模 2^n 剩余类环上的多项式变换的研究

王念平[1],宫秀华[2]
WANG Nian-ping[1],GONG Xiu-hua[2]

1.解放军信息工程大学 电子技术学院,郑州 450004
2.山东省东平县新湖中学,山东 东平 271506
1.Institute of Electronic Technology,the PLA Information Engineering University,Zhengzhou 450004,China
2.Xinhu Middle School of Dongping County,Dongping,Shandong 271506,China
E-mail:wwnnpp@126.com

WANG Nian-ping,GONG Xiu-hua.Researches on polynomial transformation over residue classes ring modulo 2^n.Computer Engineering and Applications,2008,44(33):60-61.

Abstract: Polynomial transformation over residue classes ring modulo 2^n is researched deeply in this paper.Let f be a polynomial transformation over residue classes ring modulo 2^n of degree m,a sufficiency and necessity condition such that f is a permutation is given.Upper bounds for the number of permutation polynomials over residue classes ring modulo 2^n of degree m is also given.
Key words: residue classes ring modulo 2^n;polynomial transformation;permutation polynomials

摘 要:对模 2^n 剩余类环上的多项式变换进行了详细的研究和分析。给出了模 2^n 剩余类环上的 $m(m\geqslant 1)$次多项式变换是置换的一个充分必要条件;给出了模 2^n 剩余类环上的 $m(m\geqslant 1)$次置换多项式个数的一个上界。
关键词:模 2^n 剩余类环;多项式变换;置换多项式
DOI:10.3778/j.issn.1002-8331.2008.33.019 **文章编号:**1002-8331(2008)33-0060-02 **文献标识码:**A **中图分类号:**TN918.1

1 引言

众所周知,一个 $\{0,1\}^n\rightarrow\{0,1\}^n$ 的变换可以有多种表示形式,当用多项式的形式表出时,就是所谓的多项式变换。具体地,当将$\{0,1\}^n$ 中的元素看作环 Z_{2^n} 中的元素时,相应的多项式变换就是环 Z_{2^n} 上的多项式变换。若该多项式变换还是环 Z_{2^n} 上的置换,则称该多项式变换为环 Z_{2^n} 上的置换多项式。对于多项式变换,人们关注较多的是有限域上的置换多项式[1]。本文对环 Z_{2^n} 上的多项式变换进行了详细的研究。

为方便起见,以下用 Z_{2^n} 表示模 2^n 剩余类环,用 Z_2 表示模 2 剩余类环,用“+”和“-”分别表示环 Z_{2^n} 中的加法和减法,用“$\oplus$”表示模 2 加。

2 有关的定义

定义 1 设 $\forall i,0\leqslant i\leqslant m,a_i\in Z_{2^n},a_m\neq 0$,称 $f(x)=\sum_{i=0}^{m}a_ix^i:Z_{2^n}\rightarrow Z_{2^n}$ 为环 Z_{2^n} 上的 m 次多项式变换。若该多项式变换还是 $Z_{2^n}\rightarrow Z_{2^n}$ 的置换,则称该多项式变换为环 Z_{2^n} 上的 m 次置换多项式。

引理 1 设 $f(x,y):Z_{2^n}\times Z_{2^n}\rightarrow Z_{2^n}$ 是二元多项式,则 $\forall(x,y)\in Z_{2^n}\times Z_{2^n}$,$f(x,y)$的值在 Z_{2^n} 中都可逆当且仅当将模 2^n 换成模 2,将 $f(x,y)$看作 $Z_2\times Z_2\rightarrow Z_2$ 的映射时 $f(x,y)$恒等于 1。

证明 $\forall(x,y)\in Z_{2^n}\times Z_{2^n}$,$f(x,y)$的值在 Z_{2^n} 中都可逆当且仅当 $f(x,y)$的值都是奇数,也等价于 $f(x,y)\bmod 2=1$,再注意到将 x 和 y 分别换成 $x \bmod 2$ 和 $y \bmod 2$ 时,$f(x,y)$的奇偶性并不改变,从而本引理结论成立。 证毕

3 主要结论

定理 1 环 Z_{2^n} 上的 m 次多项式变换 $f(x)=\sum_{i=0}^{m}a_ix^i$ 是置换当且仅当将模 2^n 换成模 2,将 $F(x,y)=\frac{f(x)-f(y)}{x-y}$ 看作 $Z_2\times Z_2\rightarrow Z_2$ 的映射时,$F(x,y)=\frac{f(x)\oplus f(y)}{x\oplus y}=\bigoplus_{i=1}^{m}a_i(\bigoplus_{0\leqslant j,k\leqslant i-1,j+k=i-1}x^jy^k)$恒等于1。

