M 序列反馈函数多项式表示的快速构造方法

关杰，周琮伟
（解放军信息工程大学三院，河南 郑州 450001）

摘 要：*M* 序列反馈函数的构造一直是序列密码理论的研究热点。基于由 *m* 序列构造 *M* 序列反馈函数的结构特性，结合函数变换和函数派生的方式得到一类 *M* 序列反馈函数的快速构造方法，并给出了该类 *M* 序列反馈函数的多项式表示、计数以及重量性质。

关键词：*M* 序列反馈函数；多项式表示；函数变换；函数派生
中图分类号：TN918.2
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018060

Method of fast construction of *M*-sequence feedback functions with polynomial representation

GUAN Jie, ZHOU Congwei
Department of Three, PLA Information Engineering University, Zhengzhou 450001, China

Abstract: The construction of *M*-sequence feedback functions has always been a hotspot in the theory of stream cipher. Based on the structural properties of the *M*-sequence feedback function constructed by the *m*-sequence, the method of fast construction of a class *M*-sequence feedback functions was proposed by combining the function transformation and function derivative. Meanwhile, polynomial representation, amount and weight property of the class *M*-sequence feedback functions were considered.

Key words: *M*-sequence feedback function, polynomial representation, function transformation, function derivative

1 引言

一个 n 级移位寄存器至多产生周期为 2^n 的序列，通常称达到最大周期 2^n 的序列为 *M* 序列，又叫 De Bruijn 序列。关于 LFSR 的圈结构已经可以完全刻画，并且知道最大周期的 2^n-1 的序列由其特征多项式为二元域上的本原多项式产生，此时，称周期为 2^n-1 的序列为 *m* 序列。相较于 *m* 序列，*M* 序列有着更好的线性复杂度和自相关性质，一直以来其构造问题是序列密码理论的研究热点。由于 NFSR 的圈结构没有较好的刻画手段，故其构造的经典方法一直以来局限于图论的反树和因子关联图法[1]，小项表示的圈剪接筛法[2]和由一个 *M* 序列通过对称[3]、派生[4]和递归[5]等得到一类 *M* 序列。近期，国外学者关于 *M* 序列的构造主要有“改进版”的 Martin 算法[6]以及关于 D-同态递归构造的最新研究成果[7]。而国内学者关于 *M* 序列构造的新思路和研究主要有“编织法”[8]，利用复合函数所代表的寄存器因子关联图的研究构造 *M* 序列[9~13]以及针对大级数的并圈构造[14]。以上这些构造方法大致可以分为两类，即同级直接生成的“并圈法”以及小级数递归生成大级数的“递归法”。但是“并圈法”生成的 *M* 序列往往需要大量的统计、判断和检验，并且得到的 *M* 序列往往是以小项表示；而“递归法”往往得到的 *M* 序列个数较少且 *M* 序列往往与小级数的初始序列具有较大相关性。

收稿日期：2017-07-17；**修回日期**：2018-02-27
通信作者：周琮伟，676052186@qq.com
基金项目：国家自然科学基金资助项目（No.61572516, No.61272041, No.61272488）
Foundation Item: The National Natural Science Foundation of China (No.61572516, No.61272041, No.61272488)

因此，针对以上 *M* 序列在实际构造中存在的问题，本文提出了一类可以实际应用，且以多项式表示的 *M* 序列反馈函数的快速构造方法。

2　预备知识

以下是本文用到的定义和符号说明。

Gf：以 f 为反馈函数的 n 级移位寄存器的状态图。

对偶变换 D：设 $(\underline{a})=(a_1,a_2,\cdots,a_T,\cdots)$ 为 f 产生的 $GF(2)$ 上任意一条周期为 T 的序列，令“+”为 $GF(2)$ 上的加法运算，则 $D(\underline{a})=(a_1+1,a_2+1,\cdots,a_T+1,\cdots)$。

对称变换 R：$R(\underline{a})=(a_T,a_{T-1},\cdots,a_1,\cdots)$。

组合变换 RD：$RD(\underline{a})=(a_T+1,a_{T-1}+1,\cdots,a_1+1,\cdots)$。

A_i：$f_0(x_2,\cdots,x_n)$ 中所有 $i(0\leqslant i\leqslant n-1)$ 次项的集合为 A_i，特别地，零次项为 1 以及最高次项为 $x_2\cdots x_n$。

常见的反馈函数有 2 种表示方法，即小项表示和多项式表示。在实际应用中，更实用的是用多项式表示的反馈函数，因为利用多项式表示的反馈函数其构造 *M* 序列无论从软件和硬件实现的角度都更为方便快捷。文献[15]给出了圈结构不含枝即非奇异的 n 级反馈函数，其用多项式表示 3 种函数变换的对应表达式。

