开关函数的反演公式*

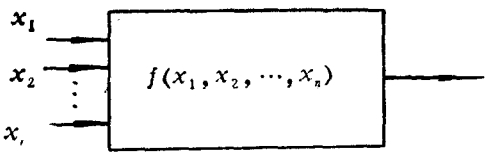
尹克震

（南京电子技术研究所）

一 引 言

本文将对 $GF(q)$（特别 $GF(2)$）上多项式形式的 n 元开关函数，利用有限域上的正交性，给出反演公式。

考察下列开关线路，这是有 n 个输入端和一个输出端的开关线路。假定此开关线路的输入和输出均在 q 个元素的有限域 $GF(q)$ 中取值，亦即，开关线路由 $GF(q)$ 上的加法器、乘法器、加常数门及乘常数门等逻辑器件所组成。



在数学上，一个有 n 个输入端和一个输出端的开关线路可由一个 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 来描述（见[1]），它是一个 n 个变元 $x_1, x_2, \cdots, x_n$ 在 $GF(q)$ 中独立取值，而函数值 $f(x_1, x_2, \cdots, x_n)$ 也在 $GF(q)$ 中取值的函数。大家知道，一个 $GF(q)$ 上的 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 可唯一地表成以下的多项式形状：

$$f(x_1, x_2, \cdots, x_n) = \sum_{i_1, i_2, \cdots, i_n = 0}^{q-1} C_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}, \quad C_{i_1 i_2 \cdots i_n} \in GF(q).$$

如通常，设 $0 \leqslant r \leqslant n(q-1)$，若有 $\partial^\circ f(x_1, x_2, \cdots, x_n) = r$ 则称此开关函数 $f(x_1, x_2, \cdots, x_n)$ 为 r 阶的开关函数。

* 1980 年 12 月 11 日收到。

推荐者：莫绍揆（南京大学数学系）。

二 反演公式与例子

对 $GF(q)$ 上多项式形式的开关函数，我们获得下列反演公式：

定理 1 如果

$$f(x_1,x_2,\cdots,x_n)=\sum_{i_1,i_2,\cdots,i_n=0}^{q-1}C_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n},\qquad C_{i_1i_2\cdots i_n}\in GF(q),$$

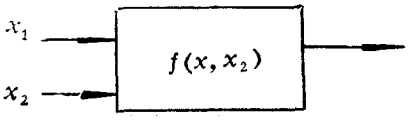
则

$$C_{i_1i_2\cdots i_n}=\sum_{x_1,x_2,\cdots,x_n\in GF(q)}f(x_1,x_2,\cdots,x_n)\,(\delta_{i_10}-x_1^{q-1-i_1})\,(\delta_{i_20}-x_2^{q-1-i_2})\cdots(\delta_{i_n0}-x_n^{q-1-i_n})$$

其中非负整数 i_j: $0\leqslant i_1,i_2,\cdots,i_n\leqslant q-1$，符号 $\delta_{ij}=\begin{cases}1, i=j;\\ 0, i\neq j.\end{cases}$

在证明反演公式前，先讨论一个具体例子。

考虑 $GF(3)$ 上的一个开关线路



已知二元开关函数 $f(x_1,x_2)$ 的真值表如下：

x_1	x_2	$f(x_1,x_2)$
0	0	2
0	1	1
0	2	1
1	0	0
1	1	2
1	2	0
2	0	1
2	1	0
2	2	1

问此开关函数 $f(x_1,x_2)$ 是怎样的多项式？

利用上述的反演公式可求得：

$$C_{00}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(1-x_1^2)(1-x_2^2)=f(0,0)=2,$$

$$C_{01}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(1-x_1^2)(-x_2)=-\sum_{x_2=1}^{2} f(0,x_2)x_2=-3=0,$$

$$C_{02}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(1-x_1^2)(-1)=-\sum_{x_2=0}^{2} f(0,x_2)=-4=2,$$

$$C_{10}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(-x_1)(1-x_2^2)=-\sum_{x_1=1}^{2} f(x_1,0)x_1=-2=1,$$

