Bounds on the Asymptotic Rate of Binary Constant Subblock-Composition Codes

Anshoo Tandon
National University of Singapore
anshoo.tandon@gmail.com

Han Mao Kiah
Nanyang Technological University
hmkiah@ntu.edu.sg

Mehul Motani
National University of Singapore
motani@nus.edu.sg

***Abstract*—The study of binary *constant subblock-composition codes* (CSCCs) has recently gained attention due to their application in diverse fields. These codes are a class of constrained codes where each codeword is partitioned into equal sized subblocks, and every subblock has the same fixed weight. We present novel upper and lower bounds on the asymptotic rate for binary CSCCs, using the sphere-packing and Gilbert-Varshamov (GV) type bounds, respectively. For a fixed subblock length and small code distance, we show that the asymptotic rate for CSCCs is strictly lower than the corresponding rate for constant weight codes (CWCs). We also provide a correction to an earlier result by Chee et al. (2014) on the asymptotic CSCC rate.**

I. Introduction

Binary *constant subblock-composition codes* (CSCCs) are a class of constrained codes where each codeword is partitioned into equal sized subblocks, and every subblock has the same fixed weight. Chee *et al.* [1] proposed the use of binary CSCCs in design of low cost authentication methods, and provided rudimentary bounds on CSCC code size. Other constructions of CSCCs have been proposed by various authors [2], [3]. Note that CSCCs were labeled as *multiply constant weight codes* (MCWCs) in [1], [2], [3]. CSCCs were shown to be suitable candidates for simultaneous energy and information transfer in [4], where bounds on CSCC capacity and CSCC error exponent over discrete memoryless channels were presented.

In this paper, we study bounds on the optimal code size and asymptotic rate for binary CSCCs with a given error correction capability. We present upper and lower bounds on the asymptotic rate for binary CSCCs, using the sphere-packing and Gilbert-Varshamov (GV) type bounds, respectively. Moreover, for fixed subblock length and small code distance, we show that the asymptotic rate for CSCCs is strictly lower than the corresponding rate for constant weight codes (CWCs).

The notation used is as follows. An n-length, binary *code* $\mathscr{C}$ is a subset of $\{0,1\}^n$. The elements of $\mathscr{C}$ are called *codewords* and $\mathscr{C}$ is said to have *distance* d if the *Hamming distance* between any two distinct codewords is at least d. A binary code of length n and distance d is called an (n,d)-code, and the largest size of an (n,d)-code is denoted by $A(n,d)$. A *constant weight code* (CWC) with parameter w is a code where each codeword has weight exactly w. We denote a CWC with weight parameter w, block-length n, and distance d by (n,d,w)-CWC, and denote its optimal size by $A(n,d,w)$.

A *subblock-constrained code* is a code where each codeword of length n is partitioned into subblocks of length L, and each subblock satisfies a fixed set of constraints. A binary CSCC is characterized by the property that each subblock in every codeword has the same *weight*, i.e. each subblock has the same number of ones. A binary CSCC with codeword length $n = mL$, minimum distance d, subblock length L, number of subblocks m, and weight w_s per subblock is called an (m,L,d,w_s)-CSCC. We denote the maximum possible size of (m,L,d,w_s)-CSCC by $C(m,L,d,w_s)$. Since an (m,L,d,w_s)-CSCC is an (mL,d,mw_s)-CWC, we have that $C(m,L,d,w_s) \leq A(mL,d,mw_s)$.

We analyze bounds on CSCC rate in the asymptotic setting where the number of subblocks m tends to infinity, but L and w_s are fixed. Formally, for fixed $0 < \delta < 1$, the asymptotic CSCC rate with fixed subblock length L, weight per subblock w_s, number of subblocks in a codeword $m \to \infty$, and distance d scaling as $d = \lfloor mL\delta \rfloor$ is defined as

$$\gamma(L,\delta,w_s/L) \triangleq \limsup_{m\to\infty} \frac{\log C(m,L,\lfloor mL\delta \rfloor, w_s)}{mL}. \quad (1)$$

This rate can be compared with related exponent for CWCs:

$$\alpha(\delta,w_s/L) \triangleq \limsup_{n\to\infty} \frac{\log A\left(n,\lfloor n\delta \rfloor, \lfloor nw_s/L \rfloor\right)}{n}. \quad (2)$$

The asymptotic CSCC rate was also studied in [1], in which an inconsistent rate definition led to an erroneous statement (see [1, Prop. 6.1]). Proposition 3 in Section III provides a correct statement for the CSCC rate in the scenario where the subblock length tends to infinity.

