Constant-Weight Array Codes
Maximilien Gadouleau*
September 12, 2017

Abstract

Binary constant-weight codes have been extensively studied, due to both their numerous applications and to their theoretical significance. In particular, constant-weight codes have been proposed for error correction in store and forward. In this paper, we introduce constant-weight array codes (CWACs), which offer a tradeoff between the rate gain of general constant-weight codes and the low decoding complexity of liftings. CWACs can either be used in the on-shot setting introduced earlier or in a multi-shot approach, where one codeword consists of several messages. The multi-shot approach generalizes the one-shot approach and hence allows for higher rate gains. We first give a construction of CWACs based on concatenation, which generalizes the traditional erasure codes, and also provide a decoding algorithm for these codes. Since CWACs can be viewed as a generalization of both binary constant-weight codes and nonrestricted Hamming metric codes, CWACs thus provide an additional degree of freedom to both problems of determining the maximum cardinality of constant-weight codes and nonrestricted Hamming metric codes. We then investigate their theoretical significance. We first generalize many classical bounds derived for Hamming metric codes or constant-weight codes in the CWAC framework. We finally relate the maximum cardinality of a CWAC to that of a constant-weight code, of a nonrestricted Hamming metric code, and of a spherical code.

1 Introduction

Binary constant-weight codes have been widely studied [1] due to their applications to codes for asymmetric channels [2], DC-free codes [3], and spherical codes [4]. Recently, their connections to constant-dimension codes [5, 6], which were proposed for error and erasure correction in noncoherent network coding [7], renewed their interest. Constant-weight codes have also been proposed for error correction in store and forward [8]. Although nonbinary constant-weight codes have also received some attention [9, 10], we shall only consider binary constant-weight codes. These codes also have a strong theoretical significance, as bounds on the maximum cardinality of a constant-weight code also yield bounds on the cardinality of binary Hamming metric codes [11, 12]. Also, the Johnsonian is a very structured mathematical object, known as an association scheme.

In [8], we showed how binary codes in general and constant-weight codes in particular can be used for error correction in store and forward. This approach generalizes the traditional approach of lifting a Hamming metric code (typically a Reed-Solomon code), and higher data rates can be achieved by using such constant-weight codes. However, the encoding and complexities when using general constant-weight codes are usually much higher than their counterparts for liftings of Reed-Solomon codes. In this paper, we introduce constant-weight array codes, which can be viewed as a tradeoff between data rate and complexity because the two extreme cases of CWACs are exactly liftings of Hamming metric codes and general constant-weight codes. Due to their particular structure, CWACs can also be viewed as generalized constant-weight codes. Therefore, we believe CWACs also have an important theoretical significance, which can already be seen through the bounds we derive in this paper.

The rest of the paper is organized as follows. Section 2 reviews some necessary background. Section 3.1 provides a construction of CWACs based on concatenation, and designs a decoding algorithm for

*Department of Computer Science, Durham University, Durham DH1 3LE, UK. Email: m.r.gadouleau@durham.ac.uk
these codes. The relations between CWACs and other classes of codes are investigated in Section 3.3 while the maximum cardinality of CWACs is studied in Section 3.

2 Preliminaries

In this section, we review the following three classes of codes: constant-weight codes, Hamming metric codes, and spherical codes. We recall that the minimum distance of a code is the minimum distance over all pairs of distinct codewords, while the diameter of an anticode is the maximum distance between two codewords.

We denote the set of all vectors in $\mathbb{GF}(2)^n$ and weight $w$ as $J(n, w)$. A constant-weight code is defined as any subset of $J(n, w)$ with a given minimum Hamming distance, while a constant-weight anticode is also a subset of $J(n, w)$ with a prescribed diameter. Let $B(n, w, d)$ be the maximum cardinality of a binary constant-weight code of length $n$, weight $w$, and minimum Hamming distance $2d$. Similarly, let $\beta(n, w, \delta)$ be the maximum cardinality of a constant-weight anticode in $J(n, w)$ with diameter $2\delta$. A lower bound on $\beta(n, w, \delta)$ is given by the number of subsets of cardinality $w$ which intersect a given subset of cardinality $w - \delta + 2i$ in at least $w - \delta$ positions for any $0 \leq i \leq \delta$:

$$\beta(n, w, \delta) \geq \max_{0 \leq i \leq \delta} \sum_{d=0}^{\delta} \binom{w - \delta + 2i}{i - \frac{d-\delta}{2}} \binom{n - w + \delta - 2i}{\frac{d+\delta}{2} - i}.$$  

The lower bound in (1) is known to be tight provided $n$ is large enough [13] and is conjectured in [14] to be tight for all values.

A nonrestricted Hamming metric code is a nonempty subset of $[q]^n$, where $q \in \mathbb{N}$ and $[q] = \{0, 1, \ldots, q - 1\}$. Let $C(q, n, d)$ be the maximum cardinality of a code in $[q]^n$ with minimum Hamming distance $d$. Finally, let $\gamma(q, n, \delta)$ be the maximum cardinality of an anticode in $[q]^n$ with diameter $\delta$. Remarkably, the value of $\gamma(q, n, \delta)$ is determined in [15] and given by

$$\gamma(q, n, \delta) = q^{\delta - 2r} \sum_{i=0}^{r} \binom{n}{i} (q - 1)^i,$$

where $r$ is the largest integer such that $2r < \min\left\{\delta + 1, \frac{2n - \delta - 1}{q - 2}\right\}$.

