의해 생성된 부분그룹의 크기에 관한 연구

(On The Size of The Subgroup Generated by Linear Factors)

취 첸*, 황 선 태**

(Qi Cheng and Suntae Hwang)

요 약

차수가 h인 다항식 $\hbar(x)\in \mathrm{F}_q[x]$에서, $x-s_1, x-s_2, \cdots, x-s_n$ 에 의해 생성된 $(\mathrm{F}_q[x]/(\hbar(x)))^*$의 multiplicative subgroup의 크기를 결정하는 것은 대단히 중요한 과제이다. 여기서 $\{s_1, s_2, \cdots, s_n\} \subseteq \mathrm{F}_q$이고 모든 i 에 대해서, $\hbar(x) \neq 0$이다. 지금까지 알려진 asymptotic lower bound는 $(rh)^{\mathrm{O}(1)}\left(2er+\mathrm{O}(\frac{1}{r})\right)^h$이며, 여기서 $r=\frac{n}{h}$이고 $e(=2.718...)$는 natural logarithm의 기저이다. 본 논문에서는, coding theory 문제와 연계해서 더 낳은 lower bound인 $(rh)^{\mathrm{O}(1)}\left(2er+\frac{e}{2}\log r-\frac{e}{2}\log\frac{e}{2}+\mathrm{O}(\frac{\log^2 r}{\mathrm{r}})\right)^h$를 증명하고자 한다. 여기서 log는 natural logarithm을 나타내며, 또한 이 방식의 제약점에 대해서도 논의한다.

Abstract

Given a polynomial $\hbar(x)\in \mathrm{F}_q[x]$ of degree h, it is an important problem to determine the size of multiplicative subgroup of $(\mathrm{F}_q[x]/(\hbar(x)))^*$ generated by $x-s_1, x-s_2, \cdots, x-s_n$, where $\{s_1, s_2, \cdots, s_n\} \subseteq \mathrm{F}_q$, and for all i, $\hbar(x) \neq 0$. So far the best known asymptotic lower bound is $(rh)^{\mathrm{O}(1)}\left(2er+\mathrm{O}(\frac{1}{r})\right)^h$, where $r=\frac{n}{h}$ and $e(=2.718...)$ is the base of natural logarithm. In this paper, we exploit the coding theory connection of this problem and prove a better lower bound $(rh)^{\mathrm{O}(1)}\left(2er+\frac{e}{2}\log r-\frac{e}{2}\log\frac{e}{2}+\mathrm{O}(\frac{\log^2 r}{\mathrm{r}})\right)^h$, where log stands for natural logarithm. We also discuss about the limitation of this approach.

Keywords: Subgroup, Linear Factor, Reed-Solomon Code

I. Introduction

Let q be a prime power and F_q be the finite field with q elements. Let S be a subset of F_q of n elements. Given a polynomial ring $\mathrm{F}_q[x]/(\hbar(x))$, it is an important problem to determine the size of multiplicative subgroup generated by $\{x-s \mid s\in\}$ where for all $s\in S$, $\hbar(s)\neq 0$. We denote this subgroup by G throughout the paper. This problem has been studied in the case that $S=\mathrm{F}_q$ and $\hbar(x)$ is irreducible[3, 5, 7]. The invention of AKS primality testing sparks a renewed interest in this problem, especially in the case when the cardinality of S is polylogarithmic in q. It was pointed out in [1] that

* 정회원, School of Computer Science, the University of Oklahoma, Norman, OK 73019, USA
(School of Computer Science, the University of Oklahoma, Norman, OK 73019, USA.)
** 평생회원, 대전대학교 정보통신공학과
(Daejeon University).
※ The research was done while visiting the University of Oklahoma
※ This work is partially supported by NSF Career Award CCR-0237845.
접수일자: 2007년10월17일, 수정완료일: 2008년6월19일

the AKS primality testing algorithm can be speed up by a factor $(\frac{\log B'}{\log B})$ if we can find a better lower bound B' rather than using the known lower bound B. Moreover, if the lower bound is $q^{h/c}$ for some positive constant c when $h = \mathrm{O}(\log q)$ and $|S| = \mathrm{O}(h)$, then the randomized AKS primality proving can run in time $\log^{3+\epsilon} q$ instead of $\log^{4+\epsilon} q$.

