Antipodal Gray Codes

Charles E. Killian, Carla D. Savage *,1

Department of Computer Science
N. C. State University, Box 8206
Raleigh, NC 27695, USA

Abstract

An n-bit Gray code is a circular listing of the 2^n n-bit strings so that successive strings differ only in one bit position. An n-bit *antipodal* Gray code has the additional property that the complement of any string appears exactly n steps away in the list. The problem of determining for which values of n antipodal Gray codes can exist was posed by Hunter Snevily, who showed them to be possible for $n = 1, 2, 3$, and 4. In this paper, we show they are not possible for odd $n > 3$ or for $n = 6$. However, we provide a recursive construction to prove existence when n is a power of 2. The question remains open for any even $n > 6$ which is not a power of 2.

Key words: Gray code, Hamiltonian cycle, n-cube

1 Introduction

A binary Gray code is a listing of all the n-bit binary strings, for a given n, such that only one bit changes. between successive items in the list, including the first and last. The classical approach, known as the binary reflected Gray code [1,2], starts with the 1-bit Gray code '$0, 1$'; for $n > 1$, construct the n-bit Gray code by first appending 0 to each element of the $(n-1)$-bit Gray code, then list the $(n-1)$-bit Gray code in reverse, appending 1 to each element. It is easy to see how this produces a complete listing of all n-bit strings, with a single bit flipped between any two elements, including the first and last.

* Corresponding author.
Email addresses: chip_killian@acm.org (Charles E. Killian), savage@csc.ncsu.edu (Carla D. Savage).
URLs: http://chip.kcubes.com/research/antipodal (Charles E. Killian), http://www.csc.ncsu.edu/faculty/savage (Carla D. Savage).
[1] Research supported by NSA grant MDA 904-01-0-0083

$n=1$	$n=2$	$n=3$	$n=4$
0	00	000	0000 1010
1	01	001	0001 1011
	11	011	0011 1001
	10	111	0111 1101
		101	1111 0101
		100	1110 0100
		110	1100 0110
		010	1000 0010

Fig. 1. Examples of 1, 2, 3, and 4 bit antipodal Gray codes.

A Gray code can be viewed as a Hamiltonian cycle in the n-cube, the graph whose vertices are the n-bit binary strings, with two strings adjacent if they differ in one bit.

More recently, Gray codes have been designed to satisfy additional requirements imposed by practical applications or curious researchers. Some examples of constraints considered are: restricting where bit flips can occur [3]; requiring the same number of flips on any given bit [4,5]; enforcing non-locality conditions [6]; maximizing the *gap*, i.e., the shortest maximal consecutive sequence of 0's (or 1's) among all bit positions [7]; and requiring certain monotonicity properties [8]. But this is just a small sample. For a survey of Gray codes see [9] and for a beautiful treatment of generating bit strings in general see [10].

In the Fall of 2000, Hunter Snevily posed a question about what he called *antipodal Gray codes* [11]. An *n-bit antipodal Gray code* must satisfy the requirements for an ordinary n-bit Gray code, but in addition it has the requirement that any item's binary complement must appear *exactly* n steps away in the list. Snevily found antipodal Gray codes for $n = 1, 2, 3$, and 4 (see Figure 1), and asked whether they exist for larger n.

In this paper we are able to at least partially answer this question. In Section 2, we develop some notation and basic results about antipodal Gray codes. In Section 3 we prove that for odd $n > 3$, an n-bit antipodal Gray code is not possible. In Section 4 we discuss our exhaustive computer search which showed that there exists no 6-bit antipodal Gray code. However, it turns out that when n is power of two, n-bit antipodal Gray codes *do* exist and we provide a recursive construction in Section 5. We conclude in Section 6 with some final remarks about the remaining open cases.

2 Sign Sequences and Signatures

Define $\overline{0} = 1$ and $\overline{1} = 0$ so that for an n-bit string $x = x_1 x_2 \cdots x_n$,

$$\overline{x} = \overline{x_1}\ \overline{x_2} \cdots \overline{x_n}.$$

Denote an n-bit Gray code G by

$$G = (G(0), G(1), \ldots, G(2^n - 1)),$$

where $G(i)$ is the ith n-bit string of G. Then G is an *antipodal Gray code* if for $0 \leq i < 2^n$,

$$\text{(i) } \overline{G(i)} = G((i+n) \bmod 2^n) \quad \text{or} \quad \text{(ii) } \overline{G(i)} = G((i-n) \bmod 2^n).$$

In case (i) i is called a *pre-element* and in case (ii) a *post-element*. To simplify notation, we let $i \oplus a$ denote $(i + a) \bmod 2^n$, for any integers i, a. Note that $\oplus$ is commutative and associative.

For the remainder of this section, we assume G is an n-bit antipodal Gray code.

Lemma 1 *If $n > 2$ and $0 \leq i < 2^n$, i is a pre-element if and only if $i \oplus n$ is a post-element.*

Proof. By definition, if i is a pre-element, then $i \oplus n$ is a post-element. For the converse, suppose both i and $i \oplus n$ are post-elements. Then

$$\overline{G(i \oplus n)} = G(i) = \overline{G(i \oplus -n)},$$

so $G(i \oplus n) = G(i \oplus -n)$ and therefore, since the elements of G are distinct, $(i \oplus n) = (i \oplus -n)$, that is, $2n$ is divisible by 2^n, which is false when $n > 2$. □