定理 1[15]　设非奇异 n 级反馈函数的多项式表示为 $f=x_1+f_0(x_2,\cdots,x_n)$，若分别用 Df、Rf 和 RDf 表示以 $D(Gf)$、$R(Gf)$ 和 $RD(Gf)$ 为状态图的 n 级移位寄存器反馈反馈函数，则

$$Df=x_1+f_0(\overline{x}_2,\overline{x}_3,\leqslant,\overline{x}_n)$$

$$Rf=x_1+f_0(x_n,x_{n-1},\leqslant,x_2)$$

$$RDf=x_1+f_0(\overline{x}_n,\overline{x}_{n-1},\leqslant,\overline{x}_2)$$

1946 年，De Bruijn 从图论的角度证明了产生 *M* 序列的非线性移位寄存器的个数等于 $\frac{2^{2^{n-1}}}{2^n}=2^{2^{n-1}-n}$，而非奇异移位寄存器的个数恰好等于 $2^{2^{n-1}}$。但是至今人们都无法证明 *M* 序列的非线性移位寄存器以 2^n 的长度划分了整个非奇异移位寄存器，即猜想若将整个非奇异移位寄存器对应的反馈函数看作一个群，而 *M* 序列的反馈函数可以看作是个数为 2^n 的陪集的代表元。20 世纪 80 年代，高鸿勋[16]在以圈剪接筛法的基础上提出了一个非奇异反馈函数为 *M* 序列反馈函数的充要条件，但对于生成全部 $n(n\geqslant 5)$ 级 *M* 序列来讲没有实际意义。

本文直接引用文献[15]中关于 *M* 序列反馈函数多项式表示的一个必要条件来说明随机寻找到一个 *M* 序列反馈函数的数据复杂度。

引理 1[15]　在 *M* 序列反馈函数 f_0 的多项式表示中，有以下性质。

1) 最高次项 $x_2\cdots x_n$ 这一项一定出现。

2) 项数一定是奇数。

3) 1 这一项一定出现。

4) 一次项 $x_2,\cdots,x_n$ 不能全部出现。

由于考虑将 1 和 $x_2\cdots x_n$ 这 2 项排除，则剩余可能出现的项的个数即为 $2^{n-1}-2$。在此基础上将 $2^{n-1}-2$ 种可能出现的项进行一个分类，即定义 $A_i(1\leqslant i\leqslant n-2)$，则可能产生 *M* 序列反馈函数的个数为 $2^{2^{n-1}-2}$。又因为项数一定是奇数，则可能产生 *M* 序列的反馈函数的个数可以降到 $2^{2^{n-1}-3}$。如果从线性项 $x_2,\cdots,x_n$ 不能全部出现的角度考虑，则可能产生 *M* 序列反馈函数的个数为 $\frac{2^{2^{n-1}-2}-2^{2^{n-1}-2-n-1}}{2}$。假设 *M* 序列的反馈函数服从均匀分布，则实际利用引理 1 寻找到一个 *M* 序列反馈函数的数据复杂度约为 $O(2^{n-3})$。

文献[15]给出了利用对偶变换 D、对称变换 R 和组合变换 RD 构造 *M* 序列的结论。如引理 2 所示。

引理 2[15]　f 是 *M* 序列的反馈函数，则 Df、Rf 和 RDf 也是 *M* 序列的反馈函数。当 $n\geqslant 3$ 时，$f\neq Df$、$f\neq Rf$；当 n 为偶数时，f、Df、Rf、RDf 这 4 个函数两两互异。

由于在实际应用中并不需要生成全部的 *M* 序列反馈函数，更多的时候是需要生成具有某些构造特点的多项式表示的反馈函数。本文的工作即是利用由 *m* 序列构造 *M* 序列反馈函数的结构特性，经上述 3 种函数变换得到一类 *M* 序列反馈函数多项式表示的快速构造方法，为了更好地说明对偶变换 D、对称变换 R 以及组合变换 RD 在构造 *M* 序列反馈函数中的应用，接下来，给出 2 个关于 *m* 序列的结论。

3　由函数变换证明的 2 个结论

本文由函数变换发现了 *m* 序列个数及其特征多项式的一些性质，并从另外一个角度证明了如下

结论。

引理 3[17] 当 $n\geqslant 3$，$\dfrac{\phi(2^n-1)}{n}$ 总为偶数。

证明 当 $n\geqslant 3$ 时，由引理 2 知，Rf 形成的必然是一条新的 m 序列，则 $f\neq Rf$，因此，由 Rf 形成的特征多项式必然异于 f 的本原多项式，而二元域上的本原多项式的总数为 $\dfrac{\phi(2^n-1)}{n}$，因此，当 $n\geqslant 3$，$\dfrac{\phi(2^n-1)}{n}$ 必然为偶数，证毕。