A spherical code of dimension $n$ is a set of points on the unit sphere in $\mathbb{R}^n$ with the Euclidean norm. The maximum cosine $s$ of a spherical code is related to its minimum Euclidean distance $d_E$ by $s = 1 - \frac{d_E^2}{2}$. The maximum cardinality of a spherical code of dimension $n$ and maximum cosine $s$ is denoted as $A_S(n, s)$. The exact value of $A_S(n, s)$ is known for $s \leq 0$ and given by (see [4])

$$A_S(n, s) = \begin{cases} 1 - \frac{1}{s}, & \text{if } s \leq -\frac{1}{n} \\ n + 1, & \text{if } -\frac{1}{n} \leq s < 0 \\ 2n, & \text{if } s > 0 \end{cases},$$

while bounds on $A_S(n, s)$ for $s > 0$ are given in [16, 17].

3 Constant-weight array codes

3.1 Construction of CWACs by concatenation

The model reviewed in Section 1 identifies a message with a binary vector whose weight is equal to the number of packets in the message. Accordingly, we investigated using constant-weight codes for error control in store and forward in [8], where each codeword corresponds to a message. This approach falls short when the number of errors that typically occur on the network is very low. For instance, in order to correct one packet loss and one packet injection every ten transmissions, one need to use...
a constant-weight code with minimum distance at least 5 for each transmission. Therefore, in this setting, we could correct one packet loss and one packet injection at every single transmission. In this section, we generalize the constant-weight code approach by considering codewords associated to sequences of messages. In the example considered above, we could then use codewords made of ten messages, and use a code with error correction capability of 2. In general, using codes on several sequences of messages allows to adjust the error correction of the code more accurately to the number of errors produced by the network, hence increasing the data rate.

A constant-weight array code (CWAC) is defined as a nonempty subset of words in $J(m, w)^n$. Hence a constant-weight code in $J(m, w)$ can be viewed as a CWAC of length 1. In this section, we design a class of good CWACs with low-complexity decoders. In Proposition 1 below we construct a CWAC by concatenation, where the outer code is a nonrestricted Hamming metric code and the inner code is a constant-weight code. This can be viewed as a generalization of the lifting operation defined in [8].

**Proposition 1** (Construction of CWACs by concatenation). Let $I \subseteq J(m, w)$ be a constant-weight code with minimum distance $2f$ and $O \subseteq I^n$ be a nonrestricted code with minimum distance $e$. Then the concatenated code $O \circ I$ is a CWAC in $J(m, w)^n$ with minimum distance at least $2ef$.

The proof of Proposition 1 is straightforward and hence omitted.

The concatenation construction is well fitted for our purpose, as it ensures that each message is a codeword in a constant-weight code with minimum distance $2f$.

We first investigate when a modified Reed-Solomon code can be used as outer code. We remark that for $w = 1$, the construction in Proposition 1 reduces to the lifting operation. The lifting of a Reed-Solomon code requires that $n \leq m$, that is, the total weight $W = n$ and the total length $M = nm$ are related by $W \leq \sqrt{M}$. Therefore, this is a strong limitation on the number of packets in a message. On the other hand, we remark that when $w > 1$, the constraint on the parameter, given by $n \leq B(m, w, f)$ is loose when $f = 1$, that is $A(m, n, w, d) \geq w^{n-d+1}$. The algorithm to decode $I$ is straightforward: enumerate all the vectors in $J(m, w)$ at distance at most $f - 1$ from the received column and check if it is a codeword. The maximum complexity is on the order of $O[\log_2 B(m, w, f)]$. The algorithm to decode $I \circ O$ is straightforward: for $m, n, w, f \in J$, then the outer code can be a Reed-Solomon code (or a modified Reed-Solomon code, either shortened or extended). The receiver can hence use the Berlekamp-Massey algorithm, which has complexity on the order of $O[2^2\log_2 B(m, w, f)]$ binary operations to correct the errors and erasures. The total complexity is hence on the order of $O[m^2(n, w, f - 1) + fe^2\log_2 B(m, w, f)]$.

### 3.2 Bounds on CWACs

Although constant-weight array codes were defined as sets of words in $J(m, w)^n$, by expanding each element of $J(m, w)$ as a column vector they can be equivalently defined as sets of matrices in $GF(2)^{mn}$ with weight $w$ on any column. Constant-weight array codes can finally be defined as a subclass of constant-weight codes of length $M = mn$, constant-weight $W = nw$, and where all columns (the vectors in $J(m, w)$) have weight $w$. Therefore, CWACs are both a special class and a generalization of constant-weight codes. Since their minimum Hamming distance is equal to twice their minimum modified Hamming distance, the main scope of this section is the study of the maximum cardinality $A(m, n, w, d)$ of a CWAC in $J(m, w)^n$ with minimum Hamming distance $2d$.

