7-2001

Constructing Critical Indecomposable Codes

Judy L. Walker
University of Nebraska - Lincoln, judy.walker@unl.edu

Published in IEEE Transactions on Information Theory, vol 47 , iss 5 (July 2001) , pp 1780-1795
DOI: 10.1109/18.930918

Constructing Critical Indecomposable Codes

Judy L. Walker

Abstract

Critical indecomposable codes were introduced by Assmus [1], who also gave a recursive construction for these objects. One of the key ingredients in the construction is an *auxiliary code*, which is an indecomposable code of minimum distance at least 3. In terms of actually being able to construct all critical indecomposable codes, however, Assmus leaves many unanswered questions about these auxiliary codes. In this paper, we provide answers to these questions, including a description of when two equivalent auxiliary codes can yield inequivalent critical indecomposable codes, and results on both the minimum length and the maximum number of critical columns of an auxiliary code. We end with an enumeration of all critical indecomposable codes of dimension at most 10.

Keywords

Automorphism group, canonical form, category, generator matrix, indecomposable, linear code.

I. Introduction

The study of error-correcting codes was given a strong impulse in 1948 with Shannon's ground-breaking paper [10]. Very early on, people took an abstract approach to this topic, and in the late 1950's Slepian [11] introduced a structure theory for binary linear codes. In particular, Slepian developed many of the ideas necessary for one to define the Grothendieck ring of the category of binary linear codes, although Roos [9] was the first to explicitly discuss this ring about five years later. Slepian's notion of "sum" is the same as the one we use below: for linear codes C and D of lengths m and n respectively, $C \oplus D$ is the code of length $m+n$ consisting of all codewords of the form $(c|d)$, where $c \in C$ and $d \in D$. Though we won't need it, we mention that Slepian's notion of "product" is the *direct* or *Kronecker product*, as described in [7].

It was Slepian's intent to show that every code is equivalent to a code which has a generator matrix in a certain canonical form. Alas, this is not true, but Slepian did manage to make some significant contributions nonetheless. Perhaps most importantly, he developed the idea of an *indecomposable code*, that is, a code which is not isomorphic to a nontrivial direct sum of two other codes. He proved two important things in this direction: First, every code is isomorphic to a unique sum of indecomposable codes. Second, for a given length and dimension, there is an indecomposable code which achieves the highest possible minimum distance.

The problem with indecomposable codes is that there are simply too many of them. It is easy to see that for a code to be indecomposable is the same thing as the code not being equivalent to a code which has a generator matrix which is block diagonal with at least two blocks. Thus, if C is any indecomposable code, then appending any column vector onto any generator matrix for C yields a new indecomposable code of the same dimension but having length equal to one more than the length of C. This left Slepian unable to achieve his original goal, and in fact, not much new was contributed to the idea of a structure theory for linear codes for about thirty years. (See, however, [2] and [4].)

The major breakthrough came in the late 1990's when Assmus ([1]) introduced the notion of *critical indecomposable* codes. The idea is that these codes are indecomposable codes with no "extra" columns tacked on. More precisely, an indecomposable code is critical indecomposable if puncturing at any column yields a code which either is decomposable or has dimension less than the dimension of the original code. A critical indecomposable code which can be obtained by puncturing an indecomposable code at one or more columns is said to be in the *spectrum* of that indecomposable code. The notion of critical indecomposable codes appears to be very promising. In fact, Assmus shows that there is a "quasi-canonical" form for the generator matrix of such a code, and this seems to be the closest that one can hope to get to Slepian's original goal. Further, Assmus gives a recursive construction for all critical indecomposable codes.

It is that construction which is the topic of this paper. There are two ingredients which go into the construction: a partition of the intended length of the code, and a so-called *auxiliary* code, which is an indecomposable code of smaller dimension having minimum distance at least 3 and a certain number (determined by the partition) of *critical columns*. While the problem of finding all possible partitions is trivial, the problem of finding all possible auxiliary codes was left wide-open in [1]. Further, as mentioned in [1], two equivalent auxiliary codes, when used with the same partition, might yield inequivalent critical indecomposable codes.

In this paper, we study these auxiliary codes as a means of clarifying Assmus's construction of critical indecomposable codes. In Section II, we review some of the major definitions and results from [1], including a description of the construction of critical indecomposable codes. In Section III, we study the question of when equivalent auxiliary codes can yield inequivalent critical indecomposable codes and give a complete answer to it. The shortest critical indecomposable code of dimension l has length $l+1$, and in Section IV we study the question of which auxiliary codes can have these short critical indecomposable codes in their

The author is with the Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588-0323. E-mail: jwalker@math.unl.edu .

Dedicated to the memory of E. F. Assmus, Jr.

spectra. At the other extreme, the longest critical indecomposable code of dimension l has length $2l-2$, and in Section V we study these codes and the question of which auxiliary codes can have them in their spectra. In Section VI we treat the general case, studying properties of all possible auxiliary codes. Section VII is an in-depth study of certain codes of dimension at most four which can be used as auxiliary codes. Finally, Section VIII applies the results of the rest of the paper to obtain an enumeration of all binary critical indecomposable codes of dimension at most 10.

II. Critical Indecomposable Codes

We begin by recalling some definitions from [1].

Definition II.1: ([1]) Let F be any field, and for a nonempty finite set X, let F^X denote the vector space of functions from X to F. Any subspace C of F^X is called a (linear) *code*. The cardinality of X is called the *length* of C, and the elements of X are called the *columns* of C.

It is often convenient to identify X with $\{1, 2, \ldots, n\}$ and to think of C as being a subspace of F^n.

The notion of morphism in the category that Assmus defined in [1] was different from the notion used by Slepian in [11]. It was this distinction which allowed Assmus to define critical indecomposable codes, and so our next order of business is to recall Assmus's definition of code homomorphism.

Definition II.2: ([1]) Let C and D be codes. Writing $\mathrm{wt}(\cdot)$ to denote Hamming weight, a *code homomorphism* from C to D is a linear transformation $\phi : C \to D$ such that $\mathrm{wt}(\phi(c)) \leq \mathrm{wt}(c)$ for all $c \in C$. Two codes are said to be *isomorphic* or *equivalent* if there is a bijective code homomorphism, whose inverse is also a code homomorphism, from one to the other.

As Assmus points out, with this definition of equivalence, all codes consisting only of the zero vector (of any length) are equivalent. Thus the length of a code is not an invariant of the equivalence class of the code. However, one may define the *support* of a code to be the set of columns which are not entirely zero, and the cardinality of the support of a code is an invariant of the equivalence class of the code. If two binary codes C and D have *full support*, that is, if their lengths equal the cardinalities of their supports, then C and D are equivalent if and only if there is some permutation of the columns of C which sends C to D. More precisely, if we denote by Σ_n the full permutation group on n symbols, then the binary linear codes C and D having full support and length n are equivalent if there is a permutation $\sigma \in \Sigma_n$ such that $(c_1, \ldots, c_n) \in C$ if and only if $(c_{\sigma(1)}, \ldots, c_{\sigma(n)}) \in D$. We will use the convention that Σ_n acts on the columns of a code C of length n on the right, that is, $(C)^\sigma = \{(c_{\sigma(1)}, \ldots, c_{\sigma(n)}) \,|\, (c_1, \ldots, c_n) \in C\}$.

Definition II.3: Let C' and C'' be linear codes of lengths m and n respectively. The *direct sum* of C' and C'' is the set $C := C' \oplus C''$ of all vectors in $\mathbb{F}^{m+n}$ such that the vector of length m formed by dropping the last n coordinates is a codeword in C' and the vector of length n formed by dropping the first m coordinates is a codeword in C''. A code C is called *indecomposable* if it is not isomorphic to $C' \oplus C''$ for any nonzero linear codes C' and C''. A code which is not indecomposable is called *decomposable*.

Notice that although some authors use the symbol "$\oplus$" to mean modulo two addition, this symbol will be used here only to mean the direct sum of codes.

Let C be an indecomposable code of length n and dimension k, and let G be a $(k \times n)$ generator matrix for C. If any nonzero column vector of length k is appended to G, we get a generator matrix of a new indecomposable code which is not equivalent to C. The dimension of this code will still be k, but the length will now be $n+1$. Roughly speaking, a *critical indecomposable* code is an indecomposable code which hasn't had extra columns appended to it.

More precisely, let C be an indecomposable code of length n and dimension k and let G be a generator matrix for C. For $1 \leq i \leq n$, define $\phi_i(C)$ to be the code which is generated by the rows of the matrix obtained from G by omitting the ith column. (This process is known as *puncturing* C at the ith column and is clearly independent of the choice of the generator matrix for C.) Then $\phi_i(C)$ will be a code of length $n-1$ and dimension either k or $k-1$, and it may or may not be indecomposable.

Definition II.4: Let C be an indecomposable code of length n. We say the ith column of C is a *critical column* of C if either $\phi_i(C)$ has dimension $k-1$ or $\phi_i(C)$ is decomposable. We say C is a *critical indecomposable code* if every nonzero column of C is critical.

Notice that the dimension of $\phi_i(C)$ is less than the dimension of C if and only if there is a codeword of C supported only on the ith column. In this case, either C has dimension one, or C is not indecomposable. Thus only the second condition in the definition of critical indecomposable codes is relevant when $k \geq 2$.

For the remainder of the paper, we will be looking at specific binary critical indecomposable codes. Thus, while many of the results in this paper either apply directly, or can be generalized easily, to the case of linear codes over any ground field, we will restrict our attention to the case of the binary field $\mathbb{F}_2$. Further, since every code is isomorphic to a code with full support (by simply puncturing at all zero columns), we will concern ourselves only with codes which have full support. Because of these reasons, the word *code* should be taken to mean *binary linear code of full support* for the rest of this paper.

It is plain to see that $\mathbb{F}_2$ is the only critical indecomposable code of dimension 1. Further, for $k \geq 2$, there is only one code (up to isomorphism) of dimension k and length $k+1$, and it is critical indecomposable. We will call this code $C_{k+1,k}$. Assmus shows that for $k = 2$ and $k = 3$ the only critical indecomposable codes of dimension k are $C_{3,2}$ and $C_{4,3}$ respectively. He also shows that, up to isomorphism, the only critical indecomposable codes of dimension

4 are $C_{5,4}$ and the code $C_{6,4}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Moreover, Assmus gives a recursive construction for all critical indecomposable codes. We include that construction here.

Let $\pi = (x_1, x_2, \ldots, x_r, x')$ be an ordered partition of n (so $n = x_1 + \cdots + x_r + x'$) such that $x' \geq 0$, $x_i \geq 2$ for $1 \leq i \leq r$, and $x_1 \geq x_2 \geq \cdots \geq x_r$. Let A be an indecomposable code of length $s := r + x'$ and minimum distance at least 3, and assume that the last x' columns of A are critical. Then a generator matrix for a critical indecomposable code can be constructed from π and A as follows:

- For $1 \leq i \leq r$, let G_i be the $(x_i - 1) \times x_i$ matrix which consists of a column of 1's followed by the identity matrix of size $x_i - 1$. Note that if $x_i = 2$, then G_i is a generator matrix for the code whose only nonzero element is the vector $(1, 1)$; otherwise G_i generates the code $C_{x_i, x_i - 1}$ described above.
- Let $l = \dim A$ and fix a generator matrix G_A for A.
- For $1 \leq i \leq r$, let L_i be the $l \times x_i$ matrix whose first column is the ith column of G_A and whose other entries are all 0. Also let $L_{r+1}, \ldots, L_{r+x'}$ be the last x' columns of G_A.
- Set

$$G := \begin{pmatrix} G_1 & & & & & & \\ & G_2 & & & & & \\ & & \ddots & & & & \\ & & & G_r & & & \\ L_1 & L_2 & \ldots & L_r & L_{r+1} & \ldots & L_{r+x'} \end{pmatrix}, \quad (*)$$

where all blank spaces are assumed to be filled in with the appropriate number of zeros.

The matrix G is a generator matrix for a critical indecomposable code of length n and dimension $k := n - s + l$. The relatively straight-forward proof is given in [1], and we will not reproduce it here.