定理 2 当 n 为偶数且 $n\geqslant 3$ 时，不存在形式为 $x^n+x^{\frac{n}{2}}+1$ 的本原三项式。

证明 当 n 为偶数且 $n\geqslant 3$ 时，对于特征多项式为 $x^n+x^{\frac{n}{2}}+1$ 的 m 序列，其反馈函数的形式为 $f=x_1+x_{\frac{n}{2}+1}$。由定理 1 可知，$Rf=f$，但是由引理 2 可知，Rf 形成的必然是一条新的 m 序列，因此，Rf、f 两者的特征多项式不相等，这与 $Rf=f$ 矛盾，则此时不存在形式为 $x^n+x^{\frac{n}{2}}+1$ 的本原三项式，证毕。

4 函数变换及函数派生在构造 *M* 序列反馈函数中的应用

4.1 函数变换在构造 *M* 序列反馈函数中的应用

在实际构造 M 序列的过程中，人们很自然地考虑从 m 序列出发，即考虑在 m 序列长度为 $n-1$ 的 0 游程中添加一个 0 得到 M 序列，这也符合对 M 序列的游程统计。这种情况构造的 M 序列反馈函数其实是在 m 序列的反馈函数表达式中添加一个小项 $x_2^0\cdots x_n^0$ [15]。当然将小项表示转化为多项式表示中，发现得到的 M 序列反馈函数满足引理 1 的性质，考虑该 M 序列反馈函数的对偶函数时，其对偶函数也应该为 M 序列的反馈函数，据此给出了一类 M 序列反馈函数 f 快速构造的多项式表示的形式，即形式 1。

形式 1 在 m 序列的反馈函数 q 的基础上添加 $1,x_2\cdots x_n$ 这 2 项，即

$$f=q+1+x_2\cdots x_n$$

容易看出，具有形式 1 的多项式表示的反馈函数 f 满足引理 1，从而可以推出 m 序列的项数为偶数项，否则与 f 中出现 1 这一项相矛盾。

同时考虑对称函数 Rf 和 RDf，当 $n\geqslant 3$，由 f 对称所形成的必然是新的一条 M 序列，所以势必由 f 可以得到一个新的满足 M 序列的反馈函数 Rf，观察其结构可知，仍然是在 m 序列的反馈函数上添加 $1,x_2\cdots x_n$ 这 2 项，其与引理 3 的结论是相对应的，同理可得 RDf 与 Df 具有相同结构。据此，可以快速构造 $\dfrac{2\phi(2^n-1)}{n}$ 个 M 序列反馈函数。

如果本文将 $x_1,1,x_2\cdots x_n$ 这 3 项单列，指出任意由形式 1 构造的 M 序列反馈函数的对偶函数 Df 具有定理 3 的形式。

定理 3 任意由形式 1 构造的 M 序列反馈函数 f 的对偶函数 Df 具有以下形式。

1) 包含 $x_1,1,x_2\cdots x_n$ 这 3 项。

2) 包含 f 在集合 $A_i(1\leqslant i\leqslant n-2)$ 中所有未出现的项。

证明 由于 $f=q+1+x_2\cdots x_n=x_1+f_0(x_2,\cdots,x_n)$，则由定理 1 知，$Df$ 包含 $x_2^0\cdots x_n^0$ 项，其多项式展开式中包含 $f_0(x_2,\cdots,x_n)$ 中所有 $i(1\leqslant i\leqslant n-2)$ 次项的集合为 A_i 以及 $1,x_2\cdots x_n$。

由于 $f_0(x_2,\cdots,x_n)$ 中的线性项共有奇数项，故 Df 一定包含 $x_1,1,x_2\cdots x_n$ 这 3 项，且其余项为 f 在集合 $A_i(1\leqslant i\leqslant n-2)$ 中所有未出现的项，故式(1)和式(2)得证。证毕。

为方便理解，本文给出定理 3 的一个实例。

例 1 当 $n=4$ 时，$f=x_1+1+x_2x_3x_4+x_4$，下面给出 Df。

由于原函数在 $A_i(1\leqslant i\leqslant 2)$ 中未出现的项有 $x_2,x_3,x_2x_3,x_2x_4,x_3x_4$，因此

$$Df=x_1+1+x_2x_3x_4+x_2+x_3+x_2x_3+x_2x_4+x_3x_4$$

同时，发现 $Df+f$ 中的函数项即是集合 $A_i(1\leqslant i\leqslant n-2)$ 中所有出现的 $2^{n-1}-2$ 项，因此，可以立即得到推论 1。

推论 1 对于任意由形式 1 构造的 M 序列反馈函数 f 和 Df，g 为任意 M 序列反馈函数，则 $f+Df+g$ 具有如下形式。

1) 包含 $x_1,1,x_2\cdots x_n$ 这 3 项。

2) 包含 g 在集合 $A_i(1\leqslant i\leqslant n-2)$ 中所有未出现的项。

4.2 函数派生在 *M* 构造序列反馈函数中的应用

根据之前对基于由 m 序列构造 M 序列的分析可知，如果仅从 A_i 选择奇数项，只能是形式 1 构造出的 $\dfrac{\phi(2^n-1)}{n}$ 个 M 序列反馈函数 f，于是，设想以

