Binary Puzzles as an Erasure Decoding Problem

Putranto Hadi Utomo   Ruud Pellikaan
Eindhoven University of Technology
Dept. of Math. and Computer Science
PO Box 513. 5600 MB Eindhoven
p.h.utomo@tue.nl   g.r.pellikaan@tue.nl

Appeared in:
Proceedings of the 36th WIC Symposium on Information Theory in the Benelux
(J. Roland, F. Horlin. Eds.) pp. 129-134, 2015
Corrected version July 28, 2016

Abstract

Binary puzzles are interesting puzzles with certain rules. A solved binary puzzle is an $n \times n$ binary array such that there are no three consecutive ones and also no three consecutive zeros in each row and each column, the number of ones and zeros must be equal in each row and in each column, every two rows and every two columns must be distinct.

Binary puzzles can be seen as constrained arrays. Usually constrained codes and arrays are used for modulation purposes. In this paper we investigate these arrays from an erasure correcting point of view. We give lower and upper bound for the rate of these codes, the probability of correct erasure decoding and erasure decoding algorithms.

1 Introduction

Sudokus are nowadays very popular puzzles and they are studied for their mathematical structure [2, 5, 18]. For instance the minimal number of entries that can be specified in a single 9×9 puzzle to ensure a unique solution was in [14] conjectured to be 17, and this was proved by means of the chromatic polynomial of the Sudoku graph [7]. Furthermore the erasure correcting capabilities and decoding algorithms of the collection of $n \times n$ a Sudokus are considered [13, 16]. The asymptotic rate is still an open problem [1, 7]. Solving an $n \times n$ Sudoku puzzle is an NP-hard problem [17].

The binary puzzle is also an interesting puzzle with certain rules and is the focus of this paper. We look at the mathematical theory behind it. The solved binary puzzle is an $n \times n$ binary array that satisfies:

1. no three consecutive ones and also no three consecutive zeros in each row and each column,

2. every row and column is balanced, that is the number of ones and zeros must be equal in each row and in each column,

3. 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 3 solutions satisfying (1) and (2). The solution satisfying three all conditions is given in Figure 2. Figure 3 and 4 are solved puzzles where the third constraint is excluded.

	0						
			1		1		0
		0					
	1						
				1			
	0				1		
	0			0			
				0		0	

Figure 1: Unsolved Puzzle

1	0	1	0	1	0	1	0
0	1	0	1	0	1	1	0
1	0	0	1	1	0	0	1
0	1	1	0	0	1	1	0
0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0
1	0	0	1	0	0	1	1
0	1	1	0	0	1	0	1

Figure 2: Solved Puzzle

1	0	1	0	1	0	0	1
0	1	0	1	0	1	1	0
1	0	0	1	1	0	1	0
0	1	1	0	0	1	0	1
0	1	0	1	1	0	1	0
1	0	1	0	1	1	0	0
1	0	0	1	0	0	1	1
0	1	1	0	0	1	0	1

Figure 3: Solved Binario Puzzle with repetition of column/row allowed

0	0	1	0	1	0	1	1
1	1	0	1	0	1	0	0
1	0	0	1	1	0	1	0
0	1	1	0	0	1	0	1
0	1	0	1	1	0	1	0
1	0	1	0	1	1	0	0
1	0	0	1	0	0	1	1
0	1	1	0	0	1	0	1

Figure 4: Solved Binario Puzzle with repetition of column/row allowed

Binary and Sudoku puzzle can be seen as constrained arrays. Usually constrained codes and arrays are used for modulation purposes [8, 9]. We investigate these arrays from an erasure correcting point of view. We give lower and upper bound for the rate of these codes, the probability of correct erasure decoding and erasure decoding algorithms.

