SIAM J. DISCRETE MATH.
Vol. 14, No. 2, pp. 237–239
© 2001 Society for Industrial and Applied Mathematics

A NOTE ON ITERATING AN α-ARY GRAY CODE*

CHI-JEN LU† AND SHI-CHUN TSAI‡

Abstract. In this note we consider the number of distinct α-ary codes produced by repeatedly applying the Gray code mapping of Sharma and Khanna [*Inform. Sci.*, 15 (1978), pp. 31–43]. This number was derived before by Lichtner [*SIAM J. Discrete Math.*, 11 (1998), pp. 381–386], and we give an alternative proof here. Our key observation is a simple connection between this number and the period of binomial coefficients modulo α. Then the result follows immediately from a known periodic property of binomial coefficients modulo α [*Fibonacci Quart.*, 27 (1989), pp. 64–79; *SIAM J. Discrete Math.*, 9 (1996), pp. 55–62; *Ann. Univ. Mariae Curie-Sklodowska Sect. A*, 10 (1956), pp. 37–47].

Key words. gray code, binomial coefficient

AMS subject classifications. 68Q25, 68R01

PII. S0895480100367688

1. Introduction.

Let ℓ and α be positive integers greater than one. An α-ary Gray code of dimension ℓ is a sequence of α^ℓ distinct α-ary strings of length ℓ such that any two adjacent strings differ in exactly one position. Therefore a Gray code corresponds to a bijection, mapping integers between 0 and $\alpha^\ell - 1$ to α-ary strings of length ℓ. When viewing such integers in base α with ℓ digits, the mapping can be seen as a permutation among α-ary strings of length ℓ. Sharma and Khanna [4] defined one such mapping, denoted by $\mathcal{K}$, in the following way.

DEFINITION 1.1 (see [4]). *$\mathcal{K}(x_1x_2\cdots x_\ell) = g_1g_2\cdots g_\ell$, where*

$$g_i = \begin{cases} x_1 & \text{if } i = 1, \\ x_i - x_{i-1} \pmod{\alpha} & 1 < i \le \ell. \end{cases}$$

Equivalently, $\mathcal{K}^{-1}(g_1g_2\cdots g_\ell) = x_1x_2\cdots x_\ell$, where

$$x_i = \begin{cases} g_1 & \text{if } i = 1, \\ g_i + x_{i-1} \pmod{\alpha} & 1 < i \le \ell. \end{cases}$$

Culberson [1] and Lichtner [3] studied the number of distinct sets of codes that can be generated by repeated applications of the mapping $\mathcal{K}$. This is the same question as determining the order of the mapping $\mathcal{K}$, defined in the following.

DEFINITION 1.2. *Let $\mathcal{K}^0 = \mathcal{I}$, the identity mapping, i.e., $\mathcal{I}(x) = x$ for all x. For $i \ge 0$, let $\mathcal{K}^{i+1} = \mathcal{K} \circ \mathcal{K}^i$, i.e., $\mathcal{K}^{i+1}(x) = \mathcal{K}(\mathcal{K}^i(x))$. The order of $\mathcal{K}$ is the smallest positive integer m such that $\mathcal{K}^m = \mathcal{I}$. Similarly, we can define $\mathcal{K}^{-(i+1)} = \mathcal{K}^{-1} \circ \mathcal{K}^{-i}$ for $i \ge 0$.*

Note that the order of $\mathcal{K}$ is the same as the order of $\mathcal{K}^{-1}$, and we will work on $\mathcal{K}^{-1}$ instead. Lichtner [3] derived an explicit formula for the order of $\mathcal{K}^{-1}$. In this note,

*Received by the editors February 1, 2000; accepted for publication (in revised form) January 9, 2001; published electronically April 3, 2001.
http://www.siam.org/journals/sidma/14-2/36768.html

†Institute of Information Science, Academia Sinica, Nankang 11529, Taipei, Taiwan (cjlu@iis.sinica.edu.tw).

