Upper bounds on |C2| for a uniquely decodable code pair (C1,C2) for a two-access binary adder channel

Citation for published version (APA):

DOI:
10.1109/TIT.1983.1056667

Document status and date:
Published: 01/01/1983

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:
- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher’s website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.

Download date: 17. Apr. 2021
Upper Bounds on $|C_2|$ for a Uniquely Decodable Code Pair $(C_1, C_2)$ for a Two-Access Binary Adder Channel

HENK C. A. VAN TILBORG, MEMBER, IEEE

DEDICATED TO JESSIE MACWILLIAMS ON THE OCCASION OF HER RETIREMENT FROM BELL LABORATORIES

Abstract—An algebraic and a combinatorial upper bound are derived on $|C_2|$ given the code $C_1$, where $(C_1, C_2)$ is a uniquely decodable code pair $(C_1, C_2)$ for a two-access binary adder channel. A uniquely decodable code with rate pair $(0.5170, 0.7814)$ is also described.

I. INTRODUCTION

Consider a binary two-access adder channel. The two users use a binary block code $C_1$, respectively $C_2$, and we shall assume that they are in bit and block synchronization. In the noiseless case (which we shall discuss here) the messages $c_1 \in C_1$, and $c_2 \in C_2$ will be received as $c_1 + c_2$, where the addition $+$ takes place in $Z$.

This noiseless two-access channel has been studied by several authors, e.g., Liao [5], Ahlswede [1], Kasami, Lin et al. [2], [3], [4], [6], [9], and van Tilborg [8].

Liao [5] has shown that the capacity region of this channel can be described by

$$0 < R_1 < 1,$$
$$0 < R_2 < 1,$$
$$R_1 + R_2 < 3/2.$$  \hspace{1cm} (1)

The code pair $(C_1, C_2)$ is called uniquely decodable if the sums $c_1 + c_2$ of all pairs $(c_1, c_2) \in C_1 \times C_2$ are all different. This means that the receiver can uniquely determine the codewords $c_1$ and $c_2$ from their sum.

In van Tilborg [8] it is shown by combinatorial methods that if $n$ is the length of the uniquely decodable code pair $(C_1, C_2)$

$$|C_1| \times |C_2| \leq \sum_{k=0}^{n} \left( \begin{array}{c} n \\ k \end{array} \right) 2^{\min(k, n-k)}.$$  \hspace{1cm} (2)

From (2) one can show with elementary asymptotic methods that the rate pair $(R_1, R_2)$ of any uniquely decodable code pair $(C_1, C_2)$ satisfies (1).

In Wei, Kasami, Lin, and Yamamura [9] the existence of certain good uniquely decodable codes is demonstrated. Asymptotic methods lead to the lower bound in Fig. 1.

In the same paper the authors associate a certain graph $\Gamma(C_1)$ with the code $C_1$. They show that determining the maximal size of a code $C_2$ such that $(C_1, C_2)$ is uniquely decodable is equivalent to determining the maximal size coclique in $\Gamma(C_1)$.

Determining maximal cocliques (or their size) soon becomes computationally infeasible for larger values of $n$. We propose an easy to compute manner of upper bounding $|C_2|$ given $C_1$. In this way one again can derive (2). Moreover by taking a closer look at these bounds one often can improve them in particular cases. We also find a uniquely decodable code $(C_1, C_2)$ with parameters $n = 5$, $|C_1| = 6$, $|C_2| = 15$. This leads to a rate pair above the time sharing line in Fig. 1 formed by the two codes $((0,0), (1,1))$ and $((0,0), (0,1), (1,0))$.

II. DEFINITIONS

Let $V_n$ denote $\{0,1\}^n$ and let $\oplus$ denote modulo 2 addition. An easy way of describing codes (subsets of $V_n$) and certain properties of codes uses the terminology of group algebras.