First of all, let $J_{m \times n}$ be the all-ones matrix in $GF(2)^{m \times n}$. Then for any matrices $M, N \in J(m, w)^n$, we have $M + J, N + J \in J(m, m - w)^n$ and $d_H(M + J, N + J) = d_H(M, N)$. Therefore, $A(m, n, w, d) = A(m, n, m - w, d)$ for all $m$, $n$, and $w$, so we assume $2w \leq m$ without loss of generality henceforth.

The term $A(m, n, w, d)$ is a non-decreasing function of $m$, and a non-increasing function of $d$. The values of $A(m, n, w, d)$ can be readily determined for extreme values of $d$: $A(m, n, w, 1) = \binom{m}{w}$, $A(m, n, w, d) = 1$ if $d > nw$, and $A(m, n, w, nw) = \left\lfloor \frac{m}{w} \right\rfloor$. 

3
The Singleton bound for Hamming metric codes can easily be extended to CWACs.

**Proposition 2** (Singleton bound for CWACs). For all \( d \geq w + 1 \),
\[
A(m, n, w, d) \leq A(m, n - 1, w, d - w).
\]

**Proof.** For any two \( c, d \in J(m, w) \) we have \( d_H(c, d) \leq 2w \). For any two \( M, N \in J(m, w)^n \) we denote the first \( n - 1 \) columns as \( M' \) and \( N' \), respectively and their last coordinate as \( m_c \) and \( m_n \), respectively. We have \( d_H(M, N) = d_H(M', N') + d_H(m_c, m_n) \leq d_H(M', N') + 2w \). Let \( C \) be a code in \( J(m, w)^n \) with minimum distance \( d > w \) and cardinality \( A(m, n, w, d) \), then the code \( C' = \{M' : M \in C\} \) has minimum distance \( d - w \) and cardinality \(|C|\). \( \square \)

The Johnson bound of type I \([19]\) can be easily generalized to the case of CWACs. However, such a generalization is straightforward and the resulting bound is not usually tight. Therefore, we focus on the Johnson bounds of type II. Before determining the generalization of the Johnson bounds of type II \([19]\) to CWACs, we study the maximum cardinality \( \alpha(m, n, w, \delta) \) of an antiCWAC in \( J(m, w)^n \) with diameter \( \delta \). First, by symmetry we have \( \alpha(m, n, w, \delta) = \alpha(m, n, m - w, \delta) \) hence we consider \( w \leq m \). Some special values include \( \alpha(m, n, w, 0) = 1 \) and \( \alpha(m, n, w, nw) = \binom{m}{w}^n \). We give a construction of antiCWACs in Lemma \([1]\) by concatenating a constant-weight anticode and a Hamming metric anticode. This, in turn, yields a lower bound on the maximum cardinality of antiCWACs.

**Lemma 1** (Construction of a CWAC anticode by concatenation). Let \( I \subseteq J(m, w) \) be a constant-weight anticode with diameter \( \phi \) and \( O \subseteq I^\perp \) be an anticode with diameter \( \phi \), then the concatenated code \( O \circ I \) is an \( (m, n, w) \) antiCWAC with diameter at most \( \phi \). Therefore, for all \( \phi \leq w \), \( \alpha(m, n, w, \delta) \geq \gamma(\beta(m, w, \phi), n, \left\lceil \frac{\delta}{\phi} \right\rceil) \).

The proof of Lemma \([1]\) is similar to that of Proposition \([1]\) and is hence omitted. The lower bound on \( \beta(n, w, \delta) \) in \([1]\) and the exact value of \( \gamma(q, n, \delta) \) in \([2]\) can hence be used to compute lower bounds on \( \alpha(m, n, w, \delta) \). We now give the Johnson bounds of type II for CWACs.

**Proposition 3** (Johnson bound of type II for CWACs). For all \( l | n, v \leq l, 0 \leq \delta \leq \frac{n}{l} \min\{v, l - v\} \),
\[
A(m, n, w, d) \leq \frac{1}{\alpha(l, \frac{n}{l}, v, \delta)} \left( \frac{m^l}{w^v(m - w)^l - v} \right)^\frac{n}{l} A\left((m - 1)l, \frac{n}{l}, lw - v, d - \delta \right).
\]

**Proof.** Let \( C \) be an \((m, n, w)\) CWAC with minimum distance \( d \) and cardinality \( A(m, n, w, d) \) and let \( L \) be an antiCWAC in \( J(l, v)\) with diameter \( \delta \) and cardinality \( \alpha(l, \frac{n}{l}, v, \delta) \). For all \( u \in [m]^n \) and all \( C \in C \), we define \( f(u, C) = (c_{0,0}, c_{1,1}, \ldots, c_{n-1, n-1}) \in GF(2)^n \). Suppose \( f(u, C_0), f(u, C_1) \in L \), then \( C_0', C_1' \subseteq J((m - 1)l, lw - v) \), where \( C_0' \) and \( C_1' \) are the puncturings of the coordinates \((u_j, j)\) of \( C_0 \) and \( C_1 \), respectively. By definition of the Hamming distance, we obtain
\[
d_H(C_0, C_1) = d_H(C_0', C_1') + d_H(f(u, C_0), f(u, C_1)). \tag{3}
\]
Since \( f(u, C_0), f(u, C_1) \in L \), we have \( d_H(f(u, C_0), f(u, C_1)) \leq 2\delta \) and \([3]\) leads to \( d_H(C_0', C_1') \geq 2(d - \delta) \).

