Digital Sequences in Communication and Coding

Tuvi Etzion

Computer Science Department
Technion - Israel Institute of Technology
etzion@cs.technion.ac.il

Fall 2010

Lecture 7 - Gray Codes
Lecture 7 - Outline

- Definition of Gray codes
- Applications
- Single-track Gray codes
- Basic properties
- Constructions based on necklaces and self-dual sequences
- Construction for length $n = 2^m$
- Nonexistence result
- Open problems
Lecture 6 - Gray Codes

Definition

A length $n$ Gray code $C$ is an ordered list of distinct binary $n$-tuples (called the codewords)

$$S_0, S_1, \ldots, S_{p-1}$$

having the property that any two adjacent codewords $S_i$ and $S_{i+1}$ differ in exactly one component. If this property holds for $S_{p-1}$ and $S_0$, as well, we say the Gray code is cyclic with period $p$, the number of different codewords. Otherwise, we say the Gray code is acyclic.
Applications of Gray codes

A typical application for Gray codes is in absolute position sensing and angle measurement. In the angle measurement application, the codewords of a length $n$, period $p$ Gray code are radially arranged around a circle on $n$ tracks (one track for each codeword component), dividing the circle into $p$ segments. By virtue of the distinctness of the codewords, the $n$ bits appearing in a particular segment uniquely identify that segment, and hence the absolute angle corresponding to it (up to some resolution). At angles close to the boundary between two segments, any of the codeword components which change at this boundary are likely to be in error when read. However, in a Gray code, there is only one such component. Moreover, if this component is in error, then the codeword which is read just identifies the neighboring segment. Thus Gray codes have the advantage that the kind of reading errors mentioned above can never result in angular errors that are larger than twice the resolution. Similar considerations apply to acyclic Gray codes used for position sensing.
Applications of Gray codes

One drawback to this approach is that \( n \) tracks (and of course \( n \) reading heads) are required, one for each codeword component. This places a physical limitation on the size of any device making use of such a code, a constraint often undesirable in practice. One way that has been suggested to overcome this is to use sequences having the so-called window property that the subsequences of \( n \) consecutive bits of the sequence are distinct. For example, a maximum-length LFSR sequence can be written on a single track and has the property that any \( n \) consecutive bits of the sequence identify a unique position out of \( 2^n - 1 \). Unfortunately, such sequences do not in general possess the Gray code property required for error resilience.
Single-track Gray Codes

Definition
Let $C$ be a length $n$ cyclic Gray code with codewords $S_0, S_1, \ldots, S_{p-1}$, where $S_i = [s_{i0}, s_{i1}, \ldots, s_{i(n-1)}]$, so that $s_{ij}$ denotes component $j$ of codeword $i$. We call the sequence $s_0^j, s_1^j, \ldots, s_{p-1}^j$ of period $p$, component sequence $j$ of $C$.

Definition
Let $C$ be a length $n$, period $p$ cyclic Gray code. Suppose that for each $1 \leq j < n$, there exists $k_j$ with $0 \leq j < p$ such that component sequence $j$ is a cyclic shift by $k_j$ of component sequence 0, i.e.

$s_0^j, s_1^j, \ldots, s_{p-1}^j = s_{k_j}^0, s_{k_j+1}^0, \ldots, s_{k_j+p-1}^0$

where subscripts are taken modulo $p$. $C$ is called a single-track Gray code.
Basic properties

**Definition**

Let $C$ be a length $n$ Gray code with codewords $S_0, S_1, \ldots, S_{p-1}$ and let $t_i$ with $0 \leq i < p - 1$ denote the unique component in which $S_i$ and $S_{i+1}$ differ (so that $0 \leq t_i < n$). Then the sequence

$$T = t_0, t_1, \ldots, t_{p-2}$$

is called the *coordinate sequence* of $C$. 
Basic properties

**Theorem (1)**

Let \( T = t_0, t_1, \ldots, t_{p-1} \) be a sequence with terms from \( 0, 1, \ldots, n-1 \). \( T \) is the coordinate sequence of length \( n \) Gray code with \( p + 1 \) codewords if and only if, in every subsequence \( t_i, t_{i+1}, \ldots, t_h \) of \( T \) with \( 0 \leq i < h \leq p - 1 \), some symbol occurs an odd number of times. \( T \) is the cyclic coordinate sequence of a length \( n \), period \( p \) Gray code if and only if, in every subsequence \( t_i, t_{i+1}, \ldots, t_h \) of \( T \) with \( 0 \leq i < h \leq p - 2 \), some symbol occurs an odd number of times, while in \( T \) itself, every symbol occurs an even number of times.
Basic properties

