剩余类环 $Z/(p^n)$上若干类单圈多项式构造

游 伟* 戚文峰
(解放军信息工程大学 郑州 450002)

摘 要：该文研究了剩余类环 $Z/(p^n)$上的单圈多项式，其中 $p\geq 5$, $n\geq 2$。由于 $Z/(p^n)$上单圈多项式的构造可以归结为 $Z/(p^2)$上单圈多项式的构造，该文首先给出了 $Z/(5)$上任意次单圈多项式的系数刻画并在此基础上给出了 $Z/(5^2)$ 上 6 次单圈多项式的全部构造。其次，该文给出了 $Z/(p^2)$上 $(p-1)$次单圈多项式的部分构造。

关键词：序列密码；置换多项式；单圈多项式；剩余类环
中图分类号：TN918.2 **文献标识码**：A **文章编号**：1009-5896(2012)04-0802-05
DOI: 10.3724/SP.J.1146.2011.00562

Construction of Several Classes of Single-cycle Polynomials over $Z/(p^n)$

You Wei Qi Wen-feng
(*Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: This paper studies single-cycle polynomials over the integer residue ring $Z/(p^n)$ with prime $p\geq 5$ and integer $n\geq 2$, and presents several classes of such single-cycle polynomials. As the research of single-cycle polynomials over $Z/(p^n)$ can be reduced to the case over $Z/(p^2)$, an exact characterization of single-cycle polynomials over $Z/(5)$ is given in terms of their coefficients, and then a complete characterization of single-cycle polynomials of degree 6 over $Z/(5^2)$ is given based on it. In addition, a partial construction of single-cycle polynomials of degree $(p-1)$ over $Z/(p^2)$ is also proposed.

Key words: Stream cipher; Permutation polynomial; Single-cycle polynomial; Integer residue ring

1 引言

若 $f(x)$是一个整系数多项式，当 x 通过模 m 的一个完全剩余系时，$f(x)$也通过模 m 的一个完全剩余系，则称 $f(x)$是模 m 的一个置换多项式。关于置换多项式的研究结果非常多，可参考文献[1–7]。引起置换多项式迅速发展的一个主要原因是它已逐渐在数论，组合论，密码系统等领域中得到应用。事实上，著名公钥密码体制 RSA[8]和分组密码算法 RC6[9]就是其中的两个应用。

本文研究的是一类特殊的置换多项式，即剩余类环上的单圈多项式(见定义 1)。单圈多项式在密码学的众多领域都有重要应用。例如，在伪随机数发生器[10]的理论中，状态转移函数必须提供伪随机性，特别地，它必须保证状态序列的元素分布和周期。为了达到这个目的，我们可以选择单圈多项式作为状态转移函数，这样就可以保证状态序列达到最大周期并且其元素满足严格一致分布。事实上，经典的线性同余发生器使用的即是一次单圈多项式，它的优势是实现速度快，但弱点是结构过于简单。本文的目标是构造任意次数的单圈多项式，这样就可以利用高次单圈多项式来产生非线性同余发生器以取代线性同余发生器。伪随机数在包括仿真，抽样，数值分析，公钥密码算法设计等众多领域中都有着不同形式的应用。另外，单圈多项式还可以用来构造拉丁方。拉丁方的应用也是极其广泛的。例如，在保密通信网络中用来做口令的分发；以及在某些密码算法的设计中作为多重置换来使用。

Knuth[11]给出了剩余类环 $Z/(m)$上的所有一次和二次单圈多项式的构造。Larin[12]和 Durand 等[13]则分别给出了 $Z/(2^n)$和 $Z/(3^n)$上任意次单圈多项式的全部构造。然而，对于一般的素数 p，关于 $Z/(p^n)$上单圈多项式的构造目前还没有任何结果。其实，这也并不奇怪，因为即使是有限域 $Z/(p)$上置换多项式的构造都是极其有限的。

本文通过刻画多项式的系数给出了 $Z/(p^n)(p\geq 5)$上若干类单圈多项式的构造。由于 $Z/(p^n)$上单圈多项式的构造可以归结到 $Z/(p^2)$上，本文首先通过刻画系数满足的条件给出了 $Z/(5)$上任意次单圈多项式的构造，并在其基础上给出了 $Z/(5^2)$上 6 次单圈多项式的全部构造。另外，本文还给出了 $Z/(p^2)$上 $(p-1)$ 次单圈多项式的部分构造。