For all \( x \in GF(2)^n \) and all \( D \subseteq GF(2)^n \), we let \( \chi(x, D) = 1 \) if \( x \in D \) and \( \chi(x, D) = 0 \) otherwise. Hence for all \( u \in [m]^n \), \( \sum_{C \in C} \chi(f(u, C), L) = |\{C \in C : f(u, C) \in L\}| \) is the cardinality of a CWAC in \( J((m - 1)l, lw - v) \) with minimum distance at least \( 2(d - \delta) \), and hence
\[
\sum_{C \in C} \chi(f(u, C), L) \leq A\left((m - 1)l, \frac{n}{l}, lw - v, d - \delta \right) \tag{4}
\]
for all \( u \in [m]^n \). Similarly, we have for all \( C \in C \), \( \sum_{u \in [m]^n} \chi(f(u, C), L) = \{u \in [m]^n : f(u, C) \in L\} \). For any \( L \in J(l, v)^\perp \), it can be easily shown that \( \{u \in [m]^n : f(u, C) = L\} = w^{\frac{n}{l}}(m - w)^{n - \frac{n}{l}} \), and hence
\[
\sum_{u \in [m]^n} \chi(f(u, C), L) = \alpha\left(l, \frac{n}{l}, v, 2\delta \right) w^{\frac{n}{l}}(m - w)^{n - \frac{n}{l}} \tag{5}
\]
for all \( C \in C \). Summing over all \( u \in [m]^n \) and all \( C \in C \), while using \([1]\) and \([2]\), then finishes the proof. \( \square \)
In practice, the bound in Proposition needs to be minimized for all \( l, u, \) and \( \delta \). However, in order to illustrate this bound, we display its values for the two extreme cases of \( \delta \) in Corollary 1.

**Corollary 1.** We have

\[
A(m, n, w, d) \leq \left( \frac{m}{w} \right)^n \left( \frac{m}{m - w} \right)^{n - w} A\left( (m - 1)l, n, lw - v, d \right),
\]

\[
A(m, n, w, d) \leq \left( \binom{m}{w} \right)^n \left( \frac{m}{(m - w)^{d - v}} \right)^n A\left( (m - 1)l, n, lw - v, d - \frac{n}{l} \min\{v, l - v\} \right).
\]

We finish this section by deriving the counterparts of the Gilbert and Hamming bounds for CWACs. First, we study the number of vectors in \( J(m, w)^n \) at distance \( d \) from a given vector in \( J(m, u)^n \). We denote the set of all nonnegative integer sequences of length \( n \) whose sum is equal to \( d \) as \( P_n(d) \).

**Lemma 2.** The number of words in \( J(m, u)^n \) at distance \( d \) from a given word in \( J(m, w)^n \) is given by \( N(m, n, w, u, d) = \sum_{\pi \in P_n(d)} \prod_{i \in \pi} \nu(i) \), where \( \nu(i) = \left( \frac{w}{w + 1} \right)^{\frac{n - w}{l + u - v}} \).

**Proof.** The proof goes by induction on \( n \). First, for \( n = 1 \), \( N(m, 1, w, u, d) \) is given by \( \nu(d) \), and hence the claim is true. Let us now assume it is true for \( n = a \). It is easily shown that

\[
N(m, a + 1, w, u, d) = \sum_{e = 0}^{d} N(m, a, w, u, e) \nu(d - e)
\]

\[= \sum_{e = 0}^{d} \nu(d - e) \sum_{\pi \in P_a(e)} \pi \prod_{i \in \pi} \nu(i). \]

For any \( \pi \in P_a(e) \), we have \( \pi' = \pi \cup \{d - e\} \in P_{a+1}(d) \); conversely, any \( \pi' \in P_{a+1}(d) \) can be expressed as \( \pi \cup \{d - e\} \), where \( \pi \in P_a(e) \). Therefore, we obtain \( N(m, a + 1, w, u, d) = \sum_{\pi' \in P_{a+1}(d)} \prod_{i \in \pi'} \nu(i) \).

Although the value of the expression in Lemma 2 cannot be computed in general, as it requires an exponential number of operations, it can be determined for relatively small values of \( d \) and \( n \). Also, Proposition 3 provides a recursive way to compute \( N(m, n, w, u, d) \).

We now determine the counterparts of the Gilbert and Hamming bounds for CWACs, whose proofs are straightforward and hence omitted.

**Proposition 4** (Gilbert and Hamming bounds for CWACs). For all parameter values, \( \frac{m^n}{\sum_{i=0}^{d-1} N(m, n, w, w, 2i)} \leq A(m, n, w, d) \leq \min_{n-\delta+1 \leq d \leq n \delta - d - 1} \left\{ \frac{\binom{m}{w}^n}{\sum_{i=0}^{d-1} N(m, n, w, u, i)} \right\} \).

