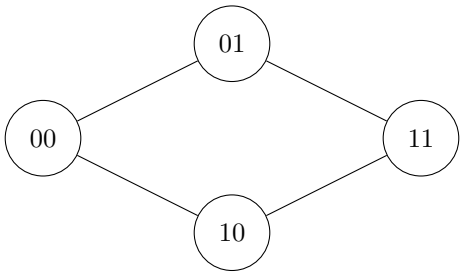
An Introduction to Steiner Systems

Gabriel Ma

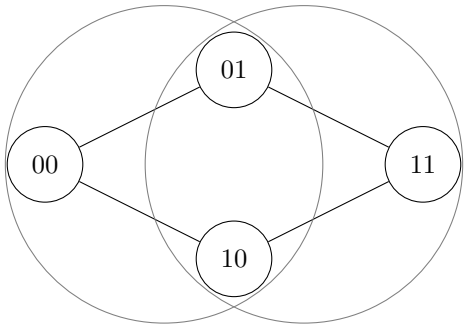
November 7, 2024

1 Motivation

Suppose I want to transmit a yes/no message in binary. I could send one bit, where 1 represents yes and 0 represents no. This would work if noise wasn't a thing. Due to potential interference when transmitting messages, there's a chance that my 1 may turn into a 0 or my 0 may turn into a 1. We call this a **bit flip**. Perhaps I could try sending two bits, where 11 represents yes and 00 represents no. Now if there's a bit flip, my message becomes 10 or 01. If the person I'm sending the mssage to knows that I'm only sending 11 or 00, then recieving a 10 or 01 automatically indicates a transmission error. However, it isn't possible to fix this error, so the code I sent is an **error-detecting code**. To visualize why such a code isn't fixable, consider the following graph:

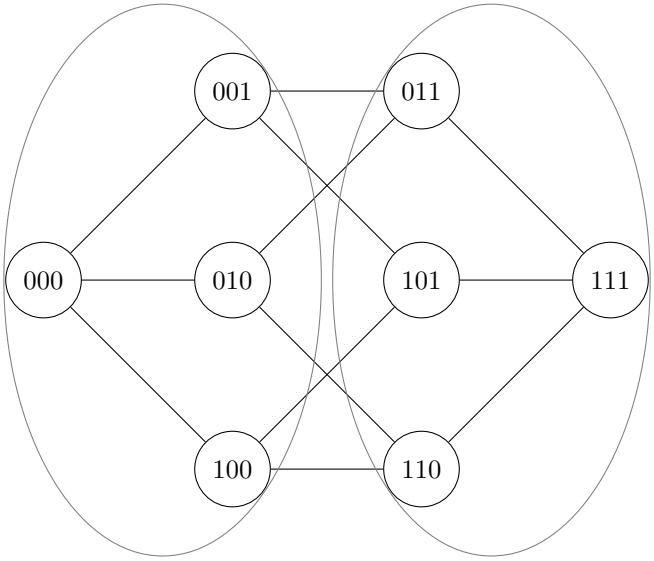


The distance between two codes is called **Hamming distance** and is calculated by counting the minimum number of bit flips needed to go from one message to another. We will refer to Hamming distance as just distance for convenience. On the graph above, each point represents a possible message, and each line connects messages with distance 1. If we were to draw a circle that encompases all messages at most a distance one away from 00 and another encompasing all messages at most a distance one away from 11, we get overlapping circles.



Due to this overlap, we cannot trace 01 and 10 back to its original message. However, let's add a third bit, where 111 represents yes and 000 represents no. If we draw a graph of all possible messages, and draw

elipses that encompas messages at most one distance away from 111 and 000 respectively, we get the graph below.



Because these elipses don't overlap, we can fix the case where one bit flip occures during transmission. If my reciever gets 010, the message can be turned back to 000 and my original message would be successfully recieved. This is an **error-correcting code**. To be able to fix more than one bit flip, we need more complicated codes. Another way to see this is that if two of the numbers in my code is a 0, then the third should also be a 0. If two of them are 1, then the remaining one should be 1. In this sense, we're ok with having some overlap because all codes other than 000 or 111 have both 0 and 1 in them. We just don't want too much overlap. Often we want to send a message more complicated than a simple yes/no. To build an error-correcting code for these scenarios, the idea remains the same: we want to construct sets that don't overlap much.

