TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 1, January 1999, Pages 379–402
S 0002-9947(99)02229-1

COMBINATORIAL FAMILIES THAT ARE EXPONENTIALLY FAR FROM BEING LISTABLE IN GRAY CODE SEQUENCE

TED CHINBURG, CARLA D. SAVAGE, AND HERBERT S. WILF

ABSTRACT. Let $S(n)$ be a collection of subsets of $\{1, ..., n\}$. In this paper we study numerical obstructions to the existence of orderings of $S(n)$ for which the cardinalities of successive subsets satisfy congruence conditions. Gray code orders provide an example of such orderings. We say that an ordering of $S(n)$ is a Gray code order if successive subsets differ by the adjunction or deletion of a single element of $\{1, \ldots, n\}$. The cardinalities of successive subsets in a Gray code order must alternate in parity. It follows that if $d(S(n))$ is the difference between the number of elements of $S(n)$ having even (resp. odd) cardinality, then $|d(S(n))| - 1$ is a lower bound for the cardinality of the complement of any subset of $S(n)$ which can be listed in Gray code order.

For $g \geq 2$, the collection $B(n, g)$ of g-blockfree subsets of $\{1, \ldots, n\}$ is defined to be the set of all subsets S of $\{1, \ldots, n\}$ such that $|a - b| \geq g$ if $a, b \in S$ and $a \neq b$. We will construct a Gray code order for $B(n, 2)$. In contrast, for $g > 2$ we find the precise (positive) exponential growth rate of $d(B(n, g))$ with n as $n \to \infty$. This implies $B(n, g)$ is far from being listable in Gray code order if n is large. Analogous results for other kinds of orderings of subsets of $B(n, g)$ are proved using generalizations of $d(B(n, g))$. However, we will show that for all g, one can order $B(n, g)$ so that successive elements differ by the adjunction *and/or* deletion of an integer from $\{1, \ldots, n\}$.

We show that, over an A-letter alphabet, the words of length n which contain no block of k consecutive letters cannot, in general, be listed so that successive words differ by a single letter. However, if $k > 2$ and $A > 2$ or if $k = 2$ and $A > 3$, such a listing is always possible.

1. INTRODUCTION

1.1. **About Gray codes.** Suppose we have some set S of objects, and we want to make a list of all of the objects in S. An interesting way to do that, particularly if our goal is to design a fast listing algorithm, might be to define a certain set of elementary transformations, and then attempt to make a list of the elements of S in such a way that each element is obtained from its immediate predecessor on the list by a single elementary transformation. That might or might not be possible to do. If it is possible then we may say that a Gray code for this situation does exist, and it is the list that satisfies the conditions stated.

If S is the set of all 2^n of the subsets of a set of n things, we might take for the elementary transformations the operations of adjoining a single element to a set or

Received by the editors February 5, 1997.
1991 *Mathematics Subject Classification.* Primary 11C08, 11L03, 05E99.
Key words and phrases. Gray code, nonexistence.
The first and second authors were supported in part by the National Science Foundation.
The third author was supported in part by the Office of Naval Research.

of deleting a single element from the set. It is possible then, for every n, to list S in Gray code order. For instance when $n = 3$ we have the list

$$S = \{\{\emptyset\}, \{1\}, \{1,2\}, \{2\}, \{2,3\}, \{1,2,3\}, \{1,3\}, \{3\}\}$$

which is an example of the family of codes that was originally found by Frank Gray [4].

One recognizes at once that we are simply asking if a certain graph has a Hamilton path or not, a notoriously difficult problem in graph theory. The vertices are the objects in the set S, and there is an edge from object u to object v if there is an elementary transformation that takes u to v.

It is often natural to consider whole *families* of S at one time, rather than just a single S. Equivalently, one can ask whether every member of a certain family of graphs has a Hamiltonian path. An example is the family of all Cayley graphs associated to pairs (G, T) in which G is a group and T is a set of generators for G. One of the major outstanding problems of the field is to decide whether all such Cayley graphs are Hamiltonian. That is, is it true that we can make a list of the group elements in such an order that each element g is obtainable by the application of a single generator or its inverse to its immediate predecessor? This problem seems very difficult.

For surveys of the general topic of Gray codes, for many more examples of such codes in a variety of combinatorial families, and for pointers to recent literature in the subject we suggest [1, 3, 6, 8].

1.2. **About this paper.** In this paper, we study a numerical obstruction to being able to list in Gray code order a collection of subsets of $\{1, \ldots, n\}$. We show that this obstruction grows exponentially in n for the collection of "g-blockfree" subsets of $\{1, \ldots, n\}$ if and only if $g > 2$. The obstruction in question is one of an infinite family of numerical invariants (described precisely below) which are useful for studying variants of Gray code orders.

We will say that an ordering of a collection $S(n)$ of subsets of $\{1, \ldots, n\}$ is a Gray code order if successive subsets differ by the adjunction or deletion of a single element of $\{1, \ldots, n\}$. The cardinalities of successive subsets in a Gray code order must alternate in parity. Thus one sees that if $d(S(n))$ is the difference between the number of elements of $S(n)$ having even (resp. odd) cardinality, then $|d(S(n))| - 1$ is a lower bound for the cardinality of the complement of any subset of $S(n)$ which can be listed in Gray code order. One should note that there is no guarantee that this lower bound can be achieved.

For $g \geq 2$, define the collection $B(n, g)$ of g-blockfree subsets of $\{1, \ldots, n\}$ to be the set of all subsets S of $\{1, \ldots, n\}$ such that $|a - b| \geq g$ if $a, b \in S$ and $a \neq b$. We will describe explicitly a Gray code order for $B(n, 2)$. In contrast, for $g > 2$ we find the precise (positive) exponential growth rate of $d(B(n, g))$ with n as $n \to \infty$. This provides a lower bound which increases exponentially with n for the size of the complement of any subset of $B(n, g)$ which can be listed in Gray code order. It remains an open question to discover how close one can come to achieving this lower bound. For example, the size of $B(n, g)$ also grows exponentially with n at a rate strictly larger than the growth rate of $d(B(n, g))$. Thus we do not know if one can find for all n a subset of $B(n, g)$ listable in Gray code order whose size is at least a fixed positive fraction of the size of $B(n, g)$.

Given a collection $\mathcal{S} = \{S(n)\}_{n=1}^{\infty}$ as above, we consider the following numerical invariants generalizing the growth rate as $n \to \infty$ of the parity difference function $d(S(n))$. Suppose $v \geq 1$ and that $h : \mathbf{Z} \mapsto \mathbb{C}$ is a nonzero complex valued function which is periodic mod v. If the limit

$$c_{h,\mathcal{S}} = \lim_{n\to\infty} \frac{\log |\sum_{S\in S(n)} h(\#S)|}{n} \tag{1.1}$$

exists and is positive, we will say $\mathcal{S}$ has an *exponential color* at h. If this is true for all nonzero h and $v \geq 1$, we will say $\mathcal{S}$ is *exponentially colorful*. This terminology arises from assigning a color to each residue class modulo v, and from considering the sum $\sum_{S\in S(n)} h(\#S)$ to be the output of a color detector described by h when applied to $S(n)$. The condition $c_{h,\mathcal{S}} > 0$ signifies that the strength of the mixture of colors in the elements of $S(n)$ which is measured by the detector associated to h increases exponentially with n as $n \to \infty$.

Suppose $v = 2$ and that $h_{-1}(j) = (-1)^j$. Then $\sum_{S\in S(n)} h_{-1}(\#S)$ is simply $d(S(n))$, and we have seen $|d(S(n))| \leq 1$ if $S(n)$ can be listed in Gray code order. Thus $\mathcal{S}$ cannot be exponentially colorful if the $S(n)$ have Gray code orders.

In contrast, we will show that $\mathcal{B}(g) = \{B(n, g)\}_{n=1}^{\infty}$ is exponentially colorful for $g > 2$, and we will evaluate the constant $c_{h,\mathcal{B}(g)}$ explicitly for all h. (If $g = 2$ and $\mathcal{S} = \mathcal{B}(2)$ the same calculation shows $c_{h,\mathcal{B}(2)} > 0$ unless h is a constant multiple of the function h_{-1} above.) The proof uses generating functions and results of Fel'dman on linear forms in logarithms of algebraic numbers. This implies, for example, that if $g \geq 2$, $v > 1$, $m, d > 0$ and $(g, v) \neq (2, 2)$, then for sufficiently large n the elements of $B(n, g)$ cannot be listed in such a way that

$$\#a_l \equiv \#a_{l+m} \bmod v \text{ if } l \geq d \tag{1.2}$$

where $\#a_l$ is the cardinality of the l^{th} element a_l on the list. (There is in fact a lower bound which increases exponentially with n for the size of the complement of any subset of $B(n, g)$ which can be listed in this way.) However, we will show in Section 7 that the elements of $B(n, g)$ can be listed so as to satisfy the less stringent adjacency requirement that successive elements differ by the adjunction and/or deletion of an integer from $\{1, \ldots, n\}$.

In Section 8 we show that, over an A-letter alphabet, the words of length n which contain no block of k identical letters cannot, in general, be listed so that successive words differ by a single letter. However, we show in Section 9 that if $k > 2$ and $A > 2$ or if $k = 2$ and $A > 3$, such a listing is always possible.

We note some related work in Section 10.

2. Sets with no consecutive elements

We will say that a set $\{a_1, a_2, \ldots, a_k\}$ with $a_1 < a_2 < \cdots < a_k$ is *blockfree* if $a_{j+1} - a_j > 1$, for all $1 \leq j \leq k - 1$. The blockfree subsets of $\{1, 2, 3, 4, 5\}$, for example, are

$$\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{3, 5\}, \{1, 3, 5\}. \tag{2.1}$$

There are 13 such subsets of $\{1, 2, 3, 4, 5\}$. In general, it is an ancient result that there are F_{n+1}, the Fibonacci number, blockfree subsets of $\{1, \ldots, n\}$, the proof being via the obvious recurrence and initial conditions.

We would like, for a given n, to list these sets in Gray code order, i.e., in a sequence such that we can always pass from a set to its successor by the adjunction

or deletion of a single element. For example, the list (2.1) can be placed in such a sequence as

$$\{1,4\},\{4\},\{2,4\},\{2\},\emptyset,\{1\},\{1,3\},\{3\},\{3,5\},\{1,3,5\},\{1,5\},\{5\},\{2,5\}.$$

This is not hard to do, by taking a cue from the Fibonacci recurrence. We use the notation $[\mathcal{L},\mathcal{L}']$ for the list that is obtained by taking first the elements of the list $\mathcal{L}$ and then those of $\mathcal{L}'$. The list $\overline{\mathcal{L}}$ is $\mathcal{L}$ with its elements listed in reverse order. The list $a\otimes\mathcal{L}$ is obtained by adjoining the element a to each set in the list $\mathcal{L}$.

Consider the lists $\mathcal{L}_0,\mathcal{L}_1,\mathcal{L}_2,\dots$, that are recursively manufactured as follows:

(a) $\mathcal{L}_0=[\emptyset]$ and $\mathcal{L}_1=[\emptyset,\{1\}]$.
(b) For each $n=2,3,\dots$, put $\mathcal{L}_n=[\overline{\mathcal{L}_{n-1}},\, n\otimes\overline{\mathcal{L}_{n-2}}]$.

