国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
一九八六年第二期　总第五十四期　　No.2 1986 Sum. 54

有限域上的多项式变换

曾济宇

摘要　本文把1977年由H.J. Nussbaumer首先提出的多项式变换推广到一般有限域上，并对其结构进行了研究。本文给出了构成这种多项式变换的各种充分必要条件，指出了求变换的方法并证明了对某个模给定长度的变换数目是多少。该理论可望在编码理论和数字信号处理中得到应用。

一、引　言

1977年，H.J. Nussbaumer提出了有理数域上的多项式变换，并把它用于通常数字卷积和DFT的计算[1][2]。设R是一个数域，$R[x]$表示R上的多项式环，对任何非零多项式$M(x)\in R[x]$，$M(x)$的剩余环记为$R[x]/(M(x))$，那么，以$M(x)$为模的一个多项式变换就是指$R[x]/(M(x))$内一个离散富里叶变换，也就是说，若N是某个正整数，$F(x)\in R[x]$，称$<N, F(x), M(x)>$构成一个长N，模$M(x)$，变换因子为$F(x)$的多项式变换，假若它是一个把$R[x]$中任何一串长N的多项式序列$H_n(x)$变换为$R[x]$中另一串长N的多项式序列$\bar{H}_k(x)$的变换，且满足：

1°. $\bar{H}_k(x)\equiv\sum_{n=0}^{N-1}H_n(x)F^{nk}(x)\bmod M(x)$　　$n=0,1,\cdots,N-1$，而且该变换是可逆的。

2°. 具有循环卷积特性(CCP)。即若

$$Y_k(x)\equiv\sum_{n=0}^{N-1}G_n(x)H_{<k-n>_N}(x)\bmod M(x)\qquad k=0,1,\cdots,N-1,$$

而$\bar{Y}_k(x)$，$\bar{G}_k(x)$，$\bar{H}_k(x)$分别表示$Y_n(x)$，$G_n(x)$，$H_n(x)$在该变换下的像，则

$$\bar{Y}_k(x)\equiv\bar{G}_k(x)\bar{H}_k(x)\bmod M(x)\qquad k=0,1,\cdots,N-1.$$

这里的定义和Nussbaumer首先提出的定义有所区别，但它们彼此等价。当R是有理数域时，Nussbaumer及后来许多人研究了变换的一些性质并把它用于二維卷积和二維DFT的计算，被证明是一种相当有效的方法，它能够不用乘法将二維卷积和二維DFT映射为一系列一維卷积和一維DFT，从而减少运算量[3][4][5]。由于在许多信号处理及编码、译码问题中要用到有限域上卷积和DFT的计算[6][7][8]，因而，研究有限域上的多项式变换及其在卷积和DFT计算中的应用是很有价值的。本文将对有限域上多

1985年9月收到

项式变换的理论进行研究。

二、有限域上多项式的性质

本节给出并证明有限域上多项式所独具的一些性质，一般域上多项式所共有的性质这里不给出。在华罗庚著的《数论导引》中对 Z_p 上的多项式的性质进行了研究，下面所陈述的性质可认为是 Z_p 上多项式性质的推广，这些性质对下节的证明至关重要。

以下总设 $R=GF(p^m)$，p 是素数。

定义 2.1 设 $f_1(x),\cdots,f_{p^{mn}}(x)$ 是 $GF(p^m)[x]$ 中 p^{mn} 个多项式，且对 n 次多项式 $\varphi(x)$ 两两互不同余，则称这些多项式构成 $\varphi(x)$ 的一个完全剩余系。

定义 2.2 设 $f_1(x),\cdots,f_k(x)$ 是一串多项式，对模 $\varphi(x)$ 两两不同余且都和 $\varphi(x)$ 互素，而且任何和 $\varphi(x)$ 互素的多项式都对模 $\varphi(x)$ 与 $f_1(x),\cdots,f_k(x)$ 中之一同余，则称这组多项式为模 $\varphi(x)$ 的一个简化剩余系。

容易验证，对同一个模 $\varphi(x)$，不同的完全剩余系或简化剩余系的多项式个数总是一样多的。我们把次数小于 $\varphi(x)$ 的次数的多项式全体称为 $\varphi(x)$ 的最小完全剩余系，而把次数小于 $\varphi(x)$ 的次数且和 $\varphi(x)$ 互素的多项式全体称为 $\varphi(x)$ 的最小简化剩余系。

以下记 $\varphi(x)$ 的简化剩余系中多项式个数为 $E(p^m,\ \varphi)$，并总设 $\deg(\varphi(x))=n$.