2 Defining a Steiner System

Consider the numbers $t = 2, k = 3, n = 7$. Suppose we have a set Ω with $n = 7$ elements. WLOG, let

$$\Omega = \{1, 2, 3, 4, 5, 6, 7\}$$

Suppose we take $x, y \in \Omega$ s.t. $x \neq y$. We can certainly find $B \subset \Omega$ of size $k = 3$ that contains both x and y (just take $B = \{x, y, z\}$ for any $z \in \Omega \setminus \{x, y\}$). But what if we wanted a collection of subsets of Ω, each with size 3, s.t. any $t = 2$ numbers we choose from Ω is contained in exactly one of the subsets in our collection? Is this even possible? Let's give it a shot.

To begin our construction, consider the pair of numbers $1, 2 \in \Omega$. We know these numbers must be contained in some subset of size 3, so let's just use $B_1 = \{1, 2, 3\} \subset \Omega$. To keep track of what we're building, let's list elements of Ω on the left-most column of a table, and gradually fill in our blocks using other columns. Since we just constructed B_1, we can list its elements as follows:

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1						
2	2						
3	3						
4							
5							
6							
7							

The pair $1, 3$ also exists in B_1, so we can move on to $1, 4$. The block B_2 that contains $\{1, 4\}$ cannot also contain 2 or 3 beacuse then the pair $1, 2$ or $1, 3$ would also be in B_2. Thus, let's let $B_2 = \{1, 4, 5\}$.

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	1					
2	2						
3	3						
4		4					
5		5					
6							
7							

The pair $1, 5$ also exists in B_2, so let's consider $1, 6$. By similar reasoning above, this time we're forced to have $B_3 = \{1, 6, 7\}$.

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	1	1				
2	2						
3	3						
4		4					
5		5					
6			6				
7			7				

Since all pairs involving the number 1 have now been considered, any additional block in cannot contain 1 because then we'd have a pair of numbers that are contained in more than one block. The pair $2, 3$ is already contained in B_1, so consider the pair $2, 4$. B_4 cannot contain 3 or 5 because then we'd get a pair of numbers contained in multiple blocks, so let's let $B_4 = \{2, 4, 6\}$.

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	1	1				
2	2			2			
3	3						
4		4		4			
5		5					
6			6	6			
7			7				

The pair $2, 5$ is yet to be in a block. To avoid letting pairs exist in multiple blocks, we're forced to have $B_5 = \{2, 5, 7\}$.

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	1	1				
2	2			2	2		
3	3						
4		4		4			
5		5			5		
6			6	6			
7			7		7		

We can follow similar reasoning, first considering the pair $3, 4$ then $3, 5$ to get $B_6 = \{3, 4, 7\}$ and $B_7 = \{3, 5, 6\}$.

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	1	1				
2	2			2	2		
3	3					3	3
4		4		4		4	
5		5			5		5
6			6	6			6
7			7		7	7	

So now we have a collection $\mathcal{B} = \{B_1, \ldots, B_7\}$ s.t. $\forall x, y \in \Omega \; \exists! B_i \in \mathcal{B}$ s.t. $\{x, y\} \subset B_i$. This leads us to the definition of a Steiner system:

A **Steiner system** $S(t, k, n)$ is a set Ω of size n and a collection $\mathcal{B}$ of blocks B where each block is of size k s.t. any t elements of Ω is contained in a unique $B \in \mathcal{B}$, where $t < k < n$.

Why require strict inequalities? If $t = k$, then we'd require every k elements of Ω to be contained in a unique block of size k. The corresponding Steiner system would be the set of all subsets of size k, which isn't that interesting. Being able to easily find the Steiner system in this case is boring, so we don't allow $t = k$. Meanwhile, if $k = n$, then that's the same as requiring a collection of blocks where each block has the same size as Ω. The corresponding Steiner system would be Ω itself. This is also boring (more boring than the $t = k$ case I'd say), so we don't allow $k = n$.