Theorem 2.1. *The lists $\mathcal{L}_n$, as constructed above, are lists of all of the blockfree subsets of $\{1,\dots,n\}$, in Gray code order. Furthermore, the first member of $\mathcal{L}_n$ is the set H_{n-1}, and its last member is the set H_n, where $H_n=\{n,n-3,n-6,\dots\}$, i.e.,*

$$H_n=\{n-3j : 0\le j\le\lfloor(n-1)/3\rfloor\}.$$

Proof. The proposition is certainly true for $n=0,1$. Suppose it is true for $0,1,\dots,n-1$. Then step (b) of the construction shows that the first and last members of $\mathcal{L}_n$ are as claimed. Since each of the components of step (b) are Gray codes, by induction, it remains only to show that the transition from the last member of the list $\overline{\mathcal{L}_{n-1}}$ to the first member of the list $n\otimes\overline{\mathcal{L}_{n-2}}$ requires only a single adjunction or deletion. In fact, one can readily check that the transition is accomplished simply by adjoining the element n. □

3. A generalization

Say that a set $a_1<a_2<\cdots<a_k$ is *g-blockfree* if $a_{j+1}-a_j\ge g$ for all $1\le j\le k-1$. For $n\ge 0$, $g\ge 1$, let $B(n,g)$ denote the collection of g-blockfree subsets of $\{1,2,\dots,n\}$. Then $B(n,2)$ is just the collection of blockfree subsets of $\{1,\ 2,\ \dots,\ n\}$ from Section 1 and $B(7,3)$ is the set

$$\{\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{5\},\ \{6\},\ \{7\},\ \{1,\ 4\},\ \{1,\ 5\},\ \{1,\ 6\},\ \{1,\ 7\},$$

$$\{2,\ 5\},\ \{2,\ 6\},\ \{2,\ 7\},\ \{3,\ 6\},\ \{3,\ 7\},\ \{4,\ 7\},\ \{1,\ 4,\ 7\}\}.$$

$B(n,g)$ can be recursively defined for $n\ge 0$, $g\ge 1$ by

$$B(n,g)=\begin{cases}\emptyset, & \text{if } n=0;\\ \{\emptyset,\{1\},\{2\},\dots,\{n\}\}, & \text{if } 1\le n\le g;\\ B(n-1,g)\cup n\otimes B(n-g,g), & \text{if } n>g.\end{cases}\tag{3.1}$$

Definition 3.1. Suppose T is an ordered list of subsets of $\{1,\dots,n\}$. Let a_l be the l^{th} element with respect to the given ordering, and let $\#a_l$ be the cardinality of a_l. Let m, v and d be positive integers. We will say the ordering of T is *eventually periodic* mod v of period m starting at position d if

$$\#a_l\equiv\#a_{l+m} \bmod v \text{ if } l\ge d.\tag{3.2}$$

We will say T is in Gray code order if the successor of each element of T differs from that element by the adjunction or deletion of a single element.

Remark 3.2. If T is eventually periodic mod v of period m starting at some position d, then it is also eventually periodic mod v of period m' starting at some position d for every positive integral multiple m' of m. In Theorem 6.4 below we discuss a recurrence condition on an ordering which forces it to be eventually periodic. If T is in Gray code order, then the parities of the orders of successive elements of T must alternate, so T is eventually periodic mod 2 of period 2 starting at position 1.

We can now state our main result concerning Gray code orderings of $B(n, g)$.

Theorem 3.3. *If $g > 2$, then except for finitely many values of n, there cannot be a listing of the g-blockfree subsets of $\{1, 2, \ldots, n\}$ in which the cardinalities of successive sets always have opposite parities. In particular, apart from finitely many n, there cannot be a Gray code ordering of $B(n, g)$. In fact, there is a lower bound which increases exponentially with n for the cardinality of the complement in $B(n, g)$ of any ordered subset T which is in Gray code order.*

This result is a special case of:

Theorem 3.4. *Suppose $g \geq 2$, $v \geq 2$, $m, d > 0$ and $(g, v) \neq (2, 2)$. There are effectively computable constants $c, c' > 0$ which depend on g, v, m and d and which have the following property. If T is an ordered subset of $B(n, g)$ which is eventually periodic mod v of period m starting at position d, then*

$$\#(B(n, g) - T) \geq c' e^{cn} - 1. \tag{3.3}$$

In particular, if n is sufficiently large, it is impossible that $T = B(n, g)$.

The lim sup of the constants c in Theorem 3.4 which result from our method is given in Theorem 7.5. This method relies on numerical invariants of collections of subsets of $\{1, \ldots, n\}$ which are defined in the next section.

4. Colors of collections of subsets of $\{1, \ldots, n\}$

We begin this section by attaching some numerical invariants to collections of subsets of $\{1, \ldots, n\}$.

Definition 4.1. Suppose T is a collection of subsets of $\{1, \ldots, n\}$ and that $v \geq 1$ is an integer. Let $V(v)$ be the $\mathbb{C}$ vector space of all functions $h : \mathbf{Z} \mapsto \mathbb{C}$ which are periodic mod v, i.e. for which $h(a + v) = h(a)$ for all $a \in \mathbf{Z}$. Let $\langle , \rangle$ be the Hermitian inner product on $V(v)$ defined by $\langle h_1, h_2 \rangle = \sum_{j=1}^{v} h_1(j)\overline{h_2(j)}$. Define the color distribution of T to be the function $C(T) \in V(v)$ such that for all $j \in \mathbf{Z}$, $C(T)(j) \in \mathbf{Z}$ is the number of subsets $S \in T$ for which $\#S \equiv j \bmod v$. The color of T with respect to $h \in V(v)$ is defined to be

$$d_h(T) = \sum_{S \in T} h(\#S) = \langle h, C(T) \rangle. \tag{4.1}$$

Example 4.2. Define $h_{\pm 1}(j) = (\pm 1)^j$ for all j. Then $d_{h_1}(T)$ is the cardinality $\#T$ of T, and $d_{h_{-1}}(T)$ is the difference between the number of elements of T of even cardinality and those of odd cardinality.

The following properties of $d_h(T)$ are clear.

Theorem 4.3. *The function $h \mapsto d_h(T)$ is a $\mathbb{C}$-valued linear form on $V(v)$. Let $(\mathbf{Z}/v)^{dual}$ be the character group of $\mathbf{Z}/v$. By character theory, we have*

$$h = \sum_{\chi \in (\mathbf{Z}/v)^{dual}} a_\chi \chi \tag{4.2}$$

for some constants $a_\chi \in \mathbb{C}$ which are uniquely determined by h. Then

$$d_h(T) = \sum_{\chi \in (\mathbf{Z}/v)^{dual}} a_\chi d_\chi(T). \tag{4.3}$$

We will call $d_\chi(T)$ the *primary color* of T associated to $\chi \in (\mathbf{Z}/v)^{dual}$.

Theorem 4.4. *For all collections T and T' of subsets of $\{1, \ldots, n\}$ one has*

$$d_h(T \cup T') = d_h(T) + d_h(T') - d_h(T \cap T'). \tag{4.4}$$

In particular, if $T \subset T'$, then

$$d_h(T') = d_h(T) + d_h(T' - T). \tag{4.5}$$

One has

$$\max\{|h(j)| : j \in \mathbf{Z}\} \cdot \{\#T\} \geq |d_h(T)|. \tag{4.6}$$

The following result is useful for bounding from below the cardinalities of complements of subsets of collections of subsets of $\{1, \ldots, n\}$.

Theorem 4.5. *Suppose T and T' are sets of subsets of $\{1, \ldots, n\}$, $T \subset T'$, and that h is nonzero. Let $M(h) = \max\{|h(j)| : j \in \mathbf{Z}\} > 0$. Then*

$$\#(T' - T) \geq \frac{|d_h(T' - T)|}{M(h)} = \frac{|d_h(T') - d_h(T)|}{M(h)} \geq \frac{||d_h(T')| - |d_h(T)||}{M(h)}. \tag{4.7}$$

The lower bounds in (4.7) are continuous functions of the image $[h]$ of h in the projective space $P_{V(v)} = (V(v) - \{0\})/\sim$, where $h \sim h'$ if $h = ch'$ for some nonzero constant $c \in \mathbb{C}$. Since $P_{V(v)}$ is compact, these lower bounds assume a maximum at some $[h]$.

Proof. This is clear from Theorem 4.4. □

Corollary 1. *Suppose that for some h, $|d_h(T)| \leq M_1$ in Theorem 4.5. Then*

$$\#(T' - T) \geq \frac{|d_h(T')| - M_1}{M(h)}. \tag{4.8}$$

Example 4.6. Suppose T is a subset of $\{1, \ldots, n\}$ which is in Gray code order. Define $h_{-1}(j) = (-1)^j$ for all $j \in \mathbf{Z}$. Then

$$|d_{h_{-1}}(T)| = |\sum_{S \in T} (-1)^{\#S}| \leq 1 \tag{4.9}$$

since the parities of successive elements of T alternate. Thus (4.7) shows

$$\#(T' - T) \geq ||d_{h_{-1}}(T')| - |d_{h_{-1}}(T)|| \geq |d_{h_{-1}}(T')| - 1. \tag{4.10}$$

5. Colorful sequences

Rather than considering $d_h(T)$ for a fixed T, it is useful to consider the asymptotic behavior of $d_h(T)$ as T ranges over some infinite set. The following definition generalizes the one given in the introduction.

Definition 5.1. Let $\mathcal{S} = \{S(n)\}_{n=1}^{\infty}$ be an infinite sequence of collections $S(n)$ of subsets of $\{1, \ldots, n\}$. Let $G : \mathbf{Z} \mapsto \mathbf{R}$ be a function such that $\lim_{n\to\infty} G(n) = +\infty$. Suppose $v \geq 1$ and that $h : \mathbf{Z} \mapsto \mathbb{C}$ is a nonzero function which is periodic mod v. Let $\log^+(r) = \max(\log(r), 0)$ for $r \geq 0$. Define

$$c^+(h, G, \mathcal{S}) = \lim_{n\to\infty} \sup \frac{\log^+ |d_h(S(n))|}{G(n)} \tag{5.1}$$

and

$$c^-(h, G, \mathcal{S}) = \lim_{n\to\infty} \inf \frac{\log^+ |d_h(S(n))|}{G(n)}. \tag{5.2}$$

If these limits (which lie in $\mathbf{R}_{\geq 0} \cup \{\pm\infty\}$) are equal, we will denote their common value by $c(h, G, \mathcal{S})$. We will say that $\mathcal{S}$ *has a color* at h with respect to G if $c(h, G, \mathcal{S})$ exists and is positive.

Example 5.2. If $G(n) = n$ for all n, we will call $c(h, G, \mathcal{S})$ the *exponential color* of $\mathcal{S}$ at h, which we will abbreviate to $c_{h,\mathcal{S}}$.

Example 5.3. The most intrinsic choice of $G(n)$ is $G(n) = \log \#S(n)$, provided $\lim_{n\to\infty} \#S(n) = \infty$. If $c(h, G, \mathcal{S})$ exists in this case, we will call it the *natural color* of $\mathcal{S}$ at h. Note that $c^+(h, G, \mathcal{S}) \leq 1$ when $G(n) = \log \#S(n)$, since $\log^+ |\sum_{S\in S(n)} h(\#S)| \leq \delta + \log \#S(n)$ for some constant δ which depends only on h, and $G(n) \to \infty$ by assumption.

The following result clarifies the variation of color functions with h.

Theorem 5.4. *Recall that $V(v)$ is the $\mathbb{C}$ vector space of all functions $h : \mathbf{Z} \mapsto \mathbb{C}$ which are periodic mod v (cf. Definition 5.1). Fix G as in Definition 5.1. For all $q \in \mathbf{R} \cup \{\infty\}$, the subset*

$$V(v, q) = V(v, q, \mathcal{S}) = \{h \in V(v) : c^+(h, G, \mathcal{S}) \leq q\} \tag{5.3}$$

is a $\mathbb{C}$-subspace of $V(v)$. These subspaces form a nondecreasing filtration of $V(v) = V(v, \infty, \mathcal{S})$. The breaks in the filtration occur at a finite subset $\{q_1, q_2, \ldots, q_d\}$ of $\{q \in \mathbf{R} : q > 0\} \cup \infty$ of cardinality $d \leq dim_{\mathbb{C}} V(v) = v$. On ordering the q_i so $0 < q_1 < q_2 < \cdots < q_d$, we have distinct subspaces

$$V(v, 0) \subset V(v, q_1) \subset V(v, q_2) \subset \ldots \subset V(v, q_d) = V(v, \infty) = V(v) \tag{5.4}$$

with $V(v, q) = V(v, q_i)$ if $q_i \leq q < q_{i+1}$, where we let $q_0 = 0$.