A. Our Contributions

The contributions of this paper are as follows:

- We provide both upper and lower bounds for $C(m,L,d,w_s)$ in Section II.
- We derive bounds on the asymptotic rate for CSCCs in Section III. Additionally, for given L and w_s, in Section IV we demonstrate the existence of an $\tilde{\delta}_L$ such that $\alpha(\delta,w_s/L) > \gamma(L,\delta,w_s/L)$ for all $\delta < \tilde{\delta}_L$.
- We provide numerical lower bounds on the asymptotic rate gap between CWCs and CSCCs in Section V.

A. Tandon and M. Motani are supported in part by the National Research Foundation Singapore under Grant No. NRF-CRP-8-2011-01.

H. M. Kiah is supported in part by the Singapore Ministry of Education under Research Grant MOE2016-T1-001-156.

978-1-5090-4096-4/17/$31.00 ©2017 IEEE

II. Bounds on optimal CSCC code size

We derive the GV and sphere-packing bounds on the optimal CSCC code size, $C(m, L, d, w_s)$, in this section and their respective asymptotic versions in Section III. We remark that while other fundamental bounds for $C(m, L, d, w_s)$ were discussed in [1], those bounds are insufficient to provide good bounds on the asymptotic rates $\gamma(L, \delta, w_s/L)$.

Let $\mathcal{C}(m, L, w_s)$ denote the space of all binary CSCC words composed of m subblocks, each subblock having length L, with weight w_s per subblock. For $\mathbf{x} \in \mathcal{C}(m, L, w_s)$, we define a CSCC ball, centered at $\mathbf{x}$ and having radius t, as

$$\mathcal{B}_{\mathcal{C}}(\mathbf{x}, t; m, L, w_s) \triangleq \{\mathbf{y} \in \mathcal{C}(m, L, w_s) : d(\mathbf{x}, \mathbf{y}) \leq t\}. \quad (3)$$

Lemma 1. *If $\mathbf{x}$ and $\tilde{\mathbf{x}}$ are two distinct words in $\mathcal{C}(m, L, w_s)$, then the ball size $|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, t; m, L, w_s)| = |\mathcal{B}_{\mathcal{C}}(\tilde{\mathbf{x}}, t; m, L, w_s)|$.*

Proof: For $1 \leq i \leq m$, let $\mathbf{x}_{[i]}$ (resp. $\tilde{\mathbf{x}}_{[i]}$) denote the ith subblock of $\mathbf{x}$ (resp. $\tilde{\mathbf{x}}$). As $\mathbf{x}_{[i]}$ and $\tilde{\mathbf{x}}_{[i]}$ have constant weight w_s, there exists a permutation π_i on L letters such that $\tilde{\mathbf{x}}_{[i]} = \pi_i(\mathbf{x}_{[i]})$. Now, if π denotes the permutation on mL letter induced by π_i, defined as $\pi(\mathbf{x}) \triangleq [\pi_1(\mathbf{x}_{[1]}) \cdots \pi_m(\mathbf{x}_{[m]})]$, then $\tilde{\mathbf{x}} = \pi(\mathbf{x})$. The proof is complete by observing that $\mathcal{B}_{\mathcal{C}}(\tilde{\mathbf{x}}, t; m, L, w_s) = \{\pi(\mathbf{y}) : \mathbf{y} \in \mathcal{B}_{\mathcal{C}}(\mathbf{x}, t; m, L, w_s)\}$. ∎

In view of the above lemma, the size of CSCC ball is independent of the center word. In contrast, for a related space where each subblock has weight *at least* w_s, we demonstrate in the full paper [5] that ball size for a fixed radius varies with the center word.

The GV bound for $C(m, L, d, w_s)$ is presented next.

Proposition 1. *If $v \triangleq \min\{w_s, L - w_s\}$, then*

$$C(m, L, d, w_s) \geq \frac{\binom{L}{w_s}^m}{\sum\limits_{\substack{2(u_1+u_2+\cdots+u_m)\leq d-1,\\ 0\leq u_i \leq v}} \prod\limits_{i=1}^{m} \binom{w_s}{u_i}\binom{L-w_s}{u_i}} \quad (4)$$

Proof: Using standard Gilbert construction [6] in the space $\mathcal{C}(m, L, w_s)$, we have the lower bound

$$C(m, L, d, w_s) \geq \frac{|\mathcal{C}(m, L, w_s)|}{|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, d-1; m, L, w_s)|}, \quad (5)$$