3 Existence of Steiner Systems

It is important to note that Steiner systems don't always exist. Consider the case where $t = 1, k = 2, n = 3$. Here,

$$\Omega = \{1, 2, 3\}$$

The number 1 must be conatined in a block of size 2, so let's let $B_1 = \{1, 2\}$. The number 3 must also be in a block of size 2. But any B_2 must contain either 1 or 2, both of which are already in B_1. Hence we're forced to have a number present in both blocks, so $S(1, 2, 3)$ doesn't exist.

Given this result, it may be of interest to know some theorems concerning existence of Steiner systems. Below are a few results:

Theorem 1. If $S(t, k, n)$ exists, then $S(t - 1, k - 1, n - 1)$ exists

Proof : Choose any element $x \in \Omega$. Remove all blocks in $\mathcal{B}$ that don't contain x. The remaining blocks satisfy the following: for any t elements of Ω, one of which is x, there exists a unique block $B \in \mathcal{B}$ that contains those t elements. Now remove x from Ω and all blocks in $\mathcal{B}$. Ω now contains $n-1$ elements, each block has size $k-1$, and every $t-1$ elements in Ω is contained in a unique $B \in \mathcal{B}$, so we have the Steiner system $S(t-1, k-1, n-1)$.

□

This theorem is useful for proving that certain Steiner systems don't exist. For instance, if $S(1000, 1001, 1002)$ exists, then applying theorem 1 999 times tells us that $S(1, 2, 3)$ should exist, but we showed earlier that it doesn't, so $S(1000, 1001, 1002)$ doesn't exist. It can also be useful for proving existence of certain Steiner systems, but that's harder. If we want to show that $S(t, k, n)$ exists, then it is also valid to show that $S(t+i, k+i, n+i)$ exists for some i because then we can apply theorem 1 i times.

Theorem 2. If $S(t, k, n)$ exists, then $\binom{k}{t}$ divides $\binom{n}{t}$.

Proof : $\binom{k}{t}$ is the number of t-subsets (subsets of size t) in a block. Let b be the total number of blocks. Then the total number of distinct t-subsets in the collection of blocks is $b\binom{k}{t}$. Since each block is itself a subset of Ω, each of these t-subsets exist in Ω. But Steiner systems require each t-element subset to appear exactly once within the collection of blocks. Thus

$$b\binom{k}{t} = \binom{n}{t}$$

so

$$\frac{\binom{n}{t}}{\binom{k}{t}} = b \in \mathbb{Z}$$

□

The contrapositive of theorem 2 tells us that if $\binom{k}{t}$ doesn't divide $\binom{n}{t}$, then we shouldn't bother looking for $S(t, k, n)$ because it doesn't exist.

In fact, we can strengthen our knowledge of which Steiner systems exist or don't exist by combining theorems 1 and 2.

Remark. If $S(t, k, n)$ exists then $\binom{k-i}{t-i}$ divides $\binom{n-i}{t-i}$ for all $i = 0, 1, \ldots, t-1$.

Proof : By continued application of theorem 1, we know that $S(t-i, k-i, n-i)$ exists for all $i = 0, 1, \ldots, t-1$. Apply theorem 2 to each of these Steiner systems to get the desired result.

□

Now what about a theorem that makes it easy to prove existence? There is a result I find quite interesting. A **Steiner triple system**, abbreviated STS, is where we fix $t = 2$ and $k = 3$. The example $S(2, 3, 7)$ that we constructed in section 2 is an example of a STS.

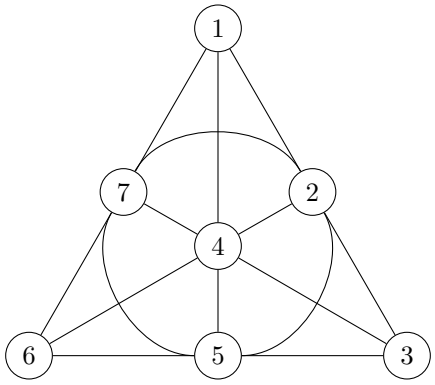
Kirkman's Existence Theorem. A STS exists iff $n \equiv 1 \pmod 6$ or $n \equiv 3 \pmod 6$.