2 Constrained sequences and constrained array

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

$$R(C) = \frac{\log_q |C|}{n}.$$

In the following $Q = \mathbb{F}_2$, $n = lm$ and $\mathbb{F}_2^{l\times m}$ is the set of binary $l \times m$ arrays. Define:

$$\begin{aligned}
A_{l\times m} &= \{X \in \mathbb{F}_2^{l\times m} \mid X \text{ satisfies (1) }\};\\
B_{l\times m} &= \{X \in \mathbb{F}_2^{l\times m} \mid X \text{ satisfies (2) }\};\\
C_{l\times m} &= \{X \in \mathbb{F}_2^{l\times m} \mid X \text{ satisfies (3) }\};\\
D_{l\times m} &= \{X \in \mathbb{F}_2^{l\times m} \mid X \text{ satisfies (1), (2) and (3) }\}.
\end{aligned}$$

The theory of constrained sequences, that is for $l = 1$, is well established and uses the theory of graphs and the eigenvalues of the incidence matrix to give a linear recurrence. An explicit formula for the number of such sequences of a given length m can be expressed in terms of the eigenvalues. The asymptotical rate is equal to $\log_q(\lambda_{max})$, where λ_{max} is the largest eigenvalue. See [8, 9]. Shannon [15] showed already that the following relation holds for $m \geq 1$:

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

Asymptotically this gives

$$R(A_{1\times m}) \approx \log_2\left(\frac{1}{2} + \frac{1}{2}\sqrt{5}\right), \quad \text{for } m \to \infty$$

The number of balanced sequence is equal to a number of combination of ones, that is $B_{1\times 2m} = \binom{2m}{m}$ and asymptotically $R(B_{1\times 2m}) \approx 1$, for $m \to \infty$.
It was shown [6, 10, 11] that the balanced property does not influence the asymptotic rate of constrained sequences. So $R(A_{1\times 2m} \cap B_{1\times 2m}) \approx \log_2\left(\frac{1}{2} + \frac{1}{2}\sqrt{5}\right)$, for $m \to \infty$.
We expect that a similar result holds for balanced constrained arrays.
For arrays we know that $\binom{2l}{l}^m \leq |B_{2l\times 2m}| \leq \binom{2l}{l}^{2m}$. From these inequalities it is can be shown that, asymptotically:

$$\tfrac{1}{2} \lesssim\leq R(B_{2m\times 2m}) \leq 1, \quad \text{for } m \to \infty$$

Four arbitrary elements of $B_{2m\times 2m}$ gives 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.

Now, consider $C_{l\times m}$. We clearly have that $|C_{l\times m}| \leq 2^m(2^m-1)\cdots(2^m-n+1)$. Furthermore, if $m=n$, $|C_{(n+1)\times(n+1)}| \geq |C_{n\times n}| \cdot (2^{2n+1} - 2n2^n + n^2)$.
This implies that, asymptotically:

$$R(C_{2m\times 2m}) \approx 1, \quad \text{for } m \to \infty$$

The size of $D_{2m\times 2m}$ can be approximated by smaller building blocks such that the conditions are still satisfied [4]. There are exactly two building block of size 2×2. Hence, $R(D_{2m\times 2m}) \geq \frac{1}{(2m)^2}\log_2(2^{m^2}) = \frac{1}{4}$, for $m \geq 1$.

Numerically, we have

m	$A_{2m\times 2m}$		$B_{2m\times 2m}$		$C_{2m\times 2m}$		$D_{2m\times 2m}$	
	Size	Rate	Size	Rate	Size	Rate	Size	Rate
1	16	1	2	0.25	10	0.83	2	0.25
2	2030	0.69	90	0.41	33864	0.94	76	0.39
3	3858082	0.61	?	?	?	?	5868	0.34

3 Erasure Channel

Suppose Q is a set of an alphabet and C is a code in Q^n.
Define $\hat{Q} = Q \cup \{-\}$, where the symbol ”-” denotes a blank, that is an erasure, and $\hat{C} = \{\mathbf{r} \in \hat{Q}^n | \mathbf{r} \text{ is obtained from a } \mathbf{c} \in C \text{ by erasures}\}$.