性质 1 $E(p^m,\ \varphi)$ 是 φ 的积性函数，即对任何 $\varphi(x)$ 和 $\psi(x)$，若 $(\varphi(x),\ \psi(x))=1$，则 $E(p^m,\ \varphi\psi)=E(p^m,\ \varphi)\cdot E(p^m,\ \psi)$，假定 $E(p^m,1)=1$.

证明 设 $f_1(x),\cdots,f_{E(p^m,\varphi)}(x)$ 表示 $\varphi(x)$ 的最小简化剩余系，

$g_1(x),\cdots,g_{E(p^m,\varphi)}(x)$ 表示 $\psi(x)$ 的最小简化剩余系。

令 $A=\{(f_i(x),\ g_j(x)\mid i=1,\cdots,E(p^m,\ \varphi),\ j=1,\cdots,E(p^m,\ \psi)\}$

$B=\{h(x)\mid h(x)$ 属于 $\varphi\psi$ 的最小简化剩余系$\}$

显然，A 的元素个数为 $E(p^m,\ \varphi)\cdot E(p^m,\ \psi)$，而 B 的元素个数为 $E(p^m,\ \varphi\psi)$。现在构造从集合 B 到集合 A 的一个映射 T，

$$T:\ B\to A,\ T(h(x))=(f(x),\ g(x))$$

其中 $f(x)\equiv h(x)\bmod\varphi(x)$，$g(x)\equiv h(x)\bmod\psi(x)$，根据孙子定理易知 T 是一个1-1对应，故 $E(p^m,\ \varphi\psi)=E(p^m,\ \varphi)\cdot E(p^m,\ \psi)$。 证毕。

性质 2 设 $\varphi(x)$ 的素因子分解式为 $\varphi(x)=\varphi_1^{l_1}(x)\cdots\varphi_k^{l_k}(x)$，其中 $\varphi_i(x)$ 的次数为 n_i，$l_1n_1+\cdots+l_kn_k=n$，则

$$E(p^m,\ \varphi)=p^{mn}\left(1-\frac{1}{p^{mn_1}}\right)\cdots\left(1-\frac{1}{p^{mn_k}}\right)$$

证明 由于 $\varphi_i(x)$ 是不可约的，故和 $\varphi_i^{l_i}(x)$ 不互素的多项式必然含有因子 $\varphi_i(x)$，注意到次数小于 $\varphi_i^{l_i}(x)$ 的次数 l_in_i 且含有因子 $\varphi_i(x)$ 的多项式恰有 $p^{mn_i(l_i-1)}$ 个，所以

$$E(p^m,\ \varphi_i^{l_i})=p^{mn_il_i}-p^{mn_i(l_i-1)}=p^{mn_il_i}\left(1-\frac{1}{p^{mn_i}}\right)$$

根据性质1，$E(p^m,\varphi)=E(p^m,\varphi_1^{l_1})\cdots E(p^m,\varphi_k^{l_k})=p^{mn}\left(1-\frac{1}{p^{mn_1}}\right)\cdots\left(1-\frac{1}{p^{mn_k}}\right)$

证毕。

性质3 若$(f,\varphi)=1$，则

$$[f(x)]^{E(p^m,\varphi)}\equiv 1 \bmod \varphi(x)$$

证明 设$f_1(x),\cdots,f_{E(p^m,\varphi)}(x)$为$\varphi(x)$的一个简化剩余系，由于$(f,\varphi)=1$，故$ff_1,\cdots,ff_{E(p_m,\varphi)}$亦为$\varphi$的一个简化剩余系，因而

$$(ff_1)\cdots(ff_{E(p^m,\varphi)})\equiv f_1\cdots f_{E(p^m,\varphi)} \bmod \varphi$$

即
$$f^{E(p^m,\varphi)}(f_1\cdots f_{E(p^m,\varphi)})\equiv f_1\cdots f_{E(p^m,\varphi)} \bmod \varphi$$

但$f_1\cdots f_{E(p^m,\varphi)}$和$\varphi$互素，故

$$f^{E(p^m,\varphi)}\equiv 1 \bmod \varphi$$ 证毕。

推论 若$\varphi(x)$不可约，$(f(x),\varphi(x))=1$，则$f^{p^{mn}-1}(x)\equiv 1 \bmod \varphi(x)$.

