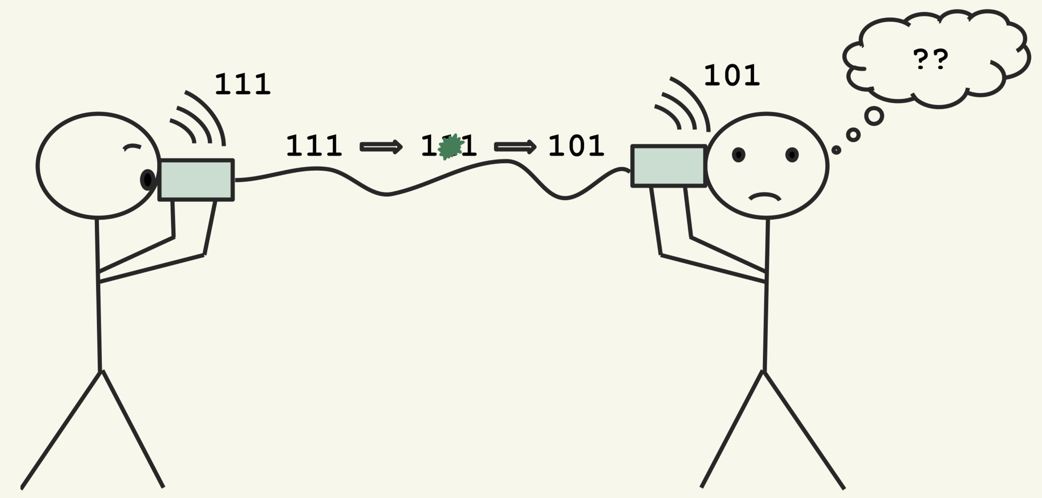
Counting Codes via the Container Method

Amy Penney, Supervised by Dr. Natasha Morrison

University of Victoria

Department of Mathematics and Statistics, University of Victoria

Why Use an Error Correcting Code?[8]



Suppose we want to communicate using binary strings of length n. We will call the set of strings that represent valid messages our *code*, and each string in the code a *codeword*. While our messages are in transit, some bits may be flipped from a 0 to a 1, or from a 1 to a 0. We would like to be able to correct such errors.

What is a t Error Correcting Code?[8,3]

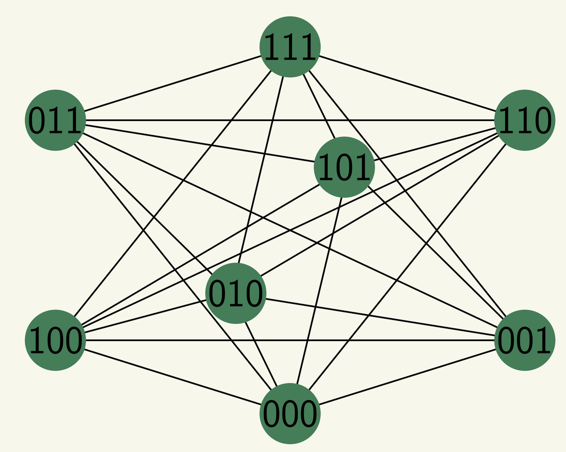
A t-error correcting code guarantees that, as long as no more than t errors occur, the receiver will always be able to recover the sent message.

Take any $x, y \in \{0,1\}^n$. The *Hamming distance* between these words, $d(x,y)$, is the number of bit positions in which they differ. Upon receiving a word not in the code, we will correct it to the codeword at minimum Hamming distance from it. In order to correct many errors, we need our codewords to be far apart. In particular, C is a t-error correcting code if and only if $\min\{d(x,y) : x, y \in C\} > 2t$.

How Can We Count the Number of t Error Correcting Codes?

Counting the number of t error correcting codes is equivalent to **counting** the number of **independent sets** of a particular graph.[3]

Let G be the graph with vertex set $\{0,1\}^n$, where there is an edge between u, v if and only if $d(u,v) \le 2t$. The number of t error correcting codes equals the number of independent sets in G.[3]



Example with $n = 3$, $t = 1$.

What is the Container Method?

The container method is a technique used to **upper bound** the number of **independent sets** of a graph.

The graph container algorithm and the idea of the container method originated from Kleitman and Winston[5,6], and Sapozheko[10]. It was developed in full generality and extended to hypergraphs independently by Saxton and Thomason[11], and Balogh, Morris and Samotij[1].

What Do We Need to Apply the Container Method?

To use the container method, we must prove that if a subgraph has 'slightly more' vertices than the largest independent set, then it contains 'a lot' of edges.[3]

This is known as a *supersaturation result*. It tells us that any subgraph with 'few' edges must contain 'few' vertices. Sometimes, to get the desired upper bound, we need two supersaturation results.[3]

How Does the Container Method Work?