此为基础加上若干偶数项可以构造新的 *M* 序列反馈函数。本先给出文献[15]中一个关于函数派生的结论，文献[15]中的证明比较烦琐，下面，利用文献[18]中状态图的连线与交点的赋值定义给出简化证明。

定理 4[15]　若 f 是 n 级 *M* 序列的反馈函数，则以下 2 个式子也是 *M* 序列的反馈函数。

$$f + x_2^1 x_3^1 \cdots x_{n-1}^1 x_n^0 + x_2^0 x_3^1 \cdots x_{n-1}^1 x_n^1 \tag{1}$$

$$f + x_2^0 x_3^0 \cdots x_{n-1}^0 x_n^1 + x_2^1 x_3^0 \cdots x_{n-1}^0 x_n^0 \tag{2}$$

证明　文献[18]指出，对于 *Gf* 状态图，任一 2 对共轭状态的连线的交点的赋值和指的是加上 2 个 $n-1$ 维的小项 $x_2^{a_2} x_3^{a_3} \cdots x_n^{a_n}$ 和 $x_2^{b_2} x_3^{b_3} \cdots x_n^{b_n}$，其中，$(a_1, a_2, \cdots, a_n)$ 与 $(\overline{a_1}, a_2, \cdots, a_n)$，$(b_1, b_2, \cdots, b_n)$ 与 $(\overline{b_1}, b_2, \cdots, b_n)$ 分别是2对共轭状态。由圈剪接的思想[15]可知，f 加上赋值和也是 *M* 序列的反馈函数。而 2 对共轭状态的连线要相交，必然在 *Gf* 中一对共轭状态之间有另一对共轭状态的其中一个。对于状态 $(0,0,1,\cdots,1,1)$ 来说，若其后继状态为 $(0,1,1,\cdots,1,0)$，由于 $((0,1,1,\cdots,1),(1,1,\cdots,1,1))$ 这条弧必然存在，则状态 $(0,1,1,\cdots,1)$ 的先导必然为 $(1,0,1,1,\cdots,1)$，且同时 $(1,1,\cdots,1,1)$ 的后继必然为 $(1,1,\cdots,1,0)$，故形成这样一条长弧 $((0,0,1,\cdots,1,1), (0,1,1,\cdots,1,0),\cdots,(1,0,1,1,\cdots,1), (0,1,1,\cdots,1),(1,1,\cdots,1,1), (1,1,\cdots,1,0))$，则说明共轭状态 $(0,0,1,\cdots,1,1)$, $(1,0,1,1,\cdots,1)$ 和 $(0,1,1,\cdots,1,0)$, $(1,1,\cdots,1,0)$ 的连线必然相交；若其后继状态为 $(0,1,1,\cdots,1)$，则状态 $(0,1,1,\cdots,1,0)$ 的先导必然为 $(1,0,1,1,\cdots,1)$，故形成这样一条长弧 $((1,0,1,1,\cdots,1), (0,1,1,\cdots,1,0),\cdots, (0,0,1,\cdots,1,1), (0,1,1,\cdots,1),(1,1,\cdots,1,1), (1,1,\cdots,1,0))$，则说明共轭状态 $(0,0,1,\cdots,1,1)$, $(1,0,1,1,\cdots,1)$ 和 $(0,1,1,\cdots,1,0)$, $(1,1,\cdots,1,0)$ 的连线必然相交。综上可知 $f + x_2^1 x_3^1 \cdots x_{n-1}^1 x_n^0 + x_2^0 x_3^1 \cdots x_{n-1}^1 x_n^1$ 也是 *M* 序列的反馈函数。同理可证 $f + x_2^0 x_3^0 \cdots x_{n-1}^0 x_n^1 + x_2^1 x_3^0 \cdots x_{n-1}^0 x_n^0$ 也是 *M* 序列的反馈函数，证毕。

下面，利用定理 4 的结论，给出了新的 *M* 序列反馈函数的 4 种形式 f', Df', f'', Df''。

本文首先利用定理 4 的式(1)，即 f 是任意以形式 1 构造的 *M* 序列反馈函数，则 $f' = f + x_2^1 x_3^1 \cdots x_{n-1}^1 x_n^0 + x_2^0 x_3^1 \cdots x_{n-1}^1 x_n^1 = f + x_2 x_3 \cdots x_{n-1} + x_3 \cdots x_{n-1} x_n$ 也是 *M* 序列反馈函数。

由此，可将 f' 描述成以下多项式表示的形式，即形式 2。

形式 2　在形式 1 生成的 f 基础上添加 $x_2 x_3 \cdots x_{n-1}, x_3 \cdots x_{n-1} x_n$ 这 2 项，即

$$f' = q + 1 + x_2 \cdots x_n + x_2 x_3 \cdots x_{n-1} + x_3 \cdots x_{n-1} x_n$$