Proof : See Steiner and Kirkman Triple Systems

□

4 Finding blocks containing a given t-subset

Given the existence of certain Steiner systems, we might want to identify the unique block that contains some t-subset. Why is this question interesting? From the pure math perspective, the uniqueness of blocks that contain any given t-subset is the key property of Steiner systems, so understanding the blocks lets us understand Steiner systems. From the applied math perspective, uniqueness of blocks is kinda like an error-correcting code. If a Steiner system is in some way your code, then if you recieve a set of messages you want to be able to quickly correct it. For example, if someone is sending you a message obeying $S(2,3,7)$, then if you get the coded message $4,7$ you want to be able to fix it to the closest valid code word (which is 3). During our construction of $S(2,3,7)$ at the beginning of section 2, we started with the pair $1,2$ and made $B_1 = \{1,2,3\}$. Other blocks were made by considering different pairs of numbers, and everything was arranged in a table. Looking through a table isn't bad for "small" Steiner systems, but they can get quite large so it is of interest to look at other visualizations. It turns out we can arrange the blocks of $S(2,3,7)$ into what's called a **Fano plane**.



Given a pair of numbers, we can use this plane to find the other number in the unique block containing our originally chosen numbers. For example, the pair $4,7$ forms a line on the plane, so we trace that line to see that 3 is the other number. Thus the pair $4,7$ is contained in the block $\{3,4,7\}$. The numbers $3,6$ also form a line on the Fano plane, which we trace to see that 5 is the missing number. So the pair $3,6$ is contained in the block $\{3,5,6\}$. Meanwhile, the pair $2,5$ is on a circle. We trace the circle to conclude that the pair $2,5$ is contained in the block $\{2,5,7\}$.

In the case of $S(5,8,24)$, there's a diagram called the **Miracle Octad Generator**, abbreviated MOG, that serves a similar purpose as the Fano plane: given any 5 elements, the diagram lets you identify the remaining 3 elements in the block that contains those 5 elements. You may read more about it here: A new combinatorial approach to M_{24}. The MOG is figure 4 of that paper.

5 Uniqueness of Steiner Systems

At the beginning of section 2 when we made B_1, we could have easily picked a different element (though this would influence valid choices for other B_i). We didn't have to have $B_1 = \{1,2,3\}$. For example, an equally valid $S(2,3,7)$ is shown below.

Ω	B'_1	B'_2	B'_3	B'_4	B'_5	B'_6	B'_7
1	1	1	1				
2	2			2	2		
3		3		3		3	
4			4		4	4	
5		5			5		5
6	6					6	6
7			7	7			7

Recall that in section 2 we derived the following table:

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7
1	1	1	1				
2	2			2	2		
3	3					3	3
4		4		4		4	
5		5			5		5
6			6	6			6
7			7		7	7	

Is the Steiner system $\mathcal{B}' = \{B'_1, \ldots, B'_7\}$ different from $\mathcal{B} = \{B_1, \ldots, B_7\}$? The elements themselves are different, but since the elements are arbitrary maybe it's possible to relabel them so that the two tabular visualizations of $S(2, 3, 7)$ look identical. If such relabelling is possible, we call these two Steiner systems **isomorphic**. There are two actions we're allowed to perform on these tables. Since the order in which blocks appear in $\mathcal{B}$ is arbitrary, we can permute their order, which corresponds to permuting columns in the table. Since relabelling of elements must result in all elements being represented, we are allowed to permute rows of the table. So, if we can permute columns and rows of the table representing $\mathcal{B}'$ such that the result looks like the table representing $\mathcal{B}$, then we can say that our two Steiner systems above are isomorphic. In this case, such permutations are possible (proof left to the reader as an exercise).

