DOI：10.13718/j.cnki.xdzk.2017.07.017

q 进制反射 Gray 码的几个注记[①]

张　帅[1]，　瞿云云[2]，　包小敏[1]，　黄华伟[2]

1. 西南大学 数学与统计学院，重庆 400715；2. 贵州师范大学 数学科学学院，贵阳 550001

摘要：对整数 $q \geqslant 2$ 给出一个计算 q 进制反射 Gray 码中码字位置的计算公式，二进制反射 Gray 码中码字的位置的计算公式是此公式的一个特例. 另外介绍了两种各具优势的生成 q 进制反射 Gray 码的算法：其中一个算法可生成 q 进制反射 Gray 码中任意位置上的码字；另一个算法可逐个生成 q 进制反射 Gray 码中的码字.

关　键　词：反射 Gray 码；位置；q-进制；自然码

中图分类号：O211.4　　**文献标志码：A**　　**文章编号：**1673-9868(2017)07-0110-05

反射 Gray 码是 1880 年由法国工程师 Baudot 发明的一种编码，因 Gray 于 1953 年申请专利而得名[1]. 反射 Gray 码属于可靠性编码，是一种错误最小化的编码，它大大减少了由一个状态到下一个状态时电路中的混淆. 由于这种编码相邻的两个码之间只有一位不同，因而在模—数转换中，当模拟量发生微小变化而可能引起数字量发生变化时，反射 Gray 码仅改变一位，这与其它编码同时改变两位和多位的情况相比更为可靠，允许代码电路能以较少的错误在较高的速度下工作.

由于反射 Gray 码是一种错误最小化的可靠性编码，因此在通信安全、数字模拟信号、编码理论研究、密码研究等领域有相当广泛的应用. 例如在文献[2]中提出的数字图像置乱技术的理论基础就是反射 Gray 码. 在过去的几十年里对反射 Gray 码的研究从未停止过[3-10]，生成反射 Gray 码的算法也有很多，但对于非二进制来说，由于反射 Gray 码自身的反射性使得这些算法错综复杂，实施起来比较困难. 为了使生成反射 Gray 码的算法更加条理化，实施起来更加方便，本文在前人的基础上给出一种可逐个生成反射 Gray 码中码字的算法.

虽然在文献[3]中有论述自然码与反射 Gray 码之间的关系，但论述较为复杂，也未对所述关系进行证明，而且没有将反射 Gray 码中具体码字的位置关系公式化，更没有给出具体的生成反射 Gray 码的算法. 本文继续研究反射 Gray 码与自然码之间的关系，给出一个可直接计算反射 Gray 码中任意码字位置的公式以及证明，进而给出另一种可直接生成反射 Gray 码中任意位置上的码字的算法.

1　反射 Gray 码背景知识

长度为 n 的 q 进制 Gray 码(称为 q 进制 n 阶 Gray 码)是所有 q 进制 n 元组的一种特殊排列，使得其中任意两个相邻的 n 元组只有一个位置上的值不同且不同位置上的值的差的绝对值为 1. 反射 Gray 码是一种特殊的 Gray 码，其归纳定义如下：

定义 1　q 进制 1 阶 Gray 码为 $G_q(1) = (0, 1 \cdots q-1)^T$. 对 $n > 1$，若 q 进制 $n-1$ 阶反射 Gray 码 $G_q(n-1)$ 已经定义，则 q 进制 n 阶反射 Gray 码为

---

① 收稿日期：2016-04-29

基金项目：国家自然科学基金项目(61462016)；贵州省科学技术基金项目(黔科合 J 字[2014]2125 号)；贵州师范大学博士启动项目(0514021)；贵州省教育厅青年科技人才成长项目(黔教合 KY 字[2016]130).

作者简介：张　帅(1991-)，男，河南安阳人，硕士研究生，主要从事编码理论和密码学的研究.

通信作者：包小敏，博士，教授.

$$G_q(n)=\begin{cases}0 & G_q(n-1)\\ 1 & G_q'(n-1)\\ 2 & G_q(n-1)\\ \cdots & \cdots\\ q-1 & \overline{G}_q(n-1)\end{cases}$$

其中 $G_q'(n-1)$ 是 $G_q(n-1)$ 的反向排列，$\overline{G}_q'(n-i)$ 是 $\overline{G}_q(n-i)$ 的反向排列，而

$$\overline{G}_q(n-1)=\begin{cases}G_q(n-1) & 若\ 2\mid q-1\\ G'_q(n-1) & 若\ 2\nmid q-1\end{cases}$$

长度为 n 的 q 进制自然码(称为 q 进制 n 阶自然码，记为 $N_q(n)$)是所有长度为 n 的 q 进制数的一个排列，其对应的十进制数分别为 $0,1,\cdots,q^n-1$.