性质4 若$\varphi(x)$不可约，则对任意$d\mid p^{mn}-1$，存在$f(x)$使得$f(x)$是模$\varphi(x)$的d阶单位根，即d是使$f^d(x)\equiv 1 \bmod \varphi(x)$成立的最小正整数，且这样的$f(x)$共有$\varphi(d)$个，它们关于模$\varphi(x)$两两互不同余。（这里的$\varphi(\cdot)$表示数论中的Euler函数）

证明 对$\forall d\mid p^{mn}-1$，令$u(d)$表示阶为d的次数小于n的多项式的个数，由于任何和$\varphi(x)$互素的多项式必然是某个r阶单位根，$r\mid p^{mn}-1$，因而$\sum\limits_{d\mid p^{mn}-1}u(d)=p^{mn}-1$，$u(d)\geqslant 0$.

若对某个$d\mid p^{mn}-1$，有d阶单位根存在，不妨设$\bar{f}(x)$是一个d阶单位根，则$1,\bar{f}(x),\cdots,\bar{f}^{d-1}(x)$便是方程$f^d(x)\equiv 1 \bmod \varphi(x)$的全部互不同余的解，而这$d$个解中恰有$\varphi(d)$个，即$\bar{f}^r(x)$，$1\leqslant r\leqslant d$且$(r,d)=1$，是$d$阶单位根，所以$u(d)=\varphi(d)$.

若d阶单位根不存在，便有$u(d)=0$，故总有$u(d)\leqslant\varphi(d)$成立。但$\sum\limits_{d\mid p^{mn}-1}\varphi(d)=p^{mn}-1$，故$\sum\limits_{d\mid p^{mn}-1}u(d)=\sum\limits_{d\mid p^{mn}-1}\varphi(d)$，因而只可能是$u(d)=\varphi(d)$对所有$d\mid p^{mn}-1$成立。即$d$阶单位根存在且恰有$\varphi(d)$个对模$\varphi(x)$两两互不同余。 证毕。

推论 若$\varphi(x)$不可约，则存在$f(x)$，使$f^{p^{mn}-1}(x)\equiv 1 \bmod \varphi(x)$且对$\forall d$，$0<d<p^{mn}-1$，$f^d(x)\not\equiv 1 \bmod \varphi(x)$，这样的$f(x)$共有$\varphi(p^{mn}-1)$个，它们关于模$\varphi(x)$两两不同余。它们叫做$\varphi(x)$的原根。

性质5 若$N\mid p^{mn}-1$，$\varphi(x)$是不可约多项式，则对任何正整数$r>0$下列关系成立：

1° $\varphi^r(x)$的N阶单位根也是$\varphi(x)$的N阶单位根。

2° $\varphi^r(x)$的N阶单位根恰有$\varphi(N)$个对模$\varphi^r(x)$两两互不同余。

证明 1°设$F(x)$是模$\varphi^r(x)$的一个N阶单位根，设$F(x)$对模$\varphi(x)$的阶为d，由于$F^N(x)\equiv 1 \bmod \varphi(x)$，所以$d\mid N$.

若$d\not\equiv N$，则$d<N$，$F^N(x)-1=(F^d(x))^{N/d}-1=(F^d(x)-1)((F^d(x))^{\frac{N}{d}-1}+\cdots+$

$F^d(x)+1)\equiv 0 \bmod \varphi^r(x)$，由于 $F^d(x)-1\not\equiv 0 \bmod \varphi^r(x)$，所以

$$(F^d(x))^{\frac{N}{d}-1}+\cdots+F^d(x)+1\equiv 0 \bmod \varphi(x)$$

但 $F^d(x)\equiv 1 \bmod \varphi(x)$，因此，$\frac{N}{d}\equiv 0 \bmod \varphi(x)$，故只有 $p\left|\frac{N}{d}\right.$，因而 $p\mid N$，这和 $N\mid p^{mn}-1$ 矛盾，因此，$d=N$.