2011-06-09 收到，2011-12-15 改回
国家自然科学基金(61070178, 60833008)资助课题
*通信作者：游伟 youwei1102@163.com

2　基础知识

定义 1[12]　设 $f(x)\in Z[x], m\geq 2$ 是正整数，若递归序列 $u_{i+1}=f(u_i)(\mathrm{mod}\ m)$ 的周期达到 m，则称 $f(x)$ 为剩余类环 $Z/(m)$上的单圈多项式。

引理 1[12]　设 $n\geq 2$，若多项式 $f(x)\in Z[x]$在 $Z/(p^n)$上是单圈，则 $f(x)$在 $Z/(p^{n-1})$上也是单圈。

引理 2[12]　设 p 为素数，若多项式 $f(x)\in Z[x]$在 $Z/(p^3)$上是单圈，则对任意正整数 n, $f(x)$在 $Z/(p^n)$上都是单圈；特别地，当 $p\notin\{2,3\}$时，若多项式 $f(x)\in Z[x]$在 $Z/(p^2)$上是单圈，则对任意正整数 n, $f(x)$在 $Z/(p^n)$上都是单圈。

注 1：由引理 1 和引理 2 可知，当 $p\geq 5$ 时，$f(x)$在 $Z/(p^n)(n\geq 2)$ 上是单圈当且仅当 $f(x)$在 $Z/(p^2)$上是单圈。因此，当 $p\geq 5$ 时，对 $Z/(p^n)(n\geq 2)$ 上单圈多项式的研究都可以归结到 $Z/(p^2)$ 上。

对 Z 上多项式，以下记 $f^2(x)=f(f(x))$，一般地，对正整数 k，记 $f^k(x)=\underbrace{f(f(\cdots f}_{k}(x)\cdots))$，并记 $f'(x)$为 $f(x)$的导数。

下面的引理刻画了 $Z/(p)$与 $Z/(p^2)$上的单圈多项式所满足条件之间的联系。

引理 3[13]　多项式 $f(x)\in Z[x]$，若 $f(x)$在 $Z/(p)$上是单圈，则下面的 3 个条件是等价的。(1) $f(x)$ 在 $Z/(p^2)$上是单圈；(2)对任意 $x\in Z$, $f^p(x)-x\neq 0(\mathrm{mod}\ p^2)$，并且 $(f^p)'(x)\equiv 1(\mathrm{mod}\ p)$; (3)存在 $x\in Z$，满足 $f^p(x)-x\neq 0(\mathrm{mod}\ p^2)$，并且 $(f^p)'(x)\equiv 1(\mathrm{mod}\ p)$。

注 2：由引理 3 可知，若 $f(x)$在 $Z/(p)$上是单圈，则 $f(x)$在 $Z/(p^2)$上也是单圈 $\Leftrightarrow$ $f^p(0)\neq 0(\mathrm{mod}\ p^2)$，并且 $(f^p)'(0)\equiv 1(\mathrm{mod}\ p)$。

3　$Z/(5)$上单圈多项式的系数刻画

3.1 常数项为 1 的情形

设 $f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+1\in Z[x]$是 d 次多项式，令 $A_0=\sum_{i\in 4Z,i\neq 0}a_i$, $A_1=\sum_{i\in 1+4Z}a_i$, $A_2=\sum_{i\in 2+4Z}a_i$, $A_3=\sum_{i\in 3+4Z}a_i$。

定理 1　设 $f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+1\in Z[x]$，则 $f(x)$在 $Z/(5)$上是单圈当且仅当 A_0, A_1, A_2, A_3 满足表 1 中条件之一。

表 1 $f(x)$在 $Z/(5)$上是单圈的条件

	(I)	(II)	(III)	(IV)	(V)	(VI)
A_0 mod 5	0	0	0	0	0	0
A_1 mod 5	1	4	1	1	4	0
A_2 mod 5	0	4	3	4	2	0
A_3 mod 5	0	3	3	2	2	3

证明　因为 $f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+1$，所以

$$\left.\begin{aligned}&f(0)=1\\&f(1)=1+A_0+A_1+A_2+A_3\\&f(2)\equiv 1+A_0+2A_1+4A_2+3A_3\,(\mathrm{mod}\,5)\\&f(3)\equiv 1+A_0+3A_1+4A_2+2A_3\,(\mathrm{mod}\,5)\\&f(4)\equiv 1+A_0+4A_1+A_2+4A_3\,(\mathrm{mod}\,5)\end{aligned}\right\}\quad(1)$$

