Gauss Period Normal Basis の最小多項式について

野上 保之
岡山大学 工学部
yasuyuki.nogami@okayama-u.ac.jp

第 11 回有限体 WS（2025 年 9 月 17 日、日田市複合文化施設 AOSE）

Abstract

本稿では，Gauss Period Normal Basis（GNB）により生成される正規基底の最小多項式の特徴づけを目指し，既知の性質に立脚した小規模パラメータでの実験的検討を報告する．特に標数 $q = 7$，拡大次数 $m \in \{2, 3, 5\}$ において，トレース分布と最小多項式の個数分布を調べ，GNB 由来の正規基底が**全てではない**一方で**分布としては特殊**である可能性を示唆する．

1 序論：背景・目的

拡大体 $\mathbb{F}_{q^m}/\mathbb{F}_q$ における正規基底は，高速乗算アルゴリズムと親和性が高く，特に Gauss period から構成される GNB は *Cyclic Vector Multiplication Algorithm (CVMA)* を適用可能とするため実装面の利点が大きい．GNB は標数 q，次数 m に加えて正の整数パラメータ h に依存して定義されるが，h は無限に取り得る一方で正規基底の同値類は有限個である．このため「h を変えても**同じ**正規基底（生成元や組成は異なるが同型な GNB）に到達する」事象が起こり得る．

本研究の目的は，**GNB 由来の正規基底の最小多項式が満たす特徴**を実験的に抽出し，将来的な**必要十分条件**の同定に繋げることである．著者はかつて「トレース 1 の全ての正規基底が GNB である」ことを期待したが，実験的には必ずしも成立しないことがわかっている．本稿ではまず奇素数次数を中心に基礎的観察を整理する．

2 基礎知識

2.1 Gauss Period Normal Basis（GNB）

$h \geq 1$ を整数として，q に対し $n = hm + 1$ が素数となる状況を典型例として考える．n 次の原始根 $\omega \in \mathbb{F}_{q^m}$ と $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ を用意し，

$$\gamma = \sum_{a \in H} \omega^a$$

で定義される γ の q-Frobenius 軌道

$$\mathcal{B} = \{\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{m-1}}\}$$

が $\mathbb{F}_{q^m}$ の $\mathbb{F}_q$-正規基底となる場合，これを GNB と呼ぶ．このとき CVMA により乗算の畳み込みが巡回構造に落ち，実装上の利点が得られる．

2.2 最小多項式とトレース

正規基底生成元 γ の最小多項式 $M_\gamma(x) \in \mathbb{F}_q[x]$ は係数にトレースの情報を反映する．特に 2 次トレース（ここでは簡便に $\mathrm{Tr}(\gamma^{1+q^j})$）の分布は $M_\gamma(x)$ の係数分布と強く関係する．

2.3 重要な性質（再掲・整形）

$0 \leq j \leq m-1$ とし，k は GNB 構成に由来する正整数（$|H| = k$）とする．k が偶数の場合，

$$\mathrm{Tr}\left(\gamma^{1+q^j}\right) = \begin{cases} 1 + k(m-1), & j = 0, \\ -k, & \text{otherwise.} \end{cases} \tag{1}$$

k が奇数の場合（このとき必然的に m は偶数），

$$\mathrm{Tr}\left(\gamma^{1+q^j}\right) = \begin{cases} 1 + k(m-1), & j = m/2, \\ -k, & \text{otherwise.} \end{cases} \tag{2}$$

これらは 2 次トレースの**現れ得る値と出現位置**を強く制限し，最小多項式の係数分布に制約を課す．

3 実験結果

以降では $q = 7$，$m \in \{2, 3, 5\}$ を対象に SageMath 等で得た観察結果を整理する．図はスライド由来の結果（`7_2.png`, `7_3.png`, `7_5.png`）を誌面向けに再掲する．

3.1 $(q, m) = (7, 2)$

この場合は全てが *GNB* であった．期待個数は $((7^2 - 7)/2)/7 = 3$ 個で，観測と一致した．

Table 1 The minimal polynomials of type–$\langle k, m\rangle$ GNB when $p = 7$ and $m = 2$.

minimal polynomial	k
$x^2 + x + 6$	$2, 11, 30, 39, 44, 53, 81, 86, 95, 114, \cdots$
$x^2 + x + 3$	$5, 8, 33, 36, 50, 75, 78, 89, 120, 131, \cdots$
$x^2 + x + 4$	$6, 20, 21, 35, 48, 63, 90, 105, 119, \cdots$

Figure 1: $q = 7,\ m = 2$ のときの最小多項式・分布の概観（スライド再掲）

3.2 $(q, m) = (7, 3)$

期待個数は $((7^3 - 7)/3)/7 = 16$ 個だが，観測できた GNB 由来の**正規基底**は 12 個に留まった．一方，2 次トレースが 5 をとる**既約多項式**自体は 4 個観測され，総数としては $12 + 4 = 16$ で**数は合う**が，その *4* つは正規基底を与えなかった．

参考表（抜粋）　スライドの行列表記を誌面用に簡約し Table 1 に示す．

Table 1: $m = 3$ における 2 次トレース分布の一部

指標 3	指標 2	指標 1	2 次 Tr
1	1	0	1
1	1	1	5
1	1	2	4
1	1	3	1
1	1	4	6
1	1	6	5

3.3 $(q, m) = (7, 5)$

理論上の期待個数は $((7^5 - 7)/5)/7 = 480$ 個に対し，観測された **トレース *1* の正規基底の最小多項式**は 60 個に大幅減少した．インデックス別個数（抜粋）は Table 2 の通りで，10/70 程度が GNB 由来の寄与であることが示唆される．