Denote $\frac{|S|}{h}$ by r. Based on[6], Bernstein[1, Section 7] formulates a lower bound for the size of G

$$\max_{0 \le c \le rh} \binom{rh}{c_-}\binom{c}{c_-}\binom{rh-c_-+r-1-c}{h-1-c}.$$

The maximum was achieved at $c = \frac{h}{2}$, $c_- = \frac{r+1-\sqrt{1+r2}}{2}h$. Plugging them in, the lower bound is $(rh)^{\mathrm{O}(1)}\gamma_1^h$, where

$$\gamma_1 = 2^{\gamma}\gamma^{\gamma}\left(1+\gamma-\sqrt{1+\gamma^2}\right)^{-1-\gamma+\sqrt{1+\gamma^2}}$$
$$\left(-\gamma+\sqrt{1+\gamma^2}\right)^{\frac{1}{2}\left(r-\sqrt{1+\gamma^2}\right)}$$
$$\times\left(-1+\gamma+\sqrt{1+\gamma^2}\right)^{1-r-\sqrt{1+\gamma^2}}$$
$$\left(\gamma+\sqrt{1+\gamma^2}\right)^{\frac{1}{2}\left(\gamma+\sqrt{1+\gamma^2}\right)}$$

In Appendix, we show that $\gamma_1 = 2er + \mathrm{O}\left(\frac{1}{r}\right)$. This gives the best known lower bound $(rh)^{\mathrm{O}(1)}\left(2er+\frac{e}{2}\log r-\frac{e}{2}\log\frac{e}{2}+\mathrm{O}(\frac{\log^2 r}{\mathrm{r}})\right)^h$. for the size of . In this paper we prove the following theorem.

Theorem [1] The group G has cardinality greater than $(rh)^{\mathrm{O}(1)}\left(2er+\frac{e}{2}\log r-\frac{e}{2}\log\frac{\mathrm{e}}{2}+\mathrm{O}\left(\frac{\log^2 r}{r}\right)\right)^h$.

Our lower bound is asymptotically better. We also calculate explicitly the low bounds for r from 1 to 100. Our bound is bigger than the best known bound starting from $r \ge 2$. If we use , then our bound speed the AKS primality algorithm by a factor $\left(\log_{11.09} 11.23\right)^2 = 1.01$. Our result is based on the observation made in [2] on the relationship between this problem and list decoding of Reed-Solomon codes. We also use the Gilbert-Varshamov bound to show the limitation of this approach.

II. The Coding Theory Connection

The Reed-Solomon code $[\mathrm{n},\mathrm{k}]_q$ with evaluation set S, is the map from

$$(a_0, a_1, \cdots, a_{k-1}) \in \mathrm{F}\frac{k}{q}$$

to

$$\left(a_0, a_1, \cdots, a_{k-1}x^{k-1}\right)_{x\in S} \in \mathrm{F}\frac{k}{q},$$

where $\mathrm{S} \subseteq \mathrm{F}_q$ and $|\mathrm{S}| = n$. The (list-)decoding problem of Reed-Solomon codes can be reformulated into the problem of noisy curve fitting or noisy polynomial reconstruction. In this problem, we are given n points

$$(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$$

in $\mathrm{F}\frac{2}{\mathrm{q}}$ where all the x-coordinates are distinct. The goal is to find polynomials of degree $k-1$ that pass at least g points.