### 3.3 Relations to other classes of codes

We first relate \( A(m, n, w, d) \) to the maximum cardinalities of constant-weight codes and nonrestricted Hamming metric codes. Proposition 5 relates \( A(m, n, w, d) \) to \( B(n, w, d) \) and \( C(q, n, d) \) for some particular values.

**Proposition 5.** For all \( d \), we have \( A(m, n, 1, d) = C(m, n, d) \) and \( A(m, 1, w, d) = B(m, w, d) \).

The proof is straightforward and hence omitted. Proposition 5 indicates that the problem of finding the maximum cardinality of a CWAC generalizes both problems of finding optimal CWCs and optimal nonrestricted Hamming metric codes. Proposition 6 on the other hand, views CWACs as a special class of constant-weight codes.

**Proposition 6** (CWACs as a subclass of constant-weight codes). For all \( a, m' \), and \( w' \) such that \( am' \leq m \) and \( aw' \leq w \leq aw' + m - aw' \), we have \( A(m, n, w, d) \geq A(m', an, w', d) \). Therefore, for all \( w \leq m \), we have

\[
C\left( \frac{m}{w}, nw, d \right) \leq A(m, n, w, d) \leq B(mn, nw, d).
\]
Proposition 8. For all $C \in J(m', w')^m$, let the $k$-th column of $f(C) \in J(m, w)^n$ consist of the columns $ak, ak + 1, \ldots, (a + 1)k - 1$ of $C$, of $w - aw'$ ones, and of $m - am' - w + aw'$ zeros. Then $f$ is an injection from $J(m', w')^m$ to $J(m, w)^n$ which preserves the distance. We hence obtain the first claim; (7) follows immediately.

Proposition 7 refines the upper bound in (7) by providing an explicit extension of a CWAC by adding several CWACs of different dimensions.

**Proposition 7 (Refined upper bound for CWACs).** For all $l \geq 1$ and any decreasing sequence of integers $\{n_0 = n, n_1, \ldots, n_{l-1}\}$ satisfying $n_i | n$ and $\frac{mn}{m} \leq n_i \leq (1 - \frac{d}{nw}) n_i - 1$ for all $1 \leq i \leq l - 1$, we have

$$
\sum_{i=0}^{l-1} B(n, n_i, d) A(m, n_i, w_i, d) \leq B(mn, nw, d),
$$

where $w_i = \frac{nw}{n_i}$.

**Proof.** We shall construct a constant-weight code in $J(mn, nw)$ with minimum distance $d$ and cardinality $\sum_{i=0}^{l-1} B(n, n_i, d) A(m, n_i, w_i, d)$. For all $i$, let $C^i = \{C^{i,k}\}$ be a CWAC in $J(m, w_i)^n_i$ with minimum distance $d$ and cardinality $A(m, n_i, w_i, d)$ and let $L^i = \{L^{i,j}\}$ be a constant-weight code in $J(n, n_i)$ with minimum distance $d$ and cardinality $B(n, n_i, d)$. Also for any $i, j$, we denote the nonzero coordinates of $L^{i,j}$ as $L^{i,j}(a)$ for $0 \leq a \leq n_i - 1$. Then for all $k$, we construct the vector $X^{i,j,k}$ as follows. For all $0 \leq a \leq n_i - 1$, the $L^{i,j}(a)$-th column of $X^{i,j,k}$ is given by the $a$-th column of $C^{i,k}$, and all the other $n - n_i$ columns are set to zero. Then the code $C = \{X^{i,j,k}\}$ is a constant-weight code in $J(mn, nw)$.

We now show that $C$ has minimum distance $d$ by considering two distinct codewords $X^{i,j,k}$ and $X^{i',j',k'}$ in $C$. First, if $i \neq i'$, without loss of generality $i < i'$ and hence $n_i > n_{i'}$, we have $d_H(X^{i,j,k}, X^{i',j',k'}) = \sum_{a=0}^{n_i-1} d_H(x^{i,j,k}_a, x^{i',j',k'}_a)$, where $x_a$ denotes the $a$-th column of $X$. Therefore,

$$
d_H(X^{i,j,k}, X^{i',j',k'}) = \sum_{a \in L^{i,j} \cap L^{i',j'}} d_H(x^{i,j,k}_a, x^{i',j',k'}_a) + \sum_{a \in L^{i,j} \setminus L^{i',j'}} d_H(x^{i,j,k}_a, 0) + \sum_{a \in L^{i',j'} \setminus L^{i,j}} d_H(0, x^{i,j,k}_a)
$$

$$
\geq \left| L^{i,j} \cap L^{i',j'} \right| (w_{i'} - w_i) + \left| L^{i,j} \setminus L^{i',j'} \right| w_i + \left| L^{i',j'} \setminus L^{i,j} \right| w_{i'}
$$

$$
\geq 2w_i (n_i - n_{i'} - 1) + 2d,
$$

(8)

where (8) follows the definition of the $\{n_i\}$ sequence. Second, if $i = i'$ and $j \neq j'$, then $d_H(X^{i,j,k}, X^{i',j',k'}) = d_H(L^{i,j}, L^{i',j'}) \geq 2d$ by the minimum distance of $C$. Third, if $i = i'$, $j = j'$, and $k \neq k'$, then $d_H(X^{i,j,k}, X^{i,j,k'}) = d_H(C^{i,k}, C^{i,k'}) \geq 2d$ by the minimum distance of $C$. Thus $C$ has minimum distance $2d$ and cardinality $\sum_{i=0}^{l-1} B(n, n_i, d) A(m, n_i, w_i, d) \leq B(mn, nw, d)$.