Definition: The group algebra $(\mathbb{C}(V_n), \oplus, \ast)$ of $V_n$ over $\mathbb{C}$ is the set of formal sums $\sum_{u \in V_n} a_u z^u$, with addition $\oplus$ and multiplication $\ast$ defined by

$$\left( \sum_{u \in V_n} a_u z^u \right) \oplus \left( \sum_{u \in V_n} b_u z^u \right) = \sum_{u \in V_n} (a_u + b_u) z^u,$$
$$\left( \sum_{u \in V_n} a_u z^u \right) \ast \left( \sum_{v \in V_n} b_v z^v \right) = \sum_{w \in V_n} \left( \sum_{u \oplus v = w} a_u \cdot b_v \right) z^w.$$  \hspace{1cm} (3)

A subset $A$ of $V_n$ can now be denoted by the element $\sum_{u \in A} a_u z^u$ of $\mathbb{C}(V_n)$. For this element we shall use the same...
letter $A$. Of particular interest will be the sets

$$Y_k := \{ u \in V_n | w_{H}(u) = k \}, \quad 0 \leq k \leq n,$$

(5)

where $w_{H}$ denotes the Hamming weight.

For the following notions and lemmas the reader is referred to MacWilliams and Sloane [7].

**Lemma 1:** The characteristic numbers $B_k$, $0 \leq k \leq n$, of a code $C$ in $V_n$ defined by

$$B_k = |C|^{-2} \sum_{u \in Y_k} \left| \sum_{c \in C} (-1)^{u_c \cdots + u_{c'}} \right|^2$$

satisfy

$$B_k = |C|^{-1} \sum_{i=0}^{n} A_i P_k(n, i),$$

(7)

where $A_i$ is the $i$th coefficient of the distance enumerator of $C$ and where the Krawtchouk polynomial $P_k(n, x)$ is given by

$$P_k(n, x) = \sum_{i=0}^{k} (-2)^{i} \binom{n-i}{k-i} \binom{x}{i}.$$

(8)

**Definition 3:** The annihilator polynomial $a(x)$ of the code $C$ with characteristic numbers $B_k$ is given by

$$a(x) = 2^n |C|^{-1} \prod_{1 \leq k \leq n} \left(1 - \frac{x}{k}\right).$$

(9)

The degree $r$ of $a(x)$ is called the external distance of $C$. The expansion of $a(x)$ in terms of the Krawtchouk polynomials

$$a(x) = \sum_{k=0}^{r} a_k P_k(n, x)$$

(10)

is called the Krawtchouk expansion of $a(x)$. The coefficients $a_k$, $0 \leq k \leq r$, are called the Krawtchouk coefficients.

**Lemma 4:**

$$C \ast Y_k = \sum_{x \in V_n} B(x, k) \cdot x.$$  

(12)

**Theorem 5:** Let $a_i$, $0 \leq i \leq r$, be the Krawtchouk coefficients of the annihilator polynomial $a(x)$ of a code $C$. Then

$$C \ast \sum_{k=0}^{r} a_k Y_k = V_n,$$

(13)

$$\sum_{k=0}^{r} a_k B(x, k) = 1, \quad \text{for all } x \in V_n.$$

(14)

**III. RESULTS**

In the sequel all the numbers $a_k$, $B(x, k)$, etc., will be defined with respect to the code $C = C_1$.

**Lemma 6:** Let $(C_1, C_2)$ be uniquely decodable. Then

$$\sum_{c_{2} \in C_2} B(c_{2}, k) \leq \binom{n}{k} 2^{n-k}.$$  

(15)

**Remark:** Note that (15) is equivalent with

$$|\{(c_1, c_2) \in C_1 \times C_2 | d_H(c_1, c_2) = k\}| \leq \binom{n}{k} 2^{n-k}.\quad (16)$$

**Proof:** It is sufficient to show that for any $u \in Y_k$

$$|\{(c_1, c_2) \in C_1 \times C_2 | c_2 = c_1 \oplus u\}| \leq 2^k.$$  

(17)