Proof

We first consider the case of (noncyclic) coordinate sequence. Suppose that $T$ is the coordinate sequence of a length $n$ Gray code and that in subsequence $t_i, t_{i+1}, \ldots, t_h$ of $T$, every symbol occurs an even number of times. Then in obtaining codeword $S_{h+1}$ from codeword $S_i$, we make an even number of changes in every component of $S_i$. Thus $S_{h+1} = S_i$, contradicting the distinctness of the codewords of a Gray code. On the other hand, suppose that $T$ on the symbols $0, 1, \ldots, n-1$ has the property that in every subsequence $t_i, t_{i+1}, \ldots, t_h$, some symbol occurs an odd number of times. Then, if we choose an arbitrary $n$-tuple $S_0$ and generate a list of $n$-tuples by interpreting $t_i$ as the unique component in which consecutive $n$-tuples $S_i$ and $S_{i+1}$ differ, it is clear that $S_{h+1} \neq S_i$ for every choice of $i, h$. Thus the list of $p+1$ $n$-tuples obtained from $T$ after choosing $S_0$ is a Gray code whose coordinate sequence is $T$. 

Tuvi Etzion - Computer Science Department, Technion
Digital Sequences in Communication and Coding
Basic properties

Proof.
A similar argument also applies to cyclic coordinate sequences, the only difference to note being that the property that every symbol occurs an even number of times in $T$ guarantees that for any $S_0$, a cyclic Gray code with cyclic coordinate sequence $T$ is obtained. □
Basic properties

Lemma (1)

Let $T = t_0, t_1, \ldots, t_{p-1}$ be the cyclic coordinate sequence of a length $n$ period $p$ single-track Gray code. Then for each symbol $j$ with $1 \leq j < n$, the positions where symbol $j$ occurs in $T$ are a cyclic shift of the positions where symbol 0 occurs in $T$. Conversely, if $T$ is a sequence that has this property and the properties of a cyclic coordinate sequence given in Theorem 1, then there exists a choice of $S_0$ such that $T$ is the cyclic coordinate sequence of a single-track Gray code with first codeword $S_0$.

Proof

In a single-track Gray code, each component sequence $(c)^j$ is a cyclic shift by some $k_j$ of $(c)^0$. Symbol $j$ occurs in position $i$ of $T$ if and only if term $i$ and term $i + 1$ of $(c)^j$ differ, or equivalently, term $i + k_j$ and term $i + k_j + 1$ of $(c)^0$ differ. In turn, this holds precisely when symbol 0 occurs in position $i + k_j$ of $T$. Thus we see that the positions where symbol $j$ occurs in $T$ are a cyclic shift (by $k_j$) of the positions where symbol 0 occurs in $T$. 

Tuvi Etzion - Computer Science Department, Technion
Digital Sequences in Communication and Coding
Basic properties

Proof.

Conversely, suppose $T$ has this property and the properties of a cyclic coordinate sequence given in Theorem 1. Then, for any choice of $S_0$, $T$ is the cyclic coordinate sequence of length $n$, period $p$ Gray code whose first codeword is $S_0$. Also, the positions where changes occur in component sequence $(c)_j$ of this code are a cyclic shift by $k_j$ of the positions where changes occur in $(c)_0$. Thus $(c)_j$ is equal to the cyclic shift by $k_j$ of either $(c)_0$ or the complement of $(c)_0$. Whether or not the complement occurs for a specific $j$ depends only on component $j$ of $S_0$, i.e., on $S_0^j$. Therefore, by an appropriate choice of $S_0$ we can ensure that in fact $(c)_j$ is equal to a cyclic shift of $(c)_0$ for every $j$, $1 \leq j < n$. \qed
Basic properties

Lemma

Suppose there exists a length \( n \), period \( p \) single-track Gray code \( C \). Then \( p \) is an even multiple of \( n \) and

\[
2n \leq p \leq 2^n
\]

Proof.