‡Department of Information Management, National Chi-Nan University, 1 University Road, Pu-Li, Nan-Tou 545, Taiwan (tsai@csie.ncnu.edu.tw). The work of this author was supported in part by the National Science Council of Taiwan under contract NSC 89-2213-E-260-009.

we give an alternative proof for Lichtner's result. The key idea is an observation on a simple connection between the order of $\mathcal{K}^{-1}$ and the period of binomial coefficients modulo α. Then the result follows immediately from a known periodic property of binomial coefficients modulo α [2, 5, 6].

In section 2, we state some relevant results. In section 3, we prove our main technical lemma. Finally, we conclude with some remarks in section 4.

2. Results. Let $x = x_1x_2\cdots x_\ell$. Define $x^i = \mathcal{K}^{-i}(x)$ for $i \geq 0$ with $x^0 = \mathcal{K}^0(x) = x$. Let x^i_j denote the jth digit of x^i. Here are some simple facts.

LEMMA 2.1 (see [3]).

1. $x^i_j \equiv x^i_{j-1} + x^{i-1}_j \pmod{\alpha}$, *where* $i \geq 1$ *and* $1 < j \leq \ell$.
2. $x^i_j \equiv \sum_{k=1}^{j} \binom{i+j-k-1}{j-k} x_k \pmod{\alpha}$, *where* $i \geq 1$ *and* $1 \leq j \leq \ell$.
3. *If* $\binom{i+j-2}{j-1} \equiv 0 \pmod{\alpha}$, *for* $2 \leq j \leq \ell$, *then* $x^i = x$.
4. *Let* $x = x_1x_2\cdots x_\ell$ *be an* α*-ary string such that* $x_1 \not\equiv 0 \pmod{\alpha}$ *and* $GCD(x_1, \alpha) = 1$. *If there is a* j, $2 \leq j \leq \ell$, *such that* $\binom{i+j-2}{j-1} \not\equiv 0 \pmod{\alpha}$, *then* $x^i \neq x$.

Lemma 2.1(1–2) follows from the definition of $\mathcal{K}$ and by induction. Lemma 2.1(3–4) follows from Lemma 2.1(1–2).

From now on, we assume that α has the form of

$$\alpha = p_1^{n_1} \cdots p_q^{n_q},$$

where p_i's are distinct primes and n_i's are positive integers. Lichtner generalized Culberson's result [1] and proved the following theorem.

THEOREM 2.2 (see [3]). *Let* $\ell > 1$ *and let* $e_i = \lfloor \log_{p_i}(\ell - 1) \rfloor$ *for* $1 \leq i \leq q$. *Then the order of* $\mathcal{K}^{-1}$ *is exactly* $L = \prod_{i=1}^{q} p_i^{n_i+e_i}$.

We will give a more straightforward proof of Lichtner's theorem above, given the following known result on the period of the function $f_{\alpha,k}$, defined as

$$f_{\alpha,k}(x) = \binom{x}{k} \pmod{\alpha}.$$

LEMMA 2.3 (see [2, 5, 6]). *Let* k *be a positive integer and let* $d_i = \lfloor \log_{p_i} k \rfloor$ *for* $1 \leq i \leq q$. *Then the period of the function* $f_{\alpha,k}$ *is exactly* $\prod_{i=1}^{q} p_i^{n_i+d_i}$.

COROLLARY 2.4. *For any positive integers* k_1, k_2 *with* $k_1 \leq k_2$, *the period of* f_{α,k_1} *divides the period of* f_{α,k_2}.

Our main technical contribution is the following simple connection.

LEMMA 2.5. *The order of* $\mathcal{K}^{-1}$ *is the same as the period of the function* $f_{\alpha,\ell-1}$.

Lemmas 2.3 and 2.5 together immediately imply Theorem 2.2. It remains to prove Lemma 2.5.