Let F be the set of functions from S to Z. For any $f \in F$, denote $\prod^{a\in S}(x-a)^{f(a)}$ by $P_f(x)$. For two real numbers $0 \le \alpha \le \beta \le 1$, define $F_{\alpha,\beta} \subseteq F$ $f \in F_{\alpha,\beta}$ as follows. A function if and only if it satisfies that $f(a) \ge 0$ for all $a \in S$,

$$\sum_{f(a\neq 0)} 1 = \lfloor \alpha n \rfloor \text{ and } \sum_{a\in S} f(a) = \lfloor \beta n \rfloor .$$

Note that

$$|F_{\alpha,\beta}| = \binom{n}{\lfloor \alpha \rfloor}\binom{\beta n}{\alpha n}.$$

Let $\hbar(x)$ be a monic polynomial over F_q of degree h, and none of elements in S is a zero of $\hbar(x)$. We may take $\hbar(x)$ as an irreducible polynomial over F_q. Define a map $\psi : \mathrm{F}_{\alpha,\beta} \to \mathrm{F}_q[x]/(\hbar(x))$ by $\psi(f) = P_f(x) \pmod{\hbar(x)}$ as is shown in Fig. 1.

For any $\mathrm{g}(x)$ in $\mathrm{F}_q[x]/(\hbar(x))$, if $\psi^{-1}(\mathrm{g}(x))$ is

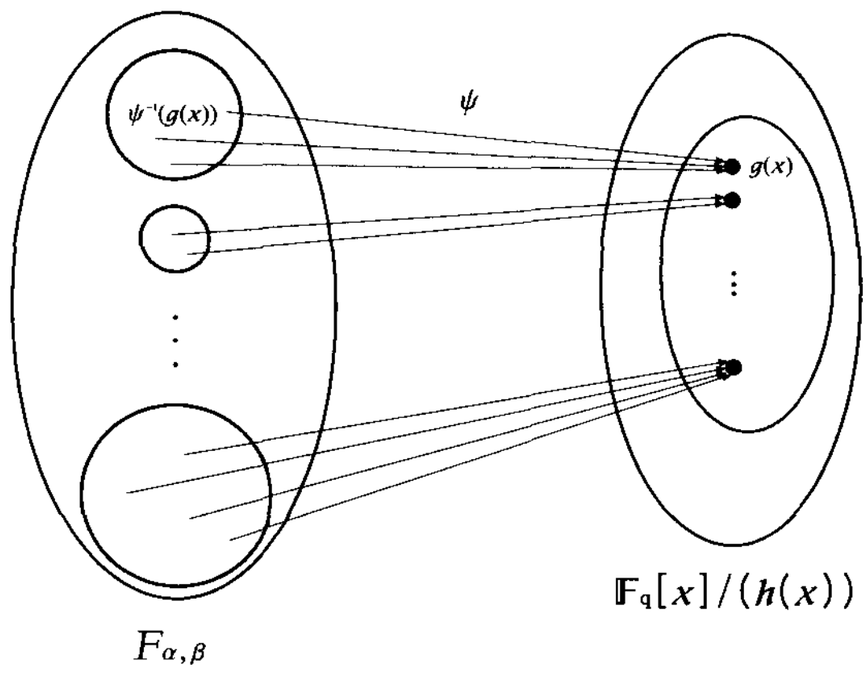


그림 1. $\{x-s \mid s \in S\}$에 의해 배수로 생성된 요소들을 포함하는 ψ의 범위

Fig. 1. The range of ψ contains elements which are multiplicatively generated by $\{x-s \mid s \in S\}$.

not empty, then there exist at least one polynomial $t(x)$ and one f such that $g(x)+t(x)\hbar(x)=P_f(x)$. For any a such that $f(a)>0$,

$$P_f(a)=0 \text{ and } t(x)=-g(a)/\hbar(a).$$

Hence there are exactly $\lfloor \alpha n \rfloor$ elements in S which are the roots of $g(x)+t(x)\hbar(x)=0$. It then implies that the curve $y=t(x)$ passes exact $\lfloor \alpha n \rfloor$ points in the following set of points:

$$\{(a,-g(a)/\hbar(a)) | a \in S\}.$$

Hence the size of $\psi^{-1}(g(x))$ is bounded from above by the number of codewords in the Hamming ball of center $(-g(a)/\hbar(a))_{a\in S}$ and of radius $n-\lfloor \alpha n \rfloor$ in the Reed-Solomon code $[n, \lfloor \beta, n \rfloor -h+1]_q$. Let $L_q(n,k,d)$ be the maximum number of codewords in Reed-Solomon code $[n,k]_q$ in any Hamming ball of radius d. We have just proved the following lemma.

