ON THE RATE OF CONSTRAINED ARRAYS

PUTRANTO UTOMO\textsuperscript{1} AND RUUD PELLIKAAN\textsuperscript{2}

Eindhoven University of Technology. Department of Mathematics and Computer Science, Coding and Crypto. PO Box 513. NL-5600 MB.

\textsuperscript{1} p.h.utomo@tue.nl \hspace{1cm} \textsuperscript{2} g.r.pellikaan@tue.nl

Abstract. Sudokus are nowadays very popular puzzles and they are studied for their mathematical structure. Binary Puzzles are also interesting puzzles with certain rules. A solved Binary Puzzle is an n by n binary array satisfying: (i) there are no three consecutive ones and also no three consecutive zeros in each row and each column, (ii) the number of ones and zeros must be equal in each row and in each column, and (iii) every two rows and every two columns must be distinct. Binary Puzzles can be seen as constrained arrays and can be used for modulation purposes, 2D recording and barcodes and is studied in statistical mechanics. In our previous paper, we outlined some problems related to Binary Puzzles such as (1) rate of these codes, (2) erasure decoding probability, (3) decoding algorithms and their complexity. In this paper, we focus on the first problem, that is finding the rate of a code based on the Binary Puzzle.

Key words and Phrases: Binary Puzzle, rate of a code, constrained arrays

1. INTRODUCTION

The Binary Puzzle is an interesting puzzle with certain rules. We look at the mathematical theory behind it. The solved Binary Puzzle is an $n \times n$ binary array that satisfies:

(i) no three consecutive ones and also no three consecutive zeros in each row and each column,

(ii) the number of ones and zeros must be equal in each row and in each column,

(iii) every two rows and every two columns must be distinct.

Figure 1 is an example of a Binary Puzzle. There is only one solution satisfying all three conditions. But there are three solutions satisfying (i) and (ii). The solution satisfying all conditions is given in Figure 2.
In our previous paper \cite{15}, we outlined some problems related to Binary Puzzles such as (1) rate of these code, (2) erasure decoding probability, (3) decoding algorithms and their complexity. In this paper, we focus on the first problem.

The computation of the number of $n \times n$ Binary Puzzles is a very difficult problem, and so far we were only able to obtain the values for small $n$, by brute force.

Since a Binary Puzzle has to satisfy the conditions (1), (2) and (3), we consider these conditions separately and split the computation in three different parts, where each part corresponds to one condition.

That means we consider the following collections of $m \times n$ binary arrays that are constrained:

- $A_{m \times n} = \{ X \in \mathbb{F}_2^{m \times n} | X \text{satisfies (i)} \}$;
- $B_{m \times n} = \{ X \in \mathbb{F}_2^{m \times n} | X \text{satisfies (ii)} \}$;
- $C_{m \times n} = \{ X \in \mathbb{F}_2^{m \times n} | X \text{satisfies (iii)} \}$;
- $D_{m \times n} = \{ X \in \mathbb{F}_2^{m \times n} | X \text{satisfies (i), (ii) and (iii)} \}$;
- $E_{m \times n} = \{ X \in A_{m \times n} | \text{each column of } X \text{ is balanced} \}$,

where $\mathbb{F}_2^{m \times n}$ is the set of all $m \times n$ binary arrays.

Although the exact size of $A_{m \times n}$, $B_{m \times n}$, $D_{m \times n}$ and $E_{m \times n}$ is still an open problem, we provide lower and upper bounds of their size, and also of the asymptotic rates. The exact size of $C_{m \times n}$ is acquired by means of a recursive formula.

2. Main Results

**Definition 2.1.** Let $C$ be a code in $Q^n$, where the alphabet $Q$ has $q$ elements. Recall that the (information) rate of $C$ is defined by

$$ R(C) = \frac{\log_q |C|}{n}. $$
Let $C$ be a collection of codes over a fixed alphabet $Q$ with $q$ elements. The length of $C \subseteq Q^n$ is $n$ and is denoted by $n(C)$. Suppose that the length $n(C)$ goes to infinity for $C \in C$. The upper and lower asymptotic rate or capacity of $C$ are defined by

$$\bar{R}(C) = \limsup_{C \in \mathcal{C}} \frac{\log_q |C|}{n(C)}, \quad R(C) = \liminf_{C \in \mathcal{C}} \frac{\log_q |C|}{n(C)}$$

and in case the limit exists, that means $\bar{R}(C) = R(C)$ it will be denoted by $R(C)$.

