# A simple proof for the existence of exponentially balanced Gray codes

I Nengah Suparta*

Department of Applied Mathematics
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
P.O. BOX 5031, 2600 GA Delft, The Netherlands
N.Suparta@ewi.tudelft.nl

Submitted: Apr 21, 2005; Accepted: Sep 9, 2005; Published: Oct 13, 2005
Mathematics Subject Classifications: 94A05, 94A12, 94A15, 94C30

**Abstract**

A Gray code of length $n$ is a circular list of all $2^n$ bitstrings or binary codewords of length $n$ such that successive codewords differ in only one bit position. The frequencies of the positions where these differences occur are called transition counts. An exponentially balanced Gray code is a Gray code the transition counts of which are all the same power of two, or are two successive powers of two. A proof for the existence of exponentially balanced Gray codes is derived. The proof is much simpler than an earlier proof presented by van Zanten and Suparta (Discrete Analysis and Operation Research, 11 (2004) 81-98 (Russian Journal)).

**Keywords:** Gray codes, exponentially balanced Gray codes, transition count spectrum.

## 1 Introduction

A *Gray code* $G(n)$ of length $n$ is a circular list of all $2^n$ bitstrings or binary codewords of length $n$ such that successive codewords differ in one bit position. The frequencies of the positions where these differences occur are called *transition counts* in [2, 4, 11]. If a Gray code is such that any two transition counts differ at most two, one says that this Gray code is *balanced*, and it is called *totally balanced* or *uniform* if all its transition counts are equal (cf. [2, 11]). The transition counts can be called *exponentially close* if they are all the same power of two, or are all two consecutive powers of two. We call a Gray code

*On leave from Dept. of Mathematics, IKIP Negeri Singaraja, Bali - Indonesia with this property an *exponentially balanced* Gray code (cf. [10]), as a generalization of (totally) balanced Gray codes. Thus, for an exponentially balanced Gray code $G(n)$ one has that the transition count of every bit position $i$, $1 \leq i \leq n$, is equal to $2^{e(i)}$ for some positive integer $e(i)$, and $|e(i) - e(j)| \leq 1$, $1 \leq i, j \leq n$. It was proved in [10, Theorem 4] that a Gray code $G(n)$ is totally balanced if and only if $e(i) = e(j)$ for all $i, j$.

In [11], Wagner and West conjectured that exponentially balanced Gray codes exist for all length $n$. By extending the method of Robinson and Cohn for the construction of Gray codes in [5], van Zanten and Suparta in [10] proved the conjecture of Wagner and West in positive sense. In this note we present a proof based on Bakos's construction of Gray codes in [1] which was reformulated in a simple way by Knuth in [4, Theorem D]. This proof is much simpler than the one given in [10].

In the sequel, codewords in a Gray code $G(n)$ will be indexed from 0 to $2^n - 1$. The codeword with index $i$, $0 \leq i \leq 2^n - 1$, is denoted by $\mathbf{x}_i$, whereas $\mathbf{x}_0$ is identified with $\mathbf{x}_{2^n}$. Let $s_i$, $1 \leq i \leq 2^n$, be the bit position where codewords $\mathbf{x}_{i-1}$ and $\mathbf{x}_i$ differ in the list of $G(n)$. We call the integers $s_i$, *transition numbers* or shortly *transitions*. The sequence of transitions $s_i$, $1 \leq i \leq 2^n$, denoted by $\bar{S}(n) := s_1, s_2, ..., s_{2^n}$, is called the *transition sequence* of $G(n)$. The last transition $s_{2^n}$ is occasionally called the *closing transition* of $\bar{S}(n)$. Moreover, we write $\bar{S}(n)^j$, $0 \leq j \leq 2^n - 1$, for the cyclic shift of $\bar{S}(n)$ over $j$ positions to the left. For instance, the 3-bit Gray code $000, 001, 011, 010, 110, 111, 101, 100$, has transition sequence $\bar{S}(3) = 3, 2, 3, 1, 3, 2, 3, 1$, while $\bar{S}(3)^3 = 1, 3, 2, 3, 1, 3, 2, 3$. With respect to the transition sequence of $G(n)$, the transition count of the integer $i$, denoted by $TC_n(i)$, is equal to the number of times the integer $i$ occurs in $\bar{S}(n)$. The distribution $TC_n :=(TC_n(1), TC_n(2), ..., TC_n(n))$ of the transition counts of $G(n)$ is called the *transition count spectrum* of $G(n)$. The above 3-bit Gray code has the transition count spectrum $(2^1, 2^1, 2^2)$.
Sometimes authors prefer to consider the distribution $(\frac{TC_n(1)}{2^n}, \frac{TC_n(2)}{2^n}, ..., \frac{TC_n(n)}{2^n})$ instead of $TC_n$, which is referred to as the *bit error probabilities* of $G(n)$ (see e.g. [3, 6]).