Lemma 1)

The group G has cardinality greater than

$$\frac{\binom{n}{\lfloor \alpha n \rfloor}\binom{\lfloor \beta n \rfloor}{\lfloor \alpha n \rfloor}}{L_q(n, \lfloor \beta n \rfloor -h+1, n-\lfloor \alpha n \rfloor)}$$

for any $0 \le \alpha \le \beta \le 1$.

We now have a lower bound

$$\max_{\alpha,\beta} \frac{\binom{n}{\lfloor \alpha n \rfloor}\binom{\lfloor \beta n \rfloor}{\lfloor \alpha n \rfloor}}{L_q(n, \lfloor \beta n \rfloor -h+1, n-\lfloor \alpha n \rfloor)}$$

for the size of G. Guruswami and Sudan[4] have shown that $L_q(n,k,d) \le O(n^2)$ if $d < n-\sqrt{nk}$.

Thus for n large enough, $L_q(n, \beta n-h+1, n-\alpha n)=O(n_2)$ if $\alpha > \sqrt{\beta-\frac{1}{r}}$. Hence there is a lower bound of form $(rh)^{O(1)}\gamma_2^h$ for the size of G, where

$$\gamma_2 = \max_{\alpha > \sqrt{\beta-\frac{1}{r}}} \left(\frac{\beta^\beta}{\alpha^{2\alpha}(1-\alpha)^{1-\alpha}(\beta-\alpha)^{\beta-\alpha}} \right)^r.$$

It is difficult to find the optimal values of α and β. For simplicity, we set $\beta=1$ and $\alpha=\sqrt{1-\frac{1}{r}}$. This gives us a lower bound which is shown numerically very close to γ_2. In order to prove Theorem 1, it remains to show the following lemma.

Lemma 2)

$$\left(\lfloor \sqrt{1-\frac{1}{r}} n \rfloor \right)^2 = \left(\lfloor \sqrt{1-\frac{1}{r}} rh \rfloor \right)^2$$
$$= (rh)^{O(1)}\left(2er+\frac{e}{2}\log r-\frac{e}{2}\log\frac{e}{2}+O\left(\frac{\log^2 r}{r}\right)\right).$$

Proof: By (A.1), we have

$$\left(\lfloor \sqrt{1-\frac{1}{r}} rh \rfloor \right)^2 = (rh)^{O(1)}\left(\frac{1}{\left(1-\sqrt{1-\frac{1}{r}}\right)^{1-\sqrt{1-\frac{1}{r}}}\sqrt{1-\frac{1}{r^{\sqrt{1-\frac{1}{r}}}}}}\right)^{2rh}.$$

Using Mathematica, we can calculate the series

$$\left(\frac{1}{\left(1-\sqrt{1-\frac{1}{r}}\right)^{1-\sqrt{1-\frac{1}{r}}}\sqrt{1-\frac{1}{r^{\sqrt{1-\frac{1}{r}}}}}}\right)^{2rh} = 2er+\frac{e}{2}\log r-\frac{e}{2}\log\frac{e}{2}+O\left(\frac{\log^2 r}{r}\right).$$

This finishes the proof. □

The table below gives a comparison of the results between γ_1 and γ_2.