Let $A_m$ be the collection of all codes $A_{m \times n}$ for fixed $m$ and all positive integers $n$ and let $A$ be the collection of all codes $A_{m \times n}$ for all positive integers $m, n$. Similarly the collections $B_m, C_m, D_m, E_m$ and $B, C, D, E$ are defined.

2.1. First Constraint.

An array that satisfies the first constraint of the Binary Puzzle is often called a constrained array. Finding the capacity of certain constrained arrays has been studied recently [3, 9, 10, 16, 17] for storage information in 2D and holographic recoding, for 2D barcodes, and in statistical mechanics.

The theory of constrained sequences, that is for $m = 1$, is well established and uses the theory of graphs and the eigenvalues of the incidence matrix of the graph to give a linear recurrence. See [5, 6, 8]. An explicit formula for the number of such sequences of a given length $n$ can be expressed in terms of the eigenvalues. The asymptotical rate is equal to $\log_2(\lambda_{max})$, where $\lambda_{max}$ is the largest eigenvalue of the incidence matrix. Shannon [12] showed already that the following Fibonacci relation holds for $n \geq 1$:

$$|A_{1 \times (n+2)}| = |A_{1 \times (n+1)}| + |A_{1 \times n}|.$$ 

Asymptotically this gives

$$R(A_1) = \lim_{n \to \infty} R(A_{1 \times n}) = \log_2 \left( \frac{1}{2} + \frac{1}{2} \sqrt{5} \right) = 0.69424 \cdots$$

Furthermore $|A_{2 \times n}| = |A_{1 \times n}|^2$, since there is no constraint for the columns in case $m = 2$. Therefore also $R(A_2) = \log_2 \left( \frac{1}{2} + \frac{1}{2} \sqrt{5} \right)$.

Using the same idea, we can find the capacity $R(A_m)$ where the code $A_{m \times n}$ of $A_m$ is viewed as a code of constrained sequences of length $n$ in the alphabet $Q_m = \mathbb{F}_2^m$. For $m$ we get in this way the graph $\Gamma_m$ with $A_{m \times 2}$ as set of vertices. A directed edge in $\Gamma_m$ is from vertex $X$ to vertex $Y$ such that $(X|Y)$ is in $A_{m \times 4}$. So the degree of the characteristic polynomial is $|A_{m \times 1}|^2$, where $|A_{m \times 1}|$ is given by the Fibonacci sequence 2, 4, 6, 10, ..., 110 for $m = 1, 2, 3, 4, \ldots, 9$. So in particular, the degree of the characteristic polynomial $p_m(\lambda)$ in case of $m = 9$ is equal to $110^2 = 12,100$. The largest eigenvalue $\lambda_m$ of the incidence matrix of $\Gamma_m$ is not computed as the largest root of $p_m(\lambda)$, but approximated numerically by Rayleigh quotients [9], that is by the power method with entry scaling. This straightforward idea is due-able for $m \leq 9$ with capacities given in Table 1.
It is clear that \(|A_{(l+m)\times n}| \leq |A_{m\times l}| \cdot |A_{m\times n}|\), since we can split an array \(Z\) in \(A_{(l+m)\times n}\) into two arrays of \(X\) and \(Y\) in \(A_{m\times l}\) and \(A_{m\times n}\), respectively, where \(X\) consists of the first \(l\) rows of \(Z\), and \(Y\) of the last \(m\) rows of \(Z\). Hence \(R(A_{m\times 2n}) \leq R(A_{m\times n})\).