**Proposition 8.** For any $a \geq 1$, we have $A(am, n, w, d) \geq C \left( a, n, \left\lceil \frac{d}{w} \right\rceil \right) A(m, n, w, d)$. Furthermore, if $a | w$ and $d \leq nw \frac{d}{a}$, then

$$
A(am, n, w, d) \geq C \left( a, n, \left\lceil \frac{d}{w} \right\rceil \right) A(m, n, w, d) + A \left( m, an, \frac{w}{a}, d \right).
$$

**Proof.** Let $C$ be a CWAC in $J(m, w)^n$ with minimum distance $d$ and cardinality $A(m, n, w, d)$ and let $V$ be a code in $[a]^n$ with minimum distance $\left\lceil \frac{d}{w} \right\rceil$ and cardinality $C \left( a, n, \left\lceil \frac{d}{w} \right\rceil \right)$. We construct the code $D \subseteq J(am, w)^n$ as follows. For any $C^i \in C$, $v^j \in V$, and all $0 \leq k \leq n - 1$, let $d^i_{k,j}$ be the vector in $GF(2)^m$ with a columns of length $m$ where only the $v^j_k$-th column is nonzero and given by the $k$-th column of $C^i$. Then the codeword $D^i_{k,j} \in D$ is defined to be $D^i_{k,j} = (d^i_{0,j}, d^i_{1,j}, \ldots, d^i_{n-1,j})$. 

6
We now show that $D$ has minimum distance at least $d$ by considering $D^{i,j}$ and $D^{i',j'}$. First, for any pair of codewords, we have
\[
d_H(D^{i,j}, D^{i',j'}) = \sum_{k=0}^{n-1} d_H(d_k^{i,j}, d_k^{i',j'}) = 2wd_H(v_j, v_{j'}) + \sum_{k:v_j = v_{j'}} d_H(C_{k}^i, C_{k}^{i'}).
\] (9)
If $i \neq i'$, \((\mathbf{9})\) leads to $d_H(D^{i,j}, D^{i',j'}) \geq d_H(C_i^{i'}, C_i^j) \geq 2d$. Also, if $i = i'$ and $j \neq j'$, \((\mathbf{9})\) yields $d_H(D^{i,j}, D^{i',j'}) \geq 2wd_H(v_j, v_{j'}) \geq 2d$. Therefore $D$ has minimum distance at least $2d$. As a corollary, the cardinality of $D$ is given by $|D| = |C||\mathcal{V}|$.

We now suppose $a|w$ and $d \leq nw\frac{a-1}{d}$, and we let $E$ be a CWAC in $J(m, \frac{w}{a})^n$ with minimum distance $2d$ and cardinality $A(m, an, \frac{w}{a}, d)$. Since any codeword in $D$ has $(a-1)n$ all-zero columns, and that the remaining ones have weight $w$, we have $d_H(E, D) \geq (a-1)n\frac{w}{a} + n(w - \frac{w}{a}) \geq 2d$. Thus the code $E \cup D$ has minimum distance $2d$ and cardinality $|E| + |D|$.

We also determine a close relation between CWACs of high minimum distance and constant-weight codes.

**Proposition 9.** For all $m$, $n$, $w$, and $d = (n-1)w + r$ with $0 < r \leq w$, $A(m, n, w, d) \leq B(m, w, r)$.

**Proof.** Let $C$ be a CWAC in $J(m, w)^n$ with minimum distance $d > (n-1)w$ and cardinality $A(m, n, w, d)$. For all $C^0, C^1 \in C$ and all $0 \leq i \leq n-1$, we have $d_H(C^i_0, C^i_1) \geq 2r$ and hence $C_i$ is a constant-weight code in $J(m, w)$ with minimum distance no less than $2r$ and cardinality $|C^i|$. Therefore, we have $A(m, n, w, d) \leq B(m, w, r)$.

The following upper bound can be viewed as the counterpart of the concatenation construction in Section 3.1.

**Proposition 10.** For all $m$, $n$, $w$, and $d$, $A(m, n, w, d) \leq C\left(\binom{m}{w}, n, \left\lfloor \frac{d}{w} \right\rfloor\right)$.

**Proof.** Let $C \in J(m, w)^n$ have minimum distance $d$ and cardinality $A(m, n, w, d)$. There is a bijection between $J(m, w)$ and $\binom{m}{w}$; applying it columnwise, we map $C$ to a code $f(C) \subseteq \binom{m}{w}^n$. For any $C^0, C^1 \in C$, we have
\[
d \leq d_H(C^0, C^1) \leq 2w|\{i : C^0_i \neq C^1_i\}| = 2wd_H(f(C^0), f(C^1)),
\]
and hence $f(C)$ has minimum distance at least $\frac{d}{w}$.