where $\mathbf{x}$ is any word in $\mathcal{C}(m, L, w_s)$, and $|\mathcal{C}(m, L, w_s)| = \binom{L}{w_s}^m$. From Lemma 1 we note that $|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, d-1; m, L, w_s)|$ is independent of the choice of $\mathbf{x}$. The proposition then follows if we show that the denominator in (4) is equal to $|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, d-1; m, L, w_s)|$. Towards this, let $\mathbf{x}_{[i]}$ be the ith subblock of $\mathbf{x}$. Then the number of length L binary vectors of weight w_s at a distance $2u_i$ from $\mathbf{x}_{[i]}$ is $\binom{w_s}{u_i}\binom{L-w_s}{u_i}$ when $0 \leq u_i \leq v$ (and 0 otherwise). Now, if $\mathbf{y} \in \mathcal{C}(m, L, w_s)$, and distance between ith subblocks of $\mathbf{x}$ and $\mathbf{y}$ is $2u_i$, then $\mathbf{y} \in \mathcal{B}_{\mathcal{C}}(\mathbf{x}, d-1; m, L, w_s)$ if and only if $2\sum_{i=1}^{m} u_i \leq d-1$. Hence, the size of CSCC ball of radius $d-1$ is given by the denominator in (4). ∎

The following proposition presents the sphere-packing bound for CSCCs.

Proposition 2. *If $t \triangleq \lfloor (d-1)/2 \rfloor$ and $v \triangleq \min\{w_s, L - w_s\}$, then we have*

$$C(m, L, d, w_s) \leq \frac{\binom{L}{w_s}^m}{\sum\limits_{\substack{2(u_1+u_2+\cdots+u_m)\leq t,\\ 0\leq u_i \leq v}} \prod\limits_{i=1}^{m} \binom{w_s}{u_i}\binom{L-w_s}{u_i}} \quad (6)$$

Proof: The claim follows from the sphere-packing argument that balls of radius $t = \lfloor (d-1)/2 \rfloor$ around codewords should be non-intersecting in an (m, L, d, w_s)-CSCC, and the fact that the denominator in (6) is equal to $|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, t; m, L, w_s)|$. ∎

III. Asymptotic Bound on CSCC Rate

The asymptotic rate for CSCCs may be studied in scenarios where the number of subblocks m, or the subblock length L, or both, tend to infinity. The following proposition states that the asymptotic rate of CSCC is equal to that of CWC when the subblock length L tends to infinity. This is not surprising as the subblock constraint fades asymptotically (i.e., $L \to \infty$), and we refer the reader to [5] for the proof.

Proposition 3. *For any positive integer m and $0 \leq \delta, \omega \leq 1$,*

$$\lim_{L\to\infty} \frac{\log C(m, L, \lfloor \delta m L \rfloor, \lfloor \omega L \rfloor)}{mL} = \alpha(\delta, \omega). \quad (7)$$

Asymptotic rate results were also presented in [1]. However, there were some inconsistencies in the definition of the asymptotic CSCC rate and the resulting claim in [1, Prop. 6.1] was incorrect. Proposition 3 above provides a correction. The inconsistency in the CSCC rate definition in [1] also renders [1, Thm. 6.3] incorrect, whose proof also contained some anomalies.

In the remainder of the paper, we fix the relative distance δ, the subblock length L, the subblock weight w_s, and provide estimates of CSCC rates when number of subblocks m tend to infinity. The motivation for fixing L to relatively small values comes from the application of CSCCs to *simultaneous energy and information transfer* [4]. Here, it is shown that CSCC with appropriate weight will avoid energy outage at the receiver if the subblock length is less than a certain threshold [4].

Using rate definitions for $\gamma(L, \delta, w_s/L)$ and $\alpha(\delta, w_s/L)$, given by (1) and (2), respectively, we have the trivial inequality

$$\gamma(L, \delta, w_s/L) \leq \alpha(\delta, w_s/L). \quad (8)$$

The following proposition shows that for the case when $L = 2$ and $w_s = 1$, the CSCC rate $\gamma(L, \delta, w_s/L)$ is *strictly* less than $\alpha(\delta, w_s/L)$ when $0 < \delta < 1/2$.

Proposition 4. *We have*

$$\gamma(2, \delta, 1/2) = \frac{1}{2}\alpha(\delta, 1/2). \quad (9)$$

Proof: It was shown in [1, Cor. 4.2] that $C(m, 2, 2d, 1) = A(m, d)$. Then (9) follows immediately from the definitions of asymptotic rates. ∎

If $\alpha(\delta)$ denotes the optimum rate using binary codes with relative distance δ (with no weight constraint), then we have $\alpha(\delta, 1/2) = \alpha(\delta)$ [7], and the relation in (9) can alternately be expressed as $\gamma(2, \delta, 1/2) = (1/2)\alpha(\delta)$. Now, from the GV bound for general binary codes [7], we know that $\alpha(\delta) > 0$ for $0 < \delta < 0.5$, while from the asymptotic Plotkin bound [8] for binary codes, we have $\alpha(\delta) = 0$ for $\delta \geq 0.5$. Thus, from (9), it follows that the inequality in (8) is strict for the case when $L = 2$, $w_s = 1$, and $0 < \delta < 0.5$.

