数理解析研究所講究録 1420 巻 2005 年 94-105

Cartesian authentication codes from diagonal forms

法政大学 工学研究科　斎藤 正顕 (Seiken SAITO) *
Graduate School of Engineering, Hosei University

東京理科大学 理学研究科　佐藤 宏樹 (Hiroki SATO) †
Graduate School of Science, Tokyo University of Science

2004年11月9日

概要

Chanson et al. は [2] において平文の集合と鍵の集合を $\mathrm{GF}(q)^n$ とし, 認証写像を n 元二次対角形式 $\sum_{i=1}^{m} x_i^2$ とする認証符号を構成し, n が偶数の場合のなりすましの成功確率の最大値 P_{d_0} と改ざんの成功確率の最大値 P_{d_1} を評価した (定理 3 参照). 今回我々は, 認証写像が $\sum_{i=1}^{m} a_i x_i{}^2$ ($n \in \mathbb{N}$, $a_i \in \mathrm{GF}(q)$) のとき (定理 5, 6), 及び n が奇数で認証写像が $x_1^k + \sum_{i=2}^{n} x_i^2$ のとき (定理 7, 8) の P_{d_0} と P_{d_1} の評価を　Gauss sum と Jacobi sum を使って得た. さらに n が偶数, $p \equiv 1 \pmod{2k}$, 認証写像が $x_1^k + \sum_{i=2}^{n} x_i^2$ のときの P_{d_0} を Jacobsthal sums を使って与えた (定理 10, 11).

1 Introduction

1.1 認証符号

認証符号 (authentication code) は 1974 年に Gilbert, MacWilliams, Sloane [3] によって考案され, 一般的な認証の理論は Simmons [7, 8] により発展させられた. Simmons のモデルは次のようなものである:

認証符号は次からなる4組 $(\mathscr{S}, \mathscr{E}, \mathscr{T}, f)$ で表わされる.

- $\mathscr{S}$: 平文の集合,
- $\mathscr{E}$: 鍵の集合,
- $\mathscr{T}$: 認証子 (authenticator) の集合,
- f : $\mathscr{S} \times \mathscr{E}$ から $\mathscr{T}$ への写像.

f は認証写像 (authentication map) とよばれる. これを使って送信者 A, 受信者 B , 第三者 C がやりとりを行う.

手順 1 (送受信・認証)　1. 秘密鍵 $e \in \mathscr{E}$ を A, B の間で決めておく.

2. A は平文と認証子の組であるメッセージ

$$m = (s, t) = (s, f(s, e))$$

を B に送信する.

3. B は秘密鍵 $e \in \mathscr{E}$ を使い $f(s, e)$ を計算し, もし $t = f(s, e)$ であれば m が A 本人から送られたものであると判断する.

さて, 第三者 C が受信者 B を欺く方法として次のなりすまし攻撃 (impersonation attack) と改ざん攻撃 (substitution attack) が考えられる.

手順 2 (なりすまし)　1. C は $s' \in \mathscr{S}$ と $t' \in \mathscr{T}$ をランダムにとって別のメッセージ $m' = (s', t')$ を B に送る.

*E-mail : i04r9601@k.hosei.ac.jp
†E-mail : j1100703@ed.kagu.tus.ac.jp

2. 偶然 $t' = f(s', e)$ だった場合, B は m' が A から送られてきたものだという誤った判断を下す.

なりすましが成功する確率の最大値を P_{d_0} で表わす.

手順 3 (改ざん) 1. C は A が B に送信したメッセージ $m = (s, t)$ を傍受し $s' \neq s$ なる s' と置き換えたメッセージ $m' = (s', t')$ を B に送る. ($t' \in \mathscr{T}$ はランダムにとってよい.)

2. 偶然 $f(s', e) = t'$ だった場合, B は m' が A から送られてきたものだという誤った判断を下す.

改ざんが成功する確率の最大値を P_{d_1} で表わす. 定義より次が従う:

$$P_{d_0} = \max_{(s,t)\in\mathscr{M}} \frac{|\{e \in \mathscr{E} : t = f(s,e)\}|}{|\mathscr{E}|},$$

$$P_{d_1} = \max_{\substack{\mathscr{M} \\ s\neq s'}} \frac{|\{e \in \mathscr{E} : t = f(s,e) \ \&\ t' = f(s',e)\}|}{|\{e \in \mathscr{E} : t = f(s,e)\}|}.$$

P_{d_1} の式で max は $s \neq s'$ なる $(s,t), (s',t') \in \mathscr{M}$ をわたる.

1.2 認証符号の構成

さて認証符号 $(\mathscr{S}, \mathscr{E}, \mathscr{T}, f)$ を定める. $(\mathscr{S}, +)$, $(\mathscr{T}, +)$ を有限アーベル群とその演算の組とし $\mathscr{S} = \mathscr{E}$ とする. F を $\mathscr{S}$ から $\mathscr{T}$ への写像とする. このとき, 認証写像 $f(s, e)$ を

$$f(s,e) = F(s+e)$$

で定める. $|\mathscr{S}| = v$, $|\mathscr{T}| = u$ とする. ここでは特に, $\mathscr{S} = \mathscr{E} = \mathrm{GF}(q)^n$, $\mathscr{T} = \mathrm{GF}(q)$, $F : \mathrm{GF}(q)^n \to \mathrm{GF}(q)$ (n は自然数, q は奇素数冪) の場合の認証符号について議論する.

補題 1 ([2] Lemma 1) メッセージ空間は $\mathscr{M} = \mathscr{S} \times F(\mathscr{S}) \subseteq \mathscr{S} \times \mathscr{T}$ ゆえ, とりうるメッセージの個数は $v|F(\mathscr{S})|$ である. メッセージ $(s,t) \in \mathscr{S} \times F(\mathscr{S})$ が使われる確率 $\Pr((s,t))$ は次である.

$$\Pr((s,t)) = \frac{F^{-1}(t)}{v^2},$$

ここに F^{-1} は t の前像 (preimage) の集合である.

定理 1 ([2] Theorem 2) $(\mathscr{S}, +), (\mathscr{T}, +)$ を各々位数 v, u のアーベル群とし F を $\mathscr{S}$ から $\mathscr{T}$ への写像とする. このとき認証符号 $(\mathscr{S}, \mathscr{E}, \mathscr{T}, f)$ を上のように定義すると

$$P_{d_0} = \max_{t'\in\mathscr{T}} \frac{|F^{-1}(t')|}{v},$$

$$P_{d_1} = \max_{\substack{s\in\mathscr{S}, \\ t\in F(\mathscr{S}), \\ s'\neq s, t'}} \frac{|(F^{-1}(t) - s) \cap (F^{-1}(t') - s')|}{|F^{-1}(t)|}.$$

1.3 Perfect nonlinear mapping

$(A, +)$ と $(B, +)$ をそれぞれ位数 n, m のアーベル群とする. $f : A \to B$ を写像とし, f の測度を次で定義する,

$$P_f = \max_{0\neq a\in A} \max_{b\in B} \Pr(f(x+a) - f(x) = b)$$

ここで $\Pr(E)$ は事象 E が起こる確率である.

補題 2 ([2] Lemma 3) f を $(A, +)$ から $(B, +)$ への写像とする. このとき

$$P_f = \max_{0\neq a\in A} \max_{b\in B} \left(\frac{\sum_{y\in B} |C_y \cap (C_{y+b} - a)|}{|A|} \right),$$

ここで, $C_y := f^{-1}(y) = \{x \in A : f(x) = y\}$ である.