The Bassalygo-Elias bound \cite{bassalygo1970bounds} is a crucial relation between the maximum cardinalities of constant-weight codes and nonrestricted binary codes. We now derive a generalization of the Bassalygo-Elias bound for CWACs.

**Proposition 11** (Bassalygo-Elias bound for CWACs). For all $w_1|w_2|m$, we have
\[
A\left(\binom{w_1}{w_2}, \frac{n}{w_1}, \frac{w_2}{w_1}, w_1, d\right) \geq \binom{m}{w_1} n A(m, n, w_2, d).
\] (10)

Therefore,
\[
\binom{m}{w} B(mn, nw, d) \leq A(m, n, w, d) \leq \binom{m}{w} n C\left(\frac{m}{w}, nw, d\right).
\] (11)

**Proof.** Let $C$ be a CWAC in $J(m, w_2)^n$ with minimum distance $2d$ and cardinality $A(m, n, w_2, d)$. Let $\mathcal{S}_m$ denote the symmetric group on $m$ elements and let $\mathcal{S}_m^n$ be its $n$-fold cartesian product. For all $\pi \in \mathcal{S}_m^n$, $C \in C$, we define the function $f(\pi, C)$ to be $f(\pi, C) = 1$ if $\pi(C) \in J\left(\binom{w_1}{w_2}, w_1\right)^n$ and $f(\pi, C) = 0$ otherwise. We have for all $\pi \in \mathcal{S}_m^n$
\[
\sum_{C \in C} f(\pi, C) = \left\{\pi(C) \in J\left(\binom{w_1}{w_2}, w_1\right)^n : C \in C\right\} \leq A\left(\binom{w_1}{w_2}, n, \frac{w_2}{w_1}, w_1, 2d\right).
\] (12)
and for all \( C \in C \)
\[
\sum_{\pi \in S_m} f(\pi, C) = \left\{ \left( m^{\frac{m}{w_2}} \right)^\frac{w_2}{w_1} w_2! (m - w_2)! \right\}^n.
\]
(13)

Combining (12) and (13), the double sum leads to (10). In particular, applying (10) with a simple change of variables leads to (11).

Proof. Applying the bounds on the binomial coefficient in [11, Ch. 10, Lemma 7] to (11), we obtain
\[
A(m, n, w, d) \geq \sqrt{\pi w n 2^{-\frac{n}{2}(3 + \log w)} B(mn, nw, d)}.
\]
(14)

Corollary 2. For \( 2w \leq m \), we have \( A(m, n, w, d) \geq \sqrt{\pi w n 2^{-\frac{n}{2}(3 + \log w)} B(mn, nw, d)} \).

Proof. Applying the bounds on the binomial coefficient in [11, Ch. 10, Lemma 7] to (11), we obtain
\[
A(m, n, w, d) \geq \sqrt{\frac{2\pi w n (1 - \frac{w}{m})}{(8w(1 - \frac{w}{m}))^n}} B(mn, nw, d).
\]
(11)

Binary codes, and especially constant-weight codes, are closely related to spherical codes. More precisely, any constant-weight code can be mapped into a spherical code of a given length [11 Theorem 2]. The cardinality of a constant-weight code is hence upper bounded by the maximum cardinality of an optimal spherical code with related dimension and maximum cosine. Proposition 12 generalizes this relation to the case of CWACs.

Proposition 12 (Relation between CWACs and spherical codes). We have
\[
A(m, n, w, d) \leq A_S \left( n(m - 1), 1 - \frac{dm}{nw(m - w)} \right).
\]

Proof. Let \( \Omega \) denote the mapping from \( \text{GF}(2)^m \) to \( \mathbb{R}^m \) which sends \( 0 \to 1 \) and \( 1 \to -1 \) coordinate-wise. Then \( \Omega(J(m, w)^n) = \{ x \in \{1, -1\}^mn : xA = (m - 2w)1 \} \), where \( A \in \mathbb{R}^{mn \times n} \) is formed by cascading \( n \) all-ones column vectors of length \( m \). Hence any point \( x \in \Omega(J(m, w)^n) \) satisfies \( (x - c)A = 0 \), where \( c = \frac{m - 2w}{m}1 \) and \( ||x - c|| = 2\sqrt{\frac{n w (m - w)}{m}} = r \). Therefore, \( \Omega(J(m, w)^n) \) is a subset of the \( n(m - 1) \)-dimensional sphere of radius \( r \) around \( c \). Also, it is easily shown that \( d_F(\Omega(X), \Omega(Y)) = 2\sqrt{d_E(X, Y)} \) for all \( X, Y \in \text{GF}(2)^mn \). Let \( C \) be a CWAC in \( J(m, w)^n \) with minimum distance \( 2d \). Then the code \( \frac{1}{2}(\Omega(C) - c) \) is a spherical code of dimension \( n(m - 1) \) with minimum Euclidean distance \( 2\sqrt{2d} \) and maximum cosine given by \( 1 - \frac{4d}{m} \).