Suppose $\mathbf{r}$ is the received word given that $\mathbf{c}$ is sent. We have $d(\mathbf{r},\mathbf{c})$ is the Hamming distance between $\mathbf{r}$ and $\mathbf{c}$. Since the errors are only blanks, $d(\mathbf{r},\mathbf{c})$ equal to the number of blanks in $\mathbf{r}$. Let $\mathbf{c}(\mathbf{r})$ be a closest codeword to $\mathbf{r}$, then $d(\mathbf{r},C) = d(\mathbf{r},\mathbf{c}(\mathbf{r}))$. Let p be the probability that a symbol is erased, and let $P_{ed,C}(p)$ denote the probability of correct erasure decoding. Then

$$P_{ed,C}(p) = \sum_{\mathbf{c}\in C} P(\mathbf{c}) \sum_{\substack{\mathbf{r}\in\hat{C} \\ \mathbf{c}(\mathbf{r})=\mathbf{c}}} P(\mathbf{r}|\mathbf{c})$$

Suppose $\mathcal{E}_i(C) = \{\mathbf{r} \in \hat{C} | d(\mathbf{r},C) = i\}$ and $E_i(C) = |\mathcal{E}_i(C)|$.
Define the homogenous erasure distance enumerator for code C by

$$E_C(X,Y) = \sum_{i=0}^{n} E_i(C) X^{n-i} Y^i$$

Proposition 3.1

$$P_{ed,C}(p) = \frac{1}{|C|} E_C(1-p, p)$$

Proposition 3.2 *Let $C \subseteq Q^m$ and $D \subseteq Q^n$. We have*

$$E_{C\times D}(X,Y) = E_C(X,Y)\cdot E_D(X,Y)$$

Corollary 3.3

$$P_{ed,C\times D}(p) = (P_{ed,C}(p))\cdot(P_{ed,D}(p))$$

Corollary 3.4

$$P_{ed,C^n}(p) = (P_{ed,C}(p))^n$$

4 Binary Puzzle Solver

Binary puzzle can be seen as a SAT problem. Since each cell in the binary puzzle can only take the values '0' and '1', we can express the puzzle as an array of binary variables, where false corresponds to '0' and true to '1'. Next, we express each condition in terms of a logical expression.

Suppose we have an $2m \times 2m$ array in the variables x_{ij}. The array satisfies the first condition, that there are no three consecutive ones and also no three consecutive zeros in each row and each column, if and only if the expression below is true:

$$\left(\bigwedge_{i=1}^{2m}\left\{\bigwedge_{k=1}^{2m-2}\left(\left[\neg\left(\bigwedge_{j=k}^{k+2} x_{ij}\right)\right]\wedge\left[\neg\left(\bigwedge_{j=k}^{k+2}\neg x_{ij}\right)\right]\right)\right\}\right)\wedge$$
$$\left(\bigwedge_{j=1}^{2m}\left\{\bigwedge_{k=1}^{2m-2}\left(\left[\neg\left(\bigwedge_{i=k}^{k+2} x_{ij}\right)\right]\wedge\left[\neg\left(\bigwedge_{i=k}^{k+2}\neg x_{ij}\right)\right]\right)\right\}\right)$$

For satisfying the second condition on balancedness, the following expression must be true

$$\left(\bigwedge_{j=1}^{2m}\left[\bigwedge_{1\le i_1<\cdots<i_{m+1}\le 2m}\left(\bigvee_{k=1}^{m+1} x_{i_k,j}\right)\right]\right)\wedge\left(\bigwedge_{i=1}^{2m}\left[\bigwedge_{1\le j_1<\cdots<j_{m+1}\le 2m}\left(\bigvee_{k=1}^{m+1} x_{i,j_k}\right)\right]\right)\wedge$$
$$\left(\bigwedge_{j=1}^{2m}\left[\bigwedge_{1\le i_1<\cdots<i_{m+1}\le 2m}\left(\bigvee_{k=1}^{m+1} \neg x_{i_k,j}\right)\right]\right)\wedge\left(\bigwedge_{i=1}^{2m}\left[\bigwedge_{1\le j_1<\cdots<j_{m+1}\le 2m}\left(\bigvee_{k=1}^{m+1} \neg x_{i,j_k}\right)\right]\right).$$

Note that the complexity of this expression grows as $\binom{2m}{m}$ which is exponentially in m. An alternative polynomial expression can be obtained.