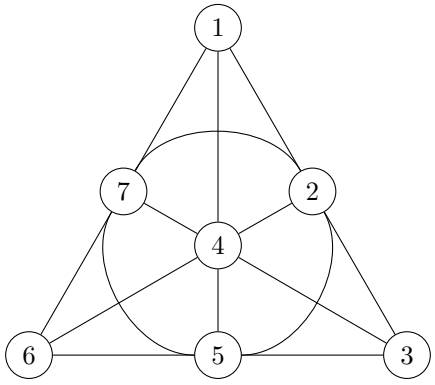
However, two representations of a Steiner system need not be isomorphic. Consider $S(2, 3, 13)$. We can have the following collection of blocks:

Ω	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}	B_{16}	B_{17}	B_{18}	B_{19}	B_{20}	B_{21}	B_{22}	B_{23}	B_{24}	B_{25}	B_{26}
1	1	1	1	1	1	1																				
2	2						2	2	2	2	2															
3	3											3	3	3	3	3										
4		4					4					4					4	4	4							
5		5						5					5							5	5	5				
6			6				6							6						6			6	6		
7			7					7							7		7								7	7
8				8					8							8	8				8		8			
9				9						9		9										9		9	9	
10					10				10					10				10				10				10
11					11						11				11				11		11			11		
12						12				12						12			12	12						12
13						13					13		13					13					13		13	

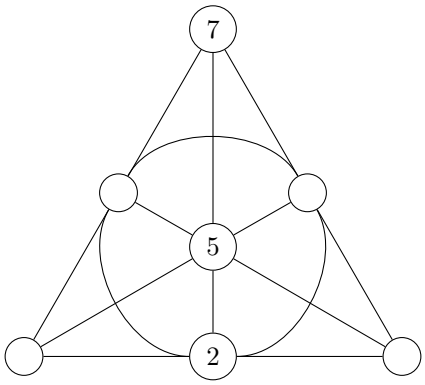
Ω	B'_1	B'_2	B'_3	B'_4	B'_5	B'_6	B'_7	B'_8	B'_9	B'_{10}	B'_{11}	B'_{12}	B'_{13}	B'_{14}	B'_{15}	B'_{16}	B'_{17}	B'_{18}	B'_{19}	B'_{20}	B'_{21}	B'_{22}	B'_{23}	B'_{24}	B'_{25}	B'_{26}
1	1	1	1	1	1	1																				
2	2						2	2	2	2	2															
3	3											3	3	3	3	3										
4		4					4					4					4	4	4							
5		5						5					5							5	5	5				
6			6				6							6						6			6	6		
7			7					7							7		7								7	7
8				8					8							8	8				8		8			
9				9						9			9					9						9	9	
10					10				10					10					10			10			10	
11					11						11	11									11			11		11
12						12				12						12			12	12						12
13						13					13				13			13				13	13			

Within the first row, the red cells indicate columns that differ between the two tables, while green indicates columns that are identical. We cannot permute the columns nor rows to fix the red columns without messing up columns that are already the same.

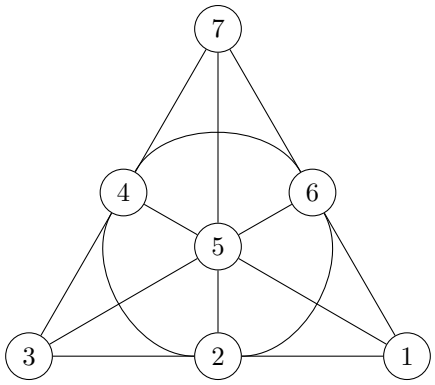
So we now know we can have Steiner systems with the same t, k, n values that are and aren't isomorphic. What about our Fano plane? Could we have placed numbers differently so that blocks are conserved? Suppose we're working with the Steiner system $S(2, 3, 7)$ as constructed from section 2, so $\mathcal{B}$ is fixed. Recall that the Fano plane I showed earlier in section 4 is as follows:



Pick any spot on the Fano plane. There are 7 choices of numbers that can go in the chosen spot. Pick any remaining spot on the Fano plane. There are 6 choices of numbers that can go in the chosen spot. But now there must be a block containing the two numbers, so the location of a third number is fixed. That number goes in the unique spot that shows up as a block on the Fano plane. For example, if we placed 7 at the top and 5 in the middle, then 2 must go at the bottom niddle.