When $n > 2$, we associate with G its *sign sequence*, $\sigma(G)$, of symbols from $\{+, -\}$:

$$\sigma_G = (\sigma_G(0), \sigma_G(1), \ldots, \sigma_G(2^n - 1)),$$

where $\sigma_G(i) =$'+' if i is a pre-element and otherwise $\sigma_G(i) =$'−'. For example, for the 4-bit antipodal Gray code G of Figure 1,

$$\sigma_G = (+, +, +, +, -, -, -, -, +, +, +, +, -, -, -, -).$$

Lemma 2 *If $n > 2$, then for any integer i such that $0 \leq i < 2^n$,*

$$\sigma_G(i) = \sigma_G(i \oplus 2n).$$

Proof. by Lemma 1, i is a pre-element if and only if $i \oplus n$ is a post-element, which occurs if and only if $i \oplus 2n$ is a pre-element. So, $\sigma(i) = \sigma(i \oplus 2n)$. □

Integer p is a *period* for σ_G if $\sigma_G(i) = \sigma_G(i \oplus p)$ for $0 \leq i < 2^n$. Cleary 2^n is a period for σ_G and Lemma 2 shows that $2n$ is a period as well.

Let $\gcd(x, y)$ denote the greatest common divisor of x and y.

Lemma 3 *If $n > 2$ and $0 \leq i < 2^n$. Then $\gcd(2^n, 2n)$ is a period for σ_G.*

Proof. There exist integers a, b such that $\gcd(2^n, 2n) = a2^n + 2bn$. Thus,

$$\sigma_G(i \oplus \gcd(2^n, 2n)) = \sigma_G(i \oplus (a2^n + 2bn)) = \sigma_G((i \oplus 2bn) \oplus a2^n) = \sigma_G(i \oplus 2bn) = \sigma_G(i).$$

□

We have found the notion of a *signature* to be instrumental in our understanding of antipodal Gray codes. The *signature* of the antipodal Gray code G is the shortest sign sequence β satisfying

$$\sigma_G = \beta\beta \cdots \beta.$$

For example, the signature of the 4-bit antipodal Gray code in Figure 1 is $(+, +, +, +, -, -, -, -)$.

Theorem 4 *If $n > 2$ and β is the signature of G then $|\beta|$ divides $gcd(2^n, 2n)$, and $|\beta|$ does not divide n.*

Proof. By Lemma 3, σ_G is periodic with period $p = \gcd(2n, 2^n)$. Thus, if α is the sequence $(\sigma_G(0), \sigma_G(1), \sigma_G(p-1))$, $\sigma_G = \alpha\alpha \cdots \alpha$, so by definition of β, we must have $|\beta| \leq |\alpha| = p$. Clearly, $|\beta|$ divides 2^n, the length of σ_G. Then since both $|\beta|$ and p are powers of 2, $|\beta|$ divides p. Finally, $|\beta|$ cannot divide n, because if it did, then $\sigma_G(i) = \sigma_G(i \oplus n)$, contradicting Lemma 1. □

3 Nonexistence of Antipodal Gray Codes for Odd $n > 3$

While an antipodal Gray code exists for $n = 1, 3$, this is not the case for the remaining odd numbers. We prove this via a sequence of lemmas, assuming in Lemmas 5 through 9 that G is an n-bit antipodal Gray code.

Lemma 5 *If n is odd and $n > 3$, then σ_G must alternate between '+' and '−' symbols.*

Proof. Let β be the signature of G. There is a one-to-one correspondence between the pre-elements and post-elements of G, so σ_G must contain the same number of '+' symbols as '−' symbols and therefore β must as well. Thus $|\beta| \geq 2$ and by Theorem 4, $|\beta|$ is a power of 2 dividing $2n$. Since n is odd, $|\beta| = 2$ is the only possibility. □

Define the *flip sequence*, f_G, of G to be the sequence where, for $0 \leq i < 2^n$, $f_G(i)$ is the bit position in which $G(i)$ and $G(i \oplus -1)$ differ. For the 4-bit Gray code of Figure 1,

$$f_G = (3, 4, 3, 2, 1, 4, 3, 2, 3, 4, 3, 2, 1, 4, 3, 2).$$

Lemma 6 *For $n > 2$, $\sigma_G(i) =$'+' if and only if $\{f_G(i \oplus k) | 1 \leq k \leq n\} = \{1, \ldots, n\}$.*

Proof. By definition of pre-element and by Lemma 1, when $n > 2$, $\sigma_G(i) =$'+' if and only if $G(i)$ and $G(i \oplus n)$ differ in all n bits. Since G is a Gray code, exactly one bit is flipped between successive elements, so the result follows.

□

For example, for the 4-bit Gray code in Figure 1, $\sigma_G(1) =$'+' and

$$\{f_G(1 \oplus k) | 1 \leq k \leq 4\} = \{4, 3, 2, 1\} = \{1, 2, 3, 4\},$$

whereas $\sigma_G(5) =$'−' and

$$\{f_G(5 \oplus k) | 1 \leq k \leq 4\} = \{4, 3, 2, 3\} = \{2, 3, 4\} \neq \{1, 2, 3, 4\}.$$

Lemma 7 *For odd $n > 3$ if $\sigma_G(i) =$'+' then $f_G(i \oplus 1 \oplus n) \neq f_G((i \oplus 1)$.*

Proof. By Lemma 5, since σ_G alternates in sign, $\sigma_G(i \oplus 1) =$'−'. Define

$$F_i = \{f_G(i \oplus k) | 1 \leq k \leq n\}.$$

By Lemma 6, $F_i = \{1, \ldots, n\}$. Since $F_{i+1} = (F_i - \{f_G(i \oplus 1\}) \cup \{f_G(i \oplus 1 \oplus n)\}$, if $f_G(i \oplus 1) = f_G(i \oplus 1 \oplus n)$, then $F_{i+1} = F_i = \{1, \ldots, n\}$. Thus, by Lemma 6, $\sigma_G(i \oplus 1) =$'+', a contradiction. □