It is also true (see [1]) that every critical indecomposable code is equivalent to a code with a generator matrix of the form $(*)$. To see this, start by defining two operations, ϵ and α, each of which take as input a critical indecomposable code C. Define $\epsilon(C)$ to be the subcode of C generated by the vectors of weight 2. It is not hard to prove that $\epsilon(C)$ is isomorphic to a code of the form $E_1 \oplus \cdots \oplus E_r$, where each E_i is either the code whose only nonzero element is $(1, 1)$ or a code of length n_i and dimension $n_i - 1$ for some $n_i \geq 2$, and we may order the E_i's in such a way that $n_1 \geq n_2 \geq \cdots \geq n_r$. Further, if C was constructed using the partition $\pi = (x_1, \ldots, x_r, x')$, we have that $\epsilon(C) = E_1 \oplus \cdots \oplus E_r$ where $E_i = C_{x_i, x_i - 1}$ is the code with generator matrix G_i as described above.

To define $\alpha(C)$, we first need to choose $c_i \in \mathrm{supp}(E_i)$ for $1 \leq i \leq r$. Then $\alpha(C)$ is the subcode of C supported only on $\{c_1, \ldots c_r\} \cup (\mathrm{supp}(C) \setminus \mathrm{supp}(\epsilon(C)))$. One can show ([1]) that $\alpha(C)$ is independent of choice of $c_1, \ldots, c_r$, that $\alpha(C)$ indecomposable of minimum weight at least 3, and that the columns of $\alpha(C)$ which were not in the support of E are all critical. Further, if C was constructed using the auxiliary code A, then $\alpha(C)$ is simply the code A with some columns of zeros inserted (see [1]). More precisely, if A had dimension l, then the last l rows of the generator matrix $(*)$ for C form a generator matrix for $\alpha(C)$.

Finally, if C is any critical indecomposable code of length n, we note that the structure of $\epsilon(C)$ implies a partition $\pi = (n_1, \ldots, n_r, n')$ of n. Let A be the code obtained by dropping the columns of zeros from $\alpha(C)$. Then it follows that the critical indecomposable code constructed from π and A is equivalent to C.

If A is an indecomposable code of dimension l, then Assmus defines the *spectrum* of A to be the set $\mathrm{Spec}(A)$ of all critical indecomposable codes of dimension l which can be obtained by deleting columns of A. Clearly $\mathrm{Spec}(A)$ is nonempty for every indecomposable code A.

We close this section with a proposition which states that critical indecomposable codes are "short". The proposition was already known to Assmus ([1]), who found it to be implied by results of Murty ([8]). The proof we give, however, is much more elementary.

Proposition II.5: Let C be a critical indecomposable code of dimension $k \geq 3$. Then the length of C is at most $2k - 2$.

Proof: The statement holds when $k = 3$, since the only critical indecomposable code of dimension 3 is $C_{4,3}$, which has length $4 = 2(3) - 2$. Assume the statement holds for all $l < k$, and let C be a critical indecomposable code of dimension k. If $C = C_{k+1,k}$, then the length of C is $k + 1 < 2k - 2$. Otherwise, let A be the auxiliary code used to construct C. Then $\dim A = l < k$, so every critical indecomposable code in $\mathrm{Spec}(A)$ has length at most $2l - 2$. Thus, at most $2l - 2$ columns of A can be critical. (In fact, we will show in Theorem VI.1 below that at most $l - 1$ columns of A can be critical.) But we have $k = n - s + l$, where s is the length of A and n is the length of C. Further, from the conditions on the partition used to construct C, we have $s = r + x' \leq (n - x')/2 + x'$. Putting this all together, we have

$$\begin{aligned} n &= k + s - l \\ &\leq k + (n - x')/2 + x' - l \end{aligned}$$

which implies that

$$n \leq 2k - 2l + x'.$$

Since $x' \leq 2l - 2$, the result follows. ∎

Assmus ([1]) also states that the results of Murty ([8]) imply that there is a unique critical indecomposable code of length l and dimension $2l - 2$. We will show that this is true without appealing to [8] in Section V below.

III. Equivalence of Critical Indecomposable Codes

The auxiliary code A in the construction of critical indecomposable codes plays a very important role. Indeed, this is the one part of the construction which remains somewhat mysterious. For example, as Assmus comments, equivalent auxiliary codes, when paired with the same partition of n, may yield inequivalent critical indecomposable codes. In this section, we determine exactly when this can happen.

First, let us look at some examples. It is easy to check that the code A with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

is indecomposable and has minimum distance 3. Further, the last column of A is critical. Let A' be the code with generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Clearly, A and A' are equivalent (but distinct) codes, and the last column of A' is still critical.

We can use A and A' along with the partition $\pi = (2, 2, 2, 2, 1)$ to construct critical indecomposable codes C and C' of length 9 and dimension 6. The generator matrices constructed for C and C' are

$$\begin{pmatrix} 11 & & & & \\ & 11 & & & \\ & & 11 & & \\ & & & 11 & \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 11 & & & & \\ & 11 & & & \\ & & 11 & & \\ & & & 11 & \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

respectively. Although these are certainly distinct subspaces of $\mathbb{F}_2^9$, applying the permutation $(3,5)(4,6)$ to C yields C', so C and C' are equivalent codes.

Now we'll use the partition $\pi = (3, 3, 2, 2, 1)$ along with the auxiliary codes A and A' to construct two critical indecomposable codes D and D' of length 11 and dimension 8. Thus,

$$\begin{pmatrix} 110 & & & & \\ 101 & & & & \\ & 110 & & & \\ & 101 & & & \\ & & 11 & & \\ & & & 11 & \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 110 & & & & \\ 101 & & & & \\ & 110 & & & \\ & 101 & & & \\ & & 11 & & \\ & & & 11 & \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

are generator matrices for D and D' respectively. This time, we see that the codes D and D' are inequivalent. In particular, the all-1 vector is a codeword of D (add up the first 7 rows of the given generator matrix) but it is not a codeword of D'.

It turns out that the question of whether the same partition and equivalent yet distinct auxiliary codes yield equivalent critical indecomposable codes depends upon certain double-cosets in the full permutation group. To make this precise, we will need a definition.

Definition III.1: Let $\pi = (x_1, \ldots, x_r, x')$ be a partition of the integer n as used in the construction of critical indecomposable codes. We define the *block permutations of* π to be the subgroup $B(\pi) \leq \Sigma_r \times \Sigma_{\{r+1,\ldots,r+x'\}} \leq \Sigma_s$ given by

$$B(\pi) := \{\sigma \in \Sigma_r \,|\, x_{\sigma(i)} = x_i \text{ for } 1 \leq i \leq r\} \times \Sigma_{\{r+1,\ldots,r+x'\}}.$$

When looking at equivalent auxiliary codes, we need to be sure that the permutation of columns preserves the property that the last x' columns are critical. Let A be an indecomposable code of length s with minimum distance at least 3 and having c critical columns. Without loss of generality, we may assume that the columns of A are arranged in such a way that the first $s-c$ are not critical and the last c are critical. Given a partition $\pi = (x_1, \ldots, x_r, x')$ to be used with A as auxiliary code, we know that $x' \leq c$. Further, the only equivalent codes $(A)^\sigma$ we need be concerned with are those where the last x' columns are critical. It is not hard to see that this is the same as requiring $\sigma \in \Sigma_r \cdot \Sigma_{\{s-c+1,\ldots,s\}}$. In what follows, we denote by $\mathrm{Aut}(A)$ the *automorphism group* of A, i.e., the subgroup of Σ_s which fixes the code A.

Theorem III.2: Let $\pi = (x_1, \ldots, x_r, x')$ be a partition of the integer n with $x_i \geq 2$ for $1 \leq i \leq r$. Let A be an indecomposable code of length $s := r + x'$ with minimum distance at least 3 and $c \geq x'$ critical columns. Assume that the last c columns of A are the critical ones. Let $\sigma, \tau \in \Sigma_{\{s-c+1,\ldots,s\}} \cdot \Sigma_r \subset \Sigma_s$, and let C_σ and C_τ be the critical indecomposable codes of length n constructed using the partition π and the auxiliary codes $(A)^\sigma$ and $(A)^\tau$ respectively. Then C_σ is equivalent to C_τ if and only if the double coset $\mathrm{Aut}(A) \cdot \sigma \cdot B(\pi)$ contains τ.

Proof: Suppose first that C_σ and C_τ are equivalent codes. Then there is some $\gamma \in \Sigma_n$ such that $C_\sigma = (C_\tau)^\gamma$. Apply the operations ϵ and α described above, choosing c_i

to be the first column of E_i for $i = 1, \ldots, r$ in the definition of α. Set $E_\sigma = \epsilon(C_\sigma)$, $E_\tau = \epsilon(C_\tau)$, $A_\sigma = \alpha(C_\sigma)$, and $A_\tau = \alpha(C_\tau)$. Then we have $E_\sigma = \epsilon(C_\sigma) = \epsilon((C_\tau)^\gamma) = (\epsilon(C_\tau))^\gamma = (E_\tau)^\gamma$ and $A_\sigma = \alpha(C_\sigma) = \alpha((C_\tau)^\gamma) = (\alpha(C_\tau))^\gamma = (A_\tau)^\gamma$. We will use these relationships to deduce information about the relationship between σ and τ.

First notice that since C_σ and C_τ were both constructed using the same partition π, we have $E_\sigma = E_\tau = E_1 \oplus \cdots \oplus E_r \oplus Z$, where $E_i = C_{x_i, x_i+1}$ and Z is the code consisting of the zero vector of length x'. It is easy to see that $\mathrm{Aut}(E_i) = \Sigma_{x_i}$. Set $\hat{B}(\pi) = \{\hat{\beta} \,|\, \beta \in B(\pi)\}$, where $\hat{\beta}$ is the obvious extension of the block permutation β to an element of Σ_n. More precisely, if we label the n columns of $\mathbb{F}_2^n$ as $(1,1), \ldots, (1,x_1), \ldots, (r,1), \ldots, (r,x_r), (r+1,1), \ldots, (r+x',1)$, then $\beta((i,j)) = (\beta(i), j)$. Therefore, since $E_\tau = E_\sigma = (E_\tau)^\gamma$, we have that

$$\gamma \in \hat{B}(\pi) \times \Sigma_{\{(1,1),\ldots,(1,x_1)\}} \times \cdots \times \Sigma_{\{(r,1),\ldots,(r,x_r)\}} \leq \Sigma_n.$$

Thus, we can write

$$\gamma = \hat{\beta} \circ \gamma_1 \circ \cdots \circ \gamma_r$$

for some $\hat{\beta} \in \hat{B}(\pi)$ and $\gamma_i \in \Sigma_{\{(1,1),\ldots,(1,x_i)\}}$, $1 \leq i \leq r$.

Next we consider information about A_σ and A_τ. Notice first that only the columns $(i,1)$ for $1 \leq i \leq r$ and $(r+1, j)$ for $1 \leq j \leq s := r + x'$ are nonzero for either of these codes, and when we drop the columns of zeros, we recover the codes $(A)^\sigma$ and $(A)^\tau$ respectively. Since we have $A_\sigma = (A_\tau)^\gamma$, the location of the columns of zeros of these codes implies that $\gamma_i((i,1)) = (i,1)$ for $1 \leq i \leq r$.

Now, since $A_\sigma = (A_\tau)^\gamma$ and γ acts as β on $\{(i,1) \,|\, 1 \leq i \leq s\}$, we have $(A)^\sigma = ((A)^\tau)^\beta$, so we have $(A)^\sigma = (A)^{\tau\beta}$, which implies that $\tau\beta\sigma^{-1} \in \mathrm{Aut}(A)$. This means that $\tau \in \mathrm{Aut}(A)\sigma\beta \subset \mathrm{Aut}(A) \cdot \sigma \cdot B(\pi)$, as desired.

On the other hand, suppose that $\tau \in \mathrm{Aut}(A) \cdot \sigma \cdot B(\pi)$. Then $\tau = \chi\sigma\beta$ for some automorphism χ of A and some block permutation β of π. Therefore, $(A)^\tau = (A)^{\chi\sigma\beta} = (A)^{\sigma\beta} = ((A)^\sigma)^\beta$, so $(A)^\tau$ is just a block permutation of $(A)^\sigma$. It is plain to see now that the codes C_σ and C_τ constructed from the partition π and the auxiliary codes $(A)^\sigma$ and $(A)^\tau$, respectively, are equivalent: simply apply $\hat{\beta}$ to C_τ to obtain C_σ. ∎

The following corollary is immediate.

