

一类有限域上的置换多项式

魏 晴 孙光洪

(河海大学理学院 南京 211100)

摘 要 有限域上的置换多项式在科学工程中的多个领域有着广泛的应用,尤其应用于现代通讯、密码学等领域中。基于 Zha 等人在文献[23]中提出,当 t 为偶数时,有限域 F_{p^n} 上形如 $(x^{p^k} - x + \delta)^t + \gamma x + \beta Tr(x)$ 的多项式是置换的,通过进一步研究,运用证明置换多项式的一般方法,将其改进为无论 t 为奇数或偶数, $(x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 形式的多项式在 F_{p^n} 上均是置换的。

关键词 有限域,置换多项式,迹函数

中图法分类号 O153.4 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.05.030

Class of Permutation Polynomials over Finite Fields

WEI Qing SUN Guang-hong

(College of Science, Hohai University, Nanjing 211100, China)

Abstract Permutation polynomials over finite fields have been applied in wild areas of science and engineering, especially in the modern communication technology, cryptography and so on. Based on paper [23], it has been proved that when t is any even integer, the form $(x^{p^k} - x + \delta)^t + \gamma x + \beta Tr(x)$ is a class of permutation polynomials over F_{p^n} . Our work proved that whenever t is any even or odd integer, the form $(x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ is permutation polynomials over F_{p^n} .

Keywords Finite fields, Permutation polynomials, Trace function

1 引言

设 p 是素数, F_p 为含有 p 个元素的有限域,其特征值为 p 。设 $F_{p^n}[x]$ 是有限域 F_{p^n} 上的多项式环。如果多项式 $f(x) \in F_{p^n}[x]$ 诱导出一个从 F_{p^n} 到自身的双射,那么称多项式 $f(x)$ 是 F_{p^n} 上的一个置换。

有关有限域上的置换多项式的研究已有多年,其在编码、密码和组合设计理论中均有着重要的应用^[1-4],因此构造新的置换多项式是人们迫切关心的问题。

Lidl 和 Mullen^[5-6]最早提出发现和构造新的置换多项式这一公开性问题。Coulter 等人^[7]利用迹函数和线性化多项式构造出形如 $L(x) + xh(Tr_{F_{q^m}/F_q}(x))$ 的置换多项式, Marcos^[8]构造了形如 $bL(x) + \gamma h(Tr_{F_{q^m}/F_q}(x))$ 的置换多项式。基于文献[8]中的前4类构造, Zieve^[9]推广为更一般的形式,如 $(x^{p^k} - x + \delta)^s + L(x)$ 。Helleseth 和 Zinoviev^[10]最早开始研究形如 $(x^{p^k} - x + \delta)^s + L(x)$ 的置换多项式。之后,更多的学者也开始研究这类置换多项式。Yuan 等^[11]在 F_{2^m} 上构造了形如 $(x^2 + x + \delta)^s + x$ 的置换多项式。进一步,构造了在 F_{p^m} 上形如 $(x^p - x + \delta)^s + L(x)$ 的置换多项式。Zeng 等^[12]补充了 Yuan 等在文献[11]中的结果,得到 F_{p^m} 上形如 $(x^{p^k} - x + \delta)^{\frac{q^m-1}{3}+1} + x^{p^k} + x$ 的置换多项式。

近年来, Cao 等人利用分段函数 $f(x) = \sum_{i=1}^m f_i(x) I_{D_i}(x)$ 构造置换多项式及置换多项式的逆^[13-14], Yuan 等人利用 AGW 准则^[15]建立交换图构造 F_p 上的置换多项式^[16-17], 其中, Yuan 等总结了形如 $(x^{p^k} + ax + \delta)^{\frac{p^d-1}{d}+1} - ax$ ($d=2, 3, 4, 6$) 多项式的置换性^[18]。之后, Zheng 等人^[19]将其推广为形如 $f(x) = (ax^q + bx + c)^r \phi((ax^q + bx + c)^{q^2-1/d}) + ux^q + vx$ 的更一般形式。Tu 等人利用迹函数构造特征值为奇的有限域 $F_{p^{2m}}$ 上形如 $(x^{p^m} - x + \delta)^s + L(x)$ 的置换多项式^[20], 以及偶特征值 $F_{2^{2m}}$ 上 $(x^{2^m} + x + \delta)^s + x^{2^1}$, 并构造 $f(x) = (Tr_m^n(x) + \delta)^s + L(x)$ 形式的置换多项式^[22]。