若 $f(x)$在 $Z/(5)$上要构成单圈，则 $f(1)=1+A_0+A_1+A_2+A_3\neq 0$ 或 $1(\mathrm{mod}\ 5)$，从而有 $A_0+A_1+A_2+A_3\equiv 1, 2$ 或 3 (mod 5)。下面分情形讨论：

(1)当 $A_0+A_1+A_2+A_3\equiv 1(\mathrm{mod}5)$，此时，$f(x)$在 $Z/(5)$上是单圈当且仅当

$$0\xrightarrow{f(x)\bmod 5}1\xrightarrow{f(x)\bmod 5}2\xrightarrow{f(x)\bmod 5}3\xrightarrow{f(x)\bmod 5}4\xrightarrow{f(x)\bmod 5}0$$

或

$$0\xrightarrow{f(x)\bmod 5}1\xrightarrow{f(x)\bmod 5}2\xrightarrow{f(x)\bmod 5}4\xrightarrow{f(x)\bmod 5}3\xrightarrow{f(x)\bmod 5}0$$

即

$$\begin{cases}f(2)\equiv 1+A_0+2A_1+4A_2+3A_3\equiv 3(\mathrm{mod}\,5)\\f(3)\equiv 1+A_0+3A_1+4A_2+2A_3\equiv 4\,(\mathrm{mod}\,5)\\f(4)\equiv 1+A_0+4A_1+A_2+4A_3\equiv 0(\mathrm{mod}\,5)\end{cases}$$

$$\text{或}\begin{cases}f(2)\equiv 1+A_0+2A_1+4A_2+3A_3\equiv 4(\mathrm{mod}\,5)\\f(3)\equiv 1+A_0+3A_1+4A_2+2A_3\equiv 0\,(\mathrm{mod}\,5)\\f(4)\equiv 1+A_0+4A_1+A_2+4A_3\equiv 3(\mathrm{mod}\,5)\end{cases}$$

连同 $f(0)=1$ 和 $f(1)\equiv 2(\mathrm{mod}\ 5)$，分别求解上述两个同余方程组可得$(A_0,A_1,A_2,A_3)\equiv(0,1,0,0)$或$(0,4,4,3)\cdot(\mathrm{mod}\ 5)$。

(2)当 $A_0+A_1+A_2+A_3\equiv 2(\mathrm{mod}\ 5)$，同理得 $f(x)$在 $Z/(5)$上是单圈当且仅当$(A_0,A_1,A_2,A_3)\equiv(0,1,3,3)$或$(0,1,4,2)(\mathrm{mod}\ 5)$。

(3)当 $A_0+A_1+A_2+A_3\equiv 3(\mathrm{mod}\ 5)$，同理得 $f(x)$在 $Z/(5)$上是单圈当且仅当$(A_0,A_1,A_2,A_3)\equiv(0,4,2,2)$或$(0,0,0,3)\ (\mathrm{mod}\ 5)$。　　证毕

3.2 常数项不为 1 的情形

设 $g(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0\in Z[x]$是 d 次多项式，令 $A_0'=\sum_{i\in 4Z,i\neq 0}a_ia_0^{i-1}$, $A_1'=\sum_{i\in 1+4Z}a_ia_0^{i-1}$, $A_2'=\sum_{i\in 2+4Z}a_ia_0^{i-1}$, $A_3'=\sum_{i\in 3+4Z}a_ia_0^{i-1}$。

推论 1　设 $g(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0\in Z[x]$，则 $g(x)$在 $Z/(5)$上是单圈当且仅当 $a_0\neq 0(\mathrm{mod}\ 5)$，且 A_0', A_1', A_2', A_3'满足表 2 中条件之一。

证明　若 $g(x)$在 $Z/(5)$上要构成单圈，则有 $g(0)=a_0\neq 0(\mathrm{mod}\ 5)$。令 $f(x)=a_0^{-1}g(a_0x)$，则 $f(x)=a_da_0^{d-1}x^d$

表 2 $g(x)$在 $Z/(5)$上是单圈的条件

	(I)	(II)	(III)	(IV)	(V)	(VI)
$A_0^{'} \bmod 5$	0	0	0	0	0	0
$A_1^{'} \bmod 5$	1	4	1	1	4	0
$A_2^{'} \bmod 5$	0	4	3	4	2	0
$A_3^{'} \bmod 5$	0	3	3	2	2	3