Table 2: $m = 5$：インデックス別 個数（抜粋）

インデックス	個数
GNB[0][0]	70
GNB[0][1]	70
GNB[0][2]	70
GNB[0][3]	70
GNB[0][4]	70
GNB[0][5]	70
GNB[0][6]	60

4　仮説

- **H1（分布の選別仮説）**：式 (1),(2) が課す 2 次トレースの**出現位置と値の制約**により，GNB 由来の正規基底は**最小多項式の係数分布として特殊な部分集合**のみを占める．
- **H2（m の偶奇依存）**：k の偶奇と m の偶奇制約（特に k 奇数 $\Rightarrow$ m 偶数）に由来して，m が奇数のときには特定トレース値（例：$m = 5$ で 2 次トレース 6）が**構成的に出現しない**領域が生じる．
- **H3（h の冗長性）**：h を変えても同値な GNB に収束する場合が多く，**異なる** h による探索は最小多項式の多様性を必ずしも増やさない．この冗長性が観測個数の「頭打ち」を招く．

5　今後の研究方針

(1) CVMA の計算係数と n 次トレースの関係を明確化

(2) GNB の個数を明確にしたい

Table 2 The minimal polynomials of type–$\langle k, m\rangle$ GNB when $p = 7$ and $m = 3$.

minimal polynomial	k
$x^3 + x^2 + 3x + 1$	4, 102, 116, 200, 466, 494, 522, 564, $\cdots$
$x^3 + x^2 + 4x + 6$	10, 80, 206, 346, 430, 542, 556, 696, $\cdots$
$x^3 + x^2 + 2x + 4$	12, 152, 166, 236, 306, 390, 460, 516, $\cdots$
$x^3 + x^2 + 1$	14, 70, 126, 252, 434, 476, 490, 532, $\cdots$
$x^3 + x^2 + x + 5$	20, 76, 174, 356, 412, 426, 566, 594, $\cdots$
$x^3 + x^2 + 6x + 5$	22, 92, 204, 246, 274, 540, 610, 750, $\cdots$
$x^3 + x^2 + 2x + 6$	26, 54, 292, 376, 404, 432, 670, 726, $\cdots$
$x^3 + x^2 + 3x + 5$	32, 46, 144, 214, 242, 312, 354, 410, $\cdots$
$x^3 + x^2 + x + 2$	34, 90, 132, 230, 244, 286, 440, 664, $\cdots$
$x^3 + x^2 + 6x + 3$	36, 50, 64, 302, 330, 372, 582, 596, $\cdots$
$x^3 + x^2 + 3$	42, 182, 210, 322, 336, 350, 364, 644, $\cdots$
$x^3 + x^2 + 4x + 3$	66, 94, 136, 192, 262, 332, 416, 584, $\cdots$

Table 3 A part of the minimal polynomials of type–$\langle k, m\rangle$ GNB when $p = 7$ and $m = 5$.

minimal polynomial	k
$x^5 + x^4 + 3x^3 + 4x^2 + 3x + 1$	2, 366, 1766, 2130, 2396, $\cdots$
$x^5 + x^4 + 2x^3 + x + 5$	6, 944, 2918, 3366, 3464, $\cdots$
$x^5 + x^4 + 5x^3 + 5x^2 + 5$	8, 120, 974, 1226, 3018, $\cdots$
$x^5 + x^4 + 4x^3 + 4x^2 + 6x + 1$	12, 306, 1538, 1580, 1622, $\cdots$
$x^5 + x^4 + 2x^2 + 4x + 1$	14, 126, 1470, 2030, 2100, $\cdots$
$x^5 + x^4 + 2x^3 + 2x^2 + 4$	20, 258, 1910, 3128, 3842, $\cdots$
$x^5 + x^4 + 4x^3 + 2x^2 + 4x + 4$	26, 852, 1496, 1818, 3120, $\cdots$
$x^5 + x^4 + 3x^3 + 2x^2 + 2$	30, 534, 674, 702, 2522, $\cdots$
$x^5 + x^4 + x^3 + 5x^2 + 4x + 6$	38, 80, 2460, 3020, 3132, $\cdots$
$x^5 + x^4 + 4x^2 + 2x + 3$	42, 896, 938, 1218, 1316, $\cdots$
$x^5 + x^4 + 2x^3 + 5x^2 + 1$	48, 482, 594, 1196, 2666, $\cdots$
$x^5 + x^4 + 5x^3 + x^2 + 6x + 2$	50, 344, 470, 1100, 1170, $\cdots$
$x^5 + x^4 + 4x^3 + 5x^2 + x + 5$	54, 698, 950, 1356, 1524, $\cdots$
$x^5 + x^4 + 5x^2 + 3x + 1$	56, 966, 1736, 1848, 2478, $\cdots$
$x^5 + x^4 + x^3 + 2x^2 + 5x + 2$	66, 654, 1130, 1788, 2768, $\cdots$
$x^5 + x^4 + 2x^2 + 3x + 4$	84, 294, 1260, 2310, 3276, $\cdots$
$x^5 + x^4 + 3x^3 + 4x^2 + 4x + 6$	86, 212, 1094, 1430, 1892, $\cdots$
$x^5 + x^4 + 5x^3 + 4x^2 + x + 1$	92, 960, 1296, 1310, 1884, $\cdots$
$x^5 + x^4 + 3x^2 + 3x + 5$	98, 140, 462, 1568, 2226, $\cdots$
$x^5 + x^4 + 2x^3 + 6x^2 + 6x + 4$	104, 804, 930, 1518, 2414, $\cdots$

$*$The tabulated minimal polynomials are not whole.

Figure 3: $q = 7,\ m = 5$ のときの分布（スライド再掲）