Definition 5.5. The sequence of ordered pairs $\{(q_i, V(v, q_i))\}_i$ appearing in (5.4) will be called the *upper color spectrum* of $\mathcal{S}$ with respect to G. Call $V(v, 0)$ the *nullspace* of $\mathcal{S}$ mod v.

Proof of Theorem 5.4. Suppose $\alpha_1, \alpha_2 \in \mathbb{C}$ and that $h_1, h_2 \in V(v)$. For $h = \alpha_1 h_1 + \alpha_2 h_2$, one has $d_h(S(n)) = \alpha_1 d_{h_1}(S(n)) + \alpha_2 d_{h_2}(S(n))$. Therefore

$$log^+|d_h(S(n))| \leq \delta + \max(log^+|d_{h_1}(S(n))|, log^+|d_{h_2}(S(n))|) \tag{5.5}$$

for some constant δ which depends only on α_1 and α_2. Since $G(n) \to \infty$ as $n \to \infty$, equations (5.1) and (5.5) show

$$c^+(h, G, \mathcal{S}) \leq \max(c^+(h_1, G, \mathcal{S}), c^+(h_2, G, \mathcal{S})). \tag{5.6}$$

This implies $V(v, q)$ in (5.3) is a $\mathbb{C}$-subspace of $V(v)$, and the remaining assertions in Theorem 5.4 follow from this. □

6. Almost periodic collections of subsets

Definition 6.1. Suppose T is a collection of subsets of $\{1, \ldots, n\}$. Let m and v be positive integers. Recall from Definition 4.1 that $C(T) : \mathbf{Z} \mapsto \mathbf{Z}$ is defined by letting $C(T)(j)$ be the number of subsets $S \in T$ for which $\#S \equiv j \bmod v$. The *almost periodicity of T mod v with respect to the period m* is defined to be the smallest nonnegative real number $s_m(T)$ having the following property. For each $j \in \mathbf{Z}$, there are $C_m(T)(j) \in \mathbf{Z}$ and $E_m(T)(j) \in \mathbf{R}$ such that

$$-s_m(T) \leq E_m(T)(j) \leq s_m(T)$$

and

$$C(T)(j) = \frac{\#T}{m} \cdot C_m(T)(j) + E_m(T)(j). \tag{6.1}$$

Lemma 6.2. *One has $s_m(T) \leq \frac{\#T}{2m}$. For each integer $j \in \mathbf{Z}$, the integers $C_m(T)(j)$ and $E_m(T)(j)$ in (6.1) are uniquely determined provided we require $E_m(T)(j) = \frac{\#T}{2m}$ if $|E_m(T)(j)| = \frac{\#T}{2m}$. Let $C_m(T)$ and $E_m(T)$ be the resulting functions from $\mathbf{Z}$ to $\mathbf{R}$. Then $C_m(T)$ and $E_m(T)$ are periodic mod v, and $0 \leq C_m(T)(j) \leq m$ for all j.*

Proof. Given j, there are unique $a \in \mathbf{Z}$ and $b \in \mathbf{R}$ such that $-\frac{\#T}{2m} < b \leq \frac{\#T}{2m}$ and $C(T)(j) = \frac{\#T}{m}a + b$. Hence $E_m(T) \leq \frac{\#T}{2m}$, and $C_m(T)(j)$ and $E_m(T)(j)$ are unique provided we require $E_m(T)(j) = \frac{\#T}{2m}$ if $|E_m(T)(j)| = \frac{\#T}{2m}$. Since $C(T)$ is periodic, so are $C_m(T)$ and $E_m(T)$. Finally, $0 \leq C(T)(j) \leq \#T$ and $|C_m(T)(j) - \frac{m}{\#T}C(T)(j)| \leq 1/2$, so $0 \leq C_m(T)(j) \leq m$ since $C_m(T)(j)$ is an integer.

We now discuss some examples of T of bounded almost periodicity. □

Theorem 6.3. *Suppose that T is periodic mod v of period m starting at position d, in the sense of Definition 3.1. Then*

$$s_m(T) \leq m + d - 1. \tag{6.2}$$

Thus eventually periodic sequences have almost periodicity bounded by a function of m and d alone.

Proof. We can find an initial interval T_0 of elements in the ordering of T such that $\#T_0 \leq d - 1 + m$ and so that as a runs over $T - T_0$, the congruence class $\#a \bmod v$ runs over an integral number of periods of length m. Thus $C(T)(j) = \beta_j \cdot \frac{\#T - \#T_0}{m} + \lambda_j$ for some integers $0 \leq \beta_j \leq m$ and $0 \leq \lambda_j \leq d - 1 + m$. Therefore

$$C(T)(j) = \frac{\#T}{m} \cdot \beta_j + (\frac{-\#T_0 \cdot \beta_j}{m} + \lambda_j) = \frac{\#T}{m}\beta_j + \epsilon_j \tag{6.3}$$

where

$$-(d - 1 + m) \leq \frac{-\#T_0 \cdot \beta_j}{m} \leq \epsilon_j \leq \lambda_j \leq d - 1 + m. \tag{6.4}$$

Now (6.4) and Definition 6.1 give (6.2). □

Theorem 6.4. *Suppose $v \geq 2$ and that T is an ordered collection of subsets of $\{1, \ldots, n\}$. Let a_l be the l^{th} element of T with respect to the given ordering, and let $b_l = \#a_l \bmod v$. If T is periodic mod v of period m starting at position d, then $b_l = b_{l-m}$ for $l \geq d + m$. Conversely, suppose there are integers $l_0 \geq l_1 > 0$ such that for all $l \geq l_0$, b_l depends only on the sequence $b_{l-l_1}, \ldots, b_{l-1}$. There is an integer m so $0 < m \leq v^{l_1}$ such that T is periodic mod v of period m starting at position $l_0 + v^{l_1}$.*

Proof. The first statement is clear from Definition 6.1. Suppose now that there are l_0 and l_1 as in Theorem 6.4. By the pigeonhole principle, there are integers l_2 and l_3 with $l_0 \leq l_2 < l_3 \leq l_0 + v^{l_1}$ such that $(b_{l_3-l_1}, \ldots, b_{l_3-1}) = (b_{l_2-l_1}, \ldots, b_{l_2-1})$. The hypothesis of the converse statement in Theorem 6.4 now implies $b_l = b_{l+l_3-l_2}$ if $l \geq l_2$. Hence we may let $m_1 = l_3 - l_2 \leq v^{l_1}$. □

Lemma 6.5. *Suppose $h \in V(v)$. Then with the notation of Definition 6.1,*

$$|\langle h, C(T)\rangle - \frac{\#T}{m}\langle h, C_m(T)\rangle| \leq s_m(T) \cdot v \cdot M(h) \tag{6.5}$$

when $M(h) = \max\{|h(j)| : j \in \mathbf{Z}\}$, where $\langle h, C(T)\rangle = d_h(T)$.

Proof. For $h \in V(v)$ one has

$$d_h(T) = \sum_{S \in T} h(\#S) = \langle h, C(T)\rangle = \sum_{j=1}^{v} h(j) \cdot C(T)(j) \tag{6.6}$$

by Definition 4.1. We now sum over $j = 1, \ldots, v$ the product of $h(j)$ with the right side of (6.1) to have

$$\langle h, C(T)\rangle - \frac{\#T}{m}\langle h, C_m(T)\rangle = \sum_{j=1}^{v} h(j) \cdot E_m(j). \tag{6.7}$$

Since $|E_m(j)| \leq s_m(j)$ for all j, (6.7) gives (6.5). □

Corollary 2. *If $h \in V(v)$ and $\langle h, C_m(T)\rangle = 0$, then*

$$|d_h(T)| = |\langle h, C(T)\rangle| \leq s_m(T) \cdot v \cdot M(h). \tag{6.8}$$

Thus if $T \subset T'$ for some collection T' of subsets of $\{1, \ldots, n\}$, and $h \neq 0$, then (4.7) implies

$$\#(T' - T) \geq \frac{|d_h(T')|}{M(h)} - s_m(T) \cdot v. \tag{6.9}$$

Definition 6.6. Let $V_m(v) \subset V(v)$ be the finite set of functions $C : \mathbf{Z} \mapsto \mathbf{Z}$ that are periodic mod v and take values in $\{0, \ldots, m\}$. Let $G : \mathbf{Z} \mapsto \mathbf{R}$ be a function such that $\lim_{n\to\infty} G(n) = \infty$. For each $C \in V_m(v)$, define

$$b_G(C) = \sup\{c^-(h, G, \mathcal{S}) : h \in V(v), M(h) = 1 \text{ and } \langle h, C\rangle = 0\}$$

where $M(h) = \max\{|h(j)| : j \in \mathbf{Z}\}$, $c^-(h, G, \mathcal{S})$ is defined as in Definition 5.1 and $\langle , \rangle$ is the usual Hermitian inner product on $V(v)$. Let $b_G : V_m(v) \mapsto \mathbf{R} \cup \{\infty\}$ be the resulting function $C \mapsto b_G(C)$.

Example 6.7. Suppose $c(h, G, \mathcal{S})$ is well defined for all $h \in V(v)$. Then $c(h, G, \mathcal{S}) = c^-(h, G, \mathcal{S})$ is determined by where h lies in the filtration

$$V(v, 0) \subset V(v, q_1) \subset V(v, q_2) \subset \ldots \subset V(v, q_d) = V(v, \infty) = V(v) \tag{6.10}$$

described in Theorem 5.4. Let $H(C) = \{h \in V(v) : \langle C, h\rangle = 0\}$, so $H(C)$ is a hyperplane in $V(v)$ if $C \neq 0$. We find $b_G(C) = \inf\{q : H(C) \subset V(v,q)\}$ must be either q_d or q_{d-1}, since (6.10) is an increasing filtration of vector spaces and $H(C)$ has codimension 0 or 1 in $V(v)$.

Theorem 6.8. *Suppose $m > 0$, $v \geq 2$ and $d > 0$. Let $\mathcal{S} = \{S(n)\}_{n=1}^{\infty}$ be given. Let C be one of the finitely many elements of $V(v,m)$, and suppose $r < b_G(C)$ in the notation of Definition 6.6. There is a constant $c_0 > 0$ depending only on m, v, d, C, r for which the following is true. Suppose that T is an ordered subset of $S(n)$ so that the almost periodicity $s_m(T)$ of T mod v with respect to the period m satisfies $s_m(T) \leq d$. Then if $C_m(T) = C$, we have $\#S(n) - T \geq c_0 e^{rG(n)} - 1$.*

Proof. Suppose T is as in the statement of the theorem and $C_m(T) = C$. By Definition 6.6, there is an $h \in V(v)$ such that $M(h) = 1$, $\langle h, C\rangle = \langle h, C_m(T)\rangle = 0$ and $c^-(h, G, \mathcal{S}) > r$. From Corollary 2 we have

$$\#(S(n) - T) \geq |d_h(S(n))|/M(h) - s_m(T) \cdot v \geq e^{\log^+ |d_h(S(n))|} - 1 - dv. \tag{6.11}$$

If $r \leq 0$, then we can choose c_0 so the required lower bound $\#S(n) - T \geq c_0 e^{rG(n)} - 1$ is trivial. Suppose $r > 0$. Then $c^-(h, G, \mathcal{S}) > r > 0$ implies $\log^+ |d_h(S(n))| > rG(n) > 0$ for n sufficiently large. Hence (6.11) shows that any $c_0 > 0$ will suffice for n sufficiently large, so if $c_0 > 0$ is sufficiently small, we will have the required lower bound for all n. □