2° 先说明模 $\varphi^r(x)$的N阶单位根存在

由性质 4 可知，存在 $F(x)$使 $F(x)$是模 $\varphi(x)$的N阶单位根。设 $F(x)$ 对 模 $\varphi^r(x)$ 的 阶 为 d （根 据 性 质 3 可 知 d 存 在），由 于 $F^d(x)\equiv 1 \bmod \varphi^n(x)$，故 $F^d(x)\equiv 1 \bmod \varphi(x)$，因而$N\mid d$.

令$\bar{F}(x)\equiv F^{\frac{d}{N}}(x)\bmod \varphi^r(x)$，易知 $\bar{F}(x)$对模 $\varphi^r(x)$的阶恰为N.

现在来看 $\varphi^r(x)$的N阶单位根的个数。

设 $F(x)$对模 $\varphi^r(x)$的阶为N，则 $F^d(x)$当$(d,\ N)=1$ 时都是 $\varphi^r(x)$ 的 N 阶 单 位根，所以至少有 $\varphi(N)$个N阶单位根对模 $\varphi^r(x)$互不同余。

现在设 $F(x)$和 $\bar{F}(x)$都是 $\varphi^r(x)$的N阶单位根，且对模 $\varphi^r(x)$不同余，由 1° 知$F(x)$和 $\bar{F}(x)$也是模 $\varphi(x)$的N阶单位根，下面证明：

$$F(x)\not\equiv\bar{F}(x) \bmod \varphi(x)$$

若不然，则 $F(x)\equiv\bar{F}(x) \bmod \varphi(x)$，不妨设 $F(x)=\bar{F}(x)+t(x)\varphi^u(x)\quad 1\leqslant u<r$，且$t(x)\not\equiv 0 \bmod \varphi(x)$

由 $\quad F^N(x)\equiv 1 \bmod \varphi(\varphi)\Rightarrow(\bar{F}(x)+t(x)\varphi^u(x))^N-1\equiv 0 \bmod \varphi^r(x)$

展开后可知，存在某个多项式 $v(x)$使

$$\bar{F}^N(x)-1+Nt(x)\bar{F}^{N-1}(x)\varphi^u(x)+v(x)\varphi^{u+1}(x)\equiv 0 \bmod \varphi^r(x)$$

所以

$$Nt(x)\bar{F}^{N-1}(x)\varphi^u(x)\equiv 0 \bmod \varphi^{u+1}(x)$$

$$\Rightarrow Nt(x)\bar{F}^{N-1}(x)\equiv 0 \bmod \varphi(x)$$

但$(N\bar{F}^{N-1}(x),\ \varphi^r(x)=1$，故 $t(x)\equiv 0 \bmod \varphi(x)$，矛盾。

因此，$\varphi^r(x)$的N阶单位根的个数不会超过 $\varphi(x)$的N阶单位根的个数，但由性质 4 知 $\varphi(x)$的N阶单位根恰好有 $\varphi(N)$个，故 $\varphi^r(x)$的N阶单位根也是 $\varphi(N)$个。 证毕。

三、GF（P^m）上多项式变换的构造

定理 3.1 $\langle N,\ F(x),\ M(x)\rangle$构成 $GF(p^m)$上一个多项式变换的充要条件是：

1° $(N,\ M(x))=1$

2° $F^N(x)\equiv 1 \bmod M(x)$

3° 对$\forall r$，$0<r<N$，r 是自然数有：

$$(F^r(x)-1,\ M(x))=1$$

该定理是孙琦等著《快速数论变换》书的 186 页的一个定理的特殊情形，故在此不作证明。且在定理条件下，若 $\bar{G}_k(x)$是 $G_n(x)$的多项式变换，则$G_n(x)\equiv\frac{1}{N}\sum_{k=0}^{N-1}F^{-nk}(x)$

$\bar{G}_k(x) \bmod M(x)$，$n=0,1,\cdots,N-1$.