r	γ_1	γ_2
1	5.828427124746190097603377448	5.177362420087329379495414137

2	11.090169943749474241022934 17	11.236640263958914686184852 27
3	16.457756896732835305182316 59	17.833844305624457574579871 79
4	21.858249318046910835463119 92	23.853073755571558348492644 86
5	27.272773395342522301252978 69	29.627363897846019631755659 98
6	32.694509357907831015265268 59	35.307267298746613062420675 90
7	38.120426353513753389375091 41	40.936793334806246939198982 17
8	43.548978886269545048702002 76	46.534912114348830420634033 42
9	48.979298076245678891470119 14	52.111217934161895970618300 36
10	54.410858530857494451155063 74	57.671007041236218446134210 36
11	59.843324112071393989971805 06	63.218153403717863517225441 67
12	65.276469861043302181399899 14	68.755262075267562843039657 78
13	70.710139588713913633684274 72	74.283834030503849986188150 57
14	76.144221485872412919524057 08	79.805249356243424273529606 66
15	81.578633417914949597563534 75	85.321636935156153110020266 10
16	87.013313699335003288964775 75	90.831561378890909233325333 38
17	92.448215106405762974722182 65	96.338648947658119401040709 39
18	97.883300876002809459966951 86	101.84062673419115055998545 04
19	103.31854196255075323441001 45	107.33943740347760722120701 86
20	108.75391511474298440756964 38	112.83569436118573309746140 94
21	114.18940149988483896200734 64	118.32817937852360849600043 80
M	M	M
99	538.22437818132776652820880 56	544.23785505118047723627207 41
100	543.66089607846778192418929 86	549.68715125344266075826893 64

Comparing $2e*100 = 543.65\cdots$ and $2e*100 + \frac{e}{2}\log 100 - \frac{e}{2}\log\frac{e}{2} = 549.49\cdots$, we conclude that both approximations are very accurate.

Ⅲ. Limitation

Let $A_q(n,d,w)$ denote the maximum cardinality of a constant weight code of length n, weight and minimum distance d over F_q. We omit the subscription if $q=2$. In the above section, we set to be smaller than Johnson bound (in the Reed-Solomon codes, it is essentially the Guruswami-Sudan bound[4]), and use

$$\max_{d,w} \frac{\binom{n}{n-w}\binom{n-d+h}{n-w}}{A_q(n,d,w)}$$

as a lower bound for the group size generated by n linear factors in the field F_{q^h}. Can we obtain a better result if we let w be bigger than the Johnson's bound? For simplicity, we first convert the problem to the binary case. There is a relation between the bound for binary constant weight codes and bound for q-ary constant weight codes.

Lemma 3)

Assume that $w < \frac{n}{2}$. We have $A_q(n,d,w) \le A(n,2(d-w),w)$.

Proof: Let C be the constant weight code with $A_q(n,d,w)$ many codewords. Define map $m : \mathrm{F}_q \to \mathrm{F}_2$ as

$$m(a) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{otherwise.} \end{cases}$$

Let $m : \mathrm{F}_q^n \to \mathrm{F}_2^n$ be the map that applies m component-wisely. For any q-ary code C with constant weight w and minimum distance d, it is easy to see that $M(C)$ is a binary constant weight code of weight and its minimum distance is at least $2(d-w)$.

□

We may plug in an upper bound of $A(n,2(d-w),w)$ into $\binom{n}{n-w}\binom{n-d+h}{n-w} / A(n,2(d-w),w)$ to obtain a lower bound for the order of G. The quantity $A(n,d,w)$ has been intensively studied and is still under active investigation. Even a good approximation is not known. This is a wide gap between the best upper bound and the best lower bound. A better upper bound will imply a better lower bound for the group size problem. In the best scenario, the lower bound of

$A(n,d,w)$, which is known as the Gilbert-Varshamov bound, is close to the true value. If we plug in the lower bound of $A(n,d,w)$, we can calculate the limit of our method. The following theorem asserts that the hypothetical lower bound is at most a cubic of what we have now.

Theorem 2) Assume that $w \le d \le w+h$ and $\frac{n}{h}=r \to \infty$. We have $\frac{\binom{n}{n-w}\binom{n-d+h}{n-w}}{A(n,2(d-w),w)} \le (\frac{4e^3r^3}{27})^h$.

Proof: The Gilbert-Varshamov bound tells us that $A(n,2\delta,w) \ge \frac{\binom{n}{w}}{\sum_{i=0}^{\delta-1}\binom{w}{i}\binom{n-w}{i}}$. We want to maximize $\binom{n-d+h}{n-w}\sum_{i=0}^{d-w-1}\binom{w}{i}\binom{n-w}{i}$.