Corollary III.3: Let $\pi = (x_1, \ldots, x_r, x')$ be a partition of the integer n with $x_i \geq 2$ for $1 \leq i \leq r$ and $x_1 \geq x_2 \geq \cdots \geq x_r$. Let A be an indecomposable code of length $s := r + x'$ with minimum distance at least 3 and $c \geq x'$ critical columns. Assume that the last c columns of A are the critical ones. Then the number of inequivalent critical indecomposable codes which can be constructed from π and codes equivalent to A is precisely the number of $\mathrm{Aut}(A) - B(\pi)$ double cosets which have representatives in the subset $\Sigma_{\{s-c+1,\ldots,s\}} \cdot \Sigma_r$ of Σ_s.

IV. Admissible Codes from Short Critical Indecomposable Codes

In the construction of critical indecomposable codes, the auxiliary code is required to have minimum distance at least 3 and at least x' critical columns. This begs the question of how many critical columns an indecomposable code of minimum distance at least 3 can have. The following definition will make the exposition a little smoother.

Definition IV.1: An indecomposable code of minimum distance at least 3 having no zero columns is called an *admissible* code.

In this section, we treat the special case of admissible codes A such that $C_{l+1,l} \in \mathrm{Spec}(A)$. The case where the spectrum of A contains a critical indecomposable code of length $2l-2$ and dimension l is treated in Section V, and the most general case is the subject of Section VI.

We will need *Slepian's Criterion*, which gives a way of deciding whether a binary linear code is indecomposable. Let C be any binary linear code, and let G be a systematic generator matrix for (a code equivalent to) C. Thus, $G = [I|M]$, where I is the identity matrix of size $\dim C$. Form a graph whose vertices correspond to the 1's in M, and draw an edge between two vertices if and only if the corresponding 1's are in either the same row or the same column of M. Then Slepian's Criterion states that C is indecomposable if and only if this graph is connected. Below, we will extend terminology and refer to M itself as being either connected or disconnected.

Theorem IV.2: Let A be an indecomposable code of minimum distance at least 3 and dimension l. Assume $C_{l+1,l} \in \mathrm{Spec}(A)$. Then A has at most $l-1$ critical columns.

Proof: Suppose the indecomposable code A of dimension l and minimum distance at least 3 has at least l critical columns. Consider a generator matrix of A of the form $[\mathbf{1}|I|M]$, where $\mathbf{1}$ is a column vector of l ones, I is the $l \times l$ identity matrix, and M is a matrix with l rows. Certainly no column of M is critical, and since $\mathrm{Aut}(C_{l+1,l})$ is the full symmetric group, we may assume that the l columns of I are the critical ones. Further, since A is admissible, we know that $d_{\min}(A) \geq 3$, so the l rows $m_1, m_2, \ldots, m_l$ of M must be distinct and nonzero. Finally, note that if we puncture A at the i^{th} column of I, we get a code equivalent to a code with generator matrix $[I|M^{(i)}]$, where $M^{(i)}$ has rows $m_1^{(i)}, m_2^{(i)}, \ldots, m_l^{(i)}$ with

$$m_j^{(i)} = \begin{cases} m_j, & \text{if } i = j \\ m_j + m_i, & \text{if } i \neq j. \end{cases}$$

Since the i^{th} column of I is thus critical if and only if the matrix $M^{(i)}$ is disconnected, it is enough to show that not all of the matrices $M^{(i)}$, $1 \leq i \leq l$, can be disconnected. In other words, we need to show that it is impossible to find a matrix M with l distinct nonzero rows such that $M^{(i)}$ is disconnected for $1 \leq i \leq l$.

Suppose we have such a matrix M. Then certainly no column of weight M has weight 1, since otherwise $M^{(i)}$ would be connected for some i. Let $t_1 > 1$ be the weight of the first column of M. Without loss of generality, we may assume that the first t_1 rows of M each have a one in the first position. It is easy to see that the rows $m_1^{(1)}$ and $m_j^{(1)}$ are connected for $t_1 + 1 \leq j \leq l$.

Since $m_1 \neq m_{t_1}$, we may assume that m_1 has a one in the second position and that m_{t_1} has a zero in the second position. Let t_2 be the number of ones in the second position in rows $m_1, \ldots, m_{t_1}$. By rearranging the rows $m_2, \ldots, m_{t_1-1}$ if necessary, we may assume that row m_i has a one in the second position for $1 \leq i \leq t_2 < t_1$, and row m_j has a zero in the second position for $t_2+1 \leq j \leq t_1$. Notice that we have no information about the second entry of row m_j for $j > t_1$. However, we may conclude that rows $m_1^{(1)}$ and $m_j^{(1)}$ are connected for $t_2+1 \leq j \leq t_1$. But also we still have that rows $m_1^{(1)}$ and $m_j^{(1)}$ are connected for $t_1+1 \leq j \leq l$ because of their first entries. Therefore, at this point we can see that rows $m_1^{(1)}$ and $m_j^{(1)}$ are connected for $t_2+1 \leq j \leq l$.

We continue this process, until we eventually have $t_s = 2$, so $m_1^{(1)}$ and $m_j^{(1)}$ are connected for $3 \leq j \leq l$. But certainly $m_1 \neq m_2$, so without loss of generality, we may assume that there is a column where m_1 has a one and m_2 has a zero. This means that $m_1^{(1)}$ and $m_2^{(1)}$ are connected as well. We conclude that the matrix $M^{(1)}$ is connected, a contradiction. ∎

By examining the proof of Theorem IV.2, we get:

Proposition IV.3: Let A be an admissible code of dimension l with $l-1$ critical columns and suppose $C_{l+1,l} \in \mathrm{Spec}(A)$. Then the length of A is at least $2l+1$. Further, up to equivalence, there is exactly one admissible code A of length $2l+1$ and dimension l having $l-1$ critical columns and $C_{l+1,l} \in \mathrm{Spec}(A)$.

For each $l \geq 2$, the unique (up to equivalence) indecomposable code of length $2l+1$, dimension l, and minimum distance 3 which has $l-1$ critical columns and has $C_{l+1,l}$ in its spectrum has generator matrix $[\mathbf{1}|I|U]$, where U is the $l \times l$ upper triangular matrix whose entries on and above the diagonal are all 1. The critical columns of this code are precisely the last $l-1$ columns of the matrix I.

V. Critical Indecomposable Codes of Length $2l-2$ and Dimension l

We have already shown that the longest critical indecomposable code of dimension l has length $2l-2$. Our goal now is to study these codes in detail. In particular, we will show three main things: First, as mentioned earlier, there is a unique critical indecomposable code of length $2l-2$ and dimension l for each $l \geq 4$. Next, any admissible code with this code in its spectrum has at most $l-1$ critical columns. Finally, any admissible code with this code in its spectrum and $l-1$ critical columns has length at least $3l-3$.

We begin by constructing a critical indecomposable code of length $2l-2$ and dimension l, where $l \geq 4$. Let π be the partition of $2l-2$ into $r := l-1$ copies of 2, and let A be the code whose only nonzero element is the all-one vector of length $l-1$. Then the critical indecomposable code constructed from π and A is the one we're looking for, and we'll call it $C_{2l-2,l}$. The generator matrix $(*)$ for this code looks like $[\bar{e}_1, e_1, \ldots, \bar{e}_{l-1}, e_{l-1}]$, where e_i is the vector of length l with a 1 in the ith position and 0's otherwise, and $\bar{e}_i$ is the same as e_i except that the lth position is 1 as well.

Lemma V.1: Let $c = (c_1, \ldots, c_l)^t$ be a column vector of length l and consider the indecomposable code of length $2l-1$ and dimension l obtained by appending c to the generator matrix for $C_{2l-2,l}$ described above. Then
1. If $c_l = 0$, then e_j is not critical for each j with $1 \leq j \leq l-1$ such that $c_j = 1$.
2. If $c_l = 1$, then $\bar{e}_j$ is not critical for each j with $1 \leq j \leq l-1$ such that $c_j = 1$.
3. If $c_i = c_j = 1$ for some $i \neq j$ with $1 \leq i, j \leq l-1$, then e_i, e_j, $\bar{e}_i$, and $\bar{e}_j$ are all not critical.

Proof: First assume $c_l = 0$, and without loss of generality, assume $c_{l-1} = 1$. Puncture the code at e_{l-1} to obtain a code equivalent to the code generated by $[e_1, \ldots, e_{l-2}, \bar{e}_{l-1}, \bar{e}_1, \ldots, \bar{e}_{l-2}, c]$. Start row reducing by adding the last row to the first row. The result is $[e_1, \ldots, e_{l-2}, f, e_l|M|c]$, where f is the vector of weight 3 with 1's in the first, $(l-1)$st, and lth positions, and M is an $l \times (l-3)$ matrix whose first and last rows are entirely 1's. Further, the $(l-1)$st row of M is entirely 0's, and the second through $(l-2)$nd rows of M form the identity matrix of size $l-2$. Finish row reducing by adding the $(l-1)$st row to the first and the lth row. The result is $[I|M|c']$, where I is the identity matrix of size l, M is the matrix described above, and c' is the same as c, except that $c'_1 = 1 + c_1$ and $c'_l = 1$. The matrix $[M|c']$ is now clearly connected since its last row is entirely ones and all other rows are nonzero. Therefore, e_{l-1} is not critical. This proves (1).

Now, assume $c_l = 1$. If this is the only nonzero entry of c then the Lemma doesn't assert anything. Therefore, we may assume $c_{l-1} = 1$. Puncture the code at $\bar{e}_{l-1}$ to obtain a code equivalent to the code generated by $[e_1, \ldots, e_{l-1}, \bar{e}_1, \ldots, \bar{e}_{l-2}, c]$. To row reduce, we just need to add the last row to the first. We get the matrix $[I|M|c'']$, where M is as described above and c'' is the same as c except $c''_1 = 1 + c_1$. This means $[M|c'']$ is connected and so $\bar{e}_{l-1}$ is not critical, which proves (2).

To prove (3), assume $c_i = c_j = 1$ for some $1 \leq i \neq j \leq l-1$. If $c_l = 0$, we know from (1) that e_i and e_j are not critical, so we need only show that $\bar{e}_i$ and $\bar{e}_j$ are not critical as well. By symmetry, we only need to show $\bar{e}_i$ is not critical, and without loss of generality, we may assume $i = l-1$. Puncture at $\bar{e}_{l-1}$ to obtain a code equivalent to the code with generator matrix $[e_1, \ldots, e_{l-1}, \bar{e}_1, \ldots, \bar{e}_{l-2}, c]$. To row reduce, we need only add the last row to the first, and we obtain the matrix $[I|M|c]$ where M is the matrix described above. Since $c_{l-1} = c_j = 1$, $[M|c]$ is connected, and $\bar{e}_{l-1}$ is not critical.

Finally, consider the case where $c_l = 1$. If $c_i = c_j = 1$ for some $1 \leq i \neq j \leq l-1$, then we know from (2) that $\bar{e}_i$ and $\bar{e}_j$ are not critical. Therefore, we only need to show that e_i and e_j are not critical. Again, by symmetry, it is enough to show that e_i is not critical, and without loss of generality, we may assume $i = l-1$. Puncture the code at e_{l-1} to obtain a code equivalent to the code with generator matrix $[e_1, \ldots, e_{l-2}, \bar{e}_{l-1}, \bar{e}_1, \ldots, \bar{e}_{l-2}, c]$. Begin row reducing by adding the last row to the first. The result is $[e_1, \ldots, e_{l-2}, f, e_l|M|c'']$, where f and M are the vector of

weight three and the $l \times (l-3)$ matrix described above and c'' is the same as c except that $c''_1 = c_1 + 1$. Finish row reducing by adding the $(l-1)$st row to the first and the lth row. The result is $[I|M|c''']$, where I is the identity matrix of size l, M is still the same matrix, and c''' is the same as c'', except that $c'''_l = 0$. The matrix $[M|c'']$ is now clearly connected since $c''_{l-1} = c''_j = 1$, so e_{l-1} is not critical. This completes the proof of (3). ∎

Theorem V.2: Let A be an indecomposable code of dimension l and minimum distance at least 3, and suppose $C_{2l-2,l} \in \mathrm{Spec}(A)$. Then
1. At most $l-1$ columns of A are critical.
2. If A has $l-1$ critical columns, then the length of A is at least $3l-3$.
3. Up to isomorphism, there is only one indecomposable code A of length $3l-3$, dimension l, and minimum distance at least 3 which has $l-1$ critical columns and satisfies $C_{2l-2,l} \in \mathrm{Spec}(A)$.