$\sum_{b\in B} \sum_{y\in B} |C_y \cap (C_{y+b} - a)| = |A|$ と上の補題より

$$P_f = \max_{\substack{0\neq a\in A \\ b\in B}} \left(\frac{\sum_{y\in B} |C_y \cap (C_{y+b} - a)|}{\sum_{b'\in B} \sum_{y\in B} |C_y \cap (C_{y+b'} - a)|} \right) \geq \frac{1}{|B|}.$$

これは A から B への写像の非線形性の下界を示している. P_f が小さいほど f の非線形性は高い. 符号・暗号理論では P_f が小さい写像を使いたい (つまり $f(x+a) - f(x) = b$ の解 $x \in A$ の個数が少ない写像 f を使いたい). $P_f = 1/m$ のとき, f は完全非線形性 (perfect nonlinearity) を持つという. f が完全非線形性を持つとき定義より 0 でない任意の固定された $a \in A$ に対して $\Pr(f(x+a) - f(x) = b) = 1/m$

である．すなわち，$f(x+a)-f(x)=b$ は0でない任意の固定された a に対する balanced function である．以上のことから次が従う．

定理 2 以下の三つの条件は同値である：

1. $f:A\to B$ が完全非線形である．
2. $$\max_{\substack{0\neq a\in A\\ b\in B}}|\{x\in A: f(x+a)-f(x)=b\}|=\frac{|A|}{|B|}.$$
3. 各 $0\neq a\in A$, $b\in B$ に対し方程式 $f(x+a)-f(x)=b$ は解 $x\in A$ を丁度 $\frac{|A|}{|B|}$ 個しかもたない．

p が奇数のとき $x^s:\mathrm{GF}(p^m)\to\mathrm{GF}(p^m)$ なる完全非線形写像のクラスとして次の三つが得られている．

補題 3 ([2] Lemma 4) p が奇数のとき $\mathrm{GF}(p^m)$ から $\mathrm{GF}(p^m)$ への冪関数 x^s は次の場合対しては perfect nonlinearity $P_f=1/p^m$ を持つ．

- $s=2$,
- $s=p^k+1$ かつ $m/\gcd(m,k)$ は奇数
- $s=(3^k+1)/2$ かつ $p=3$ かつ k は奇数かつ $\gcd(m,k)=1$.

補題 4 ([2] Lemma 5) p が奇数のとき $\mathrm{GF}(p^m)$ から $\mathrm{GF}(p^h)$ への写像 $f(x)$ をトレース

$$f(x)=\mathrm{Tr}_{\mathrm{GF}(p^m)/\mathrm{GF}(p^h)}(x^s)$$

で定める．ここに m,h は $h|m$ なる整数とし $f(x)$ は次の場合に対しては perfect nonlinearity $P_f=1/p^m$ を持つ．

- $s=2$,
- $s=p^k+1$ かつ $m/\gcd(m,k)$ は奇数
- $s=(3^k+1)/2$ かつ $p=3$ かつ k は奇数かつ $\gcd(m,k)=1$.

2 認証写像が二次形式のとき

認証符号を

$$\begin{aligned}&(\mathscr{S},\mathscr{E},\mathscr{T},f(s,e))\\ &=(\mathrm{GF}(q)^n,\mathrm{GF}(q)^n,\mathrm{GF}(q),F(s+e))\end{aligned}$$

とし，$F:\mathrm{GF}(q)^n\to\mathrm{GF}(q)$ が次の二次形式で与えられているとする：

$$F(x_1,\ldots,x_n)={x_1}^2+\cdots+{x_n}^2.$$

次の補題が必要である．

補題 5 ([2] Lemma 9, 10) n を自然数とし，$g(x_1,\ldots,x_n)$ を $\mathrm{GF}(q)$ 上の非退化な二次形式とする．$a\in\mathrm{GF}(q)$ に対し，不定方程式 $g(x_1,\ldots,x_n)=a$ の $\mathrm{GF}(q)^n$ における解の個数を N とすると，次の不等式が成り立つ：

$$\begin{aligned}N-q^{n-1}&=(1-\epsilon(n))\,\mu\left((-1)^{(n-1)/2}\Delta a\right)q^{(n-1)/2}\\ &\quad+\epsilon(n)\mu\left((-1)^{n/2}\Delta\right)\delta(a)q^{(n-2)/2}.\end{aligned}$$

ここに μ は $\mathrm{GF}(q)$ 上の二次指標とし，Δ は g の行列式とし，$\delta:\mathrm{GF}(q)\to\{-1,q-1\}$ を次のような写像とする：

$$\delta(x)=\begin{cases}-1, & x\neq 0 \text{ のとき},\\ q-1, & x=0 \text{ のとき}.\end{cases}$$

また $\epsilon:\mathbb{Z}\to\{1,0\}$ を次のような写像とする：

$$\epsilon(x)=\begin{cases}1, & x \text{ が偶数のとき},\\ 0, & x \text{ が奇数のとき}.\end{cases}$$

n が偶数のとき，Chanson らは上の補題を使って P_{d_0} と P_{d_1} の次の評価を得た．

定理 3 ([2] Theorem 11) n を偶数とする．$\mathscr{S}=\mathscr{E}=\mathrm{GF}(q)^n$, $\mathscr{S}=\mathrm{GF}(q)$ とし，$F:\mathrm{GF}(q)^n\to\mathrm{GF}(q)$ を $F(x_1,\cdots,x_n)={x_1}^2+\cdots+{x_n}^2$ としたとき，次が成り立つ：

$$P_{d_0}=\begin{cases}\frac{1}{q}+\frac{q-1}{q^{(n+2)/2}}, & n\equiv 0 \quad (4),\\ \frac{1}{q}+\frac{q-1}{q^{(n+2)/2}}, & n\equiv 2, \quad q\equiv 1 \quad (4),\\ \frac{1}{q}+\frac{1}{q^{(n+2)/2}}, & n\equiv 2, \quad q\equiv 3 \quad (4).\end{cases}$$

$$P_{d_1} \le \begin{cases} \frac{1}{q} + \frac{q+1}{q^{(n+2)/2}-q}, & n \equiv 0 \quad (4), \\ \frac{1}{q} + \frac{q+1}{q^{(n+2)/2}-q}, & n \equiv 2, \quad q \equiv 1 \quad (4), \\ \frac{1}{q} + \frac{2q-1}{q^{(n+2)/2}-(q-1)q}, & n \equiv 2, \quad q \equiv 3 \quad (4). \end{cases}$$

n が奇数のときも同様の方法で次の評価が導ける [4]:

定理 4 ([4] Theorem 13) 認証符号の構成は定理 3 と同じとする. n が奇数のとき, 次が成り立つ.

$$P_{d_0} = \frac{1}{q} + \frac{1}{q^{(n+1)/2}},$$

$$P_{d_1} \le \frac{1}{q} + \frac{1}{q^{(n-1)/2}-1}.$$

認証写像 F がより一般の対角二次形式

$$F(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i {x_i}^2$$

のときの P_{d_0} と P_{d_1} の評価は次のようになる:

定理 5 ([5]) q を奇素数冪とし, $\mathscr{S} = \mathscr{E} = \mathrm{GF}(q)^n$, $\mathscr{T} = \mathrm{GF}(q)$ とする. $F(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i {x_i}^2$ を $a_i \in \mathrm{GF}(q)$ かつ $a_1 \cdots a_n \neq 0$ なる認証写像とする. n が奇数のとき,

$$P_{d_0} = \frac{1}{q} + \frac{1}{q^{(n+1)/2}}.$$

n が偶数かつ $a_1 \cdots a_n$ が平方元のとき,

$$P_{d_0} = \begin{cases} \frac{1}{q} + \frac{1}{q^{(n+2)/2}}, & n \equiv 2, q \equiv 3 \quad (4), \\ \frac{1}{q} + \frac{q-1}{q^{(n+2)/2}}, & \text{それ以外のとき.} \end{cases}$$

n が偶数かつ $a_1 \cdots a_n$ が非平方元のとき,

$$P_{d_0} = \begin{cases} \frac{1}{q} + \frac{q-1}{q^{(n+2)/2}}, & n \equiv 2, q \equiv 3 \quad (4), \\ \frac{1}{q} + \frac{1}{q^{(n+2)/2}}, & \text{それ以外のとき.} \end{cases}$$

定理 6 ([5]) 定理 5 と同じ条件の下で次が成り立つ. n が奇数のとき,

$$P_{d_1} \le \frac{1}{q} + \frac{1}{q^{(n-1)/2}-1}.$$

n が偶数かつ $a_1 \cdots a_n$ が平方元のとき,

$$P_{d_1} \le \begin{cases} \frac{1}{q} + \frac{2q-1}{q^{(n+2)/2}-(q-1)q}, & q \equiv 3, n \equiv 2 \quad (4), \\ \frac{1}{q} + \frac{q+1}{q^{(n+2)/2}-q}, & \text{それ以外のとき.} \end{cases}$$

n が偶数かつ $a_1 \cdots a_n$ が非平方元のとき,

$$P_{d_1} \le \begin{cases} \frac{1}{q} + \frac{q+1}{q^{(n+2)/2}-q} & q \equiv 3, \ n \equiv 2 \quad (4), \\ \frac{1}{q} + \frac{2q-1}{q^{(n+2)/2}-(q-1)q} & \text{それ以外のとき.} \end{cases}$$

3 認証写像がある対角形式のとき

$q = p^r$ とする. $n \ge 3$ を自然数とし, $k \in \mathbb{Z}$ を $2 < k < q-1$ なる $q-1$ の約数とする. 認証写像が $F(x_1, \dots, x_n) = {x_1}^k + {x_2}^2 + \cdots + {x_n}^2$ のとき F は一般には perfect nonlinear ではない.

3.1 n が奇数のときの P_{d_0} と P_{d_1} の評価

n が奇数のとき, P_{d_0} と P_{d_1} の評価は次のようになる:

定理 7 ([5]) $n > 2$ を奇数とし, $\mathscr{S} = \mathscr{E} = \mathrm{GF}(q)^n$, $\mathscr{T} = \mathrm{GF}(q)$ とする. k を $2 < k < q-1$, $k \mid (q-1)$ なる整数とし, 認証写像を $F(x_1, \dots, x_n) = {x_1}^k + \sum_{i=2}^{n} {x_i}^2$ とする. このとき次が成り立つ:

$$P_{d_0} = \begin{cases} \frac{1}{q} + \frac{k-1}{q^{(n+1)/2}}, & n \equiv q \equiv 3 \quad (4), \\ \frac{1}{q} + \frac{1}{q^{(n+1)/2}}, & \text{それ以外のとき.} \end{cases}$$

定理 8 ([5]) 定理 7 と同じ条件の下で次が成り立つ.

$$P_{d_1} \le \begin{cases} \frac{k-1}{q} + \frac{k(k-1)}{q^{(n+1)/2}-(k-1)q}, & n \equiv q \equiv 3 \quad (4), \\ \frac{k-1}{q} + \frac{k-1}{q^{(n-1)/2}-1}, & \text{それ以外のとき.} \end{cases}$$

定理 5, 6, 7, 8 は Gauss 和と Jacobi 和を使って証明される.

3.2 n が偶数のときの P_{d_0} の評価 I (一般論)

n が偶数の場合の P_{d_0} の評価を考える. その際に必要な不定方程式の解の個数の評価 (後述の命題 1) のために, まず $q = p^r$ のときの Jacobsthal sums の定義を述べる [6].

定義 1 k を正整数とし, p を $p \equiv 1 \pmod{2k}$ なる素数とする. μ を有限体 $\mathrm{GF}(q)$ 上の二次の指標とする. $a \in \mathrm{GF}(q)$ に対し Jacobsthal sums $\phi_{k,r}(a)$, $\psi_{k,r}(a)$ を次で定義する:

$$\phi_{k,r}(a) := \sum_{x \in \mathrm{GF}(q)} \mu(x^{k+1} + ax),$$

$$\psi_{k,r}(a) := \sum_{x \in \mathrm{GF}(q)^*} \mu(x^k + a).$$

$\phi_{k,1} = \phi_k$, $\psi_{k,1} = \psi_k$ とかく.

注意 1 実際は文献 [6] には $\psi_{k,r}(a)$ の定義はない. また $\phi_{k,r}(a)$ も $GF(p)$ の元 a に対してのみ定義されている.

命題 1 n を偶数, $0 \neq t \in \mathrm{GF}(q)$, μ を $\mathrm{GF}(q)$ 上の 2 次指標とし, $N_{k,r}(t)$ を $x_1^k + \sum_{k=2}^n x_i^2 = t$ の解の個数とすると次の式が成り立つ:

$$\begin{aligned} N_{k,r}(t) - q^{n-1} &= \mu(-1)^{(n-2)/2} q^{(n-2)/2} \\ &\quad \times (\mu(t) + k\mu(-1)\psi_{k,r}(-t)). \end{aligned}$$

証明 まず $\mathrm{GF}(q)$ の乗法的指標 χ, χ_1, χ_2 に対し, Gauss sum $\tau(\chi)$, Jacobi sum $J(\chi_1, \chi_2)$ をそれぞれ次で定義する:

$$\tau(\chi) := \sum_{a \in \mathrm{GF}(q)} \chi(a) \exp(2\pi i \cdot \mathrm{tr}(a)/p),$$

$$J(\chi_1, \chi_2) = J_r(\chi_1, \chi_2) := \sum_{a_1 + a_2 = 1} \chi_1(a_1)\chi_2(a_2).$$

λ を $\mathrm{GF}(q)$ 上の位数 k の指標とすると n は偶数より,

$$\begin{aligned} N_{k,r}(t) - q^{n-1} &= \sum_{j=1}^{k-1} \lambda^j \mu(t) \frac{\tau(\lambda^j)\tau(\mu)^{n-1}}{\tau(\lambda^j \mu^{n-1})} \\ &= \mu(t)\tau(\mu)^{n-2} \sum_{j=1}^{k-1} \lambda^j(t) J(\lambda^j, \mu) \\ &= \mu(t)\tau(\mu)^{n-2} \sum_{j=1}^{k-1} \lambda^j(t) \sum_{a \in \mathrm{GF}(q)} \lambda^j(a)\mu(1-a) \\ &= \mu(t)\tau(\mu)^{n-2} \sum_{\substack{a \in \mathrm{GF}(q) \\ a \neq 0,1}} \mu(1-a) \sum_{j=1}^{k-1} \lambda^j(ta) \end{aligned}$$

λ は $\mathrm{GF}(q)$ 上の k 次の指標より

$$\sum_{j=1}^{k-1} \lambda^j(a) = \begin{cases} k-1, & a \text{ が } k \text{ 冪のとき}, \\ -1, & \text{それ以外のとき}. \end{cases}$$

