# Application of Hamming Code Theory in Prisoner 's Chessboard Puzzle

Jiahao Wang

School of Mathematics, Southeast University, Nanjing, Jiangsu, China, 2 11189

**Abstract.** This work proposed a universal algorithm based on the parity-check theory of Hamming code for solving the Prisoner's Chessboard Puzzle (PCP) which is known as an unsolvable mathematical problem. The solution to the simplest two-dimensional PCP is first given. However, no suitable strategy is available when the 3D PCP is transformed into a 3D cube coloring problem. To explore the existence and structure of the solution of PCP, we make the rows of the whole chessboard into a line and then uses the idea of Hamming code parity check. After proving the agreement of parity check results and XOR operation ones, we carry out XOR operation to get a universal solution for PCP. The results show that the method can solve any dimension PCP effectively.

**Keywords:** Prisoner's Chessboard Problem (PCP); Hamming Code; Parity Check; XOR Operation.

## 1. Introduction

In real communication processes, data errors inevitably occur due to imperfect channel transmission and additive noise. Error correcting codes have thus become a powerful tool for detecting and correcting errors in the transmission or storage of digital information [1]. In the 1940s, Claude Shannon [2] initiated the research of coding theory. Then, many new coding techniques and coding strategies [3-6] have been proposed and applied to many fields [5-8]. As the oldest and most widely used error-correcting code, Hamming code is simple in form and easy to implement, and it performs well in detecting and correcting single-bit errors [7-8]. On the other hand, the advanced error-correcting codes (LDPC codes, Turbo codes, etc.) provide additional choices for different application scenarios, while still have their own drawbacks [3-6].

The Prisoner's Chessboard Puzzle (PCP), regularly referred to as an unsolvable mathematical problem, has been repeatedly a benchmark problem in error-correcting code theory. Due to its uncertainty and complexity, PCP has received limited attention. Currently, no published works are about the coding theory of PCP.

This work proposes a universal solution based on Hamming theory for any dimension PCP. It is the first time that Hamming codes theory is applied to solve PCP.

The paper is organized as follows. Section II introduces Hamming codes, including their superiority and elegance. Section III states Prisoner's Chessboard Puzzle. Section IV derivates the universal method based on Hamming code for PCP after 2D and 3D PCP are solved. Section V presents some concluding remarks.

## 2. Hamming code

The abstract mathematical model of general communication mode [2] is shown in Fig.1. The error correction coding is needed to ensure the transformation of the information without distortion [9].

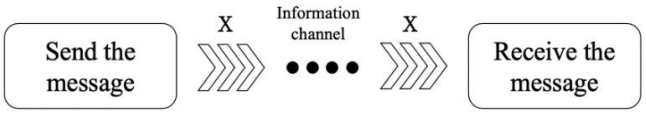



Fig. 1 General communication mode diagram

Next, the main idea and elegance of Hamming codes are described.

Hamming codes [14]: Let $m \geq 2, F_q^m$ has $q^m - 1$ non-zero vectors. Two nonzero vectors are said to be projectively equivalent if the sum of two nonzero vectors $v_1 v_2$ is $F_q$-linearly dependent if and only if there exists $\alpha \in F_q^*$ such that $v_1 = \alpha v_2$. It can be seen that there are q-1 vectors in each equivalence class, and thus there $\frac{q^m-1}{q-1}$ are equivalence classes. If a representative vector is taken from each equivalence class, a total of n= vectors can be taken $\frac{q^m-1}{q-1} u_1, \ldots, u_n$, and each vector table grows into m column vectors, arranged in $F_q$ the previous $m \times n$ matrix $H_m = (u_1, \ldots, u_n)$, and when $m \geq 2$, $H_m$ the q-ary linear code C with the check matrix is called a Hamming code.

## 2.1 Parity Check

The central idea of Hamming codes is parity check performed based on the number of "1" s in the digital bits of the transmitted group of binary codes is odd or even. Generally, calibration is specified in advance. For example, 12 bits are for information storage, and 4 bits are an error correction code in a 16-bit data information.