Since $d-w \le h$, we have that

$$\begin{aligned}\binom{n-d+h}{n-w}\sum_{i=0}^{d-w-1}\binom{w}{i}\binom{n-w}{i} &\le \binom{n-d+h}{n-d+h-(n-w)}\sum_{i=0}^{h}\binom{w}{i}\binom{n-w}{i}\\ &\le \binom{n-d+h+(d-w)}{h-(d-w)+(d-w)}\sum_{i=0}^{h}\binom{w}{i}\binom{n-w}{i}\\ &= \binom{n-w+h}{h}\sum_{i=0}^{h}\binom{w}{i}\binom{n-w}{i}\end{aligned} \quad (3.1)$$

If $2h \le w \le n-2h$, (3.1) is less than

$$h\binom{n-w+h}{h}\binom{w}{h}\binom{n-w}{h} = (rh)^{O(1)}(\frac{(r-\alpha+1)^{r-\alpha+1}\alpha^{\alpha}}{(r-\alpha-1)^{r-\alpha-1}(\alpha-1)^{\alpha-1}})^h,$$

where $\alpha=\frac{w}{h}$. Here, we need to find the optimal α to maximize

$$\frac{(r-\alpha+1)^{r-\alpha+1}\alpha^{\alpha}}{(r-\alpha-1)^{r-\alpha-1}(\alpha-1)^{\alpha-1}} \quad (3.2)$$

Differentiating (3.2) with respect to and equating it to zero results in $\alpha=\frac{r+1}{3}$. So, we have

$$(3.2)=\frac{4(r-2)^{2-r}(r+1)^{r+1}}{27}.$$

Applying the series expansions, we get

$$(3.2)=\frac{4e^3r^3}{27}-\frac{2e^3r^2}{9}-\frac{e^3r}{18}+\frac{7e^3}{108}-\frac{3e^3}{160r}+O(\frac{1}{r^2}).$$

If $w > n-2h$, $n-w < 2h$. Hence (3.1) is less than

$$h\binom{n-w+h}{h}\binom{2h}{h}\binom{n}{h} \le h4^h\binom{3h}{h}\binom{n}{h} \le h4^h(\frac{3^3}{2^2})^h\left((\frac{r}{r-1})^{r-1}r\right)^h < h(3^3er)^h$$

which is less than $\left(\frac{4e^3r^3}{27}\right)^h$. We use the fact that $(1+\frac{1}{r-1})^{r-1} < e$.

Similarly if $w < 2h$, (3.1) is less than

$$h\binom{n+h}{h}\binom{2h}{h}\binom{n}{h} < h4^h\binom{n+h}{h}^2 < h4^h(3r)^{2h}$$

which is again less than $\left(\frac{4e^3r^3}{27}\right)^h$. □

This theorem shows that we cannot prove a bound better than $(cr^3)^r$ for a constant $c > \frac{4e^3}{27}$ if we use the bound for general codes.

Ⅳ. Concluding Remarks

In the paper, we prove a new lower bound for the group size generated by linear factors in polynomial ring over a finite field. Our bound is slightly better than the bound implied in [6], which is the best known before this result.

We show that using a better upper bound on $A(n,d,w)$ can give us a better lower bound of $|G|$, but the best that we can hope for is a cubic improvement. To achieve this improvement is interesting since it will speed the AKS primality testing by a factor of 9. It is reasonable to expect that the lower bound can be as big as $q^{h/c}$ for some constant $c>1$ and r close to $\log q$. Using bounds for general codes falls short in proving the bound of this form. The limitation calls for new insights on this important problem.