Lemma 8 *If n is odd and $n > 3$ and $\sigma_G(i) =$'+' then*

$$f_G(i \oplus 1) = f_G((i \oplus 1) \oplus (n+1))$$

and

$$f_G(i \oplus 2) = f_G((i \oplus 2) \oplus (n-1)).$$

Proof. Suppose $\sigma_G(i) =$'+'. Then by Lemma 5, $\sigma_G(i \oplus 2) =$'+', so by Lemma 6

$$\{f_G(i \oplus 1), \ldots, f_G(i \oplus n)\} = \{1, \ldots, n\} = \{f_G(i \oplus 3), \ldots, f_G(i \oplus (n+2))\}.$$

Thus,

$$\{f_G(i \oplus 1), f_G(i \oplus 2)\} = \{f_G(i \oplus (n+1)), f_G(i \oplus (n+2))\}.$$

Since by Lemma 7, $f_G(i \oplus 1) \neq f_G(i \oplus (n+1))$, we know that $f_G(i \oplus 1) = f_G(i \oplus (n+2))$ and $f_G(i \oplus 2) = f_G(i \oplus (n+1)) = f_G((i \oplus 2) \oplus (n-1))$. □

Let $\mathrm{lcm}(x, y)$ denote the least common multiple of x and y.

Lemma 9 *Let $n > 3$ be odd and let $l = \mathrm{lcm}(n+1, n-1)$. Then $f_G(i) = f_G(i \oplus l)$ for $0 \leq i < 2^n$.*

Proof. Suppose $\sigma_G(i) =$'+'. Then since n is odd, by Lemma 5, for all $j \geq 0$,

$$\sigma_G(i \oplus j(n+1)) = \text{'+'} = \sigma_G(i \oplus j(n-1)),$$

so repeated application of Lemma 8 gives for all $j \geq 0$:

$$f_G(i \oplus 1) = f_G((i+1) \oplus j(n+1))$$

and

$$f_G(i \oplus 2) = f_G((i+2) \oplus j(n-1)).$$

Thus, in particular, if $\sigma_G(i) =$'+',

$$f_G(i \oplus 1) = f_G((i+1) \oplus l);$$

$$f_G(i \oplus 2) = f_G((i+2) \oplus l).$$

Since for any i, either $\sigma_G(i \oplus -1) =$'+' or $\sigma_G(i \oplus -2) =$'+', we have $f_G(i) = f_G(i \oplus l)$ for all i. □

Theorem 10 *If n is odd and $n > 3$, there exists no n-bit antipodal Gray code.*

Proof. Let $l = \text{lcm}(n+1, n-1)$. Since n is odd, $n-1$ and $n+1$ are two consecutive even integers, $2k$, $2(k+1)$. As k and $k+1$ have no common factors, $l = \text{lcm}(n+1, n-1) = (n+1)(n-1)/2 = (n^2-1)/2$. We will show that if G is an n-bit antipodal Gray code (n odd) then $G(i) = G(i \oplus 2l)$ for $0 \leq i < 2^n$. Since all elements of G are distinct, this would require $2l \equiv 0 \pmod{2^n}$. But $2l = n^2 - 1 < 2^n$ for $n > 3$, so this is a contradiction.

It remains to show $G(i) = G(i \oplus 2l)$. Let $f(i;k)$ be the sequence of flips

$$f(i;k) = (f_G(i \oplus 1), \ldots, f_G(i \oplus k)).$$

Then by Lemma 9, $f(i;l) = f(i \oplus l; l)$ and therefore the sequence of bit changes between $G(i)$ and $G(i \oplus 2l)$ is $f(i;2l) = f(i;l), f(i;l)$. Thus any bit $1, 2, \ldots, n$ occurs an even number of times in $f(i;2l)$, requiring $G(i) = G(i \oplus 2l)$. $\square$

4 Nonexistence of an Antipodal Gray for $n = 6$

We were able to show by an exhaustive search that no antipodal Gray code for $n = 6$ can exist. To focus the search, note that if β is the signature of a 6-bit antipodal Gray code, then by Theorem 4, $|\beta|$ divides $\gcd(2^6, 12) = 4$, but does not divide 6. Thus $|\beta| = 4$ and so β must be some rotation of $(+,+,-,-)$ or $(+,-,+,-)$. But the latter is excluded since β is, by definition, minimal. So, we assume, without loss of generality, that $\beta = (+,+,-,-)$.

To test for the existence of a 6 bit Gray code, then, we systematically generated all sequences of bit flips which are consistent with the signature $(+,+,-,-)$ and tested each one to see if it is indeed a Gray code. If so, then it would be an antipodal Gray code. However every sequence failed the test.

5 Antipodal Gray Codes for $n = 2^k$

In this section we prove the existence of 2^k-bit antipodal Gray codes for every $k \geq 0$. If β is the signature of a 2^k-bit antipodal Gray code, then by Theorem 4, $|\beta|$ divides $\gcd(2^{2^k}, 2^{k+1}) = 2^{k+1}$ and does not divide 2^k, so $|\beta| = 2^{k+1}$. We will show how to construct, for every k, a 2^k-bit antipodal Gray code whose signature is $(+)^{2^k}(-)^{2^k}$, a sequence of 2^k '+' signs, followed by 2^k '$-$' signs.