而此时的 f' 正好满足从 A_1 选择奇数项，A_{n-2} 选择偶数项。同时，考虑 Rf' 和 Df'，易知 Rf' 还是属于与 f' 相同的一类 *M* 序列反馈函数，而

$$\begin{aligned} Df' &= Df + x_2^0 x_3^0 \cdots x_{n-1}^0 + x_3^0 \cdots x_{n-1}^0 x_n^0 \\ &= f + 1 + x_2^1 x_3^1 \cdots x_{n-1}^1 x_n^1 + x_2^0 x_3^0 \cdots \\ &\quad x_{n-1}^0 x_n^0 + x_2^0 x_3^0 \cdots x_{n-1}^0 + x_3^0 \cdots x_{n-1}^0 x_n^0 \\ &= f + 1 + x_2^1 x_3^1 \cdots x_{n-1}^1 x_n^1 + x_2^1 x_3^0 \cdots x_{n-1}^0 x_n^1 + x_3^0 \cdots x_{n-1}^0 \end{aligned}$$

因此，Df' 还可以描述成以下多项式表示的形式，即形式 3。

形式 3　在 *m* 序列的反馈函数的基础上添加 $(1 + x_2^1 x_n^1) x_3^0 \cdots x_{n-1}^0$，转化成多项式表示后，即在形式 1 生成的 f 基础上添加 $A_j (1 \leqslant j \leqslant n-2)$ 中排除

$$x_2 x_{i_1} \cdots x_{i_{j-1}}, x_{i_1} \cdots x_{i_{j-1}} x_n (i_{t(1 \leqslant t \leqslant j-1)} \neq 2, n \text{且} x_{i_0} = 1)$$

后剩余的项。

易知，当 $n > 3$ 时，Df' 与 f, Df 不同。据此可以快速构造 $\dfrac{4\phi(2^n - 1)}{n}$ 个 *M* 序列反馈函数，分别是 f, Df, f', Df'。

接下来，再次利用定理 4 的式(2)，即 f 是 *M* 序列反馈函数，则

$$\begin{aligned} f'' &= f + x_2^0 x_3^0 \cdots x_{n-1}^0 x_n^1 + x_2^1 x_3^0 \cdots x_{n-1}^0 x_n^0 \\ &= Df + 1 + x_2^1 x_3^1 \cdots x_{n-1}^1 x_n^1 + x_2^0 x_3^0 \cdots \\ &\quad x_{n-1}^0 x_n^0 + x_2^0 x_3^0 \cdots x_{n-1}^0 x_n^1 + x_2^1 x_3^0 \cdots x_{n-1}^0 x_n^0 \\ &= f + Df + Df' \end{aligned}$$

也是 *M* 序列反馈函数。若考虑此时的 Rf'' 和 Df''，则由 f'' 的结构可知，Rf'' 还是属于与 f'' 相同的一类 *M* 序列反馈函数。当 $n \geqslant 5$ 时，$Df'' = f + Df + f'$ 以及 f'' 就与 f, Df, f', Df' 不同。此时根据推论 1，f'', Df'' 还可以描述成以下多项式表示的形式，即形式 4。

形式 4　除了有公共的 $x_1, 1, x_2 \cdots x_n$ 这 3 项外，其余项为 Df', f' 在集合 $A_i (1 \leqslant i \leqslant n-2)$ 中所有未出现的项。

据此，可以快速构造 $\dfrac{6\phi(2^n - 1)}{n}$ 个 *M* 序列反馈函数，分别是 $f, Df, f', Df', f'', Df''$。

如果考虑 $f'=f+x_2x_3\cdots x_{n-1}+x_3\cdots x_{n-1}x_n$ 中 f 是另外的 5 种 M 序列反馈函数，即 Df,f',Df',f'',Df''。由于只添加了 4 个不同的小项，且其中 2 对小项（或称为赋值和[18]）互为对偶，设 $x_2^1x_3^1\cdots x_{n-1}^1x_n^0+x_2^0x_3^1\cdots x_{n-1}^1x_n^1$ 为 X_1，$x_2^0x_3^0\cdots x_{n-1}^0x_n^1+x_2^1x_3^0\cdots x_{n-1}^0x_n^0$ 为 X_2，则 $X_2=DX_1$。所以 $Df'=D(f+X_1)=Df+X_2$，以及 $Df''=Df+X_1$，因此，当 $n\geqslant 5$ 时，还可以生成 $f+X_1+X_2$，$Df+X_1+X_2$ 共 2 类 M 序列反馈函数。