给定所有 q 进制 n 元组的一个排列，排列的序号从 0 开始. 序号为 i 的码字也称为第 i 个位置的码字. 为方便起见，下面我们总假设讨论的 n 元组的排列是写成一列的，一个 n 元组一行.

2 一个确定 $G_q(n)$ 中码字位置的公式

下面我们给出一个确定反射 Gray 码 $G_q(n)$ 中任一码字位置的计算公式.

定理 1 q 进制 n 元组 $g_{n-1}g_{n-2}\cdots g_1g_0$ 在反射 Gray 码序中的位置 k 可如下确定：令 $a_{n-1}=g_{n-1}$，对 $i=0,1,2,\cdots,n-2$，令

$$a_i=\begin{cases}g_i & 如果\ 2\mid \sum\limits_{j=i+1}^{n-1}g_j\\ q-1-g_i & 如果\ 2\nmid \sum\limits_{j=i+1}^{n-1}g_j\end{cases}$$

则

$$k=a_{n-1}q^{n-1}+a_{n-2}q^{n-2}+\cdots+a_1q+a_0$$

例 1 以 $G_3(3)$ 为例验证定理 1 中公式的正确性，其中 $G_3(3)$ 中所有码字排列如下：

000	001	002	012	011	010	020	021	022
122	121	120	110	111	112	102	101	100
200	201	202	212	211	210	220	221	222

对 $G_3(3)$ 中的码字 $\boldsymbol{g}=121$，按定理 1 中的公式有：$a_2=g_2=1$；因为 $g_2=1$ 为奇数，所以 $a_1=3-1-g_1=3-1-2=0$；而 $g_2+g_1=3$ 为奇数，故 $a_0=3-1-g_0=3-1-1=1$. 由定理 1，$\boldsymbol{g}=121$ 在 $G_3(3)$ 中的位置为 $k=a_2 3^2+a_1 3^1+a_0=3^2+1=10$，与实际情况相符.

在证明定理 1 之前我们先给一个引理.

引理 1 在 $G_q(n)$ 中与任一码字 $\boldsymbol{g}=g_{n-1}g_{n-2}\cdots g_0$ 从左向右前 i 个元素相同的不同码字($0\leqslant i\leqslant n-1$) 为 $G_q^i(n-i)$，其中：$G_q^0(n)=G_q(n)$，$G_q(0)$ 与 $G_q'(0)$ 均为空，对 $i=1,2,\cdots,n-1$

$$G_q^i(n-i)=g_{n-1}g_{n-2}\cdots g_{n-i}\begin{cases}G_q(n-i) & 2\mid \sum\limits_{k=n-i}^{n-1}g_k\\ G_q'(n-i) & 2\nmid \sum\limits_{k=n-i}^{n-1}g_k\end{cases}$$

若可以表示成上述形式，显然对于 $G_q(n)$ 中从左向右前 i 个元素相同的不同码字在 $G_q(n)$ 中是不间断地.

证 我们用数学归纳法对此引理加以证明.

对于与码 $\boldsymbol{g}$ 从左向右第 1 个元素相同的不同码字来说，若将 $G_q(n)$ 按顺序分为 q 组，则每组中码字的第一个元素相同，且不同组之间第一个元素不同，所以与码 $\boldsymbol{g}$ 从左向右第一个元素相同的不同码字就是这 q 组中的某一组，显然是不间断地，而且由定义 1 可知，从左向右第一个元素为 g_{n-1} 的不同码字可表示为 $g_{n-1}\overline{G}_q(n-1)$ 即为 $G_q{}^1(n-1)$.

当 $2\leqslant i\leqslant n-1$ 时，假设在 $G_q(n)$ 中与码 $\boldsymbol{g}$ 从左向右前 $i-1$ 元素相同的不同码字为 $G_q^{i-1}(n-i+1)$.