Ⅴ. Appendix

Asymptotic expression for γ_1

Here we use the fact about binomial coefficients:

$$\binom{an}{bn} = (an)^{O(1)}\left(\frac{a^a}{b^b(a-b)^{a-b}}\right)^n \tag{A.1}$$

Now we calculate the approximation of γ_1. Using the Taylor series expansion, we have

$$\sqrt{1+r^2} = r\sqrt{1+\frac{1}{r^2}} = r+\frac{1}{2r}+O(\frac{1}{r^3}).$$

The five parts of γ_1 are respectively:

$$2^r r^r \tag{A.2}$$

$$(1+r-\sqrt{1+r^2})^{-1-r+\sqrt{1+r^2}} = \left(1-\frac{1}{2r}+O(\frac{1}{r^3})\right)^{-\left(1-\frac{1}{2r}+O(\frac{1}{r^3})\right)} \tag{A.3}$$

$$(-r+\sqrt{1+r^2})^{\frac{1}{2}(r-\sqrt{1+r^2})} = \left(\frac{1}{2r}+O(\frac{1}{r^3})\right)^{\frac{-1}{4r}+O(\frac{1}{r^3})} \tag{A.4}$$

$$(-1+r+\sqrt{1+r^2})^{1-r-\sqrt{1+r^2}} = \left(2r-1+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{-2r+1} \times\left(2r-1+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{\frac{-1}{2r}+O(\frac{1}{r^3})} \tag{A.5}$$

$$(r+\sqrt{1+r^2})^{\frac{1}{2}(r+\sqrt{1+r^2})} = \left(2r+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{r} \times\left(2r+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{\frac{1}{4r}+O(\frac{1}{r^3})} \tag{A.6}$$

It is hard to use the mathematical software directly to compute the approximation, so we regroup the product into three parts: (A.3),

$$\left(\frac{1}{2r}+O(\frac{1}{r^3})\right)^{\frac{-1}{4r}+O(\frac{1}{r^3})}\left(2r-1+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{\frac{-1}{2r}+O(\frac{1}{r^3})} \times\left(2r+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{\frac{1}{4r}+O(\frac{1}{r^3})}, \tag{A.7}$$

and $(2r)^r\left(2r-1+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{-2r+1}\left(2r+\frac{1}{2r}+O(\frac{1}{r^3})\right)^{r}$. (A.8)

First we start with (A.3), using the facts that $\log(1+x) = x-\frac{x^2}{2}+O(x^3)$ and $e^x = 1+x+\frac{x^2}{2!}+O(x^3)$, we have

$$\begin{aligned}(A.3) &= \left(1-\frac{1}{2r}+O(\frac{1}{r^3})\right)^{-\left(1-\frac{1}{2r}+O(\frac{1}{r^3})\right)}\\ &= e^{\left(-1+\frac{1}{2r}+O(\frac{1}{r^3})\right)\log\left(1-\frac{1}{2r}+O(\frac{1}{r^3})\right)}\\ &= e^{\left(-1+\frac{1}{2r}+O(\frac{1}{r^3})\right)\left(\left(-\frac{1}{2r}+O(\frac{1}{r^3})\right)-\frac{1}{2}\left(-\frac{1}{2r}+O(\frac{1}{r^3})\right)^2+O\left(\left(-\frac{1}{2r}+O(\frac{1}{r^3})\right)^3\right)\right)}\\ &= e^{\left(-1+\frac{1}{2r}+O(\frac{1}{r^3})\right)\left(-\frac{1}{2r}-\frac{1}{8r^2}+O(\frac{1}{r^3})\right)}\\ &= 1+\frac{1}{2r}+O(\frac{1}{r^3}).\end{aligned}$$

Second, we work on (A.7)

$$\begin{aligned}(A.7) &= \left(\frac{1}{2r}\right)^{-\frac{1}{4r}+O(\frac{1}{r^3})}\left(1+O(\frac{1}{r^2})\right)^{-\frac{1}{4r}+O(\frac{1}{r^3})}\\ &\quad\times(2r)^{-\frac{1}{2r}+O(\frac{1}{r^3})}\left(1-\frac{1}{2r}+\frac{1}{4r^2}+O(\frac{1}{r^4})\right)^{-\frac{1}{2r}+O(\frac{1}{r^3})}\\ &\quad\times(2r)^{\frac{1}{4r}+O(\frac{1}{r^3})}\left(1+\frac{1}{4r^2}+O(\frac{1}{r^4})\right)^{\frac{1}{4r}+O(\frac{1}{r^3})}\\ &= (2r)^{O(\frac{1}{r^3})}\frac{\left(1+\frac{1}{4r^2}+O(\frac{1}{r^4})\right)^{\frac{1}{4r}+O(\frac{1}{r^3})}}{\left(1-\frac{1}{r}+O(\frac{1}{r^2})\right)^{\frac{1}{4r}+O(\frac{1}{r^3})}}\\ &= \left(1+O(\frac{\log r}{r^3})\right)\frac{1+O(\frac{1}{r^2})}{1+O(\frac{1}{r^2})}\\ &= 1+O(\frac{1}{r^2}).\end{aligned}$$