本文基于文献[23]的研究结果,构造 F_{p^n} 上新形式的置换多项式,如 $(x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 。

设 $n > 1$ 是一个给定的正整数。 $Tr_{F_{p^n}/F_p}(x)$ 是从 F_{p^n} 到 F_p 的迹函数,记为:

$$Tr(x) = Tr_{F_{p^n}/F_p}(x) = x + x^p + \dots + x^{p^{n-1}}$$

2 主要结果

本节构造新的形如 $(x^{p^{k+1}} - x^p + \delta)^t + L(x)$ 的置换多项式。

引理 1^[3] 设多项式 $f(x) \in F_{p^n}[x]$ 是 F_{p^n} 上的置换多项式当且仅当以下结论之一成立:

- 1) 映射 $f: c \mapsto f(c)$ 是满射;
- 2) 映射 $f: c \mapsto f(c)$ 是一一映射;
- 3) 对于任意的元素 $a \in F_{p^n}, f(x) = a$ 在 F_{p^n} 有一个解;
- 4) 对于任意的元素 $a \in F_{p^n}, f(x) = a$ 在 F_{p^n} 有唯一解。

定理 1^[23] 设 t 为偶数, $n = 2k$ 。令 $\beta, \gamma \in F_{p^k}, \gamma \neq 0, \delta \in F_{p^n}, \delta^{p^k} = -\delta$, 且 $Tr(\beta\gamma^{-1}) \neq -1$, 那么

$$f(x) = (x^{p^k} - x + \delta)^t + \gamma x + \beta Tr(x)$$

是有限域 F_{p^n} 上的置换多项式。

上述定理只讨论了 t 为偶数的情形, 当 t 为奇数时, 该多项式是否为置换多项式没有涉及。本文进一步研究得到以下定理。

定理 2 设 k 为正整数, $n = 2k$ 。令 $\delta \in F_{p^n}, \delta^{p^k} = -\delta, Tr(\beta\gamma^{-1}) \neq -1$ 。 $f(x) = (x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 是有限域 F_{p^n} 上的置换多项式当且仅当以下条件之一成立:

- 1) t 为偶数, $\beta, \gamma \in F_{p^k}$, 且 $\gamma \neq 0$;
- 2) t 为奇数, $\beta, \gamma \in F_{p^n}, \beta^{p^k} = -\beta, \gamma^{p^k} = -\gamma$ 且 $\gamma \neq 0$ 。

证明: 假设 $\exists x, a \in F_{p^n}$ 使得 $f(x) = f(x+a)$ 成立, 可得以下等式成立:

$$(x^{p^{k+1}} - x^p + \delta + a^{p^{k+1}} - a^p)^t - (x^{p^{k+1}} - x^p + \delta)^t = -\gamma a - \beta Tr(a) \tag{1}$$

对式(1)两边同时取 p^k 次幂, 可得:

$$(x^{p^{2k+1}} - x^{p^{k+1}} + \delta^{p^k} + a^{p^{2k+1}} - a^{p^{k+1}})^t - (x^{p^{2k+1}} - x^{p^{k+1}} + \delta^{p^k})^t = -\gamma^{p^k} a^{p^k} - \beta^{p^k} Tr^{p^k}(a)$$

化简可得:

$$(x^p - x^{p^{k+1}} - \delta + a^p - a^{p^{k+1}})^t - (x^p - x^{p^{k+1}} - \delta)^t = -\gamma^{p^k} a^{p^k} - \beta^{p^k} Tr(a) \tag{2}$$

1) 当 t 为偶数时, 因 $\beta^{p^k} = \beta, \gamma^{p^k} = \gamma \neq 0$, 代入式(2)可得:

$$(x^{p^{k+1}} - x^p + \delta + a^{p^{k+1}} - a^p)^t - (x^{p^{k+1}} - x^p + \delta)^t = -\gamma a^{p^k} - \beta Tr(a) \tag{3}$$

