GOLAY CODE AND RANDOM PACKING

YOSHIKI ITOH

(Received Aug. 9, 1985; revised May 21, 1986)

Summary

A random sequential packing by Hamming distance is applied to study Golay code. The probability of getting Golay code is estimated by computer simulation. A histogram of number of packed points is given to show the existence of several remarkable clusters.

1. Random sequential packing by Hamming distance

In this note we give a stochastic algorithm to generate Golay code. There is an effective and beautiful method by finite field theory to construct various codes. Hence our aim is mainly to show a method to study Golay code for the statistician who is not familiar with finite field theory.

Random sequential packing of spheres has been applied by Bernal [1] to study the structure of liquids and has been discussed by Higuti [4], Solomon [15], Tanemura [16] and others. Random sequential packing of one dimensional space is known as a car parking problem. Place unit intervals into the interval [0, x] sequentially at random. Assume that the initial point $\xi$ of the interval $I$ is a random variable uniformly distributed in the interval [0, $x-1$]. If the intervals $I_1, I_2, \ldots, I_k$ have already been chosen, the next randomly chosen interval will be kept only if it does not intersect any of the intervals $I_1, I_2, \ldots, I_k$. In this case this interval will be denoted by $I_{k+1}$. If it does intersect any of the intervals $I_1, I_2, \ldots, I_k$ we neglect it and choose a new interval. The procedure is continued until none of the lengths of gaps generated by the intervals placed in [0, x] is greater than 1. Mathematical studies are carried out by Rényi [12], Itoh [5], [6] and others.

Consider a set of $2^x$ points whose coordinates are 1 or 0 in a Euclidean space of dimension $d$. Euclidean distance is defined between two points of the $2^x$ points. The square of the Euclidean distance in this

Key words and phrases: Random sequential packing, Hamming distance, stochastic algorithm, Golay binary code, clusters of histogram.
case is called the Hamming distance in coding theory. At first we choose one point (d coordinates) at random and we record it. Choose another and record it if its Hamming distance is \( \geq k \), \((k<d)\), otherwise discard it. Now, choose the next point at random and record it if the Hamming distance from each of the 2 points is not less than \( k \), otherwise discard it and choose another point at random. We continue this procedure until there is no possible point to record among the \( 2^d \) points and we now have the number of recorded points (Itoh and Solomon [8]). For the case of Hamming distances of 2 or 3, \( d^{-\alpha} \) fits the simulation results of packing density where \( \alpha \) is an empirical constant. The variance of packing density is larger when \( k \) is even and smaller when \( k \) is odd.

2. Frequency of getting Golay code by a random sequential packing

Leech [9] gave the densest known packing of spheres in 24-dimensional space based on the Golay code, as given by Sloane [14], which is known as one of the most important linear code. Leech used the set of all possible sums of the 12 binary sequences (Fig. 1) where the addition is carried out modulo 2. Hence the set is made up of \( 2^{12} \) or 4096 binary sequences called code words. From each point of the 4096 points, out of the remained 4095 points 759 points have Hamming distance 8, 2576 points have Hamming distance 12, 759 points have Hamming distance 16, and one point has Hamming distance 24. The distribution is the same for each of 4096 points. The proof is given in the book by Thompson [17].

Consider a restricted random sequential packing into the \( 2^{12} \) points.

\[
\begin{array}{cccccccccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1
\end{array}
\]

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0
\end{array}
\]

Fig. 1. Leech's 12 by 24 matrix.
(The 11 trials of 4096 recorded points are not given here.)
At first we choose one point (24 coordinates) at random and we record it. Choose another and record it if its Hamming distance is 8, 12, 16 or 24, otherwise discard it. Now, choose the next point at random and record it if the Hamming distance from each of the previously chosen 2 points is 8, 12, 16 or 24. If the points $I_1, I_2, \ldots, I_k$ are already chosen, the next point $I_{k+1}$ will be chosen if the Hamming distance from each of the previously chosen $I_1, I_2, \ldots, I_k$ is 8, 12, 16 or 24. We continue this procedure until there is no possible point to record among the $2^k$ points and we now have the number of recorded points $N$. This random sequential packing is introduced by Itoh [7]. Here we give histogram of the number of recorded points $N$ in Fig. 2, where there are several clusters (see Itoh [7]). 11 trials out of 550 trials gave 4096 recorded points, that is to say, a code of 4096 code words of length 24 with minimum distance 8 was constructed by the above random sequential packing. Consider the first 13 vectors obtained by a random packing of 4096 recorded points (Fig. 3 (A)). Add the first vector to the other 12 vectors by modulo 2. Then we get the 12 vectors (Fig. 3 (B)). If

**FIRST 13 VECTORS**

| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |

**Fig. 3 (A)**

**ADD THE FIRST VECTOR TO THE VECTORS FROM THE SECOND TO THIRTEENTH**

| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |

**Fig. 3 (B)**

the 12 vectors are linearly independent, the all possible sum of the 12 vectors make the same distribution of Hamming distance to the one generated by the 12 vectors given in Fig. 1. Hence the first 13 vectors are enough to construct a Golay code. It has been shown that
any binary block code with $2^{12}$ code words of length 24 with minimum
distance 8 is equivalent to the one generated by the vectors in Fig. 1
(see MacWilliams and Sloane [10]). Since the works by Golay [2], Ham-
ming [3] and Shannon [13], many works are carried out on coding the-
ory. Golay discovered the code by geometrical consideration. Golay's
original idea introduced in the book by Thompson [17] is not based on
finite field theory. His geometrical discussion is not easy to follow.
The algebraic method to construct the Golay code is given in the book
by Peterson [11]. It may be remarkable that Golay code is constructed
at random without using deterministic construction.

3. Clusters in histogram

There are several evident clusters in the histogram of the recorded
number $N$ in Fig. 2. Here we give a remark on the clusters.

In our random packing the first point $I_1$ is recorded at random from
the $2^{12}$ points. The second point $I_2$ is recorded at random from the
points which have the Hamming distance 8, 12, 16 or 24 from the
point $I_1$. The $k$-th point $I_k$ is recorded at random from the points which
have the Hamming distance 8, 12, 16 or 24 from each of the previously
recorded $I_1, I_2, \cdots, I_{k-1}$. Consider the distribution of the number of
points which have the Hamming distance 8, 12, 16 or 24 from each of
the 12 points $I_1, I_2, \cdots, I_{12}$. Let $X$ be the number. We consider the
simulation of the 550 trials given in Fig. 2. Out of the 550 trials, 9
trials produced $X=4084$. The 9 trials have the recorded number of

![Fig. 4. The first 12 points and the clusters.](image-url)
points, $N=4084+12=4096$. There were 306 trials for which $X<4084$, and 235 trials for which $X>4084$. When $X>4084$, it is supposed that the 12 vectors, which represent the first 12 points, are not linearly independent. Hence we limit our analysis to the trials for which $X<4084$. We plot $(N,X)$ for each of the 306 trials in Fig. 4, which shows that the first 12 points roughly determine the recorded number $N$ and the cluster in the histogram in Fig. 2.

Acknowledgement

The author is grateful to Dr. N. Niki who provided him with a computer program in machine language to calculate Hamming distance. He is also grateful to Miss Suzu Ishihara for programming the simulation.

This study was carried out under the ISM Cooperative Research Programs 85-ISMCRP-2, and 85-ISMCRP-13,

THE INSTITUTE OF STATISTICAL MATHEMATICS

REFERENCES