综上所述，可以快速构造 $\frac{8\phi(2^n-1)}{n}$ 个 M 序列反馈函数，分别是

$$f,Df,f+X_1,f+X_2,f+X_1+X_2,$$
$$Df+X_1,Df+X_2,Df+X_1+X_2$$

对于这类 M 序列反馈函数考虑函数之间相等的情况时，仅可能是 $f+X_2=Df+X_1$ 与 $f+X_1=Df+X_2$，此时的 f 与 Df 的小项表示必然是仅有一项不同，且不同的项为 X_2 和 X_1，剩余的项必然是成对的互为对偶的项。因此，考虑到函数之间相等的情况是可能存在的，但出现的概率和个数较少，所以实际上这类方法可以构造约 $\frac{8\phi(2^n-1)}{n}$ 个 M 序列反馈函数。最后，可以用图 1 来总结这类快速构造方法生成的 M 序列反馈函数，其中，$X_1=x_2^1x_3^1\cdots x_{n-1}^1x_n^0+x_2^0x_3^1\cdots x_{n-1}^1x_n^1$，$X_2=x_2^0x_3^0\cdots x_{n-1}^0x_n^1+x_2^1x_3^0\cdots x_{n-1}^0x_n^0$。

4.3 一类 *M* 序列反馈函数的快速构造算法

为了说明这类 M 序列的构造方法可以在实际中快速生成以多项式表示的反馈函数，本文给出算法形式，如算法 1 所示。该算法分为离线和在线阶段，并且为了存储以多项式表示的反馈函数，将 $A_i(0\leqslant i\leqslant n-1)$ 中的每一元素对应到 $n-1$ 维的二元数组向量构成的集合

$$\{(a_1,a_2,\cdots,a_{n-1})\,|\,\forall j:1\leqslant j\leqslant n-1,a_j\in F_2,$$
$$w(a_1,a_2,\cdots,a_{n-1})=i\}$$

例如，常数 1 对应向量 $(0,\cdots,0)$，x_2 对应向量 $(1,0,\cdots,0)$，$x_2\cdots x_n$ 对应向量 $(1,\cdots,1)$，C_BA 表示集合 A 在 B 中的补集。

算法 1 一类 M 序列反馈函数的快速构造算法

离线阶段

对于给定级数 $n(n\geqslant 5)$ 时，以向量形式存储 $A_i(0\leqslant i\leqslant n-1)$ 中所有元素，并记全体 $n-1$ 维的二元向量集合为 U。对于给定的 m 序列的反馈函数，给出其线性项在 A_1 中的向量集合 Q，则在在线阶段只需求出 M 序列反馈函数中 f_0 的对应向量集合，将集合中元素相加再加上 x_1，即可得到 M 序列反馈函数。

在线阶段

Step1 输入 n 级 m 序列的反馈函数中线性项的向量集合 Q。

Step2 以形式 1 表示的 M 序列反馈函数中 f_0 的对应向量集合 F_0 为

$$F_0=Q\cup\{(0,\cdots,0),(1,\cdots,1)\}$$

Step3 以定理 3 表示的 M 序列反馈函数中 Df_0 的对应向量集合 DF_0 为

$$DF_0=C_UQ$$

Step4 以形式 2 表示的 M 序列反馈函数中 f_0' 的对应向量集合 F_0' 为

$$F_0'=F_0\cup\{(0,1,\cdots,1),(1,\cdots,1,0)\}$$

Step5 以形式 3 表示的 M 序列反馈函数中 Df_0' 的对应向量集合 DF_0' 为

$$DF_0'=F_0'\cup\bigcup_{j=1}^{n-3}C_{A_j}\{(1,a_2,\cdots,a_{n-2},0|w(a_2,\cdots,a_{n-2})=j-1),$$
$$(0,a_2,\cdots,a_{n-2},1|w(a_2,\cdots,a_{n-2})=j-1)\}$$

Step6 以形式 4 表示的 M 序列反馈函数中 f_0'',Df_0'' 的对应向量集合 F_0'',DF_0'' 为

$$F_0''=C_UDF_0'\cup\{(0,\cdots,0),(1,\cdots,1)\}$$
$$DF_0''=C_UF_0'\cup\{(0,\cdots,0),(1,\cdots,1)\}$$

Step7 M 序列反馈函数中 $f_0+X_1+X_2$，$Df_0+X_1+X_2$ 的对应向量集合为

$$F_0+X_1+X_2=F_0''\cup\{(0,1,\cdots,1),(1,\cdots,1,0)\}$$
$$DF_0+X_1+X_2=DF_0'\cup\{(0,1,\cdots,1),(1,\cdots,1,0)\}$$

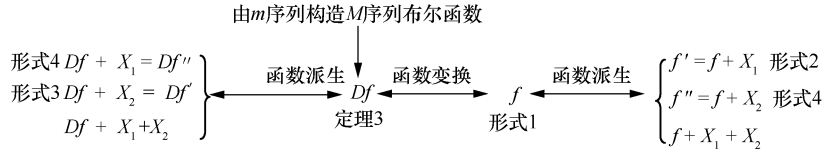


图 1 一类 M 序列反馈函数的快速构造算法

Step8　输出 $F_0, DF_0, F_0', DF_0', F_0'', DF_0'', F_0+X_1+X_2, DF_0+X_1+X_2$，并返回 Step1，输入下一个 m 序列的反馈函数中线性项的向量集合 Q。