Let \( T \) be the cyclic coordinate sequence of \( C \). Suppose symbol 0 occurs \( r \) times in \( T \). By Theorem 1, \( r \) is even, and by Lemma 1, every symbol 0, 1, \ldots, \( n-1 \) occurs \( r \) times in \( T \). Hence, \( p = nr \) and \( p \) is an even multiple of \( n \). On the other hand, \( C \) is a list of \( p \) distinct \( n \)-tuples, so \( p \leq 2^n \). \( \square \)
Construction based on necklaces

**Theorem**

Let $S_0, S_1, \ldots, S_{r-1}$ be $r$ binary pairwise nonequivalent full-order words of length $n$, such that for each $0 \leq i \leq r-1$, $S_i$ and $S_{i+1}$ differ in exactly one coordinate, and there also exists an integer $\ell$, $\gcd(\ell, n) = 1$, such that $S_{r-1}$ and $E^{\ell}S_0$ differ in exactly one coordinate, then the following words form length $n$, period $nr$ single-track Gray code

<table>
<thead>
<tr>
<th>$S_0$</th>
<th>$S_1$</th>
<th>$\cdots$</th>
<th>$S_{r-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E^{\ell}S_0$</td>
<td>$E^{\ell}S_1$</td>
<td>$\cdots$</td>
<td>$E^{\ell}S_{r-1}$</td>
</tr>
<tr>
<td>$E^{2\ell}S_0$</td>
<td>$E^{2\ell}S_1$</td>
<td>$\cdots$</td>
<td>$E^{2\ell}S_{r-1}$</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>$\vdots$</td>
<td>\vdots</td>
</tr>
<tr>
<td>$E^{(n-1)\ell}S_0$</td>
<td>$E^{(n-1)\ell}S_1$</td>
<td>$\cdots$</td>
<td>$E^{(n-1)\ell}S_{r-1}$</td>
</tr>
</tbody>
</table>
Construction based on necklaces

Example

For \( n = 5 \), the 30 words (without the all-zeros and all-ones words) of length 5 are ordered below based on an order of their 6 necklaces:

\[
\begin{align*}
00001 & \quad 00011 & \quad 10011 & \quad 11011 & \quad 11010 & \quad 10010 \\
00010 & \quad 00110 & \quad 00111 & \quad 10111 & \quad 10101 & \quad 00101 \\
00100 & \quad 01100 & \quad 01110 & \quad 01111 & \quad 01011 & \quad 01010 \\
01000 & \quad 11000 & \quad 11100 & \quad 11110 & \quad 10110 & \quad 10100 \\
10000 & \quad 10001 & \quad 11001 & \quad 11101 & \quad 01101 & \quad 01001 \\
\end{align*}
\]

The sequence of the track: \( 001111,000110,000000,011111,111100 \)

\[
\begin{align*}
0011110001100000000011111111100 \\
00011000000011111111111000011111 \\
000000011111111110001111000110 \\
0111111111000111100011000000000 \\
11110001111000110000000000111111 \\
\end{align*}
\]
Construction based on self-dual sequences

**Theorem (2)**

Let $S_0, S_1, \ldots, S_{r-1}$ be $r$ length $2n$ self-dual pairwise nonequivalent full-order words. Let $S_i = [s^0_i, s^1_i, \ldots, s^{2n-1}_i], 1 \leq i \leq r - 1$, and let

\[
F^j S_i = [s^j_i, s^{j+1}_i, \ldots, s^{j+n-1}_i]
\]

where subscripts are taken modulo $2n$.