In general, for $L \geq 3$, define

$$\delta^* \triangleq 2\left(\frac{w_s}{L}\right)\left(1 - \frac{w_s}{L}\right). \tag{10}$$

From the MRRW bound for constant weight codes [7, Eq. (2.16)], we have

$$\alpha(\delta, w_s/L) = 0, \text{ if } \delta \geq \delta^*. \tag{11}$$

From (8) and (11), it follows that

$$\gamma(L, \delta, w_s/L) = 0, \text{ if } \delta \geq \delta^*. \tag{12}$$

Theorem 1 presents a lower bound for $\gamma(L, \delta, w_s/L)$ using the GV bound for $C(m, L, d, w_s)$ when $\delta < \delta^*$. The following lemmas will be used towards proving this theorem.

Lemma 2. *For fixed positive integers m, n and z, let k_i, with $1 \leq i \leq m$, be integers which satisfy $0 \leq k_i \leq n$, $\sum_{i=1}^{m} k_i = z$. Then we have the inequality*

$$\prod_{i=1}^{m} \binom{n}{k_i} \leq \binom{n}{\lfloor z/m \rfloor}^{m_1} \binom{n}{\lceil z/m \rceil}^{m-m_1}, \tag{13}$$

where $m_1 = m\lceil z/m \rceil - z$.

Proof: Follows from log-concavity of the binomial coefficients [9]. ∎

Lemma 3. *For $0 < k \leq w_s(L - w_s)/L$, we have the inequality*

$$\binom{w_s}{k}\binom{L-w_s}{k} > \binom{w_s}{k-1}\binom{L-w_s}{k-1}. \tag{14}$$

Proof: We have

$$\frac{\binom{w_s}{k}\binom{L-w_s}{k}}{\binom{w_s}{k-1}\binom{L-w_s}{k-1}} = \frac{(w_s - (k-1))\left((L-w_s) - (k-1)\right)}{k^2} \overset{(a)}{\geq} \frac{Lk - L(k-1) + (k-1)^2}{k^2} \overset{(b)}{>} 1,$$

where (a) follows because $w_s(L - w_s) \geq Lk$, and (b) follows from the fact that $k \leq \min\{w_s, L - w_s\} \leq L/2$. ∎

Theorem 1 (Asymptotic GV bound for CSCCs)**.** *For $0 < \delta < \delta^*$, we have $\gamma(L, \delta, w_s/L) \geq \gamma_{GV}(L, \delta, w_s/L)$, where $\gamma_{GV}(L, \delta, w_s/L)$ is defined as follows*

a) For $L = 2$,

$$\gamma_{GV}(2, \delta, 1/2) \triangleq \frac{1}{2}(1 - h(\delta)), \tag{15}$$

where $h(x) \triangleq -x\log_2 x - (1-x)\log_2(1-x)$.

b) For $L > 2$, $\gamma_{GV}(L, \delta, w_s/L)$ is defined equal to

$$\frac{1}{L}\log\binom{L}{w_s} - \min\{\theta(L, w_s),\, \phi(L, \delta)\} - \left(\frac{1 + u - \lceil u \rceil}{L}\right)\log\left[\binom{w_s}{\lceil u \rceil}\binom{L-w_s}{\lceil u \rceil}\right] - \left(\frac{\lceil u \rceil - u}{L}\right)\log\left[\binom{w_s}{\lfloor u \rfloor}\binom{L-w_s}{\lfloor u \rfloor}\right], \tag{16}$$

where $\theta(L, w_s) \triangleq \frac{1}{L}\log\left(\min\{w_s, L - w_s\} + 1\right)$, $\phi(L, \delta) \triangleq \left(\frac{1}{L} + \frac{\delta}{2}\right) h\left(\frac{1}{1 + \delta L/2}\right)$, and $u \triangleq \delta L/2$.

Proof: The claim for $L = 2$ follows from (9) and the GV bound for general binary codes.

For establishing the result for $L > 2$, we use Prop. 1. The challenge is to provide an appropriate upper bound on the CSCC ball size of radius $d - 1$, $|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, d-1; m, L, w_s)|$ (the denominator in (4)). If we define $v \triangleq \min\{w_s, L - w_s\}$ and $t \triangleq \lfloor (d-1)/2 \rfloor$, then using Lemmas 2 and 3, we show in the full paper [5] that this ball size is upper bounded as

$$|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, d-1; m, L, w_s)| < Q_t \min\left\{(v+1)^m,\ \binom{t+m}{m}\right\}, \tag{17}$$