ゆえに, $B = \{a^k : a \in \mathrm{GF}(q)^*\}$ とすると

$$\sum_{a \neq 0,1} \mu(1-a) \sum_{j=1}^{k-1} \lambda^j(ta) = k \sum_{b \in B} \mu(1 - t^{-1}b) + 1.$$

これと

$$\sum_{b \in B} \mu(t-b) = \mu(-1)\psi_{k,r}(-t)$$

より主張が従う. ■

[1] Proposition 6.1.7 の拡張として次の命題が成り立つことが容易にわかる (証明も全く同じやり方でできる) :

命題 2 μ を $\mathrm{GF}(p^r)$ の 2 次指標とするとき,

$$\phi_{k,r}(a) = \begin{cases} \mu(a)\phi_{k,r}(a^{-1}), & \text{if } k \text{ is even}, \\ \mu(a)\psi_{k,r}(a^{-1}), & \text{if } k \text{ is odd}. \end{cases}$$

以下 $p = 2kf + 1$ とし, 次を仮定する: $q = p^r$ とし, $\hat{\chi}$ は位数 $2k$ の $\mathrm{GF}(q)$ の乗法的指標とし, ある固定された $\mathrm{GF}(q)$ の原始根 γ と $\zeta = \exp(2\pi i/2k)$ に対し, $\hat{\chi}(\gamma) = \zeta$ が成り立つとする. また $g = \gamma^{p^{r-1}}$ なる $\mathrm{GF}(p)$ の原始根を g とし, $\hat{\chi}$ の $\mathrm{GF}(p)$ における制限を χ とかく. 以上の仮定から $\chi(g) = \zeta$ となることに注意. 実際,

$$\chi(g) = \hat{\chi}(g) = \hat{\chi}(\gamma)^{p^{r-1}} = \zeta$$

である.

注意 2 $a \in \mathrm{GF}(q)$, $a = \gamma^e$ $(1 \leq e \leq p^r - 1)$ とすると, 上の仮定と $a^{p^{r-1}} = \gamma^{e \cdot p^{r-1}} = g^e$ より以下がなりたつ.

$$e = \mathrm{ind}_\gamma\, a = \mathrm{ind}_g\, a^{p^{r-1}}.$$

もし $a \in \mathrm{GF}(p)$ のときは $p \equiv 1 \pmod{k}$ より以下がなりたつ.

$$\mathrm{ind}_\gamma\, a = p^{r-1} \cdot \mathrm{ind}_g\, a \equiv \mathrm{ind}_g\, a \pmod{k}.$$

さて $\phi_k(a)$ $(a \in \mathrm{GF}(p))$ に対して成り立つ [1] Theorem 6.1.14 の拡張として次の定理がある:

定理 9 ([6] Theorem 3.1) p をある正整数 k に対して $p \equiv 1 \pmod{2k}$ なる素数とする．$a \in \mathrm{GF}(p^r)$ に対し，次が成り立つ．

$$\phi_{k,r}(a) = (-1)^{r-1}\hat{\chi}(-1)\hat{\chi}^{k+1}(a) \times \sum_{j=0}^{k-1} \hat{\chi}^{2j}(a) K(\chi^{2j+1})^r.$$

ここで 指標 χ に対し，$K_r(\chi) := \chi(4)J_r(\chi,\chi)$ とする．特に $r=1$ のときは，$K_1(\chi)$ を $K(\chi)$ とかく．

注意 3 実際には [6] Theorem 3.1 は $a \in \mathrm{GF}(p)$ のときの主張であるが，その証明は $a \in \mathrm{GF}(p^r)$ としても成り立つので上の定理の主張を得る．

注意 4 Davenport-Hasse relation [1] より

$$K_r(\chi) = (-1)^{r-1}K_1(\chi)^r$$

が成り立つことに注意．

k が奇数のときは $\psi_{k,r}(a) = \mu(a)\phi_{k,r}(a^{-1})$ であるから次が従う:

系 1 仮定を前の定理 9 と同じとし，さらに k が奇数のときは次が成り立つ:

$$\psi_{k,r}(a) = \mu(a)(-1)^{r-1}\hat{\chi}(-1)\hat{\chi}^{k+1}(a) \times \sum_{j=0}^{k-1} \hat{\chi}^{2j}(a) K(\chi^{2j+1})^r.$$

$\gamma \in \mathrm{GF}(q)$ を $\mathrm{GF}(q)^*$ の生成元とする．$m, j \in \mathbb{Z}$ に対し

$$\begin{aligned} \phi_{k,r}(\gamma^{km+j}) &= (-1)^{m(k+1)}\phi_{k,r}(\gamma^j), \\ \psi_{k,r}(\gamma^{km+j}) &= (-1)^{mk}\psi_{k,r}(\gamma^j) \end{aligned}$$

が成り立つので，$a \in \mathrm{GF}(q)$ に対し $|\phi_{k,r}(a)|$, $|\psi_{k,r}(a)|$ の値は指数 $\mathrm{ind}_\gamma a \pmod{k}$ により決まる．よって $0 \le j \le k-1$ に対し

$$\begin{aligned} \Phi_{k,r}(j) &:= \phi_{k,r}(\gamma^j), \\ \Psi_{k,r}(j) &:= \psi_{k,r}(\gamma^j) \end{aligned}$$

とおくと，$\mathrm{ind}_\gamma a \equiv j \pmod{k}$ のとき，

$$\begin{aligned} \phi_{k,r}(a) &\quad と \quad \Phi_{k,r}(j), \\ \psi_{k,r}(a) &\quad と \quad \Psi_{k,r}(j) \end{aligned}$$

はそれぞれ符号を除いて等しい．

定理 10 (n : even, $q = p^r$ のときの P_{d_0}) $n > 2$ を偶数とし，$q = p^r$, $p \equiv 1 \pmod{k}$ とする．$\mathscr{S} = \mathscr{E} = \mathrm{GF}(q)^n$, $\mathscr{T} = \mathrm{GF}(q)$ とし，認証写像を $F(x_1,\ldots,x_n) = {x_1}^k + \sum_{i=2}^n {x_i}^2$ とする．このとき次が成り立つ:

$$P_{d_0} = \frac{1}{q} + \frac{\max_{0\le j\le k-1}\left\{|1+k(-1)^j\Psi_{k,r}(j)|\right\}}{q^{(n+2)/2}}.$$

証明 $t \in \mathrm{GF}(q)$ をとり，$t_k \in \mathbb{Z}$ を $\mathrm{ind}_\gamma(-t) \equiv t_k \pmod{k}$, $0 \le t_k \le k-1$ とする．命題 1 から $F = x_1^k + x_2^2 + \cdots + x_n^2$, n : even のときの $F = t$ の解の個数 $N_{k,r}$ は次のように計算される:

$$\begin{aligned} \frac{N_{k,r} - q^{n-1}}{\mu(-1)^{(n-2)/2}\mu(t)q^{(n-2)/2}} &= 1 + k\mu(-t^{-1})\psi_{k,r}(-t) \\ &= 1 + k\mu(-t^{-1})(-1)^{(\mathrm{ind}_\gamma(-t))-t_k}\Psi_{k,r}(t_k) \\ &= 1 + k(-1)^{\mathrm{ind}_\gamma(-t)^{-1}}(-1)^{(\mathrm{ind}_\gamma(-t))-t_k}\Psi_{k,r}(t_k) \\ &= 1 + k(-1)^{t_k}\Psi_{k,r}(t_k). \end{aligned}$$