If for each $0 \leq i < r - 1$, $S_i$, and $S_{i+1}$ differ in exactly two coordinates, and there also exists an integer $\ell$, $\gcd(\ell, 2n) = 1$, such that $S_{r-1}$ and $E^\ell S_0$ differ in exactly two coordinates, then the following words form a length $n$, period $2nr$ single-track Gray code:

<table>
<thead>
<tr>
<th>$F^0 S_0$</th>
<th>$F^0 S_1$</th>
<th>\ldots</th>
<th>$F^0 S_{r-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F^\ell S_0$</td>
<td>$F^\ell S_1$</td>
<td>\ldots</td>
<td>$F^\ell S_{r-1}$</td>
</tr>
<tr>
<td>$F^{2\ell} S_0$</td>
<td>$F^{2\ell} S_1$</td>
<td>\ldots</td>
<td>$F^{2\ell} S_{r-1}$</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>$F^{(2n-1)\ell} S_0$</td>
<td>$F^{(2n-1)\ell} S_1$</td>
<td>\ldots</td>
<td>$F^{(2n-1)\ell} S_{r-1}$</td>
</tr>
</tbody>
</table>

Tuvi Etzion - Computer Science Department, Technion

Digital Sequences in Communication and Coding
Construction for length $n = 2^m$

Let $S_0, S_1, \ldots, S_{r-1}$ be the set of all full-order self-dual words of length $2n$ and let $\mathcal{Y}(n)$ denote the set of $2^{n-1}$ elements consisting of the $2^{n-1} - 1$ words of the form $[1, y_1, \ldots, y_{n-1}]$, where at least one of the $y_i$'s is a zero, together with the word $[0^n]$. For each $S = [X, \bar{X}]$ of length $2n$ and for every $Y \in \mathcal{Y}(n)$, let

$$S_Y = [Y, X + Y, \bar{Y}, X + \bar{Y}].$$

Lemma

The set of words

$$\bigcup_{i=0}^{r-1} S_i(n), \quad S_i(n) = \bigcup_{Y \in \mathcal{Y}(n)} (S_i)_Y$$

contains $2^{n-1} r$ inequivalent self-dual words of length $4n$. 
Construction for length $n = 2^m$

If $n$ is a power of 2, then there are $r = \frac{2^n}{2n}$ inequivalent full-period self-dual $(2n)$-tuples and these contain all the $n$-tuples as subsequences. Assume that $S_0, S_1 \ldots, S_{r-1}$, the set of all inequivalent self-dual words of length $2n$, are arranged so that the following three properties hold:

C1. For each $i$, $S_i$, and $S_{i+1}$ (subscripts taken modulo $r$) differ in exactly two positions $k$ and $k + n$ (subscripts modulo $2n$).

C2. Let $\text{diff}^*(S_i, S_{i+1})$ denote the first position in which $S_i$ and $S_{i+1}$ differ and let

$$\mathcal{D}_n = \{\text{diff}^*(S_i, S_{i+1}) : 0 \leq i < r - 2\}.$$ 

Then, $\mathcal{D}_n = \{0, 1, \ldots, n - 1\}$

C3. $E(S_{r-2})$ differs in exactly two positions from $S_0$. More precisely, we require

$$S_{r-2} = [0^{n-4}10001^{n-4}0111]$$
$$S_{r-1} = [0^{n-4}10011^{n-4}0110]$$
$$S_0 = [0^{n-4}00011^{n-4}1110]$$
Construction for length $n = 2^m$

### Example (1)

For $n = 4$, the 16 self-dual words of length 16 are ordered below so that Properties C1 to C3 hold