7. The color of $B(n, g)$

To state precisely our main result concerning $d_h(B(n,g))$, we require

Definition 7.1. Suppose ω is a root of unity and $g \geq 2$. Define $f_\omega(x) = 1 - x - \omega x^g$. Let r_ω be the minimal absolute value of a (real or complex) root of $f_\omega(x)$. Suppose now that $h : \mathbf{Z} \mapsto \mathbb{C}$ is a periodic function mod v for some integer $v \geq 2$. By (4.3), we can write

$$d_h(T) = \sum_{\chi \in (\mathbf{Z}/v)^{dual}} a_\chi \; d_\chi(T) \tag{7.1}$$

for some constants a_χ which are uniquely determined by h. If $h = 0$ let $r_h = 0$, and otherwise define

$$r_h = \min\{r_{\chi(1)} : \chi \in (\mathbf{Z}/v)^{dual} \quad \text{and} \quad a_\chi \neq 0\}. \tag{7.2}$$

Theorem 7.2. *Suppose $g \geq 2$ and $v \geq 2$ are integers. Let $h : \mathbf{Z} \mapsto \mathcal{C}$ be a nonzero function which is periodic mod v. Define $h_{-1}(j) = (-1)^j$ for all $j \in \mathbf{Z}$. If $g = 2$ and $h = c \cdot h_{-1}$ for some constant c, then $r_h = 1$ and*

$$d_h(B(n,g)) = c \cdot d_{h_{-1}}(B(n,g)) \in \{0, c, -c\}. \tag{7.3}$$

In this case, the exponential color $c_{h,\mathcal{B}(g)} = c(h, G, \mathcal{B}(g))$ of $\mathcal{B}(g) = \{B(g,n)\}_{n=1}^{\infty}$ at h with respect to the function $G(n) = n$ is 0 (cf. Example 5.2). Suppose now that $g \neq 2$ or that $h \neq c \cdot h_{-1}$ for all constants c. Then $r_h < 1$ and

$$c_{h,\mathcal{B}(g)} = \lim_{n \to \infty} \frac{\log |d_h(B(n,g))|}{n} = -\log r_h > 0. \tag{7.4}$$

The convergence of the limit (7.4) can be shown effectively.

Corollary 3. *The sequence $B(g) = \{B(n,g)\}_{n=1}^{\infty}$ is exponentially colorful, in the sense of §1, if and only if $g > 2$.*

Concerning the constants $c_{h,\mathcal{B}(g)}$ we will prove:

Theorem 7.3. *Suppose $g \geq 2$ and $v \geq 2$. Let χ and χ' be characters of $\mathbf{Z}/v$. Define $\overline{\chi} = \chi^{-1}$ to be the complex conjugate of χ. Then $c_{\chi,\mathcal{B}(g)} = c_{\chi',\mathcal{B}(g)}$ if and only if $\chi' = \chi$ or $\overline{\chi}$. If χ_1 is the trivial character, then*

$$c_{\chi,\mathcal{B}(g)} \leq c_{\chi_1,\mathcal{B}(g)} \tag{7.5}$$

with equality if and only if $\chi = \chi_1$. Let $\omega(\rho) = e^{2\pi i\rho}$. As ρ increases from 0 to $1/2$, the function $r_{\omega(\rho)} \leq 1$ is monotonically increasing.

Remark 7.4. As in Theorem 4.3, $|d_\chi(B(n,g))|$ is the strength of the primary color of $B(n,g)$ which is associated to the character χ. Theorems 7.2 and 7.3 show that the rate of growth with n of the strength $|d_h(B(n,g))|$ of an arbitrary color of $B(n,g)$ can be determined in the following way. First write $h = \sum_\chi a_\chi \chi$ as a linear combination of characters, and assume $h \neq 0$. There will be a character χ for which $c_{\chi,\mathcal{B}(g)}$ is maximal among all χ which appear in h, i.e. for which $a_\chi \neq 0$. This χ will be unique if $a_{\overline{\chi}} = 0$ and will be determined up to complex conjugation otherwise. As $n \to \infty$, the linear combination

$$\sum_{\xi = \chi \text{ or } \overline{\chi}} a_\xi d_\xi(B(n,g)) \tag{7.6}$$

of primary colors becomes the dominant term in the formula (4.3) for $d_h(B(n,g))$, and

$$c_{h,\mathcal{B}(g)} = c_{\chi,\mathcal{B}(g)} = c_{\overline{\chi},\mathcal{B}(g)}. \tag{7.7}$$

Putting together Remark 7.4, Theorem 7.3 and Theorem 7.2 shows

Corollary 4. *The upper color filtration*

$$V(v,0) \subset V(v,q_1) \subset V(v,q_2) \subset \ldots \subset V(v,q_d) = V(v,\infty) = V(v) \tag{7.8}$$

of Theorem 5.4 when $\mathcal{S} = \mathcal{B}(g)$ can be described in the following way. If $g = 2$ and v is even, there are $d = v/2$ breaks in the filtration, and $V(v,0) = \mathbb{C} \cdot h_{-1}$. If $g > 2$ or v is odd, there are $d = 1 + [\frac{v}{2}]$ breaks in the filtration, where $[x]$ is the greatest integer less than x, and $V(v,0) = \{0\}$. Let $\zeta = \exp(\frac{2\pi\sqrt{-1}}{v})$. In all cases, for $i = 0, \ldots, d-1$, one has $q_{d-i} = -log|r_{\zeta^i}|$, where r_ω is defined as in Definition 7.1. The subspace $V(v,q_{d-i})$ is the $\mathbb{C}$-linear span of the characters χ of $\mathbf{Z}/v$ for which $\chi(1) = \zeta^j$ and $v - i \geq j \geq i$.

The proofs of Theorems 7.2 and 7.3 will be given in the next sections. In view of Theorem 6.3, the following result strengthens Theorem 3.4, which implies Theorem 3.3 by Example 4.6.

Theorem 7.5. *Suppose $g \geq 2$, $v \geq 2$, $d, m > 0$ and that $(g,v) \neq (2,2)$. Let $r_\zeta < 1$ be the minimal absolute value of a root of $1 - x - \zeta x^g$ when $\zeta = e^{\frac{2\pi\sqrt{-1}}{v}}$. Suppose $0 \leq r < -log|r_\zeta|$. There is a constant $c_0 > 0$ depending on g, m, v, d, r for which the following is true. Suppose that T is an ordered subset of $S(n)$ so that the almost periodicity $s_m(T)$ of T mod v with respect to the period m satisfies $s_m(T) \leq d$. Then*

$$\#S(n) - T \geq c_0 e^{rn} - 1.$$

Proof. This is clear from Example 6.7 and Theorem 6.8. □

In view of Theorem 6.4, Theorem 3.4 gives

Corollary 5. *Suppose g, v and m are as in Theorem 3.4, and that $l_0 \geq l_1 > 0$ are integers. If n is sufficiently large, it is impossible to list the elements of $B(n,g)$ so that for $l \geq l_0$, b_l depends only the sequence $b_{l-l_1}, \ldots, b_{l-1}$, where b_j is the residue class mod v of the cardinality of the j^{th} element of $B(n,g)$.*

Example 7.6. Suppose $(g,v) \neq (2,2)$. Theorem 3.3 shows that for n sufficiently large, there is no way to list the elements of $B(n,g)$ so that the difference of the cardinalities of successive elements lies in a fixed residue class mod v.

Remark 7.7. The lower bound on $\#(B(n,g) - T)$ found in Theorem 7.5 grows at a strictly smaller exponential rate than $\#B(n,g)$ as $n \to \infty$. This will be the case, for example, if the eventually periodic ordering of T results from the assumption that T has a Gray code order. It thus remains an interesting open question whether $\frac{\#T}{\#B(n,g)}$ must tend to 0 as $n \to \infty$ if T is a subset of $B(n,g)$ having a Gray code order.

8. Feasibility and enumeration

Theorem 8.1. *For integer $g \geq 1$, let $f(n,g,k)$ be the number of g-blockfree subsets of $\{1,2,\ldots,n\}$ whose cardinality is k. Then we have*

$$\begin{aligned} F_g(x,y) \quad &\text{def} \quad \sum_{n,k} f(n,g,k) x^n y^k \\ &= \quad \frac{1 + xy\frac{1-x^{g-1}}{1-x}}{1 - x - yx^g} \\ &= \quad x^{1-g}\left(\frac{1}{1-x-yx^g} - (1 + x + \ldots + x^{g-2})\right). \end{aligned} \tag{8.1}$$

Suppose now that $h : \mathbf{Z} \mapsto \mathbb{C}$ is periodic mod v, so

$$h = \sum_{\chi \in (\mathbf{Z}/v)^{dual}} a_\chi \ \chi \tag{8.2}$$

for some constants a_χ as in (4.2). Then

(8.3)

$$\begin{aligned} \sum_{n \geq 0} d_h(B(n,g))\ x^n &= \sum_{\chi \in (\mathbf{Z}/v)^{dual}} a_\chi F_g(x, \chi(1)) \\ &= \sum_{\chi \in (\mathbf{Z}/v)^{dual}} a_\chi x^{1-g}\left(\frac{1}{1 - x - \chi(1)x^g} - (1 + x + \ldots + x^{g-2})\right). \end{aligned}$$

Proof. It follows immediately from (3.1) above that

$$f(n,g,k) = \begin{cases} f(n-1,g,k) + f(n-g,g,k-1), & \text{if } n > g, k \geq 0; \\ \delta_{k,0} + n\delta_{k,1}, & \text{if } 0 \leq n \leq g, k \geq 0; \\ 0, & \text{if } n < 0 \text{ or } k < 0. \end{cases} \tag{8.4}$$

If we multiply (8.4) by $x^n y^k$ and sum over n, k we obtain the second equality in (8.1) after the usual manipulation. The third equality in (8.1) is then checked by cross multiplying. Now (8.3) follows from (8.1), Definition 4.1 and Theorem 4.3. □

Remark 8.2. The radius of convergence of the power series $(1-x-\chi(1)x^g)^{-1}$ about $x = 0$ is the minimal absolute value $r_{\chi(1)}$ of a root of $1 - x - \chi(1)x^g$. In view of Definition 7.1, this implies r_h is a lower bound for the radius of convergence of the power series on the right side of (8.3). This lower bound is consistent via (8.3) and the root test of freshman calculus with the growth rate for $d_h(B(n, g))$ as $n \to \infty$ which is stated in Theorem 7.2. We cannot prove Theorem 7.2 directly in this way, though, since the radius of convergence of a power series does not determine bounds on all of its coefficients.

To prove Theorems 7.2 and 7.3 we now analyze the coefficients of the power series in (8.3).

Theorem 8.3. *Suppose $g > 1$ and that $|\omega| = 1$. Write*

$$f_\omega(x) = -\omega x^g - x + 1 = -\omega \cdot \prod_{i=1}^{g}(x - \alpha_i(\omega)) \tag{8.5}$$

for some complex numbers $\alpha_i(\omega)$. Let $f'_\omega(x) = -\omega g x^{g-1} - 1$ be the derivative of $f_\omega(x)$. The $\alpha_i(\omega)$ are distinct, not in $\{0, 1\}$, and $f'_\omega(\alpha_i(\omega)) \neq 0$ for all i. One has

$$\frac{1}{f_\omega(x)} = -\sum_{i=1}^{g}\sum_{q\geq 0}\frac{x^q}{\alpha_i(\omega)^{q+1}f'_\omega(\alpha_i(\omega))}. \tag{8.6}$$

For h as in (8.2) and $n \geq g - 1$ one has

$$d_h(B(n, g)) = -\sum_{\chi\in(\mathbf{Z}/v)^{dual}}\sum_{i=1}^{g}\frac{a_\chi}{\alpha_i(\chi(1))^{n+g}f'_{\chi(1)}(\alpha_i(\chi(1)))}. \tag{8.7}$$

Here each of the $\alpha_i(\chi(1))$ are algebraic integers.