よって $\max_{t\in\mathrm{GF}(q)}|F^{-1}(t)|$ の値は次に等しい:

$$q^{n-1} + q^{(n-2)/2}\max_{0\le j\le k-1}\left\{|1+k(-1)^j\Psi_{k,r}(j)|\right\}.$$

ゆえに

$$\begin{aligned} P_{d_0} &:= \max_{t\in\mathrm{GF}(q)}\frac{|F^{-1}(t)|}{q^n} \\ &= \frac{1}{q} + \frac{\max_{0\le j\le k-1}\left\{|1+k(-1)^j\Psi_{k,r}(j)|\right\}}{q^{(n+2)/2}}. \end{aligned}$$

■

k が奇数のとき命題 2 より

$$\Psi_{k,r}(j) = \begin{cases} \Phi_{k,r}(0), & j = 0 \text{ のとき}, \\ (-1)^j\Phi_{k,r}(k-j), & j \ne 0 \text{ のとき}, \end{cases}$$

が成り立つことから, 定理 10 の系として次の定理が従う:

定理 11 (n **: even,** k **: odd,** $q=p^r$ **のときの** P_{d_0}**)** 定理 10 と同じ仮定の下, さらに k が奇数のとき次が成り立つ:

$$P_{d_0}=\frac{1}{q}+\frac{\max_{0\leq j\leq k-1}\{|1+k\Phi_{k,r}(j)|\}}{q^{(n+2)/2}}.$$

補題 6 k を奇数とし, $q=p^r$, p : 奇素数, $p\equiv 1 \pmod k$ とすると,

$$\phi_{k,r}(1)\neq 0$$

である. 定義より $\Phi_{k,r}(0)\neq 0$ も従うことに注意.

証明 定義より

$$\psi_{k,r}(-1)=\sum_{m=1}^{p-1}\mu(m^k-1).$$

$p\equiv 1 \pmod k$ より $p^r\equiv 1 \pmod k$ ゆえ, $X^k-1\in \mathrm{GF}(q)[X]$ は一次式の積に分解される. また $(p,k)=1$ ゆえ, 結局 $X^k-1 \pmod p$ は異なる k 個の根をもつ. したがって列 $A:=\{\mu(1^k-1),\mu(2^k-1),\cdots,\mu((p-1)^k-1)\}$ のうち k 個が 0 で残り $p-1-k$ 個は ±1 である. k は奇数より列 A の中に ±1 が奇数個あるのでそれらを足し合わせても 0 にはならない. ゆえに

$$\psi_{k,1}(-1)\neq 0.$$

k は奇数ゆえ, 命題 2 より

$$\phi_{k,1}(1)=\phi_{k,1}((-1)^{-1})=\mu(-1)\psi_{k,1}(-1)\neq 0.$$

■

注意 5 上の補題より $q=p^r, p\equiv 1 \pmod k$, k が奇数, n が偶数のとき認証写像 $F=x_1^k+x_2^2+\cdots+x_n^2$ に対する P_{d_0} は定理 11 と補題 6 より次の不等式をみたす.

$$\begin{aligned}P_{d_0}&=\frac{1}{q}+\frac{1}{q^{(n+2)/2}}\cdot\max_{0\leq j\leq k-1}\{|1+k\Phi_{k,1}(j)|\}\\&>\frac{1}{q}+\frac{k-1}{q^{(n+2)/2}}.\end{aligned}$$

3.3 n が偶数のときの P_{d_0} の評価 II ($k=3,5$ の場合)

ここでは, n が偶数で, 認証写像が $F=x_1^k+\sum_{i=2}x_i^2$ のときの P_{d_0} の明示的な式を 特に $k=3,5$ のときにそれぞれ与える (定理 14, 17).

$k=3$ のとき　まず次の定理が必要である:

定理 12 ([1] Thm 3.1.1 & 3.1.2) $k=3$ のとき,

$$J(\chi,\chi^2)=\left(\frac{-1}{p}\right)K(\chi)=K(\chi^2)=a_3+ib_3\sqrt{3},$$

なる整数 a_3, b_3 があり, これらは次をみたす:

$$a_3^2+b_3^2=p,\quad a_3\equiv -1 \pmod 3, \tag{1}$$
$$3b_3\equiv(2g^{(p-1)/3}+1)a_3 \pmod p. \tag{2}$$

例 1 ([1], p.127) 上の定理 12 を説明するために $p=7$, $g=3$ のときを考える. 式 (1) より, $a_3=2$, $|b_3|=1$ である. 式 (2) より, $3b_3\equiv 3 \pmod 7$ ゆえ $b_3=1$ である.

ここで以下の定理のために Iverson 記号を定義しておく.

定義 2 命題 A に対し, $[A]$ を以下で定義する:

$$[A]:=\begin{cases}1, & A\text{ が真のとき},\\ 0, & A\text{ が偽のとき}.\end{cases}$$

注意 6 以降簡単のために, 数 a に対して $[a]$ は Gauss 記号による像とし, 命題 A に対して $[A]$ は Iverson 記号による像とする.

定理 13 ([1] Theorem 6.2.2 の拡張) $p\equiv 1\,(3)$ とし, a_3, b_3 を定理 12 の通りとすると $\phi_{3,r}(a)$ の値は次の通りに与えられる：

1. $\mathrm{ind}_\gamma\, a\equiv 0 \pmod 3$ のとき,

$$\frac{\phi_{3,r}(a)}{\mu^{r-1}(-1)}=-1+2\sum_{j=0}^{[\frac{r}{2}]}\binom{r}{2j}(-3)^j a_3^{r-2j}b_3^{2j}.$$

2. $\mathrm{ind}_\gamma a \equiv 1 \pmod 3$ のとき,

$$\frac{\phi_{3,r}(a)}{\mu^{r-1}(-1)} = -1 - \sum_{j=0}^{[\frac{r}{2}]} \binom{r}{2j} (-3)^j a_3^{r-2j} b_3^{2j} + 3 \sum_{j=0}^{[\frac{r}{2}]-[2|r]} \binom{r}{2j+1} (-3)^j a_3^{r-2j-1} b_3^{2j+1}.$$

3. $\mathrm{ind}_\gamma a \equiv 2 \pmod 3$ のとき,

$$\frac{\phi_{3,r}(a)}{\mu^{r-1}(-1)} = -1 - \sum_{j=0}^{[\frac{r}{2}]} \binom{r}{2j} (-3)^j a_3^{r-2j} b_3^{2j} - 3 \sum_{j=0}^{[\frac{r}{2}]-[2|r]} \binom{r}{2j+1} (-3)^j a_3^{r-2j-1} b_3^{2j+1}.$$

よって $\phi_{3,r}(a)$ は $\mathrm{ind}_\gamma a \pmod 3$ にのみ依存するので, $\phi_{3,r}$ のとりうる3つの値を順に $\Phi_{3,r}(0)$, $\Phi_{3,r}(1)$, $\Phi_{3,r}(2)$ とする. すなわち

$$\phi_{3,r} : \mathrm{GF}(p^r) \to \{\Phi_{3,r}(0), \Phi_{3,r}(1), \Phi_{3,r}(2)\}.$$