定理 3.2 $\langle N, F(x), M(x)\rangle$构成$GF(p^m)$上一个多项式变换的充要条件是：

1° $(N, M(x))=1$

2° $F^N(x)\equiv 1 \bmod M(x)$

3° 对 $\forall d$，$0<d<N$，若 $d \mid N$且$\frac{N}{d}$是素数，则$(F^d(x)-1, M(x))=1$

证明 由定理 3.1 知定理的必要性是明显的。

充分性 首先证明：在 1°，2°，3° 条件下，对 $\forall d$，$0<d<N$，若 $d \mid N$，则 $(F^d(x)-1, M(x))=1$

事实上，若$\frac{N}{d}$不是素数，不妨设$\frac{N}{d}=rp$，p是素数，于是 $\frac{N}{rd}=p$，由 3' 知 $(F^{rd}(x)-1, M(x))=1$，但 $F^d(x)-1 \mid F^{rd}(x)-1$，所以$(F^d(x)-1, M(x))=1$.

再证，对 $\forall d$，$0<d<N$，有$(F^d(x)-1, M(x))=1$.

用归纳法。

当 $d=1$ 时，由于 $d \mid N$，故$(F^d(x)-1, M(x))=1$，设对一切 u，$0<u<d$ 均有 $(F^u(x)-1, M(x))=1$，下证$(F^d(x)-1, M(x))=1$.

设$N=kd+r$，$0\leqslant r<d$。若 $r=0$. 则 $d \mid N$，故$(F^d(x)-1, M(x))=1$；若 $0<r<d$，由于

$$F^N(x)-1\equiv F^{kd+r}(x)-1\equiv F^r(x)(F^{kd}(x)-1)+F^r(x)-1\equiv 0 \bmod M(x)$$

故
$$F^r(x)(F^{kd}(x)-1)\equiv -(F^r(x)-1)\bmod M(x)$$

但 $(F^r(x)-1, M(x))=1$，故 $(F^r(x)(F^{kd}(x)-1), M(x))=1$。由于 $F^d(x)-1 \mid F^r(x)(F^{kd}(x)-1)$，所以$(F^d(x)-1, M(x))=1$. 因此，对 $\forall d$，$0<d<N$ 都有 $(F^d(x)-1, M(x))=1$，根据定理 3.1 知$\langle N, F(x), M(x)\rangle$构成一个多项式变换。

证毕。

该定理可认为是 P.J. Erdelsky 关于数论变换的一个定理之推广，见[9]。

定理 3.3 设 $\varphi(x)=\varphi_1^{l_1}(x)\cdots\varphi_k^{l_k}(x)$，$\varphi_1(x)$，$\cdots$，$\varphi_k(x)$是不可约多项式，且互不相同，其次数分别为 $n_1,\cdots,n_k$，$l_1n_1+\cdots+l_kn_k=n$，则存在以 $\varphi(x)$为模，长 N 的多项式变换的充要条件为：$N \mid O(\varphi(x))\triangleq(p^{mn_1}-1,\cdots,p^{mn_k}-1)$

证明

1)必要性若存在长为N模 $\varphi(x)$的多项式变换，则必存在 $F(x)\in GF(p^m,[x]$，使 $F^N(x)\equiv 1 \bmod \varphi(x)$，且 $F^r(x)-1$ 和 $\varphi(x)$互素，$0<r<N$. 故 $F(x)$也是模 $\varphi_i(x)$的 N阶单位根，$1\leqslant i\leqslant k$，根据二节性质3的推论易知$N \mid p^{mn_n}-1, 1\leqslant i\leqslant k$，故 $N \mid O(\varphi(x))$.

2) 充分性

设$N \mid O(\varphi(x))$，于是 $N \mid p^{mn_i}-1$，$i=1,\cdots,k$. 由二节性质 5 知存在 $F_i(x)$，使 $F_i(x)$是模 $\varphi_i^{l_i}(x)$的N阶单位根，且 $F_i(x)$也是模 $\varphi_i(x)$的N阶单位根。根据孙子定理，可构造 $F(x)$满足 $F(x)\equiv F_i(x) \bmod \varphi_i^{l_i}(x)$，$i=1,\cdots,k$，于是 $F(x)$对模 $\varphi(x)$的阶为 N，而且 $F(x)$对模 $\varphi_i(x)$的阶亦为N，$i=1,\cdots,k$.所以，对 $\forall d, 0<d<N$，$(F^d(x)-1,$

$\varphi_i(x))=1$，故 $(F^d(x)-1,\ \varphi(x))=1$. 又因为 $F^N(x)\equiv 1 \bmod \varphi^{l_i}_i(x)$，故 $F^N(x)\equiv 1 \bmod \varphi(x)$. 根据定理 3.1，$<N,\ F(x),\ \varphi(x)>$构成一个多项式变换。　　证毕。