$+a_{d-1}a_0^{d-2}x^{d-1}+\cdots+a_2a_0x^2+a_1x+1$，易知 $g(x)$在 $Z/(5)$上是单圈当且仅当 $f(x)$在 $Z/(5)$上是单圈。另外，$f(0)=1$，由定理 1 即证。

4 $Z/(5^2)$上 6 次单圈多项式的全部构造

4.1 常数项为 1 的情形

设 $f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+1\in Z[x]$是 d 次多项式，令 $D_0=\sum_{i\in 4Z,i\neq 0}i\cdot a_i$，$D_1=\sum_{i\in 1+4Z}i\cdot a_i$，$D_2=\sum_{i\in 2+4Z}i\cdot a_i$，$D_3=\sum_{i\in 3+4Z}i\cdot a_i$。

引理 4 若 $f(x)$在 $Z/(5)$上是单圈，则$(f^5)'(0)\equiv a_1[(D_1+D_3)^2-(D_0+D_2)^2][(D_1-D_3)^2-(2D_2+3D_0)^2](\bmod 5)$。

证明 因为 $f^k(x)=f(f^{k-1}(x))$，所以 $(f^k)'(x)=f'(f^{k-1}(x))\cdot(f^{k-1})'(x)$，故有$(f^5)'(x)=f'(f^4(x))\cdot(f^4)'\cdot(x)=\cdots=f'(f^4(x))\cdot f'(f^3(x))\cdot f'(f^2(x))\cdot f'(f(x))\cdot f'(x)$。又 $f(x)$在 $Z/(5)$上是单圈，从而对任意 $x\in Z$，有$(f^5)'(x)\equiv f'(0)f'(1)f'(2)f'(3)f'(4)(\bmod 5)$。

另外

$$\left.\begin{aligned}&f'(0)\equiv a_1\ (\bmod 5)\\&f'(1)\equiv D_0+D_1+D_2+D_3(\bmod 5)\\&f'(2)\equiv 3D_0+D_1+2D_2+4D_3(\bmod 5)\\&f'(3)\equiv 2D_0+D_1+3D_2+4D_3(\bmod 5)\\&f'(4)\equiv 4D_0+D_1+4D_2+D_3(\bmod 5)\end{aligned}\right\}\quad(2)$$

因此$(f^5)'(0)\equiv a_1[(D_1+D_3)^2-(D_0+D_2)^2][(D_1-D_3)^2-(2D_2+3D_0)^2](\bmod 5)$。 证毕

引理 5 $f(x)$如上，对任意素数 p 和正整数 k，若 $f^k(0)\equiv c(\bmod\ p)$，$0\le c\le p-1$，则 $f^{k+1}(0)\equiv f(c)+f'(c)(f^k(0)-c)(\bmod\ p^2)$。

证明 因为 $f^k(0)\equiv c(\bmod\ p)$，$0\le c\le p-1$，所以 $f^k(0)-c\equiv 0(\bmod\ p)$。则有

$$\begin{aligned}f^{k+1}(0)&=f(f^k(0)-c+c)=1+\sum_{i=1}^{d}a_i(f^k(0)-c+c)^i\\&\equiv 1+\sum_{i=1}^{d}a_i(c^i+i\cdot c^{i-1}\cdot(f^k(0)-c))(\bmod\ p^2)\\&\equiv\left(1+\sum_{i=1}^{d}a_ic^i\right)+(f^k(0)-c)\cdot\sum_{i=1}^{d}i\cdot a_i\cdot c^{i-1}\\&\quad\cdot(\bmod\ p^2)\equiv f(c)+f'(c)(f^k(0)-c)(\bmod\ p^2)\end{aligned}$$

证毕

注 3：若$(A_0,A_1,A_2,A_3)\equiv(0,1,0,0)(\bmod\ 5)$，则由式(1)可知 $f(0)=1$，$f^2(0)\equiv 2(\bmod\ 5)$，$f^3(0)\equiv 3\cdot(\bmod 5)$，$f^4(0)\equiv -1\ (\bmod 5)$。

由引理 5 通过迭代可得

$$\begin{aligned}f^5(0)&\equiv f(-1)+f'(4)(f^4(0)+1)(\bmod 5^2)\equiv\cdots\\&\equiv f(-1)+f'(4)(f(3)+1)+f'(4)f'(3)(f(2)-3)\\&\quad+f'(4)f'(3)f'(2)(f(1)-2)(\bmod 5^2)\end{aligned}\quad(3)$$