The satisfiability of the third condition, that every two rows and every two columns must be distinct, is equal to

$$\left(\bigwedge_{1\le j_1<j_2\le 2m}\left\{\bigwedge_{i=1}^{2m}\neg\left[(x_{i,j_1}\wedge x_{i,j_2})\vee(\neg x_{i,j_1}\wedge\neg x_{i,j_2})\right]\right\}\right)\wedge$$
$$\left(\bigwedge_{1\le i_1<i_2\le 2m}\left\{\bigwedge_{j=1}^{2m}\neg\left[(x_{i_1,j}\wedge x_{i_2,j})\vee(\neg x_{i_1,j}\wedge\neg x_{i_2,j})\right]\right\}\right).$$

It is shown in [3] that the binary puzzle is NP-complete.

References

[1] C. Atkins and J. Sayir, "Density evolution for SUDOKU codes on the erasure channel," *Proc. 8th Int. Symp. on Turbo Codes and Iterative Information Processing (ISTC),* 2014.

[2] R.A. Bailey, P.J. Cameron and R. Connelly, "Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes," *Amer. Math. Monthly*, 115(5):383–404, 2008.

[3] M. De Biasi, "Binary puzzle is NP-complete,"

`http://nearly42.org`

[4] T. Etzion and K.G. Paterson, "Zero/positive capacities of two-dimensional runlength-constrained arrays," *IEEE Trans. Information Theory*, 51(9):3186–3199, Sept 2005.

[5] B. Felgenhauer and A.F. Jarvis, "Mathematics of Sudoku I, II" *Mathematical Spectrum* 39:15–22, 54–58, 2006.

[6] H.C. Ferreira, J.H. Weber, C.H. Heymann and K.A.S. Immink "Markers to construct dc free (d, k) constrained balanced block codes using Knuths inversion" *Electronics Letters*, 48(19):1209-1211, Sept 2012.

[7] A.M. Herzberg and M. Ram Murty, "Sudoku squares and chromatic polynomials," *Notices Amer. Math. Soc.* 54 (6):708–717, July 2007.

[8] H.D.L. Hollmann. *Modulation Codes.* Philips Electronics N.V., PhD thesis Techn. Univ. Eindhoven, 1996.

[9] K.A.S. Immink, P.H. Siegel, and J.K. Wolf, "Codes for digital recorders," *IEEE Transactions on Information Theory*, 44(6):2260–2299, Oct 1998.

[10] K.A.S. Immink and J.H. Weber, "Very efficient balanced codes," *IEEE Transactions on Selected Areas in Communications,* , 28(2):188–192, Feb 2010.

[11] D.E. Knuth, "Efficient balanced codes," *IEEE Transactions on Information Theory,* , 32(1):51–53, Jan 1986.

[12] J.H. van Lint. *Introduction to Coding Theory.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1982.

[13] L.A. Phillips, S. Perkins, P.A. Roach and D.H. Smith, "Erasure correction capabilities of Sudoku and related combinatorial structures," *Proc. 4th Research Student Workshop, University of Glamorgan*, 65–69, 2009.

[14] `http://staffhome.ecm.uwa.edu.au/~00013890/sudokumin.php`

[15] C.E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, 27(10):379–423, October 1948.

[16] E. Soedarmadji and R. McEliece, "Iterative Decoding for Sudoku and Latin Square Codes," *Proceeings 45th Annual Allerton Conference on Communication, Control, and Computing,* 488–494, 2007.

[17] T. Yato and T. Seta, "Complexity and completeness of finding another solution and its application to puzzles," *Proc. National Meeting of the Information Processing Society of Japan (IPSJ),* 2002.

[18] `http://en.wikipedia.org/wiki/Mathematics_of_Sudoku`