证明 $f(x)=\sum_{i=0}^{m}a_ix^i$ 是置换当且仅当它是 $Z_{2^n}\rightarrow Z_{2^n}$ 上的单射,这也等价于 $\forall(x,y)\in Z_{2^n}\times Z_{2^n}$,若 $f(x)=f(y)$则必有 $x=y$,即若有 $f(x)-f(y)=\sum_{i=1}^{m}a_i(x^i-y^i)=(x-y)\sum_{i=1}^{m}a_i\frac{x^i-y^i}{x-y}=0$,则必有 $x=y$,这也进一步等价于 $\forall(x,y)\in Z_{2^n}\times Z_{2^n}$,$\frac{f(x)-f(y)}{x-y}=\sum_{i=1}^{m}a_i\frac{x^i-y^i}{x-y}=\sum_{i=1}^{m}a_i(\sum_{0\leqslant j,k\leqslant i-1,j+k=i-1}x^jy^k)$在 Z_{2^n} 中都可逆,再由引理 1 即证。证毕

基金项目:现代通信国家重点实验室基金资助项目(No.9140C1102060702);河南省杰出青年科学基金资助项目(No.0312001800)。
作者简介:王念平(1973-),男,博士研究生,讲师,主要研究领域为信息安全,应用数学。
收稿日期:2007-12-18 **修回日期:**2008-03-12

定理 1 将多项式变换 $f(x)=\sum_{i=0}^{m}a_ix^i$ 是否是置换的问题转换为 $Z_2\times Z_2\to Z_2$ 的映射的判定问题，从而大大简化了判定条件。事实上，该判定条件还可进一步简化为以下形式，该结论在文献[2]中首次出现。

推论 1[2] m 是奇数时，环 Z_{2^n} 上的 m 次多项式变换 $f(x)=\sum_{i=0}^{m}a_ix^i$ 是置换当且仅当 a_1 是奇数且 $a_3+a_5+a_7+\cdots+a_m$ 和 $a_2+a_4+a_6+\cdots+a_{m-1}$ 都是偶数；m 是偶数时，环 Z_{2^n} 上的 m 次多项式变换 $f(x)=\sum_{i=0}^{m}a_ix^i$ 是置换当且仅当 a_1 是奇数且 $a_3+a_5+a_7+\cdots+a_{m-1}$ 和 $a_2+a_4+a_6+\cdots+a_m$ 都是偶数。

推论 1 给出的充要条件为环 Z_{2^n} 上的 m 次置换多项式的构造提供了很大的方便。

备注 1 环 Z_{2^n} 上的同一个多项式变换有可能用不同的多项式表达式来表示。例如，环 Z_{2^n} 上的置换多项式 $f(x)=x$ 还可以表示成 $f(x)=2x^2+3x$；环 Z_{2^n} 上的多项式变换 $f(x)=2x^2+2x$ 还可以表示成零多项式变换 $f(x)=0$。一般地，环 Z_{2^n} 上 m 次置换多项式的个数不超过 Z_{2^n} 上构成双射的 m 次多项式表达式的个数。

定理 2 环 Z_{2^n} 上的 1 次置换多项式不超过 2^{2n-1} 个；2 次置换多项式不超过 $2^{3n-2}-2^{2n-1}$ 个；3 次置换多项式不超过 $2^{4n-3}-2^{3n-2}$ 个；4 次置换多项式不超过 $2^{5n-3}-2^{4n-3}$ 个。

证明 由推论 1 知，1 次多项式变换 $f(x)=a_1x+a_0$ 是置换当且仅当 a_1 是奇数，从而 a_1 有 2^{n-1} 种取法，而 a_0 有 2^n 种取法，故构成双射的 1 次多项式表达式的个数为 $2^n\times 2^{n-1}=2^{2n-1}$，再由备注 1 即证；2 次多项式变换 $f(x)=a_2x^2+a_1x+a_0$ 是置换当且仅当 a_1 是奇数，a_2 是偶数且 $a_2\neq 0$，从而 a_1 有 2^{n-1} 种取法，a_2 有 $2^{n-1}-1$ 种取法，而 a_0 有 2^n 种取法，故构成双射的 2 次多项式表达式的个数为 $2^n\times 2^{n-1}\times(2^{n-1}-1)=2^{3n-2}-2^{2n-1}$，再由备注 1 即证；3 次多项式变换 $f(x)=a_3x^3+a_2x^2+a_1x+a_0$ 是置换当且仅当 a_1 是奇数，a_2 和 a_3 都是偶数且 $a_3\neq 0$，从而 a_1 有 2^{n-1} 种取法，a_2 有 2^{n-1} 种取法，a_3 有 $2^{n-1}-1$ 种取法，而 a_0 有 2^n 种取法，故构成双射的 3 次多项式表达式的个数为 $2^n\times 2^{n-1}\times 2^{n-1}\times(2^{n-1}-1)=2^{4n-3}-2^{3n-2}$，再由备注 1 即证；4 次多项式变换 $f(x)=a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$ 是置换当且仅当 a_1 是奇数，a_3 和 a_2+a_4 都是偶数且 $a_4\neq 0$，从而 a_1 和 a_3 各有 2^{n-1} 种取法，(a_2,a_4) 有 $2^{n-1}\times 2^{n-1}+2^{n-1}\times(2^{n-1}-1)=2^{2n-1}-2^{n-1}$ 种取法，而 a_0 有 2^n 种取法，故构成双射的 4 次多项式表达式的个数为 $2^n\times 2^{n-1}\times 2^{n-1}\times(2^{2n-1}-2^{n-1})=2^{5n-3}-2^{4n-3}$，再由备注 1 即证。　　证毕