証明　χ は位数6の指標より $\chi^3 = \overline{\chi^3}$ は位数2の指標であるから [1] Theorem 2.1.1 (c) より

$$K(\chi^3) := \chi^3(4) J_1(\chi^3, \chi^3) = -\chi^3(-1)$$

と [1] Theorem 2.1.6 (2.1.2) より

$$\mu(-1) K_1(\chi^{k-1}) = K_1(\chi)$$

に注意すると

$$(-1)^{r-1}\phi_{3,r}(a) = \hat{\chi}(-1)\hat{\chi}^4(a) \sum_{j=0}^{2} \hat{\chi}^{2j}(a) K(\chi^{2j+1})^r$$
$$= (-\mu(-1))^{r-1} \left(-1 + 2\Re\left\{\overline{\hat{\chi}}^2(a) K(\chi^2)^r\right\}\right).$$

よって定理12より

$$\frac{\phi_{3,r}(a) + \mu^{r-1}(-1)}{\mu^{r-1}(-1)} = 2\Re\left\{\overline{\hat{\chi}}^2(a)(a_3 + ib_3\sqrt{3})^r\right\}.$$

$\hat{\chi}(g) = \exp(2\pi i/6) = (1 + i\sqrt{3})/2$ であるから

$\overline{\hat{\chi}}^2(a)$	$\mathrm{ind}_\gamma a \pmod 3$
1	0
$(-1-i\sqrt{3})/2$	1
$(-1+i\sqrt{3})/2$	2

よって主張がなりたつ.

定理 14 ($k=3$, $q=p^r$ のときの P_{d_0}) $n > 2$ を偶数とし, $q = p^r$, $p \equiv 1 \pmod 3$ とする. $\mathscr{S} = \mathscr{E} = \mathrm{GF}(q)^n$, $\mathscr{T} = \mathrm{GF}(q)$ とし, 認証写像を $F(x_1, \ldots, x_n) = {x_1}^3 + \sum_{i=2}^n {x_i}^2$ とする. このとき次が成り立つ:

$$P_{d_0} = \frac{1}{q} + \frac{1}{q^{(n+2)/2}} \cdot \max_{j=0,1,2}\{|1 + 3\Phi_{3,r}(j)|\}.$$

証明　$k=3$ のとき,

$\mathrm{ind}_\gamma a \pmod 3$	$\mathrm{ind}_\gamma a^{-1} \pmod 3$
0	0
1	2
2	1

よって定理13より, $F = x_1^3 + x_2^2 + \cdots + x_n^2$, n が偶数のときの $F = t$ の解の個数を $N_{3,r}$ とし, $q = p^r$ とおくと

$$\frac{N_{3,r} - q^{(n-1)}}{\mu(-1)^{(n-2)/2} q^{(n-2)/2}} = \mu(t) + 3\mu(-1)\psi_{3,r}(-t)$$
$$= \mu(t)\left(1 + 3\phi_{3,r}((-t)^{-1})\right).$$

よって $\max_{t\in\mathrm{GF}(q)} |F^{-1}(t)|$ は次の値に等しい:

$$q^{n-1} + q^{(n-2)/2} \max_{j=0,1,2}\{|1 + 3\Phi_{3,r}(j)|\}.$$

ゆえに

$$P_{d_0} := \max_{t\in\mathrm{GF}(q)} \frac{|F^{-1}(t)|}{q^n} = \frac{1}{q} + \frac{1}{q^{(n+2)/2}} \cdot \max_{j=0,1,2}\{|1 + 3\Phi_{3,r}(j)|\}.$$

■

$k=5$ のとき　$k=3$ のときの定理 12 に相当する次の定理が必要である.

定理 15 ([1] Thm 3.7.2 & 3.7.3) $k=5$ のとき,

$$\left(\frac{-1}{p}\right)K(\chi)=K(\chi^4)$$
$$=a_5+b_5\sqrt{5}+ic_5\sqrt{5+2\sqrt{5}}+id_5\sqrt{5-2\sqrt{5}},$$

なる整数 a_5, b_5, c_5, d_5 があり, これらは次をみたす:

$$a_5\equiv -1 \pmod 5, \tag{3}$$
$$a_5^2+5b_5^2+5c_5^2+5d_5^2=p, \tag{4}$$
$$a_5b_5=d_5^2-c_5^2-c_5d_5. \tag{5}$$

注意として, 上の三つの条件をみたす $\pm(a,b,c,d)$ は次の意味で「本質的に唯一」である. すなわち上の三条件をみたす他の整数の組は $\pm(a,b,-c,-d)$, $\pm(a,-b,-d,c)$, $\pm(a,-b,d,-c)$ 以外にはない.

さらに a_5, b_5, c_5, d_5 は次の合同条件をみたし, 唯一に決定される:

$$a_5+b_5(2h^2-2h^3+1)+c_5(h+h^2+h^3+h^4)$$
$$+d_5(h^2+h^3-h-h^4)\equiv 0 \pmod p, \tag{6}$$
$$5b_5^2-a_5^2\equiv(2h^2-2h^3+1)(c_5^2-d_5^2-4c_5d_5)\,(p). \tag{7}$$

さらに次が成り立つ [1] 式 (3.7.14):

$$\left(\frac{-1}{p}\right)K(\chi^3)=K(\chi^2)$$
$$=a_5-b_5\sqrt{5}-id_5\sqrt{5+2\sqrt{5}}+ic_5\sqrt{5-2\sqrt{5}}.$$

例 2 ([1], p.127) 上の Thm 15 を説明するために $p=11$, $g=2$ のときを考える.　$h=g^{(p-1)/10}=2$. $a_5\equiv-1(5)$ と $a_5^2\equiv 1(5)$ より $a_5=-1$. よって式 (4) より $b_5^2+c_5^2+d_5^2=2$. 従って,

$$(|b_5|,|c_5|,|d_5|)=(1,1,0),\ (1,0,1) \text{ or } (0,1,1).$$

式 (5) より,

$$(b_5,c_5,d_5)=(1,\pm1,0),\ (-1,0,\pm1).$$

この場合の合同式 (6), (7) は

$$\begin{cases} a_5+4b_5+8c_5+5d_5\equiv 0 \pmod{11},\\ 5b_5^2-a_5^2\equiv 4(c_5^2-d_5^2-4c_5d_5) \pmod{11}.\end{cases}$$

でこれらを満たすのは $(a_5,b_5,c_5,d_5)=(-1,1,1,0)$ のみである.

定理 16 ([1] Theorem 6.2.4 の拡張) $p\equiv 1\,(5)$ とし, a_5, b_5, c_5, d_5 を定理 15 の通りとすると $\phi_{5,r}(a)$ の値は次の通りに与えられる:

$$\frac{\phi_{5,r}(a)+\mu^{r-1}(-1)}{2\mu^{r-1}(-1)}$$
$$=r_{\bar\chi}(a)\sum_{j=0}^{[\frac{r}{2}]}\binom{r}{2j}(-1)^j\left(\alpha_+^{r-2j}\beta_+^{2j}+\alpha_-^{r-2j}\beta_-^{2j}\right)$$
$$-i_{\bar\chi}(a)\sum_{j=0}^{[\frac{r}{2}]-[2|r]}\binom{r}{2j+1}(-1)^j$$
$$\times\left(\alpha_+^{r-2j-1}\beta_+^{2j+1}+\alpha_-^{r-2j-1}\beta_-^{2j+1}\right).$$