$$C_{11}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(-x_1)(-x_2)=\sum_{x_1,x_2=1}^{2} f(x_1,x_2)x_1x_2=6=0,$$

$$C_{12}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(-x_1)(-1)=\sum_{x_1=1}^{2}\sum_{x_2=0}^{2} f(x_1,x_2)x_1=6=0,$$

$$C_{20}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(-1)(1-x_2^2)=-\sum_{x_1=0}^{2} f(x_1,0)=-3=0,$$

$$C_{21}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(-1)(-x_2)=\sum_{x_1=0}^{2}\sum_{x_2=1}^{2} f(x_1,x_2)x_2=7=1,$$

$$C_{22}=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)(-1)(-1)=\sum_{x_1,x_2=0}^{2} f(x_1,x_2)=8=2,$$

不难验证，多项式

$$f(x_1,x_2)=2+x_1+2x_2^2+x_1^2x_2+2x_1^2x_2^2$$

确是欲求的二元开关函数。

三　反演公式的证明

为证反演公式，需要下列引理：

引理 1　对于非负整数 h，有

$$\sum_{x\in GF(q)} x^h=\begin{cases}-1, & h=k(q-1)\neq 0;\\ 0, & \text{其余。}\end{cases}$$

证明见〔2〕中引理10·1(p.321)。

由引理 1，我们容易得到有限域上的正交性。

引理 2　在$GF(q)$上有下列正交性

$$\sum_{x\in GF(q)}(\delta_{i0}-x^{q-1-i})x^j=\delta_{ij}=\begin{cases}1, & j=i;\\ 0, & j\neq i,\end{cases}$$

其中 $0 \leqslant i,\ j \leqslant q-1$。

证明：因为

$$\sum_{X \in GF(q)} (\delta_{i0} - X^{q-1-i}) x^j = \begin{cases} \sum\limits_{X \in GF(q)} (-x^{q-1}) = 1, & j = i \neq 0; \\ \sum\limits_{X \in GF(q)} (1 - x^{q-1}) = 1, & j = i = 0; \\ \sum\limits_{X \in GF(q)} (-x^{j-i}) = 0, & j > i,\ i \neq 0; \\ \sum\limits_{X \in GF(q)} (-x^{q-1-(i-j)}) = 0, & j < i,\ i \neq 0; \\ \sum\limits_{X \in GF(q)} (x^j - x^j) = 0, & j \neq i,\ i = 0, \end{cases}$$

故知此引理成立。

有了正交性引理，即可证明反演定理。因

$$\sum_{x_1, x_2, \cdots, x_n \in GF(q)} f(x_1, x_2, \cdots, x_n) (\delta_{i_1 0} - x_1^{q-1-i_1}) (\delta_{i_2 0} - x_2^{q-1-i_2}) \cdots (\delta_{i_n 0} - x_n^{q-1-i_n})$$

$$= \sum_{x_1, x_2, \cdots, x_n \in GF(q)} \left(\sum_{j_1, j_2, \cdots, j_n = 0}^{q-1} C_{i_1 i_2 \cdots i_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \right) (\delta_{i_1 0} - x_1^{q-1-i_1}) \cdots (\delta_{i_n 0} - x^{q-1-i_n})$$

$$= \sum_{j_1, j_2, \cdots, j_n = 0}^{q-1} C_{j_1 j_2 \cdots j_n} \left(\sum_{x_1, x_2, \cdots, x_n \in GF(q)} (\delta_{i_1 0} - x_1^{q-1-i_1}) x_1^{j_1} \cdots (\delta_{i_n 0} - x_n^{q-1-i_1}) x_n^{j_n} \right)$$

$$= \sum_{j_1, j_2, \cdots, j_n = 0}^{q-1} C_{j_1 j_2 \cdots j_n} \left(\prod_{t=1}^{n} \sum_{x_t \in GF(q)} (\delta_{i_t 0} - x_t^{q-1-i_t}) x_t^{j_t} \right) = C_{i_1 i_2 \cdots i_n},$$