结合式(1)和式(3), 得:

$$-\gamma a - \beta Tr(a) = -\gamma a^{p^k} - \beta Tr(a)$$

$$a = a^{p^k} \text{ 即 } a^p = a^{p^{k+1}}$$

将 $a^p = a^{p^{k+1}}$ 代入式(1), 可得 $-\gamma a - \beta Tr(a) = 0$

$$a = -\beta\gamma^{-1} Tr(a)$$

$$Tr(a) = -Tr(\beta\gamma^{-1}) Tr(a)$$

又因为 $Tr(\beta\gamma^{-1}) \neq -1$, 有 $a = Tr(a) = 0$ 。从而 $f(x) = (x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 是 F_{p^n} 上的置换多项式。

2) 当 t 为奇数时, 因 $\beta^{p^k} = -\beta, \gamma^{p^k} = -\gamma \neq 0$, 再由式(2)可得:

$$-[(x^{p^{k+1}} - x^p + \delta + a^{p^{k+1}} - a^p)^t - (x^{p^{k+1}} - x^p + \delta)^t] = \gamma a^{p^k} + \beta Tr(a)$$

即

$$(x^{p^{k+1}} - x^p + \delta + a^{p^{k+1}} - a^p)^t - (x^{p^{k+1}} - x^p + \delta)^t = -\gamma a^{p^k} - \beta Tr(a) \tag{4}$$

由式(1)和式(4)可得:

$$-\gamma a - \beta Tr(a) = -\gamma a^{p^k} - \beta Tr(a)$$

$$a = a^{p^k} \text{ 即 } a^p = a^{p^{k+1}}$$

将 $a^p = a^{p^{k+1}}$ 代入式(1), 可得 $\gamma a + \beta Tr(a) = 0, a = -\beta\gamma^{-1} Tr(a), Tr(a) = -Tr(\beta\gamma^{-1}) Tr(a)$

又因为 $Tr(\beta\gamma^{-1}) \neq -1$, 故 $a = Tr(a) = 0$ 。

因此 $f(x) = (x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 是 F_{p^n} 上的置换多项式。证毕。

在定理 2 中, 无论指数 t 为奇数或偶数, $f(x) = (x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 在某种限定条件下都是 F_{p^n} 上的置换多项式。

下面, 对形如 $(x^{p^{k+1}} + x^p + \delta)^t + \gamma x + \beta Tr(x)$ 的多项式进行讨论。

定理 3 设 p 为奇素数, k 为正整数, $n = 2k$ 。若 $\delta, \beta \in F_{p^k}, \gamma \in F_{p^n}, \gamma^{p^k} = -\gamma \neq 0$ 且 $Tr(\beta\gamma^{-1}) \neq -1$, 那么 $f(x) = (x^{p^{k+1}} + x^p + \delta)^t + \gamma x + \beta Tr(x)$ 是有限域 F_{p^n} 上的置换多项式。

证明: 假设 $\exists x, a \in F_{p^n}$ 使得 $f(x) = f(x+a)$ 成立, 可知:

$$(x^{p^{k+1}} + x^p + \delta + a^{p^{k+1}} + a^p)^t - (x^{p^{k+1}} + x^p + \delta)^t = -\gamma a - \beta Tr(a) \tag{5}$$

上面等式两边同时取 p^k 次幂:

$$(x^{p^{2k+1}} + x^{p^{k+1}} + \delta^{p^k} + a^{p^{2k+1}} + a^{p^{k+1}})^t - (x^{p^{2k+1}} + x^{p^{k+1}} + \delta^{p^k})^t = -\gamma^{p^k} a^{p^k} - \beta^{p^k} Tr^{p^k}(a)$$

化简可得:

$$(x^p + x^{p^{k+1}} + \delta + a^p + a^{p^{k+1}})^t - (x^p + x^{p^{k+1}} + \delta)^t = -\gamma^{p^k} a^{p^k} - \beta^{p^k} Tr(a) \tag{6}$$

由 $\delta^{p^k} = \delta, \beta^{p^k} = \beta, \gamma^{p^k} = -\gamma \neq 0$, 结合式(5)和式(6), 可得:

$$-\gamma a - \beta Tr(a) = \gamma a^{p^k} - \beta Tr(a)$$

$$a = -a^{p^k} \text{ 即 } a^p = -a^{p^{k+1}}$$

将 $a^p = -a^{p^{k+1}}$ 代入式(5)得到 $-\gamma a - \beta Tr(a) = 0, a = -\beta\gamma^{-1} Tr(a), Tr(a) = -Tr(\beta\gamma^{-1}) Tr(a)$