Proof: Since A has minimum distance at least three, it must have a generator matrix of the form

$$[e_1, \ldots, e_{l-1}, \bar{e}_1, \ldots, \bar{e}_{l-1}|N],$$

where N is a matrix with l rows with each of its first $l-1$ rows nonzero. By Lemma V.1, this makes at least one of e_i, $\bar{e}_i$ not critical for $1 \le i \le l-1$. Therefore, at least $l-1$ of the first $2l-2$ columns of A are not critical, and certainly no column of N is critical, so the maximum possible number of critical columns of A is $(2l-2)-(l-1) = l-1$, proving (1).

To prove (2), suppose the number of critical columns of A is exactly $l-1$. Then each column of N has at most one 1 among its first $l-1$ entries, so N must have at least $l-1$ columns. Therefore, the minimum length of A is at least $(2l-2)+(l-1) = 3l-3$.

By the above argument, any A satisfying the conditions of (3) must be equivalent to a code having a generator matrix whose first $2l-2$ columns are e_i and $\bar{e}_i$ for $1 \le i \le l-1$, and whose last $l-1$ columns are $f_1, \ldots, f_{l-1}$, where each f_i is either e_i or $\bar{e}_i$. For each i such that $f_i = \bar{e}_i$, interchange the appearance of e_i and $\bar{e}_i$ among the first $2l-2$ columns. Adding the ith row to the last row yields an identical matrix to what we started with, except that f_i is replaced with e_i. Thus, A is equivalent to the code having generator matrix $[\bar{e}_1, e_1, e_1, \ldots, \bar{e}_{l-1}, e_{l-1}, e_{l-1}]$, which proves (3). ∎

Theorem V.3: For each $k \ge 4$, the only critical indecomposable code of length $2k-2$ and dimension k is $C_{2k-2,k}$.

Proof: Assmus ([1]) shows that the theorem is true when $k = 4$, so assume it is true for all $l < k$. Let C be a critical indecomposable code of length $2k-2$ and dimension k, constructed from the partition $\pi = (x_1, \ldots, x_r, x')$ and the auxiliary code A, where A is an indecomposable code of length $s := r + x'$, dimension l, and minimum distance at least three, with at least x' critical columns.

If $l = 1$, then $x' = 0$ and $(2k-2) - k = s - 1$, which means that $s = r = k-1$. The only possibility for π is then $x_i = 2$ for $1 \le i \le k-1$, so $C = C_{2k-2,k}$. Therefore, we may assume $l \ge 2$.

Since each x_i, $1 \le i \le r = s - x'$, satisfies $x_i \ge 2$, we have $2k-2-x' \ge 2(s-x')$, which means $2k \ge 2s+s-x'$. On the other hand, since $(2k-2)-k = s-l$, we have $2k = 2s-2l+4$. Putting this together, we have $2s-2l+4-2-x' \ge 2s$, which means $x' \ge 2l-2$. Since the only critical indecomposable code of dimension 1 is $\mathbb{F}_2$ and the only critical indecomposable codes of dimensions 2 and 3 are $C_{3,2}$ and $C_{4,3}$, Theorem IV.2 implies that $l \ge 4$. We know there is a critical indecomposable code of length $n \ge 2l-2$ and dimension l in the spectrum of A, but by Lemma II.5, the longest critical indecomposable code of dimension l has length $2l-2$, so $n = 2l-2$. Now by induction hypothesis, this code is $C_{2l-2,l}$, so by Theorem V.2, A has at most $l-1$ critical columns, a contradiction. Hence $l = 1$ and $C = C_{2k-2,k}$. ∎

VI. Admissible Codes: General Case

Now that we have explored the two extremes of admissible codes, we can tackle the general case. Our main result is:

Theorem VI.1: Let A be an admissible code of dimension l. Then A has at most $l-1$ critical columns.

Proof: We have already proven this in the case that $C_{l+1,l} \in \mathrm{Spec}(A)$, so in particular the theorem is true if $l = 2$ or $l = 3$. Therefore, we assume $l \ge 4$ and that the theorem is true for all $l_0 < l$. Let $C \in \mathrm{Spec}(A)$, $C \ne C_{l+1,l}$. Without loss of generality, we have that C is constructed from the partition $\pi = (x_1, \ldots, x_r, x')$ and the auxiliary code A_0 of length $s := r + x'$ and dimension l_0. Let $g_1, \ldots, g_s$ be the columns in the chosen generator matrix for A_0, so that for $1 \le i \le r$, the $l_0 \times x_i$ matrix L_i has g_i as its first column and zeros elsewhere, and for $i \ge r+1$, $L_i = g_i$. We will show:

Claim If the ith column of A_0 is not a critical column, $1 \le i \le r$, then not every column in the block of A corresponding to x_i can be critical.

Once we have shown this Claim, we will have that the number of critical columns of A is at most

$$\begin{aligned}
&\sum_{i=1}^{r}(x_i - 1) + x' + \\
&\qquad \#\{i \,|\, 1 \le i \le r \text{ and } g_i \text{ is a critical column of } A_0\} \\
&\le \quad \sum_{i=1}^{r}(x_i - 1) + \#(\text{critical columns of } A_0) \\
&= \quad l - l_0 + l_0 - 1 \\
&= \quad l - 1,
\end{aligned}$$

which completes the proof.

Thus all that remains is to show the Claim. We will do this by induction on $x_i \ge 2$. Without loss of generality, we may assume that $i = 1$, so that the two columns in question are the standard basis vector e_1, and the vector $\bar{e}_1 := e_1 + \hat{g}_1$, where $\hat{g}_1$ is the column vector obtained by prepending enough zeros to the top of g_1. Since the first column of A_0 is not critical, we may assume that the

columns of the identity matrix of size l_0 appear in some order in the list $g_2, \ldots, g_s$ of the last $s-1$ columns of our chosen generator matrix for A_0. Let G be the quasi-canonical generator matrix $(*)$ for C using this generator matrix for A_0. Since A is admissible, at least one of the columns appended to G to form a generator matrix for A must have a 1 in the first position. Let $m = (1, m_2, \ldots, m_l)^t$ be this column. Then it is enough to show that one of the first two columns of the code generated by $K = [G|m]$ is not critical.

By rearranging the columns of K, we obtain a matrix of the form

$$\begin{pmatrix} I_{(l-l_0)} & S & T & \bar{e}_1 & m \\ 0_{l_0 \times (l-l_0)} & I_{l_0} & U & \vdots & \vdots \end{pmatrix}.$$

Note that $\bar{e}_1$ and m are column vectors of length l, so they fill the entire height of the matrix. Also, the first row of the matrix $[S|T]$ is entirely zeros, and the other rows have exactly one 1. Further, since A_0 has minimum distance at least 3, every row of U has at least one 1. Finally, since g_1 doesn't represent a critical column of A_0, the matrix $[I_{l_0}|U]$ is connected.

Row reducing this matrix yields a matrix of the form

$$K' = \begin{pmatrix} I_{l-l_0} & 0_{(l-l_0)\times l_0} & T' & f & m' \\ 0_{l_0 \times (l-l_0)} & I_{l_0} & U & \vdots & \vdots \end{pmatrix}.$$

Again, f and m' are column vectors of length l; they are what comes out of $\bar{e}_1$ and m after row reduction. Also, the first row of T' still is zero and every other row has at least one 1 since it is the sum of a vector of weight 1 and a vector of weight at least 2. Further, since $[I_{l_0}|U]$ is connected, the matrix formed by dropping the first row and last two columns of K' is connected. Finally, notice that the first entry of f is 1, as is the first entry of m'.

Now, if $m' = e_1$, then the second column of our original A is not critical. If some entry of m' other than the first is nonzero, it is in the same row as either a nonzero entry of T' or a nonzero entry of $[I_{l_0}|U]$, which connects the first row of K' to the rest of K', even without using f. Therefore, f represents a noncritical column of A, so the first column of the original A (before we rearranged the columns) is not critical. Finally, we have that $m' \neq e_1$ if and only if $m \neq e_1$. Putting it all together, we see that if $m = e_1$, then the second column of our original A is not critical, and if $m \neq e_1$, then the first column of our original A is not critical. This completes the base step of our induction.

Now assume $x_i \geq 3$ and that the Claim is true for all $x < x_i$. Again, without loss of generality, we may assume that $i = 1$. Let $\mathcal{G} = [G|M]$ be a generator matrix for A, where G is the quasi-canonical form $(*)$ of the generator matrix for C. Let $\mathcal{G}' := [G'|M']$ be the matrix obtained by dropping the second column and the first row of $\mathcal{G}$. Let C' be the code generated by G' and let A' be the code generated by $\mathcal{G}'$. It is clear that C' is the critical indecomposable code constructed from the partition $(x_1 - 1, x_2, \ldots, x_r, x')$ and A_0 and that A' is admissible.

Let P' be the code obtained by puncturing A' at one of the columns in the first block. Let P be the code obtained by puncturing A at the corresponding column. If every column in the first block of A is critical, then P must be decomposable (since it clearly has dimension l), so we have $P = P_1 \oplus P_2$, where P_1 and P_2 are nonzero codes. Since A is generated by the rows $c_1, \ldots, c_l$ of $\mathcal{G}$, every element of A is of the form $\sum a_i c_i$, where $a_i \in \mathbb{F}_2$ for $i = 1, \ldots, l$. We have an onto code homomorphism

$$\begin{array}{rccc} \phi: & A & \to & A' \\ & \sum_{i=1}^{l} a_i c_i & \mapsto & \sum_{i=2}^{l} a_i c_i', \end{array}$$

where c_i' is the $i-1$st row of $\mathcal{G}'$, i.e., the ith row of $\mathcal{G}$ with the second entry removed. This induces a map

$$\bar{\phi} : P \to P',$$

which shows that $P' = P_1' \oplus P_2'$, where $P_j' = \bar{\phi}(P_j)$, $j = 1, 2$. Since neither P_1' nor P_2' can be the zero code, P' is decomposable. This means that every column of the first block of A' is critical, which contradicts our induction hypothesis. ∎

The next corollary is found in the proof of Theorem VI.1.

Corollary VI.2: Let C be a critical indecomposable code of dimension l constructed using the auxiliary code A_0 of dimension l_0. Assume A_0 has c_0 critical columns. Then any admissible A with $C \in \mathrm{Spec}(A)$ has at most $l - l_0 + c_0$ critical columns.

Theorem VI.1 is quite powerful and can be used to further determine the parameters of admissible codes. In particular, we have the following two corollaries.

Corollary VI.3: The shortest admissible code of dimension l with $l-1$ critical columns has length $2l+1$.

Proof: By Proposition IV.3, the shortest admissible code of dimension l with $l-1$ critical columns and $C_{l+1,l}$ in its spectrum has length $2l+1$. Also, the shortest admissible code of dimension 1 is the code whose only nonzero codeword is $(1,1,1)$. Therefore, the corollary is true in dimensions at most 3. So, let A be an admissible code of dimension $l \geq 4$ and let $C \in \mathrm{Spec}(A)$ of length n. Without loss of generality, C is constructed from a partition π of n and an auxiliary code of dimension $l_0 < l$. Let $G = [G_C|M]$ be a generator matrix for A, where G_C is a quasi-canonical generator matrix $(*)$ for C. If A has $l-1$ critical columns, then Corollary VI.2 implies that A_0 has $l_0 - 1$ critical columns. Thus the length s_0 of A_0 satisfies $s_0 \geq 2l_0 + 1$ by induction. Further, it follows from the proof of Theorem VI.1 that M is block diagonal and has at least $l - l_0$ columns. Therefore, the length s of A satisfies

$$\begin{aligned} s &\geq n + l - l_0 \\ &= s_0 - l_0 + l + l - l_0 = s_0 + 2l - 2l_0 \\ &\geq 2l_0 + 1 + 2l - 2l_0 \\ &= 2l + 1, \end{aligned}$$

which is the desired result. ∎

Corollary VI.4: Let C be a critical indecomposable code of dimension k, constructed using an auxiliary code A of length s. Then $s \leq k-1$.