We may assume without loss of generality that $u$ has its ones in the first $k$ coordinate places. Now assume the contrary of (17), i.e., there are more than $2^k$ pairs $(c_1, c_2)$ with $c_2 = c_1 \oplus u$ by the pigeon hole principle at least two $c_1$ must agree on the first $k$ coordinates, say $c_1'$ and $c_1''$. If one now considers the two pairs of codewords $(c_1', c_1'') = (c_1', c_1'' \oplus u)$ and $(c_1', c_1'') = (c_1', c_1' + u)$ in $C_1 \times C_2$, then one easily verifies that

$$c_1' + c_1'' = c_1' + (c_1'' \oplus u) = c_1'' + (c_1' \oplus u) = c_1'' + c_1'.$$

(18)

Indeed $(\ast)$ holds trivially at the last $n - k$ coordinates since $u_i = 0$ for $i > k$, and $(\ast)$ holds on the first $k$ coordinates since $(c_1(i)) = (c_1''(i))$ for $i \leq k$. Obviously (18) contradicts the assumption that $(C_1, C_2)$ is uniquely decodable.

**Lemma 7:** Let $(C_1, C_2)$ be uniquely decodable. Then

$$\sum_{c_{2} \in C_2} B(c_{2}, k) \leq \binom{n}{k} 2^{n-k}.$$  

(19)

**Remark:** Note again that (19) is equivalent to

$$\#\{(c_1, c_2) \in C_1 \times C_2 | d_H(c_1, c_2) = k\} \leq \binom{n}{k} 2^{n-k}.$$  

(20)
Proof: The proof is very similar to the proof of Lemma 6. Again it is sufficient to prove that for any $u \in Y_k$
\[\#(c_i, c_j) \in C_1 \times C_2 \mid c_i = c_j \oplus u\] \[\leq 2^{n-k}. \quad (21)\]
Again assume that $u$ has its ones in the first $k$ coordinate places. Assuming the contrary of (21), we now have the pairs $(c'_i, c'_j) - (c'_i, c'_j \oplus u)$ and $(c''_i, c''_j) = (c''_i, c''_j \oplus u)$ in $C_1 \times C_2$, where $c'_i$ and $c'_j$ now agree on the last $n-k$ coordinates. Again $c'_i + c'_j = c''_i + (c''_i \oplus u) = c''_i + c''_i$ because on the last $n-k$ coordinates $c'_i$ and $c''_i$ agree and on the first $k$ coordinates $c'_i \oplus (c''_i \oplus u)$ equals the all-one vector for $i = 1,2$. 

Lemmas 6 and 7 together yield another proof of (2). Indeed, summing (16) or (20) (depending on the minimum of $2k$ and $2n-k$) for $0 < k < n$ one obtains
\[|C_1| \times |C_2| \leq \sum_{k=0}^{n} \binom{n}{k} 2^{\min(k, n-k)} \quad (22)\]
From (14), (15), and (19) one easily deduces the following theorem.

Theorem 8: Let $\alpha_i, 0 < i < r$, be the Krawtchouk coefficients of the annihilator polynomial $a(x)$ of a code $C_i$. Let $(C_i, C_j)$ be uniquely decodable. Then
\[|C_2| \leq \sum_{k=0}^{r} \max\{0, \alpha_k\} \binom{n}{k} 2^{\min(k, n-k)}. \quad \text{(22)}\]

The importance of Theorem 8 lies mainly in its power to exclude large classes of candidates for the code $C_i$, when one is looking for good uniquely decodable code pairs $(C_1, C_2)$.

Example: $C_1$ is the Preparata code of length $n = 2^{m-1}, m \geq 2$, and size $2^{n-2m+1}$. It is well known (cf. [7]) that $r = 3$ for these codes and that $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = n/3$. It follows from Theorem 8 that
\[|C_1| \leq 4n^2 - 4n + 3.\]
For $m = 2$ one finds at the best the pair $(|C_1|, |C_2|) = (2^8, 843)$ of length 15 with corresponding rate pair $(R_1, R_2) = (0.5334, 0.6480)$. For $m > 2$ the results are even poorer.