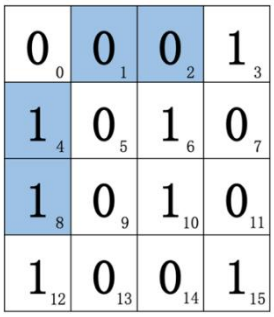



Fig. 2 bits 1,2,4,8 positions

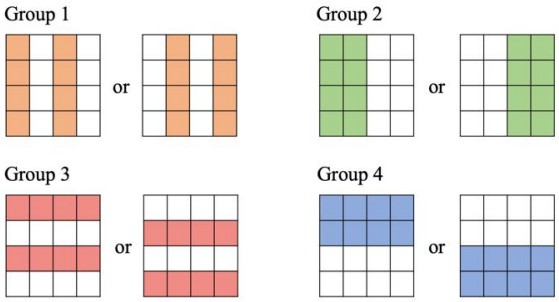



Fig. 3 Hamming code parity grouping of 16-bit data

Note that the 4-bit error correction code can only be placed at bits 1, 2, 4, and 8 (Fig. 2), generally $2^k$ (k=1, 2, 3...) for more bits, because the value is increased by a multiple of 2 in parity check processes. Figure 3 shows the parity checking principle for a 16 bits data. Four optimized parity checks are performed, corresponding to four parity check groups. Based on the results of the four sets of parity checks, the location of the information error is sure accurately. A special bit (error correction code) is needed in each group to control the parity check of the whole group.

## 2.2 Elegance of Hamming codes

Elegance of Hamming codes is its simplicity. Next, we will show the number of the error positions of parity and XOR agree in Hamming after replacing "yes" and "no" with 1 and 0, and arranging the results in 4 parity checks in Fig.3.

Introducing the exclusive OR operation, the corresponding operation rules are

$$\mathbf{0} \oplus \mathbf{0} = \mathbf{0}$$

$$\mathbf{1} \oplus \mathbf{0} = \mathbf{1}$$

$$\mathbf{0} \oplus \mathbf{1} = \mathbf{1}$$

$$\mathbf{1} \oplus \mathbf{1} = \mathbf{0}$$

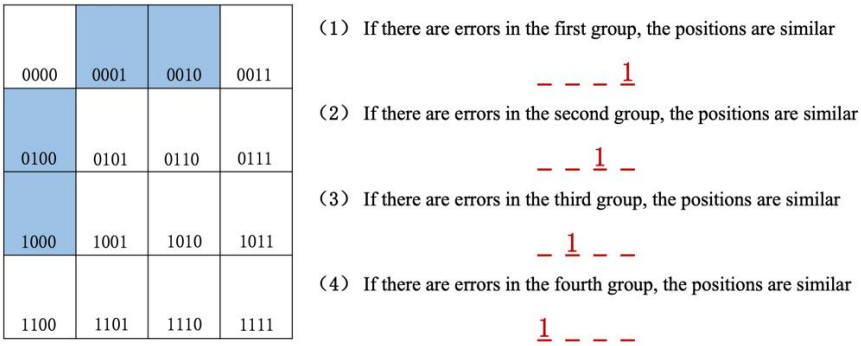



Fig. 4 Schematic diagram of Hamming code XOR operation of 16-bit data

Figure 4 shows the Hamming XOR rule for 16-bit data. The 16 bits are numbered from 0 to 15 written as a binary number (in this case, 4-bit binary). It is clear four parity-checking cases correspond to four problems, respectively. Figure 5 displays the correspondence between parity checking and exclusive OR operations in Hamming frame. The first column and second column in Figure 5 count the number of red areas in the first parity group and the second parity group, respectively (0 for even numbers, 1 for odd numbers). Thus, the final results are the same as that of the parity check.

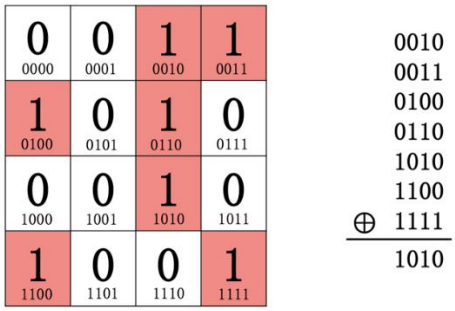
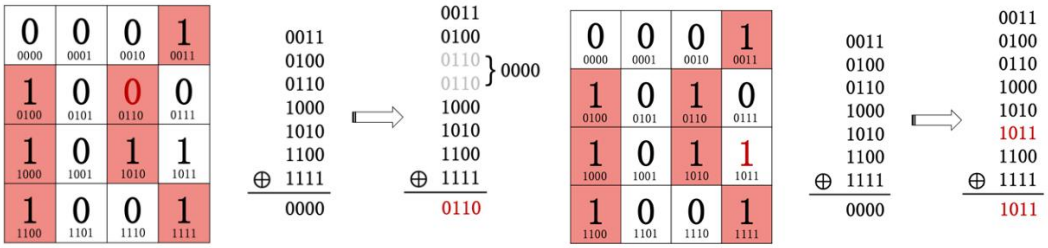



Fig. 5 Correspondence between Hamming Code XOR Operation and Parity Check of 16-bit Data




(a) (b)

Fig. 6 One-to-one correspondence between XOR operation of 16-bit data and parity check: (a) 0 becomes 1;(b) 1 becomes 0

Figure 6 shows the results when 0 is changed to 1 and when 1 is changed to 0, respectively. As can be seen in Fig. 6 (a), after 0 at any position therein becomes 1, the present operation result is the modified position. Similarly, in Fig. 6 (b), for the case where 1 becomes 0, since 1+1=0 in the exclusive OR operation, the effect of adding a binary number and subtracting a binary number at one position is equivalent. Thus, changing from 1 to 0 is equivalent to adding the binary position number of the position to the original XOR operation, and the result is the position. The result of Fig. 6 shows that the result obtained by the XOR operation is the same as the that of the parity check.