Proof. Suppose t is a common root of $f'_\omega(x) = -\omega g x^{g-1} - 1$ and $f_\omega(x)$. Then $0 = gf_\omega(t) - tf'_\omega(t) = (1 - g)t + g$, so $t = g/(g - 1)$. But then $|t| > 1$, so $0 = |f'_\omega(t)| \geq |-\omega g t^{g-1}| - 1 > 0$, which is a contradiction. If follows that $f'_\omega(x)$ and $f_\omega(x)$ have no common roots, so $f_\omega(x)$ has simple roots. Because $f_\omega(0) \neq 0 \neq f_\omega(1)$, none of the $\alpha_i(\omega)$ are in $\{0, 1\}$. Hence by partial fractions we have

$$\begin{aligned}\frac{1}{f_\omega(x)} &= \sum_{i=1}^{g}\frac{1}{(x - \alpha_i(\omega))f'_\omega(\alpha_i(\omega))}\\ &= \sum_{i=1}^{g}\frac{1}{f'_\omega(\alpha_i(\omega))(-\alpha_i(\omega))(1 - (x/\alpha_i(\omega)))}\\ &= -\sum_{i=1}^{g}\sum_{q\geq 0}\frac{x^q}{\alpha_i(\omega)^{q+1}f'_\omega(\alpha_i(\omega))}\end{aligned} \tag{8.8}$$

which proves (8.6). Now (8.7) follows from (4.3). If ω is a root of unity (such as $\chi(1)$), then $\alpha_i(\omega)$ is a root of $x^g + \omega^{-1}x - \omega^{-1}$. Since ω^{-1} is an algebraic integer in this case, so is $\alpha_i(\omega)$. □

Formula (8.7) shows that for a fixed g, $|d_h(B(n, g))|$ is bounded above by an exponential function of n. To determine when exponential growth is in fact achieved, we now analyze the roots of $f_\omega(x)$.

Theorem 8.4. *Suppose $g > 1$ and that $|\omega| = |\omega'| = 1$. Suppose μ (resp. μ') is a root of $f_\omega(x) = -\omega x^g - x + 1$ (resp. $f_{\omega'}(x)$) and $|\mu| = |\mu'| = r$. If $\mu = \mu'$, then $\omega = \omega'$. If $\mu \neq \mu'$, then $\omega' = \overline{\omega}$ and $\mu' = \overline{\mu}$.*

Proof. Note first that neither μ nor μ' is 0, since $f_\omega(0) = f_{\omega'}(0) \neq 0$. If $\mu = \mu'$, then

$$\omega = \frac{1-\mu}{\mu^g} = \frac{1-\mu'}{(\mu')^g} = \omega'. \tag{8.9}$$

Suppose now that $\mu \neq \mu'$. Then since $|\omega| = |\omega'| = 1$,

$$|\mu - 1| = |-\omega\mu^g| = r^g = |-\omega'\mu'^g| = |\mu' - 1|. \tag{8.10}$$

Hence μ and μ' both lie on the circle of radius r about 0 and the circle of radius $|\mu - 1|$ about 1. Since these circles intersect in the two distinct points μ and μ', they must intersect in exactly these two points, which must be nonreal and complex conjugates. Therefore $\mu' = \overline{\mu}$. Hence μ' is a root both of $f_{\omega'}(x)$ and $f_{\overline{\omega}}(x)$, so by what we have already shown, $\omega' = \overline{\omega}$. □

Corollary 6. *If $r = 1$ in Theorem 8.4, then μ must be one of the two (complex conjugate) primitive sixth roots of unity and $\omega = \mu^{5-g}$. Conversely, if μ is a primitive sixth root of unity and $\omega = \mu^{5-g}$, then μ is a root of $f_\omega(x)$.*

Proof. By (8.10), μ must lie on the intersection of the circles of radius $r = 1$ about 0 and 1. The intersection points of these circles are the two primitive sixth roots of unity ζ and $\overline{\zeta}$. Since $\zeta^2 - \zeta + 1 = 0$ and $\zeta^3 = -1$, we have $\omega = \frac{\zeta - 1}{-\zeta^g} = \zeta^{5-g}$. The converse statement is clear. □

Corollary 7. *For $|\omega| = 1$ define r_ω to be the minimal absolute value of a root of $f_\omega(x) = -\omega x^g - x + 1$. Then $r_\omega \leq 1$. Define $\omega(\rho) = e^{2\pi i\rho}$. As ρ increases from 0 to π, $r_{\omega(\rho)}$ is monotonically increasing.*

Proof. The product of the absolute values of the roots of $f_\omega(x)$ is 1, so $r_\omega \leq 1$. We showed in Theorem 8.3 that the roots of $f_\omega(x)$ are simple, so by the implicit function theorem, $r_{\omega(\rho)}$ is a continuous function of ρ. Therefore if $r_{\omega(\rho)}$ is not monotone for ρ in $[0, \pi]$, there exist $\rho \neq \rho'$ in $(0, \pi)$ such that $r_{\omega(\rho)} = r_{\omega(\rho')}$. But Theorem 8.4 shows this implies $\omega(\rho) = \omega(\rho')$ or $\omega(\rho) = \overline{\omega(\rho')}$, which is impossible. Hence $r_{\omega(\rho)}$ is monotone. Finally, if $r_{\omega(\rho)}$ is not increasing with ρ, it must be decreasing, so $r_{\omega(\pi)} = r_{-1}$ would be less than $r_{\omega(0)} = r_1$. However, r_1 is the unique real root of $f_1(x) = -x^g - x + 1 = 0$ in the interval $(0, 1)$. Hence if μ is a root of $f_{-1}(x) = x^g - x + 1 = 0$ and $|\mu| < r_1$, then $1 = |\mu^g - \mu| \leq |\mu|^g + |\mu| < r_1^g + r_1 = 1$. This contradiction completes the proof. □

Corollary 8. *Theorems 7.2 and 7.3 are true if $g = 2$ and $h = c \cdot h_{-1}$ for some constant c.*

Proof. When $g = 2$ and $\omega = -1$ we have $f_\omega(x) = x^2 - x + 1 = (x - \zeta) \cdot (x - \overline{\zeta})$ where $\zeta = \frac{1+\sqrt{-3}}{2}$ is a primitive sixth root of 1. Thus $r_h = 0$ if $c = 0$ and $r_h = 1$ otherwise. For $n \geq g - 1 = 1$, (8.7) gives

$$d_h(B(n,g)) = -\frac{c}{\zeta^{n+g}(2\zeta - 1)} - \frac{c}{\overline{\zeta}^{n+g}(2\overline{\zeta} - 1)} = c\frac{\zeta^{n+g} - \overline{\zeta}^{n+g}}{\sqrt{-3}} \tag{8.11}$$

and this is readily checked to lie in $\{0, c, -c\}$. □

Lemma 8.5. *Suppose $g > 2$ or that $g = 2$ and h is not a constant multiple of h_{-1}. Write*

$$h = \sum_{\chi \in (\mathbf{Z}/v)^{dual}} a_\chi \ \chi \tag{8.12}$$

for some constants a_χ as in (4.2). Let $\mathcal{C}$ be the set of characters χ for which $a_\chi \neq 0$. There is a character $\chi \in \mathcal{C}$ such that $1 > r_h = r_{\chi(1)} = r_{\overline{\chi}(1)} < r_{\chi'(1)}$ for all $\chi' \in \mathcal{C} - \{\chi, \overline{\chi}\}$, where r_h and $r_{\chi(1)}$ are defined in Definition 7.1. There is a root θ of $f_{\chi(1)}(x)$ such that $|\theta| = r_{\chi(1)}$, and $|\theta| < |\mu|$ if $\mu \notin \{\theta, \overline{\theta}\}$ is a root of $f_{\chi'(1)}(x)$ for some $\chi' \in \mathcal{C}$. If $\chi' \in \mathcal{C}$ and $\overline{\theta}$ is a root of $f_{\chi'(1)}(x)$, then $\chi' = \overline{\chi}$. Let χ_1 be the trivial character of $\mathbf{Z}/v$. Then $r_{\chi_1} \leq r_\chi < 1$, with equality if and only if $\chi = \chi_1$.

Proof. The product of the absolute values of the roots of the polynomial $f_{\chi(1)}(x) = -\chi(1)x^g - x + 1$ is equal to 1. By Corollary 6, this polynomial has at most two roots on the unit circle, and if such roots exist they are primitive sixth roots of unity. Hence $r_{\chi(1)} = \min\{|\mu| : f_{\chi(1)}(\mu) = 0\} < 1$ if $g > 2$ or if $g = 2$ and some root of $f_{\chi(1)}(x)$ is not a sixth root of unity. Thus $r_{\chi(1)} < 1$ unless $g = 2$ and $f_{\chi(1)}(\zeta) = -\chi(1)\zeta^2 - \zeta + 1 = 0$ when ζ is a primitive sixth root of unity. Since $\zeta^2 = 1 - \zeta$, we conclude $r_{\chi(1)} < 1$ unless $g = 2$ and $\chi(1) = -1$. Since we have assumed h is not a constant multiple of h_{-1} if $g = 2$, we find $r_h = \min\{r_{\chi(1)} : a_{\chi(1)} \neq 0\} < 1$.

By Theorem 8.4, the only way in which there can be characters χ, χ' such that $f_{\chi(1)}(x)$ and $f_{\chi'(1)}(x)$ have distincts roots μ and μ', respectively, of the same absolute value is for $\mu' = \overline{\mu} \neq \mu$ and $\chi'(1) = \chi(1)^{-1}$. Since $\chi'(1) = \chi(1)^{-1}$ implies $\chi' = \chi^{-1}$, this implies the assertions in Lemma 8.5 concerning θ and μ.

The last statement in the lemma is that $r_{\chi_1} \leq r_\chi < 1$, with equality if and only if $\chi = \chi_1$. This is clear from Corollary 7, since $r_\chi = r_{\overline{\chi}}$. □

Corollary 9. *To complete the proof of Theorems 7.2 and 7.3 it will suffice to show the following. Suppose $g > 2$ or that $g = 2$ and h is not a constant multiple of h_{-1}. Let χ and θ be as in Lemma 8.5, and assume $\overline{\theta} \neq \theta$. Define $A_1 = \frac{a_\chi}{\theta^g \cdot f'_{\chi(1)}(\theta)}$ and $A_2 = \frac{a_{\overline{\chi}}}{\overline{\theta}^g \cdot f'_{\overline{\chi}(1)}(\overline{\theta})}$. It will suffice to show that if $r > r_h = |\theta|$, then there are effectively computable positive constants c_0 and c_1 such that*

$$|A_1\theta^{-n} + A_2\overline{\theta}^{-n}| > c_0 r^{-n} \tag{8.13}$$

for $n > c_1$.

Proof. For large n, the dominant terms on the right-hand side of (8.7) arise from the $\alpha_i(\xi(1))$ of smallest absolute value as ξ ranges over all characters of $\mathbf{Z}/n$ for which $a_\xi \neq 0$. Lemma 8.5 shows the only roots which can contribute to the dominant term are θ and $\overline{\theta}$. If $\overline{\theta} = \theta$, then there is just one dominant term and we are done. If $\overline{\theta} \neq \theta$, then in view of (8.7), the inequality (8.13) will insure that the sum of the terms coming from θ and $\overline{\theta}$ dominates the rest of the terms and has the order of growth required for Theorem 7.2. Theorem 7.3 then follows from Lemma 8.5. □

To produce a lower bound of the form (8.13), we will use the following result of Fel'dman [2] about linear forms in logarithms of algebraic numbers. (Stronger results about linear forms in logarithms are available, but to keep the statement of Theorem 7.2 simple we will leave it to the reader to consider the resulting refinements.)

Theorem 8.6. *Suppose $\tau_1, \ldots, \tau_m, \beta$ are distinct nonzero elements of the algebraic number field K. Let $\ln(z)$ be a fixed branch of the complex logarithm of z. Suppose $\delta > 0$ and*

$$0 < |b_1 \ln(\tau_1) + \cdots b_m \ln(\tau_m) - \ln(\beta)| < \exp(-\delta H) \tag{8.14}$$

for some $b_1, \ldots, b_m \in \mathbf{Z}$, where $H = \max |b_k|$. Then $H < \lambda(1 + \ln C)$, where $C = height(\beta)$ and λ is an effectively computable constant independent of C and H.