由此得到开关函数的反演公式成立。

四 GF(2)上的反演公式

为导出$GF(2)$上的反演公式，我们需要半序集的概念。

设 $R^n = \{(a_1, a_2, \cdots, a_n) \mid a_t \in GF(2), t = 1, 2, \cdots, n\}$ 为 $GF(2)$ 上一 n 重集，今赋于 R^n 二元关系 $\leqslant$：

定义 对 $(a_1, a_2, \cdots, a_n)$、$(b_1, b_2, \cdots, b_n) \in R^n$，如果

$$a_1 \leqslant b_1,\ a_2 \leqslant b_2, \cdots, a_n \leqslant b_n,$$

则定义

$$(a_1, a_2, \cdots, a_n) \leqslant (b_1, b_2, \cdots, b_n).$$

明显，二元关系$\leqslant$是R^n上的半序关系．因此R^n是一半序集，且是局部有限半序集(见〔3〕)．利用这半序集概念，我们得到

定理 2　设R^n是如上定义的半序集，如果

$$f(x_1, x_2, \ldots x_n) = \sum_{(i_1, i_2, \cdots, i_n) \in R^n} C_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}, \quad C_{i_1 i_2 \cdots i_n} \in GF(2),$$

则

$$C_{i_1 i_2 \cdots i_n} = \sum_{\substack{(x_1, x_2, \cdots, x_n) \in R^n \\ (x_1, x_2, \cdots, x_n) \leqslant (i_1, i_2, \cdots, i_n)}} f(x_1, x_2, \cdots, x_n), \qquad (i_1, i_2, \cdots, i_n) \in R^n.$$

证明：因为在$q=2$时，定理 1 中的因子

$$\delta_{i0} - x^{1-i} = \begin{cases} 1, & i=0, \quad x=0; \\ 0, & i=0, \quad x=1; \\ -1, & i=1, \quad x=0; \\ -1, & i=1, \quad x=1. \end{cases}$$

于是

$$\prod_{t=1}^{n} (\delta_{i_t 0} - x_t^{1-i_t}) = \begin{cases} 0, & \text{至少有} - t \text{ 使 } 0 = i_t < x_t = 1; \\ 1, & \text{对每} - t \text{ 有 } x_t \leqslant i_t, \end{cases}$$

故知定理得证．

从定理 2 不难看出，对$GF(2)$上的开关函数$f(x_1, x_2, \cdots, x_n)$，欲求系数$C_{i_1 i_2 \cdots i_n}$，则需给出

$$2^{\sum_{t=1}^{n} i_t}$$

个其变元满足$(x_1, x_2, \cdots, x_n) \leqslant (i_1, i_2, \cdots, i_n)$的开关函数值．

关于$GF(q)$上多项式形式的n元开关函数，也可用布尔差分的方法来求其系数，这方面的讨论请参见〔4〕．

对南京大学莫绍揆教授给予的热情支持和宝贵指导，在此表示衷心的感谢．

参　考　文　献

〔1〕 Kautz, W.H. (ed.), Linear Sequential Switching Circuits, Holden-Day, San Francisco, U.S.A. (1965).

〔2〕 Peterson, W.W., and Weldon, E.J., Error-Correcting Codes, 2nd ed., M.I.T. Press, Cambridge, Mass. U.S.A. (1971).

〔3〕 Birkhoff, G., and Mac Lane, S., A Survey of Modern Algebra, 4th ed., Macmillan Publishing Co., Inc., New York (1977), Chapter 11.

〔4〕 Benjauthrit, B., and Reed, I.S., Galois Switching Functions and their Applications, IEEE Trans. Computers, C-25: 1 (1976), pp.78—86.

An Inversion Formula for Switching Functions

By Yin Kezhen (尹克震)

Abstract

An inversion formula for a class of n-variable switching functions in the form of a polynomial expansion over the finite field GF(q) (particularly over GF(2)) is derived in this paper by means of the orthonormality over a finite field.