where Q_t is defined as the expression below

$$\left[\binom{w_s}{\lfloor t/m \rfloor}\binom{L-w_s}{\lfloor t/m \rfloor}\right]^{m_t}\left[\binom{w_s}{\lceil t/m \rceil}\binom{L-w_s}{\lceil t/m \rceil}\right]^{m-m_t}, \tag{18}$$

with $m_t \triangleq m\lceil t/m \rceil - t$. As $d = \lfloor mL\delta \rfloor$, the t/m term in (18) tends to $\delta L/2 =: u$ as $m \to \infty$. Using (1), (5), and (17), we observe that $\gamma(L, \delta, w_s/L)$ is lower bounded by $\frac{1}{L}\log\binom{L}{w_s} - \lim_{m\to\infty}\frac{1}{mL}\log Q_t - \min\left\{\frac{1}{L}\log(v+1), \lim_{m\to\infty}\frac{1}{mL}\log\binom{t+m}{m}\right\}$. Further, we have $\lim_{m\to\infty}\frac{1}{mL}\log\binom{t+m}{m} = \left(\frac{1}{L} + \frac{\delta}{2}\right) h\left(\frac{1}{1+\delta L/2}\right)$, and hence the lower bound on $\gamma(L, \delta, w_s/L)$ simplifies to the expression on the right hand side of (16). ∎

The following theorem presents the asymptotic sphere-packing upper bound on $\gamma(L, \delta, w_s/L)$ when $\delta < \delta^*$.

Theorem 2 (Asymptotic sphere-packing bound for CSCCs)**.** *For $0 < \delta < \delta^*$, we have $\gamma(L, \delta, w_s/L) \leq \gamma_{SP}(L, \delta, w_s/L)$, where $\gamma_{SP}(L, \delta, w_s/L)$ is defined as the expression below*

$$\frac{1}{L}\log\binom{L}{w_s} - \frac{1}{L}h(\lceil \tilde{u} \rceil - \tilde{u}) - \left(\frac{1 + \tilde{u} - \lceil \tilde{u} \rceil}{L}\right)\log\left[\binom{w_s}{\lceil \tilde{u} \rceil}\binom{L-w_s}{\lceil \tilde{u} \rceil}\right] - \left(\frac{\lceil \tilde{u} \rceil - \tilde{u}}{L}\right)\log\left[\binom{w_s}{\lfloor \tilde{u} \rfloor}\binom{L-w_s}{\lfloor \tilde{u} \rfloor}\right], \tag{19}$$

with $\tilde{u} \triangleq \delta L/4$.

Proof: For proving the claim, we apply Prop. 2 and provide an appropriate lower bound on $|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, t; m, L, w_s)|$ (the denominator in (6)), where $t = \lfloor (d-1)/2 \rfloor$. If $v \triangleq$

$\min\{w_s, L-w_s\}$, $\tilde{t} \triangleq \lfloor t/2 \rfloor$, and $\tilde{v} \triangleq \tilde{t}/m$, then we show in the full paper [5] that $|\mathcal{B}_{\mathcal{C}}(\mathbf{x}, t; m, L, w_s)|$ is lower bounded by

$$\binom{m}{\tilde{m}} \left[\binom{w_s}{\lfloor \tilde{v} \rfloor} \binom{L-w_s}{\lfloor \tilde{v} \rfloor} \right]^{\tilde{m}} \left[\binom{w_s}{\lceil \tilde{v} \rceil} \binom{L-w_s}{\lceil \tilde{v} \rceil} \right]^{m-\tilde{m}}, \tag{20}$$

where $\tilde{m} \triangleq m\lceil \tilde{t}/m \rceil - \tilde{t}$. Using (20), and the fact that

$$\lim_{m\to\infty} \frac{\tilde{m}}{m} = \lim_{m\to\infty} (\lceil \tilde{v} \rceil - \tilde{v}) = \lceil \tilde{u} \rceil - \tilde{u}, \tag{21}$$

we have that $\lim_{m\to\infty} \frac{1}{mL} \log |\mathcal{B}_{\mathcal{C}}(\mathbf{x}, t; m, L, w_s)|$ is lower bounded by

$$\begin{aligned} &\frac{1}{L} h\left(\lceil \tilde{u} \rceil - \tilde{u}\right) + \left(\frac{\lceil \tilde{u} \rceil - \tilde{u}}{L}\right) \log \binom{w_s}{\lfloor \tilde{u} \rfloor} \\ &+ \left(\frac{1 + \tilde{u} - \lceil \tilde{u} \rceil}{L}\right) \log \binom{w_s}{\lceil \tilde{u} \rceil} + \left(\frac{\lceil \tilde{u} \rceil - \tilde{u}}{L}\right) \log \binom{L-w_s}{\lfloor \tilde{u} \rfloor} \\ &+ \left(\frac{1 + \tilde{u} - \lceil \tilde{u} \rceil}{L}\right) \log \binom{L-w_s}{\lceil \tilde{u} \rceil}. \end{aligned} \tag{22}$$

The theorem is proved by combining Prop. 2, (1), and (22). ∎

For $L = 2, w_s = 1$, we have $\gamma_{SP}(2, \delta, 0.5) = 0.5(1 - h(\delta/2))$, which also follows from $\gamma(2, \delta, 1/2) = (1/2)\alpha(\delta)$ and then applying the sphere-packing bound (Hamming bound) [7] for unconstrained binary codes.