Lemma 8.7. *Assume the notations of Corollary 9. The constant A_1 is not zero, and if $|A_2| \neq |A_1|$, then one can produce the required lower bound (8.13). Suppose now that $|A_2| = |A_1|$. Choose a consant c_0 so $1/2 > c_0/|A_1| > 0$. Define $\tau_1 = -1$, $\tau_2 = \theta/\overline{\theta}$ and $\beta = A_1/A_2$. Choose a branch of $\ln(z)$ so that $\ln(\tau_1) = \ln(-1) = \pi i$. One can find effectively computable $c_1 > 0$ and $\delta > 0$ (depending on g) such that if the inequality (8.13) does not hold for some $n > c_1$, then*

$$|b_1 \ln(\tau_1) + n \ln(\tau_2) - \ln(\beta)| < \exp(-\ln(r/r_0)n) < \exp(-\delta H) \tag{8.15}$$

for some integer b_1, where $H = \max(|b_1|, |n|) \geq n$.

Proof. We have $A_1 \neq 0$ by the choice of θ in Corollary 9. If $|A_2| \neq |A_1|$, then

$$|A_1 \theta^{-n} + A_2 \overline{\theta}^{-n}| \geq c_0 |\theta|^{-n} > c_0 r^{-n} \tag{8.16}$$

when $c_0 = ||A_1| - |A_2||$, so we have a lower bound of the required form. Assume now that $|A_1| = |A_2|$. If (8.13) does not hold, then

$$\left| 1 + \frac{A_2}{A_1} (\frac{\overline{\theta}}{\theta})^{-n} \right| \leq \frac{c_0}{|A_1|} \left(\frac{r}{|\theta|} \right)^{-n}. \tag{8.17}$$

This is equivalent to the statement that

$$-\beta^{-1} \cdot \tau_2^n = 1 - t \quad \text{with} \quad |t| \leq \frac{c_0}{|A_1|} \left(\frac{r}{|\theta|} \right)^{-n}. \tag{8.18}$$

Since $0 < c_0/|A_1| < 1/2$ by assumption and $r > |\theta|$, we get $|t| < 1/2$ in (8.18). Thus

$$\left| \sum_{m=1}^{\infty} \frac{-t^m}{m} \right| < \sum_{m=1}^{\infty} |t^m| = \frac{|t|}{1 - |t|} < 2|t| \leq 2 \frac{c_0}{|A_1|} \left(\frac{r}{|\theta|} \right)^{-n} \leq \left(\frac{r}{|\theta|} \right)^{-n}. \tag{8.19}$$

The left-hand side of (8.19) is the absolute value of the principal branch of the complex logarithm at $1 - t$. We now take logs of the equality $-\beta^{-1} \cdot \tau_2^n = 1 - t$ in (8.18) and use the fact that we have chosen the branch ln of the complex logarithm such that $\ln(-1) = \pi i$. This and (8.19) show there is an integer b_1 so

$$| - \ln(\beta) + n \ln(\tau_2) + b_1 \ln(-1)| \leq \left| \sum_{m=1}^{\infty} \frac{-t^m}{m} \right| < \left(\frac{r}{|\theta|} \right)^{-n} = \exp(-\ln(r/|\theta|)n). \tag{8.20}$$

Note that (8.20) can hold for at most one integer b_1 when n is fixed, since the right-hand side of (8.20) is less than 1. Thus to establish (8.15), we only have to show how to specify constants $c_1, \delta > 0$ such that if $n > c_1$ and (8.20) holds for

some (unique) $b_1 \in \mathbf{Z}$, then $-\ln(r/|\theta|)n < -\delta H$, where $H = \max(|b_1|, n)$. Now (8.20) implies

$$|b_1| < \frac{|\ln(\beta)| + n|\ln(\tau_2)| + 1}{\pi}. \tag{8.21}$$

Thus if $n > c_1 = |\ln(\beta)| + 1$, then

$$H = \max(|b_1|, n) < \max(\frac{1 + |\ln(\tau_2)|}{\pi} n, n) \tag{8.22}$$

so we can let

$$\delta = \frac{\ln(r/|\theta|)}{\max(\frac{1+|\ln(\tau_2)|}{\pi}, 1)} > 0. \tag{8.23}$$

□

Corollary 10. *To complete the proof of Theorems 7.2 and 7.3, it will suffice to show that if θ is as in Corollary 9 and $\overline{\theta} \neq \theta$, then $\theta/\overline{\theta}$ is not a root of unity.*

Proof. We first observe that Theorem 8.6 gives an effectively computable upper bound on the $H \geq n$ for which one can have an inequality of the form (8.15) for some $n > c_1$ in which the left-hand side of (8.15) is not equal to 0. Thus in view of Corollary 9 and Lemma 8.7, to complete the proof of Theorem 7.2 we need only show c_1 can be increased in an effectively computable way so that the left side of (8.15) cannot be identically 0 if $n > c_1$. If the left side of (8.15) equals 0, we have on exponentiating that

$$\left(\frac{\theta}{\overline{\theta}}\right)^{2n} = \left(\frac{A_1}{A_2}\right)^2. \tag{8.24}$$

Assume $\theta/\overline{\theta}$ is not a root of unity. If (8.24) holds, then $A_1/A_2 = \pm(\theta/\overline{\theta})^n$ lies in the number field L generated over $\mathbf{Q}$ by θ and $\overline{\theta}$, and A_1/A_2 cannot be a root of unity. One can determine effectively a finite set S of finite places of L such that A_1/A_2 is an S-unit of L. One can furthermore determine effectively a finite set of generators for the group U_S of S-units of L. The torsion subgroup μ_L of U_S is the group of roots of unity in L, and U_S/μ_L is a free finitely generated abelian group. Since A_1/A_2 is not a root of unity, it defines a nonzero element $[A_1/A_2]$ of U_S/μ_L. By expressing $[A_1/A_2]$ in terms of a basis over $\mathbf{Z}$ for U_S/μ_L we can bound the even integers $2n > 0$ for which $[A_1/A_2]$ has a $2n^{th}$ root in U_S/μ_L . This gives an effective way to increase c_1 so that $n > c_1$ implies (8.24) cannot hold, provided we know that $\theta/\overline{\theta}$ is not a root of unity.

In view of Corollary 10, the following result completes the proof of Theorems 7.2 and 7.3, since θ in Corollary 9 is not a root of unity. □

Theorem 8.8. *Suppose $g > 1$, ω is a root of unity, α is a root of $f_\omega(x) = -\omega x^g - x + 1$, and $\overline{\alpha} = \zeta\alpha$ for some nontrivial root of unity ζ. Then α is a primitive sixth root of unity and $\zeta = \alpha^{-2}$.*

Lemma 8.9. *Under the hypotheses of Theorem 8.8,*

$$\alpha = \frac{\zeta^g\overline{\omega} - \omega}{\zeta^g\overline{\omega} - \zeta\omega} \tag{8.25}$$

where $\zeta^g\overline{\omega} - \omega \neq 0 \neq \zeta^g\overline{\omega} - \zeta\omega$.

Proof. Since $\zeta\alpha = \overline{\alpha}$ is a root of $f_{\overline{\omega}}(x) = -\overline{\omega}x^g - x + 1$, we have

$$-\omega\alpha^g - \alpha + 1 = 0 = -\overline{\omega}(\alpha\zeta)^g - \alpha\zeta + 1.$$

Hence

$$-\omega\alpha^g - \alpha = -\overline{\omega}\alpha^g\zeta^g - \alpha\zeta. \tag{8.26}$$

Therefore

$$\alpha^g \cdot (-\omega + \overline{\omega}\zeta^g) = \alpha \cdot (1 - \zeta). \tag{8.27}$$

Since $f_\omega(0) \neq 0$, we see that $\alpha \neq 0$. Hence since $\zeta \neq 1$, (8.27) implies $\alpha^g \cdot (-\omega + \overline{\omega}\zeta^g) \neq 0$. Therefore $\zeta^g\overline{\omega} - \omega \neq 0$, and (8.27) gives

$$-\omega\alpha^{g-1} = (1-\zeta)/(1 - \zeta^g\frac{\overline{\omega}}{\omega}). \tag{8.28}$$

Hence

$$\begin{aligned} 0 &= -\omega\alpha^g - \alpha + 1 \\ &= \alpha \cdot (-\omega\alpha^{g-1} - 1) + 1 \\ &= \alpha \cdot ((1-\zeta)/(1 - \zeta^g\frac{\overline{\omega}}{\omega}) - 1) + 1 \\ &= \alpha \cdot (\zeta^g\frac{\overline{\omega}}{\omega} - \zeta)/(1 - \zeta^g\frac{\overline{\omega}}{\omega}) + 1. \qquad (8.29) \end{aligned}$$

This implies $0 \neq \zeta^g\overline{\omega} - \zeta\omega$, and we now solve (8.29) for α to get (8.25). □

Corollary 11. *Suppose $F = \mathbb{C}$ is the field of complex numbers. Let $\zeta^{1/2}$ be one of the two square roots of ζ, so that $\zeta^{1/2}$ is a root of unity. Then*

$$\beta = \zeta^{1/2}\alpha = \frac{\zeta^{g/2}\overline{\omega} - \zeta^{-g/2}\omega}{\zeta^{(g-1)/2}\overline{\omega} - \zeta^{-(g-1)/2}\omega} \tag{8.30}$$

is a totally real algebraic integer.

Proof. The second equality in (8.30) follows directly from (8.25). It's clear that β is an algebraic integer since α is. Because complex conjugation sends $\zeta^{1/2}$ to $\zeta^{-1/2}$ and $\overline{\omega}$ to ω we see from (8.30) that β is real. Because β lies in the abelian extension $\mathbf{Q}(\zeta, \omega)$ of $\mathbf{Q}$, this implies β is totally real. □

Lemma 8.10. *Suppose τ is a root of $f_{\omega'}(x) = -\omega'x^g - x + 1$ and ω' is a root of unity. If $g > 2$, then $0 < |\tau| < \sqrt{2}$. If $g = 2$, then $0 < |\tau| \leq \frac{1+\sqrt{5}}{2}$, with equality only if $\omega' = 1$ and $\tau = \frac{-1-\sqrt{5}}{2}$.*

Proof. Since $f_{\omega'}(\tau) = -\omega'\tau^g - \tau + 1 = 0$, $f_{\omega'}(0) \neq 0$ and $|\omega'| = 1$, we must have $|\tau| > 0$ and $|\tau|^g \leq |\tau| + 1$. Consider the function $h(r) = r^g - r - 1$. Because $h'(r) = gr^{g-1} - 1 > 0$ for $r > 1$, we see $h(r)$ is an increasing function for $r > 1$. Now $h(\sqrt{2}) = (\sqrt{2})^g - \sqrt{2} - 1 \geq (\sqrt{2})^3 - \sqrt{2} - 1 > 0$ if $g \geq 3$, and $h(\frac{1+\sqrt{5}}{2}) = 0$ if $g = 2$. Therefore since $h(|\tau|) \leq 0$, we conclude that $|\tau| < \sqrt{2}$ if $g \geq 3$, and $|\tau| \leq \frac{1+\sqrt{5}}{2}$ if $g = 2$. Suppose in what follows that $g = 2$ and $|\tau| = \frac{1+\sqrt{5}}{2}$. Then $|\tau|^2 = |\tau| + 1$ and $|\tau|^2 = |-\omega'\tau^g| = |\tau - 1|$. Thus $|\tau| + 1 = |\tau - 1|$, which forces τ to be real and $\tau \leq 0$. Hence $\tau = -\frac{1+\sqrt{5}}{2}$ and $\omega' = (1-\tau)/\tau^2 = 1$. □