Now pick an unoccupied spot. There are 4 numbers left that can go there. Placing that number on the Fano plane ends up completely defining where everything else must go (try it for yourself), so we've exhausted all possible permutations. For instance, if we placed 1 on the bottom right, we're forced to have



The total number of block-preserving permutations is therefore

$$7 \times 6 \times 4 = 168$$

6 Connections to Other Fields of Mathematics

I mention a few here. There's probably more connections I'm unaware of.

6.1 Coding Theory

The **Extended Binary Golay Code** is a code that encodes 12 bits of data in 24-bit chunks in a way that all valid code words are a distance 8 away. This means that it enables the reciever to accurately correct up to 3 bit flips per chunk of code. The **weight** of a code word is the number of 1 it has, so the code word

$$110100010110110101011000$$

has weight 12. It can be shown that the weight of valid code words for the extended binary golay code is either 0, 8, 12, 16, or 24. In particular, there are 759 code words of weight 8. But notice that

$$\frac{\binom{24}{5}}{\binom{8}{5}} = 759$$

so due to theorem 2 we might think that $S(5, 8, 24)$ is somehow linked here. It turns out that code words of weight 8 in the extended binary golay code forms a steiner system $S(5, 8, 24)$. This code was used on Voyager 1 to send pictures of Jupiter and Saturn during its flyby of those planets. Error correction was extremely important because Voyager 1 has basically no memory (only 70 kilobytes), so once it sends the image, that data is gone. If the image recieved on Earth can't be fixed, we can't ask Voyager 1 to send it again. See The Hidden Geometry of Error-Free Communication and Constructions of the Golay Codes: A Survey for more detail.

6.2 Group Theory

The classification of finite simple groups is one of the biggest achievements in algebra and revealed four infinite classes of groups that all except 26 groups can be categorized into. Among the 26 sporadic groups, 5 of them are known as **Mathieu groups**. It turns out that the generators of the Mathieu groups can be used to construct Steiner systems. In particular, the generators of M_{24} can construct the blocks of $S(5, 8, 24)$. See Generating the Mathieu groups and associated Steiner systems for more detail.

6.3 Sphere Packing

Sphere packing is a problem where you have a bunch of spheres and you want to shove as many of them into a given space as possible. We're usually interested in the density of spheres, meaning the proportion of volume it takes up relative to its container. The probablem can be formally stated as follows: How can n-spheres be positioned in $\mathbb{R}^n$ such that none are overlapping (though they may be tangent) and the volume of $\mathbb{R}^n$ covered by the spheres is maximal? This question is an active area of research, with many unanswered questions. Interestingly, the blocks of $S(5, 8, 24)$ can be used to form **Leech's lattice**, which can then be used to create the densest known sphere packing in 24 dimensions. An Introduction to S(5,8,24) provides more detail on this and Coding theory and Group theory.

6.4 Design Theory

A statement I've heard a few times is "for any concept you learn in math, there's always a generalization of it." This statement definitely holds true for Steiner systems. Steiner systems are a special case of **Balanced Incomplete Block Designs**, abbreviated BBID, which are studied heavily in design theory. Sometimes in life science research it isn't possible to perfectly control for every confounding variable. For instance, maybe you wanna test 3 brands of eye drops, but since each person only has 2 eyes, you can only test 2 eye drops per person (one in each eye). If you only want 1 datapoint per brand, then that's the same as trying to construct $S(1, 2, 3)$, which we know from section 2 doesn't exist. However, what if we relaxed the key condition of a Steiner system? Instead of each t-subset being contained in exactly 1 block, what if we required each t-subset to be contained in exactly r blocks? In our eyedrop example, we can get 2 datapoints per brand by giving one participant brands A and B, participant number 2 gets brands C and A, then participant number 3 gets brands B and C. BBIDs also have theorems regarding their existence, uniqueness, etc. See Balanced Incomplete Block Designs for more detail.