又由 $Tr(\beta\gamma^{-1}) \neq -1$, 故 $a = Tr(a) = 0$ 。

因此 $f(x) = (x^{p^{k+1}} + x^p + \delta)^t + \gamma x + \beta Tr(x)$ 是有限域 F_{p^n} 上的置换多项式。证毕。

定理 3 证明了在某些限定条件下, 无论指数 t 为偶数或奇数, 多项式 $(x^{p^{k+1}} + x^p + \delta)^t + \gamma x + \beta Tr(x)$ 在 F_{p^n} 上都是置换多项式。同样, 考察形式 $(x^{p^{k+1}} + x^p + \delta)^t - \gamma x + \beta Tr(x)$ 或 $(x^{p^{k+1}} + x^p + \delta)^t + \gamma x - \beta Tr(x)$ 的多项式在有限域 F_{p^n} 上都是置换的。

结束语 基于 Zha 等人对于 $(x^{p^k} - x + \delta)^t + \gamma x + \beta Tr(x)$ 形式的多项式的研究, 本文通过进一步研究得到无论 t 为奇数或偶数, 在某些条件下, $(x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 形式的多项式在有限域 F_{p^n} 上也是置换多项式; 并且研究了形如 $(x^{p^{k+1}} + x^p + \delta)^t + \gamma x + \beta Tr(x)$ 的多项式形式在以奇素数为特征值的有限域上也是置换的, 从而得到一类新的置换多项式 $(x^{p^{k+1}} - x^p + \delta)^t + \gamma x + \beta Tr(x)$ 。

参 考 文 献

[1] COHEN S D. Permutation group theory and permutation polynomials [M]// Algebra and Combinatorics. Hong Kong, Springer, Singapore, 1999: 133-146