定理 2 设 $f(x)=a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+1\in Z[x]$，则 $f(x)$在 $Z/(5^2)$上是单圈当且仅当 $a_1\equiv 1(\bmod\ 5)$，$a_2\equiv a_3\equiv a_5\equiv a_6\equiv 0\ (\bmod\ 5)$，$a_4\equiv 0\cdot(\bmod 5)$且 $a_4\neq 5(\bmod 5^2)$。

证明 由定理 1 及注 2 可知，若 $f(x)$在 $Z/(5)$上是单圈，即 A_0,A_1,A_2,A_3 满足表 1 中条件(I)–条件(VI)中的某一个，则 $f(x)$在 $Z/(5^2)$上是单圈当且仅当 $(f^5)'(0)\equiv 1(\bmod 5)$，及 $f^5(0)\neq 0(\bmod 5^2)$。

由 A_i 和 D_i 的定义易得

$$\left.\begin{aligned}&D_0=4a_4=4A_0\ (\bmod 5),\\&D_1=a_1+5a_5\equiv a_1(\bmod 5)\\&D_2=2a_2+6a_6\equiv A_2+a_2\ (\bmod 5)\\&D_3=3a_3=3A_3(\bmod 5)\end{aligned}\right\}\quad(4)$$

下面分情况进行讨论：

(1)当 $(A_0,A_1,A_2,A_3)\equiv(0,1,0,0)(\bmod 5)$，由式(4)可得 $D_0\equiv 0(\bmod\ 5)$，$D_1\equiv a_1\ (\bmod\ 5)$，$D_2\equiv a_2(\bmod 5)$，$D_3\equiv 0(\bmod 5)$。

由引理 4 可知 $(f^5)'(0)\equiv a_1(a_1^2-a_2^2)(a_1^2+4a_2^2)\cdot(\bmod\ 5)\equiv a_1(a_1^4-a_2^4)\ (\bmod\ 5)$。因此，$(f^5)'(0)\equiv 1(\bmod 5)$当且仅当 $a_1\equiv 1(\bmod 5)$，$a_2\equiv 0(\bmod 5)$。连同$(A_0,A_1,\ A_2,A_3)\equiv(a_4,a_1+a_5,a_2+a_6,a_3)\equiv(0,1,0,0)\cdot(\bmod 5)$可得

$$a_1\equiv 1(\bmod 5),\ a_2\equiv a_3\equiv a_4\equiv a_5\equiv a_6\equiv 0\ (\bmod 5)\quad(5)$$

由此可知，为了给出 $f(x)$在 $Z/(5^2)$上是单圈的充要条件，我们只需说明当条件式(5)满足时，$f^5(0)\neq 0\cdot(\bmod 5^2)$ 当且仅当 $a_4\neq 5(\bmod 5^2)$。

当条件式(5)满足时，由式(2)和式(4)可得 $f'(2)\equiv a_1+2a_2\equiv 1(\bmod\ 5)$，$f'(3)\equiv a_1+3a_2\equiv 1(\bmod\ 5)$，$f'(4)\equiv a_1+4a_2\equiv 1(\bmod 5)$。

另外，由式(3)可得

$f^5(0)\equiv f(-1)+f'(4)\ (f(3)+1)+f'(4)\ f'(3)\ (f(2)-3)+f'(4)\ f'(3)\ f'(2)\ (f(1)-2)(\bmod 5^2)\equiv f(-1)+(f(3)+1)+(f(2)-3)+(f(1)-2)(\bmod\ 5^2)\equiv 5a_1+15a_2+10a_3+24a_4+20a_6(\bmod 5^2)\equiv 5-a_4(\bmod 5^2)$

因此，当条件式 (5) 满足时，$f^5(0)\neq 0(\bmod 5^2)$ 当且仅当 $a_4\neq 5(\bmod\ 5^2)$。故在此情形下 $f(x)$在 $Z/(5^2)$上是单圈当且仅当 $a_1\equiv 1(\bmod\ 5)$，$a_2\equiv a_3\equiv a_5\equiv a_6\equiv 0\ (\bmod 5)$，$a_4\equiv 0\ (\bmod 5)$且 $a_4\neq 5(\bmod 5^2)$。

(2)当$(A_0,A_1,A_2,A_3)\equiv(0,4,4,3)\ (\mathrm{mod}\ 5)$，由式(4)可得 $D_0\equiv 0\ (\mathrm{mod}\ 5)$, $D_1\equiv a_1(\mathrm{mod}\ 5)$, $D_2\equiv a_2-1\cdot(\mathrm{mod}\ 5)$, $D_3\equiv -1(\mathrm{mod}\ 5)$。