On the other hand, suppose \(X \in A_{l\times n}\) with last row \(\bar{x}\) and \(Y \in A_{m\times n}\) with first row \(\bar{y}\). Let \(Z\) be the \((l+m+2)\times n\) array with \(X\) in the first \(l\) rows of \(Z\), and \(Y\) in the last \(m\) rows of \(Z\), and \(\bar{x}\) in row \(l+1\) and \(\bar{y}\) in row \(l+2\), where \(\bar{x}\) is the complementary column by changing every zero in a one and every one in a zero. Then \(Z\) is an element of \(A_{(l+m+2)\times n}\). Hence \(|A^{(l+m+2)\times n}| \leq |A_{(l+m+2)\times n}|\).

Therefore \(\frac{m}{m+1} R(A_{m\times n}) \leq R(A_{(2m+2)\times n})\). Similarly as in \([17]\), we get for the capacities

\[
\frac{m}{m+1} R(A_{m\times n}) \leq R(A_{2m+2}) \leq R(A_{m+1}).
\]

Now \(R(A_m)\) is decreasing in \(m\) and \(\frac{m}{m+1} R(A_m)\) is increasing in \(m\). So in this way we get lower and upper bounds on the lower capacity \(R(A)\):

\[
\frac{m}{m+1} R(A_m) \leq R(A) \leq R(A_{m+1}).
\]

But in contrast to the case for constrained sequences, there is so far no theory available that gives a closed formula for the capacity of constrained arrays.

<table>
<thead>
<tr>
<th>(m)</th>
<th>(\lambda_{\text{max}})</th>
<th>(R(A_m))</th>
<th>(\frac{m}{m+1} R(A_m))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.6180</td>
<td>0.69424</td>
<td>0.34712</td>
</tr>
<tr>
<td>2</td>
<td>6.8541</td>
<td>0.69424</td>
<td>0.46283</td>
</tr>
<tr>
<td>3</td>
<td>11.7793</td>
<td>0.59303</td>
<td>0.44477</td>
</tr>
<tr>
<td>4</td>
<td>23.5755</td>
<td>0.56990</td>
<td>0.45592</td>
</tr>
<tr>
<td>5</td>
<td>44.3167</td>
<td>0.54697</td>
<td>0.45581</td>
</tr>
<tr>
<td>6</td>
<td>85.3928</td>
<td>0.53467</td>
<td>0.45829</td>
</tr>
<tr>
<td>7</td>
<td>162.9352</td>
<td>0.52486</td>
<td>0.45925</td>
</tr>
<tr>
<td>8</td>
<td>312.1198</td>
<td>0.51787</td>
<td>0.46033</td>
</tr>
<tr>
<td>9</td>
<td>596.9673</td>
<td>0.51230</td>
<td>0.46107</td>
</tr>
</tbody>
</table>

Table 1. Capacity of \(A_m\)

<table>
<thead>
<tr>
<th>(m)</th>
<th>(\lambda_{\text{max}})</th>
<th>(R(E_{2m}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.6180</td>
<td>0.34712</td>
</tr>
<tr>
<td>2</td>
<td>10.0125</td>
<td>0.41546</td>
</tr>
<tr>
<td>3</td>
<td>29.3321</td>
<td>0.40620</td>
</tr>
<tr>
<td>4</td>
<td>89.7965</td>
<td>0.40553</td>
</tr>
<tr>
<td>5</td>
<td>284.9148</td>
<td>0.40771</td>
</tr>
</tbody>
</table>

Table 2. Capacity of \(E_{2m}\)

Using the same idea as before we can also find \(R(E_{2m})\). The corresponding graph \(\Lambda_m\) has \(E_{2m\times 2}\) as set of vertices, which is the subset of \(A_{2m\times 2}\) of arrays that have balanced columns. So \(\Lambda_m\) is a subgraph of \(\Gamma_{2m}\). The corresponding result is shown in Table 2. The number of vertices of \(\Lambda_5\) is 7,056.