Proof: Let n be the length of C and let l be the dimension of A. The partition π of n is of the form $(x_1, \ldots, x_r, x')$ with $x_i \geq 2$ for $i = 1, \ldots, r$ and $s = r + x'$. We have $s = n - k + l$, so $n \leq k - l + (n - x')/2 + x'$, which implies $n \leq 2k - 2l + x'$. By Theorem VI.1, $x' \leq l - 1$, so $n \leq 2k - l - 1$, which can be written as $n - k + l \leq k - 1$. Substituting s back in, we have the result. ∎

We close this section with an elementary yet extremely useful result about the minimum length of any admissible code.

Lemma VI.5: Let C be a critical indecomposable code of length n and dimension l, constructed from the partition $\pi = (x_1, \ldots, x_r, x')$ and the auxiliary code A_0 of length $s_0 = r + x'$ and dimension l_0. Then any admissible code A with $C \in \mathrm{Spec}(A)$ has length

$$s \geq n + \max\{\lceil \log_2(x_i) \rceil \mid 1 \leq i \leq r\}.$$

Proof: Let G be the quasi-canonical generator matrix for C coming from the construction described in the statement of the lemma, and suppose the code A generated by $[G|M]$ is admissible. Then each of the first $l - l_0$ rows of M is nonzero, and the rows within any one block of size $x_i - 1$ are distinct. Thus, the rows must be long enough so that we can choose $x_i - 1$ distinct nonzero rows for each i. Thus, the number of columns m of M satisfies $x_i - 1 \leq 2^m - 1$. Thus $m \geq \log_2(x_i)$ for each i, and since $m \in \mathbb{Z}$, the result follows. ∎

VII. The Necessary Auxiliary Codes

In order to construct critical indecomposable codes of dimension at most 10, we only need admissible codes of length at most 9 by Corollary VI.4. In fact, as one realizes in actually performing the construction, we need only admissible codes of length s and dimension l having c critical columns, where $(s, l; c)$ is $(5, 2; \leq 1)$, $(6, 2; \leq 1)$, $(7, 2; \leq 1)$, $(8, 2; \leq 1)$, $(9, 2; 1)$, $(6, 3; \leq 2)$, $(7, 3; \leq 2)$, $(8, 3; 2)$, $(8, 3; 1)$, $(9, 3; 2)$, $(8, 4; 2)$, and $(9, 4; 3)$. In this section, we will describe all the admissible codes which are needed to construct all binary critical indecomposable codes of dimension at most 10.

First, we recall from [1] that, up to equivalence, $\mathbb{F}_2$ is the only critical indecomposable code of dimension 1, $C_{3,2}$ is the only one of dimension 2, $C_{4,3}$ is the only one of dimension 3, and $C_{5,4}$ and $C_{6,4}$ are the only two of dimension 4. Since any admissible code of dimension l must have a critical indecomposable code of dimension l in its spectrum, these five codes are our starting points.

Every admissible code of dimension 1 is generated by the all-one vector of the appropriate length, and we will refer to the admissible code of dimension 1 and length s as $A_{s,1}$. We note that we used $A_{3,1}$ in the construction of $C_{6,4}$ given in Section II and, more generally, we used $A_{l-1,1}$ in the construction of $C_{2l-2,l}$ given in Section V. Since $A_{s,1}$ is the only admissible code of dimension 1 and length s (not just up to isomorphism), there is no need to worry about equivalence for critical indecomposable codes constructed using auxiliary codes of dimension 1.

Lemma VI.5 implies that the shortest admissible code of dimension 2 has length 5. Any admissible code of length 5 and dimension 2 is equivalent to a code with generator matrix formed by adding two distinct columns to the 2×3 matrix $[1|I]$. Up to equivalence, therefore, we may assume that the columns added are $(1, 0)^t$ and $(1, 1)^t$. The resulting code, which we call $A_{5,2;1}$, has exactly one critical column. Its generator matrix and automorphism group are given in the table below. Notice that the arrangement of columns has been chosen in such a way that the one critical column is the last one.

To form an admissible code of dimension 2 and length 6, we need to add three columns to the 2×3 matrix $[1|I]$ in such a way that the added portions of the rows are nonzero and distinct. We can either repeat one of the original three columns twice and another once or repeat all three of the original columns once each. In the first case, we get a code with one critical column which we call $A_{6,2;1}$. In the second case, we get a code with no critical columns, which we call $A_{6,2;0}$.

Admissible codes of dimension 2 and length 7 are equivalent to codes with generator matrices formed by adding 4 columns to the 2×3 matrix $[1|I]$ in such a way that the added portions of the rows are nonzero and distinct. We can do this in three different ways: (1) repeat two columns twice each, (2) repeat one column thrice and another once, or (3) repeat one column twice and the other two once each. The first two cases yield codes with one critical column, equivalent to the codes $A^1_{7,2;1}$ and $A^2_{7,2;1}$ described in the table below. The third case yields a code with no critical columns, equivalent to the code $A_{7,2;0}$.

Likewise, there are four ways to get admissible codes of length 8 and dimension 2: (1) repeat one column 4 times and another once, (2) repeat one column 3 times and another twice, (3) repeat two columns twice each and the third once, or (4) repeat one column 3 times and the other two once each. The first two cases give us one critical column, and we call the resulting codes $A^1_{8,2;1}$ and $A^2_{8,2;1}$. The last two cases give us no critical columns, and we call the resulting codes $A^1_{8,2;0}$ and $A^2_{8,2;0}$.

Finally, there are three ways to construct admissible codes of length 9 and dimension 2 which have one critical column. We can repeat one column 5 times and another once, repeat one column 4 times and another twice, or repeat two columns 3 times each. We get the codes $A^1_{9,2;1}$, $A^2_{9,2;1}$, and $A^3_{9,2;1}$, as described in the table below.

The constructions of the necessary admissible codes of dimension 3 and 4 are very similar to what we have just done, so the details are omitted. We do want to point out, however that there are no admissible codes with $(s, l; c) = (8, 4; \geq 2)$. To see this, suppose such a code exists, and call it A. Either $C_{6,4}$ or $C_{5,4}$ must be in the spectrum of A. If $C_{6,4} \in \mathrm{Spec}(A)$, then A is equivalent to a code with generator matrix $[\bar{e}_1, e_1, \bar{e}_2, e_2, \bar{e}_3, e_3, c_1, c_2]$, for some column vectors c_1 and c_2. Since A is admissible, the first three rows of $[c_1, c_2]$ are nonzero, so at least one of c_1 and c_2 has

weight at least two and the other has weight at least one. By Lemma V.1, this means that A has at most one critical column. On the other hand, if $C_{5,4} \in \mathrm{Spec}(A)$, then A is equivalent to a code with generator matrix $[1|I|M]$ where M is a 3×3 matrix with distinct nonzero rows. A check of the possibilities for M (using a strategy similar to that found in the proof of Theorem IV.2) shows that A has at most one critical column, a contradiction. Therefore, our A cannot exist.

In order to use Theorem III.2, we need to know the automorphism groups of these codes. These groups can be computed by hand or using the computer algebra package MAGMA ([3]). The following table (spanning three pages) summarizes the important information we have thus far.

TABLE I
AUXILIARY CODES AND THEIR AUTOMORPHISM GROUPS

Name	Generator Matrix	Aut(A)	$\lvert\mathrm{Aut}(A)\rvert$
$A_{5,2;1}$	$\begin{pmatrix}1&1&1&1&0\\1&1&0&0&1\end{pmatrix}$	$\langle(1,2),(3,4),(1,3)(2,4)\rangle$	8
$A_{6,2;1}$	$\begin{pmatrix}1&1&1&1&1&0\\1&1&1&0&0&1\end{pmatrix}$	$\Sigma_{\{1,2,3\}} \times \Sigma_{\{4,5\}}$	12
$A_{6,2;0}$	$\begin{pmatrix}1&1&1&1&0&0\\1&1&0&0&1&1\end{pmatrix}$	$\langle(1,2),(3,4),(5,6),$ $(1,3)(2,4),(1,5)(2,6)\rangle$	48
$A^1_{7,2;1}$	$\begin{pmatrix}1&1&1&1&1&1&0\\1&1&1&1&0&0&1\end{pmatrix}$	$\Sigma_{\{1,2,3,4\}} \times \Sigma_{\{5,6\}}$	48
$A^2_{7,2;1}$	$\begin{pmatrix}1&1&1&1&1&1&0\\1&1&1&0&0&0&1\end{pmatrix}$	$\langle\Sigma_{\{1,2,3\}},\Sigma_{\{4,5,6\}},$ $(1,4)(2,5)(3,6)\rangle$	72
$A_{7,2;0}$	$\begin{pmatrix}1&1&1&1&1&0&0\\1&1&1&0&0&1&1\end{pmatrix}$	$\langle\Sigma_{\{1,2,3\}},(4,5)$ $(6,7),(4,6)(5,7)\rangle$	48
$A^1_{8,2;1}$	$\begin{pmatrix}1&1&1&1&1&0&0&1\\0&0&0&0&0&1&1&1\end{pmatrix}$	$\Sigma_5 \times \Sigma_{\{6,7\}}$	240
$A^2_{8,2;1}$	$\begin{pmatrix}1&1&1&1&0&0&0&1\\0&0&0&0&1&1&1&1\end{pmatrix}$	$\Sigma_4 \times \Sigma_{\{5,6,7\}}$	144
$A^1_{8,2;0}$	$\begin{pmatrix}1&1&1&1&1&1&0&0\\1&1&1&0&0&0&1&1\end{pmatrix}$	$\langle\Sigma_{\{1,2,3\}},\Sigma_{\{4,5,6\}},$ $(7,8),(1,4)(2,5)(3,6)\rangle$	144
$A^2_{8,2;0}$	$\begin{pmatrix}1&1&1&1&1&1&0&0\\1&1&1&1&0&0&1&1\end{pmatrix}$	$\langle\Sigma_4,(5,6),(7,8),$ $(5,7)(6,8)\rangle$	192
$A^1_{9,2;1}$	$\begin{pmatrix}1&1&1&1&1&1&0&0&1\\0&0&0&0&0&0&1&1&1\end{pmatrix}$	$\Sigma_6 \times \Sigma_{\{7,8\}}$	1440
$A^2_{9,2;1}$	$\begin{pmatrix}1&1&1&1&1&0&0&0&1\\0&0&0&0&0&1&1&1&1\end{pmatrix}$	$\Sigma_{\{1,2,3,4,5\}} \times \Sigma_{\{6,7,8\}}$	720
$A^3_{9,2;1}$	$\begin{pmatrix}1&1&1&1&0&0&0&0&1\\0&0&0&0&1&1&1&1&1\end{pmatrix}$	$\langle\Sigma_{\{1,2,3,4\}},\Sigma_{\{5,6,7,8\}}$ $(1,5)(2,6)(3,7)(4,8)\rangle$	1152
$A_{6,3;0}$	$\begin{pmatrix}1&1&0&0&1&0\\1&0&1&0&0&1\\1&0&0&1&1&1\end{pmatrix}$	$\langle(2,6)(3,5),(2,5)(3,6),$ $(1,5)(4,6)\rangle$	24

TABLE I (CON'T)