定理 3.4　设 $\varphi(x)=\varphi^{l_1}_1(x)\cdots\varphi^{l_k}_k(x)$是 $\varphi(x)$的素因子分解式，$N\mid O(\varphi(x))$，则恰有 $\varphi^k(N)$个长N模 $\varphi(x)$且变换因子对模 $\varphi(x)$两两不同余的多项式变换。

证明　设 $F_i(x)$是模 $\varphi^{l_i}_i(x)$的一个N阶单位根，由二节性质 5 可知 $F_i(x)$ 也是模 $\varphi_i(x)$的N阶单位根，于是利用孙子定理构造 $F(x)$满足其：

$$F(x)\equiv F_i(x) \bmod \varphi^{l_i}_i(x),\ i=1,\cdots,k$$

这样的 $F(x)$对模 $\varphi(x)$唯一，而且$<N,\ F(x),\ \varphi(x)>$构成一个多项式变换；另外，若$<N,\ F(x),\ \varphi(x)>$构成一个多项式变换，由定理 3.1 可知，$F(x)$必然是模 $\varphi^{l_i}_i(x)$的N阶单位根。由于对每个 $\varphi^{l_i}_i(x)$，其N阶单位根恰有 $\varphi(N)$个对模 $\varphi^{l_i}_i(x)$两两不同余，因而对模 $\varphi(x)$两两不同余的长N模 $\varphi(x)$的变换因子恰有 $\varphi^k(N)$个。　　证毕。

由定理 3.3 可知，若 $\varphi(x)=\varphi^{l_1}_1(x)\cdots\varphi^{l_k}_k(x)$，$N\mid(p^{mn_1}-1,\cdots,p^{mn_k}-1)$，则只要 $F(x)$是每个 $\varphi^{l_i}_i(x)$的N阶单位根，$<N,\ F(x),\ \varphi(x)>$便构成一个多项式变换。因而问题是如何求 $\varphi^{l_i}_i(x)$的N阶单位根。下面的定理将使这个问题简化。

定理 3.5　设$N=N_1N_2$，$(N_1,\ N_2)=1$，则

1°　若 $F_i(x)$为 $\varphi(x)$的 N_i 阶单位根，$i=1,2$，则 $F(x)\equiv F_1(x)F_2(x)\bmod\varphi(x)$是 $\varphi(x)$的N阶单位根；

2°　若$<N_i,\ F_i(x),\ \varphi(x)>$构成一个多项式变换，$i=1,2$，则$<N,F(x),\varphi(x)>$ 构成多项式变换，其中 $F(x)\equiv F_1(x)F_2(x)\bmod\varphi(x)$.

证明　1°显然，$(F_1(x)F_2(x))^N\equiv 1 \bmod \varphi(x)$，所以，若 $F(x)$对模 $\varphi(x)$之阶为 d，则 $d\mid N$.

另一方面，$(F_1(x)F_2(x))^{dN_1}\equiv F_1^{dN_1}(x)F_2^{dN_1}(x)\equiv F_2{}^{dN_1}(x)\equiv 1 \bmod \varphi(x)$，所以 $N_2\mid dN_1$，但$(N_1,\ N_2)=1$，故，$N_2\mid d$，同理可证$N_1\mid d$，所以$N\mid d$.

综上所述得 $d=N$.

2°　由 1° 及定理 3.5 前的说明知其成立。　　证毕。

现在，我们可以给出如下求多项式变换的方法：

1°　分解 $\varphi(x)$，设 $\varphi(x)=\varphi^{l_1}_1(x)\cdots\varphi^{l_k}_k(x)$，再分解$N$，设$N=q^{r_1}_1\cdots q^{r_u}_u$，$q_1,\cdots,q_u$是互异素数（当然要求 $N\mid O(\varphi(x))$

2°　求每个 $\varphi^{l_i}_i(x)$的 $q^{r_j}_j$ 阶单位根，设为$F_{ij}(x)$，取 $F_i(x)\equiv F_{i1}(x)\cdots F_{iu}(x)\cdot \bmod\varphi^{l_i}_i(x)$.