Let $m = 2^{k-1}$ and let G be an m-bit antipodal Gray code with signature $(+)^m(-)^m$. Decompose G into $2^m/(2m)$ sublists of length $2m$ as follows. (Note that $m = 2^{k-1}$ so $2^m/(2m) = 2^{m-k}$.) For $0 \leq i < 2^{m-k}$ and $0 \leq j < 2m$, let

$$B_i(j) = G(2mi + j)$$

and let B_i be the list

$$B_i = B_i(0), B_i(1), \ldots, B_i(2m-1).$$

Then

$$G = B_0, B_1, \ldots, B_{2^{m-k}-1}.$$

For example, the 4-bit antipodal Gray code of Figure 1 with signature $(+)^4(-)^4$ has

$$B_0 = 0000, 0001, 0011, 0111, 1111, 1110, 1100, 1000;$$
$$B_1 = 1010, 1011, 1001, 1101, 0101, 0100, 0110, 0010.$$

Suppose that L is a listing of some subset of the set of all n-bit strings. Say that L is an *AGC listing* if (i) successive elements of L, including first and last, differ in just one bit and (ii) for each string on x, its complement $\overline{x}$ appears either n steps later or n steps earlier on L.

Lemma 11 *For $0 \leq i < 2^{m-k}$, any rotation of B_i is an AGC listing of its $2m$ m-bit strings and its signature is $(+)^m(-)^m$. Similarly, the reversal of (any rotation of) B_i is an AGC listing of its $2m$ m-bit strings with signature $(+)^m(-)^m$.*

Proof. First note that B_i itself is an AGC listing. By definition its signature is $(+)^m(-)^m$, so it does have the antipodal property. Successive elements of B_i are successive elements of G, so we need only check that $B_i(0)$ and $B_i(2m-1)$ differ in one bit. By Lemma 6, since $\sigma_{B_i}(0) =$'+', $B_i(m-1)$ differs from $B_i(0)$ in $m-1$ bits, thus $\overline{B_i(m-1)}$ differs from $B_i(0)$ in just one bit. But $\overline{B_i(m-1)} = B_i(2m-1)$, since $\sigma_{B_i}(m-1) =$ '+'.

If we show that the rotation

$$B_i' = B_i(1), B_i(2), \ldots, B_i(2m-1), B_i(0)$$

satisfies the required conditions, the same will be true for any rotation, by repeated application. For $1 \leq j \leq m-1$, the complement of $B_i(j)$ still occurs m steps later in the list B_i', but the complement of $B_i(0)$ now appears m steps earlier in B_i'. So, the signature of B_i' is still $(+)^m(-)^m$.

Similarly, the reverse of B_i still has signature $(+)^m(-)^m$ and successive elements, including the first and last, still differ in one bit. □

From each list B_i (of length $2m$) we create a list $A_i = A_i(0), \ldots A_i(4m-1)$ of length $4m$ by listing each element of B_i twice:

$$A_i = B_i(0), B_i(0), B_i(1), B_i(1), B_i(2), B_i(2), \ldots, B_i(2m-1), B_i(2m-1).$$

For the 4-bit antipodal Gray code of Figure 1,

$A_0 = 0000, 0000, 0001, 0001, 0011, 0011, 0111, 0111, 1111, 1111, 1110, 1110, 1100, 1100, 1000, 1000;$

$A_1 = 1010, 1010, 1011, 1011, 1001, 1001, 1101, 1101, 0101, 0101, 0100, 0100, 0110, 0110, 0010, 0010.$

Let A_j^l be the list A_j, rotated $4l+1$ positions, defined by:

$$A_j^l = A_j(4l+1), A_j(4l+2), \ldots, A_j(4m-1), A_j(0), A_j(1), \ldots, A_j(4l).$$

So, in the example above,

$A_1^1 = 1001, 1101, 1101, 0101, 0101, 0100, 0100, 0110, 0110, 0010, 0010, 1010, 1010, 1011, 1011, 1001.$

We need some notation. If L and M are lists of bit strings and L and M have the same length,

$$L = l_0, l_1, \ldots, l_{t-1}; \qquad M = m_0, m_1, \ldots, m_{t-1},$$

we let $L|M$ denote the list whose i-th element is the concatenation of the strings l_i and m_i:

$$L|M = l_0m_0, l_1m_1, \ldots, l_{t-1}m_{t-1}.$$

Now consider the collection of lists $A_i|A_j^l$, for $0 \le i,\ j < 2^{m-k}$ and $0 \le l < m$. For the 4-bit antipodal Gray code of Figure 1, we have 16 lists: $A_i|A_j^l$, for $0 \le i,\ j < 2$ and $0 \le l < 4$ and, for example,

$A_0|A_0^0 = 00000000, 00000001, 00010001, 00010011, 00110011, 00110111, 01110111, 01111111,$

$11111111, 11111110, 11101110, 11101100, 11001100, 11001000, 10001000, 10000000.$

For the remainder of this section, we assume all arguments are taken modulo $4m$.

Corollary 12 *Each list $A_i|A_j^l$ is an AGC listing, with signature $(+)^{2m}(-)^{2m}$, for its $4m$ $2m$-bit strings. This is also true for any rotation or reversal of list $A_i|A_j^l$.*

Proof. Note that successive elements of $A_i|A_j^l$ (including first and last) differ in just one bit: if t is even, $A_i(t) = A_i(t+1)$ and $A_i^l(t)$ and $A_i^l(t+1)$ differ in one bit; if t is odd, $A_i^l(t) = A_i^l(t+1)$ and $A_i(t)$ and $A_i(t+1)$ differ in one bit. The rest of the corollary follows from Lemma 11. □

Lemma 13 *In the collection of lists*

$$A_i|A_j^l, \qquad 1 \le i, j < 2^{m-k}, \qquad 0 \le l < m,$$

every 2^k-bit string occurs exactly once.

Proof. Since A_i and A_j^l are lists of m-bit strings and $m = 2^{k-1}$, $A_i|A_j^l$ is a list of 2^k-bit strings.