First we run a graph container algorithm to create a collection of subgraphs, called *containers*, with the following properties:

1. Every independent set is contained in some container.
2. There are 'few' containers.
3. There are 'few' edges in each container.

As every independent set is in a container, the sum of the number of subsets of each container upper bounds the number of independent sets. Since there are 'few' containers, each with 'few' edges (and thus, by the supersaturation result, 'few' vertices), this upper bound is not too large.

What Results Have Been Proven?

Let $H(n,t) = 2^n / \left(\sum_{k=0}^{t} \binom{n}{k}\right)$. (This is an upper bound on the size of a t error correcting code.[3]) Using the container method, Balogh, Treglown and Wagner[3] proved the following result.

Theorem ([3]). Let $t = t(n) \ll \sqrt[3]{\frac{n}{\log^2 n}}$. Then there are at most $2^{H(n,t)(1+o(1))}$ t error correcting codes.

What are r-(n,k,d) Codes?[4]

Let $\mathcal{Y}^{(r)} = \{(X_1, \ldots, X_r) : X_1, \ldots, X_r \in [n]^{(k)},\ X_1, \ldots, X_r \text{ pairwise disjoint}\}$. For $A = (A_1, \ldots, A_r), B = (B_1, \ldots, B_r) \in \mathcal{Y}^{(r)}$, the distance between A, B is

$$d(A,B) = \min_{\pi \in S_r} \sum_{i=1}^{r} |A_i \setminus B_{\pi(i)}|.$$

An r-(n,k,d) code is a set $C \subseteq \mathcal{Y}^{(r)}$ such that any two elements in C have distance at least d. Using the container method, [3] proved an upper bound on the number of 2-(n,k,d) codes.

What is the Goal of This Project?

The goal of this project is to generalize previous results to count the number of r-(n,k,d) codes.

By generalizing the supersaturation results and container method application in [3], we hope to bound the number of r-(n,k,d) codes.

This research was supported by the Jamie Cassels Undergraduate Research Award, University of Victoria.

References

UVic logo obtained from https://www.uvic.ca/brand/look-feel/logo/index.php.
All other images are my own.

[1] József Balogh, Robert Morris, and Wojciech Samotij. "Independent sets in hypergraphs". In: *J. Amer. Math. Soc.* 28.3 (2015), pp. 669–709. URL: https://doi.org/10.1090/S0894-0347-2014-00816-X.

[2] József Balogh and Šárka Petříčková. "The number of the maximal triangle-free graphs". In: *Bull. Lond. Math. Soc.* 46.5 (2014), pp. 1003–1006. URL: https://doi.org/10.1112/blms/bdu059.

[3] József Balogh, Andrew Treglown, and Adam Zsolt Wagner. "Applications of graph containers in the Boolean lattice". In: *Random Structures Algorithms* 49.4 (2016), pp. 845–872. URL: https://doi.org/10.1002/rsa.20666.

[4] Béla Bollobás et al. "A coding problem for pairs of subsets". In: *Geometry, structure and randomness in combinatorics*. Vol. 18. CRM Series. Ed. Norm., Pisa, 2015, pp. 47–59.

[5] Daniel J. Kleitman and Kenneth J. Winston. "On the number of graphs without 4-cycles". In: *Discrete Math.* 41.2 (1982), pp. 167–172. URL: https://doi.org/10.1016/0012-365X(82)90204-7.

[6] Daniel J. Kleitman and Kenneth J. Winston. "The asymptotic number of lattices". In: *Ann. Discrete Math.* 6 (1980), pp. 243–249.

[7] Robert Morris. *The Method of Hypergraph Containers.* https://www.ime.usp.br/~spschool2016/wp-content/uploads/2016/07/Morris.pdf.

[8] Natasha Morrison. "Math 322". Material taught in this course. 2022.

[9] Jonathan A. Noel. "Math 426/529: Extremal Combinatorics". In: Course notes, https://www.math.uvic.ca/~noelj/ExtremalCombinatorics202409.pdf. 2023, pp. 95–98.

[10] A. A. Sapozhenko. "On the number of independent sets in extenders". In: *Diskret. Mat.* 13.1 (2001), pp. 56–62. URL: https://doi.org/10.1515/dma.2001.11.2.155.

[11] David Saxton and Andrew Thomason. "Hypergraph containers". In: *Inventiones mathematicae* (2012), pp. 1–68.

[12] Yufei Zhao. "Probabilistic Methods in Combinatorics". In: Lecture notes, https://live.ocw.mit.edu/courses/18-226-probabilistic-method-in-combinatorics-fall-2020/mit18_226f20_lec25.pdf. Massachusetts Institute of Technology, 2020. Chap. 11, pp. 144–152.

March 9, 2024