3°　用孙子定理构造 $F(x)$满足：

$$F(x)\equiv F_i(x)\bmod\varphi^{l_i}_i(x),\ i=1,2,\cdots,k,$$

则$<N,\ F(x),\ \varphi(x)>$构成一个多项式变换。

例 在$GF(5)=Z_5$上求模x^4+1长为24的多项式变换

解 不难验证$x^4+1=(x^2+2)(x^2-2)$是它在Z_5上的不可约多项式分解，故$O(x^4+1)=(5^2-1,\ 5^2-1)=24$,由定理3.3知长24模$x^4+1$的多项式变换存在。

$$24=8\times 3$$

求x^2+2和x^2-2的8阶和3阶单位根。

对任意正整数a，若$(a,\ 5)=1$，则$a^4\equiv 1 \bmod 5$，而$x^4\equiv -1 \bmod (x^2\pm 2)$，故$(ax)^4\equiv -1 \bmod(x^2\pm 2)$，$(ax)^8\equiv 1 \bmod(x^2\pm 2)$，故$ax$是模$(x^2\pm 2)$的8阶单位根，$a=1,2,3,4$.

设$ax+b$是模x^2+2的一个三阶单位根，则必然$(ax+b)^3\equiv 1 \bmod(x^2+2)$. 故$(ax+b)^5\equiv(ax+b)^2 \bmod (x^2+2)$，注意到$(ax+b)^5\equiv ax^5+b\equiv -ax+b \bmod(x^4+1)$，所以可得

$$\begin{cases} b+2a^2-b^2\equiv 0 & \bmod 5 \\ a+2ab\equiv 0 & \bmod 5 \end{cases}$$

该方程组之非零解为

$$\begin{cases} a\equiv 0 & \bmod 5 \\ b\equiv 1 & \bmod 5 \end{cases} \qquad \begin{cases} b\equiv 2 & \bmod 5 \\ a\equiv \pm 1 & \bmod 5 \end{cases}$$

第一组解显然不是三阶单位根，因而第二组解必是三阶单位根（因为x^2+2的三阶单位根恰有两个），即$\pm x+2$是模x^2+2的两个3阶单位根。

同理可得$\pm 2x+2$是模x^2-2的两个三阶单位根。

所以x^2+2的24阶单位根为$ax(\pm x+2)$. x^2-2的24阶单位根为$bx(\pm 2x+2)$

$$a\not\equiv 0 \bmod 5,\ b\not\equiv 0 \bmod 5$$

利用孙子定理构造$F(x)$满足：

$$\begin{cases} F(x)\equiv ax(\pm x+2) \bmod(x^2+2) \\ F(x)\equiv bx(\pm 2x+2) \bmod(x^2-2) \end{cases}$$

解的一般形式为

$$F(x)\equiv ax(\pm x+2)(x^2-2)-bx(\pm 2x+2)(x^2+2) \bmod(x^4+1)$$

这样的$F(x)$便是所求的变换因子，恰有$\varphi^2(24)=64$个，它们对模x^4+1两两不同余。

取$a=b=1$，可求得4个解为

$$2x^2+2x+2,\ 4x^2+2x+1,\ x^2+2x+4,\ 3x^2+2x+3.$$

它们都是长24模x^4+1的变换因子。

四、两个有用的变换

利用上节的定理3.2可得到下面两个变换。

1° q是一个素数，$q\not\equiv p$，则$\langle q^l,\ F(x),\ M(x)\rangle$构成$GF(p^m)$上一个多项式变换。这里$M(x)=(F^{q^l}(x)-1)/(F^{q^{l-1}}(x)-1)$，$F(x)$是$GF(p^m)[x]$中任何次数不小于1的多项式，$l$是任意自然数。特别地，若取$F(x)=x$，则$\langle q^l,\ x,\ (x^{q^l}-1)/(x^{q^{l-1}}-1)\rangle$构成一个变换；又若$q=2$，便有$\langle 2^l,\ x,\ x^{2^{l-1}}+1\rangle$构成一个多项式变换（若$p$是奇素数）。

2° 设p，q是互不相同的两个奇素数，则$\langle 2q^l,\ F(x),\ M(x)\rangle$构成$GF(p^m)$上

一个多项式变换，l 是任意自然数，$F(x)$是$GF(p^m)[x]$中任何次数不小于 1 的多项式，$M(x)=(F^{q^l}(x)+1)/(F^{q^{l-1}}(x)+1)$. 特别地，若取 $F(x)=x$，便有$<2q^l, x, (x^{q^l}+1)/(x^{q^{l-1}}+1)>$构成一个多项式变换。