The total number of lists $A_i|A_j^l$ is $m(2^{m-k})(2^{m-k})$ and the length of each list is the length of A_i, which is $4m$. So the total number of elements on all the lists is

$$4m^2(2^{m-k})^2 = 4(2^{k-1})^2(2^{2m-2k}) = 2^{2m} = 2^{2^k}.$$

It remains to show every 2^k-bit string does occur.

Every string of length 2^{k-1} appears in G, since G is a 2^{k-1}-bit Gray code, and therefore occurs twice on some A_i. So consider string x on A_i. By definition of A_i, there is an even s, $0 \leq s < 4m$, such that

$$x = A_i(s) = A_i(s+1).$$

Then for fixed i, the lists $A_i|A_j^l$ contain all the strings:

$$\{xy \mid (y = A_j(s{+}4l{+}1) \text{ or } y = A_j(s{+}4l{+}2)) \text{ for some } j, l : 0 \leq j < 2^{m-k}, 0 \leq l < m\}.$$

Note $A_j(s+4l+1) \neq A_j(s+4l+2)$ since s is even. Furthermore, the A_j are pairwise disjoint, so the total number of (distinct) strings with prefix x on the lists $A_i|A_j^l$ is

$$2m(2^{m-k}) = 2(2^{k-1})(2^{m-k}) = 2^m = 2^{2^{k-1}},$$

which is the total number of 2^k-bit strings with prefix x. □

The remaining task is to show how to link the AGC listings $A_i|A_j^l$ to obtain an antipodal Gray code for all 2^k-bit strings. We first prove a linking lemma.

Lemma 14 *For $0 \leq i, j < 2^{m-k}$, if s and t are even, then each of the following pairs of 2^k-bit strings differ in one bit:*

(i) $A_i(t)A_j(s+1)$ *and* $A_i(t+3)A_j(s)$
(ii) $A_i(s)A_{j-1}(4m-1)$ *and* $A_i(s+1)A_j(0)$
(iii) $A_{i-1}(4m-1)A_j(s)$ *and* $A_i(0)A_j(s+1)$,

where addition on subscripts is modulo 2^{m-k} and addition on arguments is modulo $4m$.

Proof. For (i), by definition of A_j, $A_j(s) = A_j(s+1)$ when s is even. Also, since t is even, $A_i(t) = A_i(t+1)$ and $A_i(t+2) = A_i(t+3)$. Since $A_i(t+1)$ and $A_i(t+2)$ are consecutive elements of G, they differ in just one bit and the result follows.

For (ii) and (iii), $A_{j-1}(4m-1)$, the last element of A_{j-1} and $A_j(0)$, the first element of A_j, are consecutive elements of G, and therefore differ in just one

bit. As in (i), $A_i(s) = A_i(s+1)$. The argument for (iii) is the same with i and j exchanged. $\square$

Lemma 15 *For fixed i, j, l, with $0 \le i, j < 2^{m-k}$, and $0 \le l < m$, there are AGC listings, $U_{i,j,l}$ and $U^*_{i,j,l}$, both with signature $(+)^{2m}(-)^{2m}$, constructed from the $2m$-bit strings in the list $A_i|A^l_j$. These lists have the following first and last elements:*

$$\begin{array}{lllll} U_{i,j,l}: & \text{first: } A_i(4m-4l)A_j(1) & \cdots & \text{last: } A_i(4m-4l-1)A_j(0) \\ U^*_{i,j,l}: & \text{first: } A_i(4m-4l-2)A_j(4m-1) & \cdots & \text{last: } A_i(4m-4l-1)A_j(0). \end{array}$$

Proof. Recall that $A_iA^l_j$ is the list:

$$A_i(0)A_j(4l+1),\ A_i(1)A_j(4l+2),\ \ldots,\ A_i(4m-4l-2)A_j(4m-1),$$

$$A_i(4m-4l-1)A_j(0),\ A_i(4m-4l)A_j(1),\ \ldots,\ A_i(4m-1)A_j(4l).$$

Let $U_{i,j,l}$ be the list $A_iA^l_j$, rotated $-4l$ positions:

$$U_{i,j,l} \ = \ A_i(4m-4l)A_j(1),\ \ldots,\ A_i(4m-4l-1)A_j(0).$$

By Corollary 12, $U_{i,j,l}$ satisfies the required properties.

Let $U^*_{i,j,l}$ be the list $A_iA^l_j$, rotated $-4l-1$ positions and then reversed:

$$U^*_{i,j,l} \ = \ \text{reverse}[A_i(4m-4l-1)A_j(0), \ldots A_i(4m-4l-2)A_j(4m-1)].$$

Again, by Corollary 12, $U^*_{i,j,l}$ satisfies the required properties. $\square$

Lemma 16 *For fixed i, j, $0 \le i, j < 2^{m-k}$, there is a (not necessarily cyclic) AGC listing, $T_{i,j}$, with signature $(+)^{2m}(-)^{2m}$, of the $2m$-bit strings in all the lists*

$$\{A_i|A^l_j \mid \ 0 \le l < m\}.$$

$T_{i,j}$ has first and last elements as follows:

$$\begin{array}{lllll} T_{i,i}: & \text{first: } A_i(0)A_i(1) & \cdots & \text{last: } A_i(3)A_i(0) \\ T_{i,j}, i \ne j: & \text{first: } A_i(4m-4(j-i)-2)A_j(4m-1) & \cdot & \\ & & \cdots \text{ last: } A_i(4m-4(j-i)+3)A_j(0). & \end{array}$$

Proof. Define $T_{i,i}$ by

$$T_{i,i} \ = \ \ U_{i,i,0},\ U_{i,i,1},\ \ldots, U_{i,i,m-1}.$$

(See Figure 2.) Then using Lemma 15, and recalling that arguments are taken modulo $4m$, we have, as claimed:

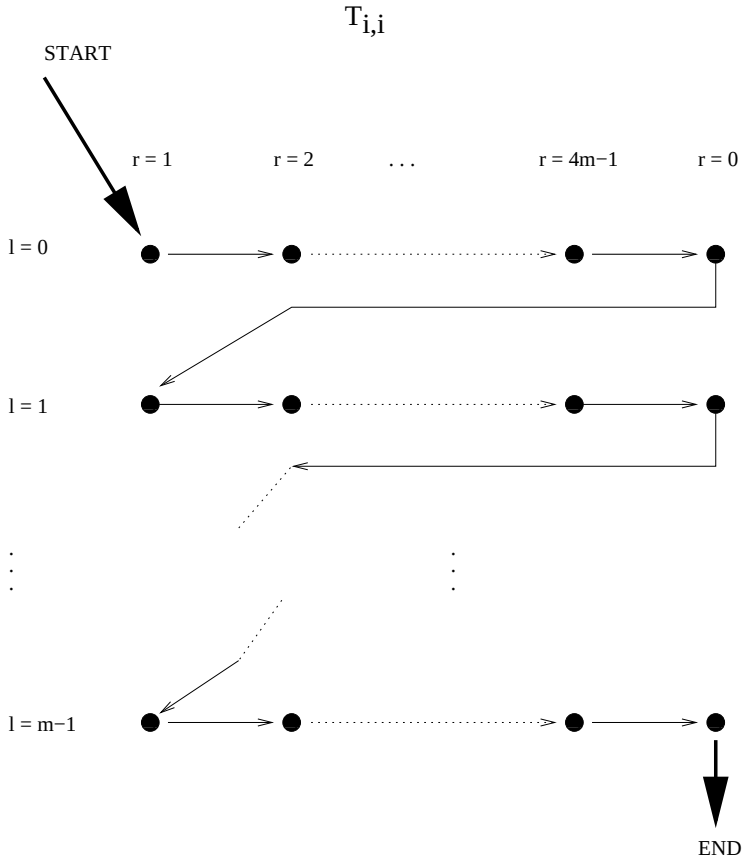

Fig. 2. Construction of $T_{i,i}$. Row l represents the list $U_{i,j,l}$. The dot in row l, column r, represents the 2^k-bit string $A_i(4m-4l+r-1)A_j(r)$.

$$\begin{aligned}\text{first element of } T_{i,i} &= \text{first element of } U_{i,i,0}\\ &= A_i(4m)A_i(1) = A_i(0)A_i(1);\\ \text{last element of } T_{i,i} &= \text{last element of } U_{i,i,m-1}\\ &= A_i(4m-4(4m-1)-1)A_i(0) = A_i(3)A_i(0).\end{aligned}$$

To check the boundaries between consecutive sublists of $T_{i,i}$, for $0 \le i < m-1$,

$$\begin{aligned}\text{last element of } U_{i,i,l} &= A_i(4m-4l-1)A_i(0);\\ \text{first element of } U_{i,i,l+1} &= A_i(4m-4l-4)A_i(1),\end{aligned}$$

which, by Lemma 14(i), differ in only one bit.

For $i \neq j$, let $t = j - i \bmod m$ and define $T_{i,j}$ by

$$T_{i,j}: \quad U^*_{i,j,t},\ U_{i,j,t+1},\ \ldots, U_{i,j,m-1},\ U_{i,j,0},\ U_{i,j,1},\ \ldots, U_{i,j,t-1}.$$

(See Figure 3.) Then by Lemma 15, we have, as claimed:

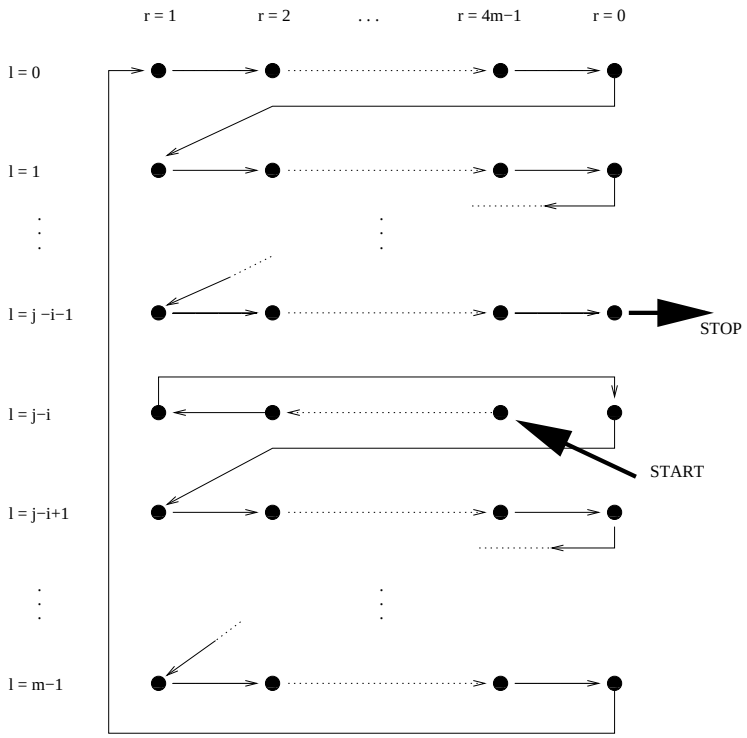

Fig. 3. Construction of $T_{i,j}$ when $i \neq j$. For $l \neq j-i$, row l represents the list $U_{i,j,l}$. The traversal of row $l = j-i$ shown represents the list $U^*_{i,j,j-i}$. The dot in row l, column r, represents the 2^k-bit string $A_i(4m-4l+r-1)A_j(r)$.