<table>
<thead>
<tr>
<th>$S_0$</th>
<th>[0000000111111110]</th>
<th>$S_8$</th>
<th>[1111000100001110]</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>[1000000101111110]</td>
<td>$S_9$</td>
<td>[1101000100101110]</td>
</tr>
<tr>
<td>$S_2$</td>
<td>[1000001101111100]</td>
<td>$S_{10}$</td>
<td>[1101100100100110]</td>
</tr>
<tr>
<td>$S_3$</td>
<td>[1100001100111100]</td>
<td>$S_{11}$</td>
<td>[0101100110100110]</td>
</tr>
<tr>
<td>$S_4$</td>
<td>[1100011100111000]</td>
<td>$S_{12}$</td>
<td>[0101100010100111]</td>
</tr>
<tr>
<td>$S_5$</td>
<td>[1101011100101000]</td>
<td>$S_{13}$</td>
<td>[0100100010110111]</td>
</tr>
<tr>
<td>$S_6$</td>
<td>[1101010100101010]</td>
<td>$S_{14}$</td>
<td>[0000100011110111]</td>
</tr>
<tr>
<td>$S_7$</td>
<td>[1111010100001010]</td>
<td>$S_{15}$</td>
<td>[0000100111110110]</td>
</tr>
</tbody>
</table>
Lemma (2)

For any $Y \in \mathcal{Y}(n)$ the list of words

$$S(Y) = (S_0)_Y, (S_1)_Y, \ldots, (S_{r-1})_Y$$

satisfies Property $C1$.

Proof.

If $X_i$ and $X_{i+1}$ differ in exactly one position then so do the words $[Y, X_i + Y]$ and $[Y, X_{i+1} + Y]$.
Construction for length $n = 2^m$

**Lemma (3)**

If $Y$ and $Y'$ differ exactly in position $d$ and $\text{diff}^*(S_i, S_{i+1}) = d$ then the list of words

$$(S_i)_Y, (S_{i+1})_Y', (S_{i+2})_Y', \ldots, (S_{r-1})_Y', (S_0)_Y', \ldots, (S_i)_Y', (S_{i+1})_Y$$

satisfies Property C1 above. The first and last pairs of the words differ only in positions $d$ and $d + 2n$, while for every $n \leq d' < 2n$, some pair of consecutive words in the list differ only in positions $d'$ and $d' + 2n$.

**Proof.**

If $S_i = [X_i, \bar{X}_i]$ where $X_i$ and $X_{i+1}$ differ exactly in position $d$ and $Y$ and $Y'$ also differ in exactly position $d$, then

$$X_i + Y = X_{i+1} + Y'$$

and hence $[Y, X_i + Y]$ and $[Y', X_{i+1} + Y']$ differ exactly in position $d$. Similarly, $[Y', X_i + Y']$ and $[Y, X_{i+1} + Y]$ differ exactly in position $d$. The statement about positions $n$ up to $2n - 1$ follows from the construction of the words $(S_j)_Y'$ and Property C2 of $S_0, S_1 \ldots, S_{r-1}$. 

Tuvi Etzion - Computer Science Department, Technion
Digital Sequences in Communication and Coding
Construction for length \( n = 2^m \)

**Lemma (4)**

If the set of self-dual words of length \( 2n = 2^{m+1} \) can be arranged so as to satisfy Properties C1 to C3, then so can the set of self-dual words of length \( 4n \).

**Proof**

We start by forming the list of words \( S(Y) \) for each \( Y \in \mathcal{Y}(n) \), as in Lemma 2. Next, we merge these lists \( S(Y) \) using Lemma 3. We order the words in \( \mathcal{Y}(n) \) as follows: we take \( Y_0 = [0^n] \), \( Y_j = [1^j0^{n-j}] \), \( 1 \leq j \leq n-1 \), and \( Y_n = [10^{n-2}1] \). Then we order the remaining words of \( \mathcal{Y}(n) \) so that each \( Y_i \) differs in exactly one position from some \( Y_j \), \( j < i \). Notice that for \( 1 \leq j < n \), \( Y_j \) differs from \( Y_{j-1} \) in position \( j-1 \), while \( Y_n \) differs from \( Y_1 \) in position \( n-1 \).