For $0 < \delta < \min\left\{\delta^*, \frac{4}{L}\right\}$, the expression for $\gamma_{SP}(L, \delta, w_s/L)$ (19), simplifies to

$$\frac{1}{L} \log \binom{L}{w_s} - \frac{\delta}{4} \log\left(w_s(L-w_s)\right) - \frac{1}{L} h\left(\frac{\delta L}{4}\right) \tag{23}$$

IV. Rate Gap between CWCs and CSCCs

The rate penalty due to constant weight per *subblock*, relative to the constraint requiring constant weight per *codeword*, is quantified by $G_{\alpha-\gamma}(L, \delta, w_s/L)$, defined as

$$G_{\alpha-\gamma}(L, \delta, w_s/L) \triangleq \alpha(\delta, w_s/L) - \gamma(L, \delta, w_s/L). \tag{24}$$

A lower bound to this rate gap is given by

$$G^{LB}_{\alpha-\gamma}(L, \delta, w_s/L) \triangleq \left[\alpha_{GV}(\delta, w_s/L) - \gamma_{SP}(L, \delta, w_s/L)\right]^+, \tag{25}$$

where the notation $[z]^+$ implies $\max\{0, z\}$, the term $\gamma_{SP}(L, \delta, w_s/L)$ is given by (19), and

$$\alpha_{GV}(\delta, \omega) \triangleq h(\omega) - \omega h\left(\frac{\delta}{2\omega}\right) - (1-\omega) h\left(\frac{\delta}{2(1-\omega)}\right), \tag{26}$$

with $\alpha_{GV}(\delta, w_s/L)$ denoting the asymptotic GV lower bound for CWCs [10], [7]. The sphere-packing upper bound on the asymptotic rate for CWCs is given by $\alpha_{SP}(\delta, \omega)$, with

$$\alpha_{SP}(\delta, \omega) \triangleq h(\omega) - \omega h\left(\frac{\delta}{4\omega}\right) - (1-\omega) h\left(\frac{\delta}{4(1-\omega)}\right). \tag{27}$$

The following theorem uses above definitions to show that rate penalty is strictly positive when δ is sufficiently small.

Theorem 3. *For even L with $L \geq 4$, we have the strict inequality $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5) > 0$ for $0 < \delta < \tilde{\delta}_L$, where $\tilde{\delta}_L$ is the smallest positive root of $\tilde{f}_L(\delta)$ defined as*

$$\tilde{f}_L(\delta) \triangleq 1 - h(\delta) - \frac{1}{L} \log \binom{L}{L/2} + \frac{\delta}{2} \log \frac{L}{2} + \frac{1}{L} h\left(\frac{\delta L}{4}\right). \tag{28}$$

Proof: Using (23), (25), and (26), we have $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5) = \tilde{f}_L(\delta)$ when $\delta < 2/L$. We show in the full paper [5] that $\tilde{f}_L(0) > 0$ and $\tilde{f}_L(1/L) < 0$, and thus the equation $\tilde{f}_L(\delta) = 0$ has a solution in $(0, 1/L)$ as $\tilde{f}_L$ is a continuous function of δ. The theorem follows by denoting the smallest positive root of $\tilde{f}_L(\delta)$ by $\tilde{\delta}_L$. ∎

Remark: Although Thm. 3 only considers $w_s = L/2$, a similar argument shows that, in general for $0 < w_s < L$, the rate gap $G_{\alpha-\gamma}(L, \delta, w_s/L)$ is strictly positive for small δ.

Proposition 5. *The rate gap between CWCs and CSCCs, $G_{\alpha-\gamma}(L, \delta, w_s/L)$, is identically zero when $\delta^* \leq \delta \leq 1$.*

Proof: Follows from (11) and (12). ∎

In [4], the gap between CWC capacity and CSCC capacity on noisy binary input channels was upper bounded by a rate penalty term defined as

$$r(L, \omega) \triangleq h(\omega) - (1/L) \log \binom{L}{L\omega} > 0, \tag{29}$$

where $\omega = w_s/L$. Further, it was shown in [4] that the actual capacity gap is equal to $r(L, \omega)$ for a noiseless channel. The following proposition shows that $G^{LB}_{\alpha-\gamma}(L, \delta, w_s/L)$ tends to $r(L, w_s/L)$ as δ tends to 0.