ここで α_+, α_-, β_+, β_- を

$$\begin{aligned}\alpha_+ &= a_5+b_5\sqrt{5},\\ \alpha_- &= a_5-b_5\sqrt{5},\\ \beta_+ &= c_5\sqrt{5+2\sqrt{5}}+d_5\sqrt{5-2\sqrt{5}},\\ \beta_- &= -d_5\sqrt{5+2\sqrt{5}}+c_5\sqrt{5-2\sqrt{5}},\end{aligned}$$

とする. また $r_{\bar\chi}(a)$ と $i_{\bar\chi}(a)$ はそれぞれ $\bar\chi^2(a)$ の実部, 虚部とし, $\mathrm{ind}_\gamma a \pmod 5$ により次の値をとる:

$$\begin{aligned} r_{\bar\chi}(a) &:= \Re\left(\bar\chi^2(a)\right)\\ &= \begin{cases} 1, & \mathrm{ind}_\gamma a\equiv 0\,(5),\\ (\sqrt{5}-1)/4, & \mathrm{ind}_\gamma a\equiv 1\,(5),\\ -(\sqrt{5}+1)/4, & \mathrm{ind}_\gamma a\equiv 2\,(5),\\ -(\sqrt{5}+1)/4, & \mathrm{ind}_\gamma a\equiv 3\,(5),\\ (\sqrt{5}-1)/4, & \mathrm{ind}_\gamma a\equiv 4\,(5),\end{cases}\end{aligned}$$

$$i_{\hat{\chi}}(a) := \Im\left(\overline{\hat{\chi}}^2(a)\right)$$
$$= \begin{cases} 0, & \mathrm{ind}_g\, a \equiv 0\,(5), \\ -\sqrt{10+2\sqrt{5}}/4, & \mathrm{ind}_\gamma\, a \equiv 1\,(5), \\ -\sqrt{10-2\sqrt{5}}/4, & \mathrm{ind}_\gamma\, a \equiv 2\,(5), \\ \sqrt{10-2\sqrt{5}}/4, & \mathrm{ind}_\gamma\, a \equiv 3\,(5), \\ \sqrt{10+2\sqrt{5}}/4, & \mathrm{ind}_\gamma\, a \equiv 4\,(5). \end{cases}$$

よって $\phi_{5,r}(a)$ は $\mathrm{ind}_\gamma\, a \pmod 5$ にのみ依存するので, $\phi_{5,r}$ のとりうる 5 つの値を順に $\Phi_{5,r}(0)$, $\Phi_{5,r}(1)$, $\Phi_{5,r}(2)$, $\Phi_{5,r}(3)$, $\Phi_{5,r}(4)$ とする. すなわち

$$\phi_{5,r} : \mathrm{GF}(p^r) \to \left\{ \begin{array}{l} \Phi_{5,r}(0), \Phi_{5,r}(1), \Phi_{5,r}(2), \\ \Phi_{5,r}(3), \Phi_{5,r}(4) \end{array} \right\}.$$

証明 χ は位数 10 の指標より $\chi^5 = \overline{\chi^5}$ は位数 2 の指標であるから [1] Theorem 2.1.1 (c) より

$$K(\chi^5) := \chi^5(4) J_1(\chi^5, \chi^5) = -\chi^5(-1)$$

と [1] Theorem 2.1.6 (2.1.2) より

$$\mu(-1) K_1(\chi^4) = K_1(\chi)$$

に注意すると

$$\begin{aligned} (-1)^{r-1}\phi_{5,r}(a) =& \hat{\chi}(-1)\hat{\chi}^6(a) \sum_{j=0}^{4} \hat{\chi}^{2j}(a) K(\chi^{2j+1})^r \\ =& \hat{\chi}(-1)\hat{\chi}^6(a) K(\chi)^r \\ &+ \hat{\chi}(-1)\hat{\chi}^6(a)\hat{\chi}^2(a) K(\chi^3)^r \\ &+ \hat{\chi}(-1)\hat{\chi}^6(a)\hat{\chi}^4(a) K(\chi^5)^r \\ &+ \hat{\chi}(-1)\hat{\chi}^6(a)\hat{\chi}^6(a) K(\chi^7)^r \\ &+ \hat{\chi}(-1)\hat{\chi}^6(a)\hat{\chi}^8(a) K(\chi^9)^r \\ =& \hat{\chi}(-1)\hat{\chi}^6(a)\{\mu(-1)K(\chi^4)\}^r \\ &+ \hat{\chi}(-1)\hat{\chi}^8(a)\{\mu(-1)K(\chi^2)\}^r \\ &+ \hat{\chi}(-1)K(\chi^5)^r \\ &+ \hat{\chi}(-1)\hat{\chi}^2(a)\{\mu(-1)K(\chi^8)\}^r \\ &+ \hat{\chi}(-1)\hat{\chi}^4(a)\{\mu(-1)K(\chi^6)\}^r \end{aligned}$$

$\chi^5 = \mu$ より, $K(\chi^5) = -\chi^5(-1)$ (Thm 2.2.1 (c)) ゆえ

$$\begin{aligned} &(-1)^{r-1}\phi_{5,r}(a) \\ &= \chi^6(-1)\hat{\chi}^6(a)\{\chi^5(-1)\}^{r-1}K(\chi^4)^r \\ &+\chi^6(-1)\hat{\chi}^8(a)\{\chi^5(-1)\}^{r-1}K(\chi^2)^r \\ &+\chi(-1)\{-\chi^5(-1)\}^r \\ &+\chi^6(-1)\hat{\chi}^2(a)\{\chi^5(-1)\}^{r-1}K(\chi^8)^r \\ &+\chi^6(-1)\hat{\chi}^4(a)\{\chi^5(-1)\}^{r-1}K(\chi^6)^r. \end{aligned}$$

これと

$$\begin{aligned} \chi(-1)\{-\chi^5(-1)\}^r &= -\chi^6(-1)\{-\chi^5(-1)\}^{r-1} \\ &= -\{-\chi^5(-1)\}^{r-1}. \end{aligned}$$

より, 次式が成り立つ:

$$\begin{aligned} \mu(-1)^{r-1}\phi_{5,r}(a) &= -1 + 2\Re\left\{\overline{\hat{\chi}}^2(a)K(\chi^2)^r\right\} \\ &\quad +2\Re\left\{\overline{\hat{\chi}}^4(a)K(\chi^4)^r\right\}. \end{aligned}$$

Thm 15 より

$$K(\chi^4) = \alpha_+ + i\beta_+.$$

式 (3.7.14) より

$$K(\chi^2) = \alpha_- + i\beta_-.$$

よって

$$\begin{aligned} K(\chi^4)^r =& \sum_{j=0}^{[\frac{r}{2}]} \binom{r}{2j} (-1)^j \alpha_+^{r-2j} \beta_+^{2j} \\ &+i \sum_{j=0}^{[\frac{r}{2}]-[2|r]} \binom{r}{2j+1} (-1)^j \alpha_+^{r-2j-1} \beta_+^{2j+1}, \end{aligned}$$

$$\begin{aligned} K(\chi^2)^r =& \sum_{j=0}^{[\frac{r}{2}]} \binom{r}{2j} (-1)^j \alpha_-^{r-2j} \beta_-^{2j} \\ &+i \sum_{j=0}^{[\frac{r}{2}]-[2|r]} \binom{r}{2j+1} (-1)^j \alpha_-^{r-2j-1} \beta_-^{2j+1} \end{aligned}$$