Lemma 8.11. *Define $r_0 = \frac{1+\sqrt{5}}{2}$ and $z(x) = (x^2 - 3x + 1) = (x - r_0^2)(x - r_0^{-2})$. For any $\epsilon > 0$, there is an integer $a > 0$ such that $r(x) = (x-2) \cdot (x-1)^a \cdot z(x)^a$ satisfies $|r(x)| < 1$ for $\epsilon < x \leq r_0^2$.*

Proof. Define $t(x) = (x-1)(x^2-3x+1) = x^3-4x^2+4x-1$. By freshman calculus, $-1 < t(x) \le 5/27$ if $0 < x \le r_0^2$ except when $x = 2$, where $t(2) = -1$. Since $x-2$ is bounded on $[\epsilon, r_0^2]$ and vanishes at $x = 2$, the lemma is clear from this. □

Lemma 8.12. *Let β be as in Corollary 11. Then $\beta = \pm 1$.*

Proof. From (8.30) we see that $\beta^2 = \zeta \cdot \alpha^2$ is an algebraic integer because ζ and α are. Corollary 11 shows that β^2 is totally real and totally positive because β is totally real and nonzero. Suppose σ is an automorphism of $\mathbb{C}$ over $\mathbf{Q}$. Then $\sigma(\beta^2) = \sigma(\zeta \cdot \alpha^2) = \sigma(\zeta) \cdot \sigma(\alpha)^2$, where $\sigma(\zeta)$ is a root of unity and $\sigma(\alpha)$ is a root of $f_{\sigma(\omega)}(x)$. Here $\sigma(\omega)$ is a root of unity because ω is. Hence Lemma 8.10 implies

$$0 < |\sigma(\beta^2)| = |\sigma(\alpha)|^2 < 2 \quad \text{if} \quad g > 2 \tag{8.31}$$

and

$$0 < |\sigma(\beta^2)| = |\sigma(\alpha)|^2 \le r_0^2 \quad \text{if} \quad g = 2. \tag{8.32}$$

Since β^2 is totally positive, (8.31) shows that if $g > 2$, $\beta^2 - 1$ is an algebraic integer having all of its conjugates in $(-1, 1)$. The norm of $\beta^2 - 1$ is the product of these conjugates and is a rational integer. Hence this norm must be 0, so $\beta^2 = 1$ and $\beta = \pm 1$.

For the rest of the proof we suppose $g = 2$. Since β^2 is totally positive, (8.32) implies β^2 is an algebraic integer having all of its conjugates in $[\epsilon, r_0^2]$ for some $\epsilon > 0$. Let $r(x) = (x-2) \cdot (x-1)^a \cdot z(x)^a$ be as in Lemma 8.11. We conclude now from Lemma 8.11 that $r(\beta^2)$ is an algebraic integer having all of its conjugates in the real interval $(0, 1)$. The norm of $r(\beta^2)$ must then be a rational integer of norm less than 1 in absolute value, so in fact $r(\beta^2) = 0$. Since $r(x) = (x-2) \cdot (x-1)^a \cdot (x - r_0^2)^a \cdot (x - r_0^{-2})^a$, we conclude that $\beta^2 \in \{1, 2, r_0^2, r_0^{-2}\}$.

If $\beta^2 = 1$, then $\beta = \pm 1$ and we are done. Suppose $\beta^2 = 2$. Then $\beta = \zeta^{1/2}\alpha = \pm\sqrt{2}$, and all conjugates of α have absolute value $\sqrt{2}$. Since α is a root of $-\omega x^2 - x + 1$ and ω is a root of unity, we find that $|-\omega\alpha^2| = 2$ equals $|1 - \alpha|$. Thus α lies on the intersection of the circles $|\alpha| = \sqrt{2}$ and $|1 - \alpha| = 2$, from which one finds $\alpha = (1 \pm \sqrt{-7})/2$. Then $\omega = (1 - \alpha)/\alpha^2$ is a root of unity in $\mathbf{Q}(\sqrt{-7})$, so $\omega = \pm 1$. But then $\alpha = (1 \pm \sqrt{-7})/2$ is not a root of $-\omega x^2 - x + 1$, so we conclude $\beta^2 = 2$ is impossible. If $\beta^2 = r_0^2$, then $\beta = \zeta^{1/2}\alpha = \pm r_0$, so $\alpha = \pm\zeta^{-1/2} r_0$ and $|\alpha| = r_0$. However, it was shown in Lemma 8.10 that $|\alpha| = r_0$ is possible only if $\alpha = -r_0$ and $\omega = 1$. Then $\zeta = \overline{\alpha}/\alpha = r_0/r_0 = 1$, contradicting our assumption that ζ is a nontrivial root of unity. Suppose finally that $\beta^2 = r_0^{-2}$. We find as above that $|\alpha| = r_0^{-1}$. The other root α' of $f_\omega(x) = -\omega x^2 - x + 1$ must have $|\alpha'| = r_0$. Lemma 8.10 now shows $\alpha' = -r_0$ and $\omega = 1$, so $\alpha = r_0^{-1}$. However, then $\zeta = \overline{\alpha}/\alpha = 1$, contrary to hypothesis. The contradiction shows $\beta^2 = r_0^{-2}$ is impossible and completes the proof. □

Proof of Theorem 8.8. Combining Corollary 11 and Lemma 8.12 shows $\alpha = \zeta^{-1/2}\beta = \pm\zeta^{-1/2}$. Hence α is a root of unity, so Theorem 8.8 now follows from Corollary 6. □

9. Pale-Gray codes

If we allow a slight relaxation of our Gray code requirements, we can still obtain a minimal change listing of $B(n, g)$ for all $n \ge 0$, $g \ge 1$: allow successive sets on the list to differ by the adjunction *and/or* deletion of an element. Call such a listing

a *pale-Gray code*. For example, for the set $B(4,3)$, no Gray code can exist since $d(4,3) = -2$. However a pale-Gray code is

$$[\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,\ 4\}].$$

Call two sets *adjacent* if they differ by the adjunction and/or deletion of an element.

For $n \geq 0$ and $g \geq 1$, define the list $\mathcal{L}_{n,g}$ recursively as follows:

(a) $\mathcal{L}_{0,g} = [\emptyset]$.
(b) For $1 \leq n \leq g$, $\mathcal{L}_{n,g} = [\{n\},\ \overline{\mathcal{L}_{n-1,g}}]$.
(c) For $g+1 \leq n < 2g$, $\mathcal{L}_{n,g} = [\{n,\ n-g\},\ \ n \otimes \mathcal{L}_{n-g-1,g},\ \ \overline{\mathcal{L}_{n-1,g}}]$.
(d) For $n \geq 2g$, $\mathcal{L}_{n,g} = [\{n,\ n-g\} \otimes \mathcal{L}_{n-2g,g},\ \ n \otimes \mathcal{L}_{n-g-1,g},\ \ \overline{\mathcal{L}_{n-1,g}}]$.

It follows from one or two applications of (3.1) that $\mathcal{L}_{n,g}$, so defined, is a listing of the elements of $B(n,g)$. We now show that it is a pale-Gray code.

Theorem 9.1. *For $n \geq 0$ and $g \geq 1$, the list $\mathcal{L}_{n,g}$ is a pale-Gray code listing of $B(n,g)$. Furthermore, if $n > 0$, the first member of $\mathcal{L}_{n,g}$ is the set $G_{n,g}$, and its last member is the set $G_{n-1,g}$, where $G_{n,g} = \{n, n-g, n-2g, \dots\}$, i.e.,*

$$G_{n,g} = \{n - jg : 0 \leq j \leq \lfloor (n-1)/g \rfloor\}.$$

Proof. Clearly the theorem holds for $n = 0$. Let $n > 0$ and assume the theorem holds for all $B(m,g)$ with $g \geq 1$ and $0 \leq m < n$.

If $1 \leq n \leq g$, $\mathcal{L}_{n,g}$ is constructed as in step (b). If $n \leq 2$, the theorem follows since step (b) gives $\mathcal{L}_{1,g} = [\{1\},\ \emptyset]$ and $\mathcal{L}_{2,g} = [\{2\},\ \emptyset,\ \{1\}]$. Otherwise, for $2 < n \leq g$, by induction, $\overline{\mathcal{L}_{n-1,g}}$ is a pale-Gray code for $B(n-1,g)$, beginning with $G_{n-2,g} = \{n-2\}$ and ending with $G_{n-1,g} = \{n-1\}$. Since $G_{n,g} = \{n\}$ is adjacent to $\{n-2\}$, the theorem follows.

If $g+1 \leq n < 2g$, the list $\mathcal{L}_{n,g}$ is constructed as in (c). Note that $g \neq 1$ since no n satisfies $2 \leq n < 2$. By induction, $\mathcal{L}_{n-g-1,g}$ and $\mathcal{L}_{n-1,g}$ are pale-Gray codes which start and end with the sets given by the theorem. Then if $g+1 \leq n < g+2$, the theorem follows, since (c) gives

$$\begin{aligned}
\mathcal{L}_{g+1,g} &= [\{g+1,\ 1\},\ (g+1) \otimes \mathcal{L}_{0,g},\ \overline{\mathcal{L}_{g,g}}] \\
&= [\{g+1,\ 1\},\ \{g+1\},\ \{g-1\}, \dots, \{g\}]. \\
\mathcal{L}_{g+2,g} &= [\{g+2,\ 2\},\ (g+2) \otimes \mathcal{L}_{1,g},\ \overline{\mathcal{L}_{g+1,g}}] \\
&= [\{g+2,\ 2\},\ \{g+2,\ 1\},\ \{g+2\},\ \{g\},\ \dots, \{g+1,\ 1\}].
\end{aligned}$$

Otherwise, for $g+2 < n < 2g$, list $n \otimes \mathcal{L}_{n-g-1}, g$ begins with $\{n,\ n-g-2\}$, which is adjacent to $\{n,\ n-g\} = G_{n,g}$, and ends with $\{n,\ n-g-2\}$ which is adjacent to $\{n-2,\ n-g-2\} = G_{n-2,g}$, the first element of $\overline{\mathcal{L}_{n-1,g}}$. Since $\overline{\mathcal{L}_{n-1,g}}$ ends with $G_{n-1,g}$, the theorem follows.

For $n \geq 2g$, the list $\mathcal{L}_{n,g}$ is constructed by step (d) and by induction, lists $\mathcal{L}_{n-2g,g}$, $\mathcal{L}_{n-g-1,g}$ and $\mathcal{L}_{n-1,g}$ are pale-Gray codes which begin and end with the sets specified by the theorem. Specifically,

$$\begin{aligned}
\{n,\ n-g\} \otimes \mathcal{L}_{n-2g,g} &= [\{n,\ n-g\} \otimes G_{n-2g,g}, \dots, \{n,\ n-g\} \otimes G_{n-2g-1,g}] \\
&= [G_{n,g}, \dots, \{n,\ n-g\} \otimes G_{n-2g-1,g}].
\end{aligned}$$

(Note that if $n = 2g$, this list contains only one set, namely $\{n, n-g\}$.) Similarly,

$$\begin{aligned}
n \otimes \mathcal{L}_{n-g-1,g} &= [n \otimes G_{n-g-1,g}, \dots, n \otimes G_{n-g-2,g}] \\
&= [\{n,\ n-g-1\} \otimes G_{n-2g-1,g}, \dots, n \otimes G_{n-g-2,g}]
\end{aligned}$$

$\{1,4,7,10\}$	$\{3,10\}$	$\{6\}$	$\{4,7\}$
$\{4,7,10\}$	$\{5,10\}$	$\{1,6\}$	$\{1,4,7\}$
$\{2,7,10\}$	$\{1,5,10\}$	$\{1,4\}$	$\{1,4,9\}$
$\{7,10\}$	$\{2,5,10\}$	$\{4\}$	$\{4,9\}$
$\{1,7,10\}$	$\{2,5,8\}$	$\{2\}$	$\{2,9\}$
$\{3,7,10\}$	$\{5,8\}$	$\{\}$	$\{9\}$
$\{3,6,10\}$	$\{1,5,8\}$	$\{1\}$	$\{1,9\}$
$\{2,6,10\}$	$\{1,4,8\}$	$\{3\}$	$\{3,9\}$
$\{6,10\}$	$\{4,8\}$	$\{5\}$	$\{5,9\}$
$\{1,6,10\}$	$\{2,8\}$	$\{1,5\}$	$\{1,5,9\}$
$\{1,4,10\}$	$\{8\}$	$\{2,5\}$	$\{2,5,9\}$
$\{4,10\}$	$\{1,8\}$	$\{2,7\}$	$\{2,6,9\}$
$\{2,10\}$	$\{3,8\}$	$\{7\}$	$\{6,9\}$
$\{10\}$	$\{3,6\}$	$\{1,7\}$	$\{1,6,9\}$
$\{1,10\}$	$\{2,6\}$	$\{3,7\}$	$\{3,6,9\}$

FIGURE 1. The pale-Gray code listing of $\mathcal{L}_{10,3}$ resulting from the construction of Theorem 9.1.

and

$$\begin{aligned}\overline{\mathcal{L}_{n-1,g}} &= [G_{n-2,g},\ldots,G_{n-1,g}]\\ &= [(n-2)\otimes G_{n-g-2,g},\ldots,G_{n-1,g}].\end{aligned}$$

The theorem follows by observing the adjacencies between successive composite lists in step (d). □

As an example, Figure 1 shows the pale-Gray code listing of $\mathcal{L}_{10,3}$ resulting from the construction of Theorem 9.1.