We remark that once the total length \( M = mn \) and the total weight \( W = nw \) of the CWAC are fixed, the maximum cosine in the upper bound of Proposition 12 remains constant, while the dimension of the space is a decreasing function of \( n \). This dimension reaches its maximum for \( n = 1 \), where Proposition 12 corresponds to [11 Theorem 2] established for constant-weight codes and reaches its minimum value for liftings of Hamming metric codes.

Using the exact values of \( A_S(n, s) \) reviewed in Section 2, Proposition 12 can be reduced as follows
\[
A(m, n, w, d) \leq \left\lfloor \frac{d}{d - \Delta} \right\rfloor, \quad \text{if } d \geq \Delta \left( 1 + \frac{1}{n(m - 1)} \right)
\]
\[
A(m, n, w, d) \leq n(m - 1) + 1, \quad \text{if } \Delta < d \leq \Delta \left( 1 + \frac{1}{n(m - 1)} \right)
\]
\[
A(m, n, w, \Delta) \leq 2n(m - 1),
\]
where \( \Delta = \frac{nw(m - w)}{m} \).
References

[1] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, “A new table of constant weight codes,” *IEEE Trans. Info. Theory*, vol. 36, no. 6, pp. 1334–1380, November 1990.

[2] S. D. Constantin and T. R. N. Rao, “On the theory of binary asymmetric error correcting codes,” *Information and Control*, vol. 40, pp. 20–36, 1979.

[3] H. C. A. van Tilborg and M. Blaum, “On error-correcting balanced codes,” *IEEE Trans. Info. Theory*, vol. 35, no. 5, pp. 1091–1095, September 1989.

[4] E. Agrell, A. Vardy, and K. Zeger, “Upper bounds for constant-weight codes,” *IEEE Trans. Info. Theory*, vol. 46, no. 7, pp. 2373–2395, November 2000.

[5] S.-T. Xia and F.-W. Fu, “Johnson type bounds on constant dimension codes,” *Designs, Codes and Cryptography*, vol. 50, no. 2, pp. 163–172, February 2009.

[6] T. Etzion and N. Silberstein, “Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams,” *IEEE Trans. Info. Theory*, vol. 55, no. 7, pp. 2909–2919, July 2009.

[7] R. Kötter and F. R. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Trans. Info. Theory*, vol. 54, no. 8, pp. 3579–3591, August 2008.

[8] M. Gadouleau and A. Goupil, “Binary codes for packet error and packet loss correction in store and forward,” in *Proc. International ITG Conference on Source and Channel Coding*, Siegen, January 2010.

[9] P. Östergård and M. Svanström, “Ternary constant-weight codes,” *The Electronic Journal of Combinatorial Theory*, vol. 9, no. R41, 2002.

[10] Y. M. Chee and S. Ling, “Constructions for q-ary constant-weight codes,” *IEEE Trans. Info. Theory*, vol. 53, no. 1, pp. 135–146, January 2007.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[12] R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr., and L. R. Welch, “New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities,” *IEEE Trans. Info. Theory*, vol. 23, pp. 157–166, 1977.

[13] P. Erdős, C. Ko, and R. Rado, “Intersection theorems for systems of finite sets,” *Quart. J. Math. Oxford*, vol. 12, pp. 313–320, 1961.

[14] P. Frankl, “The Erdős-Ko-Rado theorem is true for n = ckt,” *Proc. Hungar. Combin. Colloq.*, vol. 18, pp. 365–375, 1978.

[15] R. Ahlswede and L. Khachatrian, “The diametric theorem in Hamming spaces - optimal anti-codes,” *Advances in Applied Mathematics*, vol. 20, pp. 429–449, 1998.

[16] V. I. Levenshtein, “On bounds for packings in n-dimensional Euclidean space,” *Sov. Math.-Dokl.*, vol. 20, no. 2, pp. 417–421, March-April 1979.

[17] P. G. Boyvalenkov, D. P. Danev, and S. P. Bumova, “Upper bounds on the minimum distance of spherical codes,” *IEEE Trans. Info. Theory*, vol. 42, no. 5, pp. 1576–1581, September 1996.

[18] V. Guruswami, “List decoding of error-correcting codes,” Ph.D. dissertation, Massachusetts Institute of Technology, 2002.

[19] S. M. Johnson, “A new upper bound for error-correcting codes,” *IRE Trans. Info. Theory*, vol. 8, no. 3, pp. 203–207, April 1962.
[20] L. A. Bassalygo, “New upper bounds for error correcting codes,” *Problems of Information Transmission*, vol. 1, no. 4, pp. 32–35, October-December 1965.

[21] N. Q. A, L. Györfi, and J. L. Massey, “Constructions of binary constant-weight cyclic codes and cyclically permutable codes,” *IEEE Trans. Info. Theory*, vol. 38, pp. 940–949, 1992.

[22] E. Agrell, “Bounds for constant-weight codes.” [Online]. Available: http://webfiles.portal.chalmers.se/s2/research/kit/bounds/cw.html

[23] A. Brouwer, “Table of general binary codes.” [Online]. Available: http://www.win.tue.nl/~aeb/codes/binary-1.html