Third, for (A.8), we divide it by γ and compute its Taylor series.

$$\frac{(A.8)}{r} = 2e-\frac{e}{r}+O(\frac{1}{r^2}).$$

Hence

$$(A.8) = 2er-e+O(\frac{1}{r}).$$

Finally, putting them all together, we have

$$\begin{aligned}&\left(1+\frac{1}{2r}+O(\frac{1}{r^3})\right)\left(1+O(\frac{1}{r^2})\right)\left(2er-e+O(\frac{1}{r})\right)\\ &=\left(1+\frac{1}{2r}+O(\frac{1}{r^2})\right)\left(2er-e+O(\frac{1}{r})\right)\\ &= 2er+O(\frac{1}{r}).\end{aligned}$$

References

[1] Daniel J. Bernstein, "Proving primality in essentially quadratic random time", http://cr.yp.to/, 2003.

[2] Qi Cheng, "On the bounded sum-of-digits discrete logarithm problem in finite fields", Proc. of the 24th Annual International Cryptology Conference (CRYPTO), pp. 201-212, Springer-Verlag, 2004.

[3] F.R.K. Chung, "Diameters and eigenvalues", Journal of American Mathematical Society, Vol. 2, No. 2, pp. 187-196, 1989.

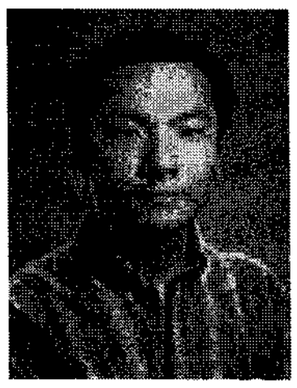
[4] Venkatesan Guruswami and Madhu Sudan, "Improved decoding of Reed-Solomon and ·algebraic-geometry codes", IEEE Transactions on Information Theory, Vol. 45, No. 6, pp. 1757-1767, 1999.

[5] Nicholas M. Katz, "Factoring polynomials in finite fields: an application of Lang-Weil to a problem in graph theory", Mathematische Annalen, Vol. 286, pp. 625-637, 1990.

[6] Jose F. Voloch, "On some subgroups of the multiplicative group of finite rings", Journal de Theorie des Nombres de Bordeaux, Vol. 16, pp. 233-239, 2004.

[7] Daqing Wan, "Generators and irreducible polynomials over finite fields", Mathematics of Computation, Vol. 66, No. 219, pp. 1195-1212, 1997.

저 자 소 개



Qi Cheng(정회원)

2001 Ph. D. in Computer Science, University of Southern California, USA.

1995 M. Sc. in Computer Science, Fudan University, China.

1992 B. Sc. in Computer Science, Nankai University, China.

Aug. 2001~Now Associate Professor, School of Computer Science, University of Oklahoma, USA.

Aug. 1995~Jul. 1996 Assistant Lecturer, Fudan University, China.

<Research Interests : Cryptography, Computational Number Theory and Computational Complexity, Algorithmic Self-assembly and DNA Computing>

황 선 태(정회원)-교신저자

1979년 서강대학교 수학과 학사 졸업.

1987년 Case Western Reserve University 전산학과 석사 졸업.

1993년 Case Western Reserve University 전산학과 박사 졸업.

1978년 12월~1982년 8월 한국과학기술연구원(KIST) 연구원.

1993년 9월~1995년 2월 현대전자연구소 책임연구원.

1995년 3월~현재 대전대학교 정보통신공학과 교수.

<주관심분야 : VLSI Testing, Smart Card/RFID 기술 및 응용, Computer Security>