と表わされる．これと

$$\begin{aligned}\phi_{5,r}(a) = &- \mu^{r-1}(-1) \\ &+ \mu^{r-1}(-1)\cdot 2\Re\left\{\bar{\hat{\chi}}^2(a)K(\chi^4)^r\right\} \\ &+ \mu^{r-1}(-1)\cdot 2\Re\left\{\bar{\hat{\chi}}^2(a)K(\chi^2)^r\right\}\end{aligned}$$

より

$$\begin{aligned}&\frac{\phi_{5,r}(a)+\mu^{r-1}(-1)}{2\mu^{r-1}(-1)} \\ &= r_{\hat{\chi}}(a)\cdot\sum_{j=0}^{[\frac{r}{2}]}\binom{r}{2j}(-1)^j\alpha_+^{r-2j}\beta_+^{2j} \\ &-i_{\hat{\chi}}(a)\cdot\sum_{j=0}^{[\frac{r}{2}]-[2|r]}\binom{r}{2j+1}(-1)^j\alpha_+^{r-2j-1}\beta_+^{2j+1} \\ &+r_{\hat{\chi}}(a)\cdot\sum_{j=0}^{[\frac{r}{2}]}\binom{r}{2j}(-1)^j\alpha_-^{r-2j}\beta_-^{2j} \\ &-i_{\hat{\chi}}(a)\cdot\sum_{j=0}^{[\frac{r}{2}]-[2|r]}\binom{r}{2j+1}(-1)^j\alpha_-^{r-2j-1}\beta_-^{2j+1}\end{aligned}$$

仮定より $g\in \mathrm{GF}(p)$ だから $\hat{\chi}(g)=\chi(g)$ ゆえ，

$$\hat{\chi}(g)=\exp\left(\frac{2\pi i}{10}\right)=\frac{(\sqrt{5}+1)+i\sqrt{10-2\sqrt{5}}}{4}$$

であり，これを ζ とすると $\zeta^2=((\sqrt{5}-1)+i\sqrt{10+2\sqrt{5}})/4$, $\zeta^3=-\overline{\zeta^2}$, $\zeta^4=-\overline{\zeta}$, $\zeta^5=-1$ であるから，$\mathrm{ind}_\gamma a \pmod 5$ の値により $\bar{\hat{\chi}}^2(a)$ の値は以下のようになる．

$\bar{\hat{\chi}}^2(a)$	$\mathrm{ind}_\gamma a \pmod 5$
1	0
$((\sqrt{5}-1)-i\sqrt{10+2\sqrt{5}})/4$	1
$(-(\sqrt{5}+1)-i\sqrt{10-2\sqrt{5}})/4$	2
$(-(\sqrt{5}+1)+i\sqrt{10-2\sqrt{5}})/4$	3
$((\sqrt{5}-1)+i\sqrt{10+2\sqrt{5}})/4$	4

よって主張がなりたつ．

定理 17 ($k=5$, $q=p^r$ のときの P_{d_0}) $n>2$ を偶数とし，$q=p^r$, $p\equiv 1 \pmod 5$ とする．$\mathscr{S}=\mathscr{E}=\mathrm{GF}(q)^n$, $\mathscr{T}=\mathrm{GF}(q)$ とし，認証写像を $F(x_1,\ldots,x_n)=x_1{}^5+\sum_{i=2}^n x_i{}^2$ とする．このとき次が成り立つ:

$$P_{d_0}=\frac{1}{q}+\frac{1}{q^{(n+2)/2}}\cdot\max_{0\le j\le 4}\{|1+\Phi_{5,r}(j)|\}.$$

証明　$k=5$, n : even, $p\equiv 1 \pmod 5$ のとき，

$\mathrm{ind}_\gamma a \pmod 5$	$\mathrm{ind}_\gamma a^{-1} \pmod 5$	$\phi_{5,r}(a^{-1})$
0	0	$\Phi_{5,r}(0)$
1	4	$\Phi_{5,r}(4)$
2	3	$\Phi_{5,r}(3)$
3	2	$\Phi_{5,r}(2)$
4	1	$\Phi_{5,r}(1)$

ただし，$\phi_{5,r}(j)$ $(j=0,1,2,3,4)$ は Thm 15 の通りとする．よって $F=x_1^5+x_2^2+\cdots+x_n^2$, n : even のときの $F=t$ の解の個数を $N_{5,r}$ とすると，

$$\begin{aligned}\frac{N_{5,r}-q^{n-1}}{\mu(-1)^{(n-2)/2}q^{(n-2)/2}} &= \mu(t)+5\mu(-1)\psi_{5,r}(-t) \\ &= \mu(t)\left(1+5\phi_{5,r}\left((-t)^{-1}\right)\right)\end{aligned}$$

$$\frac{N_{5,r}-q^{n-1}}{\mu(-1)^{(n-2)/2}\mu(t)q^{(n-2)/2}} = \begin{cases} 1+5\Phi_{5,r}(0), & \text{if } \mathrm{ind}_\gamma(-t)\equiv 0\,(5), \\ 1+5\Phi_{5,r}(4), & \text{if } \mathrm{ind}_\gamma(-t)\equiv 1\,(5), \\ 1+5\Phi_{5,r}(3), & \text{if } \mathrm{ind}_\gamma(-t)\equiv 2\,(5), \\ 1+5\Phi_{5,r}(2), & \text{if } \mathrm{ind}_\gamma(-t)\equiv 3\,(5), \\ 1+5\Phi_{5,r}(1), & \text{if } \mathrm{ind}_\gamma(-t)\equiv 4\,(5). \end{cases}$$

よって $\max_{t\in\mathrm{GF}(q)}|F^{-1}(t)|$ の値は次に等しい:

$$q^{n-1}+q^{(n-2)/2}\max_{0\le j\le 4}\{|1+5\Phi_{5,r}(j)|\}.$$

ゆえに

$$\begin{aligned}P_{d_0} &:= \max_{t\in\mathrm{GF}(q)}\frac{|F^{-1}(t)|}{q^n} \\ &= \frac{1}{q}+\frac{1}{q^{(n+2)/2}}\cdot\max_{0\le j\le 4}\{|1+5\Phi_{5,r}(j)|\}.\end{aligned}$$

■

参考文献

[1] B. C. Berndt, R. J. Evans, K. S. Williams, Gauss and Jacobi Sums, Canad. Math. Soc. series of monographs and advanced texts. **21**, A Wiley-Interscience Publication, 1998.

[2] S. Chanson, C. Ding, and A. Salomma, Cartesian authentication codes from functuons with optimal nonlinearity, Theoretical Computer Science **290** No.3 (2003), 1737-1752.

[3] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, Codes which detect deception, Bell System Technical Journal **53** (1974), 405-424.

[4] 船水祐輔, Some extensions for a function to construct a class of authentication codes, 平成 15 年度東京理科大学理学研究科数学専攻修士論文.

[5] Y. Funamizu, S. Saito, H. Sato, Cartesian authentication codes from diagonal forms, preprint.

[6] M. Haneda, M. Kawazoe, T. Takahashi, Formulae of the order of Jacobians for certain hyperelliptic curves, 数理解析研究所講究録 **1361** (2004), 102-115.

[7] G. J. Simmons, Authentication theory/coding theory, in "Advances in Cryptology – CRYPTO '84", G. R. Blakley and D. Chaum, eds., Lecture Notes in Computer Science **196** (1985), 411-432.

[8] G. J. Simmons, A survey of information authentication, in "Contemporary Cryptology, The Science of Information Integrity", G. J. Simmons, ed., IEEE Press, 1992, 379-419.