2.2. Second Constraint.

A sequence of even length is called balanced, if the number of zeros is equal to the number ones. The number of balanced sequences of length \(2m\) is \((\frac{2m}{2m})\). The rows of an \(2\times 2m\) array in \(B_{2\times 2m}\) are complementary to each other. Hence \(|B_{2\times 2m}| = (\frac{2m}{m})\) and \(R(B_2) = \frac{1}{2}\).
The number of all \( l \times 2m \) binary matrices such that all the rows are balanced is equal to \( \binom{2m}{l} \). If \( X \) is an \( l \times 2m \) binary matrix such that all its rows are balanced, then the \( 2l \times 2m \) binary matrix that is obtained by adding \( \bar{X} \) under \( X \) has all its rows and columns balanced, where \( \bar{X} \) is the complement of \( X \). Hence
\[
\binom{2m}{l} \leq |B_{2l \times 2m}| \leq \binom{2m}{l}^{2l}.
\]
From these inequalities it follows that, asymptotically:
\[
\frac{1}{2} \leq R(B_{2l}) \leq 1 \text{ for all } l.
\]

<table>
<thead>
<tr>
<th>( l )</th>
<th>( R(B_{2l}) )</th>
<th>( m )</th>
<th>( R(B_{2m \times 2m}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.5</td>
<td>1</td>
<td>0.25000</td>
</tr>
<tr>
<td>2</td>
<td>0.6462</td>
<td>2</td>
<td>0.40574</td>
</tr>
<tr>
<td>3</td>
<td>0.7203</td>
<td>3</td>
<td>0.50502</td>
</tr>
<tr>
<td>4</td>
<td>0.7259</td>
<td>4</td>
<td>0.57448</td>
</tr>
<tr>
<td>5</td>
<td>0.7977</td>
<td>5</td>
<td>0.62546</td>
</tr>
<tr>
<td>6</td>
<td>0.8210</td>
<td>6</td>
<td>0.66453</td>
</tr>
<tr>
<td>7</td>
<td>0.8389</td>
<td>7</td>
<td>0.69550</td>
</tr>
</tbody>
</table>

Table 3. Capacity of \( B_{2l} \)

Table 4. Rate of \( B_{2m \times 2m} \)

Four arbitrary elements of \( B_{2m \times 2m} \) give an element of \( B_{4m \times 4m} \). So \(|B_{4m \times 4m}| \geq |B_{2m \times 2m}|^4 \). Therefore \( R(B_{2m \times 2m}) \) is increasing in \( m \).

Referring to [1], we have a good approximation of \(|B_{2m \times 2m}|\):
\[
|B_{2l \times 2m}| = \frac{l!}{l!(2m)} \frac{(2m-1)}{2l} \frac{(2l-1)/2}{(2m-1)/2} \exp\left(\frac{l}{2} + o(1)\right)
\]
for \( l, m \to \infty \). From this it follows that
\[
R(B_{2l}) = \frac{1}{2l} \log_2 \left( \frac{2l}{l} \right)
\]
and therefore \( R(B) = 1 \), which was already shown in [11].

Let \( b_{l \times m} = |B_{l \times m}| \). The exact number of \( b_{2m \times 2m} \) can be obtained recursively. Let \( i = (i_1, \ldots, i_l) \) and \( j = (j_1, \ldots, j_m) \). Denote by \( b_{l \times m}(i; j) \) the collection of all \( l \times m \) arrays with 0/1’s such that there are \( i_s \) ones in row \( s \), for all \( s = 1, \ldots, l \), and there are \( j_t \) ones in column \( t \), for all \( t = 1, \ldots, m \).

Suppose we know the number of \( b_{l \times m}(x; j) \) and \( b_{l \times m}(y; j) \) for all \( x \) and \( y \). It is clear that \( b_{l \times (m+n)}(i; [j, k]) \) is equal to summation of \( b_{l \times m}(x; j) \cdot b_{l \times n}(y; k) \) for all possible \( x \) and \( y \) such that \( x + y = i \). In other word,
\[
b_{l \times (m+n)}(i; [j, k]) = \sum_{x \cdot y = i} b_{l \times m}(x; j) \cdot b_{l \times n}(y; k),
\]
where \( k = (k_1, \ldots, k_n) \), \( x = (x_1, \ldots, x_l) \) and \( y = (y_1, \ldots, y_l) \).
2.3. Third Constraint.