分析该算法可知，由于离线阶段存储了所有多项式以次数为序的项数集合，存储复杂度即为 $O(2^{n-1})$，则在线阶段，对于求一个给定集合在有序集合中的补集，只需要遍历输出该有序集合的部分元素即可，因此，时间复杂度为 $O(2^{n-1})$。对比直接利用“并圈法”得到的以小项表示的 M 序列反馈函数，在其转化成多项式表示上所需要的时间复杂度将大大降低。同时，本文也是首次给出以多项式表示的 M 序列反馈函数的构造算法，下面，本文将简要分析该算法给出的这类 M 序列反馈函数的重量性质。

5　新的 *M* 序列反馈函数的重量性质

由于 M 序列反馈函数的结构总可以表示成 $f=x_1+f_0(x_2,\cdots,x_n)$，因此，$M$ 序列反馈函数的重量指的是 f_0 的重量或 f_0 小项表示的项数，即为 $w(f_0)$。在文献[15]给出了 M 序列小项表示的反馈函数的一个必要条件，有以下结论。

定理 5[15]　当 $n\geqslant 3$ 时，对于 $Z(n)-1$ 与 $2^{n-1}-Z^*(n)+1$ 之间的一切奇数都有以这奇数为重量的 M 序列反馈函数存在，其中，$Z(n)=\frac{1}{n}\sum_{d|n}\phi(d)2^{\frac{n}{d}}, Z^*(n)=\frac{1}{2}Z(n)-\frac{1}{2n}\sum_{2d|n}\phi(d)2^{\frac{n}{2d}}$。

根据定理 5，实际上，本文限制了 $w(f_0)$ 的取值，并且 $w(f_0)$ 的取值是 M 序列反馈函数在实际应用中的重要参考指标，因此，接下来，考虑快速构造方法生成的 M 序列反馈函数的重量 $w(f_0)$。

首先，可以合理限定 m 序列的反馈函数为二项式，即表示为 x_1+x_i，则通过形式 1 生成的 M 序列反馈函数 $f_0=x_i+1+x_2\cdots x_n$ 转化成小项表示后，其项数为 $w(f_0)=2^{n-2}+1$。当 n 较大时，$Z(n)$ 和 $Z^*(n)$ 都远远小于 2^{n-2}，因此，$w(f_0)$ 的取值大概在重量区间的中间。由于函数变换不改变 $w(f_0)$ 的取值，以及这种函数派生方式重量的增减幅度为 2 或 4，因此，新的 M 序列反馈函数 $w(f_0)$ 为以下取值之一：$2^{n-2}-3$、$2^{n-2}-1$、$2^{n-2}+1$、$2^{n-2}+3$、$2^{n-2}+5$。

其次，考虑 m 序列的反馈函数为四项式，即在二项式的基础上添加 2 个线性项。由于 $w(f_0)$ 从另一个角度可以看成 $f_0=1$ 的 $n-1$ 维向量个数，新添加的 2 个线性项的取值（即该线性项等于 0 或 1）使 f_0=1 的情况个数与原有二项式比较不变，因此，此时 $n-1$ 维向量满足 $f_0=1$ 的个数不变，即此时通过形式 1 生成的 M 序列反馈函数的 $w(f_0)$ 取值为 $2^{n-2}+1$。以此类推，通过形式 1 生成的 M 序列反馈函数 $w(f_0)$ 取值为 $2^{n-2}+1$[19]，此时，新的 M 序列反馈函数 $w(f_0)$ 为以下取值之一：$2^{n-2}-3$、$2^{n-2}-1$、$2^{n-2}+1$、$2^{n-2}+3$、$2^{n-2}+5$。

综上所述，可以得到以下结论。

结论　M 序列反馈函数 f（其中，f 为图 1 所示的 8 类 M 序列反馈函数）的重量 $w(f_0)$ 的取值必然在以下集合中：$\{2^{n-2}-3, 2^{n-2}-1, 2^{n-2}+1, 2^{n-2}+3, 2^{n-2}+5\}$。

6　结束语

由 m 序列构造 M 序列反馈函数一直以来是实际应用中常见的构造方法，本文充分利用 m 序列构造 M 序列反馈函数的结构特性，结合函数变换以及函数派生，得到了一类个数较多且多项式表示和小项表示的重量都可以确定的 M 序列反馈函数。这种构造丰富了由 m 序列构造 M 序列反馈函数的方法，并且给出了其他项数和重量条件的反馈函数，克服了单一由 m 序列构造 M 序列反馈函数的构造缺陷，在实际应用中有更多可供选择的以多项式表示的 M 序列反馈函数。由于在构造过程中，多项式表示的方法还过于烦琐，是否还存在类似形式 1 的项数较少的 M 序列反馈函数的构造方法，是下一步研究的目标。

参考文献：

[1] 中国科学院数学研究所代数组. 关于 *M* 序列反馈函数的构造方法[J]. 应用数学学报, 1977, 4:11-22.
Institute of Mathematics, Chinese Academy of Sciences. The methods of constructing *M*-sequence feedback functions[J]. Acta Mathematicae Applicatae Sinica, 1977, 4:11-22.