由引理 4 可知$(f^5)'(0)\equiv a_1[(a_1-1)^2-(a_2-1)^2][(a_1+1)^2+(a_2-1)^2](\mathrm{mod}\ 5)$。

(3)当$(A_0,A_1,A_2,A_3)\equiv(0,1,3,3)(\mathrm{mod}\ 5)$，同理得$(f^5)'(0)\equiv a_1\ [(a_1-1)^2-(a_2-2)^2][(a_1+1)^2+(a_2-2)^2]\cdot(\mathrm{mod}\ 5)$。

(4)当$(A_0,A_1,A_2,A_3)\equiv(0,1,4,2)\ (\mathrm{mod}\ 5)$，同理得$(f^5)'(0)\equiv a_1\ [(a_1+1)^2-(a_2-1)^2][(a_1-1)^2+(a_2-1)^2]\cdot(\mathrm{mod}\ 5)$。

(5)当$(A_0,A_1,A_2,A_3)\equiv(0,4,2,2)\ (\mathrm{mod}\ 5)$，同理得$(f^5)'(0)\equiv a_1[(a_1+1)^2-(a_2+2)^2][(a_1-1)^2+(a_2+2)^2]\cdot(\mathrm{mod}\ 5)$。

(6)当$(A_0,A_1,A_2,A_3)\equiv(0,0,0,3)\ (\mathrm{mod}\ 5)$，同理得$(f^5)'(0)\equiv a_1[(a_1-1)^2-a_2^2][(a_1+1)^2+a_2^2](\mathrm{mod}\ 5)$。

在情况(2)– 情况(6)中，遍历 a_1 和 a_2 的所有取值，易知 $(f^5)'(0)\neq 1(\mathrm{mod}\ 5)$。这意味着在这些情况下 $f(x)$在 $Z/(5^2)$上都不可能构成单圈。　　证毕

4.2 常数项不为 1 的情形

推论 2　设 $g(x)=a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0\in Z[x]$，则 $g(x)$在 $Z/(5^2)$上是单圈当且仅当 $a_1\equiv 1(\mathrm{mod}\ 5)$, $a_2\equiv a_3\equiv a_4\equiv a_5\equiv a_6\equiv 0(\mathrm{mod}\ 5)$, $a_0\neq 0(\mathrm{mod}\ 5)$且 $a_0\neq(a_4/5)(\mathrm{mod}\ 5)$。

证明　若 $g(x)$在 $Z/(5^2)$上要构成单圈，则有 $g(0)=a_0\neq 0(\mathrm{mod}\ 5)$，即 $\gcd(a_0,5)=1$。令 $f(x)=a_0^1\,g(a_0x)$，则 $f(x)=a_0^5\,a_6x^6+a_0^4\,a_5x^5+a_0^3\,a_4x^4+a_0^2\,a_3x^3+a_0a_2x^2+a_1x+1$，易知 $g(x)$ 在 $Z/(5^2)$ 上是单圈当且仅当 $f(x)$ 在 $Z/(5^2)$ 上是单圈。另外，$f(0)=1$，由定理 2 可知 $f(x)$ 在 $Z/(5^2)$上是单圈当且仅当 $a_0\neq 0\cdot(\mathrm{mod}\ 5)$, $a_1\equiv 1(\mathrm{mod}\ 5)$, $a_0a_2\equiv a_0^2\,a_3\equiv a_0^4\,a_5\equiv a_0^5\,a_6\equiv 0(\mathrm{mod}\ 5)$, $a_0^3\,a_4\equiv 0(\mathrm{mod}\ 5)$且$a_0^3\,a_4\neq 5(\mathrm{mod}\ 5^2)$。容易验证上述条件即等价于推论 2 中的条件。证毕

5　$Z/(p^2)$上$(p-1)$次单圈多项式的部分构造

引理 6　设素数 $p>3$，则

$$1^{2k}+2^{2k}+\cdots+((p-1)/2)^{2k}\equiv\begin{cases}0(\mathrm{mod}\ p), & 1\le k\le\dfrac{p-3}{2}\\ \dfrac{p-1}{2}(\mathrm{mod}\ p), & k=\dfrac{p-1}{2}\end{cases}$$