$$\begin{aligned}\text{first element of } T_{i,j} &= \text{first element of } U^*_{i,j,j-i}\\ &= A_i(4m-4(j-i)-2)A_j(4m-1);\\ \text{last element of } T_{i,j} &= \text{last element of } U_{i,j,j-i-1}\\ &= A_i(4m-4(j-i-1)-1)A_j(0) = A_i(4m-4(j-i)+3)A_j(0).\end{aligned}$$

To check the boundaries between consecutive sublists of $T_{i,j}$, if $t \leq l \leq m-1$ or $0 \leq l \leq t-2$, then

$$\begin{aligned}\text{last element of } U_{i,j,l} \text{ or } U^*_{i,j,l} &= A_i(4m-4l-1)A_j(0);\\ \text{first element of } U_{i,j,l+1} &= A_i(4m-4l-4)A_j(1),\end{aligned}$$

which, by Lemma 14(i), differ in only one bit. □

Lemma 17 *If $m = 2^{k-1} \geq 8$, then for fixed i, $0 \leq i < 2^{m-k}$, there is a (not necessarily cyclic) AGC listing, S_i, with signature $(+)^{2m}(-)^{2m}$, of the $2m$-bit*

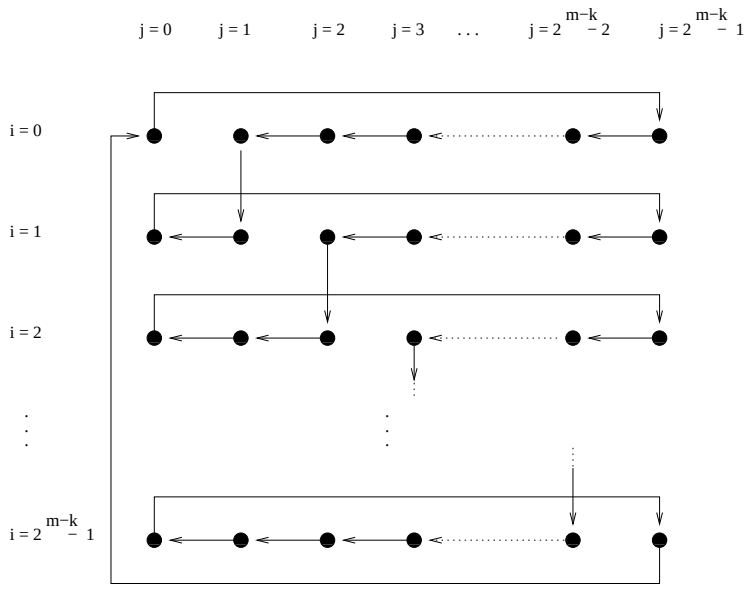

Fig. 4. Construction of the S_i and H. Row i represents list S_i. The dot in row i, column j, represents list $T_{i,j}$.

strings in all the lists

$$\{A_i|A_j^l \mid 0 \le j < 2^{m-k},\ 0 \le l < m\}$$

of the form:

$$S_i: \quad A_i(0)A_i(1),\ \ldots,\ A_i(4m-1)A_{i+1}(0).$$

Proof. Define S_i by

$$S_i \ = \ T_{i,i},\ T_{i,i-1},\ \ldots, T_{i,0},\ T_{i,2^{m-k}-1},\ \ldots, T_{i,i+2},\ T_{i,i+1}.$$

(See Figure 4.) To check the first and last elements of S_i, by Lemma 16,

$$\begin{aligned}\text{first element of } S_i &= \text{first element of } T_{i,i}\\ &= A_i(0)A_i(1);\\ \text{last element of } S_i &= \text{last element of } T_{i,i+1}\\ &= A_i(4m-4(1)+3)A_{i+1}(0) = A_i(4m-1)A_{i+1}(0).\end{aligned}$$

To check whether successive sublists of S_i, are adjacent, first consider $T_{i,0}, T_{i,2^{m-k}-1}$.

$$\begin{aligned}\text{last element of } T_{i,0} &= A_i(4m+4i+3)A_0(0);\\ \text{first element of } T_{i,2^{m-k}-1} &= A_i(4m-4(2^{m-k}-1-i)-2)A_{2^{m-k}-1}(4m-1).\end{aligned}$$

$(A_0|A_0^0;\ 0)$, $(A_0|A_0^1;\ 14)$, $(A_0|A_0^2;\ 12)$, $(A_0|A_0^3;\ 10)$,
$(A_0|A_1^0;\ 8)$, $(A_0|A_1^1;\ 6)$, $(A_0|A_1^2;\ 4)$, $(A_0|A_1^3;\ 2)$,
$(A_1|A_1^0;\ 14)$, $(A_1|A_1^1;\ 12)$, $(A_1|A_1^2;\ 10)$, $(A_1|A_1^3;\ 8)$,
$(A_1|A_0^2;\ 6)$, $(A_1|A_0^3;\ 4)$, $(A_1|A_0^0;\ 0)$, $(A_1|A_0^1;\ 12)$

Fig. 5. An 8-bit antipodal Gray code with signature $(+)^8(-)^8$. The notation $(L;i)$ means that list L is rotated to start at element $L(i)$. (Read across.)

For these to differ in one bit, since $A_0(0)$ and $A_{2^{m-k}-1}(4m-1)$ differ in one bit (they are the first and last elements of the antipodal Gray code G), and $A_i(4m-4(2^{m-k}-1-i)-2) = A_i(4m-4(2^{m-k}-1-i)-2)+1$, we must have, as in Lemma 14(i),

$$(4m-4(2^{m-k}-1-i)-2)+1 \equiv 4m+4i+3 \pmod{4m}.$$

That is, since $m = 2^{k-1}$,

$$2^{m-k+2} \equiv 0 \pmod{4m}.$$

This means that $2^{k-1}-k+2 \geq k+1$, which is true for $k \geq 4$, i.e., for $m \geq 8$, which is given as hypothesis.