# 3. Prisoner's Chessboard puzzle (PCP)

The Prisoner's Chessboard puzzle is about: A warden gives two prisoners a chance at freedom after they solve a conundrum that the warden orchestrated. The warden brings the first prisoner to a room, where a 64-square chessboard is placed with a coin placed on each square. The key of the prison is in a dark box under one of the squares. The first prisoner is only allowed to choose one of the coins and flip it over, then walk out of the room. Then, the second prisoner enters (no conversation allowed), and is required to accurately find the key without any additional information.

PCP involves complex combinatorial problems, error-correcting coding problems, etc., and is often referred to as an impossible mathematical problem.

# 4. Hamming Codes for PCP

## 4.1 Two-dimensional PCP problem

We first consider the simplest case. Suppose only two squares are on the chessboard, the coin status on a grid is the key position.

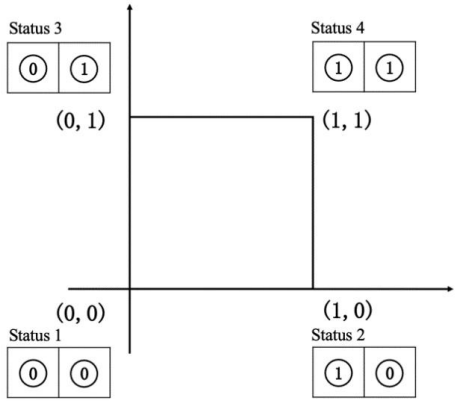



Fig. 7 Flowchart of solving two-dimensional PCP

Figure 7 shows the solving process of the two-dimensional PCP problem. If 0 and 1 are the state of the coin with the back side on the top and the front side on the top, and the two squares are 0 and 1 from left to right, so the whole chessboard is two-dimensional in Cartesian coordinates. There are four cases of bits 0 and 1 (status 1 - 4). If the key is at position 0, the corresponding coordinates are (0, 0) and (1, 0). If the key is at position 1, the corresponding coordinates are (0, 1) and (1, 1). No matter which status is considered, the prisoner can easily find the right key position which is 0 or 1.

## 4.2 Three-dimensional PCP

3D board puzzle problem has eight ways to place the coin when there are 0, 1 and 2 positions. The situation is more difficult. We equal the 3D PCP to color the vertices of the cube, any color of red, green and blue can be reached from any vertex. Only one of these strategies is discussed here. Suppose that the position of the key is given by

$$\boldsymbol{Key = (0 \cdot C_0 + 1 \cdot C_1 + 2 \cdot C_2) mod\ 3}$$

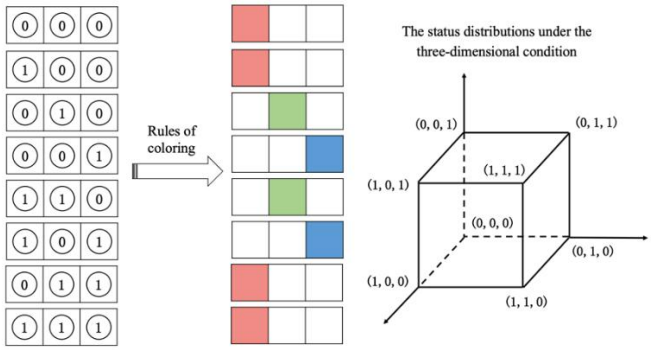



Fig. 8 Schematic diagram of solving three-dimensional PCP problem

Figure 8 shows a simple way to solve a three-dimensional PCP. Assuming that the initial position is (0, 0, 0), you can reach any color in red, green and blue, but if the initial position is changed to (0, 1, 0), you can only reach green or red, and never reach blue. Under this circumstance, the strategy doesn't work, that is, if the warden places the coin (0, 1, 0) and the key under position 2, the prisoners will never find the key.

### 4.3 Multidimensional chessboard puzzle problem

4.3.1 Existence of the solution

Supposing we can change one of the positions of an n-dimensional data, it is equivalent to moving on one side of the hypercube in n-dimensional space, so the original problem can be transformed into a similar coloring problem.

Figure 9 shows a schematic diagram of the existence of n-dimensional data policies. It is obvious the number of vertices corresponding to each color is an integer with a form $\frac{2^n}{n}$. Obviously, there have suitable strategies if and only if n=1, 2, 4, and 8.