It should be mentioned here that the Gray code constructions in [4, Theorem D], [9], and in [8, 10], which are an extended version of the construction in [5], are all modified versions of a method of Bakos in [1], who proved his results in quite a different context, and who's work was unnoticed for long by authors of articles in the field of ordered codes. Furthermore, we remark that an extension of [4, Theorem D] which holds for the opposite parity of $l$, was introduced in [4, Exercise 50 ] and was also proved in [7, Construction 1].

# 2 A construction of Gray codes

In this note the word *subsequence* (of some sequence $S$) stands for what sometimes is called a *contiguous* or *consecutive* subsequence, i.e. all elements of this subsequence are consecutive in $S$. Let $u$ be a subsequence of $\bar{S}(n)$ which may be empty. We denote by $u^R$ the sequence obtained from $u$ by reversing its order. The following theorem is due to Knuth [4, Theorem D]. The differences in notation and the opposite parity of $l$ compared with the formulation in [4] are due to our convention with respect to the labelling of bit positions and the indexing of codewords as introduced in Section 1.

**Theorem 2.1** *Let $\bar{S}(n) := u_0, j_0, u_1, j_1, ..., u_{l-1}, j_{l-1}, u_l, j_l$ be the transition sequence of an $n$-bit Gray code, where each $j_k$ is a single transition, each $u_k$ is a possibly empty sequence of transitions, and $l$ is even. Then the sequence*

$$\begin{aligned} &u_0, j_0, u_1, ..., j_{l-1}, u_l, n+1, u_l^R, n+2, u_l, n+1, u_l^R, j_{l-1} \\ &\quad u_{l-1}^R, n+1, u_{l-1}, n+2, u_{l-1}^R, j_{l-2} ..., u_1^R, n+1, u_1, n+2, u_1^R, j_0, \\ &\qquad u_0^R, n+2, u_0, n+1, u_0^R, n+2, \end{aligned}$$

*is the transition sequence of an $(n+2)$-bit Gray code.*

In the proof of Theorem 3.1 below, the sequence $j_0, j_1, ..., j_{l-1}$, will be denoted by $T$. Thus, the length of the sequence $T$ is equal to $l$. We emphasize that the sequence $T$ does not include the closing transition $s_{2^n} := j_l$ of $\bar{S}(n)$, as is evident from the notation in Theorem 2.1.

It is easy to observe that the Gray code of length $n+2$ constructed by applying Theorem 2.1, has transition count spectrum $(TC_{n+2}(1), TC_{n+2}(2), ..., TC_{n+2}(n+2))$, with

$$TC_{n+2}(i) := \begin{cases} l+2, & \text{if } i = n+1, n+2, \\ 4TC_n(i) - 2b(i), & \text{if } i \in \{1, ..., n\} \backslash \{s_{2^n}\}, \\ 4(TC_n(i) - 1) - 2b(i), & \text{if } i = s_{2^n}. \end{cases} \tag{1}$$

where $b(i)$ is the number of times the integer $i$ occurs in the sequence $T$. Note that the sum of all $b(i)$, $1 \leq i \leq n$, is equal to $l$, the length of $T$.

# 3 A simple proof for the existence of exponentially balanced Gray codes

As mentioned in Section 1, the existence of exponentially balanced Gray codes was a longstanding conjecture of Wagner and West in [11]. In [10] we introduced a technique how to construct exponentially balanced Gray codes by applying the Robinson-Cohn Gray code construction [5], thus proving the conjecture of Wagner and West,

**Theorem 3.1** *For every $n \geq 1$, there exists an $n$-bit exponentially balanced Gray code, and if $n$ is a power of two, there exists an $n$-bit totally balanced Gray code.*

Here, we shall present a proof using Theorem 2.1. The proof is constructive like the proof in [10], but much simpler.

*Proof:* We accomplish the proof using the principle of mathematical induction. It is obvious that Gray codes of length $1, 2$, and $3$ are exponentially balanced. Assume that an exponentially balanced Gray code $G(n)$ of length $n \geq 3$ exists with transition count spectrum

$$(TC_n(1), TC_n(2), ..., TC_n(n)) := (\underbrace{2^v, ..., 2^v}_{k}, \underbrace{2^{v+1}, ..., 2^{v+1}}_{n-k}), \tag{2}$$

for some $k$ with $0 \leq k < n$. We distinguish two cases: $n - k > 1$ and $n - k = 1$.