3. Proof of Lemma 2.5. Let $x = x_1x_2\cdots x_\ell$ be an arbitrary α-ary string and let $x^i = \mathcal{K}^{-i}(x)$. Item 2 of Lemma 2.1 states that

$$x^i_1 \equiv \binom{i-1}{0} x_1 \pmod{\alpha},$$

$$x^i_2 \equiv \binom{i}{1} x_1 + \binom{i-1}{0} x_2 \pmod{\alpha},$$

$$x^i_3 \equiv \binom{i+1}{2} x_1 + \binom{i}{1} x_2 + \binom{i-1}{0} x_3 \pmod{\alpha},$$

$$\vdots$$
$$x_\ell^i \equiv \binom{i+\ell-2}{\ell-1}x_1 + \binom{i+\ell-3}{\ell-2}x_2 + \cdots + \binom{i}{1}x_{\ell-1} + \binom{i-1}{0}x_\ell \pmod{\alpha}.$$

Observe that there are ℓ different binomial coefficients above, so $\mathcal{K}^{-i}$ is completely determined by the vector $c^i = c_1^i c_2^i \cdots c_\ell^i$, where

$$c_j^i = \binom{i+j-2}{j-1} \pmod{\alpha}.$$

We use the convention that $\binom{a}{0} = 1$ for any integer a. Note that $c^0 = 100\cdots0$. As i increases, the vector c^i changes in a periodic fashion due to the periodic behavior of its components. Recall that $L = \prod_{i=1}^{q} p_i^{n_i+e_i}$. We show that the period is L and the cycle occurs exactly when the vector becomes $100\cdots0$ again.

Clearly $c_1^L = 1$. From Lemma 2.3 and Corollary 2.4, we know that for $1 < j \le \ell$, $c_j^L = \binom{L+j-2}{j-1} \pmod{\alpha} = \binom{0+j-2}{j-1} \pmod{\alpha} = 0$. Therefore $c^L = 100\cdots0 = c^0$. Now, as $c_1^i = 1$ and for $j > 1$,

$$c_j^i = c_{j-1}^i + c_j^{i-1} \pmod{\alpha},$$

we see that the vector c^i is completely determined by the vector c^{i-1}. Therefore the same pattern repeats again from c^L. The cycle could not be shorter since $c_\ell^i = f_{\alpha,\ell-1}(i+\ell-2)$, considered as a function of i, has a period of exactly L. Therefore L is the smallest positive integer i such that $c^i = c^0$.

Since $c^L = 100\cdots0$, $\mathcal{K}^{-L}$ is the identity mapping. On the other hand, for any positive $i < L$, $c^i \neq 100\cdots0$. Item 4 of Lemma 2.1 tells us that $\mathcal{K}^{-i}x \neq x$ for any x with $x_1 = 1$ and thus $\mathcal{K}^{-i} \neq \mathcal{I}$. Therefore the order of $\mathcal{K}^{-1}$ is exactly L.

4. Conclusion and remarks. By using the periodic property of binomial coefficients, we give a proof on the order of the mapping $\mathcal{K}$. Lichtner's proof could have been more straightforward if he had known the periodic property of binomial coefficients. Such a periodic property has also been applied to results in computational complexity [5]. We expect that this nice property should have more applications to be discovered.

REFERENCES

[1] J. Culberson, *Mutation-crossover isomorphisms and the construction of discriminating functions*, Evolutionary Comput., 2 (1995), pp. 279–311.

[2] Y.H. Kwong, *Minimum periods of binomial coefficients modulo M*, Fibonacci Quart., 27 (1989), pp. 64–79.

[3] J. Lichtner, *Iterating an α-ary Gray code*, SIAM J. Discrete Math., 11 (1998), pp. 381–386.

[4] B.D. Sharma and R.K. Khanna, *On m-ary Gray codes*, Inform. Sci., 15 (1978), pp. 31–43.

[5] S-C. Tsai, *Lower bounds on representing boolean functions as polynomials in Z_m*, SIAM J. Discrete Math., 9 (1996), pp. 55–62.

[6] S. Zabek, *Sur la periodicite modulo m des suits de nombres $\binom{n}{k}$*, Ann. Univ. Mariae Curie-Sklodowska Sect. A, 10 (1956), pp. 37–47.