To check the remaining list boundaries,

$$\begin{aligned}\text{last element of } T_{i,j} &= A_i(4m-4(j-i)+3)A_j(0);\\ \text{first element of } T_{i,j-1} &= A_i(4m-4(j-1-i)-2)A_{j-1}(4m-1)\\ &= A_i(4m-4(j-i)+2)A_{j-1}(4m-1),\end{aligned}$$

which, by Lemma 14(ii), differ in only one bit. □

Theorem 18 *For every $k \geq 0$, there is a 2^k-bit antipodal Gray code, H, with signature $(+)^{2^k}(-)^{2^k}$.*

Proof. For $k = 0, 1, 2$, H is given in Figure 1. An 8-bit antipodal Gray code, with signature $(+)^8(-)^8$, derived from the $2^2 = 4$-bit antipodal Gray code in Figure 1, is given in Figure 5.

Assume $m = 2^{k-1} \geq 8$ and let G be an m-bit antipodal Gray code with signature $(+)^m(-)^m$. We construct a $2m$-bit antipodal Gray code with signature $(+)^{2m}(-)^{2m}$. As described at the beginning of this section, decompose G into $2^m/(2m) = 2^{m-k}$ sublists of length $2m$,

$$G = B_0, B_1, \ldots, B_{2^{m-k}-1},$$

and construct from each B_i the list

$$A_i = B_i(0), B_i(0), B_i(1), B_i(1), B_i(2), B_i(2), \ldots, B_i(2m-1), B_i(2m-1).$$

By Lemma 13, the lists $A_i A_j^l$, for $0 \leq i, j < 2^{m-k}$ and $0 \leq l < m$, together contain every $2m$-bit string exactly once. By Lemma 17, since $m \geq 8$, there is a (not necessarily cyclic) AGC listing S_i, with signature $(+)^{2m}(-)^{2m}$, of all the $A_i A_j^l$ for each fixed i.

We claim that the list

$$H \;=\; S_0, S_1, \ldots, S_{2^{m-k}-1}$$

is a $2m$-bit antipodal Gray code. (See Figure 4.) Furthermore, its signature is $(+)^{2m}(-)^{2m}$ since this was the case for each of the S_i. It only remains to check the adjacencies at the boundaries of list S_i and S_{i+1} for $0 \leq i < 2^{m-k}$:

$$\begin{aligned} \text{last element of } S_i &= A_i(4m-1)A_{i+1}(0); \\ \text{first element of } S_{i+1} &= A_{i+1}(0)A_{i+1}(1), \end{aligned}$$

which, by Lemma 14(iii), differ in only one bit. □

6 Open Problems and Concluding Remarks

Other than for $n = 6$, when n is even and not a power of 2 it remains open to determine if there exist n-bit antipodal Gray codes. We suspect the answer is no. The smallest value of n in question is $n = 10$ and although exhaustive search may still be feasible, it would be more illuminating to find a proof of nonexistence like the one for odd n, or a construction if the answer is yes.

We include two suggestions from one of the referees. First, for *every* n, there is an antipodal $2n$-cycle on the n-cube, namely one whose flip sequence is $1, 2, \ldots, n, 1, 2, \ldots, n$. In extension, we may ask which values of $k > n$ also have antipodal $2k$-cycles on the n-cube? Similarly, what is the longest antipodal cycle on the n-cube? (Clearly, for ones shown in this paper, it is 2^n.) Second, since any even n which is not a power of 2 can be 'halved' to its odd factor, one might ask, is there a 'halving' operation which can be performed on all such codes, reducing a $2m$-bit code to an m-bit code? This would prove the non-existence of n-bit codes for even n which are not powers of 2, since there is no corresponding code for the odd factor.

Acknowledgements

We are grateful to Hunter Snevily for sharing this problem with us, and to the referees for helpful comments.

References

[1] Gilbert, E. N., Gray codes and paths on the n-cube, Bell System Tech. J 37 (1958) 815–826.

[2] Gray, F., Pulse code communications. U.S. Patent 2632058 (March 1958).

[3] Bultena, Bette and Ruskey, Frank, Transition restricted Gray codes, Electron. J. Combin. 3 (1) (1996) Research Paper 11, 11 pp. (electronic).

[4] Vickers, V. E. and Silverman, J., A technique for generating specialized Gray codes, IEEE Trans. Comput. 29 (4) (1980) 329–331.

[5] Robinson, John P. and Cohn, Martin, Counting sequences, IEEE Trans. Comput. 30 (1) (1981) 17–23.

[6] Ramras, Mark, A new method of generating Hamiltonian cycles on the n-cube, Discrete Math. 85 (3) (1990) 329–331.

[7] Goddyn, Luis and Lawrence, George M. and Nemeth, Evi, Gray codes with optimized run lengths, Utilitas Math. 34 (1988) 179–192.

[8] Savage, Carla D. and Winkler, Peter, Monotone Gray codes and the middle levels problem, J. Combin. Theory Ser. A 70 (2) (1995) 230–248.

[9] Savage, Carla, A survey of combinatorial Gray codes, SIAM Rev. 39 (4) (1997) 605–629.

[10] Donald E. Knuth, Pre-fascicle 2a: Generating all n-tuples, a preview of section 7.2.1.1 of Volume 4 of The Art of Computer Programming, http://www-cs-faculty.stanford.edu/∼knuth/news.html.

[11] Hunter S. Snevily, private email communication, October 13, 2000.