10. Blockfree words

Consider a word w over an alphabet $\mathcal{A}$ of A letters. We say that w is k-blockfree if w contains no block of k or more consecutive identical letters. If A, k, and n are fixed, we ask if there exists a Gray code listing of all of the k-blockfree n-letter words over $\mathcal{A}$, where the Gray code condition means that successive words differ in only a single letter.

It turns out that the cases $A = 2$ and $A \geq 3$ are quite different. Consider first $A = 2$, so we are trying to make a list of all strings of n bits that have no blocks of k or more consecutive 0's or 1's, arranged so that consecutive elements of the list differ in a single bit position. For this to be possible it is obviously necessary that the number of such blockfree words that have an even number of 1's differs by at most 1 from the number of such blockfree words that have an odd number of 1's. We will compute this excess as a function of n and k:

$$\sum_h (-1)^h f(n,h,k), \tag{10.1}$$

where $f(n,h,k)$ is the number of n-bit strings that have exactly h 1's, and no block of k or more consecutive 0's or 1's. Let $F(n,h,k)$ be the set counted by $f(n,h,k)$,

let $f_0(n,h,k)$ be the number of bit strings in $F(n,h,k)$ which start with '0' and let $f_1(n,h,k)$ be the number which start with '1'. Since $f_1(n,h,k) = f_0(n,n-h,k)$,

$$\sum_h (-1)^h f(n,h,k) = \begin{cases} 2\sum_h (-1)^h f_1(n,h,k) & \text{if } n \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

We focus on the cases when n is even and show that there are pairs (n,k) for which

$$\sum_h (-1)^h f_1(n,h,k)$$

exceeds 1 and hence also for (10.1).

Let w denote a word in $F(n,h,k)$ that begins with a 1. Let the sizes of the consecutive blocks of 1's and 0's be

$$a_1, b_1, a_2, b_2, \ldots, a_r, b_r$$

in which $r \geq 1$ and

- For all $i = 1, \ldots, r$: $1 \leq a_i \leq k-1$;
- For all $i = 1, \ldots, r-1$: $1 \leq b_i \leq k-1$;
- $0 \leq b_r \leq k-1$;
- $a_1 + \cdots + a_r = h$; $b_1 + \cdots + b_r = n-h$.

The number of such pairs of compositions of h and $n-h$ is evidently ("$[x^m]\{\ldots\}$" is the coefficient of x^m in "$\ldots$")

$$\begin{aligned} &[x^h y^{n-h}](x + x^2 + \cdots + x^{k-1})^r (y + y^2 + \cdots + y^{k-1})^{r-1}(1 + y + y^2 + \ldots y^{k-1}) \\ &\quad = [x^h y^{n-h}] x^r y^{r-1} \frac{(1-x^{k-1})^r (1-y^{k-1})^{r-1}(1-y^k)}{(1-x)^r (1-y)^{r-1}(1-y)}, \end{aligned}$$

which is to say that

$$\begin{aligned} \sum_{n,h} f_1(n,h,k) x^h y^{n-h} &= \sum_{r \geq 1} x^r y^{r-1} \frac{(1-x^{k-1})^r (1-y^{k-1})^{r-1}(1-y^k)}{(1-x)^r (1-y)^r} \\ &= \frac{x(1-y^k)(1-x^{k-1})(1-y^{k-1})}{(1-x)(1-y) - xy(1-x^{k-1})(1-y^{k-1})}. \end{aligned}$$

Next, replace x by xy throughout, and then set $x := -1$. This yields

$$\begin{aligned} &\sum_n \left\{ \sum_h (-1)^h f_1(n,h,k) \right\} y^n \\ &\qquad = \begin{cases} -y(1-y^{2k-2})/(1+y^k) & \text{if } k \text{ is even,} \\ -y(1-y^k)(1-y^{k-1})^2/(1-2y^{k+1}+y^{2k}) & \text{if } k \text{ is odd} \end{cases} \end{aligned}$$

which means that the coefficient of y^n in the series on the right is the excess of the number of words with an even number of 1's over the number with an odd number of 1's in our class of k-blockfree bit strings of length n which start with a '1'.

If we now double these generating functions, to take account of the excess among words that start with a '0', we see that when n is even, *a Gray code is possible for n-bit k-blockfree strings, if k is even, only if n is neither $\equiv 1$ mod k nor $\equiv -1$ mod $2k$, and if k is odd, only if the coefficient of y^n in the series*

$$-2y \frac{(1-y^k)(1-y^{k-1})^2}{1-2y^{k+1}+y^{2k}} \tag{10.2}$$

vanishes. Since n is even, a Gray code is not precluded for k even. However, in tabulations for $n = 2, 4, \ldots, 98$, and $k = 3, 5, 7, 9$, we find that for $n \geq k$ in this range, the coefficient of y^n in (10.2) vanishes only for (n, k) in the set

$$\{(5,8),(7,10),(7,11),(7,18),(7,28),(9,12),(9,14),(9,16),$$

$$(9,22),(9,24),(9,26),(9,32),(9,34),(9,42),(9,54)\}.$$

In fact, it appears from more extensive tabulation, that for each odd k, the coefficient of y^n in (10.2) never vanishes once n becomes large enough.

11. Alphabets of more than two letters

If $\mathcal{A} = \{a, b, c\}$, it is not possible to list the 2-blockfree words of length 3 over $\mathcal{A}$. For example, both *bca* and *acb* must be listed between *aca* and *bcb*, the only two words to which they are adjacent. However, for alphabets with more than two letters we do have the following.

Theorem 11.1. *If $k > 2$ and $|\mathcal{A}| \geq 3$ or if $k = 2$ and $|\mathcal{A}| \geq 4$, then the k-blockfree words of length n over $\mathcal{A}$ can be listed so that successive words differ only in a single letter.*

Proof. If $n = 1$, a listing of the elements of $\mathcal{A}$ in any order satisfies the required property. For $n > 1$, assume inductively that there is a Gray code listing

$$\mathcal{L}(n-1) = x_1, x_2, \ldots, x_t$$

of the k-blockfree words of length $n-1$ over $\mathcal{A}$.

Before constructing $\mathcal{L}(n)$, we define from $\mathcal{L}(n-1)$ a sequence $\mathcal{A}_1, \ldots, \mathcal{A}_t$ of subsets of $\mathcal{A}$ and a sequence $y_0, y_1, \ldots y_t$ of letters in $\mathcal{A}$ as follows:

For $i = 1, \ldots, t$, if word x_i of $\mathcal{L}(n-1)$ ends with $k-1$ copies of the letter $z \in \mathcal{A}$, then let $\mathcal{A}_i = \mathcal{A} - \{z\}$; otherwise, let $\mathcal{A}_i = \mathcal{A}$.

Note that if $k > 2$, then since x_i and x_{i+1} differ in only one letter, $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ have at least $|\mathcal{A}| - 1 \geq 2$ elements in common. If $k = 2$, then $|\mathcal{A}_i \cap \mathcal{A}_{i+1}| \geq |\mathcal{A}| - 2 \geq 2$.

Now choose $y_0 \in \mathcal{A}_1$ arbitrarily and for $i = 1, \ldots, t$, successively choose

$$y_i \in (\mathcal{A}_i \cap \mathcal{A}_{i+1}) - \{y_{i-1}\}.$$

Since $|\mathcal{A}_i \cap \mathcal{A}_{i+1}| \geq 2$, there is at least one choice for each y_i.

Now, for each $i = 1, \ldots, t$, let $\mathcal{M}_i$ be a list of the words

$$\{x_i v | v \in \mathcal{A}_i\}$$

starting at $x_i y_{i-1}$ and ending with $x_i y_i$. The concatenation of the lists $\mathcal{M}_i$ gives the required list $\mathcal{L}(n)$:

$$\mathcal{L}(n) = [\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_t].$$

□

12. Remarks

We mention some related work for blockfree words.

In [5], Guibas and Odlyzko give a generating function for the number of words over an alphabet $\mathcal{A}$ which do not contain any of a finite given set of strings. This can be applied to obtain a generating function for the number of k-blockfree n-letter words over $\mathcal{A}$ by choosing the set of patterns to be $\{a^k | a \in \mathcal{A}\}$, from which we must then compute the parity difference to get the result of Section 10.

In [7], Squire studies the existence of Gray codes for n-letter words over $\mathcal{A}$ which do not contain a given string. For the case of k-blockfree words, Squire's results do not apply since we are dealing with a set of several forbidden strings. However, the special structure of these strings allows us to construct a simple Gray code.

It is interesting to note that there are cases where, according to [7], Gray codes do not exist if the forbidden string is a^k for some $a \in \mathcal{A}$, $k > 1$, but, according to our results, do exist when the *set* of forbidden strings is $\{a^k | a \in \mathcal{A}\}$.

Acknowledgment

The first author thanks the I.H.E.S. for its hospitality during part of the preparation of this paper.

References

[1] S. J. Curran and J. A. Gallian, Hamiltonian cycles and paths in Cayley graphs and digraphs - a survey, *Discrete Math.* **156** (1996), 1-18. MR **97f:**05083

[2] N. I. Fel'dman, A certain inequality that is connected with linear forms of logarithms of algebraic numbers, (Russian), *Dokl. Akad. Nauk. SSSR* **207** (1972), 41-43. MR **47:**1755

[3] R. J. Gould, Updating the Hamiltonian problem - a survey, *Journal of Graph Theory* **15**, No. 2 (1991), 121 -157. MR **92m:**05128

[4] F. Gray, Pulse code communication, U. S. Patent 2632058 (1953).

[5] L. J. Guibas and A. M. Odlyzko, String overlaps, pattern matching, and nontransitive games, *Journal of Combinatorial Theory A* **30** (1981) 183-208. MR **82g:**05007

[6] C. D. Savage, A survey of combinatorial Gray codes, *SIAM Review*, **39**, No. 4, to appear Dec. 1997. CMP 98:06

[7] M. B. Squire, Gray codes for A-free strings, *Electronic Journal of Combinatorics* **3**, R17 (1996). MR **97j:**68106

[8] H. S. Wilf, *Combinatorial Algorithms: An Update*, SIAM, Philadelphia, 1989. MR **90g:**05002

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6395

E-mail address: ted@math.upenn.edu

Department of Computer Science, North Carolina State University, Raleigh, North Carolina 27695-8206

E-mail address: cds@cayley.csc.ncsu.edu

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6395

E-mail address: wilf@math.upenn.edu