Name	Generator Matrix	Aut(A)	$\lvert\mathrm{Aut}(A)\rvert$
$A_{7,3;2}$	$\begin{pmatrix}1&1&1&1&1&0&0\\1&1&0&0&1&1&0\\1&1&0&0&0&0&1\end{pmatrix}$	$\langle(1,2),(3,4),$ $(1,3)(2,4)(6,7)\rangle$	8
$A_{7,3;1}$	$\begin{pmatrix}1&1&0&0&0&0&1\\0&0&1&1&0&0&1\\0&0&0&0&1&1&1\end{pmatrix}$	$\langle(1,2),(3,4),(5,6),$ $(1,3)(2,4),(1,5)(2,6)\rangle$	48
$A^1_{7,3;0}$	$\begin{pmatrix}1&1&0&0&1&0&1\\1&0&1&0&0&1&1\\1&0&0&1&1&1&1\end{pmatrix}$	$\langle(1,7),(2,3)(5,6),$ $(2,6)(3,5)\rangle$	8
$A^2_{7,3;0}$	$\begin{pmatrix}1&1&0&0&1&0&1\\1&0&1&0&0&1&1\\1&0&0&1&1&1&0\end{pmatrix}$	$\langle(1,2)(5,7),(2,3)(5,6),$ $(3,4)(5,7),(3,7)(4,5)\rangle$	168
$A^1_{8,3;2}$	$\begin{pmatrix}1&1&1&0&0&1&0&1\\0&0&0&1&1&0&0&1\\0&0&0&0&0&1&1&1\end{pmatrix}$	$\Sigma_{\{1,2,3\}}\times\Sigma_{\{4,5\}}$	12
$A^2_{8,3;2}$	$\begin{pmatrix}1&1&0&0&1&1&0&1\\0&0&1&1&0&0&0&1\\0&0&0&0&1&1&1&1\end{pmatrix}$	$\langle(1,2),(3,4),(5,6),$ $(1,3)(2,4)(7,8)\rangle$	16
$A^1_{8,3;1}$	$\begin{pmatrix}1&1&1&0&0&0&0&1\\0&0&0&1&1&0&0&1\\0&0&0&0&0&1&1&1\end{pmatrix}$	$\langle\Sigma_{\{1,2,3\}},(4,5),(6,7),$ $(4,6)(5,7)\rangle$	48
$A^2_{8,3;1}$	$\begin{pmatrix}1&1&0&0&0&0&1&1\\0&0&1&1&0&0&0&1\\0&0&0&0&1&1&1&1\end{pmatrix}$	$\langle(1,2),(3,4),(5,6),$ $(1,5)(2,6)\rangle$	16
$A^1_{9,3;2}$	$\begin{pmatrix}1&1&1&1&0&0&1&0&1\\0&0&0&0&1&1&0&0&1\\0&0&0&0&0&0&1&1&1\end{pmatrix}$	$\Sigma_{\{1,2,3,4\}}\times\Sigma_{\{5,6\}}$	48
$A^2_{9,3;2}$	$\begin{pmatrix}1&1&1&0&0&0&1&0&1\\0&0&0&1&1&1&0&0&1\\0&0&0&0&0&0&1&1&1\end{pmatrix}$	$\langle\Sigma_{\{1,2,3\}},\Sigma_{\{4,5,6\}},$ $(1,4)(2,5)(3,6)(8,9)\rangle$	72
$A^3_{9,3;2}$	$\begin{pmatrix}1&1&1&0&0&1&1&0&1\\0&0&0&1&1&0&0&0&1\\0&0&0&0&0&1&1&1&1\end{pmatrix}$	$\Sigma_{\{1,2,3\}}\times\Sigma_{\{4,5\}}\times\Sigma_{\{6,7\}}$	24
$A^4_{9,3;2}$	$\begin{pmatrix}1&1&0&0&1&1&1&0&1\\0&0&1&1&0&0&0&0&1\\0&0&0&0&1&1&1&1&1\end{pmatrix}$	$\langle\Sigma_{\{5,6,7\}},(1,2),(3,4),$ $(1,3)(2,4)(8,9)\rangle$	48

TABLE I (CON'T)

Name	Generator Matrix	Aut(A)	$\lvert\text{Aut}(A)\rvert$
$A^1_{9,4;3}$	$\begin{pmatrix}1&1&1&1&1&1&0&0&0\\1&1&0&0&1&1&1&0&0\\1&1&0&0&0&1&0&1&0\\1&1&0&0&0&0&0&0&1\end{pmatrix}$	$\langle(1,2),(3,4)$ $(1,3)(2,4)(5,6)(7,9)\rangle$	8
$A^2_{9,4;3}$	$\begin{pmatrix}1&1&0&0&0&0&1&0&0\\0&0&1&1&0&0&0&1&0\\0&0&0&0&1&1&0&0&1\\0&0&0&0&0&0&1&1&1\end{pmatrix}$	$\langle(1,2),(3,4),(5,6),$ $(1,3)(2,4)(7,8),$ $(1,3,5)(2,4,6)(7,8,9)\rangle$	48

As discussed in Section III, equivalent auxiliary codes, when paired with the same partition, can yield inequivalent critical indecomposable codes. Theorem III.2 and Corollary III.3 described exactly when that could happen, and it boiled down to looking at double-cosets of the automorphism group of the auxiliary code with the block permutation group of the partition. The next proposition gathers the information of this sort that we will need in Section VIII below.

Proposition VII.1: Table II (which spills onto the next page) gives the number of, and representatives for, the $\text{Aut}(A) - B$ double cosets with representatives inside the subset T of Σ_s for various values of A, B, T, and s.

TABLE II
DOUBLE-COSET REPRESENTATIVES

A	T	B	$\#\text{Aut}(A) - B$ Double-Cosets with reps inside T	Non-Identity Reps
$A_{5,2;1}$	Σ_4	$\Sigma_{\{2,3,4\}}$	1	–
		$\Sigma_{\{1,2,3\}}$	1	–
		$\Sigma_{\{3,4\}}$	2	$(2,3)$
		$\Sigma_{\{1,2\}} \times \Sigma_{\{3,4\}}$	2	$(2,3)$
		$\Sigma_{\{2,3\}}$	2	$(1,3)$
	Σ_5	$\Sigma_{\{2,3,4,5\}}$	2	$(1,5)$
		$\Sigma_{\{1,2\}} \times \Sigma_{\{3,4,5\}}$	3	$(1,3),(1,5)$
		$\Sigma_{\{1,2,3\}} \times \Sigma_{\{4,5\}}$	3	$(1,5),(3,5)$
		$\Sigma_{\{3,4,5\}}$	4	$(1,5),(2,5),$ $(2,3)$
$A_{6,2;1}$	Σ_5	$\Sigma_{\{2,3,4,5\}}$	2	$(1,5)$
		$\Sigma_{\{1,2\}} \times \Sigma_{\{3,4,5\}}$	3	$(1,5),$ $(1,4)(2,5)$
		$\Sigma_{\{3,4,5\}}$	4	$(1,5),(2,5),$ $(1,4)(2,5)$
		$\Sigma_{\{1,2,3\}} \times \Sigma_{\{4,5\}}$	3	$(1,5),$ $(1,4)(2,5)$
	Σ_6	$\Sigma_{\{2,3,4,5,6\}}$	3	$(1,4),(1,6)$
		$\Sigma_{\{1,2\}} \times \Sigma_{\{3,4,5,6\}}$	5	$(2,6),(1,4),$ $(1,4)(2,5),$ $(1,5)(2,6)$
$A_{6,2;0}$	Σ_6	$\Sigma_{\{2,3,4,5,6\}}$	1	–
		$\Sigma_{\{1,2\}} \times \Sigma_{\{3,4,5,6\}}$	2	$(1,6)$

TABLE II (CON'T)

A	T	B	$\#\mathrm{Aut}(A)-B$ Double-Cosets with reps inside K	Non-Identity Reps
$A_{7,3;2}$	$\Sigma_{\{6,7\}}\cdot\Sigma_6$	Σ_6	1	–
		$\Sigma_{\{2,3,4,5,6\}}$	4	$(6,7),(1,6),(1,5)$
	$\Sigma_5\times\Sigma_{\{6,7\}}$	$\Sigma_{\{2,3,4,5\}}\times\Sigma_{\{6,7\}}$	2	$(1,5)$
		$\Sigma_{\{1,2\}}\times\Sigma_{\{3,4,5\}}\times\Sigma_{\{6,7\}}$	3	$(1,5),(2,3)$
$A^1_{7,2;1}$	Σ_6	$\Sigma_{\{2,3,4,5,6\}}$	2	$(1,6)$
		$\Sigma_{\{1,2\}}\times\Sigma_{\{3,4,5,6\}}$	3	$(1,6),(1,5)(2,6)$
	Σ_7	$\Sigma_{\{2,3,4,5,6,7\}}$	3	$(1,7),(1,5)$
$A^2_{7,2;1}$	Σ_6	$\Sigma_{\{2,3,4,5,6\}}$	1	–
		$\Sigma_{\{1,2\}}\times\Sigma_{\{3,4,5,6\}}$	2	$(1,6)$
	Σ_7	$\Sigma_{\{2,3,4,5,6,7\}}$	2	$(1,7)$
$A^1_{8,3;2}$	$\Sigma_{\{7,8\}}\cdot\Sigma_7$	Σ_7	2	$(7,8)$
	$\Sigma_6\times\Sigma_{\{7,8\}}$	$\Sigma_{\{2,3,4,5,6\}}\times\Sigma_{\{7,8\}}$	3	$(1,6),(1,4)$
$A^2_{8,3;2}$	$\Sigma_{\{7,8\}}\cdot\Sigma_7$	Σ_7	1	–
	$\Sigma_6\times\Sigma_{\{7,8\}}$	$\Sigma_{\{2,3,4,5,6\}}\times\Sigma_{\{7,8\}}$	2	$(1,6)$
$A^1_{8,2;1}$	Σ_7	$\Sigma_{\{2,3,4,5,6,7\}}$	2	$(1,7)$
$A^2_{8,2;1}$	Σ_7	$\Sigma_{\{2,3,4,5,6,7\}}$	2	$(1,7)$
$A_{6,3;0}$	Σ_6	$\Sigma_{\{2,3,4,5,6\}}$	1	–
$A_{7,3;1}$	Σ_6	$\Sigma_{\{2,3,4,5,6\}}$	1	–
$A_{7,2;0}$	Σ_7	$\Sigma_{\{2,3,4,5,6,7\}}$	2	$(1,7)$

Proof: The main tool is the standard formula

$$|H\cdot x\cdot K| = \frac{|H||K|}{|H\cap xKx^{-1}|} \qquad (**)$$

where H and K are subgroups of the group G and $x\in G$. (See, for example, [6].) The computations can easily be done by hand or with a computer algebra package such as MAGMA ([3]) or GAP ([5]). The proofs all follow roughly the same method and we will give the details of only one line of the table here. The example we give has many complicating details; most lines of the table are in fact much easier to verify.

We will prove that there are precisely four $\mathrm{Aut}(A_{7,3;2})-\Sigma_{\{2,3,4,5,6\}}$ double-cosets with representatives inside the set $\Sigma_{\{6,7\}}\cdot\Sigma_6$. First, we recall that $\mathrm{Aut}(A_{7,3;2}) = \langle(1,2),(3,4),(1,3)(2,4)(6,7)\rangle$ has order 8, and we note that $\Sigma_{\{2,3,4,5,6\}}$ is isomorphic to Σ_5 and thus has order 120. Since $\tau\Sigma_{\{2,3,4,5,6\}}\tau^{-1} = \Sigma_{\{\tau(2),\tau(3),\tau(4),\tau(5),\tau(6)\}}$ for any $\tau\in\Sigma_7$, applying formula $(**)$ is easy. We find that

$$|\mathrm{Aut}(A_{7,3;2})\cdot\Sigma_{\{2,3,4,5,6\}}| = \frac{(8)(120)}{2} = 480,$$

$$|\mathrm{Aut}(A_{7,3;2})\cdot(6,7)\cdot\Sigma_{\{2,3,4,5,6\}}| = \frac{(8)(120)}{|\mathrm{Aut}(A_{7,3;2})\cap\Sigma_{\{2,3,4,5,7\}}|} = \frac{(8)(120)}{2} = 480,$$

$$|\mathrm{Aut}(A_{7,3;2})\cdot(1,6)\cdot\Sigma_{\{2,3,4,5,6\}}| = \frac{(8)(120)}{|\mathrm{Aut}(A_{7,3;2})\cap\Sigma_5|} = \frac{(8)(120)}{4} = 240,$$

and

$$|\mathrm{Aut}(A_{7,3;2})\cdot(1,5)\cdot\Sigma_{\{2,3,4,5,6\}}| = \frac{(8)(120)}{|\mathrm{Aut}(A_{7,3;2})\cap\Sigma_{\{1,2,3,4,6\}}|} = \frac{(8)(120)}{4} = 240.$$

Our next task is to see if these four double-cosets are distinct. Clearly, the only way that this could fail is if the first two are equal or the last two are equal. However, any element of the second double-coset is of the form $\alpha(6,7)\beta$, where $\alpha\in\mathrm{Aut}(A_{7,3;2})$ and $\beta\in\Sigma_{\{2,3,4,5,6\}}$. Such a permutation cannot fix both 1 and 7, and so the identity permutation (which is clearly a member of the first double-coset) is not contained in the second double-coset. This shows that the first two double-cosets are distinct. Similarly, any element of the fourth double-coset sends 5 to 1, and so the permutation $(1,6)$ (which is clearly a member of the third double-coset) is not an element of the fourth double-coset. This shows that the last two double-cosets are distinct.