定理 3 设 $m\geqslant 5$，则环 Z_{2^n} 上的 m 次置换多项式不超过 $2^{mn+n-3}-2^{mn-3}$ 个。

证明 按 m 的奇偶性分两种情形进行证明。

情形之一：m 是奇数时。

此时，由定理 2 知，m 是奇数时构成双射的 m 次多项式表达式的个数就是使得 a_1 是奇数且 $a_3+a_5+a_7+\cdots+a_m$ 和 $a_2+a_4+a_6+\cdots+a_{m-1}$ 都是偶数的 $a_0,a_1,\cdots,a_m$ 的取法数。显然 a_0 有 2^n 种取法；a_1 有 2^{n-1} 种取法；$a_2+a_4+a_6+\cdots+a_{m-3}$ 各有 2^n 种取法，a_{m-1} 有 2^{n-1} 种取法，从而使得 $a_2+a_4+a_6+\cdots+a_{m-1}$ 是偶数的 $a_2+a_4+a_6+\cdots+a_{m-1}$ 共有 $2^{\frac{m-3}{2}\times n+(n-1)}=2^{(mn-n-2)/2}$ 种取法。

(1)当 a_m 是奇数时，a_m 有 2^{n-1} 种取法；使得 $a_3+a_5+a_7+\cdots+a_m$ 是偶数的 $a_3,a_5,a_7,\cdots,a_m$ 的取法数就是使得 $a_3+a_5+a_7+\cdots+a_{m-2}$ 是奇数的 $a_3,a_5,a_7,\cdots,a_{m-2}$ 的取法数的 2^{n-1} 倍，而 $a_3,a_5,a_7,\cdots,a_{m-4}$ 各有 2^n 种取法，a_{m-2} 有 2^{n-1} 种取法，从而使得 $a_3+a_5+a_7+\cdots+a_{m-2}$ 是奇数的 $a_3,a_5,a_7,\cdots,a_{m-2}$ 的取法共有 $2^{\frac{m-5}{2}\times n+(n-1)}=2^{(mn-3n-2)/2}$ 种，进而使得 $a_3+a_5+a_7+\cdots+a_m$ 是偶数的 $a_3,a_5,a_7,\cdots,a_m$ 的取法共有 $2^{(mn-3n-2)/2+(n-1)}=2^{(mn-n-4)/2}$ 种；故使得 a_1 是奇数且 $a_3+a_5+a_7+\cdots+a_m$ 和 $a_2+a_4+a_6+\cdots+a_{m-1}$ 都是偶数的 $a_0,a_1,\cdots,a_m$ 的取法共有 $2^{n+(n-1)+(mn-n-2)/2+(mn-n-4)}=2^{mn+n-4}$ 种，从而 m 和 a_m 都是奇数时，构成双射的 m 次多项式表达式的个数为 2^{mn+n-4}，进而由备注 1 知，m 和 a_m 都是奇数时，环 Z_{2^n} 上的 m 次置换多项式不超过 2^{mn+n-4} 个。