Case I. $n - k > 1$. This case implies that $TC_n(n-1) = TC_n(n) = 2^{v+1}$. Let $\bar{S}(n)$ be the transition sequence of $G(n)$, and let $i$ be some integer in $\{0, 1, ..., 2^n - 1\}$ such that the closing transition of $\bar{S}(n)^i$ is the integer $n$. Take a sequence $T$ from the cyclically shifted transition sequence $\bar{S}(n) := \bar{S}(n)^i$ with length $l := 2^{v+2} - 2$, consisting of $2^{v+1} - 2$ occurrences of integer $n$ and all $2^{v+1}$ occurrences of integer $n-1$. Here, $b(1) = \cdots = b(n-2) = 0$, $b(n-1) = 2^{v+1}$, and $b(n) = 2^{v+1} - 2$. Apply Theorem 2.1 with this sequence $T$. Then we obtain a Gray code of length $n+2$ with transition counts satisfying the following (cf. eq. (1))

$$TC_{n+2}(i) := \begin{cases} 2^{v+2}, & \text{for all } i \in \{1, ..., n+2\} \backslash \{k+1, ..., n-2\}, \\ \\ 2^{v+3}, & \text{for all } i \in \{k+1, ..., n-2\}. \end{cases}$$

Thus, the resulting Gray code of length $n+2$ is exponentially balanced with transition count spectrum $(\underbrace{2^{v+2}, \ldots, 2^{v+2}}_{k+4}, \underbrace{2^{v+3}, \cdots, 2^{v+3}}_{n-k-2})$.

Notice that if $n-k = 2$ or equivalently $n+2 = 2^{n-v}$ (a power of two), the resulting $(n+2)$-bit Gray code is *totally* balanced with transition count spectrum $(2^{v+2}, 2^{v+2}, ..., 2^{v+2})$.

Case II. $n - k = 1$. The transition count spectrum (2) now becomes

$$(TC_n(1), TC_n(2), ..., TC_n(n)) := (\underbrace{2^v, \ldots, 2^v}_{n-1}, 2^{v+1}). \tag{3}$$

Here, the transition count of integer $n$ is equal to $2^{v+1}$. Again we assume that $n$ is the closing transition of $\bar{S}(n)^i$, for some integer $i$, $0 \leq i \leq 2^n - 1$. Take a sequence $T$ from $\bar{S}(n) := \bar{S}(n)^i$ consisting of only $2^{v+1} - 2$ occurrences of integer $n$, and then apply Theorem 2.1. The resulting Gray code of length $n+2$ will have transition counts

$$TC_{n+2}(i) := \begin{cases} 2^{v+1}, & \text{if } i = n+1, n+2, \\ \\ 2^{v+2}, & \text{if } i \in \{1, ..., n\}. \end{cases}$$

Again the resulting Gray code of length $n+2$ is exponentially balanced with transition count spectrum $(2^{v+1}, 2^{v+1}, \underbrace{2^{v+2}, \ldots, 2^{v+2}}_{n})$.

We see that in each case the produced Gray code is exponentially balanced. Since exponentially balanced Gray codes of length 1, 2, and 3 exist, the Theorem is proved now by the principle of mathematical induction. □

**Acknowledgements** The author is indebted to Prof. Dr. A.A. Evdokimov (Novosibirsk State University) and Prof. Dr. A.J. van Zanten (Delf University of Technology) for drawing his attention to reference [1]. The author also would like to thank an anonymous referee for suggestions which lead to the final presentation of this article.

# References

[1] A. Ádám, *Truth Functions and the Problem of their Realization by Two-Terminal Graphs,* Akadémiai Kiadó, Budapest 1968.

[2] G.S. Bhat, and C. D. Savage, *"Balanced Gray codes", The Electronic Journal of Combinatorics,* vol. 3 (1996), paper 25.

[3] J.E. Ludman,"Gray code generation for MPSK signal", *IEEE Trans. Comm.,* vol. COM-29, No. 10 (1981), pp. 1519-1522.

[4] Donald E. Knuth, *The Art of Computer Programming, Volume 4*, Addison-Wesley as part of "fascicle" 2, USA, 2005.

[5] J.P. Robinson and M. Cohn,"Counting sequence", *IEEE Trans. Computers,* vol. C-30, No. 1 (1981), pp. 17-23.

[6] Carl-Erik Sundberg, "Bit error probability properties of Gray-coded M.P.S.K. Signals", *Electronics Letters*, vol. 11 (1975), pp. 542-544.

[7] I N. Suparta and A.J. van Zanten, "A construction of Gray codes inducing complete graphs", submitted for publication.

[8] I N. Suparta and A.J. van Zanten, "Balanced Gray codes", *rept. CS 03-03, Institute for Knowledge and Agent Technology, Universiteit Maastricht,* Maastricht, The Netherlands 2003.

[9] Suparta, I N. and A.J. van Zanten, *"A note on balanced Gray codes"*, submitted for publication.

[10] A.J. van Zanten and I N. Suparta, "Totally balanced and exponentially balanced Gray codes", *Discrete Analysis and Operation Research,* vol. 11, No. 4 (2004), pp. 81-98. (Russian Journal)

[11] D.G. Wagner and J. West, "Construction of uniform Gray codes", *Congressus Numerantium,* vol. 80 (1991), pp. 217-223.