Proposition 6. *For $0 < w_s < L$, we have*

$$\lim_{\delta\to 0} G^{LB}_{\alpha-\gamma}(L, \delta, w_s/L) = r(L, w_s/L) > 0. \tag{30}$$

Proof: Take the limit $\delta \to 0$ in (19) and (26). ∎

Proposition 7. *The lower bound on the rate gap between CWCs and CSCCs, $G^{LB}_{\alpha-\gamma}(L, \delta, w_s/L)$, is tight when $\delta \to 0$.*

Proof: Combine Prop. 6 with the observation that upper bound on rate gap, given by $\alpha_{SP}(\delta, w_s/L) - \gamma_{GV}(\delta, \omega)$, also tends to $r(L, w_s/L)$ as δ tends to 0 (see (15), (16), and (27)). ∎

V. Numerical Results

Fig. 1 plots $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5)$ as a function of the subblock length. The upper bound on the gap between CWC capacity and CSCC capacity on noisy binary channels for $w_s = L/2$, given by $r(L, 0.5)$ (see (29)), is also plotted in red. As shown in Proposition 6, the figure demonstrates that $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5)$ tends to $r(L, 0.5)$ as δ gets close to zero. For a fixed value of w_s/L, note that $\alpha_{GV}(\delta, w_s/L)$ is independent of L. Thus, for a given δ, the decrease in $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5)$ with increasing L is due to an increase in CSCC rate. This is intuitively expected, because an increase in L allows for greater flexibility in the choice of bits within every subblock. Further, from Prop. 3, it follows that $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5) \to 0$ as $L \to \infty$.

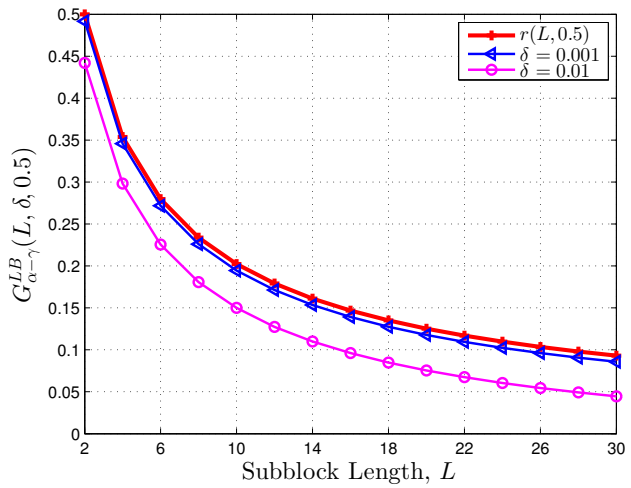

Fig. 1. $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5)$ versus subblock length, L.

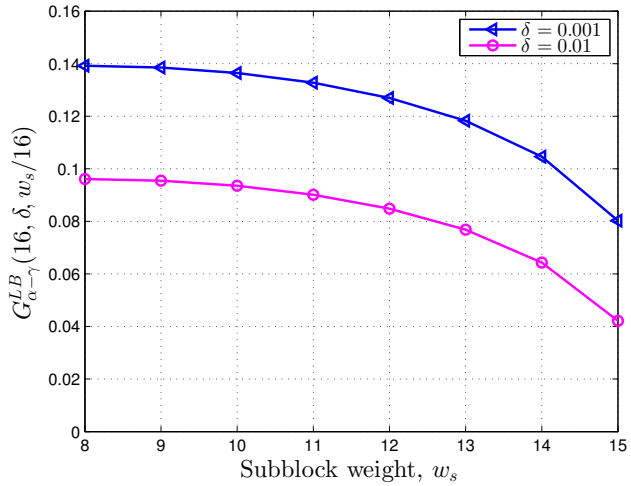

Fig. 2. $G^{LB}_{\alpha-\gamma}(16, \delta, w_s/16)$ as a function of subblock weight, w_s.

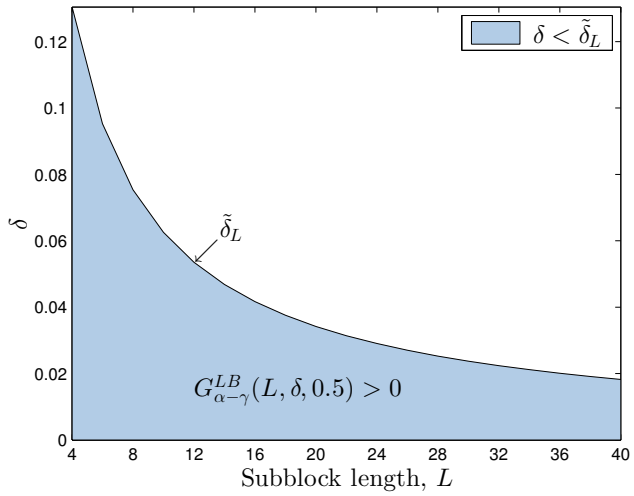

Fig. 3. Area where $G^{LB}_{\alpha-\gamma}(L, \delta, 0.5)$ is strictly positive.