It is easy to check that each of these four double-cosets is entirely contained in $\sigma_{\{6,7\}}\cdot\Sigma_6$. Thus, since $480+480+240+240 = 1440 = |\Sigma_{\{6,7\}}\cdot\Sigma_6|$, we have

found all the $\mathrm{Aut}(A_{7,3;2}) - \Sigma_{\{2,3,4,5,6\}}$ double-cosets with representatives inside $\Sigma_{\{6,7\}} \cdot \Sigma_6$. ∎

VIII. Enumeration of Critical Indecomposable Codes of Dimension At Most 10

Using the results discussed so far, we can write down constructions for all critical indecomposable codes of dimension at most 10. Recall that in order to construct a critical indecomposable code of dimension k and length n, we need two things: (1) a partition $\pi = (x_1, \ldots, x_r, x')$ of n where $x' \geq 0$ and, for $1 \leq i \leq r$, we have $x_i \geq 2$, and (2) an auxiliary code A of length $s := r + x'$ and dimension $l := s + k - n$, such that the last x' columns of A are critical. For clarity, we make two notational conventions. First, when several values of x_i have the same value, we will group them and use an exponent to signify the number of x_i's with the value. For example, we will write $(4, 2^3)$ rather than $(4, 2, 2, 2)$. Second, when we use a partition with $x' = 0$, we will write $\pi = (x_1, \ldots, x_r)$, omitting the "0", and when we have $x' > 0$, we will write $\pi = (x_1, \ldots, x_r, 1^{x'})$. Thus (2^7) unambiguously means the partition of 14 into $r = 7$ parts of size 2, while $(2^6, 1^2)$ means the partition of 14 into $r = 6$ pieces of size 2 and $x' = 2$ pieces of size 1. In particular, the second partition can be used only with $A^1_{8,3;2}$ or $A^2_{8,3;2}$ as the auxiliary code (yielding in either case a critical indecomposable code of length 14 and dimension 9), while the first partition can be used with $A_{7,3;2}$, $A_{7,3;1}$, $A^1_{7,3;0}$, or $A^2_{7,3;0}$ to obtain a critical indecomposable code of length 14 and dimension 10, or with $A^1_{7,2;1}$, $A^2_{7,2;1}$, or $A_{7,2;0}$ to obtain a critical indecomposable code of length 14 and dimension 9.

We have already discussed critical indecomposable codes of dimension at most 4, so we begin with dimension 5. For each dimension, we discuss the parameters of auxiliary codes which must be used and the partitions which can go along with them. When necessary, we refer to the results of the previous section to determine equivalence. We do only dimension 5, dimension 6, and one case of dimension 10 in detail; all other cases are very similar. At the end of this section is a theorem summarizing our results, including a table giving the complete enumeration of critical indecomposable codes of dimension at most 10.

A. Critical Indecomposable Codes of Dimension 5

Any critical indecomposable code of dimension 5 has length n with $6 \leq n \leq 8$, and we know that there is exactly one, $C_{6,5}$, of length 6 and one, $C_{8,5}$, of length 8. For length 7, the formula $s = l + (n - k)$ gives $s = l + 2$. This means that $l = 1$ and $s = 3$. Therefore we need to find all partitions of 7 into 3 pieces, each one of which is at least 2. The only such partition is $(3, 2^2)$. This partition, when paired with the auxiliary code $A_{3,1}$, yields the unique critical indecomposable code of length 7 and dimension 5.

B. Critical Indecomposable Codes of Dimension 6

The possible lengths n must satisfy $7 \leq n \leq 10$. In length 7, there is only $C_{7,6}$, and in length 10, there is only $C_{10,6}$. In length 8, we have $s = l + 2$, so $A_{3,1}$ is the only possible auxiliary code. It can be paired with either of two partitions: $(4, 2^2)$ and $(3^2, 2)$.

For length 9, we have $s = l + 3$. On the other hand, by Corollary VI.4, we have $s \leq 6 - 1 = 5$. Thus we have 2 possibilities: $l = 1$, $s = 4$ or $l = 2$, $s = 5$. In the first case, we need the auxiliary code $A_{4,1}$, paired with a partition of 9 into 4 pieces, each of which is at least 2. The only such partition is $(3, 2^3)$. In the second case, we need an auxiliary code of dimension 2 and length 5, and the only such code is $A_{5,2;1}$. Therefore, we need a partition of 9 into 5 pieces, at most one of which is 1, and the other four of which are at least 2. The only such partition is $\pi = (2^4, 1)$. It is clear that any permutation of the columns of $A_{5,2;1}$ which preserves the last column as being critical will yield, when paired with the partition π, the same critical indecomposable code (up to equivalence).

C. Critical Indecomposable Codes of Dimensions 7, 8, 9, and 10

The construction of critical indecomposable codes of dimensions 7, 8, 9, and 10 follows the same pattern as indicated above. As we did in Section VII, we will choose one particularly complicated example to do in detail, and leave the rest to the reader.

To construct all critical indecomposable codes of dimension 10 and length 14, Corollary VI.4 combined with the formula $n - k = s - l$ gives us that we need $s = l + 4 \leq 9$. Thus the possibilities for (s, l) are $(5, 1)$, $(6, 2)$, $(7, 3)$, $(8, 4)$, and $(9, 5)$. However, to partition 14 into nine pieces, we need at least four 1's, and the shortest admissible code of dimension 5 with 4 critical columns has length 11 by Corollary VI.3. Thus $(s, l) = (9, 5)$ is not possible. Also, since we saw in Section VII that every admissible code of length 8 and dimension 4 has at most one critical column, and any partition of 14 into 8 pieces must involve at least two 1's, $(8, 4)$ is not possible either. In the case $(s, l) = (5, 1)$ we have the auxiliary code $A_{5,1}$ and the partitions $(6, 2^4)$, $(5, 3, 2^3)$, $(4^2, 2^3)$, $(4, 3^2, 2^2)$, and $(3^4, 2)$.

When $(s, l) = (6, 2)$, we have $A_{6,2;1}$ and $A_{6,2;0}$. Our possible auxiliary codes are $A_{7,3;2}$, $A_{7,3;1}$, $A^1_{7,3;0}$, and $A^2_{7,3;0}$. We have five possible partitions: $\pi_1 = (4, 2^5)$, $\pi_2 = (3^2, 2^4)$, $\pi_3 = (5, 2^4, 1)$, $\pi_4 = (4, 3, 2^3, 1)$, and $\pi_5 = (3^3, 2^2, 1)$. Their corresponding block permutation groups are $B(\pi_1) = \Sigma_{\{2,3,4,5,6\}}$, $B(\pi_2) = \Sigma_{\{1,2\}} \times \Sigma_{\{3,4,5,6\}}$, $B(\pi_3) = \Sigma_{\{2,3,4,5\}}$, $B(\pi_4) = \Sigma_{\{3,4,5\}}$, and $B(\pi_5) = \Sigma_{\{1,2,3\}} \times \Sigma_{\{4,5\}}$. The first two partitions can be used with either $A_{6,2;0}$ or $A_{6,2;1}$ as auxiliary codes, and, by Corollary III.3, we need to look inside Σ_6 for double-coset representatives. The last three partitions can only be used with $A_{6,2;1}$, and we need to look inside Σ_5 for double-coset representatives.

By Proposition VII.1, π_1 yields exactly one critical indecomposable code when paired with $A_{6,2;0}$, and π_2 yields exactly two. Similarly, the auxiliary code $A_{6,2;1}$ yields three codes with π_1, five with π_2, two with π_3, four with π_4, and three with π_5.

Now we look at constructing critical indecomposable codes of length 14 with auxiliary codes satisfying $(s, l) = (7, 3)$. This time, there are four possible partitions: $\pi_1 =$

(2^7), $\pi_2 = (3, 2^5, 1)$, $\pi_3 = (4, 2^4, 1^2)$, and $\pi_4 = (3^2, 2^3, 1^2)$. The first partition can be used with any of the four auxiliary codes $A^1_{7,3;0}$, $A^2_{7,3;0}$, $A_{7,3;1}$, or $A_{7,3;2}$, and it is clear that, no matter which of these auxiliary codes is used, we don't need to worry about double-cosets. We have $B(\pi_2) = \Sigma_{\{2,3,4,5,6\}}$ and we need to look for double-cosets inside Σ_6 when we use π_2 with $A_{7,3;1}$, and inside $\Sigma_{\{6,7\}} \cdot \Sigma_6$ when we use π_2 with $A_{7,3;2}$. (We are not allowed to use $A^1_{7,3;0}$ or $A^2_{7,3;0}$ because π_2 requires at least one critical column in our auxiliary code.) By Proposition VII.1, we get one critical indecomposable code from π_2 and $A_{7,3;1}$ and four from π_2 and $A_{7,3;2}$. We have $B(\pi_3) = \Sigma_{\{2,3,4,5\}} \times \Sigma_{\{6,7\}}$ and $B(\pi_4) = \Sigma_{\{1,2\}} \times \Sigma_{\{3,4,5\}} \times \Sigma_{\{6,7\}}$. These two partitions can only be used with $A_{7,3;2}$, and we need to look inside $\Sigma_5 \times \Sigma_{\{6,7\}}$ for double-cosets. Again referring to Proposition VII.1, we find that we obtain two critical indecomposable codes from π_3 and three from π_4.

D. Summary

The remaining critical indecomposable codes of dimensions at most 10 are constructed in a similar manner, giving the following theorem:

Theorem VIII.1: The critical indecomposable codes of dimension at most 10 can be described as follows:

1. $\mathbb{F}$ is the unique critical indecomposable code of dimension 1.
2. $C_{3,2}$ is the unique critical indecomposable code of dimension 2.
3. $C_{4,3}$ is the unique critical indecomposable code of dimension 3.
4. There are exactly two critical indecomposable codes of dimension 4: $C_{5,4}$ and $C_{6,4}$.
5. There are exactly three critical indecomposable codes of dimension 5: $C_{6,5}$, $C_{8,5}$, and a code of length 7.
6. There are exactly six critical indecomposable codes of dimension 6: $C_{7,6}$, $C_{10,6}$, two codes of length 8, and two of length 9.
7. There are exactly eleven critical indecomposable codes of dimension 7: $C_{8,7}$, $C_{12,7}$, three codes of length 9, four of length 10, and two of length 11.
8. There are exactly twenty-four critical indecomposable codes of dimension 8: $C_{9,8}$, $C_{14,8}$, four codes of length 10, eight of length 11, seven of length 12, and three of length 13.
9. There are exactly fifty-one critical indecomposable codes of dimension 9: $C_{10,9}$, $C_{16,9}$, five codes of length 11, fifteen of length 12, sixteen of length 13, ten of length 14, and three of length 15.
10. There are exactly one hundred and twenty critical indecomposable codes of dimension 10: $C_{11,10}$, $C_{18,10}$, seven codes of length 12, twenty-four of length 13, thirty-nine of length 14, thirty of length 15, fourteen of length 16, and four of length 17.