Consider $\bar{C}_{m \times n}$, the set of all $m \times n$ binary arrays that have mutually distinct columns. Let $Q_m = \mathbb{F}_2^m$. Then $\bar{C}_{m \times n}$ can be identified with all words in $Q_m$ with mutually distinct entries. Hence $|\bar{C}_{m \times n}| = 2^m(2^m - 1) \cdots (2^m - n + 1)$. Now $C_{m \times n}$ is a subcode of $\bar{C}_{m \times n}$. Therefore

$$|C_{m \times n}| \leq 2^m(2^m - 1) \cdots (2^m - n + 1).$$

In particular $|C_{m \times n}| = 0$ for all $n > 2^m$. So $R(C_m) = 0$. Therefore $R(\mathcal{C}) = 0$.

Let $X$ in $C_{m \times m}$. Then all the rows of $X$ are distinct and all its columns are distinct. We can extend $X$ to an $(m + 1) \times (m + 1)$ array in $C_{(m+1) \times (m+1)}$ by appending a column $y$ and a row $z$ to $X$, such that still all rows are distinct and all columns are distinct. Then $y$ is an $m \times 1$ array and $z$ is an $(m + 1) \times 1$ array. There are $2^m - m$ possibilities for $y$ and $2^{m+1} - m$ possibilities for $z$. Hence, if $m = n$, we have

$$|C_{(m+1) \times (m+1)}| \geq |C_{m \times m}| \cdot (2^{2m+1} - 3m2^m + m^2).$$

Suppose we have an arbitrary $m \times m$ binary array, say $X$. Let $l = \lceil \log_2(m) \rceil + 1$. Let $Y$ be an $l \times m$ binary array such that all its columns are mutually distinct and have weight not equal to one. Such an array exists, since $m \leq 2^l - l$. Then $(Y|I_l)$ is an $l \times (m + l)$ array such that all its columns are mutually distinct. Let $Z$ be the $(m + l) \times (m + l)$ array such that $X$ is the upper $m \times m$ subarray of $Z$ in the first $m$ rows and columns, with $(Y|I_l)$ in its last $l$ rows and $(Y|I_l)^T$ in its last $l$ columns. Then $Z$ is an array with mutually distinct columns and mutually distinct rows. Hence $|C_{(m+l) \times (m+l)}| \geq 2^{ml^2}$. So

$$R(C_{(m+l) \times (m+l)}) \geq \frac{m^2}{(m + l)^2}.$$ 

Therefore $\lim_{m \to \infty} R(C_{m \times m}) = 1$, since $\lim_{m \to \infty} \frac{l}{m} = 0$. Therefore $\bar{R}(\mathcal{C}) = 1 \neq R(\mathcal{C})$, and $R(\mathcal{C})$ is not defined.

A partition of a set of $m$ elements is a collection of non-empty subsets that are mutually disjoint and their union is the whole set. The collection of all partitions of $t$ non-empty subsets of the set of $\{1, \ldots, m\}$ is denoted by $S(m, t)$. The number $|S(m, t)|$ is called the Stirling number of the second kind and is denoted by $S(m, t)$. Then $S(m, 0) = 0$, $S(m, 1) = S(m, m) = 1$ and the following recurrence relations hold [14]:

$$S(m + 1, t) = tS(m, t) + S(m, t - 1).$$

The following explicit formula holds [13]:

$$S(m, t) = \frac{1}{t!} \sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} j^m.$$
Proposition 2.1. The numbers $|C_{m \times n}|$ satisfy the following recurrence:

$$
\sum_{t=1}^{m} |C_{t \times n}| \cdot S(m, t) = 2^m (2^m - 1) \cdots (2^m - n + 1).
$$

Proof. Let $C_{m \times n}^t$ be the collection of all $m \times n$ binary arrays that have mutually distinct columns and have exactly $t$ mutually distinct rows. Then in particular $|C_{m \times n}^1| = |C_{1 \times n}| = |\tilde{C}_{1 \times n}|$ and $|C_{m \times n}^m| = |C_{m \times n}|$.

Since the $C_{m \times n}^k$ are mutually distinct for $k = 1, \ldots, m$, and give a partitioning of $\tilde{C}_{m \times n}$, we have that $\sum_{t=1}^{m} |C_{m \times n}^t| = |\tilde{C}_{m \times n}|$.