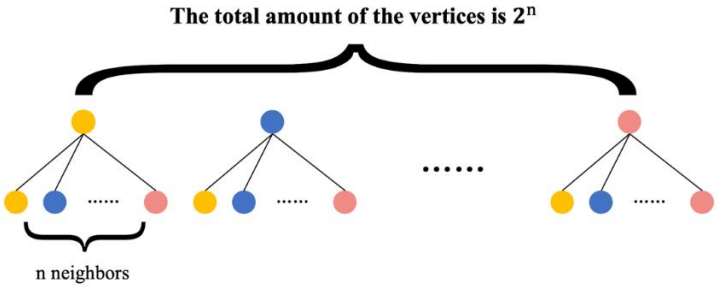



Fig. 9. Existence of n-dimensional data policies

4.3.2 Hamming code method for solving general PCP

As the number of squares increases, the board becomes increasingly complex. Here we remark the position of the key as the error position. Thus, the PCP is turned into the second prisoner finds the error position after the first prisoner enters the room and adjusts a coin to make the key position is the error position. The first prisoner does XOR for all binary numbers of face-up squares on the 64-square chessboard., and make sure which coin he can flip so that the result can be located at the error location. And the second prisoner also does the XOR operation and find out the error position. As shown in Section 4.3.1, if $\frac{2^n}{n}$ is an integer, that is, $n = 2^k (k = 0,1,2,\dots)$, the number of squares on the chessboard must be even, we can get a strategy to solve PCP.

Figure10 shows an n-dimensional checkerboard parity packet. We group n-dimension in "half and half" way, and select 1, 2, 4..., $2^{k-1}$, and then k parity check groups are subjected to grouping check. For simplicity, all the chessboards are regarded as a single row in row order, and this will not affect the parity check of the Hamming code. Similarly, the above checkerboard can also be

numbered and written as binary positions, and we do exclusive-OR at the position of the code number 1, and the result of the operation does correspond to the error position, that is, the position of the key.

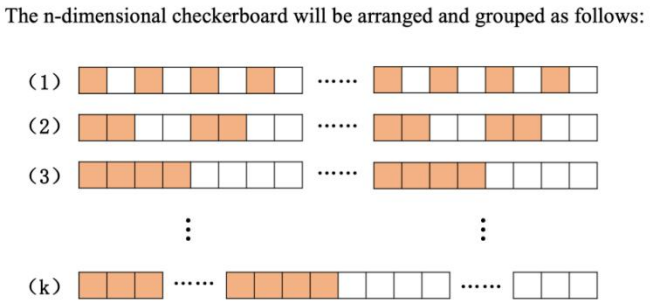



Fig. 1 0 n-dimensional checkerboard parity packet

## 5. Conclusions

This work proposes a universal algorithm based on Hamming code for any dimension PCP. To explore the existence conditions and the structure of the solutions of the PCP, we verify that the parity check and XOR operations agree in Hamming frame. The XOR operation is then used to find the encoded error position, which is the position of the key, based on the entire chessboard is lined up in a straight line according to the rows. It has been shown that the proposed method is effective to solve any dimension PCP. The present study extends the range of applications of the theory of error-correcting codes based on Hamming codes.

## References

[1] Cheng Longxin. The development of error-correcting coding and its application in communication [C], Sichuan Province Communication Society. Proceedings of the 1993 Annual Conference of Sichuan Province Communication Society. 1993:132-140.

[2] C. E. Shannon. A mathematical theory of Communication[J]. Bell System Technical Journal,1948, 27(4): 623-656.

[3] R. G Gallager. Low-density parity-check codes. IRE Transactions on Information Theory, 1963, 8(1): 21-28.

[4] C. Berrou, A. Glavieux and P. Thitimajshima, Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1, Proceedings of ICC '93 - IEEE International Conference on Communications, Geneva, Switzerland, 1993, (2): 1064-1070.

[5] I. S. Reed, G. Solomon. Polynomial codes over certain finite fields[J]. Journal of the Society for Industrial and Applied Mathematics,1960, 8(2): 300-304.

[6] Zhengming Ma. Algebraic structure of convolutional codes [J]. Journal of Sun Yat-sen University, 1992, (02): 88-93.

[7] Zhu Zhixian. Application of generalized Hamming code in data communication coding and decoding [J]. Electronic Technology Application, 1990, (08): 20-24.

[8] Xin Ying. Analysis and application of error correction and detection ability of Hamming code [J]. Journal of Yancheng Institute of Technology (Natural Science Edition), 2008, (01): 34-36.

[9] Yao Youming. Mathematical theory and development of error-correcting codes [J]. Charming China, 2010, (12): 235.

[10] Feng Keqin. Algebraic theory of error-correcting codes. Tsinghua University Press, 2005.