More precisely, Table III (which spans the rest of this article) describes the partitions and auxiliary codes needed to construct all critical indecomposable codes of dimension at most 10.

TABLE III
CRITICAL INDECOMPOSABLE CODES OF DIMENSION AT MOST 10

Dim.	Length	Partition	Aux. Code
1	1	–	–
2	3	–	–
3	4	–	–
4	5	–	–
	6	(2^3)	$A_{3,1}$
5	6	–	–
	7	$(3, 2^2)$	$A_{3,1}$
	8	(2^4)	$A_{4,1}$
6	7	–	–
	8	$(4, 2^2)$	$A_{3,1}$
		$(3^2, 2)$	
	9	$(3, 2^3)$	$A_{4,1}$
		$(2^4, 1)$	$A_{5,2;1}$
	10	(2^5)	$A_{5,1}$
7	8	–	–
	9	$(5, 2^2)$	$A_{3,1}$
		$(4, 3, 2)$	
		(3^3)	
	10	$(4, 2^3)$	$A_{4,1}$
		$(3^2, 2^2)$	
		$(3, 2^3, 1)$	$A_{5,2;1}$
		(2^5)	
	11	$(3, 2^4)$	$A_{5,1}$
		$(2^5, 1)$	$A_{6,2;1}$
	12	(2^6)	$A_{6,1}$
8	9	–	–
	10	$(6, 2^2)$	$A_{3,1}$
		$(5, 3, 2)$	
		$(4^2, 2)$	
		$(4, 3^2)$	
	11	$(5, 2^3)$	$A_{4,1}$
		$(4, 3, 2^2)$	
		$(3^3, 2)$	
		$(3, 2^4)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(1,5)}$
		$(4, 2^3, 1)$	$A_{5,2;1}$
		$(3^2, 2^2, 1)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(2,3)}$
	12	$(4, 2^4)$	$A_{5,1}$
		$(3^2, 2^3)$	
		(2^6)	$A_{6,2;0}$
			$A_{6,2;1}$
		$(3, 2^4, 1)$	$A_{6,2;1}$
			$(A_{6,2;1})^{(1,5)}$
		$(2^5, 1^2)$	$A_{7,3;2}$
	13	$(3, 2^5)$	$A_{6,1}$
		$(2^6, 1)$	$A^1_{7,2;1}$
			$A^2_{7,2;1}$
	14	(2^8)	$A_{8,1}$

TABLE III (CON'T)

Dim.	Length	Partition	Aux. Code
9	10	–	–
	11	$(7,2^2)$	$A_{3,1}$
		$(6,3,2)$	
		$(5,4,2)$	
		$(5,3^2)$	
		$(4^2,3)$	
	12	$(6,2^3)$	$A_{4,1}$
		$(5,3,2^2)$	
		$(4^2,2^2)$	
		$(4,3^2,2)$	
		(3^4)	
		$(4,2^4)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(1,5)}$
		$(3^2,2^3)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(1,3)}$
			$(A_{5,2;1})^{(1,5)}$
		$(5,2^3,1)$	$A_{5,2;1}$
		$(4,3,2^2,1)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(2,3)}$
		$(3^3,2,1)$	$A_{5,2;1}$
		(2^6)	$A_{6,3;0}$
	13	$(5,2^4)$	$A_{5,1}$
		$(4,3,2^3)$	
		$(3^3,2^2)$	
		$(3,2^5)$	$A_{6,2;0}$
			$A_{6,2;1}$
			$(A_{6,2;1})^{(1,4)}$
			$(A_{6,2;1})^{(1,6)}$
		$(4,2^4,1)$	$A_{6,2;1}$
			$(A_{6,2;1})^{(1,5)}$
		$(3^2,2^3,1)$	$A_{6,2;1}$
			$(A_{6,2;1})^{(1,5)}$
			$(A_{6,2;1})^{(1,4)(2,5)}$
		$(2^6,1)$	$A_{7,3;1}$
			$A_{7,3;2}$
		$(3,2^4,1^2)$	$A_{7,3;2}$
			$(A_{7,3;2})^{(1,5)}$
	14	$(4,2^5)$	$A_{6,1}$
		$(3^2,2^4)$	
		(2^7)	$A_{7,2;0}$
			$A^1_{7,2;1}$
			$A^2_{7,2;1}$
		$(3,2^5,1)$	$A^1_{7,2;1}$
			$(A^1_{7,2;1})^{(1,6)}$
			$A^2_{7,2;1}$
		$(2^6,1^2)$	$A^1_{8,3;2}$
			$A^2_{8,3;2}$

TABLE III (CON'T)

Dim.	Length	Partition	Aux. Code
9 *(con't)*	15	$(3,2^6)$	$A_{7,1}$
		$(2^7,1)$	$A^1_{8,2;1}$
			$A^2_{8,2;1}$
	16	(2^8)	$A_{8,1}$
10	11	–	–
	12	$(8,2^2)$	$A_{3,1}$
		$(7,3,2)$	
		$(6,4,2)$	
		$(5^2,2)$	
		$(6,3^2)$	
		$(5,4,3)$	
		(4^3)	
	13	$(7,2^3)$	$A_{4,1}$
		$(6,3,2^2)$	
		$(5,4,2^2)$	
		$(5,3^2,2)$	
		$(4^2,3,2)$	
		$(4,3^3)$	
		$(5,2^4)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(1,5)}$
		$(4,3,2^3)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(1,5)}$
			$(A_{5,2;1})^{(2,5)}$
			$(A_{5,2;1})^{(2,3)}$
		$(3^3,2^2)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(1,5)}$
			$(A_{5,2;1})^{(3,5)}$
		$(6,2^3,1)$	$A_{5,2;1}$
		$(5,3,2^2,1)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(2,3)}$
		$(4^2,2^2,1)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(2,3)}$
		$(4,3^2,2,1)$	$A_{5,2;1}$
			$(A_{5,2;1})^{(1,3)}$
		$(3^4,1)$	$A_{5,2;1}$
		$(3,2^5)$	$A_{6,3;0}$
	14	$(6,2^4)$	$A_{5,1}$
		$(5,3,2^3)$	
		$(4^2,2^3)$	
		$(4,3^2,2^2)$	
		$(3^4,2)$	
		$(4,2^5)$	$A_{6,2;0}$
			$A_{6,2;1}$
			$(A_{6,2;1})^{(1,4)}$
			$(A_{6,2;1})^{(1,6)}$

TABLE III (CON'T)

Dim.	Length	Partition	Aux. Code
10 *(con't)*	14 *(con't)*	$(3^2, 2^4)$	$A_{6,2;0}$
			$(A_{6,2;0})^{(1,6)}$
			$A_{6,2;1}$
			$(A_{6,2;1})^{(2,6)}$
			$(A_{6,2;1})^{(1,4)}$
			$(A_{6,2;1})^{(1,4)(2,5)}$
			$(A_{6,2;1})^{(1,5)(2,6)}$
		$(5, 2^4, 1)$	$A_{6,2;1}$
			$(A_{6,2;1})^{(1,5)}$
		$(4, 3, 2^3, 1)$	$A_{6,2;1}$
			$(A_{6,2;1})^{(1,5)}$
			$(A_{6,2;1})^{(2,5)}$
			$(A_{6,2;1})^{(1,4)(2,5)}$
		$(3^3, 2^2, 1)$	$A_{6,2;1}$
			$(A_{6,2;1})^{(1,5)}$
			$(A_{6,2;1})^{(1,4)(2,5)}$
		(2^7)	$A^1_{7,3;0}$
			$A^2_{7,3;0}$
			$A_{7,3;1}$
			$A_{7,3;2}$
		$(3, 2^5, 1)$	$A_{7,3;1}$
			$A_{7,3;2}$
			$(A_{7,3;2})^{(6,7)}$
			$(A_{7,3;2})^{(1,6)}$
			$(A_{7,3;2})^{(1,5)}$
		$(4, 2^4, 1, 1)$	$A_{7,3;2}$
			$(A_{7,3;2})^{(1,5)}$
		$(3^3, 2^3, 1^2)$	$A_{7,3;2}$
			$(A_{7,3;2})^{(1,5)}$
			$(A_{7,3;2})^{(2,3)}$
	15	$(5, 2^5)$	$A_{6,1}$
		$(4, 3, 2^4)$	
		$(3^3, 2^3)$	
		$(3, 2^6)$	$A_{7,2;0}$
			$(A_{7,2;0})^{(1,7)}$
			$A^1_{7,2;1}$
			$(A^1_{7,2;1})^{(1,7)}$
			$(A^1_{7,2;1})^{(1,5)}$
			$A^2_{7,2;1}$
			$(A^2_{7,2;1})^{(1,7)}$
		$(4, 2^5, 1)$	$A^1_{7,2;1}$
			$(A^1_{7,2;1})^{(1,6)}$
			$A^2_{7,2;1}$

TABLE III (CON'T)

Dim.	Length	Partition	Aux. Code
10 *(con't)*	15 *(con't)*	$(3^2, 2^4, 1)$	$A^1_{7,2;1}$
			$(A^1_{7,2;1})^{(1,6)}$
			$(A^1_{7,2;1})^{(1,5)(2,6)}$
			$A^2_{7,2;1}$
			$(A^2_{7,2;1})^{(1,6)}$
		$(2^7, 1)$	$A^1_{8,3;1}$
			$A^2_{8,3;1}$
			$A^1_{8,3;2}$
			$(A^1_{8,3;2})^{(7,8)}$
			$A^2_{8,3;2}$
		$(3, 2^5, 1^2)$	$A^1_{8,3;2}$
			$(A^1_{8,3;2})^{(1,6)}$
			$(A^1_{8,3;2})^{(1,4)}$
			$A^2_{8,3;2}$
			$(A^2_{8,3;2})^{(1,6)}$
		$(2^6, 1^3)$	$A^1_{9,4;3}$
			$A^2_{9,4;3}$
	16	$(4, 2^6)$	$A_{7,1}$
		$(3^2, 2^5)$	
		(2^8)	$A^1_{8,2;0}$
			$A^2_{8,2;0}$
			$A^1_{8,2;1}$
			$A^2_{8,2;1}$
		$(3, 2^6, 1)$	$A^1_{8,2;1}$
			$(A^1_{8,2;1})^{(1,7)}$
			$A^2_{8,2;1}$
			$(A^2_{8,2;1})^{(1,7)}$
		$(2^7, 1^2)$	$A^1_{9,3;2}$
			$A^2_{9,3;2}$
			$A^3_{9,3;2}$
			$A^4_{9,3;2}$
	17	$(3, 2^7)$	$A_{8,1}$
		$(2^8, 1)$	$A^1_{9,2;1}$
			$A^2_{9,2;1}$
			$A^3_{9,2;1}$
	18	(2^9)	$A_{9,1}$

REFERENCES

[1] E. F. Assmus, Jr. The category of linear codes. *IEEE Transactions on Information Theory*, 44:612–629, 1998.

[2] E. F. Assmus, Jr and H. F. Mattson, Jr. Error-correcting codes: An axiomatic approach. *Inform. Contr.*, 6:315–330, 1963.

[3] W. Bosma and J. J. Cannon. *Handbook of Magma Functions*. Sydney, Australia, 1996.

[4] J. Fripertinger and A. Kerber. Isometry classes of indecomposable linear codes. In G. Cohen and M. Guisti, editors, *Proc. Int. Symp., AAECC-11, Paris 1995*, volume 948 of *Lecture Notes in Computer Science*, pages 194–204, Berlin, 1995. Springer-Verlag.

[5] The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.2*, 1999. (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[6] I. N. Herstein. *Topics in Algebra*. John Wiley & Sons, New York, second edition, 1975.

[7] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1993.

[8] U.S.R. Murty. Extremal critically connected matroids. *Discr. Math.*, 8:49–58, 1979.

[9] J. E. Roos. An algebraic study of group and nongroup error-correcting codes. *Inform. Contr.*, 8:195–214, 1965.

[10] C. E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. Journal*, 27:379–423 and 623–656, 1948.

[11] D. Slepian. Some further theory of group codes. *Bell Syst. Tech. Journal*, 39:1219–1252, 1960.