We have seen before that $|\tilde{C}_{m \times n}| = 2^m (2^m - 1) \cdots (2^m - n + 1)$.

Let $X \in C_{m \times n}^t$ and let $x_i$ be the $i$-th row of $X$. Define the sequence $y_1, \ldots, y_t$ by induction as follows $y_1 = x_1$. Suppose that $y_1, \ldots, y_i$ are defined. Then $y_{i+1}$ is the first row in $X$ that is distinct from $y_1, \ldots, y_i$. Then $y_1, \ldots, y_t$ are mutually distinct and give a $t \times n$ array $Y \in C_{t \times n}$ such that $y_i$ is the $i$-th row of $Y$. Let $I_j = \{i | x_i = y_j \}$ for $j = 1, \ldots, t$. Then $I = \{I_1, \ldots, I_t\}$ is a partitioning of $\{1, \ldots, m\}$ with $t$ non-empty subsets.

Conversely, Let $Y$ be in $C_{t \times n}$ with rows $y_1, \ldots, y_t$. Let $I = \{I_1, \ldots, I_t\}$ be a partitioning of $\{1, \ldots, m\}$ with $t$ non-empty subsets. Without loss of generality we may reorder $I_1, \ldots, I_t$ such that $1 \in I_1$ and the minimal $j \in \{1, \ldots, m\}$ that is not in $I_1 \cup \cdots \cup I_t$, is in $I_{t+1}$ for all $i < t$. Let $X$ be the $m \times n$ matrix such that the $i$-row of $X$ is equal to $y_j$ is $i \in I_j$. Then $X \in C_{m \times n}^t$.

In this way we have obtained a bijection between $C_{m \times n}^t$ and $C_{t \times n} \times S(m, t)$.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$R(C_{m \times m})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.00000</td>
</tr>
<tr>
<td>3</td>
<td>0.89382</td>
</tr>
<tr>
<td>5</td>
<td>0.96765</td>
</tr>
<tr>
<td>8</td>
<td>0.99527</td>
</tr>
<tr>
<td>11</td>
<td>0.99936</td>
</tr>
<tr>
<td>12</td>
<td>0.99967</td>
</tr>
<tr>
<td>15</td>
<td>0.99995</td>
</tr>
<tr>
<td>17</td>
<td>0.99998</td>
</tr>
<tr>
<td>25</td>
<td>0.99999</td>
</tr>
</tbody>
</table>

Table 5. Rate of $C_{m \times m}$

<table>
<thead>
<tr>
<th>$m$</th>
<th>$R(D_{2m \times 2m})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.25</td>
</tr>
<tr>
<td>2</td>
<td>0.39</td>
</tr>
<tr>
<td>3</td>
<td>0.34</td>
</tr>
</tbody>
</table>

Table 6. Rate of $D_{2m \times 2m}$

2.4. All Constraints.

The size of $D_{2m \times 2m}$ can be approximated by smaller building blocks such that the conditions are still satisfied. There are exactly two building block of size $2 \times 2$. Hence, $R(D_{2m \times 2m}) \geq \frac{1}{(2m)^2} \log_2(2m^2) = \frac{1}{4}$, for $m \geq 1$. 
By brute force computations, we could give only a few values in Table 6. It is shown by De Biasi [2] that asymptotically the rate rate of $D_{2m \times 2m}$ is the same as $A_{2m \times 2m} \cap B_{2m \times 2m}$ as $m$ goes to infinity, by an argument similar to our proof showing that $\lim_{m \to \infty} R(C_{m \times m}) = 1$.

For constrained sequences it is known that the capacity does not change if one adds the condition that the sequence is balanced [4, 7]. It seems that a similar balancing argument as in [16] is not true for our constrained arrays, since

$$A_{2m \times 2m} \cap B_{2m \times 2m} \subseteq E_{2m \times 2m} \subseteq A_{2m \times 2m}$$

and Tables 1 and 2 indicate that $R(E_{2m}) < R(A_{2m})$. Therefore more research is needed to determine $R(D)$, that is the capacity of Binary Puzzles.

REFERENCES