我们来证明对于 $G_q(n)$ 中从左向右前 i 个元素相同的码字也具有同样的形式：

1）当 $2 \mid \sum_{k=n-i+1}^{n-1} g_k$，由反射 Gray 码的定义可知：

$$G_q(n-i+1)=\begin{cases}0 & G_q(n-i)\\ 1 & G_q'(n-i)\\ \cdots & \cdots\\ q-1 & \overline{G}_q(n-i)\end{cases}$$

若将 $G_q(n-i+1)$ 按顺序分为 q 组，每一组第一个元素相同，不同组左边第一个元素不同. 所以若取第 i 个相同的元素为 g_{n-i} 即取 $G_q(n-i+1)$ 中第一个元素为 g_{n-i} 的所有码字，则在 $G_q(n-i+1)$ 中可表示为：

$$g_{n-i}\overline{G}_q(n-i)$$

又因为 $\sum_{k=n-i+1}^{n-1} g_k$ 为偶数，所以 g_{n-i} 与 $\sum_{k=n-i}^{n-1} g_k$ 的奇偶性相同. 所以 $G_q(n)$ 中从左向右前 i 个元素为 $g_{n-1}g_{n-2}\cdots g_{n-i}$ 的不同码字可表示为 $G_q^i(n-i)$.

2）当 $2 \nmid \sum_{k=n-i+1}^{n-1} g_k$ 时，由反射 Gray 码的定义可知：

$$G_q'(n-i+1)=\begin{cases}q-1 & \overline{G}_q'(n-i)\\ \cdots & \cdots\\ 1 & G_q(n-i)\\ 0 & G_q'(n-i)\end{cases}$$

若将 $G_q'(n-i+1)$ 按顺序分为 q 组，每一组左边第一个元素相同，不同组左边第一个元素不同. 所以若取第 i 个相同的元素为 g_{n-i} 即取 $G_q'(n-i+1)$ 中第一个元素为 g_{n-i} 的所有码字，则在 $G_q'(n-i+1)$ 中可表示为：

$$g_{n-i}\overline{G}_q'(n-i)$$

又因为 $\sum_{k=n-i+1}^{n-1} g_k$ 为奇数，所以 g_{n-i} 与 $\sum_{k=n-i1}^{n-1} g_k$ 的奇偶性相反. 所以 $G_q(n)$ 中从左向右前 i 个元素为 $g_{n-1}g_{n-2}\cdots g_{n-i}$ 的不同码字可表示为 $G_q^i(n-i)$.

此种形式的码字在 $G_q(n)$ 中的不间断性是显然的，因此引理得证.

下面我们来证明定理 1.

证　任取 $G_q(n)$ 中的一个码字 $\boldsymbol{g}=g_{n-1}g_{n-2}\cdots g_0$，若定理 1 中的 $a_{n-1-i}\cdot q^{n-1-i}(0\leqslant i\leqslant n-1)$ 表示的是将 $G_q^i(n-i)$ 按顺序分为 q 组后，码 $\boldsymbol{g}$ 所在组之前的码字的个数，那么显然 $\sum_{i=0}^{n-1} a_{n-i-1}q^{n-i-1}=\sum_{i=0}^{n-1} a_i q^i$ 表示在 $G_q(n)$ 中码 $\boldsymbol{g}$ 之前码字的个数，也就是码 $\boldsymbol{g}$ 在 $G_q(n)$ 中的位置，下面证明这一点：

当 $i=0$ 时，将 $G_q^0(n-0)=G_q(n)$ 分为 q 组，则 $\boldsymbol{g}$ 在第 $g_{n-1}+1$ 组，此组前面共有 g_{n-1} 组，而每组中码字的个数为 q^{n-1}，所以此组前面共有 $g_{n-1}q^{n-1}$ 个码字，即为定理 1 中的 $a_{n-1}q^{n-1}$.

当 $1\leqslant i\leqslant n-1$ 时，由引理 1 可知，与码 $\boldsymbol{g}$ 从左向右前 i 个元素相同的码字必属于 $G_q^i(n-i)$，而且 $G_q^i(n-i)$ 在 $G_q(n)$ 中是不间断地，我们分两种情况对 a_i 加以证明：

1）当 $2 \mid \sum_{k=n-i}^{n-1}$ 时，将 $G_q^i(n-i)$ 分为 q 组，码 $\boldsymbol{g}$ 在第 $g_{n-i-1}+1$ 组，此组前面有 g_{n-i-1} 组，每组中有 q^{n-i-1} 个码字，所以此组前面共有 $g_{n-i-1}q^{n-i-1}$ 个码字，即定理 1 中的 $a_{n-1-i}q^{n-1-i}$；