[2] 康庆德. GF(2)上 *M* 序列的构造方法[J]. 通信学报, 1983(4): 2-10.
KANG Q D. The methods of constructing *M*-sequence over GF(2)[J]. Journal on Communications, 1983(4): 2-10.

[3] 熊荣华. *M* 序列反馈函数的构造方法 I [J]. 应用数学学报, 1986(2): 227-236.
XIONG R H. On methods of constructing the feedback functions of *M* sequences I[J]. Acta Mathematicae Applicatae Sinica, 1986(2): 227-236.

[4] 朱士信. *M* 序列反馈函数的派生方法[J]. 合肥工业大学学报(自然科学版), 1991(4): 138-144.
ZHU S X. Methods for the derivation of feedback functions of *M* se-

quences[J]. Journal of Hefei University of Technology, 1991(4): 138-144.

[5] 章照止, 罗乔林. 产生*M*序列的一个递推算法[J]. 系统科学与数学, 1987(4): 335-343.
ZHANG Z Z, LUO Q L. A recursive algorithm for the generation of De Bruijn sequences[J]. Journal of System Science and Mathematical Science Chinese Series, 1987(4): 335-343.

[6] SAWADA J, WILLIAMS A, WONG D. A surprisingly simple de Bruijn sequence construction[J]. Discrete Mathematics, 2016, 339(1): 127-131.

[7] ABBAS A. Stretching De Bruijn sequences[J]. Designs Codes & Cryptography, 2017, 85(2):381-394.

[8] 高杨, 刘松华, 王中孝. 一种基于“编织法”的 De Bruijn 序列构造算法[J]. 电子学报, 2018, 46(1): 48-54.
GAO Y, LIU S H, WANG Z X. A De Bruijn sequence construction algorithm based on “interleaving” construction method[J]. Acta Electronica Sinica, 2018, 46(1): 48-54.

[9] LI C, ZENG X, LI C, et al. Construction of De Bruijn sequences from LFSRs with reducible characteristic polynomials[J]. IEEE Transactions on Information Theory, 2015, 62(1):610-624.

[10] CHANG Z, EZERMAN M F, LING S, et al. Construction of De Bruijn sequences from product of two irreducible polynomials[J]. Cryptography & Communications, 2018, 10(2):251-275.

[11] LI M, JIANG Y, LIN D. The adjacency graphs of some feedback shift registers[J]. Designs Codes & Cryptography, 2016, 82(3):1-19.

[12] LI M, LIN D. The adjacency graphs of LFSRs with primitive-like characteristic polynomials[J]. IEEE Transactions on Information Theory, 2017, 63(2):1325-1335.

[13] LI M, LIN D. De Bruijn sequences, adjacency graphs and cyclotomy[J]. IEEE Transactions on Information Theory, 2017, PP(99): 1.

[14] DONG J, PEI D. Construction for De Bruijn sequences with large stage[J]. Designs Codes & Cryptography, 2016:1-16.

[15] 万哲先, 代宗铎, 刘木兰, 等. 非线性移位寄存器[M]. 北京:科学出版社, 1978.
WAN Z X, DAY Z D, LIU M L, et al. Non-linear shift register[M]. Beijing: Science Press, 1978.

[16] 高鸿勋. 非奇函数是 *M* 序列反馈函数的一个充要条件[J]. 应用数学学报, 1984(1): 9-10.
GAO H X. A necessary and sufficient condition for nonsingular function to be feedback function of *M*-sequences[J]. Acta Mathematicae Applicatae Sinica, 1984(1): 9-10.

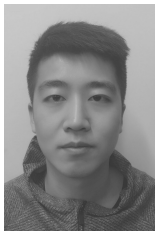
[17] 万哲先. 代数与编码[M]. 北京:科学出版社, 1976.
WAN Z X. Algebra and coding[M]. Beijing: Science Press, 1976.

[18] 高鸿勋. 求全部*n*级*M*序列及其反馈函数的一个方法与证明[J]. 应用数学学报, 1979(4): 316-324.
GAO H X. A method and proof of finding all *n*-stage of *M*-sequences and their feedback functions[J]. Acta Mathematicae Applicatae Sinica, 1979(4): 316-324.

[19] 许军进, 尹克震. *M* 序列反馈函数重量与项数的分析[J]. 杭州电子科技大学学报, 2007(1): 24-28.
XU J J, YI K Z. Analysis on weights and terms of feedback functions for Sequences[J]. Journal of Hangzhou Dianzi University, 2007(1): 24-28.

[作者简介]

关杰（1974-），女，河南郑州人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为序列密码。



周琮伟（1994-），男，四川眉山人，解放军信息工程大学硕士生，主要研究方向为序列密码。