证明　因为有限域 $Z/(p)$中的所有非零元素构成乘法循环群 Z_p^*，设 $Z_p^*=\langle g\rangle$。所以

$$\begin{aligned}&2[1^{2k}+2^{2k}+\cdots+((p-1)/2)^{2k}]\\&\equiv 1^{2k}+2^{2k}+\cdots+((p-1)/2)^{2k}+((p+1)/2)^{2k}+\cdots\\&\quad+(p-2)^{2k}+(p-1)^{2k}\ (\mathrm{mod}\ p)\\&\equiv g^{2k}+(g^2)^{2k}+\cdots+(g^{p-1})^{2k}\ (\mathrm{mod}\ p)\\&\equiv g^{2k}+(g^{2k})^2+\cdots+(g^{2k})^{p-1}\ (\mathrm{mod}\ p)\end{aligned}$$

当 $1\le k\le(p-3)/2$ 时，$g^{2k}\neq 1\ (\mathrm{mod}\ p)$，故

$$2[1^{2k}+2^{2k}+\cdots+((p-1)/2)^{2k}]\equiv\frac{g^{2k}-(g^{2k})^{p-1}\cdot g^{2k}}{1-g^{2k}}\equiv 0(\mathrm{mod}\ p)$$

因为 $\gcd(p,2)=1$，所以 $1^{2k}+2^{2k}+\cdots+((p-1)/2)^{2k}\equiv 0(\mathrm{mod}\ p)$。

当 $k=(p-1)/2$ 时，由欧拉定理可知

$$\begin{aligned}&1^{2k}+2^{2k}+\cdots+((p-1)/2)^{2k}=1^{p-1}+2^{p-1}+\cdots+((p-1)/2)^{p-1}\\&\equiv\underbrace{1+1+\cdots+1}_{(p-1)/2}\ (\mathrm{mod}\ p)\\&\equiv(p-1)/2(\mathrm{mod}\ p)\end{aligned}$$

证毕

定理 3　设素数 $p>3$, $f(x)=a_{p-1}x^{p-1}+a_{p-2}x^{p-2}+\cdots+a_1x+1\in Z[x]$，若 $f(x)$ 的系数满足如下条件：$a_1\equiv 1(\mathrm{mod}\ p)$, $a_2\equiv a_3\equiv\cdots\equiv a_{p-2}\equiv 0(\mathrm{mod}\ p)$, $a_{p-1}\equiv 0\ (\mathrm{mod}\ p)$且 $a_{p-1}\neq p(\mathrm{mod}\ p^2)$。则 $f(x)$在 $Z/(p^2)$上是单圈。

证明　首先，因为 $a_1\equiv 1\ (\mathrm{mod}\ p)$, $a_2\equiv a_3\equiv\cdots\equiv a_{p-2}\equiv a_{p-1}\equiv 0\ (\mathrm{mod}\ p)$，所以 $f(x)\equiv x+1(\mathrm{mod}\ p)$。显然 $f(x)$在 $Z/(p)$上是单圈。另外，$f'(x)=(p-1)a_{p-1}x^{p-2}+(p-2)a_{p-2}x^{p-3}+\cdots+2a_2x+a_1$，因此可得 $f'(x)\equiv a_1\equiv 1(\mathrm{mod}\ p)$。

其次，因为 $f(x)$在 $Z/(p)$上是单圈，类似引理 4 的证明可得 $(f^p)'(0)\equiv f'(0)f'(1)f'(2)\cdots f'(p-1)(\mathrm{mod}\ p)\equiv 1(\mathrm{mod}\ p)$。

最后，因为 $f(x)\equiv x+1(\mathrm{mod}\ p)$，由引理 5 可得

$$\begin{aligned}f^p(0)&\equiv f(p-1)+f'(p-1)\,(f(p-2)-(p-1))+f'(p-1)\\&\quad\cdot f'(p-2)\,(f(p-3)-(p-2))+\cdots+f'(p-1)\\&\quad\cdot f'(p-2)\cdots f'(2)(f(1)-2)(\mathrm{mod}\ p^2)\\&\equiv f(p-1)+(f(p-2)-(p-1))+(f(p-3)-(p-2))\\&\quad+\cdots+(f(1)-2)(\mathrm{mod}\ p^2)\\&\equiv[f(p-1)+f(1)]+[f(p-2)+f(2)]+\cdots+[f((p\\&\quad+1)/2)+f((p-1)/2)]-[p(p-1)/2-1]\ (\mathrm{mod}\ p^2)\\&\equiv[2a_{p-1}+2a_{p-3}+\cdots+2a_2+pa_1+2]\\&\quad+[2a_{p-1}\cdot 2^{p-1}+2a_{p-3}\cdot 2^{p-3}+\cdots+2a_2\cdot 2^2+pa_1+2]\\&\quad+\cdots+[2a_{p-1}((p-1)/2)^{p-1}+2a_{p-3}((p-1)/2)^{p-3}\\&\quad+\cdots+2a_2((p-1)/2)^2+pa_1+2]-[p(p-1)/2-1]\\&\quad\cdot(\mathrm{mod}\ p^2)\\&\equiv 2a_{p-1}[1+2^{p-1}+3^{p-1}+\cdots+((p-1)/2)^{p-1}]+2a_{p-3}\\&\quad\cdot[1+2^{p-3}+3^{p-3}+\cdots+((p-1)/2)^{p-3}]+\cdots+2a_2\\&\quad\cdot[1+2^2+3^2+\cdots+((p-1)/2)^2]+a_1p(p-1)/2+2\\&\quad\cdot(p-1)/2-[p(p-1)/2-1](\mathrm{mod}\ p^2)\end{aligned}$$