- ter[C]//ACM SIGMOD International Conference on Management of Data. ACM,2014;147-156.
- [4] KREPS, JAY, NEHA N, et al. Kafka: A distributed messaging system for log processing[C]//Proceedings of the NetDB. 2011.
- [5] VAVILAPALLI, VINOD K, et al. Apache hadoop yarn: Yet another resource negotiator[C]//Proceedings of the 4th Annual Symposium on Cloud Computing. ACM,2013.
- [6] <http://samza.apache.org>.
- [7] WANG C K, MENG X F. Relational Query Techniques for Distributed Data Stream; A Survey [J]. Chinese Journal of Computers, 2016, 39(1): 80-96. (in Chinese)
王春凯, 孟小峰. 分布式数据流关系查询技术研究[J]. 计算机学报, 2016, 39(1): 80-96.
- [8] RocketMQ[OL]. <https://github.com/alibaba/rocketmq>.
- [9] RabbitMQ[OL]. <https://www.rabbitmq.com>.
- [10] ZAHARIA, MATEI, et al. Discretized streams; Fault-tolerant streaming computation at scale[C]//Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles. ACM, 2013.
- [11] ARMBRUST, MICHAEL, et al. Spark sql: Relational data processing in spark[C]//Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data. ACM, 2015.
- [12] StreamingSQL [OL]. <https://github.com/Intel-bigdata/spark-streaming-sql>.
- [13] Squall[OL]. <https://github.com/epfldata/squall>.
- [14] Flink[OL]. <http://flink.apache.org>.
- [15] ZAHARIA, MATEI, et al. Resilient distributed datasets: A fault-tolerant abstraction for in-memory cluster computing [C]//Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation. USENIX Association, 2012.
- [16] HOFFMAN S. Apache Flume: Distributed Log Collection for Hadoop[M]. Packt Publishing Ltd, 2013.
- [17] Kafka_flume[OL]. http://www.cloudera.com/documentation/kafka/lat-est/topics/kafka_flume.html.
- [18] Kafkacat[OL]. <https://github.com/edenhill/kafkacat>.
- [19] KafkaProducer[OL]. <https://kafka.apache.org/090/javadoc/index.html?org/apache/kafka/clients/producer/KafkaProducer.html>.
- [20] SNYDER, PETER. tmpfs: A virtual memory file system[C]//Proceedings of the Autumn 1990 EUUG Conference. 1990.
- [21] GRAEFE G, MCKENNA W J. The Volcano optimizer generator; Extensibility and efficient search[C]//International Conference on Data Engineering. IEEE Xplore, 1993; 209-218.
- (上接第 171 页)
- [2] LAIGLE-CHAPUY Y. Permutation polynomials and applications to coding theory [J]. Finite Fields Appl, 2007; 13(1): 58-70.
- [3] LIDL R, NIEDERREITER H. Introduction to finite fields and their applications[M]. Cambridge University Press, 1986.
- [4] MULLEN G L. Permutation polynomials over finite fields [C]//Proc. Conf. Finite Fields and Their Applications in Lect. Notes Pure Appl. Math., Marcel Dekker, New York, 1993; 131-151.
- [5] LIDL R, MULLEN G L. When does a polynomial over a finite field permute the elements of the field [J]. American Math Monthly, 1988, 95(3): 243-246.
- [6] LIDL R, MULLEN G L. When does a polynomial over a finite field permute the elements of the field? II [J]. Amer Math Monthly, 1993, 100; 71-74.
- [7] COULTER R, HENDERSON M, MATTHEWS R. A note on constructing permutation polynomials [J]. Finite Fields Appl, 2009, 15; 553-557.
- [8] MARCOS J E. Specific permutation polynomials over finite fields [J]. Finite Fields and Their Applications 2008, 17(2): 105-112.
- [9] ZIEVE M E. Classes of permutation polynomials based on cyclotomy and an additive analogue[M]//Additive Number Theory. Springer-Verlag, 2010; 366-361.
- [10] HELLESETH T, ZINOVIEV V. New Klooserman sums identities over F_{2^m} for all m [J]. Finite Fields Their Applications, 2003, 9(2): 187-193.
- [11] YUAN J, DING C, WANG H, et al. Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$ [J]. Finite Fields Appl, 2008, 14; 482-493.
- [12] ZHENG X, ZHU X, HU L. Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over F_{2^n} [J]. Applicable Algebra in Engineering, Communication and Computing, 2010, 21(2); 145-150.
- [13] CAO X, HU L, ZHA Z. Constructing permutation polynomials from piecewise permutations[J]. Finite Fields & Their Applications, 2014, 26(3); 162-174.
- [14] ZHENG Y, YU Y, ZHANG Y, et al. Peicewise constructions if inverses of cyclotomic mapping permutation polynomials [J]. Finite Fields & Their Applications, 2016, 40(c): 1-9.
- [15] HOU X. Permutation polynomials over finite fields—A survey of recent advances [J]. Finite Fields & Their Applications, 2015, 32; 82-119.
- [16] ZHENG Y, YUAN P, PEI D. Peicewise constructions of inverses of some permutation polynomials [J]. Finite Fields & Their Applications, 2015, 36; 151-169.
- [17] YUAN P, DING C. Further results on permutation polynomials over finite fields [J]. Finite Fields & Their Applications, 2014, 27; 88-103.
- [18] YUAN P, ZHENG Y. Permutation polynomials from piecewise functions [J]. Finite Fields & Their Applications, 2015, 35(c): 215-230.
- [19] ZHENG Y, YUAN P, PEI D. Large classes of permutation polynomials over F_{q^2} [M]. Springer Science+ Business Media New York, 2016.
- [20] TU Z, ZENG X, LI C, et al. Permutation polynomials of the form $(x^{2^m} - x + \delta)^s + L(x)$ over the finite field $F_{2^{2m}}$ of odd characteristic [J]. Finite Fields Appl, 2015, 34(c): 20-35.
- [21] TU Z, ZENG X, JIANG Y. Two classes of permutation polynomials having the form $(x^{2^m} + x + \delta)^s + x$ [J]. Finite Fields Appl, 2015, 31; 12-24.
- [22] ZENG X, TIAN S, TU Z. Permutation polynomials from trace functions over finite fields [J]. Finite Fields Appl, 2015, 35; 36-51.
- [23] ZHA Z, HU L. Two classes of permutation polynomials over finite fields [J]. Finite Fields Appl, 2012, 18(4): 781-790.