We take as the initial main list \( S(Y_0) \). Assume that the lists \( S(Y_1), S(Y_2), \ldots, S(Y_{\ell-1}) \) have been successfully inserted into the main list. We will show that \( S(Y_\ell) \) can also be introduced.
Proof (continue)

Now, there exists a word $Y_j$ with $j < \ell$ such that $Y_j$ and $Y_\ell$ differ in exactly one position, say $d$, and, for some $0 \leq i < r - 2$, there exist a pair of words $S_i = [X_i, \bar{X}_i]$ and $S_{i+1} = [X_{i+1}, \bar{X}_{i+1}]$ such that $X_i$ and $X_{i+1}$ also differ in exactly position $d$. We claim that the words

$$[Y_j, X_i + Y_j, \bar{Y}_j, X_i + \bar{Y}_j] \text{ and } [Y_j, X_{i+1} + Y_j, \bar{Y}_j, X_{i+1} + \bar{Y}_j]$$

still lie adjacent in the main list. For if not, then some list $S(Y_m)$ ($m \neq \ell$) must have been inserted between them. This only occurs if $Y_j$ and $Y_m$ differ in exactly position $d$. This in turn implies that $Y_\ell = Y_m$ – a contradiction, since these words are distinct.

Therefore, we can insert a cyclic shift of the code $S(Y_\ell)$ between the words

$$[Y_j, X_i + Y_j, \bar{Y}_j, X_i + \bar{Y}_j] \text{ and } [Y_j, X_{i+1} + Y_j, \bar{Y}_j, X_{i+1} + \bar{Y}_j]$$

using Lemma 3, extending the main list.
Construction for length $n = 2^m$

Proof.

Executing this process beginning with $S(Y_1)$ and ending with $S(Y_{2^{n-1}-1})$, we obtain a list of all $2^{n-1}r$ inequivalent self-dual words which obviously satisfy Property C1.

Observe that in the above procedure, we never insert any words in positions between the last two words and the first word of the initial set $S(Y_0)$. These three words are:

\[
\begin{align*}
[0^{2n-4}10001^{2n-4}0111], \\
[0^{2n-4}10011^{2n-4}0110], \\
[0^{2n-4}00011^{2n-4}1110].
\end{align*}
\]

Thus, these words remain the last two words and first word of the final list, so that the final list satisfies Property C3.

Examining the last list inserted, we see that Lemma 3 guarantees that there are pairs of consecutive words in the list which differ in positions $n$ up to $2n - 1$. From the choice of words $Y_0, \ldots, Y_n$ and Lemma 3, there are pairs of consecutive words in the list which differ in positions $0$ up to $n - 1$. Hence Property C2 holds.
Construction for length $n = 2^m$

An immediate consequence of Example 1 and Lemma 4 is the following theorem:

**Theorem (3)**

For every $m \geq 3$, there exists an arrangement of the self-dual words of length $2n = 2^{m+1}$ satisfying Properties C1 to C3.

For $m \geq 3$ and $n = 2^m$, let the list of words in Theorem 3 be $S_0, S_1, \ldots, S_{r-1}$, where of course $r = \frac{2n}{2n}$. Consider the list $S_0, S_1, \ldots, S_{r-2}$. Now, for each $0 \leq i < r - 2$, $S_i$ and $S_{i+1}$ differ in exactly two positions, while $ES_{r-2}$ differs in exactly two positions from $S_0$, Thus, Theorem 2 applies (with $\ell = 2n - 1$) to show:

**Theorem**

If $n$ is a power of 2, $n \geq 8$, then there exists a single-track Gray code of length $n$ and period $2^n - 2n$. 
Nonexistence result

Lemma

Let $S$ be a sequence of length $r = p^{\ell_1}$ over $GF(q)$, where $q = p^{\ell_2}$, $p$ prime. Let $S(x)$ be the generating function of $S$. The linear complexity of $S$ is $c$ if and only if

$$(x - 1)^{c-1}S(x) \equiv d(1 + x + x^2 + \cdots + x^{r-1}) \pmod{x^r - 1} \quad (1)$$

for some $d \neq 0$.

Lemma (5)

Let $S$ be a binary sequence of length $m = 2^m$. $S$ is self-dual if and only if $C(S) = 2^{m-1} + 1$.

Theorem

There is no ordering of all the $2^n$ words of length $n = 2^m$, $m \geq 2$, in a list which satisfies all the following requirements.