2）当 $2 \nmid \sum_{k=n-i}^{n-1}$ 时，将 $G_q^i(n-i)$ 分为 q 组，码 $\boldsymbol{g}$ 在第 $q-g_{n-i-1}$ 组，此组前面有 $q-g_{n-i-1}-1$ 组，每组中有 q^{n-i-1} 个码字，所以此组前面共有 $(q-1-g_{n-i-1})q^{n-i-1}$ 个码字，即定理 1 中的 $a_{n-1-i}q^{n-1-i}$. 所以 $a_{n-1-i}q^{n-1-i}(0\leqslant i\leqslant n-1)$ 表示的是将 $G_q^i(n-i)$ 按顺序分为 q 组后，码 $\boldsymbol{g}$ 所在组之前码字的个数，所以 $\sum_{i=0}^{n-1} a_{n-i-1}q^{n-i-1}=\sum_{i=0}^{n-1} a_i q^i$ 表示码 $\boldsymbol{g}$ 在 $G_q(n)$ 中的位置，因此定理 1 得证.

二进制 n 元组 $a_{n-1}a_{n-2}\cdots a_1a_0$ 在二进制反射 Gray 码序中的位置 k 可如下确定：对 $i=0,1,2,\cdots,n-1$,

令

$$b_i=\begin{cases}0 & \text{如果 } 2 \mid \sum\limits_{j=i}^{n-1} a_j \\ 1 & \text{如果 } 2 \nmid \sum\limits_{j=i}^{n-1} a_j\end{cases}$$

则

$$k=b_{n-1}2^{n-1}+b_{n-2}2^{n-2}+\cdots+b_1 2+b_0$$

不难发现，二进制反射 Gray 码中码字位置的计算公式[5]是我们在定理 1 中给出公式的一个特例，因此我们将反射 Gray 码中码字的位置公式由二进制推广到了 q 进制.

3 生成反射 Gray 码的两个算法

位置公式一旦确定，不难找到 $G_q(n)$ 与 $N_q(n)$ 之间存在的映射：我们取 $G_q(n)$ 和 $N_q(n)$ 中任意对应位置上的码字分别为 $\boldsymbol{g}=g_{n-1}g_{n-2}\cdots g_0$，$\boldsymbol{x}=x_{n-1}x_{n-2}\cdots x_0$，则 $\mathscr{F}(\boldsymbol{g})=\boldsymbol{x}$，其中

$$x_i=\begin{cases}g_{n-1} & i=n-1 \\ g_i & 0 \leqslant i \leqslant n-2 \text{ 且 } 2 \mid \sum\limits_{k=i+1}^{n-1} g_k \\ q-1-g_i & 0 \leqslant i \leqslant n-2 \text{ 且 } 2 \nmid \sum\limits_{k=i+1}^{n-1} g_k\end{cases}$$

而 $\mathscr{F}^{-1}(\boldsymbol{x})=\boldsymbol{g}$，其中

$$g_i=\begin{cases}x_{n-1} & i=n-1 \\ x_i & 0 \leqslant i \leqslant n-2 \text{ 且 } 2 \mid \sum\limits_{k=i+1}^{n-1} g_k \\ q-1-x_i & 0 \leqslant i \leqslant n-2 \text{ 且 } 2 \nmid \sum\limits_{k=i+1}^{n-1} g_k\end{cases}$$

下面给出两种生成反射 Gray 码的算法：

算法 1

Input：整数 $q \geqslant 2$，$n \neq 0$

Output：$q^n \times n$ 矩阵 $\boldsymbol{G}$

$\boldsymbol{N} \leftarrow \boldsymbol{N}_q(\boldsymbol{n})$；// 矩阵 **N** 的每一行均为自然码

$G \leftarrow 0_{q^n \times n}$；//$\boldsymbol{G}$ 初始化为 $q^n \times n$ 的 0 矩阵

for $i=1:n$ do

$G(i,:) \leftarrow \mathscr{F}^{-1}(N(i,:))$；//$N$ 中每一行都用 $\mathscr{F}^{-1}$ 作用，$\mathscr{F}^{-1}$ 即为上述 $N_q(n)$ 到 $G_q(n)$ 的映射

end

return $\boldsymbol{G}$

算法 2

Input：q，n

Output：$G_q(n)$

$g_{n-1}g_{n-2}\cdots g_0 \leftarrow 0^n$；$G_q(n) \leftarrow g_{n-1}g_{n-2}\cdots g_0$；$i \leftarrow 0$

while $(2 \mid q$ and $g_{n-1},g_{n-2},\cdots,g_0 \neq q-1,0^{n-1})$ or $(2 \nmid q$ and $g_{n-1},\cdots,g_0 \neq (q-1)^n)$ do