我们选择 2° 加以证明。1° 的证明类似。

根据定理 3.2，只需证明 $(F^{q^l}(x)-1, M(x))=1$，且$(F^{2q^{l-1}}(x)-1, M(x))=1$（因为显然$[F(x)]^{2q^l}\equiv 1 \bmod M(x)$）

事实上，由于$2^{-1}(F^{q^l}(x)+1)-2^{-1}(F^{q^l}(x)-1)=1$，故$(F^{q^l}(x)+1, F^{q^l}(x)-1)=1$，但$M(x)\mid F^{q^l}(x)+1$，所以$(F^{q^l}(x)-1, M(x))=1$.

另外，
$$M(x)=(F^{q^l}(x)+1)/(F^{q^{l-1}}(x)+1)$$
$$=\sum_{i=0}^{q-1}(-1)^i F^{iq^{l-1}}(x)=\sum_{i=1}^{(q-1)/2}\cdot[(-1)^{2i-1}F^{(2i-1)q^{l-1}}(x)+(-1)^{2i}F^{2iq^{l-1}}(x)+1]$$
$$=\sum_{i=1}^{\frac{q-1}{2}}\{(-1)^{2i-1}[F^{(2i-1)q^{l-1}}(x)+1]+(-1)^{2i}]F^{2iq^{l-1}}(x)-1]\}+q$$

注意到上式中和式的每一项都可以被 $F^{q^{l-1}}(x)+1$ 整除，故可设整个和式为$(F^{q^{l-1}}(x)+1)Q(x)$，于是 $M(x)=(F^{q^{l-1}}(x)+1)Q(x)+q$. 由于$(q, M(x))=1$，所$(F^{q^{l-1}}(x)+1, M(x))=1$，又因为 $F^{q^{l-1}}(x)-1\mid F^{q^l}(x)-1$，故 $(F^{q^{l-1}}(x)-1, M(x))=1$，综上有$(F^{2q^{l-1}}(x)-1, M(x))=1$. 证毕

在实际应用中，通常要求变换因子越简单越好，而上面两个变换中，变换因子可取 x，因而是很好的。

致谢 本文承蒙蒋增荣老师指导，深表谢意。

参 考 文 献

[1] H.J. Nussbaumer, P. Quandalle, Computation of Convolution and Discrete Fourier Transform by Polynomial Transforms, IBM J. Res. Develop., Vol.22, No.2, March 1978.

[2] H.J. Nussbaumer, Fast Fourier Transform and Convolution Algorithms, Spring-Verlag Berlin Heidelkerg New York 1981.

[3] 蒋增荣，多项式变换及其在卷积计算中的应用，计算数学，第3期，1983年8月。

[4] 蒋增荣，用快速多项式变换(FPT)计算二维离散富里叶变换(DFT)，高校计算数学学报，第2期，1984年6月。

[5] B. Arambepola, P. J. W. Rayner: Efficient transforms for multidimensional convolutions. Electron. Lett. 15, 189-190(1979)

[6] N.J. Sloane and F.J. Mcwillams, The Theorey of Error Correcting Codes. Amsterdam, The Netherlands, North-Holland, 1978.

[7] G.R. Redinbo, B.O. Carhoum, and B.L. Johnson, Fast algorithms for signal processing using finite field operations, Proc. 1982 IEEE Int. Conf. Assp, Paris, France.

[8] I.S. Reed et al., Fast transforms for decoding jReed-Solomon codes, Proc. IEE, Vol. 128, pt.F, pp9-14, Feb. 1981.

[9] P.J. Erdelsky, Exact convolutions by number-theoretic transforms, Rept. No. AD-A013 395, San Diego, Calif, Naval Undersea Center (1975)

Polynomial Transform Over Finite Field

Zeng Jiyu

Abstract

Polynomial transform over rational number field was first proposed by H.J. Nussbaumer in 1977. In this paper we introduce polynomial transform over finite field. This paper presents various necessary and sufficient conditions for causing such a transform and gives a method to obtain the transform. We have also found the number of polynomial transforms for a fixed transform module and fixed transform length. The theory is expected to be widely used in signal processing, encoding and decoding.