- Each two adjacent words have different parity.
- The list has the single-track property.
- Each word appears exactly once.
Nonexistence result

Proof (by contradiction)

Let \( s \) be the track of a single-track code in which each \( n \)-tuple appears exactly once and each two adjacent words have different parity. Let \( s(x) \) be the associated polynomial of \( s \) and \( \theta_1 \) the largest integer for which there exists a polynomial \( p_1(x) \) which satisfies

\[
s(x) \equiv (x + 1)^{\theta_1} p_1(x) \pmod{x^{2^n} + 1} \tag{2}
\]

Let \( k_0, k_1, \ldots, k_{n-1} \) be the locations of the heads in the list

\[
h(x) \overset{\text{def}}{=} \sum_{i=0}^{n-1} x^{k_i}
\]

the head locator polynomial of the list, and \( h \) the associated length \( 2^n \) word of \( h(x) \). Let \( \theta_2 \) be the largest integer for which there exists a polynomial \( p_2(x) \) which satisfies

\[
h(x) \equiv (x + 1)^{\theta_2} p_2(x) \pmod{x^{2^n} + 1}. \tag{3}
\]
Nonexistence result

Proof (continue)

Since $x^{2^n} + 1 = (x + 1)^{2^n}$ over GF(2), it follows that $0 \leq \theta_1$, $\theta_2 \leq 2^n - 1$. Since each two adjacent words have different parity it follows that

$$(x + 1)h(x)s(x) \equiv 1 + x + x^2 + \cdots + x^{2^n-1} \pmod{x^{2^n} + 1}. \quad (4)$$

Since $(x + 1)^{2^n} = x^{2^n} + 1$ and

$$(x + 1)^{2^n-1} = 1 + x + x^2 + \cdots + x^{2^n-1} \pmod{x^{2^n} + 1}$$

it follows from (1)-(4) that

$$\theta_1 + \theta_2 = 2^n - 2. \quad (5)$$
Equations (1)-(4) also imply that $\theta_1 + 2$ is the linear complexity of $h$, and $\theta_2 + 2$ is the linear complexity of $s$. Since each word appears in the list exactly once, it follows that $s$ must be of full cyclic order, and hence

$$\theta_2 \geq 2^{n-1} - 1. \quad (6)$$

If we assume that $h$ is not a full-order word, then

$$\{k_i\}_{i=0}^{n-1} = \{2^{n-1} + k_i\}_{i=0}^{n-1}$$

and the $i$th word and the $(i + 2^{n-1})$th word contain exactly the same components of the generating track $s$. The all-zero word appears somewhere in the list, and hence it will appear at least twice, which is a contradiction. Thus, $h$ is of full-order and, therefore, $\theta_1 \geq 2^{n-1} - 1$. 
Nonexistence result

**Proof.**

Self-dual sequences of length $2^n$ have weight $2^{n-1}$ and since $h$ has weight $n$, it is not self-dual when $2^n \geq 4$, and hence by Lemma 5 the linear complexity of $h$ is not $2^{n-1} + 1$. Therefore,

\[ \theta_1 \geq 2^{n-1} \]  

(7)

Summing (6) and (7) we get that

\[ \theta_1 + \theta_2 \geq 2^n - 1 \]

in contradiction to (5). Thus, no such single-track code with track $s$ exists. \qed
Corollary

There are no single-track Gray codes of length $n \geq 3$ and period $2^n$.

Corollary

The single-track Gray codes of length $n = 2^m$ and period $2^n - 2n$ are optimal.
Open problems

- Let $p$ be a prime number. Is there a length $p$, period $2^p - 2$ single-track Gray code? A code based on necklaces is known for $p \leq 19$.

- The middle level problem: is there a Gray code of length $2^{2k+1} \binom{k}{k}$ which contains exactly all the $(2k + 1)$-tuples with weight $k$ and weight $k + 1$?

- What is the longest period of a Gray code in which $|\text{diff}^*(S_i, S_{i+1}) - \text{diff}^*(S_{i+1}, S_{i+2})| = 1$?