Of course if one does not know the $\alpha_i$'s from the literature, then one can compute the $\alpha_i$ quite easily from the distance distribution by means of (7), (9), and (10). If Theorem 8 leaves us with a promising candidate $C_j$, then a closer look at Lemmas 6 and 7 will often help in eliminating $C_j$ as good candidate or in finding the code $C_2$. The idea is that instead of using (13), we try to "cover" $V_n$ or most of $V_n$ by $C \ast Y_1, \ldots, C \ast Y_s$, minimal. The following example may clarify this idea.

Example: Consider $n = 5, C_1 = \{0, 3, 12, 21, 26, 31\}$ in binary notation. It is rather easy to check that
\[A(z) = (3 + 4z^2 + 8z^3 + 2z^4 + 4^2)/3,\]
\[B(z) = (9 + 10z + 16z^2 + 13z^3)/9,\]
\[a(x) = 2x^6 - 1(1 - x)/(1 - x)/(1 - x/3)(1 - x/4)\]
\[= \frac{1}{3}P_0(5, x) + \frac{1}{3}P_1(5, x) + \frac{1}{6}P_2(5, x) + \frac{1}{6}P_3(5, x).\]
It follows from Theorem 8 that
\[|C_2| \leq \frac{1}{3} \times \frac{1}{3} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = 17.\]

With (16) it is not difficult to obtain a smaller upper bound for $|C_2|$. Indeed (16) implies that
\[|C_2| \leq \sum_{k=0}^{n} \binom{n}{k} 2^{\min(k, n-k)}.\]
It is easy to check that
\[k+1 \leq \sum_{k=0}^{n} \binom{n}{k} 2^{\min(k, n-k)}.\]

Example: Consider $n = 5, C_1 = \{0, 3, 12, 21, 26, 31\}$ in binary notation. It is rather easy to check that
\[A(z) = (3 + 4z^2 + 8z^3 + 2z^4 + 4^2)/3,\]
\[B(z) = (9 + 10z + 16z^2 + 13z^3)/9,\]
\[a(x) = 2x^6 - 1(1 - x)/(1 - x)/(1 - x/3)(1 - x/4)\]
\[= \frac{1}{3}P_0(5, x) + \frac{1}{3}P_1(5, x) + \frac{1}{6}P_2(5, x) + \frac{1}{6}P_3(5, x).\]
It follows from Theorem 8 that
\[|C_2| \leq \frac{1}{3} \times \frac{1}{3} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = 17.\]

With (16) it is not difficult to obtain a smaller upper bound for $|C_2|$. Indeed (16) implies that
\[|C_2| \leq \sum_{k=0}^{n} \binom{n}{k} 2^{\min(k, n-k)}.\]
### TABLE I

<table>
<thead>
<tr>
<th>Example</th>
<th>0, 31, 3, 12, 21, 26, 5, 10, 19, 28, 15, 16, 1, 13, 24, 27, 29, 17, 11, 8, 2, 20, 14, 30, 23, 7, 18, 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1 \oplus (0,0,0,0,0)$</td>
<td>$1 1 1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (1,0,0,0,0)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (0,1,0,0,0)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (0,0,1,0,0)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (0,0,0,1,0)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (0,0,0,0,1)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (1,1,1,1,1)$</td>
<td>$1 1 1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (0,1,1,1,1)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (1,0,1,1,1)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (1,1,0,1,1)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (1,1,1,0,1)$</td>
<td>$1 1 1$</td>
</tr>
<tr>
<td>$C_1 \oplus (1,1,1,1,0)$</td>
<td>$1 1 1$</td>
</tr>
</tbody>
</table>

### REFERENCES