由引理 6 和 $a_1\equiv 1(\mathrm{mod}\ p)$, $a_2\equiv a_3\equiv\cdots\equiv a_{p-2}\equiv a_{p-1}\equiv 0(\mathrm{mod}\ p)$，有 $f^p(0)\equiv 2a_{p-1}(p-1)/2+p\ (\mathrm{mod}\ p^2)\equiv p-a_{p-1}\neq 0\ (\mathrm{mod}\ p^2)$。由注 2 可知，$f(x)$在 $Z/(p^2)$上是单圈。　　证毕

6 结束语

目前，只有 p=2,3 时，针对剩余类环 $Z/(p^n)$上单圈多项式的研究才全部得以解决。本文对 $Z/(5)$上的任意次单圈多项式进行了完整的系数刻画，进一步，对 $Z/(5^2)$上的 6 次单圈多项式进行了完整的系数刻画；另外，本文给出了 $Z/(p^2)(p>3)$上的$(p-1)$次单圈多项式的部分构造。我们下一步的工作有两个方向：第一，对 $Z/(p)(p>5)$上的单圈多项式进行完整的系数刻画；第二，对 $Z/(p^2)(p>3)$上的任意次单圈多项式进行完整的系数刻画。

参 考 文 献

[1] Rivest R L. Permutation polynomials modulo 2^w. *Finite Fields and Their Applications*, 2001, 7(2): 287–292.

[2] Weng Guo-biao and Dong Chao-ping. A note on permutation polynomials over Z/nZ. *IEEE Transactions on Information Theory*, 2008, 54(9): 4388–4390.

[3] Coulter R, Henderson M, and Matthews R. A note on constructing permutation polynomials. *Finite Fields and Their Applications*, 2009, 15(5): 553–557.

[4] Ostafe A. Multivariate permutation polynomial systems and nonlinear pseudorandom number generators. *Finite Fields and Their Applications*, 2010, 16(3): 144–154.

[5] Li Ji-you, Chandler D B, and Xiang Qing. Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2. *Finite Fields and Their Applications*, 2010, 16(6): 406–419.

[6] Akbary A, Ghioca D, and Wang Qiang. On constructing permutations of finite fields. *Finite Fields and Their Applications*, 2011, 17(1): 51–67.

[7] Marcos J E. Specific permutation polynomials over finite fields. *Finite Fields and Their Applications*, 2011, 17(2): 105–112.

[8] Rivest R L, Shamir A, and Adleman L M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, 21(2): 120–126.

[9] Rivest R L, Robshaw M J B, Sidney R, *et al*.. The RC6 block cipher. http://theory.lcs.mit.edu/~rivest/rc6.pdf, 1998.

[10] Anashin V and Khrennikov A. De Gruyter Expositions in Mathematics. Berlin: Walter de Gruyter, 2009, Vol.49: Applied Algebraic Dynamics.

[11] Knuth D E. The Art of Computer Programming. Reading, MA: Addison-Wesley Publ. Co, 1998, Vol.2: Seminumerical Algorithms (3rd Edition).

[12] Larin M V. Transitive polynomial transformations of residue class rings. *Discrete Mathematics and Applications*, 2002, 12(2): 127–140.

[13] Durand F and Paccaut F. Minimal polynomial dynamics on the set of 3-adic integers. *Bulletin of the London Mathematical Society*, 2009, 41(2): 302–314.

游 伟： 男，1984 年生，博士生，研究方向为密码学.

戚文峰： 男，1963 年生，教授，博士生导师，研究领域包括密码学与信息安全.