Fig. 2 plots $G^{LB}_{\alpha-\gamma}(L, \delta, w_s/L)$ when the subblock length is fixed at $L = 16$, and w_s varies from $L/2$ to $L-1$. Note that $G^{LB}_{\alpha-\gamma}(L, \delta, (L-w_s)/L) = G^{LB}_{\alpha-\gamma}(L, \delta, w_s/L)$. As expected, the lower bound on the rate gap is seen to decrease with δ.

Fig. 3 depicts the region where $G_{\alpha-\gamma}(L, \delta, 0.5)$ is provably strictly positive. Note that when L fixed and $w_s = L/2$, then $\tilde{\delta}_L$ is the smallest value of δ for which the lower bound $G^{LB}_{\alpha-\gamma}(L, \delta, w_s/L)$ is zero (see Thm. 3). The figure shows that $\tilde{\delta}_L$ decreases with L, and from Prop. 3 it follows that $\tilde{\delta}_L \to 0$ when $L \to \infty$. Moreover, using Prop. 5, it is seen that the actual rate gap $G_{\alpha-\gamma}(L, \delta, 0.5)$ is provably zero for $\delta \geq 0.5$.

VI. Reflections

We derived the GV and sphere-packing bounds for CSCCs. These bounds were used to show that rate gap between CWCs and CSCCs is strictly positive when relative distance δ is small. In particular, for a fixed subblock length L and weight w_s, we demonstrated the existence of some $\tilde{\delta}_L$, such that the gap $G_{\alpha-\gamma}(L, \delta, w_s/L)$ is strictly positive for $\delta < \tilde{\delta}_L$. Furthermore, we provided an estimate on $\tilde{\delta}_L$ via Theorem 3.

The converse problem, on identifying an interval for δ where $G_{\alpha-\gamma}(L, \delta, w_s/L)$ is provably zero was addressed via Proposition 5. An open problem in this regard is to characterize the smallest δ beyond which the respective rate penalties are zero. The results in [4] indicate a nonzero gap between CWC and CSCC capacities on noisy channels, suggesting that for a fixed subblock length L, the rate penalties are zero if and only if the respective asymptotic rates themselves are zero.

In the full paper [5], we also study the *subblock energy-constrained codes* (SECCs) where the constraint on each subblock having weight *exactly* w_s, is replaced by the constraint that subblock weight is *at least* w_s. We show that for $w_s \geq L/2$ and small δ, the asymptotic SECC rate is sandwiched *strictly* between CWC and CSCC asymptotic rates.

References

[1] Y. M. Chee *et al.*, "Multiply constant-weight codes and the reliability of loop physically unclonable functions," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7026–7034, Nov. 2014.

[2] Y. M. Chee, H. M. Kiah, H. Zhang, and X. Zhang, "Constructions of optimal and near-optimal multiply constant-weight codes," *IEEE Trans. Inf. Theory*, Accepted Nov. 2016.

[3] X. Wang, H. Wei, S. Chong, and G. Ge, "New bounds and constructions for multiply constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6315–6327, Sep. 2016.

[4] A. Tandon, M. Motani, and L. R. Varshney, "Subblock-constrained codes for real-time simultaneous energy and information transfer," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 4212–4227, Jul. 2016.

[5] A. Tandon, H. M. Kiah, and M. Motani, "Bounds on the size and asymptotic rate of subblock-constrained codes," Jan. 2017, arXiv:1701.04954 [cs.IT].

[6] E. N. Gilbert, "A comparison of signalling alphabets," *Bell Syst. Tech. J.*, vol. 31, no. 3, pp. 504–522, May 1952.

[7] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 2, pp. 157–166, Mar. 1977.

[8] M. Plotkin, "Binary codes with specified minimum distance," *"IRE Trans. Inform. Theory"*, vol. 6, no. 4, pp. 445–450, Sep. 1960.

[9] R. P. Stanley, "Log-concave and unimodal sequences in algebra, combinatorics, and geometry," *Ann. N.Y. Acad. Sci.*, vol. 576, no. 1, pp. 500–535, 1989.

[10] R. Graham and N. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inf. Theory*, vol. 26, no. 1, pp. 37–43, Jan. 1980.