$\sigma \leftarrow (g_{n-1}+g_{n-2}+\cdots+g_{i+1}) \bmod 2$

if $\sigma=0$ and $g_i \neq q-1$ then

$g_i \leftarrow g_i+1$；$i \leftarrow 0$；

else if $\sigma=1$ and $g_i \neq 0$ then

$g_i \leftarrow g_i-1$；$i \leftarrow 0$；

else

$i \leftarrow i+1$;

if $i=n-1$ and $g_i \neq q-1$then

$g_i \leftarrow g_i+1$; $i \leftarrow 0$;

Row Append $g_{n-1} g_{n-2} \cdots g_0$ to $G_q(n)$

end

两个算法各有其优点，其中算法1可以生成反射Gray中任意位置上的码字；算法2可以逐个生成反射Gray码中的码字，当然也可以生成反射Gray码中任一码字的下一个码字.

4　结束语

本文给出了一个确定 q 进制反射Gray码中码字的位置的计算公式，而且已知的二进制反射Gray中码字的位置计算公式是其特例，这样我们便将反射Gray码中码字的位置公式由二进制推广到了 q 进制. 有了本文给出的两种生成反射Gray码的算法，若给定 q 进制反射Gray码的一个位置，我们便可由算法1生成此位置上的码字，若给定 q 进制反射Gray码中的任意一个码字，我们可由算法2生成它的下一个码字，当然我们也可以由这两个算法分别生成 q 进制反射Gray码中的所有码字，这在通信安全以及数字模拟信号中的应用是相当广泛的.

参考文献：

[1] GRAY F. Pulse Code Communication: U. S, 2632058 [P]. 1953-03-17.

[2] ZOU J C, LI G F, QI D X. Generalized Gray Code and Its Application in the Scrambling Technology of Digital Images [J]. Applied Mathematics a Journal of Chinese Universities, 2002, 3(3): 363-370.

[3] FLORES I. Reflected Number Systems [J]. IRE Transactions on Electronic Computers, 1956, 5(2): 79-82.

[4] ER M C. On Generating the N-Ary Reflected Gray Codes [J]. IEEE Transactions on Computers, 1984, 100(8): 739-741.

[5] BRUALDI R A. Introductory Combinatorics [M]. 5th ed. New Riders: Pearson, 2009: 100-119.

[6] LEE E T, LEE M E. Algorithms for Generating Generalized Gray Codes [J]. Kybernetes, 2013, 28(28): 837-844.

[7] SHARMA B D, KHANNA R K. On m-Ary Gray Codes [J]. Information Sciences, 1978, 15(1): 31-43.

[8] LICHTNER J. Iterating an α-Ary Gray Codes [J]. SIAM J Discrete Math, 1998, 11(3): 381-386.

[9] COHN M. Affine m-Ary Gray Codes [J]. Information and Control, 1963, 6(1): 70-78.

[10] IRSHID M I. Gray Code Weighting System [J]. IEEE Transactions on Information Theory, 1978, 33(6): 930-931.

Notes on the Q-ary Reflected Gray Codes

ZHANG Shuai[1], QU Yun-yun[2],
BAO Xiao-min[1], HUANG Hua-wei[2]

1. School of Mathematics and Statistics, Southwest University, Chongqing 400715, China;

2. School of Mathematics and Computer Science, Guizhou Normal University, Guiyang 550001, China

Abstract: The formula for calculating the position of a code in the binary reflected Gray codes is already known. This paper presents a formula for calculating the position of a codeword in the q-ary reflected Gray codes for any integer $q \geqslant 2$, and this formula takes the binary case as a special case. This paper also introduces two algorithms for generating the q-ary reflected Gray codes: the first one can generate a codeword at any position in the q-ary reflected Gray; the other one can generate a codeword that comes after any given codeword in the q-ary reflected Gray.

Key words: reflected Gray code; position; q-ary; natural code

责任编辑　张　枸