COMBINATORIAL CONSTRUCTIONS

SARTHAK BAL MITRA

1. Introduction

Problem Statement:
There is a famous Error Correcting Code known as the Hamming Code, it is a known result that the length 7 Hamming Code can be constructed from the game of NIM. Can this construction be generalised? To study Golay Codes and the game of Turning Turtles.

Pre-requisites:
What N and P positions of an Impartial Game are. How to play NIM.

2. Binary Codes

To understand more about the relation between impartial games and Error Correcting Codes, we take a look into Binary Codes.

Definition 2.1. Binary Code: A binary [n,k,d] code is a code that corrects strings of length n that contains 2^k code words, where k is known as the dimension of the code, with a Hamming distance of d.

There are obvious constraints on the relation between n,k,d. For example the Hamming Code with length 7 which can correct 1 error will have a maximum of $\frac{2^7}{8} = 2^4 = 16$ code words. Using the notation above, it is represented as $[7, 4, 3]$.

A useful thing to know is what your Hamming distance should be in relation to the number of errors produced. We have seen that the $[7, 4, 3]$ Hamming Code can correct a maximum of 1 error. Generally we see that:

Theorem 2.2. *A binary code having a Hamming distance d can correct $floor(d-1/2)$ errors. (This can also be stated as: to correct q errors, you need to have a Hamming distance of at least 2q+1.)*

Proof: Assume a Hamming distance of 2q is sufficient. Consider two code words 0000..00 with $> 2q + 1$ 0's and 00..01..111 with 2q 1's in the beginning (from the right). Note that these are the first two lexicographic codes with a Hamming distance of 2q. According to our assumption, this should be able to differentiate any string with up to q errors.

Now consider the string (after distortion) 00..01..11 with just q 1's at the beginning. We realise that there is no way of figuring out whether this is the first code word with q 0's distorted to q 1's or the second code word with q 1's distorted to q 0's.

Date: July 2021.

Lets take a look at a Hamming distance of 2q + 1: Consider a similar arrangement with two code words being the first two lexicographic codes with a Hamming distance of 2q + 1. Now the (worst case) distorted string is all 0's except the right-most q places with 1's; we can deduce that the original string was the first code word since it would require q+1 errors for it to have originated from the second code word, similarly if you consider a distorted string with q+1 1's in the right-most positions and 0 everywhere else, you'll know that its from the second code word.

We now look at the Binary Golay Code.

Definition 2.3. The Binary Golay Code is a perfect binary code $[23, 12, 7]$ which corrects up to 3 errors. There is a Ternary Golay Code as well (in base 3 or a code with digits 0,1,2) $= [11, 6, 5]$ which corrects up to 2 errors, but this contains 3^6 code words as it is Ternary. The Extended Binary Golay Code is the Binary Golay Code with a parity/check bit $= [24, 12, 8]$.

One of the most well-known appearance of the Binary Golay Code is in the Voyager 1 and 2 spacecrafts. The spacecrafts sent 100's of coloured pictures of Jupiter and Saturn and they had a constrained telecommunication bandwidth to work with. The standard Reed-Muller Code was always used for Black and White Images but for coloured, which required the transmission of 3 times the amount of data, the Extended Binary Golay Code was used!

We will now see that the Binary Golay Code can be constructed with the game Mogul, which generally is known as the game Turning Turtles. We will also see that the Extended Binary Golay Code can be constructed with a variant of Mogul.

3. Turning Turtles and The Construction

Definition 3.1. Turning Turtles is a generalisation of NIM and is played like so. There are n turtles in a row, some might be on their backs. There is a positive integer f and on your turn you have to flip at most f turtles with the left most turtle being flipped from its back to its feet. Let us denote a Turning Turtle game with (n,f).

Note that:
NIM is Turning Turtles with f = 2.
Mogul is Turning Turtles with f = 6, n = 23.
The variant of Mogul which creates the Extended Binary Code is Turning Turtles with f= 7, n = 24.

Theorem 3.2. *P positions of Turning Turtles are lexicographically first with positions which are different in at least f+1 places.*

Proof: For a Turning Turtles Game (n,f); We note that since we can flip at most f turtles, we cannot have any 2 P positions be different only in f places since then you would be able to go from a P position to the other. This does not respect the Partition Theorem and hence, we see that P positions will always be different in at least f+1 places.

To prove that P positions are lexicographically first, we use induction. Assuming that the current P positions are lexicographically different in f+1 places, we see that the next lexicographic position with f+1 different places is also a P position. By the Partition Theorem, we need every move from this to be an N position. Since we have already proved that if two

positions are different in f+1 places, you cannot move from one to the other; we see that all moves are to an N position. Hence proven.

We can similarly show that the code words of an [n,k,d] Binary Codes are lexicographically first with a difference in d bits.

Note that the way we "convert" Turning Turtle games to their binary representation, is by adding a weight from numbers 1 to n from the 1st turtle to the nth turtle (the turtles act as heaps), and using the nim-sum operation you can always reduce the weight of a certain turtle. The turtles facing right side up are 1's and the turtles flipped upside down are 0's. We now have our result:

Theorem 3.3. *P positions of a Turning Turtles Game (n,f) are the same as the code words for a Binary Code (n,k,d = f+1).*

Example: Consider the game Mogul which is Turning Turtles (23,6). The P positions will be the code words of length 23 and with a Hamming Distance of 7 = 6+1, hence; creating the [23,12,7] Binary Golay Code. Similarly the [24,12,8] Extended Binary Golay Code is created from Mogul (24,7).

You might be thinking, if I want to make a Binary Code, how can I? You would need the code words or the P positions of the respective game. If let's say you have some trivial P positions. You could come up with more by the following method.

Theorem 3.4. *The sum of any 2 P positions gives you a P position. This would imply, the NIM-SUM of two code words is also a code word.*

Proof: Let's say G and H are two P positions. In G+H, I can either move in G or in H. Say I start in G, this leads to an N position in G and a P position in H. You would then play the winning move in G back to a P position to again give me a sum of P positions. The same would apply if I started in H. Doing this recursively we can see that eventually it will be my turn to play in $G_n + 0$ or $0 + H_n$ where G_n and H_n are sub - P positions of G and H respectively. You will continue to win that game and therefore G+H is also a P position.