(2)当 a_m 是偶数时，因 $a_m\neq 0$，故 a_m 有 $(2^{n-1}-1)$ 种取法；使得 $a_3+a_5+a_7+\cdots+a_m$ 是偶数的 $a_3,a_5,a_7,\cdots,a_m$ 的取法数就是使得 $a_3+a_5+a_7+\cdots+a_{m-2}$ 是偶数的 $a_3,a_5,a_7,\cdots,a_{m-2}$ 的取法数的 $(2^{n-1}-1)$ 倍，而 $a_3,a_5,a_7,\cdots,a_{m-4}$ 各有 2^n 种取法，a_{m-2} 有 2^{n-1} 种取法，从而使得 $a_3+a_5+a_7+\cdots+a_{m-2}$ 是偶数的 $a_3,a_5,a_7,\cdots,a_{m-2}$ 的取法共有 $2^{\frac{m-5}{2}\times n+(n-1)}=2^{(mn-3n-2)/2}$ 种，进而使得 $a_3+a_5+a_7+\cdots+a_m$ 是偶数的 $a_3,a_5,a_7,\cdots,a_m$ 的取法共有 $2^{(mn-3n-2)/2}\times(2^{n-1}-1)=2^{(mn-n-4)/2}-2^{(mn-3n-2)/2}$ 种；故使得 a_1 是奇数且 $a_3+a_5+a_7+\cdots+a_m$ 和 $a_2+a_4+a_6+\cdots+a_{m-1}$ 都是偶数的 $a_0,a_1,\cdots,a_m$ 的取法共有 $2^{n+(n-1)+(mn-n-2)/2}\times(2^{(mn-n-4)/2}-2^{(mn-3n-2)/2})=2^{mn+n-4}-2^{mn-3}$ 种，从而 m 是奇数且 a_m 是偶数时，构成双射的 m 次多项式表达式的个数为 $2^{mn+n-4}-2^{mn-3}$，进而由备注 1 知，m 是奇数且 a_m 是偶数时，环 Z_{2^n} 上的 m 次置换多项式不超过 $2^{mn+n-4}-2^{mn-3}$ 个。

由(1)和(2)知，m 是奇数时，环 Z_{2^n} 上的 m 次置换多项式不超过 $2^{mn+n-4}+2^{mn+n-4}-2^{mn-3}=2^{mn+n-3}-2^{mn-3}$ 个。

情形之二：m 是偶数时。

此时，由推论 1 知，m 是偶数时构成双射的 m 次多项式表达式的个数就是使得 a_1 是奇数且 $a_3+a_5+a_7+\cdots+a_{m-1}$ 和 $a_2+a_4+a_6+\cdots+a_m$ 都是偶数的 $a_0,a_1,\cdots,a_m$ 的取法数。显然 a_0 有 2^n 种取法；a_1 有 2^{n-1} 种取法；$a_3+a_5+a_7+\cdots+a_{m-3}$ 各有 2^n 种取法，a_{m-1} 有 2^{n-1} 种取法，从而使得 $a_3+a_5+a_7+\cdots+a_{m-1}$ 是偶数的 $a_3,a_5,a_7,\cdots,a_{m-1}$ 共有 $2^{\frac{m-4}{2}\times n+(n-1)}=2^{(mn-2n-2)/2}$ 种取法。

(1)当 a_m 是奇数时，a_m 有 2^{n-1} 种取法；使得 $a_2+a_4+a_6+\cdots+a_m$ 是偶数的 $a_2,a_4,a_6,\cdots,a_m$ 的取法数就是使得 $a_2+a_4+a_6+\cdots+a_{m-2}$ 是奇数的 $a_2,a_4,a_6,\cdots,a_{m-2}$ 的取法数的 2^{n-1} 倍，而 $a_2,a_4,a_6,\cdots,a_{m-4}$ 各有 2^n 种取法，a_{m-2} 有 2^{n-1} 种取法，从而使得 $a_2+a_4+a_6+\cdots+a_{m-2}$ 是奇数的 $a_2,a_4,a_6,\cdots,a_{m-2}$ 的取法共有 $2^{\frac{m-4}{2}\times n+(n-1)}=2^{(mn-2n-2)/2}$ 种，进而使得 $a_2+a_4+a_6+\cdots+a_m$ 是偶数的 $a_2,a_4,a_6,\cdots,a_m$ 的取法共有 $2^{(mn-2n-2)/2+n-1}=2^{(mn-4)/2}$ 种；故使得 a_1 是奇数且 $a_3+a_5+a_7+\cdots+a_{m-1}$ 和 $a_2+a_4+a_6+\cdots+a_m$ 都是偶数的 $a_0,a_1,\cdots,a_m$ 的取法共有 $2^{n+(n-1)+(mn-2n-2)/2+(mn-4)/2}=2^{mn+n-4}$ 种，从而 m 是偶数且 a_m 是奇数时，构成双射的 m 次多项式表达式的个数为 2^{mn+n-4}，进而由备注 1 知，m 是偶数且 a_m 是奇数时，环 Z_{2^n} 上的 m 次置换多项式不超过 2^{mn+n-4} 个。

（下转 78 页）